



Al Fairuz, Mohamed Ali Suleiman (2011) *An Investigation into the Usability and Acceptability of Multi-channel Authentication to Online Banking Users in Oman*. PhD thesis.

<http://theses.gla.ac.uk/3078/>

Copyright and moral rights for this thesis are retained by the author

A copy can be downloaded for personal non-commercial research or study, without prior permission or charge

This thesis cannot be reproduced or quoted extensively from without first obtaining permission in writing from the Author

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the Author

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given

An Investigation into the Usability and Acceptability of Multi-channel Authentication to Online Banking Users in Oman



University of Glasgow | School of
Computing Science

Mohamed Ali Al-Fairuz

Ph.D.

2011

School of Computing Science

Collage of Information and Mathematical Sciences

Abstract

Authentication mechanisms provide the cornerstone for security for many distributed systems, especially for increasingly popular online applications. For decades, widely used, traditional authentication methods included passwords and PINs that are now inadequate to protect online users and organizations from ever more sophisticated attacks.

This study proposes an improvement to traditional authentication mechanisms. The solution introduced here includes a one-time-password (OTP) and incorporates the concept of multiple levels and multiple channels – features that are much more successful than traditional authentication mechanisms in protecting users' online accounts from being compromised.

This research study reviews and evaluates current authentication classes and mechanisms and proposes an authentication mechanism that uses a variety of techniques, including multiple channels, to resist attacks more effectively than most commonly used mechanisms. Three aspects of the mechanism were evaluated:

1. The security of multi-channel authentication (MCA) was evaluated in theoretical terms, using a widely accepted methodology.
2. The usability was evaluated by carrying out a user study.
3. Finally, the acceptability thereof was evaluated by asking the participants in study (2) specific questions which aligned with the technology acceptance model (TAM).

The study's analysis of the data, gathered from online questionnaires and application log tables, showed that most participants found the MCA mechanism superior to other available authentication mechanisms and clearly supported the proposed MCA mechanism and the benefits that it provides.

The research presents guidelines on how to implement the proposed mechanism, provides a detailed analysis of its effectiveness in protecting users' online accounts against specific, commonly deployed attacks, and reports on its usability and acceptability. It represents a significant step forward in the evolution of authentication mechanisms meeting the security needs of online users while maintaining usability.

Acknowledgements

In the name of Allah, the Beneficent, the Merciful.

قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ
الْحَكِيمُ

*They said, "Exalted are You; we have no knowledge except what You have taught us.
Indeed, it is You who is the Knowing, the Wise."
Quran (Surat Al Baqarah) – verse 32*

First and foremost, all praise is for Allah, Who enlightened us with faith and knowledge, and Who is sufficient for us and has sheltered us.

To my mother, thanks and may Allah bless you and give you health and long life.

To my father, thanks and may Allah bless your soul.

My wife and daughters thanks for being with me throughout this journey.

My supervisor, Karen Renaud, thanks for trust, time, and patience.

My family, grandmom, brothers and sisters, you were special people, thanks for everything.

My friends: Munther Al Busaidi, Shahid Al Balushi, Qais Al Yahyahi, and my colleagues: Thiam Kian (TK), Dora, Mariam, and Melissa, thanks to you all for the support and help. May Allah grant you a bright future and everlasting success.

Table of Contents

ABSTRACT	I
TABLE OF CONTENTS.....	III
LIST OF TABLES.....	VII
LIST OF FIGURES	IX
LIST OF PUBLICATIONS.....	XII
CHAPTER 1 INTRODUCTION.....	1
1.1 RESEARCH OBJECTIVES.....	2
1.2 HYPOTHESIS AND THESIS STATEMENT.....	3
1.3 THESIS STRUCTURE	4
CHAPTER 2 BACKGROUND AND RELATED WORK	6
2.1 INTRODUCTION	6
2.2 THE NEED FOR AUTHENTICATION.....	8
2.2.1 <i>Knowledge-based Authentication (KBA)</i>	11
2.2.2 <i>Token-based Authentication (TBA)</i>	14
2.2.3 <i>Biometric-based Authentication (BBA)</i>	17
2.2.4 <i>Others</i>	18
2.2.5 <i>Summary</i>	23
2.3 AUTHENTICATION IMPLEMENTATION.....	25
2.3.1 <i>Single-factor Authentication</i>	25
2.3.2 <i>Multi-factor Authentication</i>	25
2.3.3 <i>Multilevel Authentication</i>	26
2.3.4 <i>Multilevel, Multi-channel Authentication</i>	27
2.4 AUTHENTICATION ATTACK METHODS.....	30
2.4.1 <i>Attacks on Online Service Provider (OSP)</i>	30
2.4.2 <i>Attacks on Communication Channels (CC)</i>	35
2.4.3 <i>Attacks on End Users (EU)</i>	37
2.5 CHAPTER SUMMARY	43
CHAPTER 3 USABILITY AND ACCEPTABILITY	44
3.1 INTRODUCTION	44
3.2 USABILITY.....	45
3.2.1 <i>Usability Attributes</i>	45

3.2.2	<i>Usability of Authentication Mechanisms</i>	47
3.3	USABILITY EVALUATION	49
3.3.1	<i>Assessing Usability of Online Banking Systems' Authentication</i>	50
3.4	ACCEPTABILITY	52
3.4.1	<i>Information Technology Acceptance</i>	53
3.5	ASSESSING ACCEPTABILITY OF ONLINE BANKING SYSTEMS.....	57
3.5.1	<i>Demographic characteristics</i>	57
3.5.2	<i>Internal and external variables</i>	58
3.5.3	<i>Summary</i>	60
3.6	USABILITY AND ACCEPTABILITY MEASUREMENT.....	60
3.7	CHAPTER SUMMARY	61
CHAPTER 4	ONLINE BANKING AND MOBILE COMMUNICATION	62
4.1	ONLINE BANKING.....	62
4.1.1	<i>Factors Influencing the Adoption of Online Banking</i>	63
4.1.2	<i>Current Status</i>	68
4.1.3	<i>Authentication Mechanisms in Online Banking</i>	71
4.2	MOBILE COMMUNICATION	80
4.2.1	<i>Usability of mobile devices and network</i>	80
4.2.2	<i>Security of mobile devices and network</i>	83
4.2.3	<i>Mobile Devices as Authentication Tokens</i>	84
4.3	SUMMARY	85
CHAPTER 5	PROPOSED SOLUTION.....	86
5.1	INTRODUCTION	86
5.2	PROPOSED INFRASTRUCTURE.....	86
5.2.1	<i>MCA for Online Banking</i>	88
5.2.2	<i>Applicability of MCA</i>	90
5.2.3	<i>Cost of MCA</i>	92
5.2.4	<i>Feedback</i>	93
5.2.5	<i>Advantages over Single Channel Authentication (SCA)</i>	94
5.3	MOBILE NETWORK AS SECONDARY CHANNEL	95
5.4	THEORETICAL EVALUATION OF MCA	96
5.4.1	<i>MCA Application Model and Attack Target Nodes</i>	98
5.4.2	<i>Identify and Categorize Application Threats Based on STRIDE</i>	100
5.4.3	<i>Build an Attack Tree</i>	104
5.4.4	<i>Evaluation of Threats</i>	104
5.4.5	<i>Risk Mitigation and Security Controls</i>	110
5.4.6	<i>Rate the Threats (based on DREAD)</i>	110

5.5	CHAPTER SUMMARY	112
CHAPTER 6	DESIGN AND IMPLEMENTATION	114
6.1	INTRODUCTION	114
6.2	ASPECTS OF THE MCA	114
6.2.1	<i>Levels.....</i>	<i>115</i>
6.2.2	<i>Factors.....</i>	<i>117</i>
6.2.3	<i>Channels.....</i>	<i>118</i>
6.3	DESIGN RECOMMENDATIONS.....	120
6.3.1	<i>User Defined versus System Generated Passwords.....</i>	<i>120</i>
6.3.2	<i>Language Support.....</i>	<i>120</i>
6.3.3	<i>Encryption / Securing Key Delivery.....</i>	<i>121</i>
6.4	MCA - DESIGN OPTIONS.....	121
6.4.1	<i>Design option 1 – Transaction-based Authentication.....</i>	<i>121</i>
6.4.2	<i>Design option 2 – Beneficiary-based Authentication.....</i>	<i>123</i>
6.5	MCA IMPLEMENTATION – XYZ BANK.....	124
6.5.1	<i>Application Overview.....</i>	<i>125</i>
6.6	IMPLEMENTATION GUIDELINES	128
6.6.1	<i>Security guidelines:.....</i>	<i>129</i>
6.6.2	<i>Usability guidelines:</i>	<i>130</i>
6.7	SUMMARY	131
CHAPTER 7	EVALUATION	132
7.1	SURVEY DESIGN.....	134
7.1.1	<i>Online Questionnaire Design</i>	<i>134</i>
7.1.2	<i>Indirect Observation.....</i>	<i>135</i>
7.2	EXPERIMENT TRIALS	136
7.2.1	<i>First Experiment Trial.....</i>	<i>136</i>
7.2.2	<i>Pilot Test of the Second Experiment Trial</i>	<i>140</i>
7.2.3	<i>Usability Issues Addressed in the Second Trial.....</i>	<i>140</i>
7.2.4	<i>Application Requirements/Tasks (Second Trial)</i>	<i>142</i>
7.2.5	<i>Participants.....</i>	<i>156</i>
7.3	DEMOGRAPHIC PROFILE OF PARTICIPANTS.....	156
7.3.1	<i>Dropout Rates</i>	<i>158</i>
7.3.2	<i>Affects of Social Relationships on Dropout Rates</i>	<i>160</i>
7.4	PRELIMINARY TEST	161
7.4.1	<i>Data Preparation.....</i>	<i>161</i>
7.4.2	<i>Data Screening.....</i>	<i>163</i>
7.4.3	<i>Summary</i>	<i>172</i>

7.5	FACTORS INFLUENCING ADOPTION OF ONLINE BANKING	173
7.5.1	<i>Demographic Variables Hypotheses</i>	173
7.5.2	<i>Hypotheses Testing – Demographic Variables</i>	173
7.5.3	<i>External TAM Variables Hypotheses</i>	179
7.5.4	<i>Hypotheses Testing – TAM External Variables</i>	181
7.5.5	<i>Research Model</i>	183
7.6	MCA – USABILITY AND ACCEPTABILITY	184
7.6.1	<i>Measuring Usability of MCA</i>	184
7.6.2	<i>Measuring Acceptability of MCA</i>	193
7.6.3	<i>Comparison with Other Studies</i>	196
7.7	CHAPTER SUMMARY	198
CHAPTER 8 CONCLUSION		200
8.1	INTRODUCTION	200
8.2	RESEARCH OBJECTIVES AND CONTRIBUTIONS	201
8.3	FUTURE WORK	204
8.3.1	<i>More Usable Channels</i>	204
8.3.2	<i>MCA for the Disabled</i>	204
8.3.3	<i>MCA for Corporate Banking</i>	204
8.4	A FINAL WORD	205
BIBLIOGRAPHY		206
APPENDIX A WEB-APPLICATION CODES/SCRIPTS		219
APPENDIX B ONLINE QUESTIONNAIRES		225
APPENDIX C DATA SCREENING RESULTS		235
APPENDIX D DEMOGRAPHICS CHARACTERISTICS		239

List of Tables

<i>Table 2-1: Summary table of different authentication classes.....</i>	<i>24</i>
<i>Table 3-1: Overview of Usability dimensions (adapted from [103]).....</i>	<i>46</i>
<i>Table 5-1: Threats affecting elements [219].....</i>	<i>101</i>
<i>Table 5-2: Threat rating table [227].....</i>	<i>111</i>
<i>Table 5-3: DREAD-rating table.....</i>	<i>112</i>
<i>Table 5-4: Threat modelling based on STRIDE process and DREAD rating summary table.....</i>	<i>113</i>
<i>Table 7-1: The list of hypotheses developed in this study.....</i>	<i>133</i>
<i>Table 7-2: Chi-square test for independence summary results between demographic profile and dropout rates.....</i>	<i>158</i>
<i>Table 7-3: Cross tabulation between education level and dropout rates.....</i>	<i>159</i>
<i>Table 7-4: The 5 tasks identifiers.....</i>	<i>162</i>
<i>Table 7-5: Pre-questionnaire variables that incurred a “missingness” rate higher than 5%.....</i>	<i>164</i>
<i>Table 7-6: Crosstabulations of education level verses other common variables.....</i>	<i>166</i>
<i>Table 7-7: Crosstabulations of monthly income group verses other common variables.....</i>	<i>168</i>
<i>Table 7-8: Descriptive statistics for the raw data from logs.....</i>	<i>169</i>
<i>Table 7-9: Descriptive statistics of a clean version of logs data.....</i>	<i>171</i>
<i>Table 7-10: Chi-square test for independence summary results between demographic profile and attitude towards adopting online banking.....</i>	<i>173</i>
<i>Table 7-11: Cross tabulation between age group and users with online banking (OB) experience.....</i>	<i>177</i>
<i>Table 7-12: Cross tabulation between monthly income group and users with online banking (OB) experience.....</i>	<i>179</i>
<i>Table 7-13: Summary of the ‘Factor Analysis’ for factors influencing adoption of online banking.....</i>	<i>180</i>
<i>Table 7-14: Correlation analysis results.....</i>	<i>182</i>
<i>Table 7-15: Assessment of the TAM external variables.....</i>	<i>183</i>
<i>Table 7-16: Sub-tasks completion and dropout rates.....</i>	<i>186</i>
<i>Table 7-17: Completion time of experiment tasks.....</i>	<i>188</i>
<i>Table 7-18: Results of Mann-Whitney U Test and independent-sample t-test for differences between experience, gender and age group on overall tasks completion time.....</i>	<i>189</i>
<i>Table 7-19: Descriptive statistics of usability questions.....</i>	<i>190</i>
<i>Table 7-20: Comparative evaluation of social relationships on satisfaction using Mann-W. U Test.....</i>	<i>191</i>
<i>Table 7-21: Comparative evaluation of experience, gender, and age on users’ satisfaction (MCA) using Mann-Whitney U Test.....</i>	<i>192</i>
<i>Table 7-22: Paired-samples t-test comparing online users’ preferences for using online banking services on systems with MCA and without MCA.....</i>	<i>194</i>
<i>Table 7-23: Wilcoxon Signed Rank Test comparing online users’ preferences for using online banking services on systems with MCA and without MCA.....</i>	<i>195</i>

<i>Table 7-24: Comparison of findings between this research and another study in the same area.....</i>	<i>197</i>
<i>Table 7-25: Hypotheses testing results.....</i>	<i>198</i>
<i>Table 8-1: Hypotheses tested in this study.....</i>	<i>201</i>
<i>Table 8-2: Hypotheses testing results.....</i>	<i>203</i>

List of Figures

Figure 2-1: Applicable attacks on the main three communication elements.....	8
Figure 2-2: Username and password are common shared and secret knowledge factors used in KBA.....	12
Figure 2-3: Magnetic strip cards.....	14
Figure 2-4: (a) Proximity card, (b) Smart card.....	15
Figure 2-5: Different types of tokens used to generate one-time pin (OTP) numbers.....	16
Figure 2-6: Biometrics: A) ear, B) face, C) facial thermogram, D) hand thermogram, E) hand vein, F) hand geometry, G) fingerprint, H) iris, I) retina, J) signature, and K) voice.....	17
Figure 2-7: Vouching authentication mechanism [48].....	19
Figure 2-8: PBA class by [49].....	21
Figure 2-9: Single-factor authentication mechanism.....	25
Figure 2-10: Multi-factor authentication mechanism.....	26
Figure 2-11: Multilevel authentication mechanism.....	27
Figure 2-12: Multilevel, multi-channel authentication mechanism.....	27
Figure 2-13: Multilevel, single channel approach vs. multilevel, multi-channel approach.....	28
Figure 2-14: Botnets: a) DDoS, b) DRDoS attacks[65].....	31
Figure 2-15: (a) Non-persistent XSS attack; (b) Persistent XSS attack.....	33
Figure 2-16: Web-application vulnerability disclosures by attack categories 2004 – 2009 (adapted from [52]).....	33
Figure 2-17: Security policy violation.....	35
Figure 2-18: Man-in-the-middle (MITM) attack.....	36
Figure 2-19: IFRAME element within HTML web-document.....	37
Figure 2-20: Phishing attack via e-mail.....	40
Figure 2-21: DNS spoofing attack [84].....	41
Figure 2-22: Man-in-the-browser (MITB) attack.....	43
Figure 3-1: Evaluating usability by associating the context of use (adapted from [95]).....	49
Figure 3-2: Relationship between usability, quality, convenience, and security [122].....	51
Figure 3-3: A model of the attributes of system acceptability [98].....	53
Figure 3-4: Technology Acceptance Model (TAM) [136].....	54
Figure 3-5: Critical success factors of online banking [140].....	55
Figure 4-1: Cost per transaction for each banking channel.....	64
Figure 4-2: USA banking delivery transactions by channel (2006-2010).....	68
Figure 4-3: Types of online banking applications (OBA): (a) Informational OBA, (b) Local-transactional OBA, (c) Transactional OBA.....	69
Figure 4-4: Online services page.....	72
Figure 4-5: (a) Login screen, (b) Home page screen.....	73
Figure 4-6: Creation of a beneficiary account.....	74

Figure 4-7: Authentication code via SMS.....	75
Figure 4-8: Details of beneficiary accounts after activation.....	76
Figure 4-9: The quadruple login authentication process.....	77
Figure 4-10: Add local beneficiary account authentication method.....	78
Figure 4-11: Internet and Mobile User Stats from 1998 to 2008 [201, 202].....	81
Figure 4-12: Preferred payment method of Internet users if away.....	83
Figure 5-1: The proposed MCA infrastructure.....	88
Figure 5-2: The proposed MCA in online banking.....	91
Figure 5-3: Threat modelling six-stage process.....	97
Figure 5-4: The proposed online-banking application architecture diagram.....	99
Figure 5-5: EU to web server (Informational Level) data flows threats.....	101
Figure 5-6: Data store (database) STRIDE threats.....	102
Figure 5-7: An attack tree for the proposed online banking with MCA approach.....	105
Figure 5-8: Security controls implemented for the MCA infrastructure (adapted from [220]).....	110
Figure 6-1: System levelling structure.....	115
Figure 6-2: Services level diagram.....	116
Figure 6-3: MCA architecture session management.....	116
Figure 6-4: The implementation of factors into multi-level system.....	117
Figure 6-5: MCA architecture diagram.....	119
Figure 6-6: Design option 1 – Transaction-based authentication process.....	122
Figure 6-7: Design option 2 - Beneficiary-based authentication process.....	123
Figure 6-8: XYZ Bank prototype application storyboard.....	125
Figure 6-9: The prototype application architecture.....	126
Figure 6-10: Common application templates layout.....	126
Figure 6-11: MCA application - Home page (login) - Implementation.....	128
Figure 7-1: First trial, prototype, application structure.....	136
Figure 7-2: Dropouts of participants in the first trial.....	138
Figure 7-3: First trial sample profile.....	139
Figure 7-4: On screen mobile simulation for SMS reading and sending.....	141
Figure 7-5: Second trial prototype application structure.....	141
Figure 7-6: Task 1 - Storyboard.....	143
Figure 7-7: Registration - stage 1 - WebMD activity diagram.....	143
Figure 7-8: Registration page – stage 1 - Implementation.....	144
Figure 7-9: Registration task - stage 3 - implementation.....	145
Figure 7-10: Mobile simulator - (a) Welcome message, (b) SMS message.....	146
Figure 7-11: Task 2 - Storyboard.....	147
Figure 7-12: Verifying OTP through the web channel.....	147
Figure 7-13: Verifying OTP through the mobile network channel.....	148
Figure 7-14: Task 3 - Storyboard.....	148
Figure 7-15: Add new beneficiary account form - implementation.....	149
Figure 7-16: SMS message format for activating a beneficiary account.....	149

<i>Figure 7-17: Activate beneficiary account - implementation.....</i>	<i>150</i>
<i>Figure 7-18: Task 4 – Storyboard</i>	<i>151</i>
<i>Figure 7-19: Beneficiary accounts page - implementation.....</i>	<i>152</i>
<i>Figure 7-20: Money transfer form - implementation</i>	<i>152</i>
<i>Figure 7-21: Money transfer confirmation page - implementation.....</i>	<i>153</i>
<i>Figure 7-22: Task 5 - Storyboard</i>	<i>154</i>
<i>Figure 7-23: Beneficiary activation window - Task 5 - implementation</i>	<i>154</i>
<i>Figure 7-24: The SMS message format sent to the alternative mobile number</i>	<i>155</i>
<i>Figure 7-25: Beneficiary account activation window - alternative channel mode - implementation.....</i>	<i>155</i>
<i>Figure 7-26: Percentage of friends and colleagues compared to other participants in the study</i>	<i>156</i>
<i>Figure 7-27: Demographic profile of all participants.....</i>	<i>157</i>
<i>Figure 7-28: Relationship between online banking (OB) experienced users and dropout rates.....</i>	<i>160</i>
<i>Figure 7-29: Relationship between social relationship and dropout rates</i>	<i>160</i>
<i>Figure 7-30: Common variables between the pre and post-questionnaire data files</i>	<i>162</i>
<i>Figure 7-31: Relationship between gender and percentage of online banking (OB) experience.....</i>	<i>174</i>
<i>Figure 7-32: Relationship between marital status and percentage of online banking (OB).....</i>	<i>175</i>
<i>Figure 7-33: Relationship between education level and percentage of online banking (OB) users</i>	<i>176</i>
<i>Figure 7-34: Relationship between age group and online banking (OB) users</i>	<i>177</i>
<i>Figure 7-35: Relationship between monthly income group (in OMR) and percentage of online banking (OB) users</i>	<i>178</i>
<i>Figure 7-36: The measurement model of the study based on TAM</i>	<i>181</i>
<i>Figure 7-37: Extended TAM for online banking in Oman (Note: the results shown for internal TAM constructs were extracted from [147]).....</i>	<i>183</i>
<i>Figure 7-38: Completion task rate for all participants.....</i>	<i>185</i>

List of Publications

- Karen Renaud, Richard Cooper and Mohamed Al-Fairuz *Support Architecture for Multi-Channel, Multi-Factor Authentication*, e-commerce 2007 IADIS International Conference e-commerce 2007 Algarve, Portugal, 7-9 December 2007
- Mohamed Al-Fairuz and Karen Renaud. *Multi-Channel, Multi-level Authentication for More Secure eBanking*. ISSA 2010. Johannesburg, South Africa. 2-4 August, 2010.

Chapter 1

Introduction

Advances in Internet technologies have created many opportunities for offering consumers different electronic services online. Some of these services support communication between people while others offer online market places where people can choose products and services while they remain at home. The Web, as one service provided by the Internet, is a remarkable network with huge potentialities that can be accessed from almost all countries around the globe [1]. This network offers online business players a wider domain of consumers that is not restricted by geographical areas and a new arena of competition. On the other hand, it offers customers a virtual market place with a variety of products and services from different businesses around the world that are, otherwise, hard to bring together in one physical place.

Banks, as one of the fast growing online businesses, utilize the Web as a marketing and delivery medium, which offers them an open market with equal opportunities to compete with other banking players. For online banking customers, the Web offers an online market place with a wide range of services that are just a click away [2]. However, there is a huge volume of communication traffic between banks and customers, full of threats and anonymous users with financial gain or subversive goals in mind. It is important to prevent such users from gaining unauthorized access to other users' online accounts. This is especially important for financial firms, such as banks, that need to identify and authenticate their customers reliably before granting them access to their services.

Most of the online businesses that maintain users' accounts today make use of passwords to authorize their customers to permit access their online accounts. This authentication mechanism, however, is most effective when used as an access credential for accessing standalone computers, not connected to any network. Today, almost all computers are Internet-ready machines and many of them are already connected to at least one network, whether that is a home network, an office network, and/or the Web. This technological advancement has brought many electronic services to users' computers and mobile phones. Many of these services require passwords for authentication. Users often reuse the same

password, write passwords down, or ask the browser to remember them [3]. Such behaviours put the users' accounts in danger. Even if we trust the user, the fact that these computers connect to a global network is, in itself, a reason for not relying on passwords as a sole authentication factor for authorizing critical transactions. As a consequence, many alternative authentication mechanisms were proposed in the past few years in order to provide stronger alternatives to the traditional password.

This study focuses upon Sultanate of Oman, a developing country where online banking is less widely adopted and used by bank customers than in developed countries such as UK. There are few published studies [4, 5] exploring online banking adoption and authentication techniques to date. Until May 2009, only four out of a total of 7 local banks in Oman offered online banking services to their customers [6]. Some of the current existing online banking systems implemented by banks, including the major leading bank [7], offer only limited functionality such as account statements and payment history with payment transfers between customer accounts and bill payments. This made Oman an interesting place to explore in the context of online banking adoption using novel authentication techniques.

This study proposes a solution that offers online banking users a more secure authentication mechanism while maintaining usability. The solution is based on a multilevel authentication approach where services are classified into informational and transactional services. Each level must be independent from the other and the user must always be authenticated when moving to a higher level. To obtain maximum benefit, secrets or keys used to authorize transactional services must be delivered via an independent channel other than the primary channel used to authorize users to access informational services. This authentication mechanism is based on previous research [8] and extends the study by means of theoretical and practical evaluations. The study first evaluates the security of the proposed solution theoretically, using threat-modelling techniques, and then uses an online experiment to evaluate, in practical terms, usability and acceptability of the proposed solution.

1.1 Research Objectives

Objective 1. Review the most commonly used authentication classes, authentication mechanisms, and authentication attacks (Chapter 2).

- Objective 2.** Review the usability and acceptability aspects of authentication mechanisms and the evaluation techniques used to assess them for new information technologies.
- Objective 3.** With respect to online banking, discuss some of the currently used authentication mechanisms and identify their weaknesses, showing how they fail to protect customers' accounts against different attacks identified in objective 1 (Chapter 4).
- Objective 4.** Propose an authentication mechanism solution that addresses the security and usability problems identified and listed in objective 2. Theoretically evaluate the security of this solution and identify all features needed for implementation (Chapter 5).
- Objective 5.** Empirically evaluate the new proposed mechanism with respect to usability and acceptability (Chapter 7).

1.2 Hypothesis and Thesis Statement

The thesis statement is:

It is possible to design an authentication mechanism that uses multiple channels to resist attacks more effectively than most commonly used mechanisms. Furthermore, such a mechanism will also be both usable and acceptable to users in Oman.

The first part of the thesis statement is addressed theoretically using threat-modelling analysis in Chapter 5. The second part of the statement is practically evaluated in Chapter 7 where usability and acceptability aspects are thoroughly addressed. The practical evaluation of usability and acceptability in this study involved testing the following hypotheses in order to support the second part of the thesis statement:

- H1a. Gender significantly influences customers' usage of online banking
- H1b. Marital status significantly influences customers' usage of online banking
- H1c. Education level significantly influences customers' usage of online banking
- H1d. Age significantly influences customers' usage of online banking
- H1e. Income significantly influences customers' usage of online banking
- H1f. Trust & relationship has a positive effect on Perceived Ease of Use (PEU)
- H1g. Ease of access has a positive effect on Perceived Ease of Use (PEU)
- H1h. Security has a positive effect on Perceived Ease of Use of OB

- H2a. Multi-channel authentication is effective
- H2b. Multi-channel authentication is efficient
- H2c. Multi-channel authentication is satisfactory
- H2d. Multi-channel authentication is acceptable to users

The hypotheses are split into two categories: H1 and H2 hypotheses. The H1 hypotheses are concerned with the factors influencing the adoption (acceptance) of online banking in Oman. H2 hypotheses, however, address the usability and acceptability of multi-channel authentication, proposed in Chapter 5, to Omani users.

1.3 Thesis Structure

The dissertation is organized into the following chapters:

- Chapter 2 Background and Related Work: this chapter presents a thorough literature review on authentication, its types, and implementation mechanisms found in the literature. The chapter also covers attack methods used to target these authentication mechanisms.
- Chapter 3 Usability and Acceptability: this chapter reviews usability and acceptability of authentication mechanisms. It also discusses the importance of evaluating usability and acceptability of new information technologies in information system and how they can be evaluated in practical terms.
- Chapter 4 Online Banking and Mobile Communication: this chapter discusses authentication mechanisms implemented in online banking applications. It also covers the important role of mobile communication as a usable and secure complementary authentication channel.
- Chapter 5 Proposed Solution: this chapter proposes the multi-channel authentication (MCA) mechanism and discusses how it overcomes the security and usability issues of other alternatives. It also presents a widely accepted threat evaluation technique, suggested by Microsoft, to test the security level offered by MCA against most known forms of attack.
- Chapter 6 Design and Implementation: this chapter covers MCA design options and implementation. It reviews the prototype application and explains how users will go about testing it in the data-gathering phase.

Chapter 7 Evaluation: this chapter presents the results of the evaluation of the data gathered from users who tested the prototype application. The study bases its evaluation on questionnaire results and data gathered from log tables.

Chapter 8 Conclusion: this final chapter concludes the study by giving an overview of all chapters discussed in this thesis. It also summarizes the main results and lists future research paths.

Chapter 2

Background and Related Work

2.1 Introduction

When personal home computers started to appear in the 1970s, they were mainly used for basic computational tasks or to store data. The most powerful selling tool at that time was entertainment software. However, after the development of electronic mail (e-mail) a few years later and the introduction of the Web service in the 1980s, there was a shift of users' interests towards using personal computers mainly for communications [9]. This change led to interconnected computers in a network, the Internet, replacing the previous era when computers were solely standalone machines. According to [10], there were almost 1.73 billion Internet users worldwide in September 2009, with an increase of 18% since the previous year. The e-mail users (81% of the total Internet users) sent around 90 trillion e-mails in 2009 alone.

From a business perspective, the Internet (which offers e-mail and Web services) has also become the most convenient and cost-effective environment for businesses around the globe [1]. It is a place where people with different cultural backgrounds and from different geographical places connect as if they are in one physical place, sharing and communicating with each other in different electronic forms. For business organizations, the web offers an open market with equal opportunities to compete regardless of business size or geographical location. For consumers, it offers an online market place with a wide variety of products from different suppliers with different prices [2]. Thus, anyone can start a business online and compete with other business players. Statistics show e-commerce or online retailing is one of the fastest growing markets in Europe with online sales totalling approximately 4.7% of retail marketplace sales in 2009 (expected to increase to 5.5% in 2010) [11].

The afore-mentioned trends have made personal computers an integral part of our lives. However, this change soon led to security problems. From the users' side, such problems appear in the form of malicious programs, loss of privacy, and floods of unwanted advertisement and spam [9]. From the businesses' side, it is less important to know

whether you can do business than to know how to deploy this business in the online market [12] and how to maintain the business presence [1] in such an open, networked market full of threats and ambiguous users who are connected, along the way, with subversive goals in mind.

According to CERT statistics, the total vulnerabilities reported jumped from 171 to 2,437 to 7,236 in 1995, 2001, and 2008 respectively [13]. This increase requires that close attention be given to security, which itself progresses in parallel with the technological advances of computers and the Internet. Before the development of computers, security meant a means to secure assets physically, with traditional access controls such as keys, guards, walls, and fences. However, after the invention of computers, the science of encryption and cryptography offered practical controls for information assets. These have improved very quickly over time. Nevertheless, since the introduction of the Internet and the tremendous growth of Internet users and e-commerce web applications, user identification and authentication have become major research areas charged with keeping pace and withstanding networking changes and increasing numbers of information security threats and attacks, evolving over time. These attacks use various technologies and techniques, and exploit various vulnerabilities; they have the potential to damage any of the three key elements involved in an online communication model. These three key elements are: the source, the transmission system, and the destination [14]. In this research, source and destination are referred to as *end user (EU)* and *online service provider (OSP)*, respectively. The transmission system is referred to as the *communication channel (CC)*.

Figure 2-1 shows the applicable known attacks on each of the key elements of the online communication model. These attacks are discussed in more detail later in section 2.4 of this chapter.

In this chapter, section 2.2 defines authentication and lists the major classes of authentication commonly used by information technology systems. Section 2.3 explains how these authentication classes are being implemented and discusses the different types of authentication mechanisms that are proposed in the literature or that are currently implemented in different online applications. Following the authentication classes and implementation mechanisms, section 2.4 pinpoints the various attacks on these mechanisms. This section covers most known attacks that target each of the three core

communication elements: *end user (EU)*, *communication channel (CC)*, and *online service provider (OSP)*.

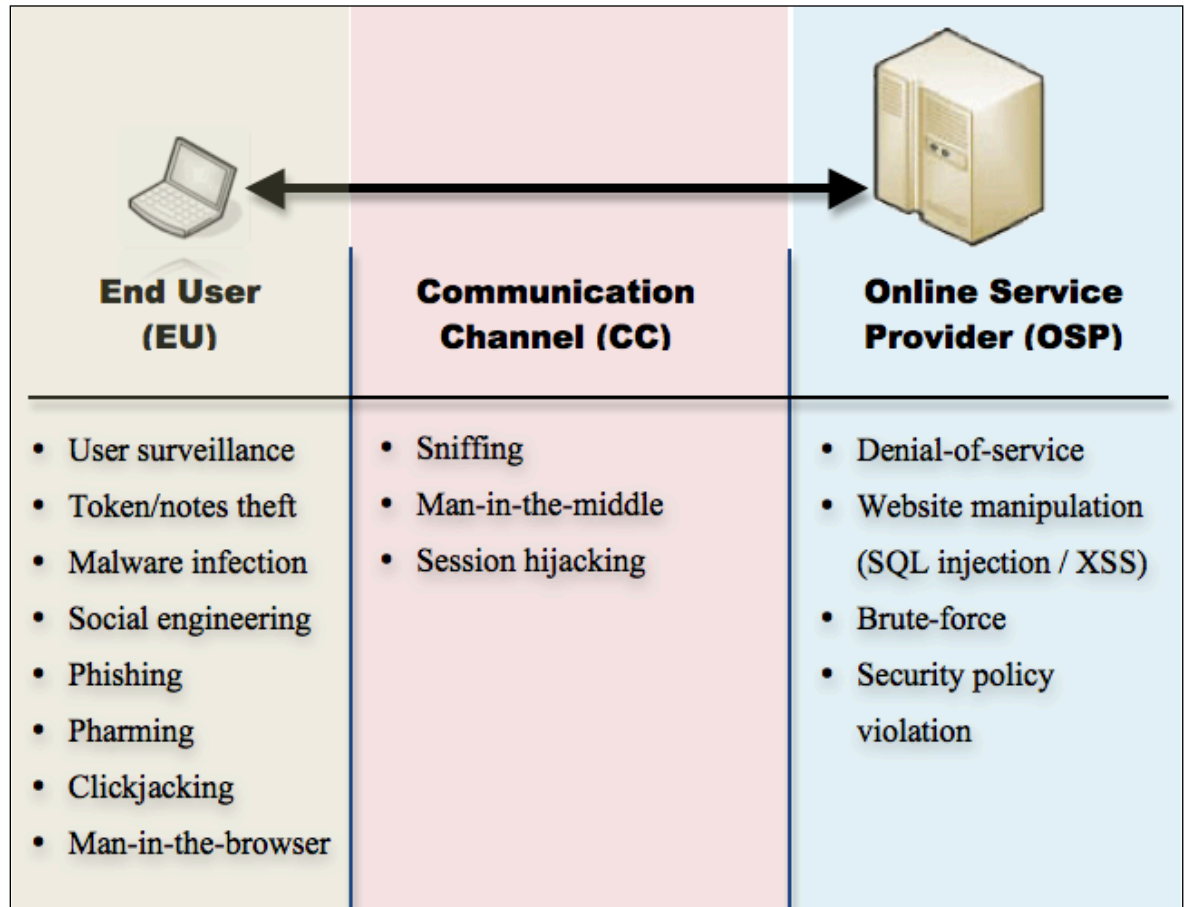


Figure 2-1: Applicable attacks on the main three communication elements

2.2 The Need for Authentication

With the rapid progress of technologies related to networking facilities, more computers than ever before are now connected with each other. Unlike local limited networks, most computers are now connected to a larger global network to communicate and exchange resources electronically [15]. With this networking progress, there is a need to offer security that will help protect connected users' resources and services from other users. Yang and Shieh [15] described network security in terms of two basic requirements: secrecy and authentication. The former protects sensitive data against eavesdropping and modification, ensuring privacy and integrity of the electronic data available or exchanged within the network. The latter prevents forgery and unauthorized access to the network's resources, ensuring the authenticity of the user. The authentication process was described by Renaud's model as three phases: identification, authentication, and authorization [16].

1. User identification is the process in which users are identified to a system in terms of who they are. The user supplies an identification code or name to the system, which accordingly, looks into the database for a matching record. Online user identification is insufficient by itself and it is typically necessary to proceed to the user authentication phase to verify the identity [17].
2. User authentication is the process of confirming the user identification supplied in the previous phase. Usually the user must supply a secret factor in this phase, which should match the one assigned to the user's record identified in the previous phase. Like user identification, user authentication is insufficient by itself and is a prerequisite for the user authorization phase.
3. If both user identification and authentication phases are successful, user authorization follows. This phase specifies the user's access and usage privileges on the system. This phase usually is maintained and it remains live as long as the user session is active. This is to ensure that the user is accessing only information he/she is authenticated to access.

Computer systems and online applications use different authentication mechanisms. Some choose to use basic authentication mechanisms such as username and password while others invest resources to implement suitable authentication mechanisms such as biometric recognition hardware and software to protect their reputations and enhance their presence in the (online) market. While it is difficult to pin down how much an attack costs an organization in terms of damage and recovery, some security and research organizations have been running surveys to estimate the costs of attacks and computer security breaches. In 2003, viruses (i.e., considered as malware that attack computers) alone cost businesses \$55 billion, almost double the damage they inflicted in 2002 [18].

Sometimes, security breaches come from the employees within the organization and not from outsiders. In a 2009 survey of American companies and government agencies conducted by the Computer Security Institute, 25% of respondents indicated that more than 60% of financial losses came from accidental breaches by insiders, not external hacks, and 16.1% said 81 to 100% of all losses came from accidental breaches [19]. One should also note that many organizations, especially financial firms, are very reluctant to report hacker-related break-ins as this could affect customers' and stakeholders' impression of their security [18] and might, therefore, affect the organization stocks in the stock market [20].

Authentication is not only implemented in information technology, but rather is seen and dealt with everywhere. The amount of proof a user is required to provide increases or

decreases based on the amount of risk associated with the services or resources delivered. This is referred to as risk-based authentication [21].

A restaurant receptionist requests a customer's name to verify which table is booked for that customer, for example. A college student is asked by the registration office for information regarding full name, date of birth, and student identification number (ID) to receive a transcript. A bank customer calling a credit card department by phone is asked for full name, full address, date of birth, and maybe details of recent transactions on the account or a special online personal identification number (PIN) to verify his or her identity.

The verification process in our daily life is related to the risk associated with the service or resources to be acquired. In the restaurant case, for example, there is very little or no risk at all if the customer who just entered the restaurant has impersonated another customer who booked a table by phone. If the legitimate customer shows up anytime, he or she can be offered another table or, in the worst case, the restaurant manager can request that the other customer leave the place in favour of the legitimate customer who booked that table by phone.

In the college student case, transcript details are usually confidential and only a legitimate student can request a copy from the registration office. However, the risk associated with the student grades being compromised is very low. Students sometimes share their grade scores with each other and a copy of the transcript is often attached to every job application made after graduation. Therefore, the verification process implemented by the registration office is limited only to information that could easily be known by other students like the student's name, date of birth, and student ID.

Unlike the restaurant customer and the college student, the bank customer has to provide more details that identify him or her more clearly (e.g., date of birth, full address) as well as information that is treated as confidential and is not known to anyone else (e.g., last transaction details, PIN). This is important due to the high risk associated with the customer's bank account. If someone were able to impersonate a bank customer when phoning the credit card department, he or she could request payment transactions that might be of a criminal nature, affecting the bank and the customer at the same time.

Hastings and Dodson [22] described the authentication process in terms of *claimants*, *relying parties*, and *verifiers*. A claimant is the individual claiming to be a legitimate user

to receive services and resources. A relying party is the provider of the services and resources the user needs. A verifier is another individual or an automated system, which verifies the claimant's legitimacy to authorize delivery of services and resources provided by the relying party. The verification process is usually based on authentication factors like facts, characteristics, behaviours, or knowledge known only to both the claimant and the verifier. Based on these authentication factors, the researchers have classified authentication in information technology into three classes: knowledge-based (KBA), token-based (TBA), and biometrics based (BBA).

This section discusses these three classes and the possible implementation strengths and weaknesses of each in detail. Examples of some implementations of these classes proposed in the literature are also presented.

2.2.1 Knowledge-based Authentication (KBA)

KBA is also called *something the user knows* and it refers to the method of verifying a user's identity by matching one or more pieces of "secret" information supplied by an individual (claimant) against information sources associated with the claimant [23]. KBA is the most common authentication approach used in most distributed systems today [24]. This is due to many factors including simple implementation requirements, low implementation and administration costs [25], and a high level of user acceptance.

The authentication method used in KBA usually involves two factors: *shared knowledge* and *secret knowledge*. Shared knowledge is a piece of information that describes the user and people who interact with the user sometimes know the information. Examples of such shared factors include the user date of birth, living address, social security number, city of birth, and the name of a best friend. Secret knowledge, on the other hand, is considered secret and only the user usually knows it. This includes fixed passwords, passphrases, and PINs.

A fixed password (see Figure 2-2) as an authentication factor is the most widely used KBA mechanism [15, 16, 25]; it acts as the first line of defence against unauthorized access [26]. Most of the time, a user is requested to enter a username as well as an identification name. Following that, the user enters a secure password. The system will then consult a database or a data file to locate a matching record. If it finds one, then the password entered by the user will be compared against the password in the record. If they match, then the user

receives access permission. Sometimes passwords are encrypted in the database so the comparison process is only done after the entered password is encrypted using the same encryption algorithms. This encryption sometimes uses a one-way function. A one-way encryption function is a computational process that encrypts a given string (password) so it is computationally infeasible to decrypt it afterwards [27]. This function is used to protect users' passwords from being compromised if an attacker were to gain access to the database file.

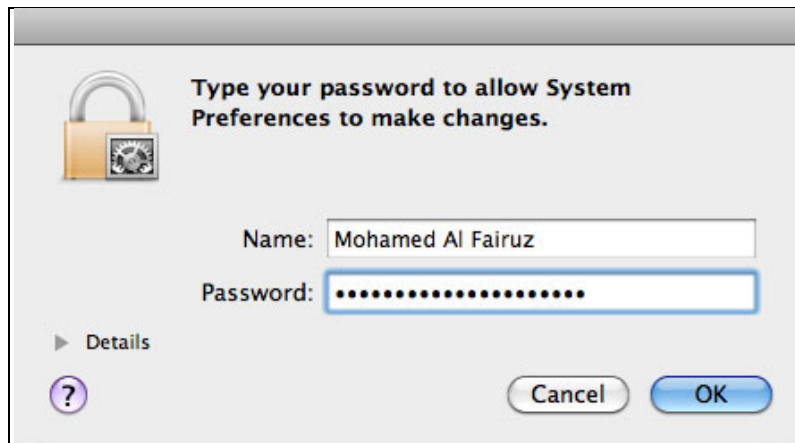


Figure 2-2: Username and password are common shared and secret knowledge factors used in KBA

Despite the fact that passwords are the most commonly used KBA, it is clear that they still have several weaknesses and are vulnerable to different attacks, especially if their database is available offline [28, 29] or is attacked by an insider. Passwords in most systems are user defined and users tend to use memorable weak passwords. Such passwords are highly susceptible to observation and guessing [30] and can be intercepted and replayed [25] if communication channels are not properly encrypted and secured. Statistics show that there is a significant growth of Internet services offered to online users [31] and users are now required to manage many different accounts online. Accordingly, the number of passwords needed to secure these accounts per person has increased. However, users tend to reuse their passwords across these accounts, which makes the case even worse because compromising one account allows the attacker to take over several accounts [3].

In order to overcome these weaknesses, some organizations have made use of system-generated passwords. This could be counter-productive as system generated passwords tend to be very complex, and therefore, hard to remember. Consequently, users might write these passwords down and degrade the overall security of the system. The same goes for organizations that set password policies that include rules requiring user-defined passwords to be very complex (i.e., force the use of special characters, combination of small and

capital letters, and numbers). As a result, passwords become more secure, yet hard to remember, and therefore, the whole system may be compromised by the written records. Thus, a very long password is actually as bad as a weak one.

One of the most common security mechanisms applied to password authentication is to restrict the allowed number of invalid retries. This usually locks down the account for a period of time if invalid passwords are submitted several times (i.e., usually three). Another common mechanism is to force the user to change the password regularly. Online organizations, especially financial firms, do this to ensure that their customers do not use the same password among their other accounts that they may access frequently, such as e-mails, social networking, and instant messaging accounts. All these mechanisms apparently help protect the users' accounts in some ways but there is always a usability cost. For example, modern browsers and Internet applications keep users logged in and request them to verify their passwords only to re-login to their accounts. However, users sometimes forget to disable the caps-lock key or use multi-language keyboards and define their passwords in languages other than the language they used when they created them. When they enter their passwords in the wrong case or language, they find it difficult to understand the reason for the authentication failure due to routine password obfuscation. For these reasons, an account could accidentally be locked and access denied to a legitimate user for a period of time.

Making passwords complex, and therefore, hard to guess does not prevent other types of attacks like Trojans and sniffing (discussed in more detail in section 2.4). Even a strong password can easily be captured if a key-logger is used. Key-loggers usually come in different techniques. Some are software that are installed into the system (Spector Pro, eBlaster, SpyAgent, SpyBuddy) and some are used to reprogram the BIOS memory (memory responsible for the computer firmware, which controls devices like the keyboard). Other types of key-loggers come as hardware such as a circuit with an internal memory, which is attached somewhere between the I/O port and the keyboard. Other hardware key-loggers do not need to be connected, having wireless sniffing ability to capture wireless keyboards' signals/waves. All these types of key-loggers (software or hardware) have the ability to capture the keystrokes, which sometimes represent the user identification and secret factors of the user.

Despite the security and usability issues related to the use of passwords as an authentication factor, most systems today are still using passwords as the only secret for

user authentication. Even systems that implement a high level of security and utilize other forms of authentication are still using password authentication as a complementary authentication at some point.

2.2.2 Token-based Authentication (TBA)

Token-based authentication (TBA), sometimes referred to as *something you hold*, is an authentication class based on tokens possessed by the user. The authentication principle does not rely on user's memory but rather on the ability of the user to prove the ownership of a token. In real life, these tokens are usually used to identify the user who carries them (e.g., ID card, hospital card, social security card) while in information technology, these tokens are used and processed as part of the authentication mechanism. Such tokens include an ATM card, smart card, and the one-time hash calculator.

Several technologies have been used for authentication based on tokens. These include *magnetic strip card*, *proximity card*, and *smart cards*.



Figure 2-3: Magnetic strip cards

A magnetic strip card (see Figure 2-3) is a token card with a magnetic band capable of storing data (e.g., ATM card, credit card, and transport card). They are widely used as a substitute for cash by financial firms as well as to carry out financial transactions. Other

companies also use this type of token as a substitute for physical access keys (i.e., accessing a hotel room), while others use them to control access and payment of time controlled services such as car parking area. A set of standards such as ISO 7810, 7811, 7813 [32-34] and ISO 4909 [35] have been issued to define the physical characteristics and the magnetic track data structure of these cards.

Magnetic strip cards are easy to carry and cheap to replace. However, they are also cheap to duplicate. There are commercial devices that are capable of reading the magnetic strip to duplicate its contents onto another template card. Thus, some authentication mechanisms implemented by organizations like banks also request their customers to provide another authentication factor on top of the token. If a token has been stolen or duplicated, they should be useless without the other authentication factor associated with the token; a PIN is commonly used as a second authentication factor.

A proximity card (see Figure 2-4a), also known as a contactless smart card, is another form of token used for authentication. Unlike a magnetic strip card, a proximity card does not require physical contact with a reading device to read its contents. It transmits its data to a monitoring device wirelessly, which makes it more practical than the magnetic strip. However, the use of proximity cards introduces another major security issue as the signals sent by this type of token can be read by a remote receiver located within the transmission range of the proximity card [36]. For this reason, the implementation of this type of token focuses mainly on access control and identification systems rather than on serving as an authentication token.



Figure 2-4: (a) Proximity card, (b) Smart card

The smart cards (see Figure 2-4b), also known as challenge/response cards, are cards with a built-in chip used as memory and/or as a microprocessor. The development of smart

cards dates back to the 1970s when patents were filed by France, Germany, and Japan [37]. They are capable of performing computational algorithms and are able to store passwords and certificates. There are many applications where smart cards are used, either as identification tokens of their owners or as authentication factors. In computer systems, smart cards are used to allow single sign-ons and as an encryption factor to encrypt the file system. In financial firms, smart cards are used as ATM cards, credit/debit cards, fuel cards, SIM cards, and electronic wallets. Electronic wallets can be loaded with cash (electronically) that can later be transferred or used to pay for products.

The smart cards are governed by ISO 7816 (parts 1, 2, & 3) [38], which defines their physical/communication characteristics and application identifiers. In terms of security, smart cards use public key infrastructure (PKI) where the private key is stored in the card and cannot be copied. Usually it utilizes a two-factor authentication protocol where the token itself is considered one factor and a PIN the other. It limits the number of invalid trials before the card becomes inactive. Nevertheless, as for other token-based authentication, smart cards are prone to theft, and therefore, can be compromised, especially if the PIN number is written down on the card itself or is captured by covert user surveillance, such as over-shoulder sniffing or surveillance spy cameras. It has been estimated that around 25% of ATM card owners write down their PIN numbers on their cards [39].



Figure 2-5: Different types of tokens used to generate one-time pin (OTP) numbers

Other types of tokens also exist (see Figure 2-5). These include USB drives, key fobs, and one-time pin (OTP) calculators. Overall, token-based authentication offers better security than the traditional knowledge-based authentication and protects online users from guessing, interception, social engineering, and brute-force attacks. However, the tokens

used to authenticate users can be shared or duplicated [40], and therefore, can be used illegally by people other than the legitimate user. Token-based authentication is more expensive to deploy and maintain than knowledge-based authentication, especially when implemented on a large-scale. Moreover, some token-based technologies suffer from the same problems as traditional KBA because they still rely on memory in addition to remembering to carry the token.

2.2.3 Biometric-based Authentication (BBA)

Biometric authentication refers to the use of *physiological* and *behavioural* biometrics to authenticate users [41]. No secrets are used to authenticate a user. This type of authentication relies on matching patterns of user characteristics or behaviours that are unique and distinguished [42] and assumes that similarities of these characteristics or behaviours cannot be found in two or more users (see Figure 2-6).

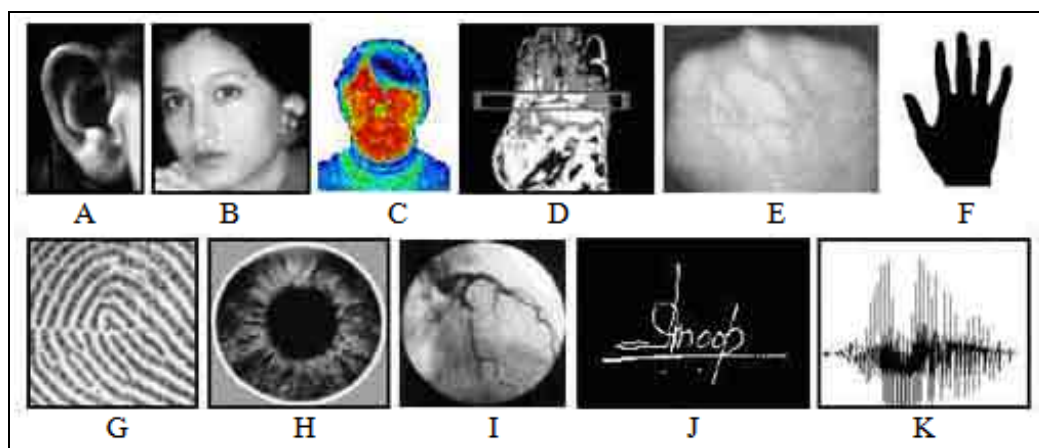


Figure 2-6: Biometrics: A) ear, B) face, C) facial themogram, D) hand thermogram, E) hand vein, F) hand geometry, G) fingerprint, H) iris, I) retina, J) signature, and K) voice

Photo source: <http://www.instrumentalanalysis.com/images/biometrics.jpg>

Biometric authentication overcomes the drawbacks of other authentication classes (i.e., users tend to forget passwords and lose tokens). Unlike conventional passwords and tokens, biometrics cannot easily be shared or duplicated. They always accompany the user and they cannot be forgotten. However, not all people are willing to put part of their body in a machine or to accept a laser beam directed into their eye for retinal scans. In addition, some people are disabled (e.g., lost fingers or eyes) and cannot utilize the biometrics authentication class due to the nature of their limited abilities.

Biometric authentication's underlying technology is even more expensive than authentication technology involving tokens due to the high tech infrastructure required to

process authentication data, especially if implemented on a large scale [43]. Furthermore, there are accuracy issues related to what is known as false negative and false positive rates. False negatives occur when the biometric recognition device denies access to an authentic user while false positive errors happen when it allows access to an unauthorized user. This usually happens because matching captured patterns against stored templates will never result in an exact match, unlike other authentication classes where authentication is only processed if there is a 100% match between the stored factor and the entered value by the user. Exact matches in biometrics authentication cannot be achieved due to the noise usually associated with the biometrics sensors [44] such as sensing device, humidity and biometric position.

Despite the high security offered by biometrics, they are not impossible to break. Contact lenses and sticky residue can be used to capture iris data and fingerprints, respectively [43]. A behavioural pattern can be captured in the browser or by manipulating the scanner [45] before it's sent online. Besides, biometrics are very hard to change or replace; therefore, if an attacker intercepts a biometric pattern, the pattern will often match that of the user and it can then be replayed to compromise the user's account [46].

2.2.4 Others

The three afore-mentioned authentication classes are considered the core authentication techniques that have formed the basis for most of the authentication mechanisms implemented in the industry. However, new authentication technologies have been introduced recently to form extra authentication classes: *relationship-based*, *process-based*, and *location-based authentication technologies*.

2.2.4.1 Relationship-based authentication (RBA)

Relationship-based authentication (referred to as social network authentication by [47]) or the *somebody you know* authentication class was first introduced by [48]. It is an authentication protocol based on the classic human social relationship. The study classifies authentication into two categories: primary and emergency. The primary authentication occurs where a user is usually authenticated to a system using token-based authentication (TBA) (i.e., the study takes RSA SecureID as an example of TBA). The latter occurs when the primary authentication factor (the token) is not available, and therefore, other alternative means should be available to authenticate the user. The RSA Security Inc.

SecureID is a one-time code calculator/generator that usually comes in forms like cards or key fobs. These generate what is called a tokencode or a passcode every given period (i.e. usually 60 seconds). This time-based tokencode is calculated based on time and other user details like PIN. This setup assumes that the account owner must provide a username, PIN, and the tokencode generated by the SecureID to authenticate into a system successfully.

The fourth authentication factor comes when the SecureID is not in working order or is not available for some reason (i.e., lost, stolen, or maybe the user has forgotten the device at home or work). RSA [48] illustrates how the proposed fourth authentication factor should work in the following scenario. The authentication is done collectively between two people; one of them is the account owner (identified as asker) and the other one is a trusted party (identified as helper) who was enrolled in the system to help authenticate the asker. The helper has no other roles or privileges to access the asker account and the only role assigned is to request a vouch code - a server generated code that substitutes the tokencode usually generated by the RSA SecureID - from the server. The helper then passes the code on to the asker. This is illustrated by Figure 2-7.

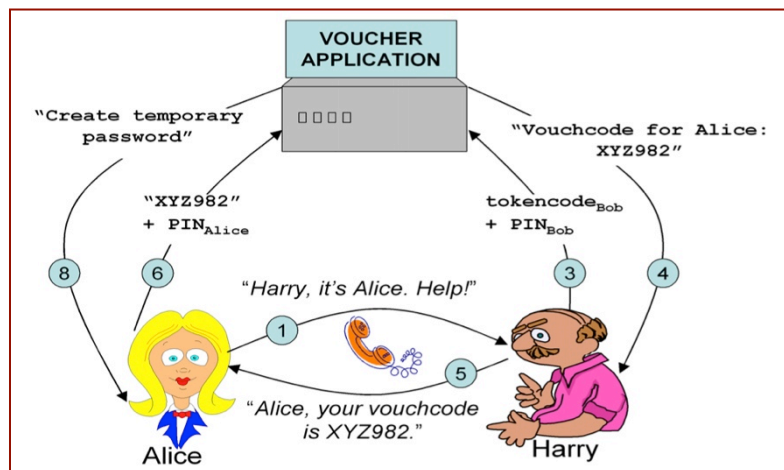


Figure 2-7: Vouching authentication mechanism [48]

When the asker's token is not available, it is not possible to acquire a tokencode to initiate an authentication procedure. Therefore, the asker contacts the associated helper (this association is first identified at the enrolment time based on certain policies defined by the online service provider) in a way that the helper would be able to confirm the identity of the asker (i.e., by a phone call or a direct face-to-face contact). Once the helper confirms the identity of the asker, and after the user requests help, the helper connects to the service provider's server and through a specific vouching system page where a two-factor authentication mechanism is implemented, the helper is able to login. Once successfully logged-in, the helper has to specify the person's identity and the system will check if there

is a valid association between the helper and the given asker in the database. If a record is found, the system will generate a vouchcode and a session that are both valid for a given period (i.e., defined by the service provider's policies). The helper then passes the system-generated vouchcode to the user using a secure channel. The study suggests that the exchange of vouchcodes must not be carried out by e-mail and only exchanged by other more secure means like phone or face-to-face.

The asker, at this point, has a time-based (i.e., something between 1 to 2 days) vouchcode which can be used along with the username and PIN number, known to the asker, as authentication factors to access a given page on the service provider's system to generate a time-based password of the asker's choice. This step is important, as the user-defined passwords are easier to remember than the system-generated vouchcodes. The username, PIN, and the newly created password can then be used to authenticate the asker to the system for a restricted period. The process can be repeated for as long as the token used to generate the tokencode is out of order.

This authentication method is unsuitable for day-to-day authentication tasks and can only be used in situations when a password reset is needed by the account owner. The implementation proposed by Brainard has usability issues. For instance, the helper must have an Internet connection when the account owner requests a vouchcode. Without an Internet connection, the helper will not be able to request a vouchcode for the asker. This could also affect the relationship between the helper and the asker if the helper is usually unable to offer the asker a vouchcode.

Nevertheless, the potential of this authentication technology as a secondary authentication method is very high. It is a cost-effective alternative option to call centres and help-desk services when a password reset is needed. A better implementation design (discussed in Chapter 7) can overcome all the usability issues discussed above.

2.2.4.2 Process-based authentication (PBA)

Also known as *something you process* class of authentication. This type of authentication method is based on human ability to process things. That is, instead of requesting the user to enter a password into a machine, the system will rather ask the user to perform mathematical or logical operations based on secrets known to the user combined with variable inputs provided by the system. The output of such a process should form an

authentication pass that will construct an authenticated session between the user and the system.

An example of this authentication methodology was presented by [49]. The user is requested to do a mathematical operation (+, -, *) based on a formula (password) and numbers assigned to letters randomly that appear on the screen (see Figure 2-8). Here, the user is not asked to enter the password for authentication, the system will rather ask the user to recall the formula, which is actually the password, and process it based on a given set of letters/numbers. The result of the calculations should form a one-time password that allows the user to login to the system successfully.

Log on to System					
A:2	B:9	C:7	D:7	E:5	F:1
G:8	H:4	I:3	J:1	K:5	L:0
M:4	N:6	O:1	P:0	Q:5	
R:2	S:3	T:0	U:9	V:9	
W:6	X:1	Y:4	Z:7		
Answer: <input type="text" value="14"/>					
Log On		Cancel			

Figure 2-8: PBA class by [49]

This system involves more than one activity: recalling the formula and performing mathematical calculations at the primary level of the authentication process. The main reason behind introducing this type of authentication method is to protect users from attacks like shoulder surfing, brute-force, guessing, dictionary, and social engineering attacks. It actually further helps users from more sophisticated attacks like man-in-the-middle and phishing. A user never needs to enter the password into a machine, and therefore, capturing the password on the fly or while it is being entered into the system is not possible. The answer or authentication factor entered by the user, which is the result of the computational process, changes every time the system requests the user to enter a password. This is because the formula the user uses to process the answer depends mainly on the random figures appearing on the screen, which change every time the user needs to login.

This system, however, is time consuming and cognitively demanding, far more than other conventional KBA mechanisms. As mentioned above, the primary phase of authentication

is split into two phases: recalling and processing. The latter will take extra time and users might consider using pen and note to do the calculations if their formula is somehow complex or long. This poses a severe security issue, as these notes are prone to theft.

2.2.4.3 Location-based authentication (LBA)

Location-based authentication is about authenticating a user based on his or her presence at a distinct location. Implementation of location-based authentication is currently limited in online systems, unlike the wide range of its implementation in the physical world. Applications like buildings' automatic doors are common systems that use LBA to operate. In the literature, Denning and MacDoran [46] were the first to propose location-based authentication for computer systems. They claimed that LBA was a new authentication class by itself and formed a new dimension to user authentication and access control. They proposed the use of a location signature (LS), which defines the unique physical location of a particular user or network terminal at a given time, and is created by a location signature sensor (LSS). The implementation of this proposal is based on the microwave signals transmitted by satellites that are part of the global positioning system (GPS). An independent device can be used to determine the geodetic location - latitude, longitude, and height in a precisely defined geocentric coordinate reference system.

A patent was recently registered by [50] which utilizes the location-based authentication approach for online banking and other financial firms' transactions using mobile devices. The invention suggests the use of a location-based system to check if a mobile device, such as a cellular telephone, is proximate to the computer being used by the customer in the transaction. Based on the result, the system can decide whether to accept or reject the requested transaction. An assessment risk should define the level at which this proposal should be implemented. For example, systems that present information of low-risk after the user logs in can implement this approach at the transactional level only, while systems posing high-risk information after the user log-in should implement it right at the beginning.

The implementation of location-based authentication in general offers many advantages over other authentication classes. The use of open proxy servers has become a major source for launching online attacks [51]. IBM reported in 2009 that the number of online proxies have tripled in the past two years [52]. The main reason for using proxy servers is the anonymity they offer for the attackers to hide their online behaviours. It becomes infeasible for a victim to trace the original source of such attacks. Therefore, restricting

online account access to specific locations defined by the user (e.g., office, home, and mobile device) could be the best possible solution to protect user accounts against anonymous attacks.

LBA also offers a solution to session hijacking attacks. Sometimes users leave their session open without logging out on a terminal they are using to connect to different online accounts. Any other user who uses that terminal can utilize the opened sessions to impersonate the legitimate user. This is most common on online applications that allow a long period before an idle session is automatically destroyed. LBA can solve this by authenticating the user's mobile device location continuously. If the user connects to the account from a terminal, a session can be built based on the location of devices, the terminal used, and the user's mobile device. This session should remain active as long as the user did not logout and both locations are identical (with enough location error margin based on the accuracy of the geodetic location system). If either of these two conditions changes, the application should automatically destroy the session. This feature makes LBA a good authentication method to implement in conjunction with single sign-ons [46].

Despite the advantages of LBA mentioned above, there are a few limitations. Since GPS signals are used to authenticate users based on their locations, its performance in certain environments and for some applications can be quite limited [53]. This is mainly due to the GPS signal that cannot penetrate water, soil, walls, and other obstacles. In addition, the accuracy of the location has an error rate of a few meters sometimes and cannot guarantee the exact location point. Moreover, there are privacy concerns about LBA. The system could be used to track an individual's location, especially when continuous authentication is active. Therefore, access to, and dissemination of, users' location information that has been collected for authentication purposes should be strictly limited [46].

2.2.5 Summary

Table 2-1 presents a summary of different authentication classes covered in the literature along with some examples currently implemented in the market.

Class	Examples	Advantages	Disadvantages
Knowledge-based (KBA)	<ul style="list-style-type: none"> • Secret questions • User ID and password • PIN 	<ul style="list-style-type: none"> • High user-acceptance • Easy to implement and administer • Cheap to deploy and maintain 	<ul style="list-style-type: none"> • Can be shared • Users tend to re-use • Subject to guessing and reply attacks • Prone to eavesdropping • Can be forgotten
Token-based (TBA)	<ul style="list-style-type: none"> • Magnetic stripe cards • Contactless cards • Smart cards • Badges • USB drives • Mobile software • Keys 	<ul style="list-style-type: none"> • Ease of use and management • Cheap to implement • Better accountability as tokens are tangible • Matured and widespread • High user acceptance 	<ul style="list-style-type: none"> • Can be shared • Can be duplicated • Susceptible to loss and damage • Can be stolen and re-used • Requires hardware to replace • Limited lifetime
Biometrics based (BBA)	<ul style="list-style-type: none"> • Fingerprint • Face Iris • Voice print 	<ul style="list-style-type: none"> • Difficult to share or duplicate • Repudiation unlikely • Forging difficult • Cannot be lost or stolen 	<ul style="list-style-type: none"> • Expensive on wide-scale • Availability issues • Low user-acceptance • Accuracy issues • Reliability issues under abnormal conditions • Patterns can be captured and replayed
Relationship-based (RBA)	<ul style="list-style-type: none"> • Vouchcode 	<ul style="list-style-type: none"> • Cost-effective 	<ul style="list-style-type: none"> • Social relationship issues • Availability
Process-based (PBA)	<ul style="list-style-type: none"> • Mathematical calculation 	<ul style="list-style-type: none"> • Secret is not involved in authentication process • One-time factor 	<ul style="list-style-type: none"> • Time consumption • Limited audience
Location-based (LBA)	<ul style="list-style-type: none"> • Location signature via GPS 	<ul style="list-style-type: none"> • Cannot spoof • Easy to trace attacks • Continuous authentication • Protect against session hijacking • No secret to store or manipulate 	<ul style="list-style-type: none"> • Users privacy • Location accuracy error rate • GPS limited signal coverage

Table 2-1: Summary table of different authentication classes

2.3 Authentication Implementation

The previous section reviewed and discussed different authentication classes proposed in the literature. Many arguments, however, also exist in the literature and in industry about how these classes should be implemented in real applications. This section discusses different authentication mechanisms based on the classes covered by the previous section. These mechanisms are *single-factor*, *multi-factor*, *multilevel*, and *multi-channel* authentication mechanisms.

2.3.1 Single-factor Authentication

This is the most basic and widely implemented authentication mechanism in information technology. Knowledge-based factors (e.g., password, passphrase, and PIN) are the most commonly used factors (discussed in section 2.2.1) and users accept this authentication mechanism as the most usable.

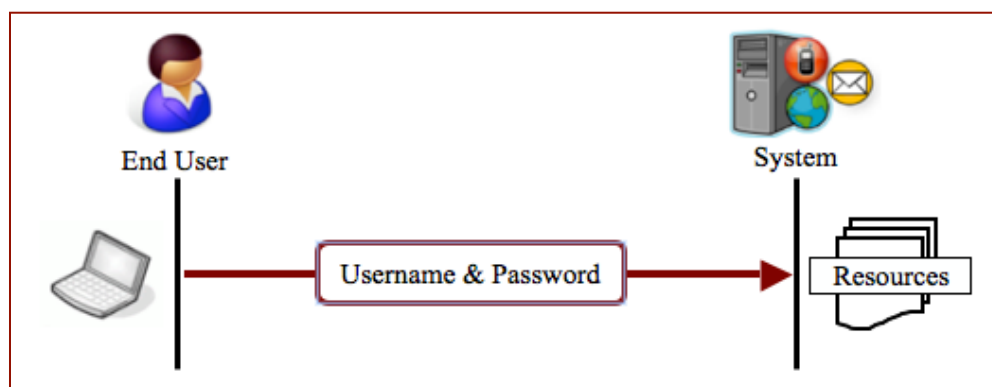


Figure 2-9: Single-factor authentication mechanism

Single-factor, in terms of security, is the weakest authentication mechanism among all other mechanisms. The fact that this mechanism utilizes only a single factor (e.g., password), which is passed to the other end using a single channel, makes it prone to many different attacks covered in section 2.4 (see Figure 2-9).

2.3.2 Multi-factor Authentication

Some organizations propose the use of multi-factor authentication to counter the weaknesses of the single-factor mechanism. This is implemented by adding extra authentication factors to the process of authenticating a user into a system (see Figure 2-10). For instance, an online banking application requests the customer to enter the bank

card number. After the application verifies the card number (i.e., a unique number identifies the customer record in the bank database), the customer is asked to enter a secret answer to one of the questions this customer has previously answered at enrolment time. If the customer answers correctly, the application finally requests a password to allow the customer access to his or her account (a similar real case is discussed in detail in section 4.1.3.3).

In terms of security, multi-factor authentication offers better protection against several attacks such as guessing, brute-force, and phishing (discussed in section 2.4). However, the one channel used in this mechanism is the weakest part because, if the channel is compromised, all factors exchanged between the end-user and the system can be captured accordingly.

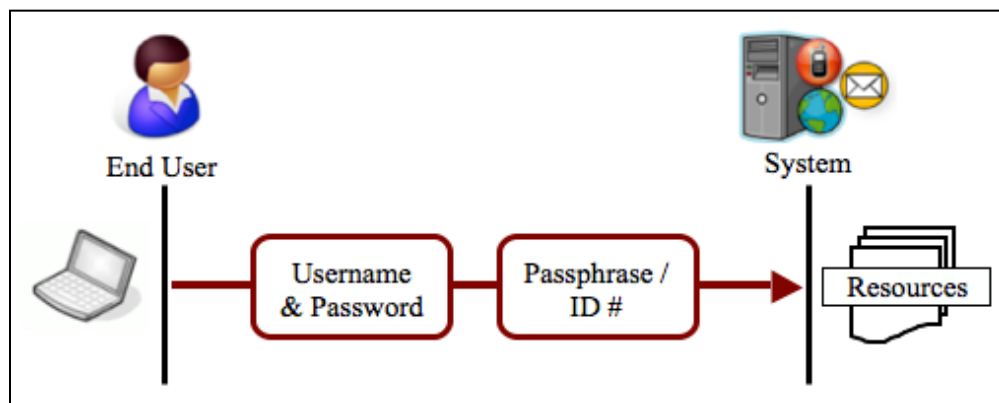


Figure 2-10: Multi-factor authentication mechanism

2.3.3 Multilevel Authentication

Some businesses have implemented multilevel authentication mechanisms [26]. This can be achieved by allowing users limited access to the system resources after their initial login. The user is requested to submit a secondary secret factor (e.g., password, passphrase, or PIN) to access other restricted resources (see Figure 2-11). The main reason behind this upgrade was to secure the critical transactions within the system from attacks such as eavesdropping, social engineering, phishing, and others if the first authentication factor was compromised. A good example of such a mechanism can be found in most of the current online banking applications (OBAs). These OBAs allow bank customers to login to their online banking account using a password. However, to pay utility bills, or to transfer money, the customer has to provide another password or passphrase to authorize the transaction (i.e., known as multilevel authentication).

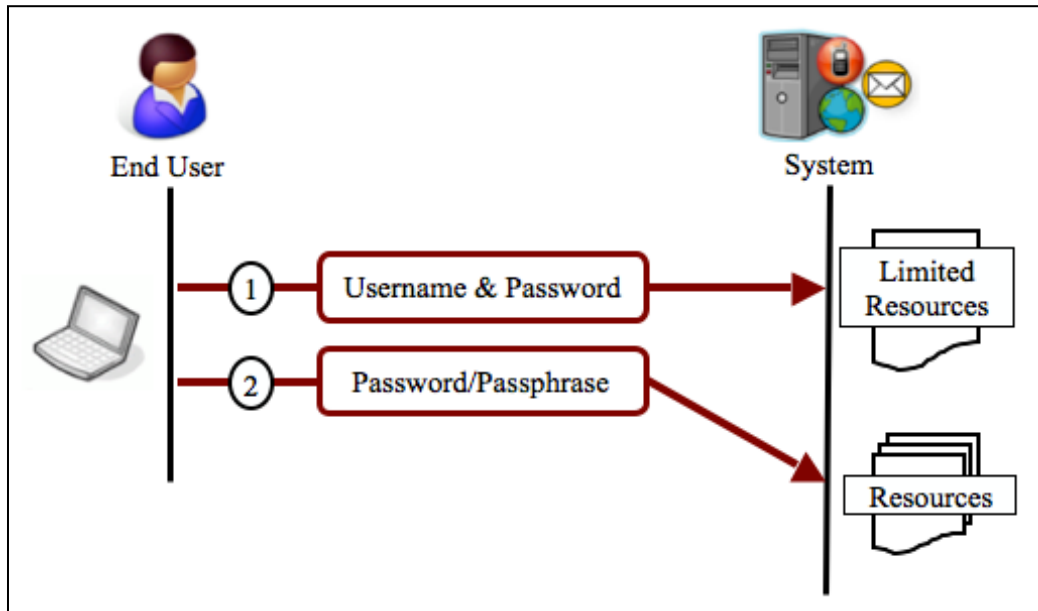


Figure 2-11: Multilevel authentication mechanism

2.3.4 Multilevel, Multi-channel Authentication

Although the multilevel authentication mechanism has improved overall security, it has not eliminated the fear of the kinds of attacks that could compromise all security levels (e.g., real-time phishing/pharming (RTP/P), and malware [27]). An attack like man-in-the-browser (MITB) can simply alter transaction details before they are sent to the OBA without the user knowing that such an alteration has occurred. The customer, therefore, authorizes the transaction (e.g., payment or money transfer) by entering the second authentication factor whenever the OBA requests it for final check.

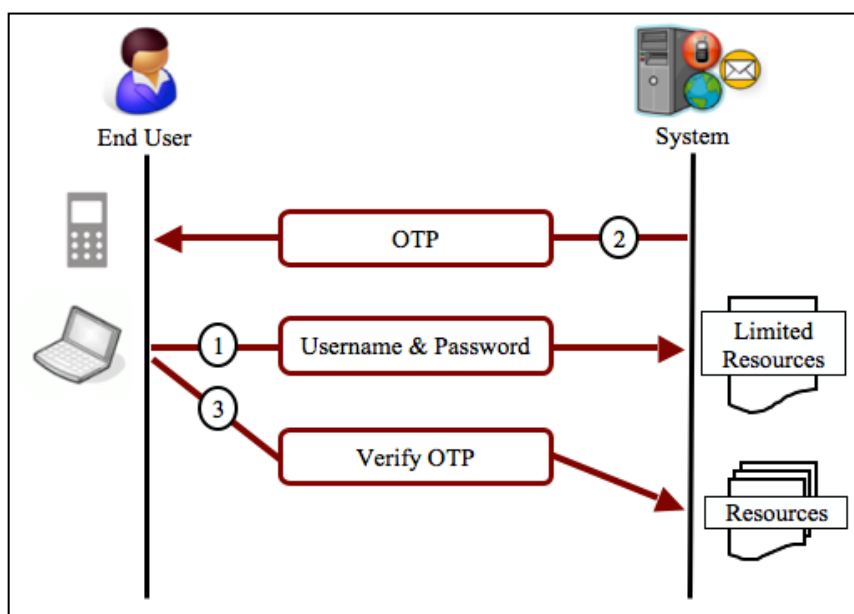


Figure 2-12: Multilevel, multi-channel authentication mechanism

To overcome such multilevel weaknesses, some organizations, especially financial firms, which comprise the sector most affected by online attacks (see section 2.4.3.5), have improved the way multilevel authentication is implemented in online banking by integrating the multi-channel authentication (MCA) approach (Figure 2-12). MCA works just like multilevel authentication but uses independent channels (e.g., web channel combined with mobile network channel). For instance, the primary authentication factor is delivered using the web channel while the secondary authentication factor is delivered to the customer via an SMS using the mobile network infrastructure (see Figure 2-13).

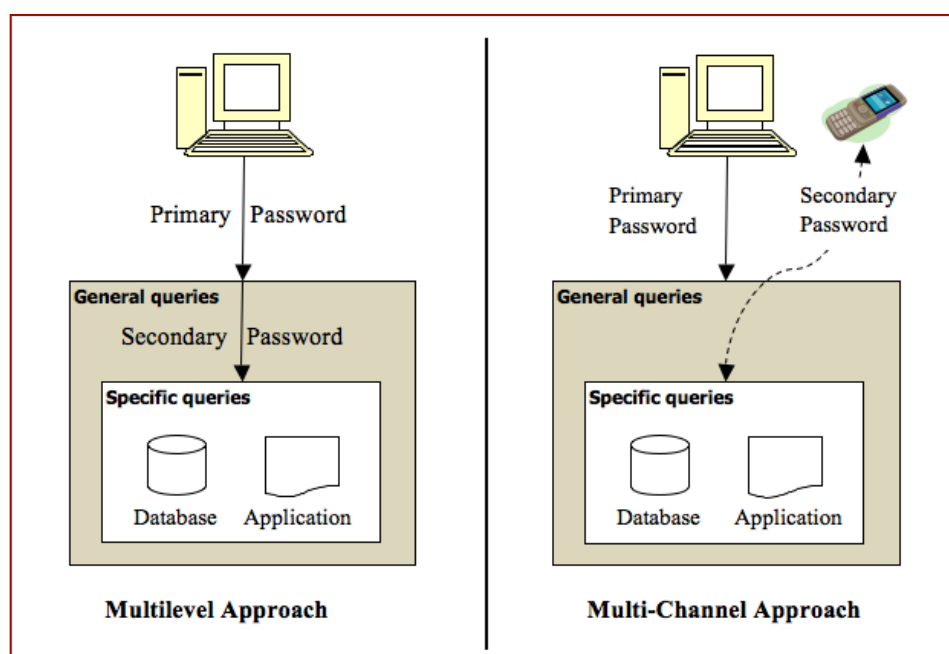


Figure 2-13: Multilevel, single channel approach vs. multilevel, multi-channel approach

Figure 2-13 illustrates the difference between multilevel, single channel and multilevel, multi-channel authentication mechanisms. In multilevel, single channel authentication, only one channel is used to deliver and receive authentication factors for different OBA levels. If that channel is compromised, all exchanged factors can be compromised accordingly, whether the communication channel is encrypted or not. Attacks, such as MITB, are able to capture exchanged factors at end-user's browser level even before these factors are encrypted and sent to the other side (MITB attacks are covered in Section 2.4.3.8).

Multilevel, multi-channel authentication (referred to as multi-channel authentication or MCA in this thesis), as a protocol, has been implemented by different systems for increased security. The most commonly used channels for authentication along with the Internet channel are the telephone and cellular networks. For instance, a patent filed by

Goldthawite [54] suggests the use of mobile devices to authorize card payments. Another by Yates [55] also suggests the use of mobile devices to authorize payments for vending machines. The proposed scenario suggests that the user enters the transaction details as well as the mobile phone number into the vending machine. The machine establishes a connection with a service provider, which in turn, contacts the user through the mobile network and requests a one-time pin number as an answer to an automated call or by entering them directly into the vending machine along with a PIN number known only to the user [55].

There are also many commercial products and services, such as Identrica [56], SAINTlogin [57] and Lloyds TSB [58], which offer multi-channel authentication services using telephone and mobile networks. Identrica requests the user to enter the access login details along with the mobile number into a login page. Then, to complete the login process, the user has to call a given number of the company. The company's system does not answer the call but checks the caller number to verify if it matches the customer's phone number who just submitted login credentials. If it matches, the user is allowed full access to the system.

SAINTlogin offers the same multi-factor, multi-channel authentication mechanism. However, here the system provides the user a random phone number, which will only be allocated for single login sessions. The user has to call that number to be granted access to the system.

Lloyds TSB, on the other hand, offers the same multi-factor, multi-channel authentication mechanism but the bank is the caller in this case. The customer initially must register different phone numbers with the bank. After registration, the user can create new beneficiary accounts or standing orders online that cannot be activated without answering a phone call from the bank and entering a one-time pin number shown in the screen.

MCA is currently offered by different commercial applications in a number of different ways. It is vital for any business to carry out a risk analysis and verify the need for MCA before implementing it. The following section discusses the flexibility of MCA in meeting the different requirements of many types of online applications while maintaining security and usability.

2.4 Authentication Attack Methods

Improving security and hardening authentication protocols is the ultimate need for every organization around the world. This ranges from physical access controls to biometrics authentication. To some extent, everyone in this chain requires security to thwart possible illegal break-ins or attacks to their systems. Security measures have evolved over time and there is a great deal of work being done in this area. However, no matter how secure the system is, there will always be a chance for someone to break it [59]. So hardening authentication tokens provides only limited and temporary security until an attacker discovers a new way to break the encryption.

This section presents a discussion of attack methods, categorizing attacks based on each of the following core Internet communication elements: *online service provider (OSP)*, *the communication channel (CC)*, and *the end user (EU)*.

2.4.1 Attacks on Online Service Provider (OSP)

An Online Service Provider (OSP) is any organization that provides an electronic service for users via the Internet. This includes online banking services provided by banks, electronic mail services provided by companies like Microsoft, Google, and Yahoo!, and other online services that are owned and managed by individuals and are hosted by different data centres around the world (e.g., Internet relay chat (IRC), social community forums, hosting services, online file sharing, blogging, and online gaming).

There are many reasons why attackers target OSPs. Some aim to utilize the OSP resources for illicit materials [60]; they might store hacking tools and pornography and set the server to be part of a DDoS attack (more information about DDoS is available in section 2.4.1.1). Others attack OSPs to steal services or valuable files, to spy on friends and family members, or to build reputations, especially if attacking well-known high profile or secured organizations where there are clashes of interests related to politics and religion (e.g., [61, 62]).

The following sub-sections discuss the types of attacks that target OSPs.

2.4.1.1 Denial-of-Service Attack (DoS)

This type of attack aims at making the OSP's online services unavailable or unreachable to users, turning services down. Denial-of-Service (DoS) is about involving only one source (i.e., a single person or a group of people) to exhaust OSP resources, such as network bandwidth, computing power, or operating system data structures, and to limit or stop completely the delivery of services to end users. However, the DoS has been improved to a distributed denial-of-service (DDoS). DDoS involves many different sources on the net (known as zombies or bots after they are successfully compromised by the attacker [63]) to form botnets (see Figure 2-14a). Botnets are usually controlled by one attacker and aim at initiating DDoS attacks or spreading spam and phishing e-mails [64].

DDoS attacks one target, usually by overloading the server offering the services with heavy traffic initiated by zombies (infected computers) so it becomes slow and unable to process further requests by legitimate users.

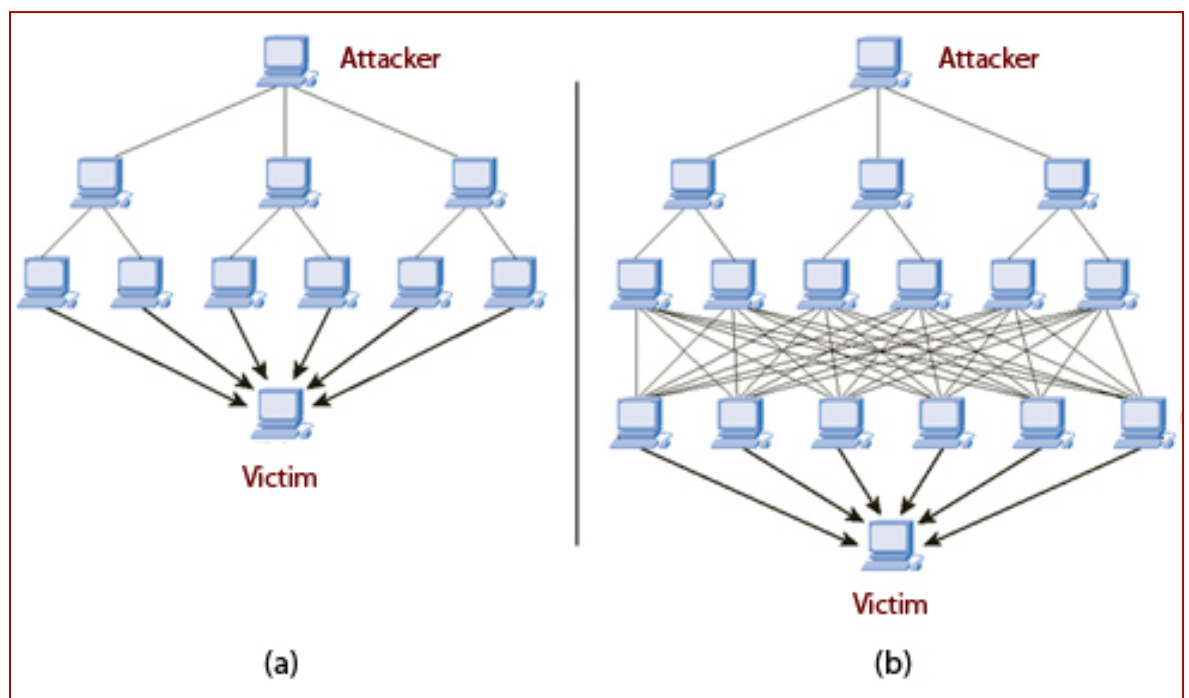


Figure 2-14: Botnets: a) DDoS, b) DRDoS attacks [65]

Another sophisticated version of DDoS has more recently been introduced. This improved version is called the distributed reflection denial-of-service attack (DRDoS). Unlike DDoS, the DRDoS involves another layer of computers in the attack. These computers are not actually infected or compromised (not zombies) and their users do not really know that they are involved in a DRDoS attack. This usually happens when an attacker compromises different computers on the Internet, which in turn, try to infect other uninfected computers.

However, the source address of these connections is altered to reflect the victim's OSP IP address. The uninfected computers think that the OSP is trying to establish a connection with them and they cumulatively send heavy traffic back to the OSP server as replies to the fake requests received by zombie machines (see Figure 2-14b).

The first known attack using DoS was recorded when Panix, the New York area's oldest and largest Online service provider, was attacked from unknown sources on September 6th, 1996 [66]. However, Spanish police caught the biggest DDoS attack ever known in 2010 when three people were controlling nearly 13 million zombie personal computers from 190 different countries [67]. This included computers inside more than 1000 companies and 40 major banks around the world.

2.4.1.2 Website/application Manipulation

Website/application attacks are considered the most common attacks targeting OSPs with 49% of total known OSP attacks [52]. Unlike DDoS, which normally causes temporary denial of service, manipulation of website site contents or the web application database can be very harmful and destructive in nature if recovery plans are not properly set by the OSP management. For example, an SQL injection type of attack, where database SQL statements are injected into the URL as a query string because of poorly designed web application, can allow the attacker to gain administrative privileges for a security-policy maintained web application. The attacker can also wipe all database records, and if there were no proper frequent backup rules set in place, especially for an interactive web application, updated frequently by the OSP and customers, this can cause severe implications for the OSP's reputation and its online business.

There are many types of website/application manipulation attacks; the most common ones are the SQL injection and cross-site scripting (XSS). The latter is usually used to hijack users' cookies or sessions. XSS comes in two forms: *non-persistent* and *persistent*. Non-persistent attacks cannot be carried out unless the attacker is able to contact the victim user by e-mail or other means to pass a crafted link with a malicious code. Once the user clicks on the link, it opens a legitimate website the user visits that may have an account that is authenticated by a cookie stored in the user's machine. The malicious code injected in the link will be executed by the user's browser after it is rendered by the website the user visits. Depending on the code functions, it can copy the user's cookie or session and pass it on to the attacker (see Figure 2-15a).

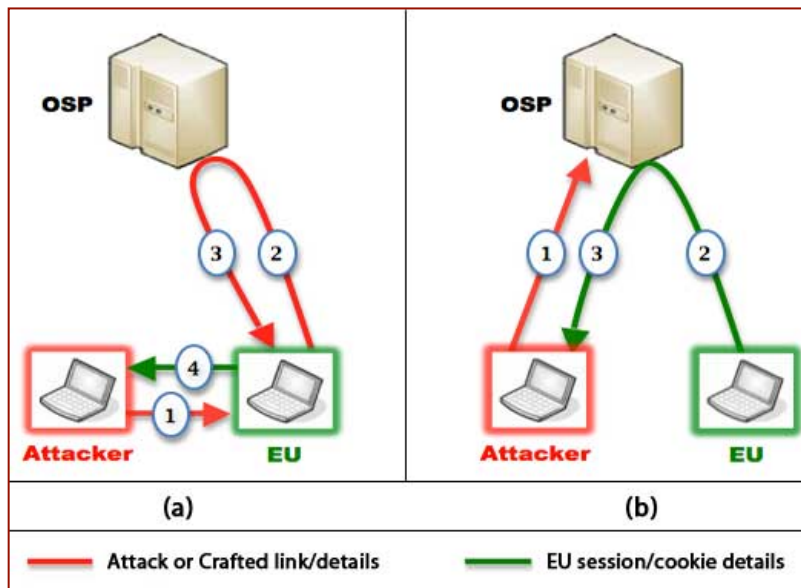


Figure 2-15: (a) Non-persistent XSS attack; (b) Persistent XSS attack

Persistent XSS attacks are more dangerous and can affect more than one user at a time. This usually happens on web applications like message boards and blogs where the attacker can inject the malicious code in the page itself and then access all users' sessions (see Figure 2-15b).

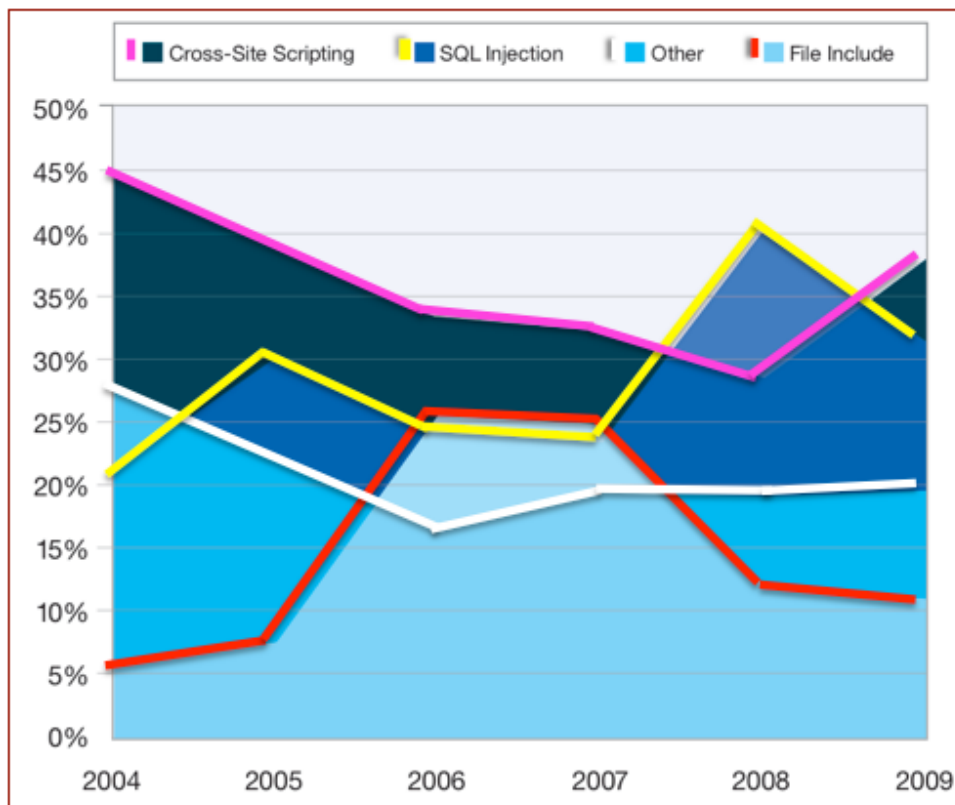


Figure 2-16: Web-application vulnerability disclosures by attack categories 2004 – 2009 (adapted from [52])

SQL and XSS injections as well as other website/applications manipulations usually attack web applications with poorly written validation controls. Figure 2-16 presents web-application vulnerability disclosures by attack categories between 2008 and 2009. It also shows how the number of Cross-Site Scripting surpassed SQL Injection disclosures in 2009, putting it back as the web-application top vulnerability for the year 2009 [52].

2.4.1.3 Brute-force Attack

This type of attack aims at compromising users' accounts at the server level by randomly checking the validity of usernames and passwords with infected zombie personal computers. Usually this happens in a distributed manner as discussed in DoS attacks. The response of the OSP is recorded and passed back to the original attacker. This can be either an invalid username and password or a valid session establishment, which normally means a valid username and password.

2.4.1.4 OSP Security Policy Violation

The study [68] identified security policy (SP) violation as one of the factors that could result in a successful online banking attack. An employee may cause an internal security incident and expose customers' information if violating the OSP's security policies while there are weak access controls and logging mechanisms. This also could lead to unauthorized access to the OSP's servers.

Unauthorized access showed a dramatic increase and replaced denial of service as the second most significant contributor to computer crime losses, accounting for 24 percent of overall reported losses and showing a significant increase in average dollar loss.

10th CSI/FBI survey (2005) [69]

In the digital world, improper definition of a web application's SP or violations to SPs could result in an attacker being able to acquire administrative privileges by attacking an employee's machine. This usually happens when an employee, who has administrative privileges to access the OSP's servers, is accessing the OSP local network while, at the same time, is connected to other public web services like e-mail, chatting, and social networking sites from the same machine. The computer here is the weakest link because personal computers are usually prone to attacks like viruses, worms, Trojans, and other common malware (see Figure 2-17). A good security policy would strictly disallow

employees to connect one machine to the local network and to the Internet at the same time.

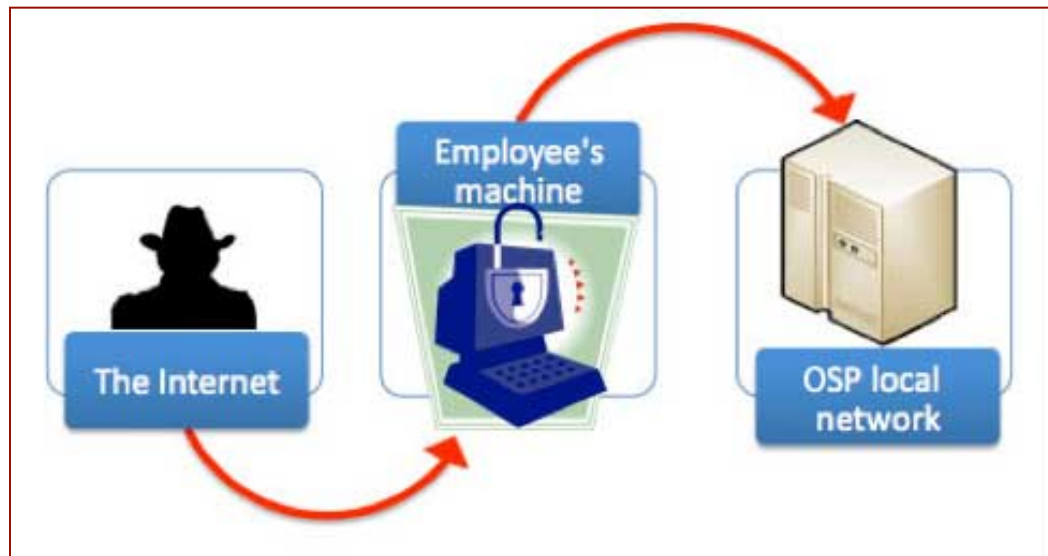


Figure 2-17: Security policy violation

2.4.2 Attacks on Communication Channels (CC)

This type of attack focuses on communication channels between the EU and OSPs. It could be limited to a local area network LAN (e.g., home or office networks) but could have a more far-reaching effect if an attacker is able to attack wide area networks (WAN) (e.g., telecommunication companies that provide Internet services to others). This section discusses three common attacks targeting CC: sniffing, man-in-the-middle (MITM), and session hijacking.

2.4.2.1 Sniffing

Sniffing is a type of attack that compromises the communication channel between the end-user and the OSP. The attacker uses sniffing to listen to and interpret the data exchanged between the parties, and therefore, is able to capture factors sent by the user for authentication and authorization. This kind of attacks is passive and does not alter the data exchanged between the communicating parties.

2.4.2.2 Man-in-the-middle attacks (MITM)

This type of attack allows an attacker to intercept the data exchanged between the EU and the OSP. Unlike a sniffing attack, man-in-the-middle is a real-time attack and has the

ability to alter captured packets and to capture sensitive information about other websites directly from the user's machine (see Figure 2-18).

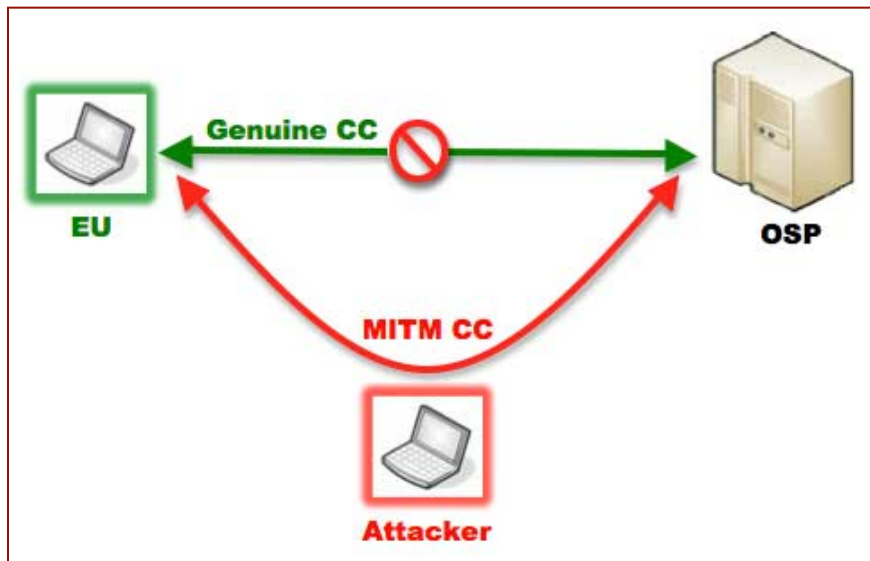


Figure 2-18: Man-in-the-middle (MITM) attack

A whitepaper by IBM [52] categorizes MITM attacks into passive and active attacks. Passive MITMs are those attacks that only listen, capture, and/or modify data transmitted between the EU and the OSP. However, active MITMs are more dangerous and are able to compromise the user's access credentials to websites that the user did not visit. This can be achieved by [70]:

1. Stealing the victim's session cookies for any other site.
2. Overriding Same Origin Policy for any other site, (this has the same impact as XSS).
3. Stealing the browser's saved passwords for any other site.
4. Poisoning the browser cache for any other site, (this will make the attack persistent).

Usually an active MITM depends first on the passive attack. They rely on HTML elements such as inline frame, also known as IFRAME. An IFRAME allows web authors to display multiple documents in one window [71]. This allows designers to keep one document visible while scrolling or replacing another. Among the many attributes an IFRAME has is the "src" attribute that allows the designer to include any web-document, internal or external, in an IFRAME. The HTML codes in Figure 2-19 show how an IFRAME can be used to include an external web-document/file into an existing web-document.

```
<HTML>
<HEAD>
<TITLE>IFRAME Element</TITLE>
</HEAD>
<BODY>
This is the main document body. Next an inline frame displays an
external document from example.com<br />
  <IFRAME src="http://www.example.com/foo.html" width="40" height="50"
    scrolling="auto" frameborder="1">
    Here is the external IFRAME document's body
  </IFRAME>
</BODY>
</HTML>
```

Figure 2-19: IFRAME element within HTML web-document

A user could be browsing a news website. The attacker injects a hidden IFRAME element in the contents coming from the OSP as a reply to a user request. This IFRAME will load another website of interest to the attacker where the user has an online account that can be accessed using a stored cookie file in the user's machine. The attacker will then use a passive attack again to capture the cookie's sessions that are loaded in the injected IFRAME, and therefore, will initiate a session hijack attack to impersonate the user and get access to the user account.

The success or failure of MITM attacks is not based on bugs or un-patched software residing on the EU's machine nor does it depend on what users are browsing at the time when the attack is launched. It is solely a matter of whether the network the user is connected to is secured and trusted or not. Public networks (especially those which provide a Wifi connection feature) are always unsafe networks, no matter what website the user is intending to visit [70].

2.4.2.3 Session hijacking

Session hijacking is usually a result of other attacks like sniffing, phishing and pharming (see Section 2.4.3), and MITM attacks; it utilizes the user's connection session ID to spoof the user's identity.

2.4.3 Attacks on End Users (EU)

Users remain the weakest link in security [72]. Online businesses' current attention is focused on the advances of attacks targeting OSPs and CCs [73] while neglecting the end users who are the only element that cannot be technically controlled [74, 75]. Schneier said

in [76]: “Security is only as good as it’s weakest link, and people are the weakest link in the chain”.

Some studies (e.g., [77, 78]) refer the weaknesses of users to the fact that people receive conflicting demands or do not receive proper support and training. Others (e.g., [64, 79, 80]) claim that users behaviour often appears to be the main factor behind security breaches, and therefore, users are considered an essential part of prevention and reduction of security incidents.

In this section, attacks that target end users to compromise their systems or online accounts are discussed in more details. In terms of methods used, these attacks by far outnumber the other, previously discussed attacks used to target other Internet communication parts (e.g., OSP and CC).

2.4.3.1 User surveillance

User surveillance is the use of hardware devices to monitor or record users' input to computers or teller machines (ATMs). It is electronic, over-shoulder surfing. This attack can capture user passwords/PINs used in the authentication process.

2.4.3.2 Token/notes theft

We mentioned earlier in section 2.2.1 that some OSPs implement system-generated passwords to overcome password guessing. On the other hand, making passwords hard to guess makes them hard to remember for legitimate users. Users tend to write their passwords down in a note when they cannot remember them [81]. Sometimes this also happens when a bank sets complex password policies to achieve hard-to-guess passwords and forces the user to select one that matches all the rules.

Token theft is another type of attack where users' tokens, like ATM bank cards, smart cards, mobile phones, OTP calculators, and other authentication tokens, are stolen. Although some of these tokens will not fully authenticate the attacker unless another form of authentication (e.g., PIN for ATM cards) is used, others do not need further authentication to be of benefit to the attacker. Examples of the latter tokens include those used for access control (i.e., key fob or contactless card used for accessing a building or a car park area) and older versions of ATM cards, which are still used by some banks in different countries, that allow swiping the card into a card reader without the need to verify further by PIN number.

2.4.3.3 Malware infection

This is considered the most common type of attack that targets users. A recent survey by CSI Computer Crime and Security [19] found that 64.3% of respondents cited malware infection as an incident they encountered in 2009. This was the highest rate among other attacks examined in the survey.

Malware could be a virus, a worm, a mobile code, a backdoor, a Trojan, or a rootkit. The installation of any such malware/malicious software can be used for different purposes (e.g., files corruption, controlling, storage, and turning to act as a zombie). However, all have the ability to capture authentication factors once they are installed in a victim's machine. Depending on how the malware is designed, it can pass these credentials to the attacker via e-mail or in an online form or it can allow the attacker to connect to the user's machine to collect these details. Other types of malware are programmed to carry out changes to the details transferred from/to the user machine where no further interaction by the attacker is required, (some examples of this type of malware are described in detail in section 2.4.3.8).

2.4.3.4 Social engineering

Social engineering attacks usually aim at stealing authentication factors by fooling the access credential holders. This type of attacks takes two forms: technical and non-technical. The credential holders may be the customers who are the account holders or even the support help desk people who have administrative privileges to access and reset customer credentials.

Non-technical social engineering attacks aim at deceiving users by means of convincing and trust building. For example, an attacker introduces himself/herself to the user as a banker or a technician and requests the user's credentials for help and support purposes. Another attacker calls the help centre, impersonates a legitimate user, and requests a password reset to the account. This kind of conversation takes place through a call or e-mail most of the time, as it is very hard or dangerous for the attacker to impersonate someone else and deceive a user or a help desk face-to-face.

Technical social engineering, on the other hand, involves other types of attacks such as phishing (see section 2.4.3.5) and pharming (see section 2.4.3.6). These require the

attacker to have technical or web development skills, usually to masquerade the OSP's web presence to capture users' access credentials.

2.4.3.5 Phishing

Phishing is an example of technical, social engineering where the attacker designs and hosts a fake page or website, which has the same look and feel of a legitimate website. Then the attacker invites people to submit log-in credentials using e-mails or instant messaging (IM) that claim to be from a legitimate source but contain links to the fake spoofed page or website. Figure 2-20 displays an example phishing e-mail message which introduces itself as if it comes from a legitimate HSBC source and asking the client to identify him/herself to the bank website using a misleading web link. That link displays a real valid link to hsbc.co.uk but the source (which is usually hidden) directs the client to a fake website hosted by another domain name.



Figure 2-20: Phishing attack via e-mail

According to an Anti-Phishing Working Group (APWG), financial and payment services are the industry sectors most targeted by phishing attacks with almost 72% of total attacks in the 4th quarter of the year 2009 [82]. A Gartner consulting firm study [83] recorded an increase in phishing attacks by 40% in 2008, where only 56% of the victims have recovered their losses (i.e., 56% of 5 million who lost money in the US as of September 2008).

2.4.3.6 Pharming

Pharming is yet another social engineering attack that targets end-users. Pharming and phishing implement the same techniques to capture end-users' access credentials. However, they use different strategies to complete this task. Unlike phishing, pharming attacks first compromise the user's machine to alter the host's file before the user is deceived and taken to a fake website. The host's file is a file residing in personal computers and used to speed up domain name resolution. When a user tries to access a domain name, if that domain name is not defined in the host's file, the machine will try to contact a domain name server (DNS) to resolve the IP address associated with the domain name. If it is defined in the local machine host's file, then there is no need to contact a DNS server.

This is more sophisticated than phishing techniques as it involves the altering of a file in the user's machine. It has a better impact than phishing as users will probably not notice that they are visiting a counterfeit website; the user is not required to click on a misleading link received by e-mail or found in a website because, whenever the user tries to access the actual website using its domain, the local hosts file will redirect the user to the fake website automatically.

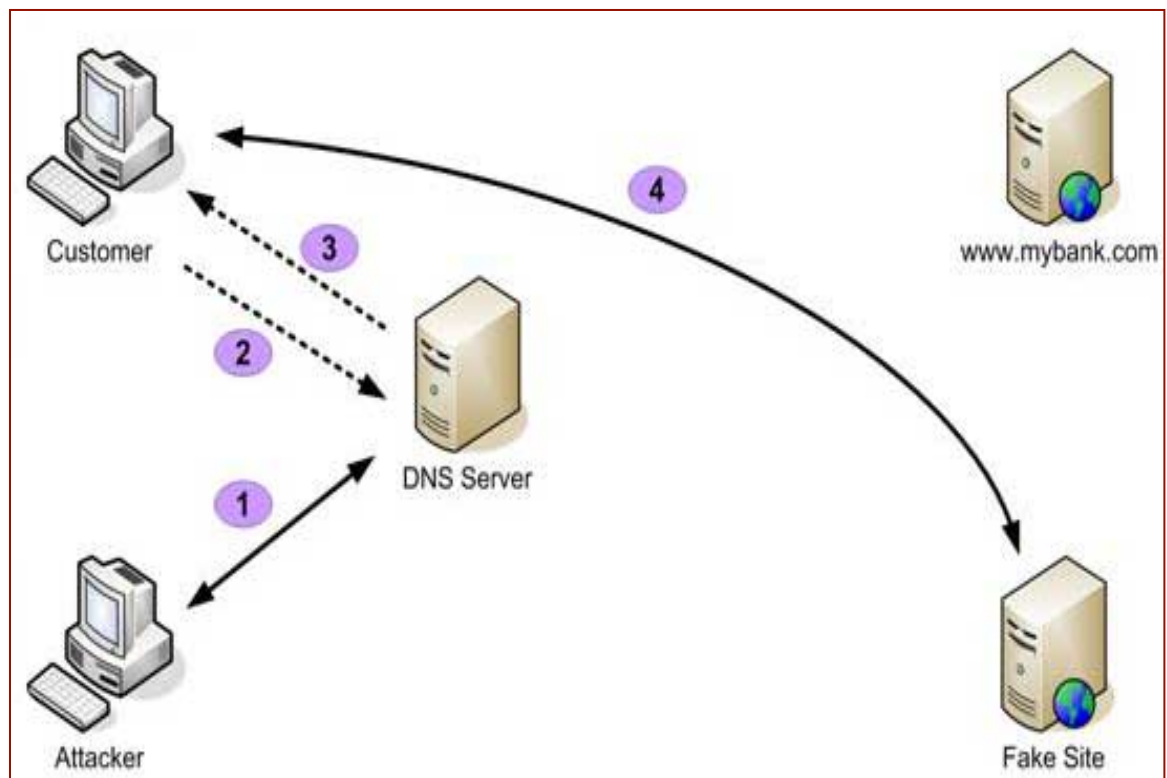


Figure 2-21: DNS spoofing attack [84]

More sophisticated and dangerous pharming techniques exist at network or communication channel (CC) levels. This happens when DNS tables of routers and servers are attacked and altered so they will redirect DNS resolution requests on a mass scale. This is known as DNS spoofing and is illustrated in Figure 2-21.

In the above figure, the attacker first attacks a DNS server and alters or adds an entry for `www.mybank.com` website so it will point to the different IP address of the attacker's fake website. Any customer requests for DNS resolution of `www.mybank.com` from the attacked DNS server will be redirected to the fake website rather than to the actual `www.mybank.com` site.

2.4.3.7 Clickjacking

Clickjacking, also known as user-interface (UI) redressing, is an attack technique based on HTML codes being used to hide a layer on top of the displayed contents to perform unexpected actions after the user clicks on it. This exploit was officially released to the public in 2008 but it has existed for many years [85]. It can be used in different ways. For example, an attacker can send an e-mail to a victim with an embedded video clip. The video clip has a play button, which, if clicked, installs malicious software into the user's machine (i.e., malware infection attack). This is achieved by placing an invisible layer on top of that button to run such an unexpected action.

A clickjacking attack has the ability to allow an attacker to completely control the victim's desktop; thus, it hijacks the victim's active sessions or captures the authentication factors exchanged with other sites.

2.4.3.8 Man-in-the-browser attacks (MITB)

A man-in-the-browser attack is one of the recently developed attacks that target users' machines (specifically users' browser software). It is a malware type of attack that installs itself in the user browser and has the ability to intercept and modify transmitted details before they are sent out to the OSP (see Figure 2-22). It also intercepts replied details from the OSP and is able to modify them before they are displayed in the user's browser. All of these alterations are performed in real-time and the user will find it difficult to identify the changes carried out by the MITB.

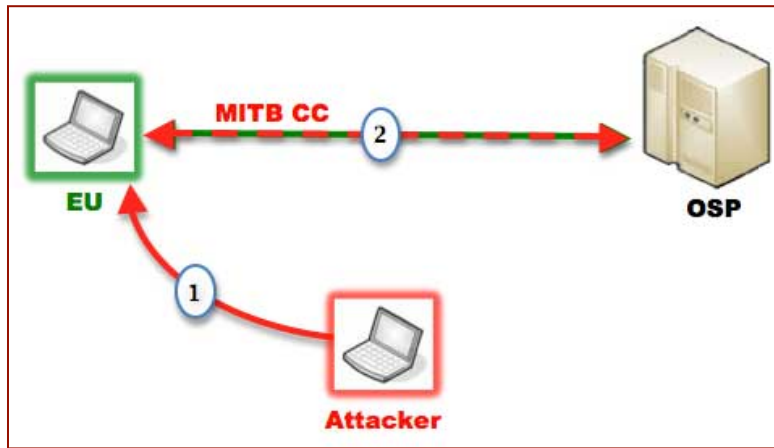


Figure 2-22: Man-in-the-browser (MITB) attack

MTIB is one of the most advanced attacks affecting organizations from around the world today [86]. It is considered a global threat and it mainly targets users for economic gain. According to RSA [86], one of the financial institutions in the UK reported a loss of £600,000 because of MTIB attacks.

2.5 Chapter Summary

This chapter covered the importance of authentication in distributed systems. It discussed different authentication classes found in literature and defined how they compare to each other. It then categorized the implementation of these authentication classes into four mechanisms: single-factor, multi-factor, multilevel, and multilevel multi-factor authentication mechanism. Finally, the chapter presented the most known attacks that target these authentication mechanisms. These attacks were classified, based on the communication node they target, into three categories: attacks on Online Service Providers (OSP), attacks on Communication Channels (CC), and attacks on End Users (EU).

The next chapter discusses usability and acceptability of information technologies. These two topics are vital to evaluate, in practical terms, whether any new technology proposed for implementation is usable and acceptable by customers or not. The next chapter forms the basis for the formulation of the hypotheses that will be tested and evaluated later in Chapter 7.

Chapter 3

Usability and Acceptability

3.1 Introduction

The increasing amount of interaction between users and Internet services, such as the Web, instant messaging and social networks, poses new and emerging security issues [87]. Despite the advanced new security solutions proposed by practitioners and academics, user perceptions of these new technologies are often ignored. These security technologies are designed to protect the users, but users are not usually consulted about their needs [88], or their perspectives of imposed usage considered.

End users of distributed systems perceive security and usability differently depending on context. For example, people's perception of security is more positive in the financial domain while more negative in other areas [89]. People tend to perceive usability more than security until they realize the importance of security after falling victim to an online attack that compromises their privacy or assets. Ignoring user perceptions of new technologies might result in dissatisfaction, leading users to abandon the service and look for alternative service providers. On average, one dissatisfied user will tell 13 other people about his or her experiences with the system [90]. Even worse, for every 30 users having problems with a system, only one user, on average, will call customer support. According to the same source, usually users do not complain to the company about usability issues and do not report them to the service provider. They usually prefer to abandon the service when they are dissatisfied.

Because of this, online organizations, especially banks and other financial sectors, must take care when implementing new security technologies. These particular technologies can affect users' overall acceptance if the organization does not research their attitudes as well as the technology's usability [91, 92].

In this chapter, section 3.2 defines usability history and its relationship with software quality. Within this section, subsections 3.2.1 and 3.2.2 cover usability attributes and

usability of authentication mechanisms. Next, section 3.3 pinpoints the various metrics used to evaluate usability in general and in online banking in particular. Section 3.4 discusses acceptability and its application to the adoption of information technology acceptance. Finally, section 3.5 lists the important variables from literature that are used to evaluate acceptability and information technology acceptance in the context of online banking.

3.2 Usability

The term “usability” first appeared in the 1960s [93] to define the ease with which people, other than software designers, can use a program. It was later introduced in early 1980s as a replacement for the term ‘user-friendly’ [94] and was defined as “the user’s view of software quality”. The quality itself is a multifaceted concept [95] and includes five different views (based on Garvin [96]): the transcendental-based view, the product-based view, the manufacturing-based view, the economics-based view, and the user-based view. These views are also relevant to usability and have helped to shape a standard definition of usability with multiple attributes, as discussed in the following section.

3.2.1 Usability Attributes

Different researchers define usability based on a list of attributes or dimensions. It is not a single concept but rather a multi-dimensional property of a user interface that has multiple components [97]. For example, Nielsen identifies the following five usability attributes [98]:

- **Learnability:** measured by how easy the system can be learned so the users can start using it at minimum time expected.
- **Efficiency:** another usability attribute that measures the time users need to accomplish tasks after they have learned how to utilize the system.
- **Memorability:** measures how easy to remember the system if the user used it again after he or she has to leave it for a period of time.
- **Errors:** an attribute that measures the rate of errors that the users make during their use of the system. These errors, if exist, have to be minimal and easy to recover from. They must not be of a catastrophic nature.
- **Satisfaction:** measures the users’ satisfaction how much did they like using the system.

Whitney Quesenbery [99] also defined usability based on five dimensions (called the 5Es):

- Effective: how complete and accurate the work is to accomplish.
- Efficient: how quickly the work can be completed.
- Engaging: how pleasant and satisfying the product interface is to use.
- Error tolerant: how good the product is in preventing errors and how it can help the user to recover from mistakes.
- Easy to learn: how well the product supports learning throughout its lifetime of use.

A more formal and widely accepted definition of usability [100] is the one by The International Organization for Standardization (ISO). Their definition reduced the number of the usability dimensions to three: *effectiveness*, *efficiency* and *satisfaction*. The ISO defines usability of a product or service as “the extent to which the product can be used by specified users to achieve specified goals with *effectiveness*, *efficiency*, and *satisfaction* in a specified context of use [101].”

The following bullet points explain the three usability attributes identified by the ISO:

- Effectiveness: means that the users can do the tasks without making mistakes. This suggests that the user is not likely to request help.
- Efficiency: this attribute suggests that the users can complete the tasks in a reasonable time and effort.
- Satisfaction: the most important attribute which reflects the desirability of a product. It determines the extent to which the user finds the product to be effective and efficient.

Table 3-1 provides an overview of usability definitions by Nielsen, Quesenbery and other usability metrics by Schneiderman and matches their usability dimensions to these of the ISO.

ISO 9241-11 [101]	Schneiderman [102]	Nielsen [98]	Quesenbery [99]
Efficiency	Speed of performance	Efficiency	Efficient
	Time to learn	Learnability	Ease to learn
Effectiveness	Retention over time Rate of errors by users	Memorability Errors/Safety	Effective Error tolerant
Satisfaction	Subjective satisfaction	Satisfaction	Engaging

Table 3-1: Overview of Usability dimensions (adapted from [103])

3.2.2 Usability of Authentication Mechanisms

More people now need to utilize networked devices, especially to connect to online resources and communicate with others using the Internet. The variety of online services offered has attracted people from different backgrounds (e.g. cultures, education levels, age, geographical areas) to communicate and utilize them. Along with other factors, such as availability of Internet and communication services, even the average citizen who is barely computer literate is now communicating and interacting, on daily basis, with many online services.

Online users are also encouraged to carry out critical online transactions, such as money transfer. Such online services are crucial and pose greater damage to customers and organizations than do other online services. That is why companies that offer online services, especially financial firms, allocate more money every year for security technologies and products in order to protect their assets against security breaches. According to Forrester Research, IT security spending has increased dramatically from 8.2% in 2007 to 14% in 2010 out of the total IT spending in North America and European enterprises [104].

Despite this increase in security spending, the number of security breaches still show rapid increase over time [105] and usually affect not only the organization's image and services, but also its customers as a whole. In October 2011, Sony had to shut down almost 93,000 users' accounts after a security breach to its online gaming and entertainment networks [106]. According to Liebowitz [107], the first 6 months of year 2011 have been the worst in terms of the number of security breaches in a decade. He listed different major companies that were victims of security breaches in 2011. Among these companies were Sony, RSA, Lockheed Martin, Epsilon, the Fox broadcast network, NASA, FBS, FBI, Citigroup and French treasuries.

Unfortunately, hardening computer systems by implementing firewall rules and hard-to-compromise authentication mechanisms does not always lead to more secure systems and therefore lessen the security breaches. The problem, as suggested by many studies [77, 108-111], is that these security techniques and authentication mechanisms are only effective when used correctly. Many of the implemented security controls are either inconvenient or hard to use. Therefore, online users sometimes turn them off or try to

circumvent them [109]. It was found that users tend to circumvent security controls that they find cumbersome [92].

Authentication mechanisms, in particular, such as strong passwords, multi-level systems, graphical and multi-factor authentication cannot protect assets if users do not use them properly. For example, forcing users to use complex and hard to remember passwords might will encourage them to write these passwords down or store them electronically in plain text so they can copy and paste them every time they login. Also they could include an incrementing digit if the system forces them to change their passwords regularly. For example, a user could use the password “john6(usa” as a replacement for his old password “john5(usa” after the system forces him to change it. Such behaviours render the best technical security controls ineffective.

Although security awareness is among the solutions that online service providers provide to users to ensure proper use of the newly implemented authentication mechanisms, it is only effective to a minimal extent and does not fill the gap between security and the mentioned users’ behaviours [112]. Customers usually do not like to be trained or instructed on how to use online services and reject security advices. This is not because they are not intelligent, but because security advice is rather a daily burden that offers users a poor cost-benefit tradeoff. They prefer to look for alternative service providers who have minimal requirements and instructions [112]. Cost, time and support are factors associated with every new security mechanism the end-users have to use. These factors could, in the end, overcome the expected benefits of any new technological solution [113].

Overall, these conflicts exist because of the unbalanced attention given to security and usability in the authentication technologies. In literature, among many success factors for authentication technology identified by researchers, *security* and *usability* appear at the top of the list [1, 114-116]. However, Braz [115] stated that most of the primary research done on usable security did not cover user authentication. Therefore, most of these systems neglect usability and focus on security. The relationship between security and usability does not always have to be negative or inversely proportional as has been viewed in the past, it also can be positive [95]. Authentication, in particular, is only successful when security and usability are aligned. Authentication is the most important goal when security is implemented [117] and the most challenging part of any application’s usability.

To overcome these conflicts, the usability of authentication mechanisms can be considered to be as important as their security and among the main drivers for final acceptance of an online system by end-users.

“Usability becomes a strategic issue in the establishment of user authentication methods” [115]

“Security only works if the secure way also happens to be the easy way” [118]

There is a growing need for secured yet usable online systems. Security experts demand secured applications while usability experts demand easy-to-access and user friendly applications. With proper implementation, a secured and usable application can be achieved [119]. To achieve this, it is important to evaluate usability while implementing security technologies. The next section covers usability evaluation in more detail.

3.3 Usability Evaluation

The usability of given software cannot be measured in isolation because usability is an extrinsic property of a system software. One can only measure usability by explicitly associating the context of use. This can only be achieved by evaluating users carrying out tasks on a software system (see Figure 3-1).

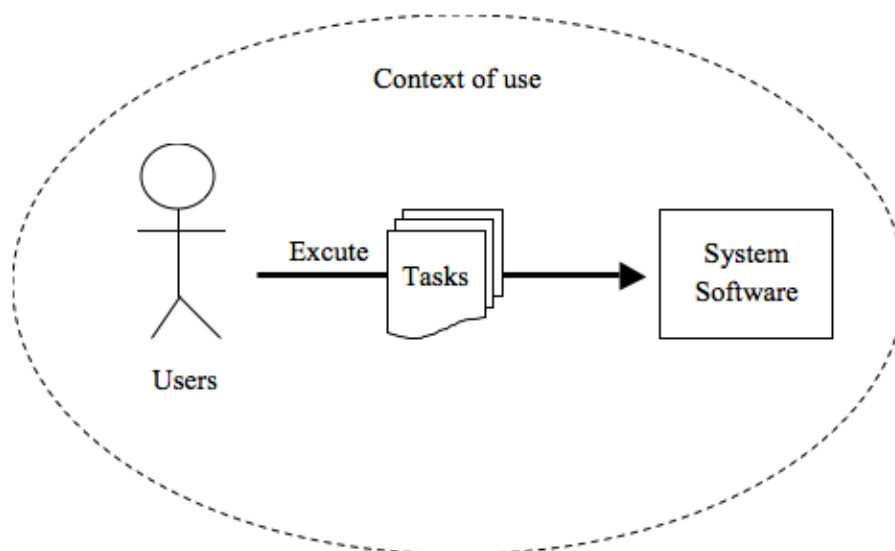


Figure 3-1: Evaluating usability by associating the context of use (adapted from [95])

As per the ISO definition, “usability is considered a context-dependent agreement of the *effectiveness*, *efficiency* and *satisfaction* with which specific users should be able to perform tasks” [95].

Although *effectiveness* and *efficiency* are, to some extent, measured by the user's perceptions of these qualities, the *satisfaction* attribute has no quantitative specification and is the only metric that is measured as a whole based on the user experience with the system. It can be measured by subjective rating on scales such as liking or acceptability when carrying out different tasks. Thus, the technology is considered as satisfactory only if the user considers it to be so [95, 120].

3.3.1 Assessing Usability of Online Banking Systems' Authentication

The majority of security-related usability studies focus on specific measures, such as password selection and user behaviours, rather than looking at usability of a system or service as a whole [92]. Although several publications discuss the relationship between usability and security, few studies provide empirical data in this area.

For example, Piazzalunga [121] compared three different token-based authentication methods for email protection. The usability metrics used in this study were set according to the ISO 9126 standard for evaluation of software products. The usability attributes used were: learnability, operability and attractiveness.

A more comprehensive study by Weir [122] reported results on the evaluation of usability and user preferences for authentication methods in online banking in the UK. The usability evaluation was based on the ISO definition of usability incorporating the three usability attributes of *effectiveness*, *efficiency* and *satisfaction*. The study compared three online banking authentication mechanisms: one-factor authentication, two-factor token-based authentication using a OTP generator device and another two-factor multi-channel authentication via SMS messages to a mobile phone device. The study aimed to determine the levels of experience, user acceptance and adoption of these technologies and investigated how online banking users affected user attitudes towards usability and acceptability of these authentication techniques.

This experiment categorized the participants into two groups: novice and experienced users. It also classified users who participated in the study into three types of participants in terms of their level of experience of online banking:

1. Migrants: the current users of the service (online banking users) who were familiar with the single-factor authentication mechanisms and might be potential migrants to the new two-factor authentication mechanisms studied.

2. Adopters: these are the novice banking users who had never used online banking services before and were unfamiliar with the alternative authentication mechanism being studied.
3. Switchers: experienced users (online banking users) were aware of similar two-factor authentication mechanisms, but had no specific knowledge of the methods being compared in the experiment.

Interestingly, one outcome of this study suggests that the relationship between security and usability *can* be positive. Weir found that participants considered the two-factor (via SMS) authentication mechanism to be less secure and less usable than the two-factor (via device) authentication mechanism. As shown in Figure 3-2, usability and security decreased together when participants used mobiles for authentication. This contradicts the commonly-held assumption of an inversely proportional relationship (increased security leads to poorer usability and vice versa). The reason for these attitudes, as mentioned by Weir, is related to technological problems such as network coverage, mobile battery life, cost associated with SMSs. Other issues raised by participants were related to the fact that some did not own or want to own a mobile; others did not want to share their mobile number. However, delivery delays of SMS messages experienced by some mobile users were considered unreliable for online banking authentication.

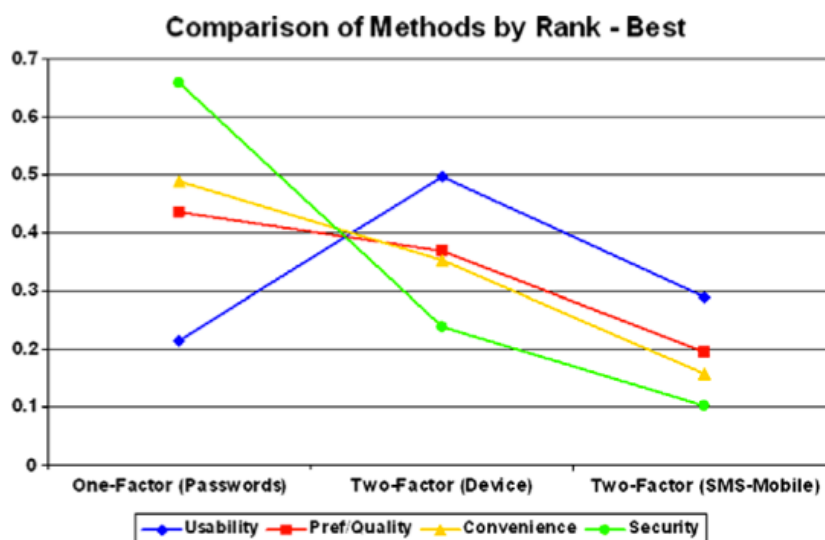


Figure 3-2: Relationship between usability, quality, convenience, and security [122]

Another outcome of the study also provided empirical evidence of the trade-off between usability and security when comparing one-factor with two-factor authentication (see Figure 3-2). Although participants choose two-factor authentication via SMS to be the least preferable authentication method, the results did show that mobile authentication was more

usable than one-factor authentication mechanism. Weir attributed this to awareness and other technical issues related to the mobile service. She argued that the participants did not understand how OTP methods worked, which resulted in rating security without this key information. On the other hand, these participants were more familiar with knowledge-based authentication mechanisms and did not widely appreciate security advancements associated with OTP authentication mechanisms.

Another study by Gunson [92] investigated usability by describing an empirical evaluation of two different methods for user authentication: single-factor and two-factor. The study aimed to measure usability (using a range of usability metrics), quality and preferences of each. The participants were real-life UK bank customers. The experiment was based on an automated telephone banking system.

Gunson provided empirical evidence of a negative relationship between usability and security in authentication systems. She found significant evidence that the single-factor knowledge-based authentication mechanism was more usable than the two-factor knowledge-based and token-based authentication mechanism. In contrast, the latter scored significantly higher only on the issue of security. This also conforms to the mentioned results of Weir's study between single-factor and two-factor authentication mechanisms.

Overall, usability evaluation is an important research area which helps to understand how a security technology can be implemented properly. Finding out whether an improving security affects the usability, either in a positive or negative way, would greatly help to optimize the implementation process to achieve the best of both.

Acceptability of security technology (i.e. the level of user acceptance of the technology), on other hand, is known as the *perceived usability*. Unlike usability, acceptability is measurable based on user perceptions, attitudes, and intentions towards different aspects of the technology [123] and is subjective. The next section covers acceptability and these aspects in detail.

3.4 Acceptability

Acceptability is defined as a measurement that depends on "whether the system is good enough to satisfy all the needs and requirements of the users and other potential stakeholders" [98]. Usability and acceptability share the same exclusive target: humans.

However, the goals are different. “The goal of usability is to characterize the extent to which a software system can be used ” [95] while the goal of acceptability is to ensure that the system supports the daily business and user scenarios in a sufficient, i.e. capable of meeting users’ needs, and in a correct way [124].

Jacob Nielsen [98] categorized usability as a subset of overall system acceptability (see Figure 3-3). It was also pointed out, using empirical studies, that usability plays a key role in user acceptance [125].

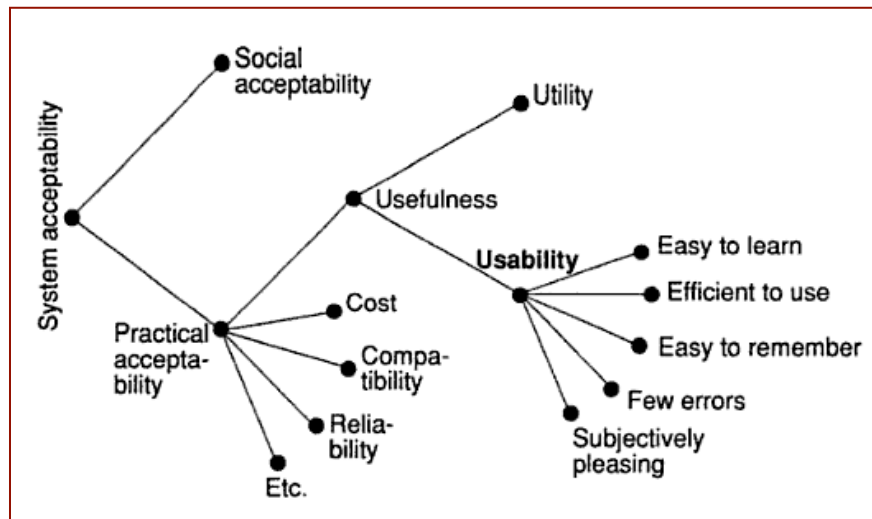


Figure 3-3: A model of the attributes of system acceptability [98]

3.4.1 Information Technology Acceptance

Although usability is an important factor deriving appropriate design targets, it does not fully predict actual system use. A system might be well designed and meet all functional requirements but still fail to earn the acceptance of users. In other words, usability alone is an insufficient determinant of use [126, 127].

According to Thomas [123], to determine actual use of a technology, usability should be measured both objectively and subjectively. Objective measures of usability include user performance, error rates, or time taken to complete tasks. Subjective measures, on the other hand, include user perceptions of ease-of-use and impression of satisfaction, enjoyment and usefulness of the technology. While the objective measures are based on usability attributes defined by ISO, such as effectiveness and efficiency, an acceptance model is required to explain the behavioural intention of using the technology within a given system (the objective measures of usability).

Technology acceptance is one of the research areas that has been studied and modelled to suit different fields, each with a different set of acceptance determinants [128]. The Technology Acceptance Model (TAM) by Davis [129] is one of the most utilized and widely accepted models among the information system researchers [130-133]. TAM proposes *perceived usefulness (PU)* and *perceived ease of use (PEU)* as two primary elements in determining user attitude towards adopting new technologies. According to Davis, PU is “the extent to which a person believes that using the system will enhance his or her job performance”. He also defines PEU as “the extent to which a person believes that using the system will be free of effort”. PU and PEU affect user’s attitude, which relates to intention, towards using the information system. In literature, TAM is considered one of the most influential extensions of the Theory of Reasoned Action (TRA) by Fishbein [134]. TRA is a widely studied model from social psychology and is used to explain users’ performance behaviour [135]. According to TRA, someone’s performance behaviour is determined by his or her behavioural intention (BI), which is in turn determined by his or her attitude (AT) and subjective norm (SN) concerning the behaviour being studied [136].

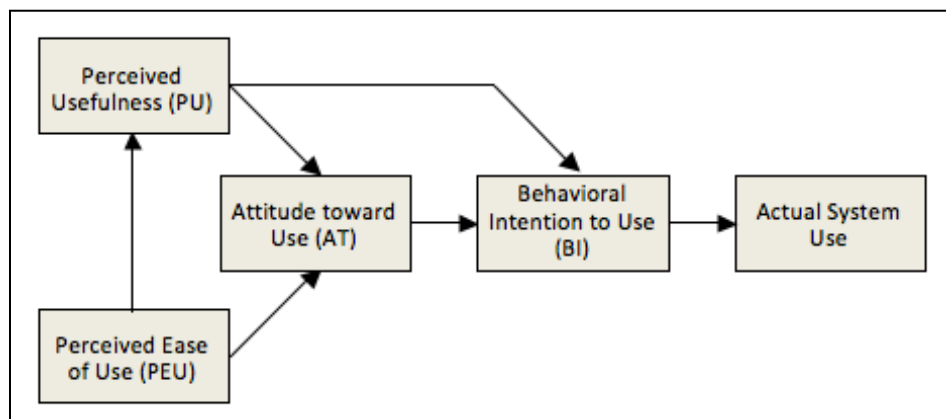


Figure 3-4: Technology Acceptance Model (TAM) [136]

Besides PU and PEU, TAM incorporates three other distinct factors (see Figure 3-4):

- *Attitudes towards use (AT)*: is defined as “the user’s desirability of his or her using the system” [136] and is determined by PU and PEU.
- *Behavioural Intention to Use (BI)*: is determined by users’ attitudes toward using a system.
- *Actual System Use*: is the adoption of the system, which is determined by BI.

Despite the frequent use of TAM model and the validity and reliability of its instruments [137], it has been criticised. According to Bagozzi [138], TAM focuses on how an

individual (user) perceives usefulness and ignores group and social aspects. Wang [131] empirically validated TAM using different populations of users and different software choices. Based on 88 published papers, King [139] statistically confirmed these results using meta-analysis of TAM based on different context of use. The context of use included type of user, such as students, professionals and general users, as well as type of usage, such as job-related, office and task applications. The results proved that TAM is powerful, highly reliable, valid and robust predictive model for different context of information technology acceptance.

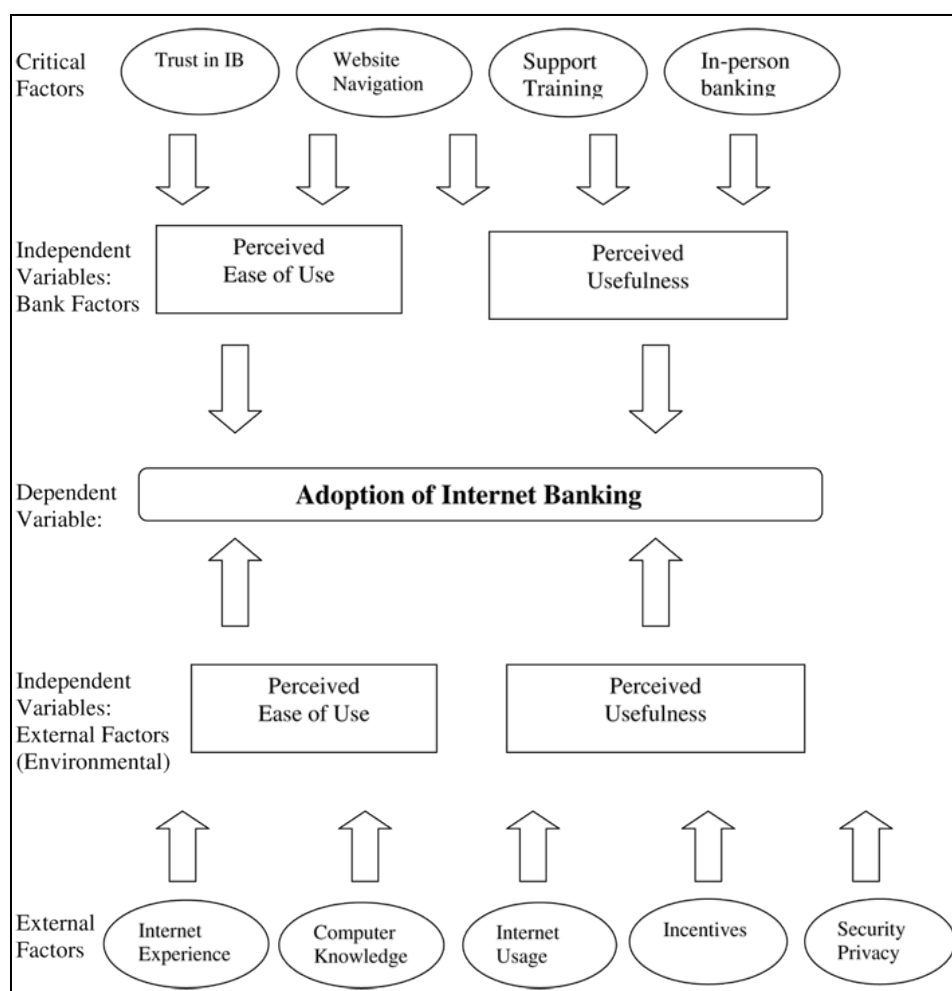


Figure 3-5: Critical success factors of online banking [140]

While the basic constructs of TAM, PU and PEU, have been considered as primary determinants of individual's acceptance of technology, it was found that TAM has limitations in some cases such as involving students as the empirical sample, examining office automation software or system development applications, and self-reported usage [137]. Many researchers, therefore, have suggested that including new variables as extensions to the original TAM can improve its applicability and explanatory ability as well as its predictive power in various aspects of IS [141-144].

Venkatesh [128] extended TAM to what he called Unified Theory of Acceptance and Use of Technology (UTAUT). He proposed this model as complete model for understanding the acceptance and the adoption of information technologies. The UTAUT model shows that the four elements namely performance expectance, effort expectance, social influence and facilitating conditions play a significant role towards user acceptance and usage behaviour.

Renaud [145] used demographic variables, social influence, and personal factors as external variables to develop a Senior Technology Acceptance Model (STAM) to model the acceptance process as driven by the factors that influence mobile phone adoption in the context of the elderly mobile phone user. In the context of online banking, Gefen [132] and Nor [146] found that trust has a significant effect on attitude towards using online banking. Al-Somali [147] added demographic variables as well as other variables like security, trust, quality of the Internet connection, and awareness of service and its benefits as external variables to TAM to model and analyse the factors that affect customers' attitudes towards Internet banking acceptance. A more recent study by Al-Somali [133] also added resistance to change, social influence and self-efficacy to the model. The studies by Khalfan [5] and Al-Sabbagh [4] both examined variables such as trust, security, and ease of access as factors influencing adoption of online banking in Oman. Furthermore, Hosein [140] developed 9 different factors that he categorized into external (Internet experience, computer knowledge, Internet usage, incentives, and security privacy) and bank (trust in online banking, website navigation, support training, and in-person banking) factors (see Figure 3-5) to examine how these factors affect online banking adoption.

Information technology acceptance, therefore, is an important research area to study and understand how users accept and use technologies. In literature, TAM is found to be the most commonly used theory by researchers to model user acceptance of a technology. It also suggests different factors that influence the users' decision on how and when they will use it. Despite Bagozzi's criticism, this process can reasonably be considered a solitary activity and therefore TAM can be considered to be an appropriate model for this research. The research being reported here needs to evaluate acceptability in the context of a single user, using personal computer, performing tasks to complete personal online banking transactions. The next section covers the modelling and identifying the factors found in the literature that are known to influence users' acceptance of online banking systems using TAM.

3.5 Assessing Acceptability of Online Banking Systems

The previous section looked at acceptability of security technologies and introduced Technology Acceptance Model (TAM) in general. This section considers how acceptability of security technologies, particularly in online banking systems, is assessed. This includes looking at how TAM can be tailored to reflect acceptance factors for these systems.

The majority of acceptability studies utilize evaluation models such as TAM to measure specific variables. These variables range from demographic characteristics, such as gender, marital status, age group, monthly income group, and education level, to internal variables within the evaluation TAM model. Other external variables found in the literature also exist for different models based on different requirements and cultural backgrounds. For example, factors such as ease of access, trust and relationship and security were found to be among major factors influencing the adoption of online technologies, such as online banking, in Oman and other developing countries in the middle east [4, 5, 133, 147]. These factors and other internal and external TAM variables are discussed in the following sub-sections.

3.5.1 Demographic characteristics

Many studies [147-150] have investigated the effects of users' demographic characteristics on their adoption of online banking technology. One study [147] presented the relationship between the demographic profile of people in Saudi Arabia (a developing country bordered by Oman on the southeast) and their attitude towards adoption of online banking. The outcome revealed that only education level had a significant relationship with acceptance and adoption of online banking. Other demographic variables such as age, income, and gender were not confirmed to have effects on online banking adoption.

Jaruwachirathanakul [149] investigated the attitudinal factors that encourage online banking adoption in Thailand. The study found that moderating factors such as gender, educational level, income, and Internet banking experience were significant factors influencing adoption. Age was confirmed not to be significant in this study.

The empirical results of Chang [150] showed that gender, age, and marital status were characteristics that influenced the adoption of online banking.

3.5.2 Internal and external variables

Internal and external TAM variables were the factors, other than the demographic characteristics, that were found to influence customers' decisions to adopt online banking. The internal variables were the primary determinants found in the original TAM by Davis [151]: *perceived usefulness (PU)* and *perceived ease of use (PEU)*. Many studies have found that customers have accepted online banking as a technology that improves performance, increases productivity, and enhances effectiveness [129, 141, 152].

The external variables, on the other hand, are suggested by the literature, all of which were found to influence customers' adoption. Previous studies [153, 154] grouped these variables into five components: *trust and relationship*, *ease of access*, *security*, *convenience*, and *ease of use*. This grouping process was based on what is known as 'Factor Analysis'. Factor analysis is a statistical approach that looks into the variables and identifies their interrelationships with each other [154]. It looks into a large set of variables and tries to condense or summarize them into smaller sets of factors or components. This is done by looking for groups among the intercorrelations of a set of variables [155].

While *convenience* and *ease of use* represent the same primary constructs (internal variables) PU and PEU respectively, the other three components namely trust and relationship, ease of access, and security are discussed below.

3.5.2.1 Trust and relationship

Trust and relationship are two factors that play an important role in financial sector. Some researchers have argued that customer confidence in online banking transactions is an essential determinate of adoption of online banking [156]. According to Stewart [157], customers' lack of trust in electronic channels is one of the major factors that contributes towards failures in adopting online banking.

Trust and relationship are inter-related factors in the sense that the customer's relationship with the online banking providers is more efficient in face-to-face communication than online. Some studies found significant relationships between proximity and personal relations [158, 159]. This lack of relationship in the online context can be alleviated by trust, which is more important online as opposed to face-to-face banking [160]. Parties involved in financial transactions usually exchange sensitive information and therefore

they are more concerned about privacy and security of these information while they are exchanged over the Internet, not the case in offline banking. According to Rotchanakitumnuai [161], reliability of the service is one of three reasons of customers' distrust of Internet technology. However, for customers whose relationship is primarily based on efficiency of services, online banking is an attractive alternative [153]. In this matter, Tomiuk [162] stated that 'richness' and 'sound presence' of the online banking environment affects the ability of a bank to create a trusting relationship between its employees and customers.

3.5.2.2 Ease of access

Internet ease of access is one of the important predictors for adoption of online banking. Many studies [133, 140, 147, 158, 163] stated that without a reliable and high quality Internet connection, customers are unlikely to consider using online banking.

According to [153], "provision of infrastructural facilities is another factor that could lead to quicker diffusion of innovation". There is a significant correlation between download speed of a website and its users' satisfaction [164]. Al-Somali [133] stated that there is a positive relationship between connection speed and the adoption of online banking. She found that the current lack of infrastructure in Saudi Arabia plays a vital role in limiting adoption rates of online banking by Saudi customers. These results confirmed the study by Almogbil [165] who found that about 63% of the customers in Saudi Arabia access the Internet through dial up services.

3.5.2.3 Security

Security perception has been widely recognized as one of the main issues inhibiting online banking adoption [4, 166, 167]. Despite the advancements of security in Internet communication such as cryptography, digital signature and certificates, and multi-factor/level authentication methods, online customers are still concerned about security especially when monetary transactions are involved [168].

There are many studies concerning the importance of security to the acceptance of online banking [140, 147, 154, 158, 169, 170]. Sathye [158] found that almost 3 quarters of all customers decided not to adopt online banking because they were concerned about the safety and security of the transactions over the Internet. Another paper by Howcroft [171] argued that "although customers' confidence in their bank is strong, their confidence in

technology is weak”. The empirical results by Cheng [170] showed that perceived web security has a direct effect on the intention. This results confirms earlier empirical results by Salisbury [172].

3.5.3 Summary

In conclusion, aspects such as ease of access, trust and relationship, and security are important factors to be included in acceptability testing of authentication in online banking. Along with other internal factors, an extended technology acceptance model can be formed and tested to identify which of these factors influence the customers’ adoption of the technology.

3.6 Usability and Acceptability Measurement

Usability and acceptability testing is carried out to evaluate the usability and acceptability of a technology in the context of a single user performing a task to achieve a goal [173]. In the context of online banking, usability and acceptability are evaluated by asking participants to perform tasks (e.g. logging in, creating beneficiary account) to achieve a goal such as money transfer. Different tools can be used to capture users’ input and feedback. Among many techniques available, this study uses questionnaires to capture users’ feedback. This technique is widely used and implemented by researchers to evaluate usability and acceptability of security technologies. For example, Weir [122] used three questionnaires throughout her study to collect usability comments from the participants. She also used a pre-questionnaire to collect users’ demographics such as age, gender, use of online banking, locations of use and mobile phone ownership. The usability questionnaires were based on set of positive and negative statements on a 7-point agree-disagree Likert scale.

Another study by Gunson [92] used questionnaires to measure participants’ attitudes towards three different security technologies. She used agree-disagree Likert scale type of questions in the form of stimulus statements for each usability attribute. According to Coolican [174], participants preference of Likert scaling technique is due to its natural way to complete. It also has been shown to have a high degree of validity and reliability. Furthermore, it has been shown to be effective in measuring changes over time.

User action logging is another recognized technique, and is used to capture the measures of users' specific interaction with the system. These variables include the time users spend on each task, the sequence of pages users follow in order to complete these tasks, and the exit pages for those who leave the system without completing all tasks. The quantifiable data collected from this technique usually used to evaluate the quantitative side of usability, which includes *effectiveness* and *efficiency* covered in section 3.3. For example, Weir in another study [91] used time logs to measure efficiency. She also used completion time logs to measure the effectiveness of three different security technologies.

Similar survey and data collection techniques were also used to measure the mentioned quantitative attributes of usability as well as the subjective side of usability (e.g. satisfaction) and acceptability (e.g. TAM internal and external variables) of the online banking. The use of these survey techniques in this research is detailed in Chapter 7.

3.7 Chapter Summary

This chapter discussed the importance of evaluating usability and acceptability of new information technologies in information system. It first defined usability and listed different usability attributes found in literature. It then discussed usability evaluation in the context of online authentication mechanisms.

The second half of the chapter covered acceptability and information technology acceptance models found in the literature. The history of TAM and different studies undertaken to validate TAM were presented and an argument made for the suitability of TAM for this research. Finally, the chapter presented different external variables used in the literature to assess how they affected the adoption of online banking and explained how they can be incorporated into TAM for the purposes of this research.

The next chapter will discuss online banking and mobile communication. These two topics are essential to promote a better understanding of how authentication is implemented in online, distributed systems and to foster a better appreciation of why there is a need to improve the existing single and two factor authentication mechanisms.

Chapter 4

Online Banking and Mobile Communication

4.1 Online Banking

Banking and telecommunication sectors are two major business players in today's market; their services have become necessities to many people around the globe. The high level of user-acceptance and the technological advances of security [169] have led the banking sector to introduce online banking, or what is known as branchless or virtual banking. This refers to the use of the Internet as a remote delivery channel for banking services. This delivery channel includes traditional services, such as opening a deposit account or transferring funds among different accounts, and new banking services, such as electronic bill disbursement and payment (allowing customers to receive and pay bills via a bank's website).

Internet banking refers to the deployment over the Internet of retail and wholesale banking services. It involves individual and corporate clients, and includes bank transfers, payments and settlements, documentary collections and credits, corporate and household lending, card business and some others [175].

Although the infrastructure of banking systems is based on information technology, which places the systems among those most easily shifted online, they are also among the most critical applications that need to be secured online. An effective and reliable authentication method must accompany any form of engagement in online banking.

This section provides a discussion of the main factors influencing the adoption of online banking, followed by a detailed summary of the status of online banking and the authentication mechanisms implemented by different real, online, banking applications.

4.1.1 Factors Influencing the Adoption of Online Banking

Online banking has become one of the core technology advancements [176] of the Internet and is considered one of the most successful business-to-consumer applications in electronic commerce [177]. For banks, cost reduction, market share increase, and competition [164, 178] are the main factors driving online banking adoption. They can also now provide more diversified, convenient and flexible services than before [179]. From the customer's point of view, low fees, accessibility, and availability are the main advantages of online banking services [159, 169]. That is, bank services are now cheap to access, accessible from any Internet connection point (i.e., home, work, or even mobiles), and available 24 hours a day, 7 days of the week.

On the other hand, some customers still refuse to adopt online banking services. Kusima [180] identified several barriers affecting online banking adoption. The functional barriers are categorized into *usage barriers*, such as the absence of concrete elements provided by ATM machines, and *value barriers* such as perceived insecurity and inefficiency. Some customers are used to the ATM machines and find them more convenient than the Web. Others trust them more than online banking. They believe it is more secure to have a bar-code reader reading code off the bill than keying it manually from a keyboard [180]. Other studies found that perceived risks in general are the most prominent barriers to online banking adoption [160, 181-183].

The following points will further discuss the incentives and risks for banks as well as for customers that influence them to respond to online banking positively or negatively.

4.1.1.1 Incentives

Many incentives make online banking an essential service for banks and customers. Here follows a list of incentives that banks would consider when deciding to offer online banking services:

- **Accuracy:** humans directly affect the reliability of transactions, especially when the transactions occur in a face-to-face manner. There is always a possibility of errors originating from either the employees or customers. Human error accounts for three-quarters of negative transaction incidents, mainly because of policy violations [184]. However, building a computerized application fully interactive with the customers

reduces human error, and hence, improves the reliability and accuracy of a higher percentage of bank transactions.

- **Service:** the Web offers equal opportunities to all competitors. Banks do not have to worry about approaching customers in different geographical areas but rather have only to concentrate on providing a central web presence approachable from everywhere. This gives the bank focused management as well as zero-delay service quality to offer to customers.
- **Market share:** offering new competitive services for customers is known to be the driving force behind the introduction of online banking [185]. That is, offering competitive services retains existing customers, increases their loyalty, and attracts new clients to maintain and increase the market share.
- **Profit:** is among the most attractive incentives for any commercial organization. For banks, online banking has emerged as one of the most profitable products over the past decade [186]. This is likely a direct result of cost reduction in labour, building construction and maintenance, and service and transaction provision. For example, Figure 4-1 shows that online banking has a transaction cost of almost 1 cent compared to \$1.07 for a transaction carried out on-site [187].

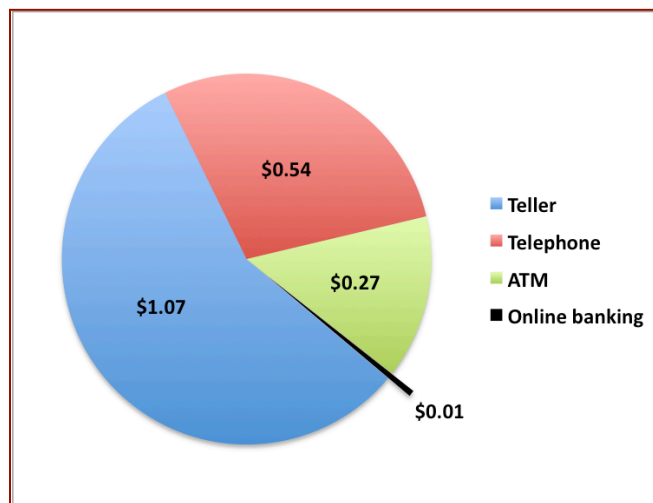


Figure 4-1: Cost per transaction for each banking channel

From customers' perspectives, online banking offers many advantages over retail banking. These advantages result from the overall quality of service offered by online banking, and can be categorized into convenience, user experience and control, and transaction speed.

- **Convenience:** this involves accessibility and availability of the service to customers. A customer does not have to drive to a nearby ATM machine or bank branch to carry out banking transactions, but can use online banking from any Internet access point.

Customers do not have to wait for branch working hours and can utilize the banking services and carry out transactions any time. Moreover, some banks offer a variety of services online (e.g., long dated payment history and outstanding orders setup/cancellation), which are not usually offered by other electronic banking channels such as ATMs, tele-banking, and mobile banking.

- User experience and control: online banking usually offers customers clear and easy-to-follow instructions. All the tasks are equipped with verification mechanisms that make customers feel in control.
- Transaction speed: customers are sometimes involved in long queues in bank branches to request transactions. Online banking has eliminated the need for the delay and customers are able to process their transactions as soon as they click on the confirmation button.

4.1.1.2 Risks

Despite the benefits of online banking to both banks and customers, there are always risks involved that affect both parties' decisions to adopt online banking services.

For banks, just like other organizations that do business on the Web, online attacks are the major threats to their online presence. These attacks, when successful, cost the businesses a considerable amount of money. In 2008, online attacks on the Pentagon cost almost \$100 million [188] for computer equipment, contractors, and manpower to clean up. In the banking sector, information related to cyber attacks is usually kept confidential as it might affect the bank's image and their customers' trust. However, some figures leak to the press and other survey firms because other parties involved in the attacks on bank accounts reveal the customers as victims. Banks do not always compensate their customers (especially those who hold commercial accounts [189]) for losses due to attacks, and some victims file lawsuits against them, at which time this information becomes public and accessible.

According to [190], "a Texas manufacturing firm filed a counter lawsuit against PlainsCapital bank of Lubbock in connection with the cyber theft of some \$800,000 from its online banking account" on February 2010. This case involved an online wire-transfer of the mentioned amount to an overseas account in 2009. The bank was later able to recover only 75% of the total amount, refusing to compensate the firm for the other 25%. The bank claimed that it processed the transaction because the thief used valid access credentials of the firm when placing the transaction request.

A similar case in late 2009 involved a Michigan-based firm that filed a lawsuit against Comerica Bank after a series of 107 unauthorized online wire-transfers and transfer-of-funds requests were carried out on their behalf that resulted in a transfer of more than half a million U.S. dollars to different accounts in Russia, Estonia, Scotland, Finland, China, and the U.S. [191]. In this case, the thieves acquired the firm's bank account access credentials from one of the firm's employees in response to a man-in-the-middle phishing e-mail that purported to come from the bank (more details about e-mail phishing and man-in-the-middle attacks are found in sections 2.4.3.5 and 2.4.3.6 respectively).

Although Comerica Bank was utilizing a two-factor authentication procedure at the time of the incident, it did not protect the Michigan firm from real-time phishing attacks.

Computer scams targeting small businesses cost U.S. companies \$25 million in the third quarter of 2009 [192]

The ability of the bank to provide an authentication mechanism that is able to protect customers from all known attacks is the only way to withstand the risks of adopting online banking services. The Federal Financial Institutions Examination Council (FFIEC) released guidelines for banking and financial services in 2005, titled "Authentication in an Internet Banking Environment", which addressed overhauling security in the Internet-based environment and suggested that banks upgrade their authentication mechanisms from single-factor authentication to stronger two-factor authentication mechanisms by the end of 2006 [193]. However, currently, even multi-factor authentication does not withstand the new attacks, which have appeared since 2005 (e.g., man-in-the-browser attack in section 2.4.3.8).

From the customer's perspective, five dimensions of perceived risks have been identified [194]: security/privacy, financial, social, time/convenience, and performance risks. The following explanations and real stories show how these risks are related to the adoption of online banking and provide some examples that prove the reality of these perceived risks

1. Security/privacy risks: these can be identified as the risks caused by compromising users accounts by means of hacking (details of hacking and attacking methods were covered in section 2.4). The effects of such attacks can lead to money loss and identity theft, both of which have a big impact on users' decisions to adopt online banking. Researchers at security firm Finjan [195] reported a new Trojan horse called "URLzone bank Trojan" in 2009 that does not steal user's online bank account

credentials but rather steals money once the user is logged into the online account. Once this Trojan installs itself onto the victim's machine, it remains inactive until the victim logs into an online bank account. At that point, the Trojan initiates its attack against the user's account by checking the available balance and deciding on the amount to transfer from the victim's account. This decision is based on defined formulas that will ensure the stolen amount will not reach a limit that would trigger the antifraud online bank system. The transaction is very transparent and is invisible to the victim. All communications happen behind the scene. Moreover, the Trojan hides the history of these transactions and manipulates the information received from the bank so it displays a fake balance on the user's screen. The report stated that this Trojan was able to steal about €300,000 from German bank accounts during its first 22 days.

2. Financial risks: these are identified as the risks related to transaction errors or account misuse. A story published by Olsen [196] about an online banking customer in Norway who was trying to transfer a large sum of money (about \$100,000) electronically using an online banking service. She mistyped the account number, which resulted in transferring the money to another bank customer who thought the money was the result of a lottery win, and therefore, spent much of it gambling before police were able to recover it.
3. Social risks: adopting a service or product can have an impact on someone's status among other social group members. It depends on one's social group's view (i.e., favourable or unfavourable) towards online banking but either view can affect peer opinion of its adopters [186].
4. Time/convenience risks: these refer to the time gaps between the submission of transactions and the actual time the bank processes them, especially in cases where payments are involved. On 30th of December 2009, this researcher bought an Apple laptop online and had to process the payment transaction before getting to the year 2010 as taxes in the UK were officially to increase from 15% to 17.5%. There was not enough cash to pay for the laptop using the credit card as the available limit was less than the price of the laptop by almost £500. To overcome this issue, the researcher thought of paying previous credit card bills by transferring an amount of £500 from his savings account to the credit card account so he would be able to pay Apple Inc. for the new laptop. However, after transferring the money online, a message popped-up saying, "Please allow 3 working days to process your payment!" After calling the bank, they confirmed that online credit card bill settlements required 3 working days while paying off the bills in person updates the records instantly. If Apple Inc. had not finally

accept another form of payment, the researcher could have paid an extra 2.5% of the laptop price because of the delays involved in online payment transactions.

5. Performance risks: these are related to the losses incurred when the website or online banking application is not able to process user requests properly due to bad design or malfunction. A similar story to the one just mentioned could occur if the bank online application were to go down at the time of payment.

4.1.2 Current Status

With the growth of Internet services and the increased level of user acceptance of online business transactions, more financial institutions (i.e. banks) have found that shifting their services online is very competitive [164]. Therefore, online banking, or e-banking, has experienced strong and sustained growth in the past few years.

Figure 4-2 shows a 10% average increase of online banking users in addition to other banking channels (e.g., call centres, branches, and ATMs) in the U.S. between 2006 and 2010.

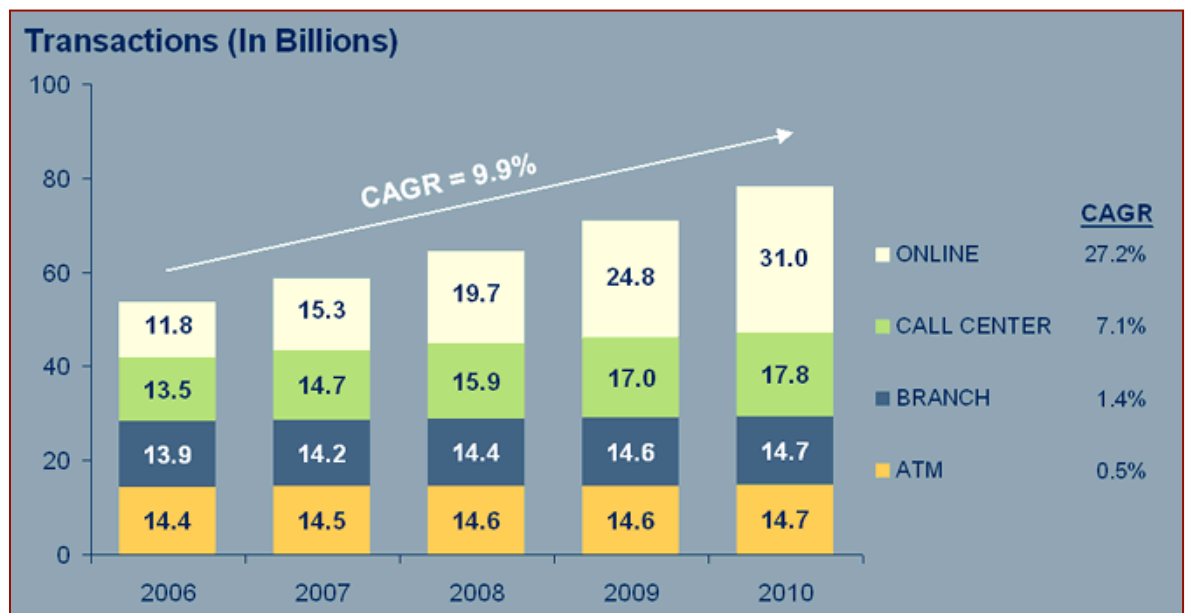


Figure 4-2: USA banking delivery transactions by channel (2006-2010)

CAGR: Compound Annual Growth Rate

Source: <http://www.towergroup.com/research/content/page.jsp?pageId=1522>

Traditionally, bankers request customers' signatures or fingerprints to authenticate them for payment and other banking transactions. However, with the introduction of electronic banking channels, customer identification for transaction authorization has become one of the biggest challenges for banks [197]. In the early days, banks used the Web only for

marketing purposes. They published only informational websites to market their products and services that could be utilized by visiting their branches in person [169].

The current implementation of Online Banking Applications (OBA), online services and levels of authentication can be categorized into three dimensions: informational, local-transactional, and transactional online banking applications.

4.1.2.1 Informational OBA

The basic level of OBA is informational. Banks adopt these applications with only online marketing strategies in mind. They are not willing to deliver transactional services online and their electronic presence is focused only on information about their services and products.

Customers, on the other hand, may be offered only basic informational services such as balance inquiry, transactions history, and other value-added services. The risk is relatively low, as the customers have no ability to write/modify access to their accounts in the database. This means the customers and the transactional database can be physically separated from the database feeding this kind of OBA, or the connections can have limited privileges with no ability to alter the records (see Figure 4-3a).

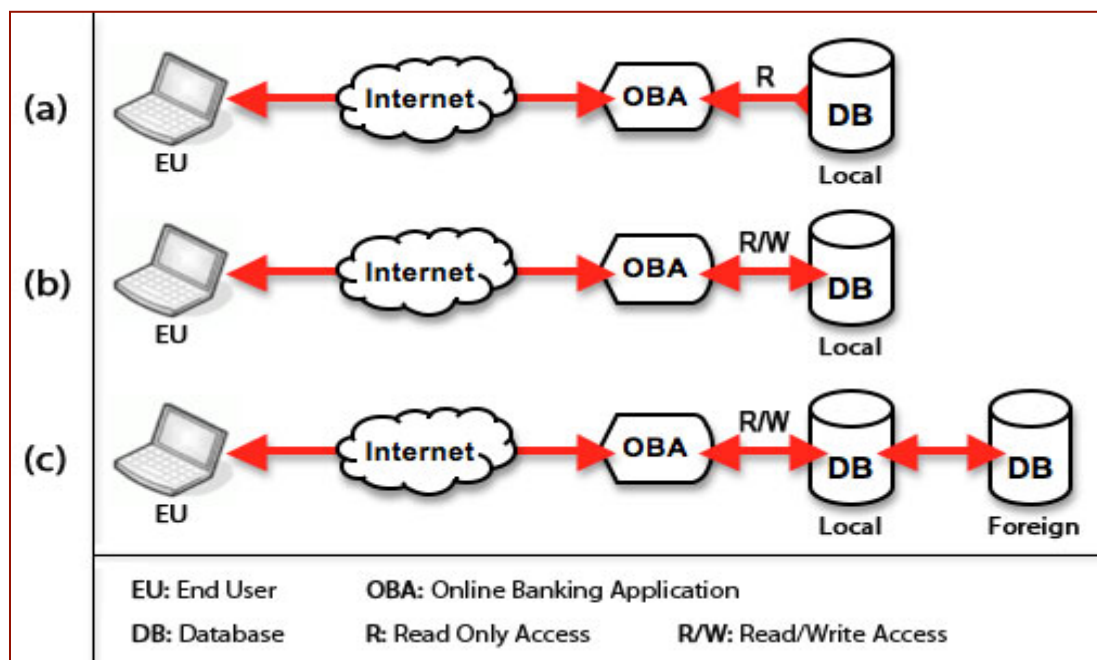


Figure 4-3: Types of online banking applications (OBA): (a) Informational OBA, (b) Local-transactional OBA, (c) Transactional OBA

Authentication, if customers are allowed access to their accounts, is usually accomplished by means of a traditional username and password. This type of authentication mechanism

does not protect the customer from most of the attacks that target the end-user (EU) such as user surveillance, notes theft, brute-force, and social engineering (more details in section 2.4.3).

Privacy and identity theft are the main security threats to the Informational OBAs. Since an attacker can gain access to the customer account using different attack methods, user details (i.e., name, account balance, payment history, and other private details such as passwords) can be disclosed; if the user is using a password that he or she uses for other web accounts, the attacker may be able to compromise those accounts as well.

4.1.2.2 Local-transactional OBA

The local-transactional OBA is more interactional than the informational OBA. It offers customer services that involve record alteration in the database such as money transfer from one account to another and paying utility bills (see Figure 4-3b). The risk is higher to the system, and therefore, most local-transactional OBAs require more advanced authentication than username and password only.

For example, customers in some banks that offer local-transactional OBA are required to submit more than one authentication factor to gain full access to online banking services. Some banks allow customers to submit one factor (e.g. a password) to login and check balance statements, while another factor (e.g. passphrase or password) is required to authorize transactions such as online bill payments and fund transfers between the customer's own accounts.

Usually this type of OBA does not allow customers to exchange funds between different customers' accounts or to transfer money to a foreign bank account (i.e., hence the name local-transactional). These OBAs are not willing to afford such high risk, given the limitations of the use of single channel authentication mechanisms that are usually prone to various attacks such as user surveillance, notes theft, malware infection, and social engineering.

Threats concerning local-transactional OBAs are not limited to privacy and identity theft, but extend to include financial, social, and time threats. An attacker can transfer money from the victim's account to another even if the beneficiary account does not belong to the attacker. This can negatively affect both the victim and the bank. The victim will have to report the incident and wait for long investigation procedures to recover the money. The

time interval between the time the attack was initiated and the time the money is recovered fully can result in bad debits on the victim's account where regular direct debit transfers or bill payment orders to third parties might be set up (financial and time threats). The bank, on the other side, might have to recover the losses of such incidents and cover all expenses needed for the investigation. In addition, the bank's reputation may be damaged, which can have a major effect on its customers (financial and social threats).

4.1.2.3 Transactional OBA

This type of OBA offers a transactional level of service that can empower local and foreign international banking servers. That is, the customers can transfer money between different accounts within the same bank, the same country, or even belonging to two customers across different banks in different countries (see Figure 4-3c). These applications pose the highest possible risk to online banking and a large number of online authentication mechanisms and controls have to be implemented in order to assure the integrity and legitimacy of transactions. That is, controls must ensure that legitimate bank customers have initiated all online transactions and that the details have been received by the OBA without modifications.

Some banks use multi-factor authentication through different channels to secure this OBA. This uses the same authentication techniques as local-transactional OBA; however, some factors are not fixed knowledge selectable by the customers, but are rather a one-time authentication factor sent to the customer through a secondary channel other than the primary web channel (e.g., mobile network as an SMS). This factor has to be confirmed by the customer to carry out advance critical transactions involving money transfer from one account to another.

Although this approach seems to be the most secure, unfortunately it still fails to protect against man-in-the-middle/browser attacks. Threats are more dangerous since a path to external OBAs exists. The chance of recovering transferred-away money by an attacker is low, especially if money is transferred internationally.

4.1.3 Authentication Mechanisms in Online Banking

As discussed in previous sections, there are a variety of authentication techniques and methods ranging from single-factor authentication mechanisms (i.e. passwords and personal identification numbers (PINs)) to more complicated multi-factor authentication

mechanisms (i.e. one-time-passwords (OTPs) combined with the use of voice biometric recognition). However, for any financial institution to facilitate online banking services, the implementation of a suitable authentication mechanism should depend upon the results of the financial institution's risk-assessment process. The risk-assessment process usually involves the identification of the customer type (e.g. personal or corporation), the level of services offered online (e.g., informational, local-transactional, or transactional), the usability of the system, and the volume of transactions [41].

In the following section, some online banking applications currently offered by real financial institutions are discussed. More focus is given to the authentication methods implemented and the types of services offered. The icon “|🔑” will be used in all figures to identify that the field is requesting a secret factor to be entered or identified by the online banking customer. A discussion will follow each case to cover the advantages of the methods implemented as well as to describe what attack methods are applicable and how they can successfully attack the implemented security measures.

4.1.3.1 Case 1: Multi-level Authentication

One bank makes use of multi-level authentication. This bank provides limited online services such as account balances, inter-account transfers, mobile top-ups, and bill payments. It also provides speed transfer to India, which is the only foreign transfer provided by the bank. Other applications (i.e. new chequebook requests, demand draft requests) and reporting (i.e. lost ATM cards reporting) services are also available (see Figure 4-4).



Figure 4-4: Online services page

The bank requests users to provide a username and password (both defined by the customers at enrolment) for account login. After login, the user is redirected to the home page, which lists all personal accounts with their balances (see Figure 4-5).

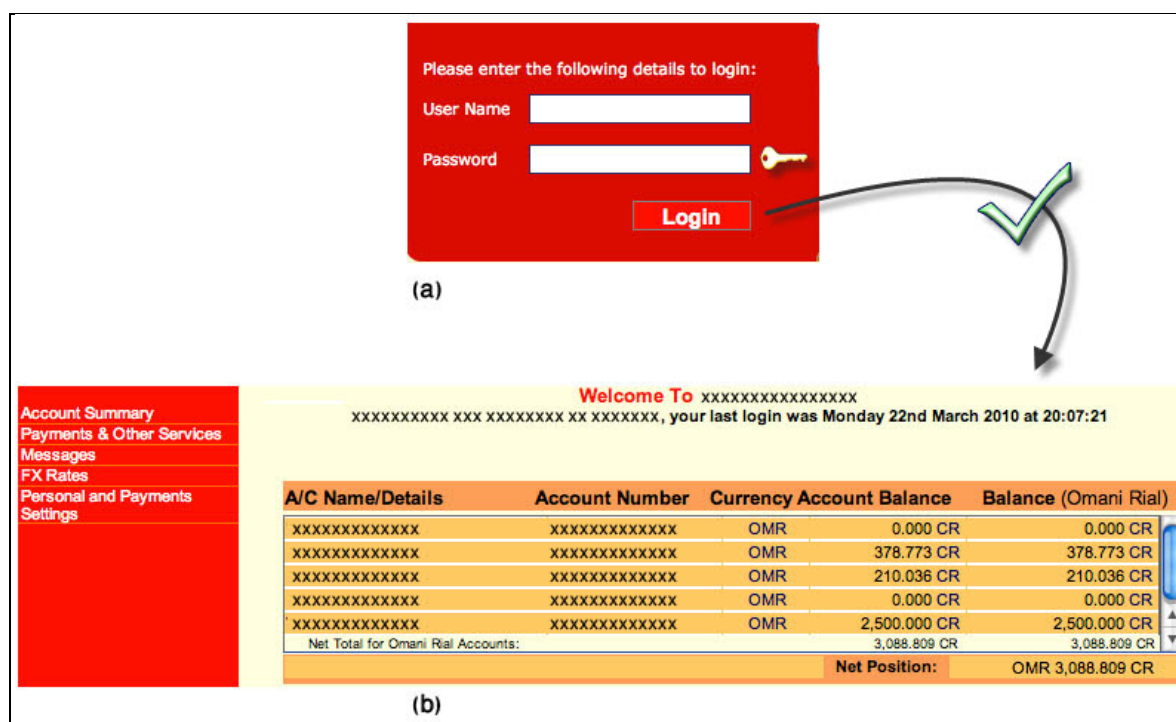


Figure 4-5: (a) Login screen, (b) Home page screen

At this point in the application, users have only read access where they can neither transfer money between their own accounts nor utilize other services offered by this online banking application. However, these services can be accessed and confirmed by a secondary secret (e.g., passphrase) defined at enrolment. This secondary passphrase is required only to authorize transactions. However, both password and passphrase are sent to the system using the web channel and both can be intercepted by an attacker.

Discussion

The services provided by this bank are very limited. The transfer option is only allowed between accounts linked to the customer and other top-up service and utilities bill payments are restricted to certain local companies. A customer is not allowed to add any account or utility company apart from the ones provided and supported by the OBA of this bank. However, there is a foreign transfer option available to one foreign country (India). This makes it a transactional OBA.

In terms of authentication methods, although this bank is using a multi-level authentication approach, it uses only one class of factor for both levels (the password and passphrase are

both considered examples of something the user knows). This means that both authentication levels have the same security drawbacks as traditional authentication mechanisms and they can be compromised by different attacks. These attacks include social engineering, pharming, brute-force, guessing, user surveillance, and note theft [43].

If both authentication factors (e.g. the password and passphrase) are captured by an attacker, they can be used to utilize fully all services in the customer's online bank account. The bank has not enforced any password policies such as password length or special character requirements, and does not notify customers of any transactions being activated or processed unless the amount of money involved in the transaction is higher than a given figure amount of about £180.

Finally, the OBA offered by this bank is transactional (since it offers international transfer to banks in India). However, the authentication mechanisms do not match transactional OBAs' risks; they are more suitable for lower-risk types of OBAs, such as local-transactional OBAs.

4.1.3.2 Case 2: Multi-level, Multi-channel Authentication

A second bank offers more services through its OBA. It allows customers to do inter-account transfers, international telex transfers, and local third party transfers. The latter allows customers to transfer money from their accounts to any other national bank account. However, the way this OBA works is different from the one discussed in the previous section. Here, the customer has to create what is called a "beneficiary account". This beneficiary account is the intended account to which the customer would like to transfer money. Once all the details of the beneficiary account are provided, the system sends a one-time pin number to the customer's registered mobile number (i.e., appears on the screen) by SMS (see Figure 4-6).

The figure illustrates the process of creating a beneficiary account in three stages:

- Stage 1: Create Local Third Party Transfer Beneficiary**
This form is divided into two sections:
 - BeneficiaryDetails**: Includes fields for Beneficiary Name, Beneficiary Address, Beneficiary Country (set to Oman), and Beneficiary Account Number.
 - Beneficiary Bank Details**: Includes a dropdown for Beneficiary Bank Name (selected: NATIONAL BANK OF OMAN-MUSCAT), Beneficiary Bank Country (set to OMAN), and a Swift Code field (set to NBOMOMXXXX).Buttons for 'Submit' and 'Cancel' are at the bottom.
- Stage 2: Authorize ThirdPartyTransfer Beneficiary**
This form prompts the user to 'Click on Proceed to receive Authorization Code. Click on Modify Details if below information is incorrect.' It contains a 'Mobile Phone Number' field with the value 96899422294 and buttons for 'Proceed' and 'Modify Details'.
- Stage 3: Confirmation Message**
A message box with a yellow warning icon stating: 'The page at <https://netbank.natbankoman.com> says: Your Authorization Code is sent to : 96899422294'. An 'OK' button is at the bottom right.

Figure 4-6: Creation of a beneficiary account

A request code (i.e., made of 5 digits) is sent along with the OTP to help the customer trace which OTP should be entered in the screen if more than one SMS message with different OTPs have arrived on the customer's mobile device (see Figure 4-7).

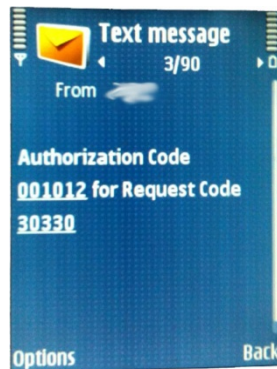


Figure 4-7: Authentication code via SMS

Once the customer confirms the OTP as received via SMS, the beneficiary account becomes activated and only then can the customer transfer money to it. The bank also implements this feature for the international telex transfer service where customers are allowed to transfer money to an account in a foreign country.

Discussion

This bank also implements a multi-level authentication mechanism. The customers are required only to provide a username and password to login to their online banking account. The password is chosen by the customer but it has to follow a password policy implemented by the bank. The implemented password policy suggests that a password should contain a minimum of 1 numeric character, a minimum of 1 alphabetic character (a-z/A-Z), and a minimum of 1 special character. The system allows only balance statements and other information (i.e. payments history) after a customer authenticates successfully.

The authentication method implemented at the transactional level, however, is more secure and utilizes more than one communication channel to authenticate new beneficiary accounts. It also uses one-time PIN (OTP) as authorization code to authenticate the beneficiaries.

Although this setup protects customers from most known attacks (e.g., user surveillance, phishing, and pharming attacks), this multi-channel authentication implementation has one major flaw. Attacks like man-in-the-middle (MITM) and man-in-the-browser (MITB) are still possible. For example, if a customer logs in and requests to add a new beneficiary account, he or she will input the beneficiary details in the form and submit. At this stage, a

MITM or MITB could alter the details entered in the form before they leave the customer browser to be transmitted to the bank server (e.g. alter beneficiary account number from 1111 to 2222). The bank server receives the beneficiary details and processes them immediately. It creates a valid request code and an OTP for the activation. These details are sent to the customer by SMS and the customer activates the beneficiary account by entering the received OTP via the webpage. The customer believes that he or she is activating the account number 1111 entered in the beneficiary account form, and the bank believes that the customer has added a new beneficiary account number 2222 (since the attacker altered the details). There is no way for the legitimate customer, nor the bank, to know that the beneficiary account details have been intercepted and altered, even after the customer confirms the addition of the new beneficiary account, because only the nickname the customer selected for that beneficiary account, the bank name, and the request code of the transaction appear in the beneficiaries list (see Figure 4-8). The beneficiary account number has been modified but does not appear in the beneficiary accounts list (i.e., if we assume that the altered account number 2222 and the original account number 1111 entered by the customer belong to the same bank). Although the account number will appear in the transfer page along with other details, it is not usually something a customer checks since the OBA has already advised the customer that the beneficiary account has been activated.


 Local Third Party Transfer Account List					
Beneficiary Name	Beneficiary Bank Name	Request Code	Status	Action	Delete
Mohamed AlFairuz BM	BANKMUSCAT SAOG-MUSCAT	04042	Authorised	Transfer	Delete
HUMAID ALI SULIMAN	NATIONAL BANK OF OMAN-MUSCAT	41202	Authorised	Transfer	Delete
Dawood	NATIONAL BANK OF OMAN-MUSCAT	02420	Authorised	Transfer	Delete
Mohamed	BANK SOHAR-RUWI	30330	Authorisation Pending	Transfer	Delete
Mohamed	BANK SOHAR-RUWI	00332	Send Authorization Code	Transfer	Delete
Create Local Third Party Transfer Beneficiary					

Figure 4-8: Details of beneficiary accounts after activation

The results of attacks based on such insecure implementation can be problematic. Neither the customer nor the bank is able to prove that the information submitted by the customer was altered, and the attacker receives payments (e.g. intended to be transferred to a different account number) from the legitimate customer without worrying about being caught, as the legitimate customer has approved the payments.

4.1.3.3 Case 3: Multi-factor, Multi-level Authentication

A third bank operates in Kuwait offers its customers a different experience of authentication. Instead of using only one method to authenticate users at login (i.e., username and password), it offers quadruple authentication methods consecutively. First, the user has to provide his or her bankcard number. Second, a random security question from five different security questions associated with the bank account is displayed and the user is requested to provide a valid answer. This answer should act as a secret factor known by the user. Third, an image and secret phrase, which have been selected by the user at an earlier stage, are displayed on the screen. The customer has to verify that these are the image and the phrase selected at enrolment time (i.e. only one image and one phrase is registered for each customer). Fourth, the user enters their online password.

The diagram illustrates a four-step authentication process, connected by red downward arrows:

- Card number:** A form with input fields for '4644', a dropdown menu for '5200', and two empty fields. A 'Login' button and a key icon are present.
- Security Question:** A form asking 'In what city were you born? (Enter full name of city only)'. It includes an input field, a 'Proceed' button, and a key icon.
- Your Image and Phrase:** A form asking the user to recognize a security image and phrase. It includes a 'Proceed' button, a key icon, and a link: 'Forgot or incorrect XXX Key?'. To the right, there is a box labeled 'Your Image:' containing a red computer monitor icon, and below it, 'Your Phrase:' followed by 'XXXXXXXX'.
- Please enter your XXXXX Online Password:** A form with a password input field, a 'Login' button, and a key icon.

Figure 4-9: The quadruple login authentication process

Finally, if the customer has successfully validated all previous phases, the OBA requests the account password to complete the login process (see Figure 4-9).

This bank provides many online services. These services include money transfers to credit and benefit cards, bill payments, and money transfers to other local and international accounts. However, an additional authentication level is required to complete these transactions. For example, to transfer money to a local bank account, the customer has to add the new account as a beneficiary account (the same technique as discussed in the previous case).

To authenticate the new local bank beneficiary account, the application requests that the customer provide three digits from different places within the customer registered civil ID, corporate number, passport number or military ID, which has been registered at the time of enrolment (see Figure 4-10).

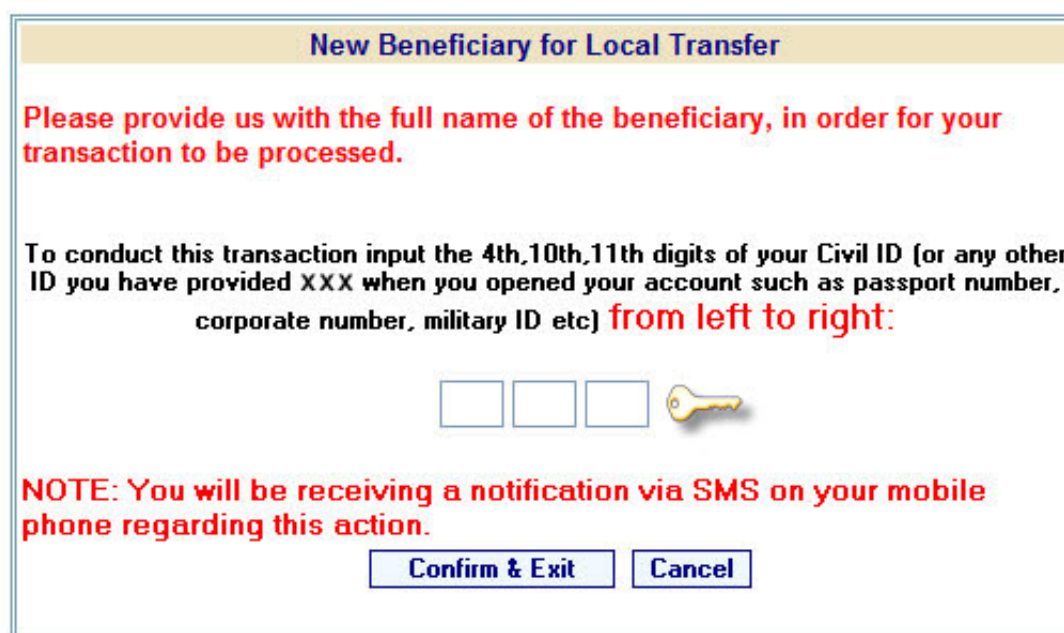


Figure 4-10: Add local beneficiary account authentication method

After the activation of the new beneficiary account, the customer is authorized to transfer money to it anytime without further authentication.

For international transfers, the application adds yet another authentication layer where the customer is required to validate the process of adding an international beneficiary account using authentication (in Figure 4-10) and a predefined PIN number known by the customer only.

Discussion

The authentication method used by this bank is different from the other traditional authentication mechanisms. The authentication at login is carried out at four different levels: the request of the customer bankcard number, the secret question, the image and phrase verifications, and finally, the online banking account password. Although the card number and the answers to the secret questions cannot be considered highly secret details, they work perfectly against attackers who are not in direct contact or relationship with the bank customer.

The image and phrase verification process is meant to fight phishing attacks. If a bank customer is directed to a fake bank website, which requests his or her authentication details, that website will not be able to display the image and phrase the user selected at enrolment time since these details do not require user input; rather they are retrieved from the bank database. The implementation of this method is proposed in the literature by Dhamija and Tygar [198]; they called it “Security Skin”. However, this only works perfectly in non-targeted first time phishing attacks, where the attacker has not previously intended to attack a specific customer. If an attacker has launched a targeted phishing attack against one customer, the attacker will be able to gain knowledge of the type of image and phrase the user has selected at enrolment time, especially if the customer has repeatedly answered secret questions from the second authentication phase after the attacker has captured the first factor (the card number); this allows the collection of the different secret questions from the original OBA to inject them into the fake website.

At the transactional level, the bank implements another authentication method for creating beneficiary accounts (e.g. local and international). It requests customers to input certain digits of their registered civil ID, corporate number, passport number, or military ID.

From a security point of view, all authentication methods used at login and transactional level phases are sent using the web channel. If an attacker is able to compromise this channel, any or all details can be captured and changed. Although the image and phrase verification at login, as well as the input of certain digits of the customer ID, protect the customer from a single non-targeted attack, all authentication factors can be captured in targeted attacks after the customer logs in and makes several transactions, repeatedly entering different digits of the ID as requested by the application.

Moreover, attacks like man-in-the-middle and man-in-the-browser are able to compromise the authentication methods implemented by this bank from the very first attempt. This is possible by altering the transaction details the customer enters to create beneficiary accounts.

4.2 Mobile Communication

Although mobile devices are increasingly becoming susceptible to many threats, as we will see in the review covered in this section, the security properties offered by mobile devices can achieve the best possible protection for online authentication if combined with other independent authentication mechanisms such as the conventional username and password. This section presents a review and discussion of the mobile network and mobile devices, in terms of usability and security.

4.2.1 Usability of mobile devices and network

Mobile calls and SMS (Short Messaging Services) messages are globally accepted wireless services that enable the transmission of voice and alphanumeric messages between mobile subscribers. These services were first introduced by the European standard for digital wireless (now known as the Global System for Mobile Communications or GSM) in 1991 in Europe.

Mobile phones, unlike other personal belongings, are considered to be the most personal devices (linked to one person) [35]. Compared to other tokens such as bank cards, they are faster to notice if lost or stolen [199], and therefore, many researchers and current online applications are using them as authentication factors for business transactions. Moreover, almost every mobile user, who has a contract, is known and registered by the mobile service provider, which in turn, acts as a trusted third party in any business transaction.

Mobile phones have become tools that are carried and used by people everywhere and their services are not limited to a geographical area (i.e., the roaming service has made it possible for someone to utilize the mobile phone connection without having to change the mobile service provider when travelling abroad).

In the past few years, mobile phones have become the most widely used personal devices ever among users. Statistics show that there were approximately 60 people out of 100

using mobile phones in the world in 2008 (see Figure 4-11). People use mobile phones to make and send more than a billion calls and text messages every day [200].

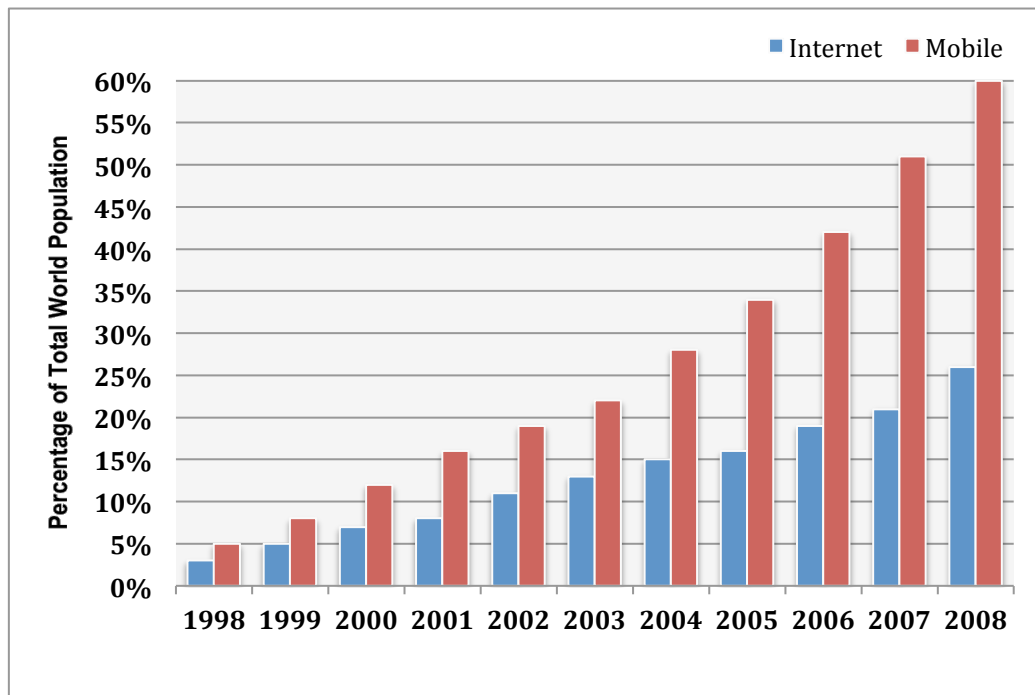


Figure 4-11: Internet and Mobile User Stats from 1998 to 2008 [201, 202]

Unlike other services provided by mobile networks, SMS is the most convenient and most realistic and achievable approach [203]. It has become the most popular service for the following reasons [204]:

- Globally accepted wireless service
- Enables the transmission of alphanumeric messages between mobile phones
- Uses store and forward asynchronous delivery method; messages are stored and delivered whenever end-user becomes available.
- Supports notification of delivery
- Supports multi-languages

These SMS features have encouraged different businesses to implement and utilize SMS messages in various ways. Some examples of these implementations are listed below [205].

- Marketing: many organizations use SMS messages for advertisement purposes. They send information about their products and offers to all mobile subscribers (who opt-in) for a relatively lower cost compared to other advertising media like TV programs and newspapers.

- Authentication: some businesses are using SMS messages to authenticate transactions by delivering PIN numbers to/from mobile users. Sometimes SMS authentication works together with other authentication methods for better security.
- Collection of payments: several companies like Paybox and Paypal have implemented payments via SMS successfully. Mobile users can pay for products and services if they are registered customers of these companies. There are also other forms of payment that utilize a derivative protocol from SMS called premium-rate SMS (PSMS). This protocol allows organizations to subscribe for special numbers, which charge subscribers' SMS messages a premium rate higher than the standard SMS rate set by the mobile operator. This is commonly seen on TV and SMS guessing contests.
- Couponing and ticketing: just another two forms of payment collections that are mainly used to cut the operation cost of issuing coupons and tickets. Car parking tickets through an SMS messages is one example of this service.
- Direct sales: people can download contents or applications to their mobile devices and charge on their bill (e.g., ring tones, wallpapers, applications, etc...).
- Interactivity and data collection: this is a very attractive business to broadcasting channels. People can vote for their favourite actor or player by sending SMS messages, which cost relatively less than other voting media. However, on a high scale, millions of SMS messages are received, and therefore, big profit margins are generated at the end of the day.
- Micro-finance: M-Pesa by Vodafone and MobileMoney by MTN and Standard Bank are two micro-finance systems. People are able to transfer money from one mobile user's account to another using their mobile phone devices.
- Support and maintenance: mobile service providers usually send service updates to mobile users via SMS. Other companies utilize SMS messages to notify their customers about a recent purchase or after sale maintenance status.

Despite these many features available via SMS and other mobile services, when payments are involved, users' level of acceptance is directly affected by the amount of payment required. According to SpeedFacts [206], users prefer to pay by mobile if the amount of payment is between 12.5 and 50 Euros while they prefer to use other payment options (e.g., debit/credit cards or cash) when the amount is more than 50 Euros (see Figure 4-12).

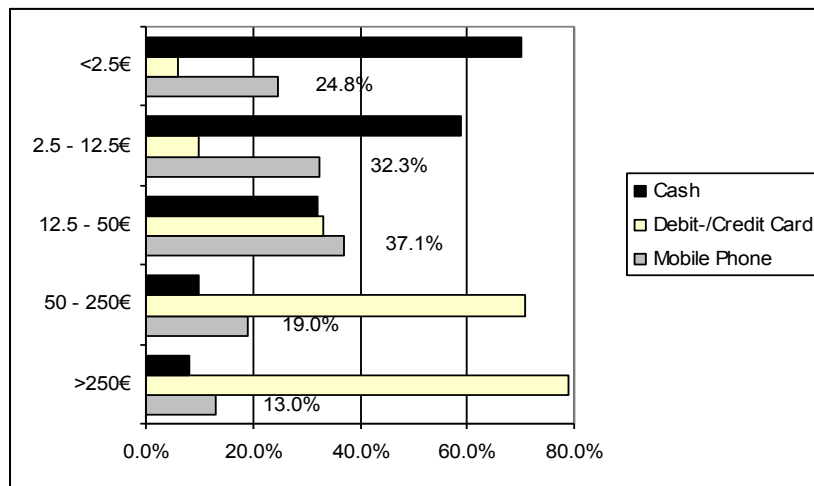


Figure 4-12: Preferred payment method of Internet users if away

4.2.2 Security of mobile devices and network

Despite the high user acceptance of mobile network services (e.g., voice calls and SMS messages), mobile networks, and mobile phones are not 100% secured. There are many articles published, which address the weaknesses of the mobile network infrastructure. Odell published a story in Financial Times about the Italian police who were able to track the location of a suspect using his mobile device. He also stated that mobile operators are able to tap all calls made from/to any mobile device utilizing their network, and worse, they can remotely install a piece of software that will turn the mobile device into a microphone, which transmits the user voice even when no call is active [207].

Another story published by Gupta [208] addressed one of Germany's computer scientists, named Karston Nohl, and his team of 24 hackers who successfully cracked the algorithm used to encrypt mobile calls in GSM networks. Likewise, an article published by Stanley [209] about intercepting and tapping mobile calls without the need for cracking the algorithms. He claimed that installing a fake base station to be used by mobile devices that are closer to it than to other real base stations allows an attacker to tap mobile calls passing through the fake base station. This is achieved with the help of a few software products that are available for free and the fake base station materials that cost an average of £1000 .

SMS messages have suffered widely from what is known as SMS spoofing. It occurs when a fraudster manipulates the SMS message address information in order to impersonate a subscriber [210]. Therefore, SMS spoofing can be used for spamming or for posing social and/or political conflicts between different parties (i.e., an attacker, A, can spoof and send

a SMS message with unacceptable texts to user X, which will appear to him as if it is coming from user Y).

Mobile devices are also now more prone to attacks than ever because of the increasing number of smart phones, which were introduced to replace the traditional cell phones. The main difference between a cell phone and a smart phone is that a cell phone does not have an operating system, although it can still make calls and send SMS messages and e-mails [211]. The mobile's operating system (e.g., Windows Mobile, Google's Android, iPhone's iOS, and Nokia's Symbian) is what makes a cell phone become a smart phone with more services like e-mail clients, web browsers, and other Internet services. Smart phones provide the user with the ability to connect to different networks at the same time (i.e., the ability to connect to the GSM network while surfing the web using EDGE, 3G, or Wifi networks). This makes the device vulnerable to different attacks (especially attacks from the Internet networks) that can compromise and utilize all other services and networks used by the mobile device (including services provided by GSM and CDMA).

Hoffman [212] stated that the number of malware products targeting mobile devices is increasing. He said that most of the mobile platforms are susceptible to malware and they are not shipped with anti-virus software. Moreover, he stated that more than 400 mobile malware programs have already been detected; some are keyloggers, while others intercept communication and run functions without the need for user interaction.

4.2.3 Mobile Devices as Authentication Tokens

Recently, mobile devices have been widely used to authenticate payments or customers' transactions online. Mobile devices are not used to identify a user; rather, the SIM card and the mobile number associated with it can be uniquely used to identify a user. This type of identification is similar to the use of a username in the traditional username/password authentication mechanism. The mobile number of a user cannot be considered as a secret since it is available for the user's friends and relatives and sometimes it is listed in public mobile phone directories or published online. Hence, mobile phone numbers can offer more than what a username offers in traditional authentication. A mobile number is usually assigned to a SIM card, which by itself can work as an authentication token if it requires a PIN number to unlock and operate.

4.3 Summary

Online banking has been among the fastest growing online businesses in the past few years. The services offered to bank customers online are critical and risky. People can perform a number of financial transactions, including the transfer of money from their accounts to other foreign accounts online. Thus, there is always a need to secure online banking systems with the latest and most trusted authentication mechanisms that are able to withstand most known attacks online.

In this chapter, the status of online banking applications were classified into three categories: informational, local-transactional, and transactional online banking applications. The chapter then studied and discussed different cases of currently implemented authentication mechanisms in online banking and compared their security against the attacks covered in Chapter 2.

Mobile communication is also considered one of the fastest growing and most acceptable communication channels around the globe. Mobile devices are the most personal devices today and people carry them more than any other personal item or device. For this reason, some researchers proposed the use of mobile devices as complementary authentication tokens that could play a major role in improving overall security if integrated with other authentication mechanisms.

The next chapter proposes a multi-channel, authentication mechanism solution. This solution benefits from the advantages offered by a secondary channel other than the Web (e.g. mobile network) in a multilevel online banking environment. More details of the advantages of mobile devices in authentication are discussed in Chapter 5: Proposed Solution.

Chapter 5

Proposed Solution

5.1 Introduction

Chapter 2 focused on authentication classes as well as attacks that can target any of the three core communication elements: *end-user (EU)*, *communication channel (CC)*, and *online service provider (OSP)*. Chapter 4 introduced online banking as one of the most critical and widely used online applications. Evidence was provided to support the assertion that current authentication mechanisms introduced by online banking applications are vulnerable to several online attacks. The evidence suggests that there is a need for a more secure authentication mechanism that is capable of providing better security while maintaining usability and fostering acceptability to end users.

This chapter proposes a multi-channel authentication (MCA) infrastructure that is able to withstand the most popular, previously identified online attacks while maintaining acceptable levels of usability and acceptability. First, section 5.2 discusses the proposed infrastructure in terms of online banking, applicability, feedback, and its advantages over the single channel approach. Section 5.3 discusses the importance of the mobile network to the proposed MCA mechanism and highlights those features that make it the most suitable secondary channel for MCA. In section 5.4, the proposed MCA infrastructure is assessed by means of threat modelling based on the STRIDE process. The evaluation addresses all applicable attacks that target end-users (EU) and communication channels (CC) covered in Chapter 2.

5.2 Proposed Infrastructure

Authentication mechanisms currently implemented by online banking sites are criticized for their inability to deliver systems that meet the highest standards of security while maintaining high usability. Some online banking systems offer their customers advanced security technology and features using tokens and biometrics. However, because usability

is neglected in most of these systems, customers sometimes find it difficult to do banking online. For example, some online banking systems require the use of a SecureID token for the customer to transfer money from one account to another. The token by itself is not a personal device that one would carry all the time. If the customer does not have the token at the time of transfer, he or she will not be able to complete the task. Another usability issue occurs when the bank implements Java-based add-ons (e.g., on-screen virtual keyboard) that are not compatible with all browsers. These usability issues may lead to customers not fully accepting these authentication mechanisms and this may lead to reduced customer loyalty. It is, therefore, important to introduce an authentication mechanism that is perceived by customers to offer superior security to other alternatives while being usable in terms of effectiveness, efficiency, and satisfaction [213].

MCA has the potential to protect customers from most known attacks. However, a suboptimal implementation of MCA could lead to security problems and/or usability weaknesses and possible rejection by customers. In terms of security, the online banking application case discussed in Chapter 4 (section 4.1.3.3) proves this argument. In terms of usability, improper implementation of MCA could cause frustrations leading to rejection of the mechanism and the site, which could negatively affect the market share of the organization. Therefore, it is vital to ensure the optimal implementation of MCA.

Figure 5-1 provides a general overview of how a multi-channel authentication mechanism should be implemented. However, there will be variations depending on business needs and security level requirements.

This proposal suggests that MCA should be implemented on a multilevel structure. A user should be able to carry out basic functions throughout the web application by logging in using a conventional authentication mechanism (e.g., knowledge-base authentication). At this stage, only read-access is granted. If the user wants write/modify access, then a random one-time “secret” with the task details should be passed to the user over a secondary channel (this must be a non-web channel). It is important to ensure that the system delivers the secret factor through a channel other than the one used for user login, which might be compromised. Task details are sent along with the secret factor to make sure that the user is aware of the task he or she is verifying (i.e., to contextualize the message). This is vital to avoid any possibility of man-in-the-middle or man-in-the-browser (both will be abbreviated as MITM/B) and real-time phishing/pharming

(abbreviated as RTP/P) attacks. These attacks are discussed in sections 2.4.2 and 2.4.3 of Chapter 2.

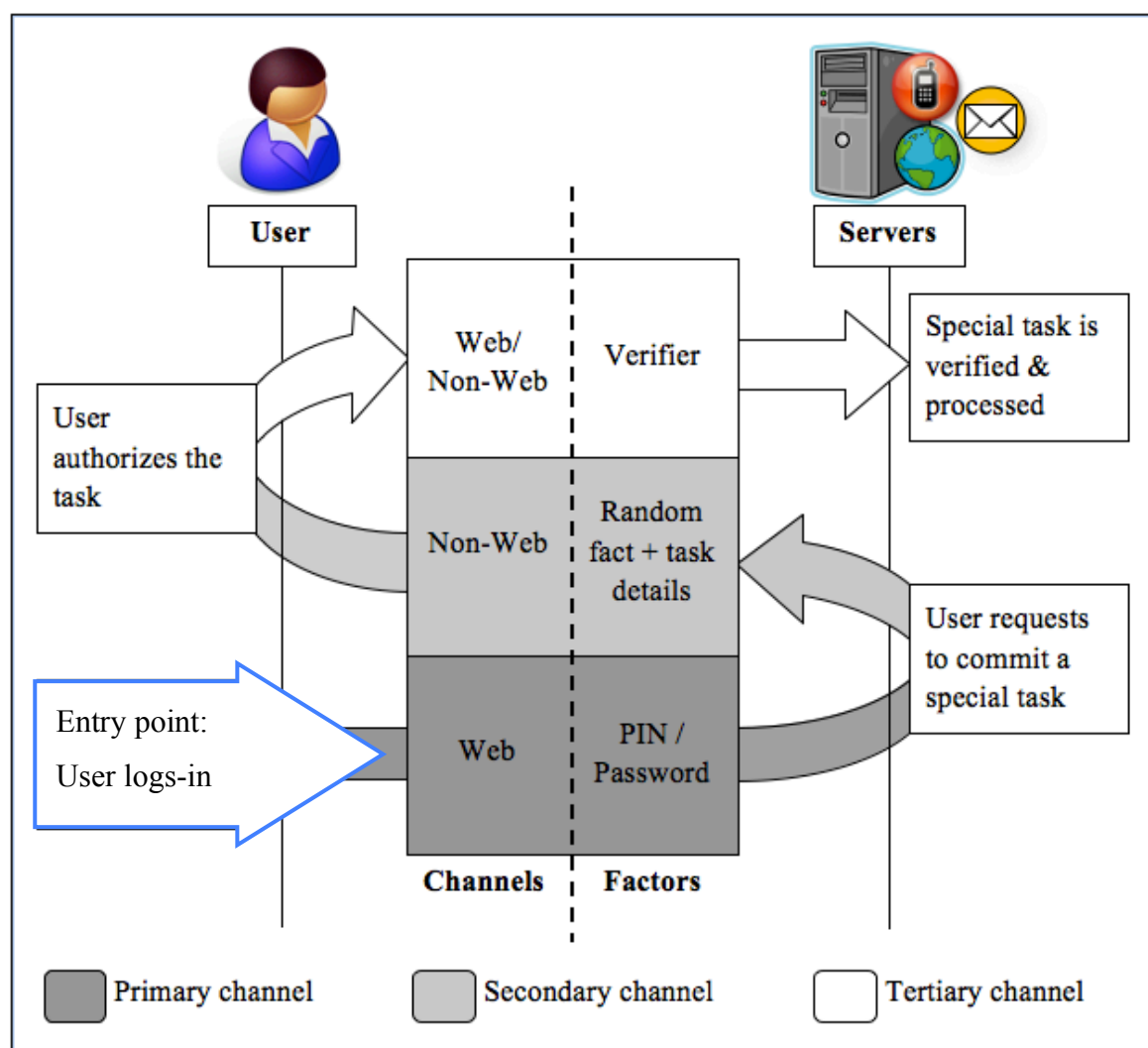


Figure 5-1: The proposed MCA infrastructure

Once the OTP is received via the secondary channel, the user can verify his/her secret using any available channel. Only at this stage will the write/modify task be authenticated by the system.

5.2.1 MCA for Online Banking

Online banking systems are the most critical online business applications due to the risk involved in the financial transactions they offer to their customers. High security measures are crucial to foster a trusting relationship between the bank offering the online banking services and its customers. Usability, on the other hand, is also important to keep these customers loyal to the bank. There is no single solution that is favourable to all customers and that meets all of their different expectations. However, providing a system that is

customizable to match the different needs and preferences of different customers without compromising security gives the bank a competitive advantage over other banks. This can be achieved, in the context of the proposed MCA, by offering the users the opportunity to select *where* and *how often* to activate the MCA throughout the system. A minimum requirement must be implemented at some point before online transactions can be electronically carried out. This flexible customization does not affect the level of security offered by MCA; rather, it makes the application more usable and acceptable to users by matching their levels of risk appetite and awareness.

To illustrate how this can be achieved, each of the customization factors (*where* and *how often*) is described in the practical scenarios below:

- Where to implement: users should be given the ability to select where to implement the MCA mechanism throughout the online banking application. A user with low or no privacy concerns might prefer to use MCA only at times when external financial transactions, such as “money transfer to an external account” and “bill payments”, are required. This means that MCA would not be required for balance checking or internal financial transactions (e.g., transferring money from account A to account B of the same user, credit card bill payment, etc...). If the user is very concerned about security and privacy, he or she might prefer to require MCA for every single transaction (internal or external) or even request to have MCA implemented at login.
- How often to implement: some users might not be willing to involve their mobile phones or other channels into their online banking experience, and therefore, they would tend to minimize MCA to the least options available. For example, they may only activate MCA for financial transactions that involve more than a specific amount of money (individually and collectively). For example, if the amount specified were £100, no individual transaction that is more than £100 would be processed without MCA (whether in one transaction or multiple transactions with smaller amounts). This amount would be considered a threshold and it would trigger the MCA mechanism whenever the transacted amount reached or exceeded the limit. Feedback plays a complementing role here as the user could be informed by SMS or by other means about every single transaction completed. In contrast, users who are very concerned about security and would like to be in more control of their accounts might prefer to have the MCA mechanism involved in every single transaction no matter how much money is transacted.

This study proposes a default moderate implementation of MCA. That is, a user is allowed to login to the online account using a conventional authentication mechanism (e.g., username and password). This first level privilege gives the user access to account statements. To carry out a financial transaction (e.g., money transfer to another account) the user has to create a beneficiary account record for the target account. This process requires use of the MCA mechanism. The system sends the user an SMS message containing a one-time pin (OTP) and the details of the transaction and requests the user to validate the transaction by providing the OTP received. Once this procedure is completed, the beneficiary account becomes active and the user can then transfer money to it anytime, using only the standard authentication.

It is important to mention that this proposal should support feedback. The application should also allow only a certain number of retries when verifying the OTPs. This helps avoid brute-force attacks (covered in section 2.4.1.3) that can succeed if no limitations are enforced. The flow chart depicted in Figure 5-2 further explains the way the proposed MCA implementation works.

As shown in Figure 5-2, password retry limitations are implemented in three places throughout the application: the login phase, the activation of beneficiaries phase, and finally, when confirming transactions. If an invalid password or OTP is entered three times in any of these authentication phases, the account is deactivated automatically. The re-activation procedure can be implemented in different ways. However, discussion of this is beyond the scope of this study.

5.2.2 Applicability of MCA

MCA can meet different needs depending on the business type and the level of security. Some applications might require military-grade authentication mechanisms while others might require the conventional username and password to authenticate users.

Correspondence applications, as an example, might require MCA to be applied as the primary authentication level. Access to the user account can be denied until all authentication requirements have been met. However, the user is the one who should decide whether to enable these extra security measures or to disable them as the need for security varies from one user to another and even between different tasks by the same user.

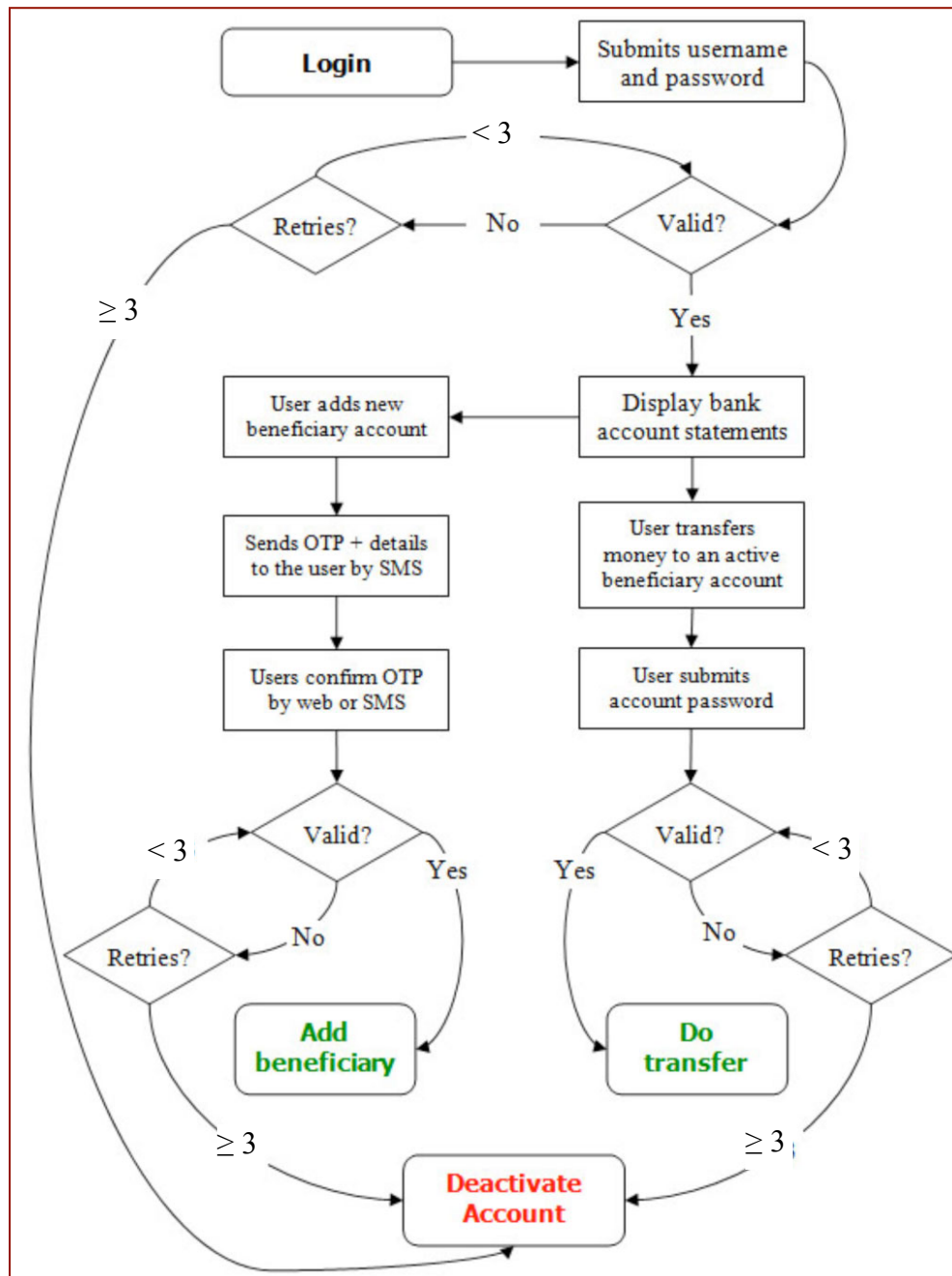


Figure 5-2: The proposed MCA in online banking

For example, a user uses the e-mail address `x@example.com` to communicate socially with friends and family members. This user utilizes this e-mail address every day and does not keep confidential e-mails stored in the account after they are pushed to e-mail client software installed on the user machine. In this case, this user does not require another verification channel for each login attempt to the e-mail client. Moreover, implementing a multi-channel authentication mechanism for this e-mail account could be considered a usability drawback since the user would need to be authorized several times a day using different channels.

Consider that the same user has another e-mail address `y@example.com`. This e-mail address is used as a main contact address for the user's payment account with Paypal, for eBay transactions, and as an alternative e-mail address to reset other e-mail accounts belonging to the user. Although the user might not need to access this account every day, it is more important and critical to secure this account than to do so with the first e-mail address. Therefore, the user is more likely to choose to use multi-channel authentication to control access to the second e-mail account.

Online banking accounts might require a different setup as covered in section 5.2.1. The most important tasks carried out are those that require modification of the user's balance statement (transferring money or paying utility bills). MCA should be implemented only when a request is issued by the user to initiate such transactions. Otherwise, traditional authentication may be enough for read-only access to the user records (e.g., checking account statements and payment histories).

Another example is online community forums. MCA can be used by moderators or site administrators as they have privileges to change the site's global settings and to edit other users' posts and threads. The forum members, however, do not require such advanced authentication mechanism since their actions do not pose high risks that would require MCA.

The proposed multi-channel infrastructure can meet the needs of many different online applications with many different purposes. However, the implementation should focus first on the usability and security requirements of the target application, and above all, should consider the costs and benefits of running such an infrastructure from the user's point of view.

5.2.3 Cost of MCA

The running cost of MCA is relatively low, compared to other authentication technologies. The proposed MCA is the cheapest token-based authentication mechanism since it does not require introducing new tokens to the customers. The tokens are something the customers already have (e.g., mobile devices). Other token-based technologies invest heavily in designing and building the hardware. They then have to spend more on teaching the customers how to use these technologies. Worse, they are responsible for maintaining these tokens and offering customers live support. All these issues are avoided with MCA. Users

usually buy their own mobile devices and they maintain them directly with the supplier company. In terms of token awareness and use, SMS is an inexpensive, ubiquitous worldwide service that is used by most mobile users today.

The only running cost of MCA is the cost of delivering the OTP, which is borne by the organization. In the proposed MCA, this means the cost of SMS messages exchanged between both OSP and EU. However, since there are two options for authorizing tasks in MCA, a customer is not required to send out SMS messages since it is sufficient to receive the SMS message that carries the OTP and transaction details. The customer then can confirm the OTP received by entering it into the screen using the Web channel (see Figure 5-1).

5.2.4 Feedback

Feedback is one of the core aspects of good interface design. Nielsen included the visibility of system status as one of the top 10 usability heuristics [214]. He argued that any given system must inform its users about what is going on by means of an appropriate feedback.

Feedback is categorized into two categories [215]: *required* and *confirmatory*. The required feedback is the feedback given during task execution. According to [216], “when the feedback is immediately available, the user will be less likely to automate the task, and more likely to work in a controlled mode – making less errors”. Based on this, required feedback is about making the system more usable to users. The confirmatory feedback, on the other hand, is the information given to the user at the end of a task. In the context of MCA, this can be represented by a confirmation SMS message that is sent to the users to inform them about the completion of a task and its details. For example, the banking organization may send a SMS message informing the customer that an amount of £100 has been transferred to the account number 12345678 successfully on Monday 13th of September 2010, 11:04:25pm. This feedback is a very important element of the overall security proposed in the MCA infrastructure.

Another complementary feature of feedback suggested by the proposed MCA infrastructure is to allow transfer delays of a few minutes before the transaction completes. This delay can be set to zero seconds if the amount transferred is below a certain amount (e.g., £100). If the amount exceeds the specified amount, the system should incur a delay period before the transaction takes place. This allows the legitimate account owner to

report a fake/illegal transaction upon the receipt of the confirmatory feedback SMS message before the transaction is finalized. This is demonstrated in the scenario-based evaluation of the MCA mechanism covered in section 5.4.

5.2.5 Advantages over Single Channel Authentication (SCA)

The use of multi-channel authentication (MCA), as opposed to single channel authentication (SCA), can offer significant advantages in terms of both security and usability [217]. A number of different independent channels have to be compromised before full access to the user account is granted to an attacker. This makes non-targeted attacks almost impossible. It also makes targeted attacks harder, especially if the attacker is not geographically close to the user to be able to gain physical access to devices used as verification channels.

Unlike SCA, MCA provides protection against most real-time attacks including MITM/B, RTP/P, and malware. Some of these attacks have the potential to capture and manipulate, in real time, the data exchanged between users (e.g., bank customers) and the online service (e.g., online banking web application). These attacks target organizations and users for economic gain and are considered global threats [86]. Data integrity is not maintained and both sides (i.e., users and online service providers) are often unaware of such attacks. With MCA, the attack is made visible to the user to reveal that the exchanged data has been altered by an attacker or malware (more evaluation of other attacks in section 2.4 of Chapter 2). MCA is safer because the online service provider will not process transactions without user confirmation nor will the user verify transactions he or she did not request. The whole idea behind using two different independent channels is to ensure integrity and authenticity even if one particular channel is compromised at the time of the attack.

Since MCA is not limited to specific channels as long as they are very independent from the primary channel, various independent channels can be used in the MCA infrastructure. However, the proposal suggests that mobile networks (e.g., GSM, TDMA, and CDMA) should be used to achieve the best possible balance of security and usability. Mobile networks are the most practical and usable networks found to serve MCA implementation best. This recommendation is justified in the following section.

5.3 Mobile Network as Secondary Channel

Mobile communication is currently the most widely spread and fastest growing communication technology around the world [218]. Since its introduction in the 1970s, mobile technology has undergone dramatic improvements and enhancements. Such improvements have expanded mobile communication functionality and added significant value to it. SMS has become a critical aspect of mobile communication and it is commonly used by different organizations and people around the globe (see section 4.2.1 for details and examples of the current use of SMS in mobile commerce). The Internet, on the other hand, has played a vital role in mobile communications along with SMS. The introduction of smart phones has expanded the range of services offered by mobile communication. For these reasons, mobile communication has become an integral part of day-to-day life. The ubiquitous influence of mobile technology has been significant in the past few years due to the emergence of various “m-“ services, such as m-commerce, m-learning, m-government, m-entertainment, m-gaming, and m-etiquette [218].

Mobile communication is protected against attacks by means of cryptography. For some mobile communication services, such as SMS, the cryptography is available to the public and can be used to decrypt SMS messages. For this reason, SMS messages do not offer a secure channel, and therefore, it has not been used solely as an authentication factor by itself, but rather as a complementary channel for authentication as discussed in section 4.2.3 of Chapter 4. MCA currently proposes the use of SMS as a secondary channel. The status of mobile SMS messages makes them the most usable independent channel besides the Web for authentication. However, other channels can also be integrated into the structure as long as these channels are usable and do not share the same device used to serve the primary channel. For example, automated calls can be used to pass the OTP to the users via mobile or telephone networks. A user would receive an automated call from the service provider that would dictate the OTP number. This service can further be used to secure the phone call and verify that the mobile device holder is the legitimate account holder. This can be done by asking the customer to answer one of the registered secret questions (e.g., date of birth, social security number, PIN number, etc...). The answers provided by the customer can be entered numerically by keying the numbers using the mobile numpad. If the answer is correct, the program that is controlling the phone call can then dictate the OTP number to the customer. In this manner, the system ensures that the customer account remains secured even in case of targeted attacks. For example, if an

attacker was able to compromise a customer online account as well as physically to get hold of the mobile device used as a secondary authentication channel, the attacker would still need to know the answer to the secret questions asked by the automated call, which makes it harder to compromise.

It is, however, very important to reiterate that the secondary channel cannot share the same device as the primary channel. As mentioned earlier, smart phones now offer different services other than the conventional voice calling service. A smart phone device can be used for Internet browsing as well as SMS, instant messaging, and voice-over-IP (VoIP) calling. If the same device is used as a primary channel (e.g., using the smart phone web browser to login to the bank account) and, at the same time, to receive SMS with OTP as a secondary channel, then compromising the device means compromising both channels at once. Therefore, the MCA proposed in this study strongly suggests the use of two physically separated independent channels to achieve the highest possible level of security to protect an online banking customer from the common attacks listed in section 2.4.

5.4 Theoretical Evaluation of MCA

The quality attributes of any given system architecture can be evaluated either theoretically or practically. These analyses complement each other to determine the extent to which such systems meet the desirable benefits and fits the needs of users. In terms of the MCA proposed in this study, secure Internet banking is the ultimate goal to reach. Although it is often impossible to prove that a given design is secure, a proper evaluation of the security properties of the design will usually enhance security. This is the essence of what is known as *threat modelling* [219].

According to Jones [220], “*Threat modelling is the core step in any security solution. It is a way to start making sense of the vulnerability landscape*”. It is a six-stage process illustrated in Figure 5-3. These stages are required to evaluate a system thoroughly at the design phase. This study does not evaluate a complete, online banking system infrastructure. Rather, it evaluates only the authentication mechanism at the application level where the underlying network, host infrastructure design, and web-server technologies are ignored.

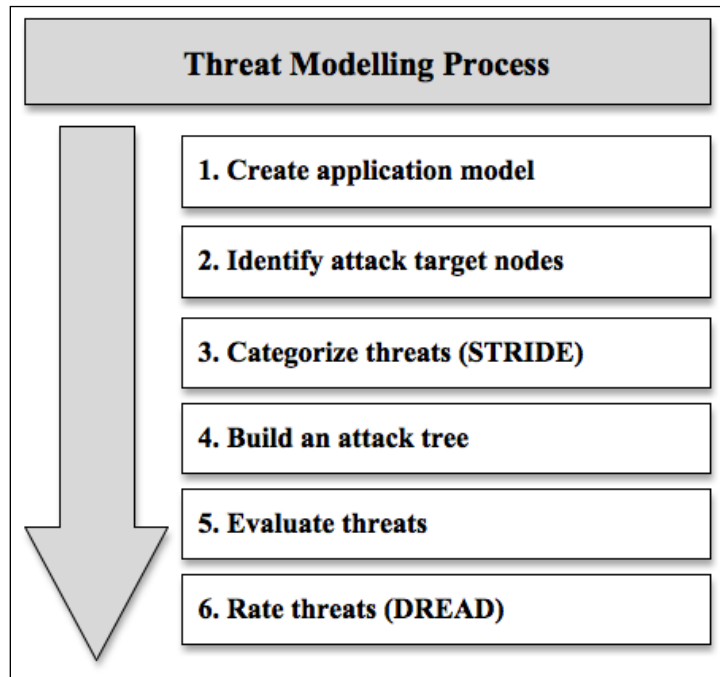


Figure 5-3: Threat modelling six-stage process

To evaluate MCA architecture theoretically, a scenario-based evaluation suggested by [221] is used. This employs threat modelling using STRIDE (an acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege) and DREAD (Damage potential, Reproducibility, Exploitability, Affected users and Discoverability). STRIDE and DREAD are processes developed by the Microsoft Application Consulting and Engineering Team to represent various methods or scenarios through which an adversary may attack a system [222]. These processes will involve examining the proposed MCA architecture against attacks that target the communication channels (CC) and end-users (EU) listed in sections 2.4.2 and 2.4.3 respectively. The attacks on online service providers (OSP), however, are ignored here because the MCA provides protections for the user and communication channel levels only.

The practical evaluation of the proposed MCA architecture, on the other hand, involves empirical prototype testing on a sample of Internet users, which is covered thoroughly in Chapter 7. Information about attempted/successful attacks on banks' online systems was not included in this chapter as banks treat these figures as strictly confidential and refuse to release them to the public. They believe that these statistics would severely affect their image and customers' trust if made public. A few cases, leaked to the press about successful attacks on bank customers' accounts, were covered in section 4.1.1.2. These cases support the fact that the existing banks' authentication mechanisms are still unable to

protect customers from cyber attacks. However, these limited cases do not reflect the real impact of cyber attacks on online banking systems.

There are other threat modelling systems exist such as AS/NZS [223], CVSS [224] and OCTAVE [225]. However, the threat modelling process by Microsoft is the most suitable threat modelling approach for web application security risks and was used by Microsoft for their internal software threat and risk modelling for years. According to [226], AS/NZS approach is applicable for non-technical risks and does not provide structured methods to enumerate web application security risks. CVSS also, unlike threat modelling by Microsoft, suffers from a complex ranking system and does not cover design flaws. Although OCTAVE threat modelling is considered as a heavyweight risk methodology approach for large and small organizations, it does not provide assessment and mitigation of web application security risks.

The following sub-sections will cover the six-stage process of threat modelling for MCA architecture using the STRIDE and DREAD processes as suggested by [220].

5.4.1 MCA Application Model and Attack Target Nodes

Figure 5-4 shows a high-level architecture diagram that describes the composition and structure of an online banking application with MCA. The diagram illustrates how the main elements are connected to each other. These elements are:

- Data Flows: represented by the one way arrows
- Processes: represented by large diamonds
- Data Stores: represented in the figure by the database
- Interactors: represented by the EU and the web server
- Trust boundaries: represented by the dotted lines

The diagram also presents the assets of the system that need to be protected against attacks. Some of these assets (e.g., end user, informational services) do not pose high risks by themselves. However, if an attacker compromises them along with other types of assets such as transactional services, they could severely affect the overall security of the customer's account.

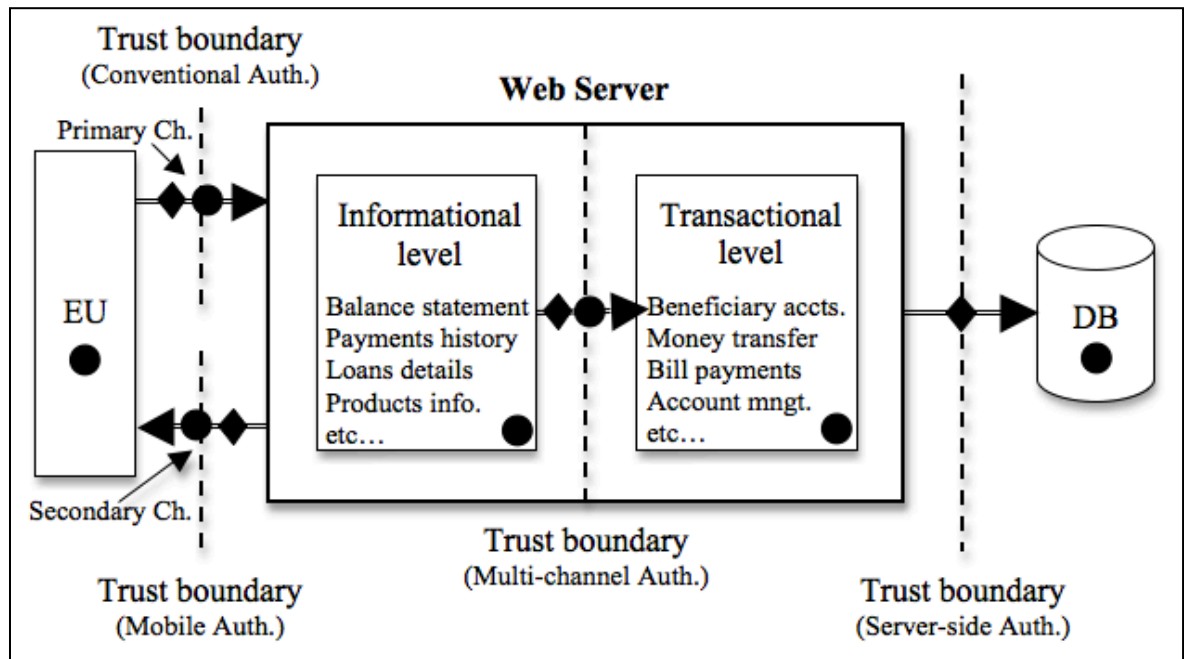


Figure 5-4: The proposed online-banking application architecture diagram

The attack target nodes, which are represented in Figure 5-4 by the large dots, show the parts that need critical analyses at component levels to identify the threats. Trust boundaries, on the other hand, guard the entry points of the system where the passing data need to be validated, authenticated, and authorized. Four trust boundaries exist in the proposed architecture:

- A trust boundary exists between the EUs and the OSP's web server. It is responsible for authenticating end users and authorizing them to access the informational services of their accounts on the OSP's web server. A conventional authentication mechanism is sufficient at this stage as discussed earlier in section 5.2.1.
- Another trust boundary exists between the OSP's web server and the EU. This addresses the delivery of transaction details and OTPs that the customers need to authorize transactions. The data flow is contained entirely within a trust boundary and no further authentication factors are needed. For example, in the case of mobile SMS messages, a mobile number of the customer identifies him/her to the system and the SIM unlock code, if it exists, represents the authentication factor.
- A third trust boundary lies within the web server itself and splits the services offered by the system into informational and transactional. This trust boundary is responsible for authorizing customers to carry out transactional services that are assumed to be of high-risk nature (e.g., money transfer, bill payments, etc...). In this stage, multi-channel authentication is the proper authentication mechanism to apply (see section 5.2.1).

- The last trust boundary exists between the web server and the database and it protects the database from unauthorized read/write requests. Usually the database resides in a separate server, and therefore, this trust boundary allows the web application to access the database server using a fixed and trusted identity. This type of authentication mechanism is not related directly to the end users and is, therefore, out of the scope of this research.

5.4.2 Identify and Categorize Application Threats Based on STRIDE

According to [227], the identification of threats requires three tasks to be performed: identification of network threats, identification of host threats, and identification of application threats. Since this research is solely concerned with the authentication mechanisms of an online banking application, the focus is on the third task only.

The identifying and analyzing process requires categorizing the threats into the following six STRIDE nodes:

- Spoofing: occurs when an attacker pretends to be a legitimate user/customer while he/she is not.
- Tampering: occurs when the data sent by a legitimate user/customer is modified in transit before it gets to its final destination.
- Repudiation: the ability for someone to deny that he/she has performed an action.
- Information disclosure: occurs when an attacker is able to read confidential information.
- Denial of service: occurs when an attacker disables the communication between the EU and the OSP.
- Elevation of privilege: occurs when an attacker is able to takeover access controls/privileges that he/she would not normally have.

Each of the elements (data flows, data stores, processes, and interactors) depicted in Figure 5-4 has a set of threats. Table 5-1 shows the threats affecting each of these elements.

The following sub-sections analyze and identify these elements individually based on the attack target nodes and the STRIDE approach.

	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data Flows		X		X	X	
Data Stores		X		X	X	
Processes	X	X	X	X	X	X
Interactors	X		X			

Table 5-1: Threats affecting elements [219]

5.4.2.1 Analyzing data flows

This section will cover the analysis of threats identified in the data flows. There are four data flows identified in Figure 5-4, which can be broken down and analyzed into the following:

1. EU to web server (Informational Level): The data flows from end users to the web server are sensitive and confidential and might carry access credentials. This data might be sniffed (Information Disclosure) either before they leave the EU or while they travel over the Internet. In addition, the web server might be targeted by an attack that could result in a complete failure either to accept the data or to respond to the customers' requests (Denial of Service). Figure 5-5 presents the type of STRIDE threats category for this data flow level.

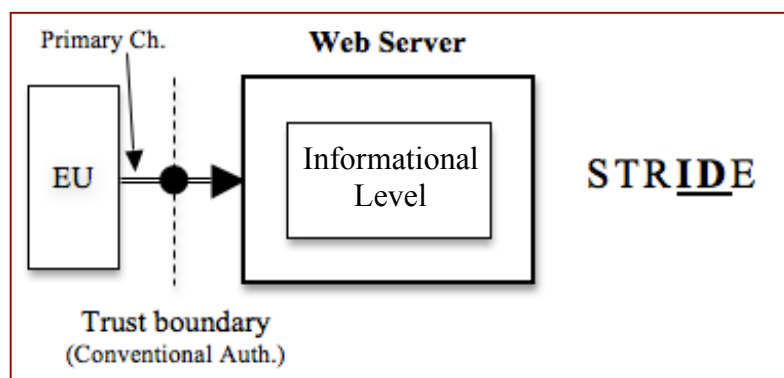


Figure 5-5: EU to web server (Informational Level) data flows threats

2. Web server to EU (via a secondary channel): The data flows from the web or Short Message Service Center (SMSC) server (in the case that SMS messages are used to serve as a secondary channel), which is responsible for delivering the verification codes to the customers via a secondary channel. This data can be captured at the user end or on the fly (section 0 covers how this could be done on mobile networks), and

thus, are vulnerable to information disclosure types of STRIDE threats. Although there is no single incident recorded yet on a targeted denial of service on mobile devices, there are commercial devices used to disable mobile devices by preventing them from receiving signals from the base station. These devices are called “mobile phone jammers” and are primarily found in places where mobile phones must be switched off. These jammers can also be used as targeted attacks on mobile phones near the attacker to block the signals and ensure that the victim’s mobile coverage is lost (Denial of Service).

3. EU to web server (Transactional Level): The data flows from end users to the web server at the transactional level are susceptible to similar threats as those discussed for data flows from EUs to web servers at the informational level.
4. Web server to the database: This data flow is out of the scope of this research since it does not relate to the end user or the multi-channel authentication mechanism.

5.4.2.2 Analyzing data stores

The application model shows only one data store represented by a database component. This data store is vulnerable to tampering, especially if the attacker is among the bank employees who have legitimate access credentials to access the database. Information disclosure is another major threat since customers’ records in banking systems might contain very sensitive information such as credit card numbers, account details, and online banking access details.

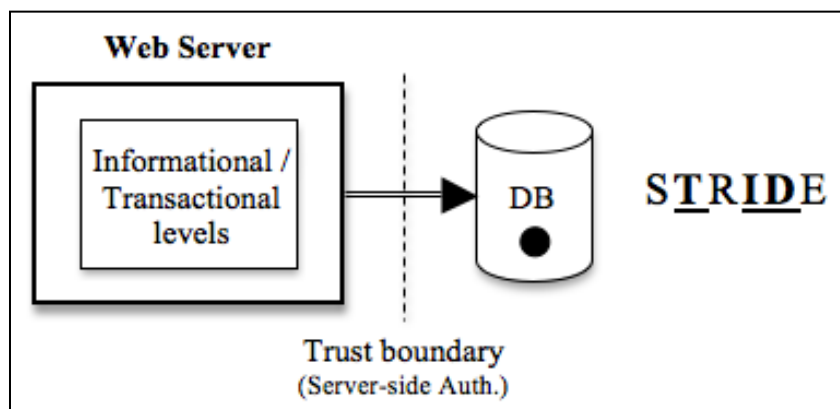


Figure 5-6: Data store (database) STRIDE threats

Databases are also prone to denial of service attacks. This could happen intentionally, caused by an attacker (whether an outsider or insider) or unintentionally due to a simple database error or a technical problem such as a full database drive. These kinds of issues might corrupt the database files and cause the database services to stop functioning or to go

down, hence causing a total failure in responding to queries. Figure 5-6 identifies the STRIDE threats applicable to the data store.

5.4.2.3 Analyzing processes

Processes are the only element susceptible to all STRIDE threats. A process that pretends to be the web server (Spoofing) has the ability to collect all the data that are submitted by the deceived customers. This also leads to information disclosure since these data could be sensitive and must only be known to the legitimate user. Furthermore, denial of service is another applicable threat here since the actual process is not accessible to the deceived customers.

Elevation of privilege occurs when an attacker is able to tamper with the customer records or get physical access to the secondary channel. For example, an attack from an insider (employee) could modify the customer's mobile number registered in the bank database with his/her own number. This allows the attacker to receive verification codes (OTPs) that are meant to be sent to the account holder's mobile phone. If this occurs, the attacker will be able to carry out transactions on behalf of the legitimate customer.

If there is no logging mechanism applied within the system or if an attacker were able to access the logs database, he/she could tamper with the data stored and modify the records. These records usually contain valuable tracing details such as the destination bank account number of the transaction the attacker accomplishes on behalf of the account holder. Thus, access to the database would allow the attacker to wipe out the evidences of such action (Repudiation Threat).

5.4.2.4 Analyzing interactors

Interactors are the end points of the system, such as EUs and OSPs. According to [219], interactors “are the data providers and consumers that are outside the scope of your system, but clearly related to it.”

From the OSP side, the web server does not know who is connected to the customer's account when a session starts. If the user is able to provide valid access credentials, then the web server assumes it is a legitimate user. However, if an attacker, at some point in time, were able to capture these credentials, then it could be the attacker who is connected to the web server (Spoofing), not the customer. The same threat types apply to the web server (OSP side). Sections 2.4.3.5 to 2.4.3.7 covered different attack techniques used to

deceive customers to provide access credentials to a fake website different from the original one hosted by the bank's web server.

Repudiation is another attack threat that occurs at times when an attacker is able to login to a customer account and request transactions on the customer's behalf using a proxy server that is untraceable.

5.4.3 Build an Attack Tree

An attack tree is a formal and methodical way of collecting, documenting, and describing potential attacks on any given system in a structured and hierarchical manner [59, 227]. It contains a root node that represents the optimum goal of the attacker. It also contains leaf nodes, which are the attack methodologies used to achieve this goal. Figure 5-7 represents an attack tree for the proposed online banking application with MCA approach. The figure illustrates how an attacker could compromise a user online bank account and identifies the path the attacker would follow in order to accomplish this task. The main entries to achieve a successful attack are the EU, the CC, and the OSP.

5.4.4 Evaluation of Threats

Evaluating identified threats is the fifth step in the threat modelling process and it is about investigating each threat/attack and exploring how the new technology can mitigate its risk. A scenario-based evaluation is considered in the following sub-sections for this purpose where each applicable attack is evaluated individually. A user named "Ahmed" (the EU) who has a bank account with XYZ Bank (the OSP) will be used hereafter as an example case scenario for all the attacks. Another Internet user called "Zaid" will be considered as an attacker who will try all applicable attacks to compromise Ahmed's online banking account. The evaluation assumes that XYZ Bank is implementing MCA as proposed in this research and will, therefore, show how it can mitigate the risk of the identified attacks.

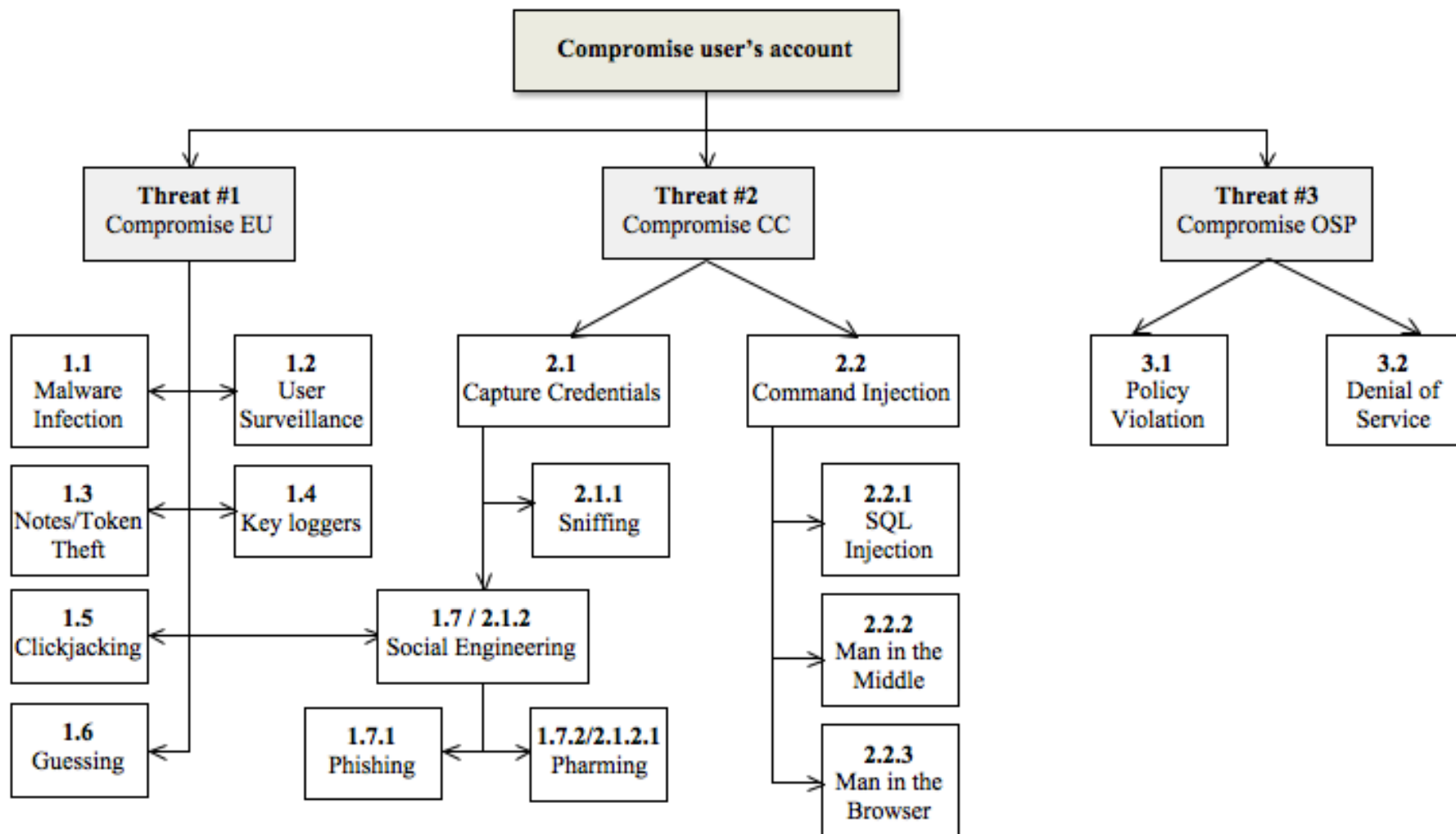


Figure 5-7: An attack tree for the proposed online banking with MCA approach

5.4.4.1 Sniffing (2.1.1)

Sniffing, the attack represented by 2.1.1 in Figure 5-7, is an attack that captures information transferred between EUs and OSPs. If Zaid has the proper tools that allow him to intercept Ahmed's data transferred over the Web channel (the primary CC), he could extract Ahmed's credentials (e.g., username and password) if this channel is not encrypted using SSL. If for some reason encryption were not implemented, MCA would protect Ahmed's account by disallowing Zaid from initiating critical transactions such as money transfer. The only access Zaid will gain after he captures Ahmed's username and password is the informational services offered by Ahmed's bank, such as the account balance statement. The only transactional service allowed, at this point, for Zaid is money transfer to the beneficiary accounts that have been already approved by Ahmed. However, to mitigate this threat, the approved beneficiary accounts can be hidden so that only Ahmed can reach them using a search engine. This search engine allows Ahmed to locate an approved beneficiary account by searching for the nickname he set for that account, the beneficiary account, holder name, the beneficiary account number, or any other details associated with any of the approved beneficiary accounts. Zaid, on the other hand, will not be able to see any beneficiary account unless he is able to figure out a searchable piece of information that could retrieve the beneficiary account details. Even if this occurred, and Zaid were able to transfer money to an approved beneficiary account, the money could easily be traced since the beneficiary account is always an account Ahmed has previously approved and used.

Moreover, with the confirmatory feedback feature implemented, Ahmed will receive an SMS message from the OSP informing him of the transaction. This will allow him to report such an incident quickly to the designated authority, especially if the amount is very high and the delay transfer feature is turned on. After all, capturing primary channel access credentials does not allow Zaid, even in the best scenarios, to create beneficiary accounts or transfer money from Ahmed's online account to his account. The only way Zaid can transfer money to his own account is if his account were approved by Ahmed as a beneficiary account. This again would be easy to trace from the transactions log.

Zaid will not be able to create new beneficiary accounts since this task requires a confirmation of the OTP that will be sent to Ahmed's phone over a mobile network.

5.4.4.2 Man-in-the-middle (2.2.2) attacks of MCA

MITM, indicated by the box 2.2.2 in Figure 5-7, attacks are real-time sniffing attacks. This type of attack is capable of altering the intercepted data between the EU and the OSP. The attack is transparent and neither end (EU or OSP) is aware of the attack. As a result, both ends assume data integrity. However, with the MCA mechanism implemented within the system, the potential damage of such an attack becomes very low.

For example, if Zaid is able to compromise the CC and divert all communication traffic from both communicating sides (Ahmed and the XYZ Bank), he is only sniffing the traffic without interfering (passive mode). He watches the details Ahmed is requesting from his online account. Once Ahmed sends a request to add a new beneficiary account, Zaid will then intercept the request and change the beneficiary account details so it will reflect his own account number rather than the beneficiary's account number. The bank will receive the request and will process it accordingly. As proposed by the MCA infrastructure, the beneficiary accounts must be approved by an OTP, which is passed to the user via an independent secondary channel other than the Web (e.g., mobile network). This means that Ahmed will receive a SMS message from XYZ Bank with the beneficiary account details and an OTP that will allow him to approve the beneficiary account. Here Ahmed will realize that the beneficiary account details received via the SMS message do not match the one he requested via the Web channel. He should not approve the transaction but should rather report this incident to the bank support for further investigation. As a result, the attack fails.

5.4.4.3 User surveillance (1.2)

User surveillance aims at capturing user credentials by monitoring the users through surveillance devices such as cameras. The main objective of such attacks is to replay the captured secrets later. With the MCA mechanism implemented, even if the surveillance devices were able to capture the OTP received by Ahmed's mobile phone, that OTP is only valid for one time. Once Ahmed uses the received OTP to approve the designated beneficiary account, the same OTP cannot be reused again to approve another beneficiary account. Moreover, each OTP is linked with one and only one beneficiary account. Thus any given OTP will not activate/approve any beneficiary account other than the one associated with it.

5.4.4.4 Notes/token theft (1.3)

Token or note theft, in the context of MCA, exists when the password is written down or when Zaid physically gets hold of Ahmed's mobile (i.e., the mobile phone in this case acts as an authentication token since it receives the OTP). The former, if it occurs, would help Zaid to gain access to the informational services of Ahmed's account. He would have limited access privileges similar to the ones covered in sniffing attack section 5.4.4.1. The latter should grant Zaid even fewer privileges although getting physical access to Ahmed's mobile allows Zaid access to the stored SMS messages. Despite the fact that these messages could contain confidential information such as OTPs used to activate beneficiary accounts, this information is considered out-dated as long as Ahmed has already used it. Even if Ahmed has not used some of them at the time Zaid is able to compromise them, they are still associated with only the beneficiary accounts Ahmed has created.

By physically getting control over the secondary channel, Zaid would have no access to Ahmed's online bank system. This attack would only deny Ahmed from accessing his services temporarily. Therefore, token and note thefts are applicable attacks on MCA but they cannot offer Zaid full access to compromise Ahmed's online account.

5.4.4.5 Malware infection (1.1)

Malware infection attacks using viruses, Trojans, or any other malicious software are capable of capturing access credentials and pass them to the attacker. Sometimes they are able to modify the transaction details the user is passing to the OSP. Considering MCA, in the former case, the attack outcome is similar to the user surveillance and notes theft attacks discussed in the previous sections. They will fail as the OTP protects users from any type of replay attacks. The second case is addressed with more details in section 5.4.4.8.

MCA also has the potential to protect end users from technical and non-technical social engineering attacks. For example, Ahmed receives a call from Zaid who is pretending to be one of the IT technicians that received a report about an issue with Ahmed's account. Even if Zaid were able to deceive Ahmed and able to obtain the login password of the account, Ahmed would receive a SMS message whenever Zaid tries to create a beneficiary account (i.e., the proposal suggests that a beneficiary account must be created for any account to which the user needs to transfer money). If Zaid's account were among the beneficiary accounts that have been approved earlier by Ahmed, a confirmatory SMS message

(feedback) would be sent to Ahmed's mobile phone to confirm the transaction. This would help Ahmed to report the incident and trace the issue before the money is transferred away (if delayed transfer feature is implemented as discussed in section 5.2.4).

5.4.4.6 Phishing (1.7.1) and Pharming (1.7.2 / 2.1.2.1)

Phishing and Pharming are considered as technical social engineering types of attacks. Unlike non-technical social engineering, the attacker approaches online banking customers by means of electronic mails, websites, or DNS spoofing (see section 2.4.3.6 for more details). For example, Ahmed receives an e-mail from Zaid that apparently contains a link to XYZ Bank. The URL behind that link would take Ahmed to a fake website that is designed to match the look and feel of the original XYZ Bank. If Ahmed logs into that website, his access credentials would be stored and captured by Zaid. However, those login details would not help Zaid to request a money transfer from Ahmed's account. He first needs to create a new beneficiary account for his own account and approve it before he is able to transfer money to it.

5.4.4.7 Clickjacking (1.5)

Clickjacking has an effect similar to the effects of malware infection attacks. It installs malicious software in the victim's machine so the attacker can control it remotely.

As an example in the case of online banking with MCA, if Ahmed clicks on a button on a website that results in installing a virus or Trojan in his machine, all access credentials can be captured and controlled by Zaid. However, Zaid also needs to control Ahmed's mobile phone in order to accept and manipulate the OTP numbers sent by the OSP whenever there is a new request to create beneficiary accounts.

5.4.4.8 Man-in-the-browser (2.2.3) attacks

Man-in-the-browser (MITB) attacks are similar to the MITM attacks. The difference is that with MITB, the controlling element that intercepts the data and alters its details is a computer program residing in the victim's machine. If such a program were able to control Ahmed's web browser, it could create beneficiary accounts or alter existing beneficiary account details requested by Ahmed in the background, before these requests are sent to the OSP. However, as covered in section 5.4.4.2, Ahmed would know if his request has been altered once he receives the SMS message that contains the transaction details and the

OTP. If the details do not match, then Ahmed would know that his original request was altered.

5.4.5 Risk Mitigation and Security Controls

According to [220], four security controls can be adequately used to mitigate the risks presented by threats identified in any threat modelling. These security controls are corrective control, deterrent control, detective control, and finally, preventive control. Figure 5-8 illustrates how these controls are put in place based on the security controls structure presented in [220].

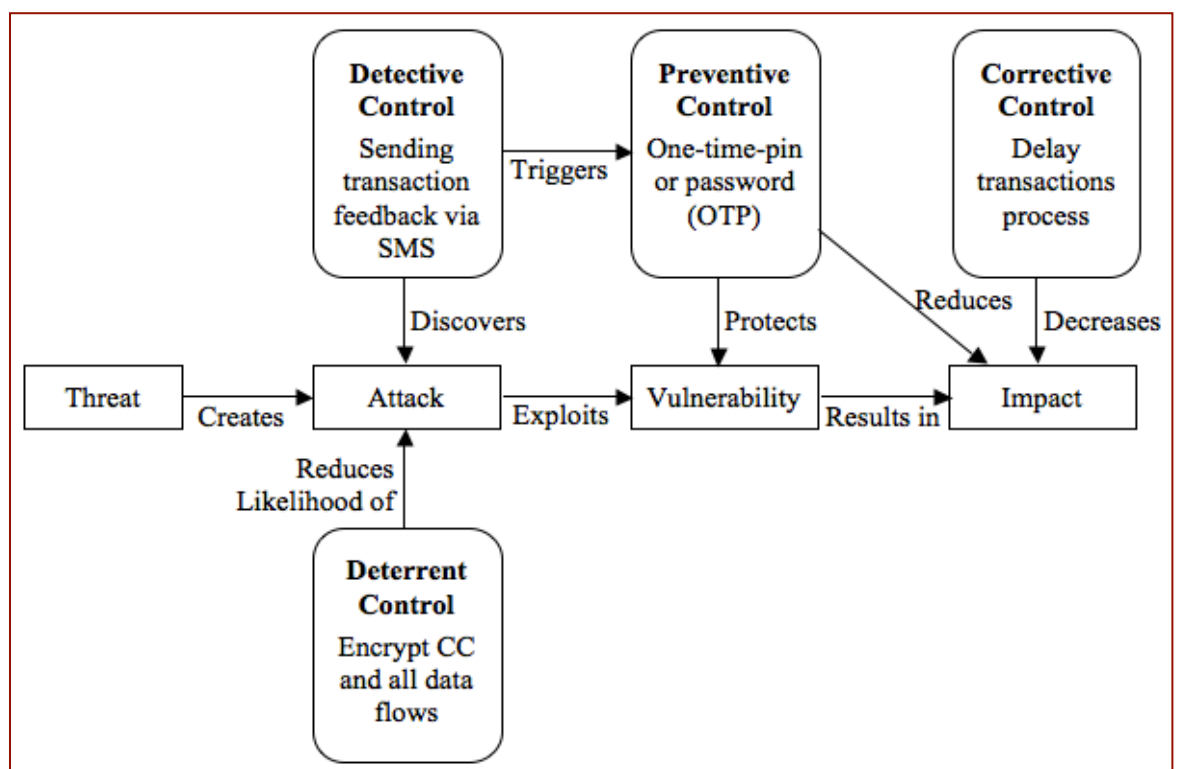


Figure 5-8: Security controls implemented for the MCA infrastructure (adapted from [220])

These security controls are expanded further in Table 5-4, which summarizes the outcome of the threat modelling analysis based on the STRIDE process.

5.4.6 Rate the Threats (based on DREAD)

The final step in the threat modelling is to prioritize the identified threats based on the risks they pose. The risk rate is calculated based on what is called “DREAD model” suggested by Microsoft. It stands for the following parameters [227]:

- *Damage potential*: the damage effect that can be caused by the vulnerability if exploited.
- *Reproducibility*: the easiness of reproducing the attack.
- *Exploitability*: the easiness of launching the attack.
- *Affected users*: the scope of affected users by the attack.
- *Discoverability*: the easiness of discovering the vulnerability.

The scale used to rate the risk of the threats is represented by the values 3 (High), 2 (Medium), and 1 (Low). Table 5-2 shows a suggested interpretation of this scale on DREAD model.

	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

Table 5-2: Threat rating table [227]

To calculate the risk rate (high, medium, or low) for any given threat identified in this study, we need to count the risk value of each DREAD attributes based on the risk each threat poses to the online banking application with MCA. Then the total value of these ratings will indicate the proper risk rating each threat has. Microsoft suggested that a total rating from 12 to 15 should be considered (High risk), a rating from 8 to 11 is considered (Medium risk), and finally from 5 to 7 is considered as (Low risk) where 5 is the minimum

score any threat could get due to the fact that there are 5 parameters exist for each threat (each will get at least a score of 1).

Table 5-3 represents the outcome of the DREAD and risk rating calculations for each attack on the proposed MCA separately.

Attacks	D	R	E	A	D	Total	Risk Rating
Malware infection (1.1)	2	3	1	1	2	9	Medium
User surveillance (1.2)	2	1	2	1	1	7	Low
Notes theft (1.3)	2	3	3	1	1	10	Medium
Tokens theft (1.3)	1	1	3	1	1	7	Low
Key loggers (1.4)	2	2	2	1	3	10	Medium
Clickjacking (1.5)	2	1	1	3	3	10	Medium
Guessing (1.6)	2	1	1	1	1	6	Low
Social engineering (non-technical) (1.7)	2	1	3	1	1	8	Medium
Phishing (1.7.1)	2	1	2	2	2	9	Medium
Pharming (1.7.2)	2	2	1	1	2	8	Medium
Pharming (2.1.2.1)	2	2	1	3	2	10	Medium
Sniffing (2.1.1)	2	2	1	1	2	8	Medium
SQL Injection (2.2.1)	2	2	1	3	2	10	Medium
MITM (2.2.2)	2	2	2	1	1	8	Medium
MITB (2.2.3)	2	3	1	1	2	9	Medium
Policy Violation (3.1)	3	2	2	3	2	12	High
DoS (3.2)	3	1	1	3	1	9	Medium

Table 5-3: DREAD-rating table

5.5 Chapter Summary

This chapter proposed a MCA solution that is capable of better withstanding most known attacks that target online banking applications than are other existing authentication mechanisms. Based on a theoretical evaluation, while the main aim of this solution is to offer better security, it was also important to ensure usability and acceptability.

To assess the security of the MCA theoretically, this chapter reported on a threat modelling evaluation of the MCA based on the STRIDE process and DREAD rating by Microsoft. The outcome of the evaluation has proven that no single point of attack in the MCA solution poses high risk or allows the attacker to compromise the customers' online banking accounts. The usability and acceptability of MCA, however, can only be assessed practically. Chapter 6 covers the design and implementation of the proposed MCA mechanism. This allows better evaluation of both usability and acceptability from the users' point of view.

	STRIDE Classification	Entry Points	Impact	DREAD Risk Rating	Security Controls
User surveillance (1.2)	• Information disclosure	EU	1. Disclose confidential access/financial info. 2. Transfer money to approved beneficiary accounts	Low	• Encrypting EU to OSP data flow • Hide beneficiary accounts by allowing access to them via a search engine
Sniffing (2.1.1)		CC		Medium	
Man-in-the-middle (2.2.2) and Man-in-the-browser (2.2.3)	• Spoofing • Tampering • Repudiation • Info. disclosure • Denial of service • Elevation of privilege	CC	3. Altering transaction details sent by the customer 4. Transfer money to approved beneficiary accounts 5. Modify transaction details originated from both sides (EU and OSP)	Medium	• OTP must be valid for one use only • Every OTP must be associated with only one beneficiary account
Notes theft (1.3)	• Info. disclosure	EU	6. Disclose confidential access/financial info.	Low	• Provide alternative secondary channel at emergencies
Token theft (1.3)	• Denial of service		7. Deny customer access to mobile service	Medium	
Malware infection (1.1) and Clickjacking (1.5)	• Tampering • Information disclosure • Repudiation	EU	8. Disclose confidential access/financial information 9. Modify transaction details originated from both sides (EU and OSP)	Medium	• Implement feedback through the secondary channel for every transaction
Social engineering (non-technical) (1.7)	• Spoofing • Information disclosure	EU	10. Disclose confidential financial info. including the OTP sent to the customer 11. Create beneficiary accounts and initiate money transfer to them	Medium	• Send beneficiary account details along with the OTP via the secondary channel • Delay process of critical transactions for few minutes to allow customers to report attack attempts on their accounts
Phishing (1.7.1)	• Spoofing	EU	12. Disclose confidential financial info.	Medium	
Pharming (1.7.1 / 2.1.2.1)	• Info. disclosure • Denial of service	EU/CC	13. Deny customer access to the legitimate OSP	Medium	

Table 5-4: Threat modelling based on STRIDE process and DREAD rating summary table

Chapter 6

Design and Implementation

6.1 Introduction

The main objective of the proposed MCA solution is to provide an online banking solution that offers better *security* for the customers and, at the same time, is *usable* and *acceptable*. These three variables (*security*, *usability*, and *acceptability*) need to be evaluated against the proposed MCA solution in order to check that it meets all proposed requirements. Security was evaluated theoretically using threat-modelling evaluation (covered in Chapter 5). Usability and acceptability, on the other hand, can be assessed only in practical terms where users are consulted to give their feedback based on their experience with the proposed solution.

In order to evaluate the usability and the acceptability of MCA, a prototype application that simulates an existing online banking system was developed. This prototype application was designed to meet the main requirements of the proposed MCA architecture.

This chapter first presents the main aspects of the MCA in section 6.2. The design recommendations of the proposed MCA solution constitute section 6.3. The design options and implementation are discussed in sections 6.4 and 6.5 respectively. This chapter concludes with a list of security and usability guidelines for real online banking application design and implementation.

6.2 Aspects of the MCA

The proposed MCA infrastructure, as proposed in Chapter 5 and shown in Figure 5-1, has the following aspects: *levels*, *factors*, and *channels*. These are the main aspects of any MCA design option. The requirements of any given system will specify *how*, *what*, *when*, and *where* to implement these elements.

This section discusses these aspects and shows why they are important characteristics of the proposed MCA mechanism. The section also presents a guideline for the implementations of these elements.

6.2.1 Levels

Levels describe what service level a customer would have in an online banking system. This can be achieved by dividing the system core services or functions into different levels. Each level can be assigned to a specific group of users (see Figure 6-1). More privileges are granted to the users when moving to a higher level. For instance, level 1 in Figure 6-1 offers limited services (i.e. informational services) to user group 1 while level 2 offers more services (i.e. transactional services) to user group 2.

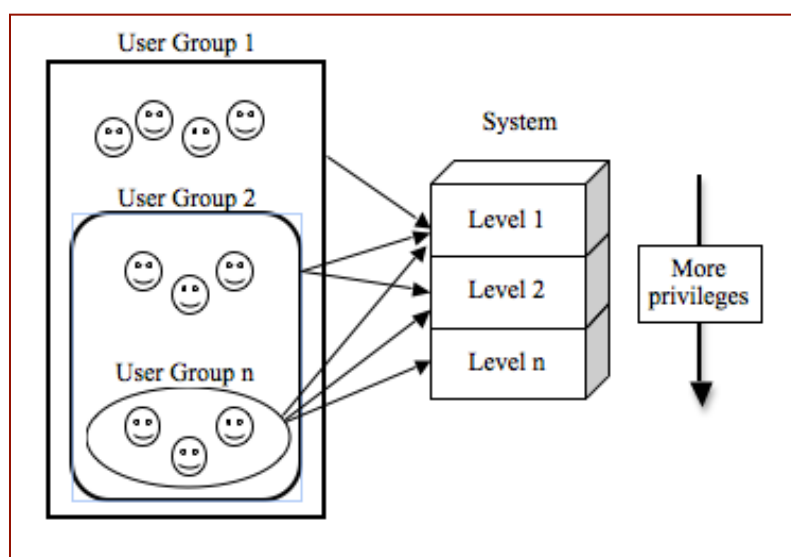


Figure 6-1: System levelling structure

Dividing an online banking system into multiple levels is a vital step towards securely and effectively managing services and functions for different groups of users using single application interface.

The MCA architecture suggests the following guidelines to implement levelling properly:

- Service level: the services offered to the users throughout the system must be represented in a cumulative way. A user authenticated to access higher-level services should be able to utilize the services offered by that level as well as the services offered by all preceding levels (see Figure 6-2).

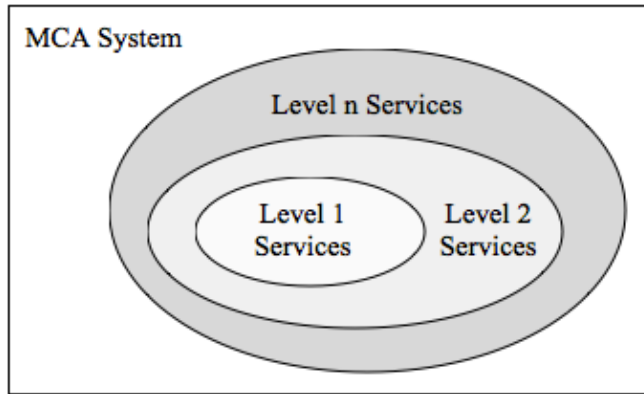


Figure 6-2: Services level diagram

- Session management: despite the fact that sessions must be managed and kept alive for the time the users are logged-in, these sessions must be terminated at once if there is a suspicion of an attack, such as the account being accessed by different IP addresses at the same time. Also, and most importantly, the session used to authenticate users on transactional levels must be valid for one-time use only. The user must authenticate each transaction individually (see Figure 6-3).

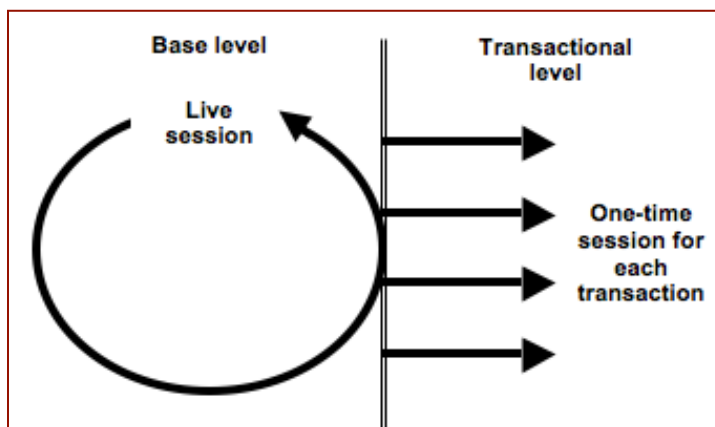


Figure 6-3: MCA architecture session management

- Sequential authentication: a user should not be granted a higher-level access unless he or she is already authenticated in all lower-levels. This is important to ensure that all channels are used to carry out a transaction.
- Single user interface: although the system will be divided into different levels, all these levels must be represented by a consistent user interface. This is important so that users do not feel they are being diverted to different systems or interfaces while moving from one level to another.

6.2.2 Factors

Factors complement the role of levels. They are the secret keys used by users to get access to their accounts or to authorize critical actions within the system. Sometimes the system administrator can assign different levels to one or more groups of users where these users can use different access keys (the factors) to access each level individually (see Figure 6-4). This is known as multi-level authentication [26] and is covered with more detail in Chapter 2.

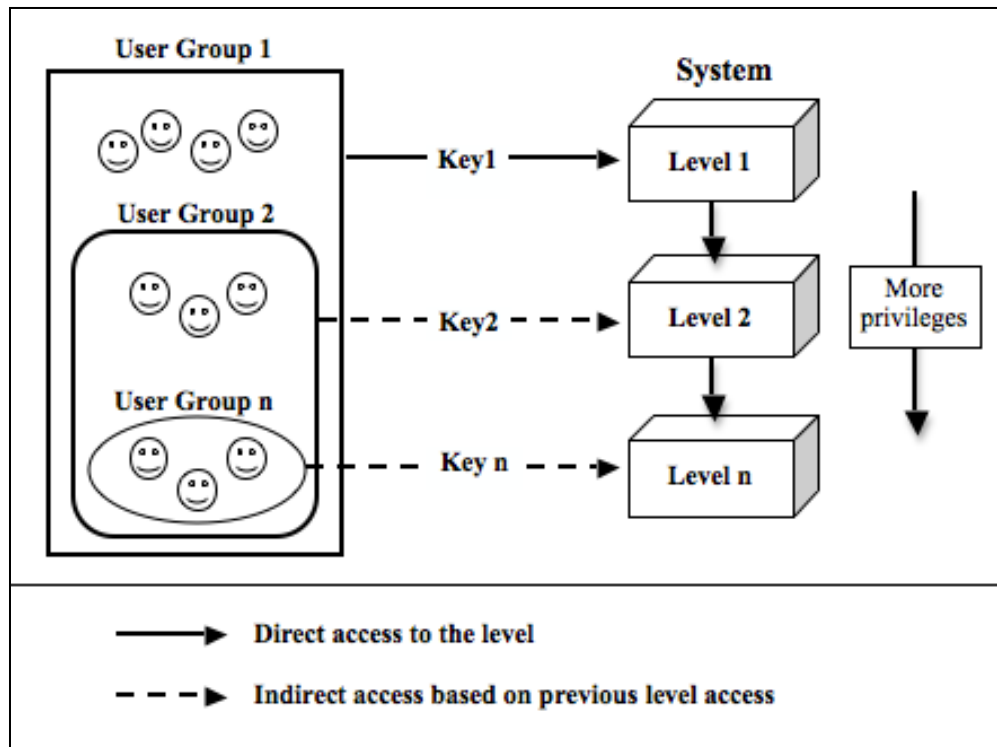


Figure 6-4: The implementation of factors into multi-level system

The MCA architecture suggests the following guidelines concerning factor implementation:

- Multi-factor: each user must use multiple factors in order to get access to services provided by different levels throughout the system. It is recommended that basic informational services are provided at the base level where users can access them using traditional authentication factors such as a username and password. This authentication mechanism can also be used in higher transactional levels but not as a primary mechanism. It can be used, rather, as a complementary authentication mechanism along with another authentication mechanism that is delivered over a different independent channel.

- One-time factors: the factors used to authenticate users to the transactional level of their account must be *single-use*, only valid for one use, *linked*, linked to one transaction only, and *time-limited*, valid for a specific period. These transactional-level factors must be delivered to the users via a different channel other than the primary Web channel used to authenticate these users at the Information Level of their accounts.

6.2.3 Channels

Channels are a vital component of MCA. While factors ensure proper management of user privileges, channels assert that these factors are exchanged between the system and the users in a proper and un-compromisable way. The proposed MCA architecture suggests the following guidelines with respect to channel implementation:

- Multi-channel: each level of the system must be authenticated using a different factor, as stated previously, and by means of different channels where possible. The minimum requirement is that at least two channels be used before the user is able to access any upper level transactions within the system.
- Independence: the channels must be independent. That is, factors and information exchanged via different channels must not be delivered using the same delivery path or medium. For example, if the factor used to authenticate users to the first level was exchanged between the system and the users through the Web channel, then the factor used to authenticate the users for the second level must not be delivered using the Web channel. The second factor must be delivered over a different independent channel such as mobile network.

The proposed MCA solution suggests that SMS messages are used as a communication medium to exchange the secondary channel factors with the user. However, other communication media can be used as long as they are independent of the primary channel used to authenticate users to their accounts.

To summarize, Figure 6-5 encompasses all three aspects of MCA in one architecture diagram.

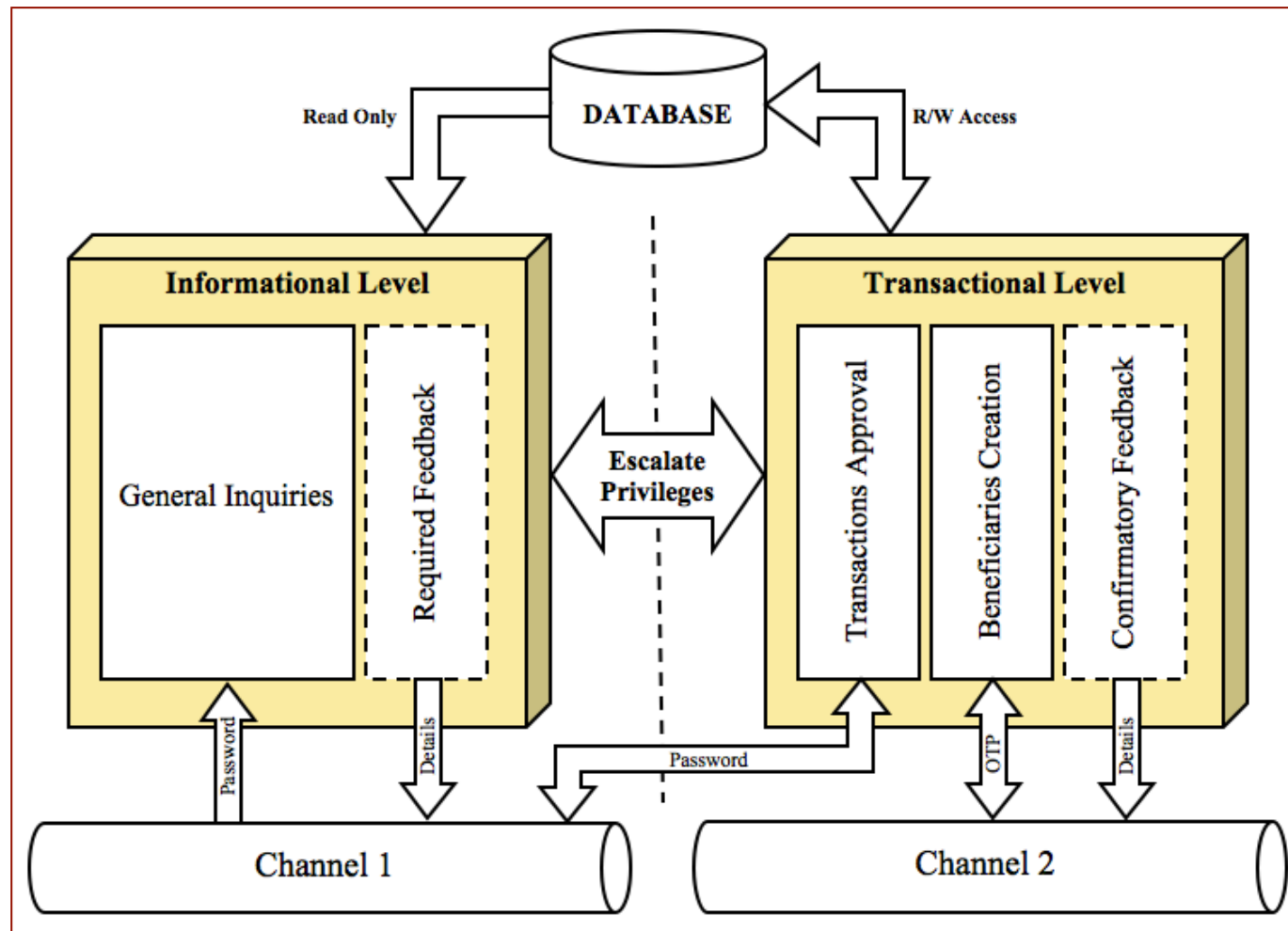


Figure 6-5: MCA architecture diagram

6.3 Design Recommendations

6.3.1 User Defined versus System Generated Passwords

The passwords used to authenticate users to the base/primary level should be user-defined passwords. Simple password policies that ensure a balance of security and usability should be enforced rather than complex policies. This is important to minimize the user passwords being written down on notes or papers. These passwords, on their own, do not pose high risk since they alone cannot grant an attacker access to the transactional level of the user account. The users will need to use other authentication factors to access the transactional levels as pointed out in section 6.2.2.

6.3.2 Language Support

Language differences are an important aspect of cultural background. It is a neglected security feature in almost all online applications that, if utilized, can improve security. The alphabet used to form a password can be treated as a knowledge-based authentication factor. In fact, it is the hardest type of knowledge-based authentication since it requires compatible peripheral devices beside knowledge to extract and understand. For instance, a user from Oman who speaks Arabic can choose to receive the OTP in Arabic alphabets. This will limit the chances of a foreign attacker who does not understand or read Arabic alphabets to extract the OTP from the SMS message if he or she were able to physically compromise the user's mobile phone or capture the message on the fly. Even in the case where the attacker uses a translator to translate the text message to English or a language he or she understands, an input device (e.g. keyboard) has to be available so the attacker would be able to send the OTP in the correct language alphabet to the bank system. It would be even harder for the attacker to extract the OTP if an automated call was initiated from the bank servers to dictate the OTP to the user rather than sending the OTP in an SMS message.

The language support can also be used for the conventional username and password. The user should be allowed to enter the password in his or her language or using in different language alphabets. The system should implement a feature that would allow the application to detect the language used in the password and compare it with the one stored in the user account record in the database. This would make it harder for the attacker to

recognize what languages the user has used since there is no form field submitted along with the password that will tell the attacker which language the user has used in the password.

6.3.3 Encryption / Securing Key Delivery

The factors travelling between users and the system should be encrypted using the latest, up-to-date, cryptography formulas. This is vital to ensure that data are delivered securely without interference or interception. Although not all channels are considered secure, such as SMS messages, they significantly improve the overall security of the system when used as an auxiliary delivery channel alongside the Web channel.

6.4 MCA - Design Options

MCA is a flexible authentication mechanism that caters to different organizations' and clients' needs. This section will cover the design options of MCA based on the three aspects (levels, factors, and channels) discussed in the previous section. The details of each of these designs, the advantages and disadvantages, and the criteria for selecting the best design for online banking are presented next.

6.4.1 Design option 1 – Transaction-based Authentication

This design suggests that the customer must always be authenticated using the MCA mechanism to access each successive level of the system. For instance, a user is required to enter the username and password to access his or her account. If both username and password matches the user record in the database, the system would prepare an OTP and deliver it to the user via a secondary channel such as a mobile network. Once the user successfully verifies the transaction by entering the OTP via the bank server, the system would then open a new session for him or her to access the first level services. This session would be responsible to keep the user authenticated for the first level of services as long as the user does not logout or keep the application idle for a specific length of time. These level services are only informational where the customer has only read-access to the records stored under his or her account.

For transactional level services, the user must authenticate each transaction individually. A new session would be created for each transaction after the application verifies the OTP submitted by the user. This session would be live until the transaction is carried out and then it would be terminated and would no longer be valid for another transaction. Here the user does not have to logout to terminate the session; the session is valid only for one transaction. For example, if the user would like to transfer an amount of money to another account, the bank will send a new OTP to the user's mobile number. Once he or she verifies this OTP, the transaction will be carried out and no further transactions can be carried out without a new OTP (see Figure 6-6).

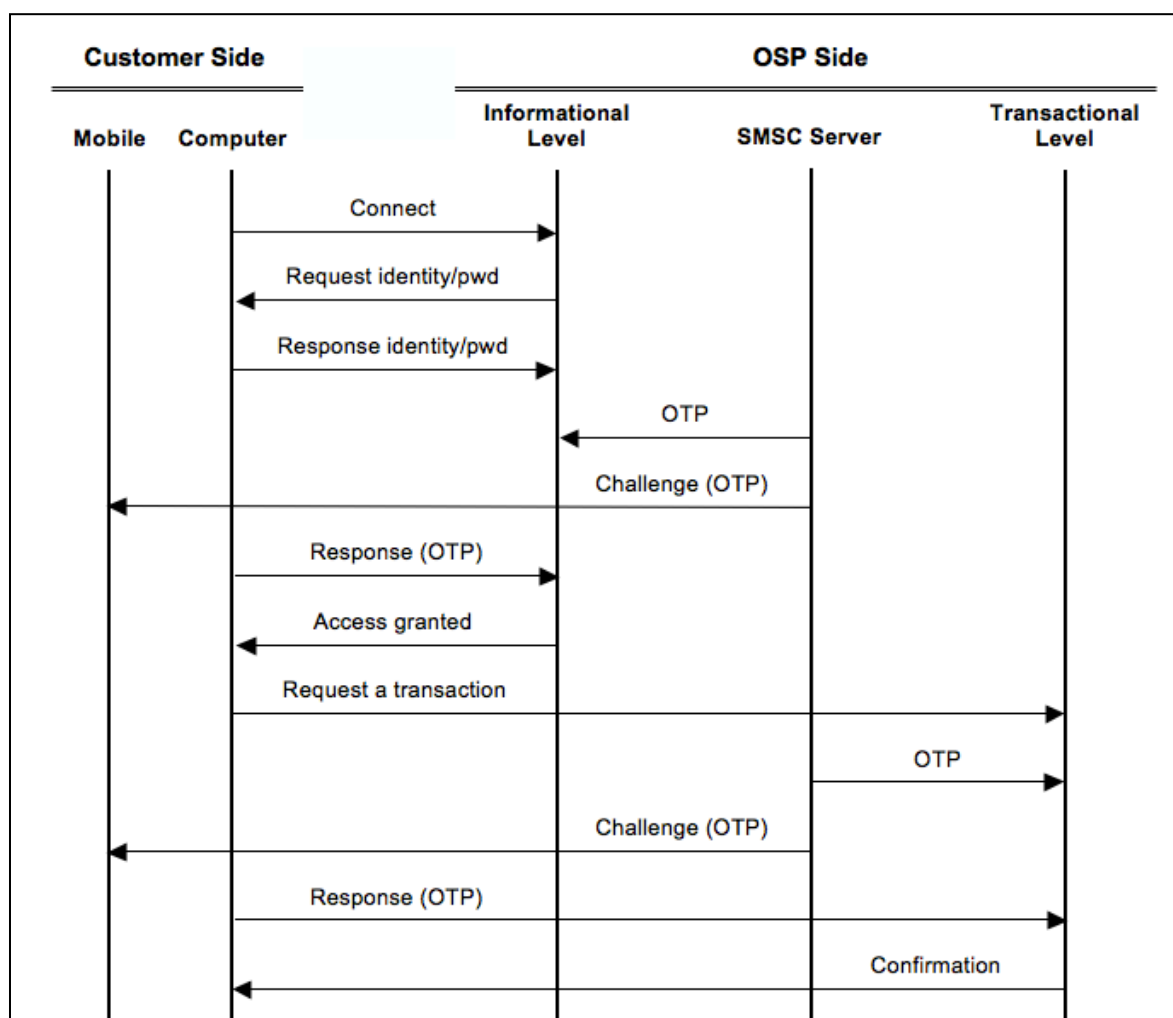


Figure 6-6: Design option 1 – Transaction-based authentication process

Although this design offers the highest possible MCA security, it uses the secondary channel authentication mechanism exhaustively. This will increase the running cost of the MCA mechanism for the user since each transaction must be validated by an OTP that is delivered to the customer via an independent channel. It will also degrade the overall usability and accessibility of the system. The users are required to access the other channel

each time they want to access their accounts. If the other channel is unavailable, it will cause disruption and latency in accessing online services.

6.4.2 Design option 2 – Beneficiary-based Authentication

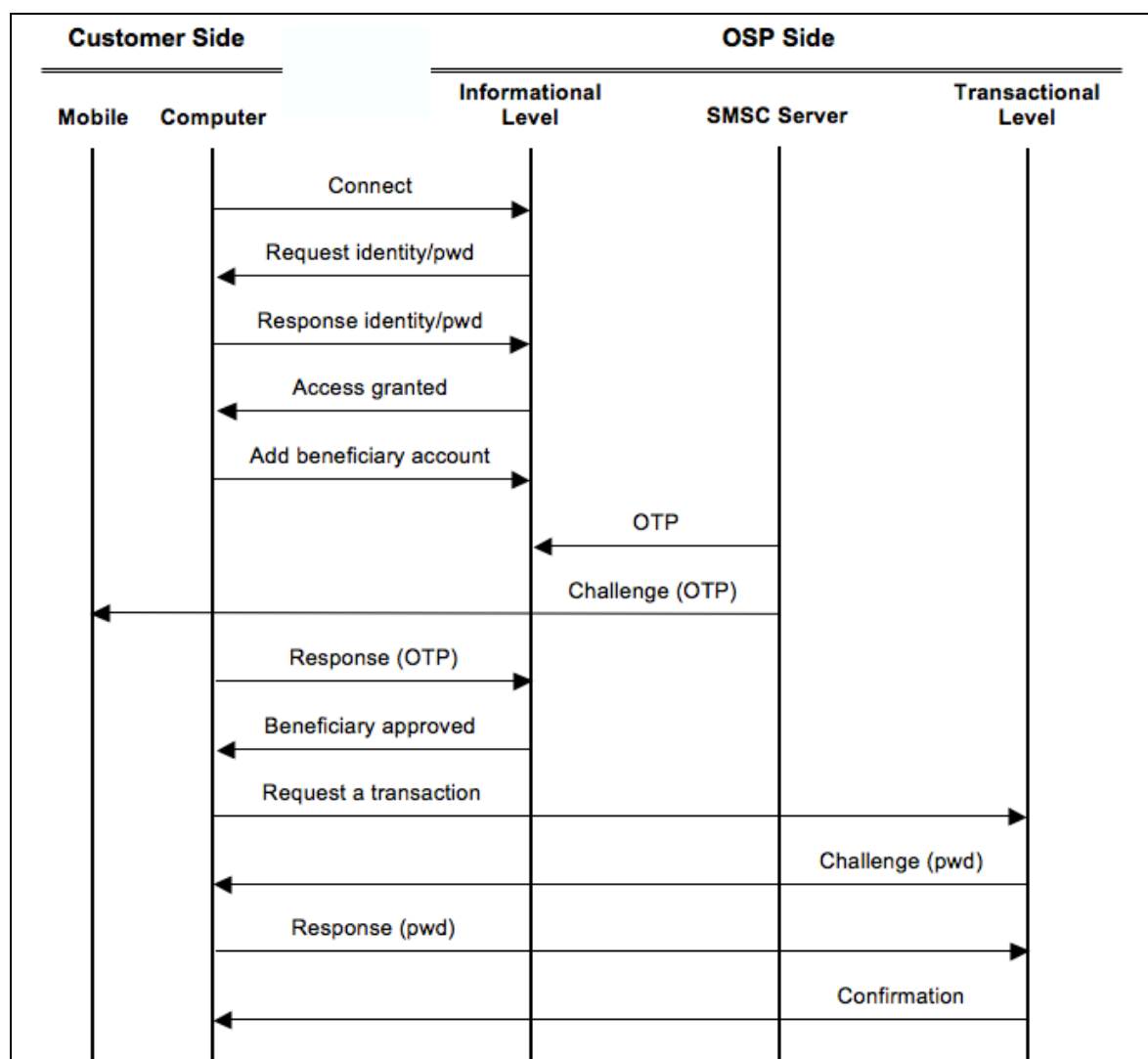


Figure 6-7: Design option 2 - Beneficiary-based authentication process

This granularity option aims at minimizing the use of the secondary channel while maintaining security. It suggests that customers should have access to the informational level using only the conventional one factor authentication mechanism such as username and password. The same authentication mechanism should also be used to authorize transactions at higher levels. However, these transactions are only allowed for the beneficiary accounts pre-approved. These beneficiary accounts can be manipulated at the informational level but they are only approved by OTPs that are delivered through the secondary channels. Thus, secondary channels are used only to approve beneficiary

accounts once and customers are not required to utilize the secondary channel every time they want to authorize a transaction.

This design offers better usability and is more cost effective than design option 1. Security is maintained since the attacker will not be able to create beneficiary accounts without compromising the secondary channel. For transactions to be carried out, the attacker also needs to compromise the conventional access credentials since they are requested by the system as depicted in Figure 6-7.

6.5 MCA Implementation – XYZ Bank

The implementation of the MCA proposal is an important part of this study. It was stated that the aim of this research is to “*design an authentication mechanism that uses multiple channels to resist attacks more effectively than most commonly used mechanisms. Furthermore, such a mechanism will also be usable and acceptable to users*”. One can only test the usability and acceptability by involving end users in the evaluation process. Such evaluation goes beyond the technical evaluation of utility and can provide accessibility in-context [228].

To facilitate the evaluation, a prototype online banking web-application was implemented. The application features an MCA mechanism that complies with design option 2 described in section 6.4.2 since this design offers a moderate implementation of authentication via SMS. Figure 6-8 shows a storyboard for different pages designed to achieve proper implementation of the proposed MCA solution.

The storyboard illustrates how the application pages are connected to each other. It also reflects the sequence in which these pages are to be accessed. For instance, the user cannot access page 1.1.4 (secondary channel selection) before first completing page 1.1.3 (mobile verification). A money transfer request (page 1.2.2.1) is a sub-page of the beneficiary accounts page (page 1.2.2), and therefore, the user will not be able to access this page unless the request to access it comes from the beneficiary accounts page. The same sequence is repeated for the rest of all other pages displayed in Figure 6-8.

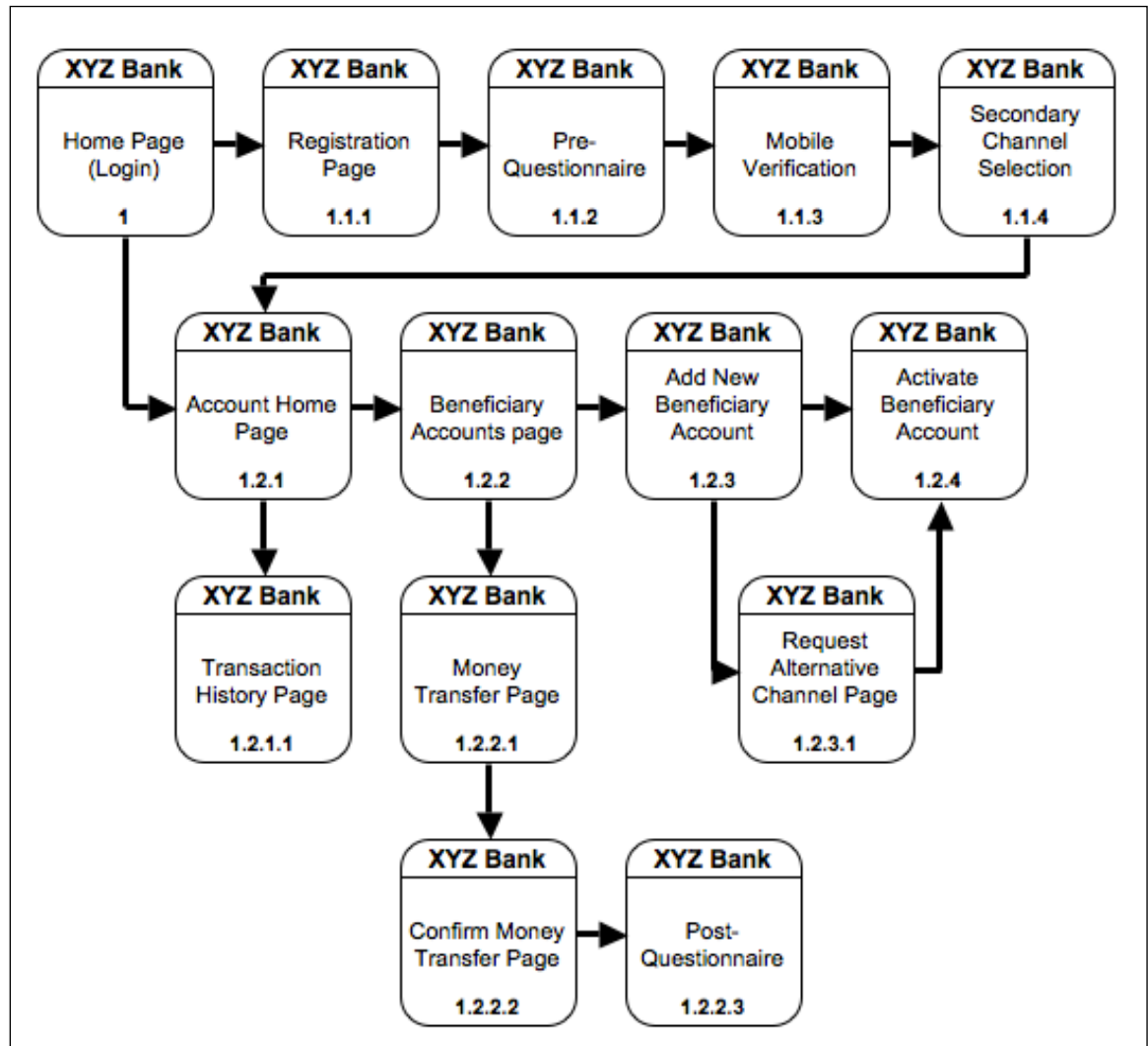


Figure 6-8: XYZ Bank prototype application storyboard

6.5.1 Application Overview

The prototype application has been put into five separate tiers as depicted in Figure 6-9: PHP files tier, Presentation logic tier, Business logic tier, Configuration tier, and the Data stores tier.

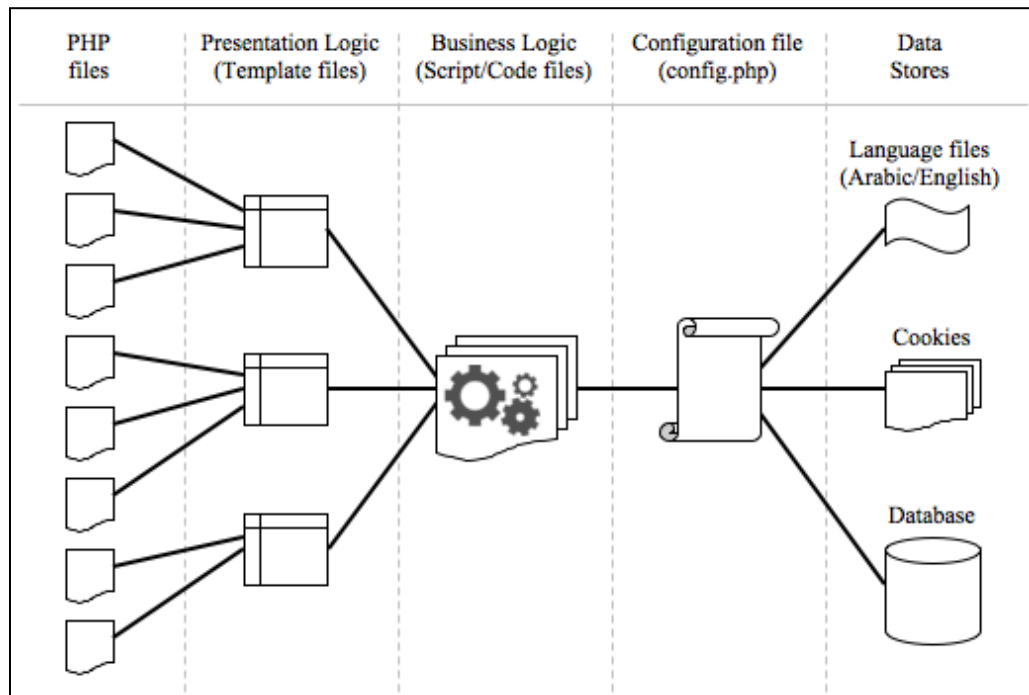


Figure 6-9: The prototype application architecture

Each of these five tiers plays an important role in the application architecture. Their functions are described in the following bullets:

- **PHP files tier:** this tier contains all web-application files that are accessible directly by the users. They produce HTML documents that are formatted in a way that users can read and understand.
- **Presentation logic tier:** this tier is responsible for styling PHP files. They are usually made of templates that work as base format that will later shape the front-end style of the PHP files. The application uses templates to present the interface layout. These templates share almost the same layout with only differences in the codes and the links they display to the users. Figure 6-10 illustrates the common layout for all templates used in the MCA prototype application.

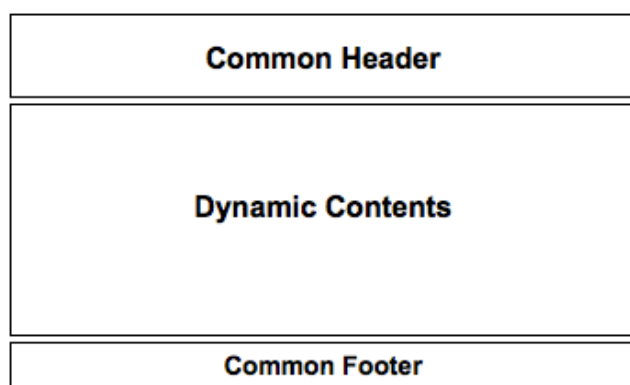


Figure 6-10: Common application templates layout

There are three main templates used in the application:

- *Guest template*: is a template responsible for pages that the users visit without the need to login. These pages include Home page, Research page, Contact researcher, Tasks page, Information sheet page, and Registration page.
- *Signed-in template*: is a template that presents all private pages that the user can access after he or she is signed in. These pages are restricted from other users who do not have accounts or records in the database.
- *Pop-up template*: this template is responsible for presenting the layout of the pop-up windows that appear throughout the application.
- **Business logic tier**: this is the tier where data are manipulated and processed. It acts as the brain of the application, which decides what output should be produced to the users. The outcomes of this tier move to the presentation tier for styling and formatting before they are finally displayed to the users through the PHP files.
- **Configuration tier**: is the tier that holds the configuration files. These files hold the key setting values that help the application to decide which language to use, which cookies are responsible for which elements, and which database to connect to and use. Configuration files also hold sensitive information such as database access credentials. For this reason, these files are the most critical files that should be kept secured from unauthorized access.
- **Data stores**: these are represented by the database, cookies, and language files. All these data stores are connected so that none of them can work independently. For instance, the language files contain Arabic and English phrases that are used throughout all templates and PHP pages. The cookies stored in the users' machines will have a value that will specify which language the user prefers to use. If the user has selected Arabic, then the cookie will store the value that represents the Arabic language in his machine. The Arabic language file will then be used to represent data in the templates and PHP files. Finally, the data sent back from the users will be stored in the database in the same language currently used (Arabic language in this case).

As shown in Figure 6-9, all five tiers are separated from each other. This is important to improve performance, to update easily and efficiently and to maintain the core functions without the need to compromise the other tiers [229].

Multi-Channel Authentication

Interface Language: English - العربية

This is an evaluation application and does not reflect real information of real customers!

[Home](#)
[About The Research](#)
[Contact Researcher](#)

Welcome to XYZ Bank


Please use the following login form to login to your e-banking account. If you are a first time user please [click here to register!](#)

Once you test the application, it is very important that you do the **Questionnaires**. (you will find the links once you register)

Username:

Password:

- [About The Research](#)
- [View tasks outline](#)
- [Read the Information Sheet](#)



Now feel secured while authorizing your payments with Multi-channel Authentication. You can use a combination of different channels to authorize payments! Read more in the next box.

Online Security!

- What is Multi-channel Authentication?
- How it could possibly protect me as an online banking customer?
- How does the system work?
- What options does it provide?

To learn more about this study and how it will protect the end-user from all known online fraud attacks, please [click here to read the research summary](#).

Please be aware that this is not a real Internet banking system and it does not represent any existing financial firm anywhere around the world. This application was designed solely for the purpose of evaluating the Multi-channel authentication approach and to test the change of customers level-of-acceptance and experience.

Copyrighted by Mohamed Al-Fairuz

Figure 6-11: MCA application - Home page (login) - Implementation

The main page of the application presented as Figure 6-11 gives a brief illustration of how these five tiers communicate with each other to present the pages to the users. This document uses the Guest template (*Presentation logic tier*) to present the header and footer. The login form is directly connected to the database (*Data stores tier*) for a quick check if the user has entered a valid username and password or not. The configuration file is the intermediary connector that makes such communication possible (*Configuration tier*). The cookies' default language value is English; therefore, the English language file will be used to display the contents of the page (*Data stores tier* again). Finally, the page is accessed directly by the user through the file `index.php` (*PHP files tier*) which is processed in the web-server and converted to an HTML document as seen in Figure 6-11.

6.6 Implementation Guidelines

For any online banking system to implement MCA, there are several guidelines that have to be taken into consideration. Some of these guidelines were already implemented in the prototype application and some others were not implemented (marked with [*]) as part of this research study. They are categorized into security and usability guidelines below.

6.6.1 Security guidelines:

- [*] Users should not be allowed to enrol into the system online. There must be a way to verify that the user registered to use the online service is legitimate and that he or she is the real owner of the mobile number provided.
- User correspondence details (e.g. mobile number, alternative mobile number) must not be displayed in the user online account and must be kept hidden from online access at all levels. Although there are on going studies proposing encrypted version of SMS messages such as the one proposed in [230], current SMS protocol and the encryption formula are publicly available for software developers. Therefore, if an attacker were able to capture the account holder's mobile numbers, he or she would be able to send out SMS messages to the OSP on behalf of the legitimate customer.
- [*] The primary communication channel (web channel) between the user and the bank web-server must be encrypted and secured. This can be achieved by using the HTTPS protocol (based on the design recommendations covered by section 6.3.3).
- [*] Transaction processing delays should be implemented, especially for transactions that involve large amounts of money. This will give the customer time to report the incident in case of a social engineering attack that has successfully deceived the customer to give out the informational level factors as well as the OTP to activate a beneficiary account. A scenario-based evaluation of this feature was covered in Chapter 5.
- [*] A further process-based authentication class can be implemented after the customer receives the OTP. For example, a partial disclosure technique can be used to extract a 3 or 4 digits that can be used to confirm a transaction from 6 or more digits sent to the user's mobile as OTP. The user remembers a private number which represents the places of these digits in the OTP (e.g. 356 represents the 3rd, 5th and 6th digits of a given OTP). Such mechanism is applied by Swivel Authentication Solution [231].
- [*] The bank should enforce access policies that restrict customers from using the same smart phone to access the bank online application while receiving OTPs via SMS messages. The bank can also impose this policy by restricting mobile phone browsers from accessing their online applications. This will ensure that there is no single point of attack that will help an attacker to compromise the user's account fully. Rather, for any attack to succeed, different independent authentication channels have to be compromised. More details of smart-phones' security were covered in section 0 of Chapter 4.

- Login authentication and transaction authorization must not share the same channel. If conventional authentication mechanisms, such as username and password, are used to authenticate users to login, then transactional services must be authorized using an independent secondary channel such as a mobile network (see section 6.2.3).
- Users must be allowed limited retries to authorize critical transactions before the account is deactivated. This will secure the account from brute-force attacks that could try to figure out the OTPs used to authorize transactions.
- Confirmatory feedback via SMS messages is vital when transactions are carried out. It is also important to notify the account holder by SMS message when the account has been deactivated for any reason (the importance of feedback is further covered by section 5.2.4).
- [*] Users should be given the option to lock their accounts anytime using the mobile network channel. If the user receives an SMS message, for example, requesting to verify a given OTP without being logged into his account, this means that an attacker was able to compromise the account and is trying to authorize a critical transaction. At this time, the user should be able to lock down the account by sending an SMS message command followed by the same OTP received or by sending the OTP in reverse order to the bank server from his or her mobile device. This will deny the attacker any further actions in the account and will allow the user to have enough time to report this incident to the bank. The SMS message requesting to lock the account down has to include the OTP sent to the user (whether in reverse order or following a command) to ensure that this message has been received from the legitimate account holder after he or she has received the SMS message that has the OTP.
- [*] Users should be allowed to unlock their accounts manually only (by approaching the bank in person or by any other legitimate means).

6.6.2 Usability guidelines:

- Users should be allowed to choose whether to utilize MCA at the beneficiary account-creation level or at the authorizing payment transactions level. Some users are more interested in authenticating each and every critical transaction while others prefer to minimize the number of times they use their mobiles to authenticate transactions. MCA mechanism can also be offered at login level as suggested in design option 1 if necessary (see section 6.4.1).

- Users should be allowed to request the bank server to resend the OTP by SMS messages in case of delays or mobile network lagging. However, each SMS message must have a unique code that would differentiate it from other SMS messages. This is important to avoid confusion about which OTP to use if more than one message has arrived.

6.7 Summary

The developed prototype web-application was designed to comply with the guidelines and MCA mechanism design option presented in this study. The web application was designed to support testing the usability and user acceptability of the proposed MCA solution. After the application was designed, a set of 5 tasks was prepared for the users to do. All users' actions were logged into the database to examine the time each user took to fulfil each task alone. The evaluation of the data gathered from users who tested the application is covered thoroughly in Chapter 7.

Chapter 7

Evaluation

Thesis Statement

It is possible to design an authentication mechanism that uses multiple channels to resist attacks more effectively than most commonly used mechanisms. Furthermore, such a mechanism will also be both usable and acceptable to users in Oman.

This chapter presents an overview research methodology used to test this hypothesis. The results show that online banking is indeed acceptable to Omani users and that MCA is, in particular, usable and acceptable to users in Oman. The first part of the thesis statement was addressed thoroughly in Chapter 5 and this chapter will only address the usability and acceptability aspects.

The study reported here was carried out to assess users' acceptance of online banking in Oman in general as well as usability and acceptability of the multi-channel authentication (MCA) mechanism to Omani users. Overall acceptance of online banking is an important step prior to studying the usability and acceptability of any new technology under online banking applications (including MCA). This is vital to ensure the clarity of feedback recorded from users of MCA as some users might not accept MCA because they originally have negative perceptions of online banking as a whole.

The hypotheses are discussed in different sections of this chapter. In section 7.5.1, the demographic characteristics and their effects on the attitudes of customers to accept and adopt online banking were tested (Hypotheses H_{1a} to H_{1e}, see Table 7-1). In section 7.5.3, internal and external variables of the Technology Acceptance Model (TAM) were hypothesized to test the proposed extended TAM for online banking technology (Hypotheses H_{1f} to H_{1h} in Table 7-1). Finally, the main hypotheses on usability (section 7.6.1) and acceptability (section 7.6.2) of multi-channel authentication were developed (Hypotheses H_{2a} to H_{2d} in Table 7-1); they are reviewed towards the end of this chapter. A total of 12 hypotheses are listed in Table 7-1.

The usability and acceptability hypothesis has been split up into the following:

Hypotheses	Source	Mechanism
Online banking is acceptable to users in Oman		
H _{1a} : Gender significantly influences customers' usage of online banking	[232]	Pre-questionnaire
H _{1b} : Marital status significantly influences customers' usage of online banking	[232]	Pre-questionnaire
H _{1c} : Education level significantly influences customers' usage of online banking	[232]	Pre-questionnaire
H _{1d} : Age significantly influences customers' usage of online banking	[232]	Pre-questionnaire
H _{1e} : Income significantly influences customers' usage of online banking	[232]	Pre-questionnaire
H _{1f} : Trust & relationship has a positive effect on Perceived Ease of Use (PEU)	[232]	Pre-questionnaire
H _{1g} : Ease of access has a positive effect on Perceived Ease of Use (PEU)	[232]	Pre-questionnaire
H _{1h} : Security has a positive effect on Perceived Ease of Use (PEU)	[232]	Pre-questionnaire
Multi-channel Authentication is usable and acceptable to users in Oman		
H _{2a} : Multi-channel authentication is effective	[48, 233]	Post-questionnaire, Logs
H _{2b} : Multi-channel authentication is efficient	[48, 233]	Logs
H _{2c} : Multi-channel authentication is satisfactory	[48, 233]	Post-questionnaire
H _{2d} : Multi-channel authentication is acceptable to users	[232]	Post-questionnaire

* OB: online banking

Table 7-1: The list of hypotheses developed in this study

This chapter is divided into six sections: the first section 7.1 covers the survey design and techniques used to collect data from participants. Section 7.2 presents the experiment trials and the difficulties encountered during the data-gathering phase. Section 7.3 outlines the demographic profile of all participants and discusses the dropout rates from the experiment. Section 7.4 presents a series of preliminary tests that are essential for further analysis testing of the hypotheses. Next, section 7.5 discusses the factors affecting adoption of online banking in Oman. The first part of this section assesses the demographic variables hypotheses for possible influence on the adoption of online banking in Oman. The second part hypothesizes some external TAM variables found in the literature to affect users' adoption of online banking. It then presents the results of the hypotheses testing; the resulting extended TAM is presented in Figure 7-37. Section 7.6 covers the usability and acceptability of the multi-channel authentication mechanism and addresses the outcome of the last two hypotheses being tested in this chapter.

7.1 Survey Design

A survey is one of the most popular methods used in social science to capture users' reactions and performance with a system or prototype [234, 235]. *Questionnaire* and *observation* are two main survey techniques used for data gathering. Sharp defines questionnaires as "a series of questions designed to be answered asynchronously"; they can be conducted either on paper or in online format (i.e., via e-mails or web) [235].

According to him, observations may be direct or indirect. Direct observation involves live monitoring of things as they happen, while indirect observation involves recording the user's activities to be investigated at a later time. In this research, web-based online questionnaires and indirect observations were used together to record data and collect feedback from users. The following sections will outline the design of both techniques.

7.1.1 Online Questionnaire Design

Online questionnaires are becoming an increasingly common research tool for a variety of research fields [235, 236]. They offer distinctive advantages over traditional paper questionnaires such as the ability to reach a wider sample quickly and easily. They are interactive and cost effective (e.g., printing, travelling, data entry), and they generate a fast response, data validation (i.e., users input such as e-mail address, mobile number, and age can be validated and checked whether or not the user has entered them correctly), rule enforcement (i.e., selecting only one radio option), and data entry direct from users to the database [235, 237]. Other advantages of web-based questionnaires, compared to paper and e-mail-based questionnaires include live and centralized management of the questions in case further modifications are needed to the questionnaire items.

Most of the scales used in the online questionnaire adopted in this study were derived from existing scales in the literature and adapted to fit this study's context. For example, the study [232] used a list of online banking services to determine which of the services the users used. This list was compared with the online banking services offered by banks operating in Oman. Only those services that matched were presented in the questionnaire. These services were presented in two columns, each of which used a 5-option Likert scale. Each column represented a different online banking method: the first column represented conventional online banking systems and the second one represented the online banking system with multi-channel authentication. Users selected how likely they were to use each

of the listed services based on the types of online banking used. The scale is presented in Appendix B.

To test the usability of the proposed multi-channel authentication mechanism and the functionality of the alternative channel mechanism, questions from the survey presented by [48] were used. These questions were originally used to study the usability of fourth-factor authentication (voucher system). The same technique is also included in the prototype application as an emergency authentication factor.

Finally, to identify the factors affecting the adoption of online banking in Oman, five survey questions from [232] were used. These assessed *ease of access*, *trust and relationship*, *security*, *convenience*, and *ease of use*. These factors have been previously tested in Oman by [5] and [4]. The former found that *security* and *data confidentiality* issues have been major barriers in adopting online banking in Oman. It also found that the banking sectors in Oman were reluctant to use e-commerce applications due to the security weaknesses these applications have. The latter study found that *usefulness* and *ease of use* factors were among the main drivers of online banking adoption in Oman. It also found that *trust* and *ease of access* were the major inhibitors. This study sought to confirm both results and to determine whether customers in Oman have changed their opinions about adopting online banking in the intervening 4 to 6 years.

The questionnaire was posed in two languages: English and Arabic. This was necessary because all users are non-native English users, and this could make some questions presented in the questionnaire unclear or misinterpreted if posed only in English, as argued by [238].

7.1.2 Indirect Observation

Indirect observation is another important technique commonly used to capture user activity and interaction with a prototype system. In this study, it was not feasible to monitor the users directly in person or indirectly by recording their interaction with the system on surveillance cameras. Most of the participants accessed the application and tested it from different geographical places during the same period in Oman. Thus, the only realistic observation was to automate the process and log all user actions in the database. This logging script ran every time the user loaded a web page. It recorded the user's identity, the page's filename, the time the user visited the page (i.e., in Unix system-based time which

represents the number of seconds from midnight January 1, 1970), query strings, and form variables. Query strings and form variables (i.e., also known as GET and POST methods respectively) provided important details, along with the page's filename, to better identify the task the user engaged in at a given time (more details in section 7.4.1.2).

7.2 Experiment Trials

The experiment underwent various trials and improvements between 2008 and 2010. The first pilot study did not reveal any issues. However, after moving to the trial phase, the outcome revealed usability issues that were corrected for the second trial of the prototype application. The results of the first trial were published in 2010 [239].

The following sections will report on all issues encountered in the first trial and the issues addressed in the second trial to overcome the emergent usability and ease of access issues.

7.2.1 First Experiment Trial

The application was hosted on a local web-server connected to the Sultan Qaboos University's network in Oman. The server was a personal computer with limited resources such as low memory and slow speed. A mobile modem was connected to this server to send and receive SMS messages from/to the users. SMS gateway software was installed to serve as an intermediate gateway between the application database and the mobile modem (see Figure 7-1).

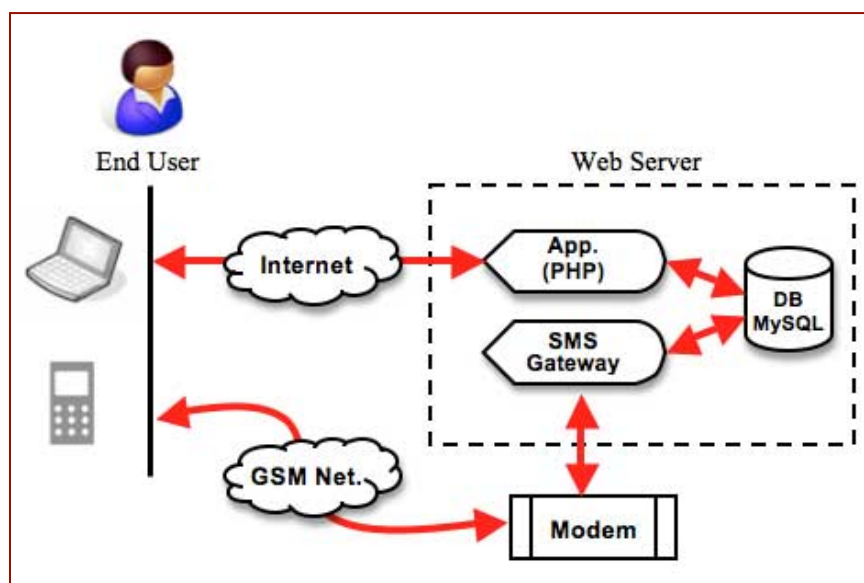


Figure 7-1: First trial, prototype, application structure

The first version of the application included many features, such as a real SMS gateway and support for the security skin (covered in section 4.1.3.3) allowing the users to upload a profile image. The initial pilot study of the first experiment trial did not reveal any usability issues. After the trial began on the 25th of August 2008 and web users started using the application, the researcher started receiving negative feedback from some participants complaining about various aspects, summarized in the following points:

- SMS messages: some users did not receive the SMS messages from the system in good time. Such SMS messages should normally arrive in real time from the SMS gateway installed on the web server hosting the application. Other users complained that they had received more than one message with different one-time pin (OTP) numbers. Still others received advertisement messages related to the SMS gateway installed on the server instead of the message containing the OTP.
- Unclear instructions: many users were lost in some of the tasks and did not know how to complete them. This issue was also reported by similar study carried out in the UK [91]. The participants did not read or follow the instructions, which were printed in a sheet given to each of them, for testing a 2-factor authentication method. They had difficulties completing the tasks.
- Compatibility: some reported that some features were not compatible with their systems (e.g., the Java script live countdown timer on the `activate_beneficiary.php` page did not work).

After investigating these complaints, the researcher was able to pinpoint different issues that needed to be corrected.

The delay that some users experienced in receiving SMS messages was related to the fact that the personal mobile modem had a limited capacity to send more than one SMS message at a time. Thus, if many users were connected to the server and were requesting the application to send SMS messages all at once, the modem would queue the messages and send them one by one until all messages were sent. This practice also sometimes led to messages being sent repeatedly. The users tended to request new messages to be sent to their mobile phones if the first SMS did not arrive immediately. Hence, a number of SMS messages resulted, each with a different OTP.

Some users received advertisement SMS messages rather than the messages with OTP. This was because the SMS gateway installed in the web server was commercial software called “Ozeki NG SMS Gateway” and was acquired on a trial basis due to the high cost of

the full license version. Hence, the software dropped every 10th to 20th SMS message sent from the application and replaced it with an advertisement SMS message for Ozeki NG Informatics Ltd.

Some instruction clarity issues also needed to be addressed. In this first trial, users were instructed to download a guide, which had all the instructions on how to complete all required tasks. The guide was in PDF format. However, most participants ignored this guide and started using the application directly to do the tasks. Many of these users had problems completing the tasks due to usability issues.

Most of the respondents experienced difficulties understanding task 7, which was the task requesting them to utilize the fourth authentication factor as an alternative channel as if the primary channel were temporary unavailable. Others suggested making the application friendlier and presenting it in two languages (English and Arabic).

The following subsections will discuss the outcomes of the first trial analysis and cover other difficulties the users encountered and reported.

7.2.1.1 Sample profile and results

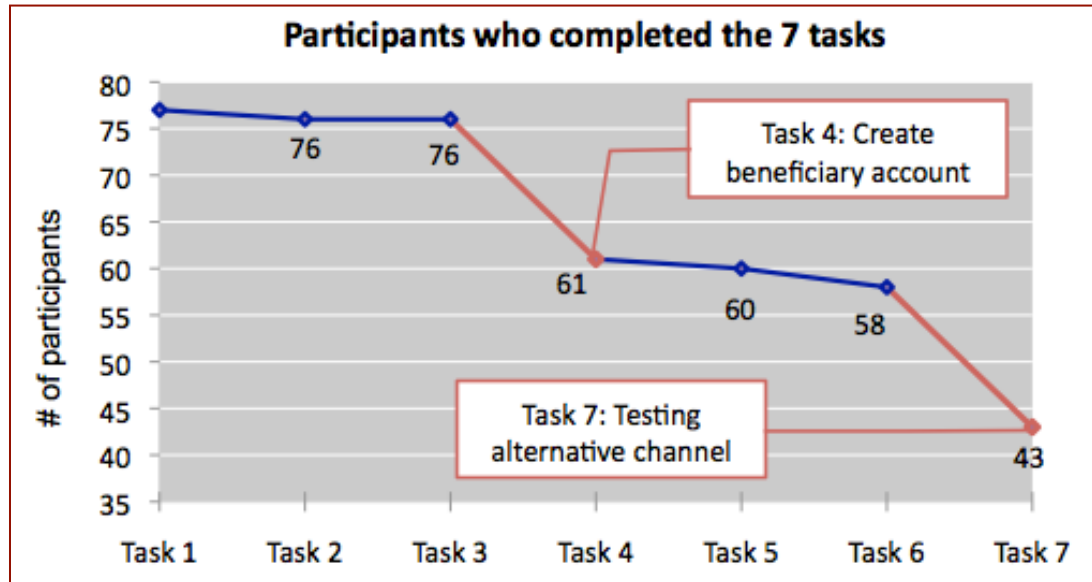


Figure 7-2: Dropouts of participants in the first trial

A total of 77 people participated in the study. However, only 43 completed the questionnaire. Figure 7-2 shows the major dropouts of participants in tasks 4 and 7. Users completed mobile activation to have their bank account activated in Task 4. Participants who dropped out at this point confirmed that they thought it was the end of the testing

process and they did not realize that they needed to complete further tasks, which they did not notice in the task guide.

Task 7, on the other hand, asked the users to test the fourth authentication factor by pretending that their primary authentication device was not available. The fact that the users were testing this feature for the first time and that most of them had difficulties understanding the requirements could be the reasons for so many dropouts at this stage.

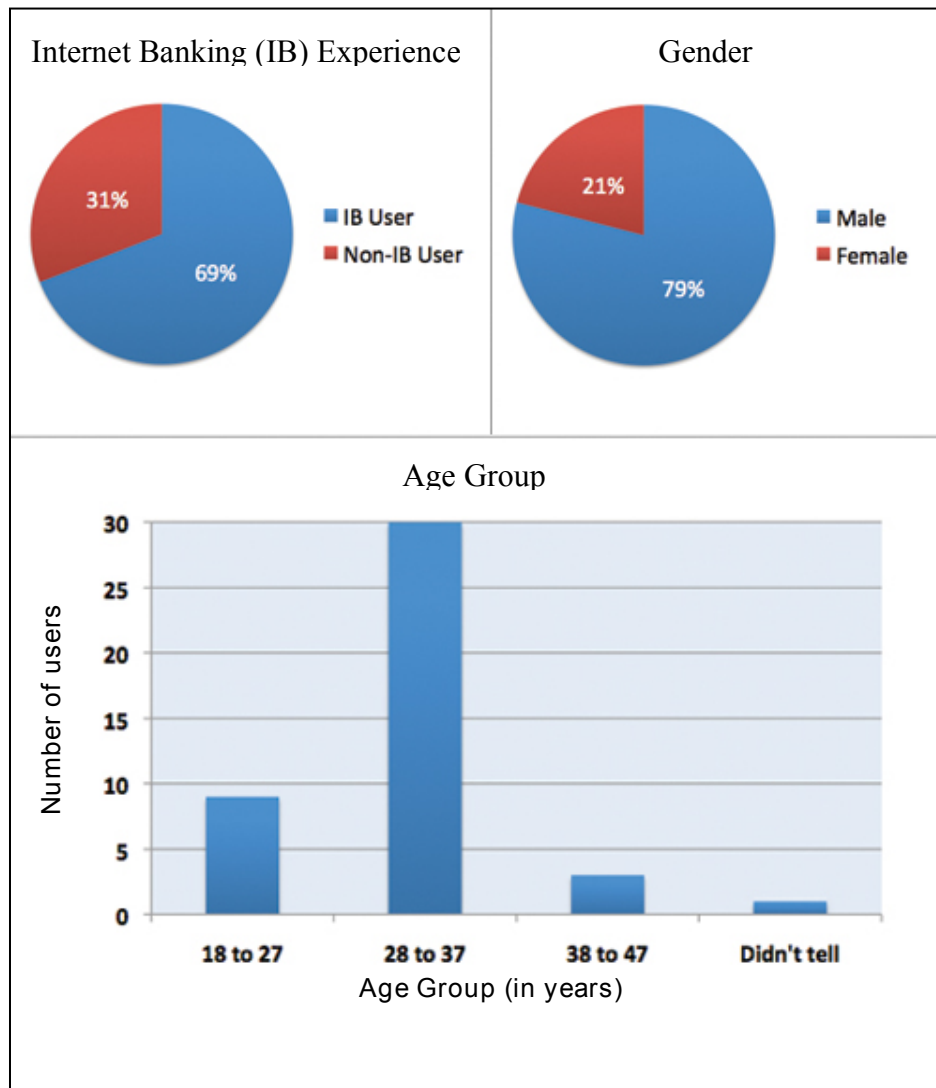


Figure 7-3: First trial sample profile

Unfortunately, it was difficult to determine the demographic background (education level, age group, gender, etc...) of those who dropped out because the questionnaire was posed at the end of the application. Users in the first trial were not requested to complete the questionnaire before they completed all required tasks, and therefore, valuable details on those who dropped out in the middle were missed. Figure 7-3 presents the first trial's statistical information.

7.2.2 Pilot Test of the Second Experiment Trial

A pilot test is a small trial of the main study and aims at ensuring that the proposed research methods are viable [235]. Performing a pilot test is especially important when data are collected through self-administered questionnaires where the investigator is not available to assist participants when they need help [240].

The pilot test was first tested by a research fellow from the University of Glasgow who provided valuable comments on the questionnaire and the wording used throughout the application. Another research colleague commented on questions in the questionnaire and advised on breaking down some general questions into sub-questions to enhance clarity. A few other pilot tests were carried out by academics in Sultan Qaboos University and by some industry personnel in Oman and revealed some minor cosmetic issues that were resolved before the final trial. Finally, some specialists from the banking sector in Oman helped in reviewing the Arabic terms used in the questionnaire and suggested some more appropriate alternatives commonly used by the banking sector.

7.2.3 Usability Issues Addressed in the Second Trial

The second trial commenced on the 21st of February 2010. Major changes were implemented in this version. First, the “upload profile image” feature was no longer available as the results showed that only 2 to 3 participants uploaded images to their profiles in the first trial. Some might well have withdrawn from the application at this stage because they could not find images to upload on their machines.

Secondly, the survey was split into two questionnaires: pre and post questionnaire. The split process was based on questionnaire focus. Those items not directly related to the application and multi-channel authentication were posed in the pre-questionnaire (e.g., user demographic details, factors influencing the adoption of online banking, etc...). The user was requested to complete the pre-questionnaire directly after the registration process. This ensured that there was a record of those users who dropped out without completing all tasks. The post-questionnaire was administered towards the end of the trial after the user had completed all required tasks.

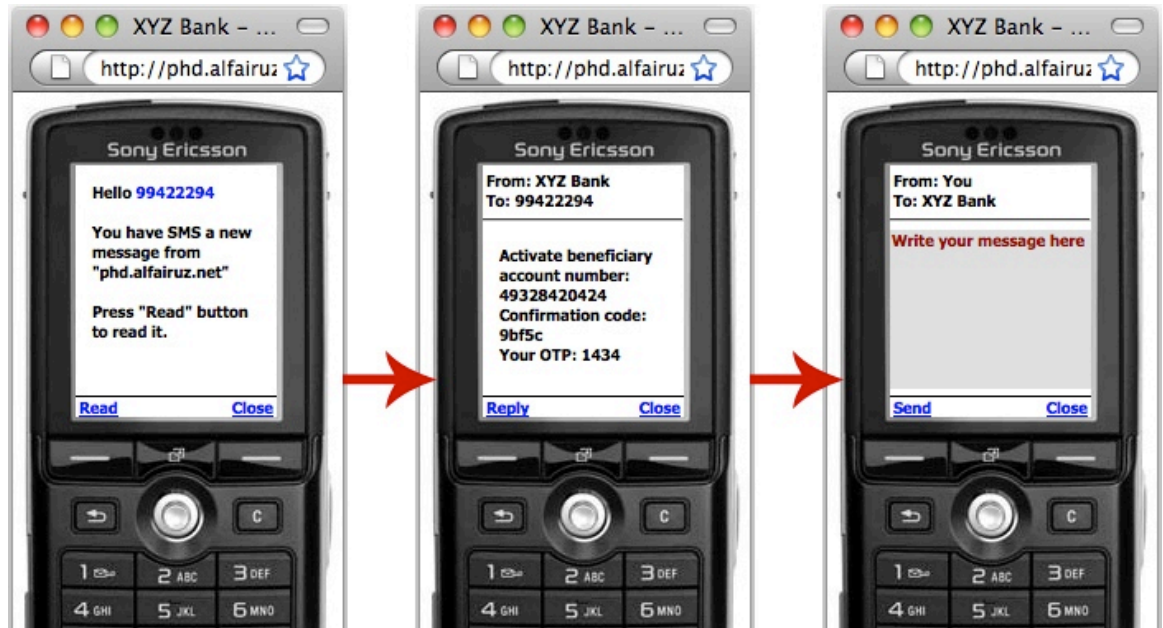


Figure 7-4: On screen mobile simulation for SMS reading and sending

Thirdly, it was decided to incorporate a mobile simulator that appeared on the screen to substitute for the user mobile phone (see Figure 7-4). This was another vital improvement so the application could be independent of any physical modem or SMS gateway (which were limited by capacity and trial-based license in the first trial). Furthermore, this change allowed the researcher to host the application on a much more efficient, more reliable, and faster web-server hosted in the USA since there was no need for an SMS modem to be physically connected to the web-server, as in the first trial (see Figure 7-5). This change also allowed the participants who were concerned about divulging their mobile number to register fake mobile numbers since no real SMS messages were involved. Participants who had privacy concerns on the first trial were now free to use a spurious mobile number to test the application.

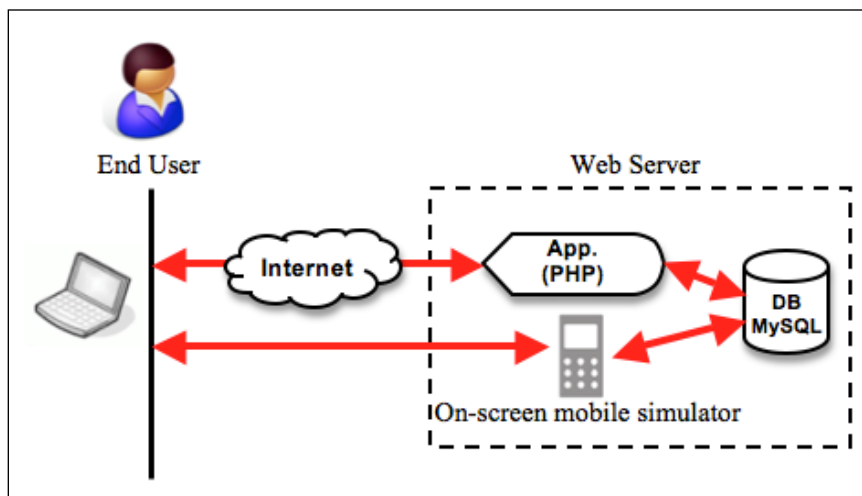


Figure 7-5: Second trial prototype application structure

Another major change was to improve the “ease of use” and to integrate the instructions and task guide into the application. The number of tasks was reduced to 5 and the interface was redesigned so each web page gave an indication of the user’s progress at any single point (i.e., a progress indicator displayed the user’s progress in percentage and displayed the tasks that were not yet completed). Moreover, along with on-screen systematic instructions, flash tutorials with recorded screen and mouse movements were designed to help the user to understand how to complete the required tasks. These instructions were available on every web page of the application. In addition to these instructional details, every link that the user was required to click as the next step in the process was designed to blink so that the user could find his or her way to complete all tasks without any issues.

Finally, some bugs reported in the first trial were fixed in the second trial and the overall design was improved to serve users better without any browser compatibility issues. The core templates were modified and restructured so the prototype application could serve users in both languages: English and Arabic. The user could switch between languages anytime along the way without losing any saved data. The session remained live even after the language had been switched. All instructions, tutorials, feedback, and phrases were translated into Arabic accordingly. The results of the second trial are discussed in subsequent sections of this chapter.

7.2.4 Application Requirements/Tasks (Second Trial)

There were five different requirements or tasks set up for users to test this application, starting with registration and finishing with money transfer. The users were asked to follow a list of tasks that provided information on all the requirements the user had to meet in order to test all the features of the prototype application. These tasks are described in the following subsections.

7.2.4.1 Task 1: Registration

The registration process was the first requirement. It served as the enrolment process to the bank system. However, in real online banking systems, this element would not exist and the only way for the user to enrol would be to approach the bank in person and apply for an online banking account. This is important because there must be a way to check that the people applying for this service are who they claim they are.

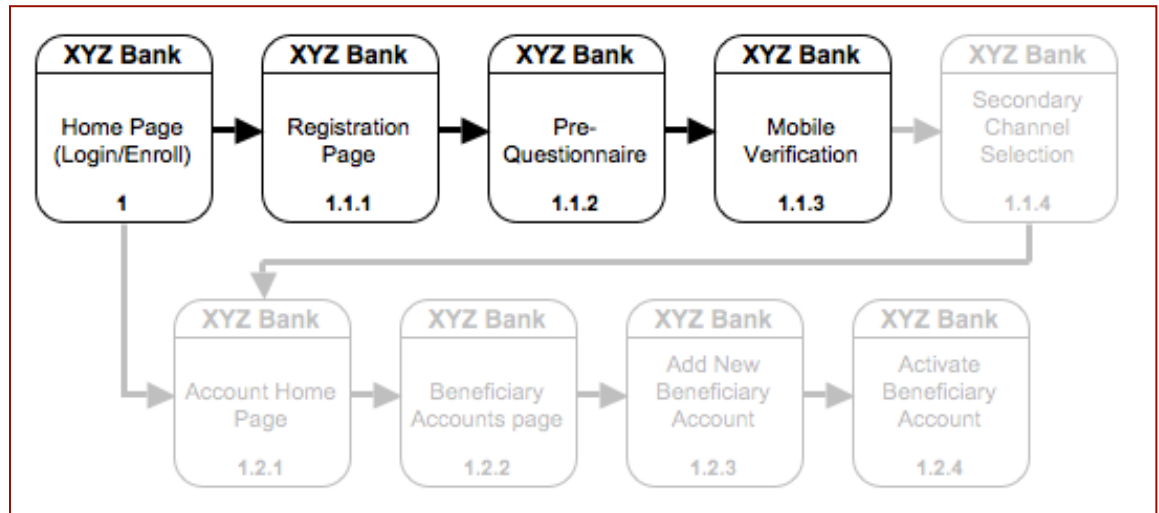


Figure 7-6: Task 1 - Storyboard

The prototype registration process had three stages: initial registration and mobile number registration, pre-questionnaire, and primary mobile number activation (see Figure 7-6).

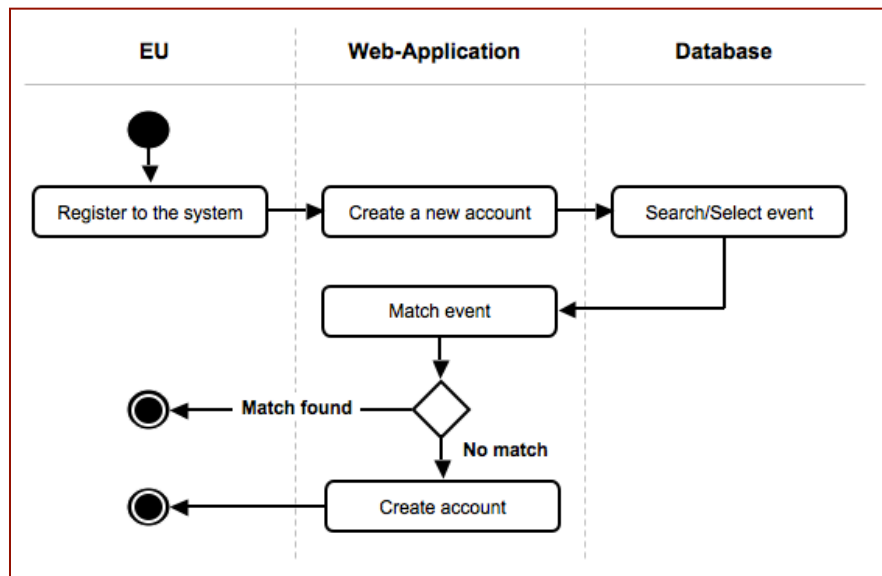


Figure 7-7: Registration - stage 1 - WebMD activity diagram

In the first stage, the user was asked to open an account by choosing a username, a password, and an e-mail address. The application checked username availability. If no matches were found, the new username was registered and a new account for the user was created in the database (see Figure 7-7).

Multi-Channel Authentication

Interface Language: English - العربية

This is an evaluation application and does not reflect real information of real customers!

[Home](#)
[About The Research](#)
[Contact Researcher](#)

[Home](#) » [New Registration](#)

Username

Check Availability

Password

Password

Confirm Password

Password Strength

Weak

E-mail Address

E-mail Address

Confirm E-mail Address

Register

Figure 7-8: Registration page – stage 1 - Implementation

Figure 7-8 presents the implementation design of the registration process (stage 1). This page included an AJAX feature that allowed the user to check the availability of the new username without the need to reload the page. It also featured a password strength bar, which reflected how strong the chosen password was. This feature utilized a formula that calculated the strength of a string based on factors like length, case, and special characters. It categorized the passwords into six categories: very weak, weak, better, medium, strong, and strongest.

Once this first stage was completed, a new account was created for the user and the application advised him or her to complete a pre-questionnaire. After the user completed the pre-questionnaire, the application initiated the 2nd stage of registration. At this stage, the user was asked to enter his or her name, mobile number, and an alternative mobile number. The user's mobile number would be used to interact with the user directly (i.e., passing the OTP to the user and receiving confirmation from him or her when the mobile network channel is selected for verifications). The alternative mobile number, on the other hand, would be used solely for situations where the primary mobile number is lost or unavailable; hence, it exemplifies the use of 4th factor authentication [48] as an emergency authentication mechanism as discussed later in this chapter.

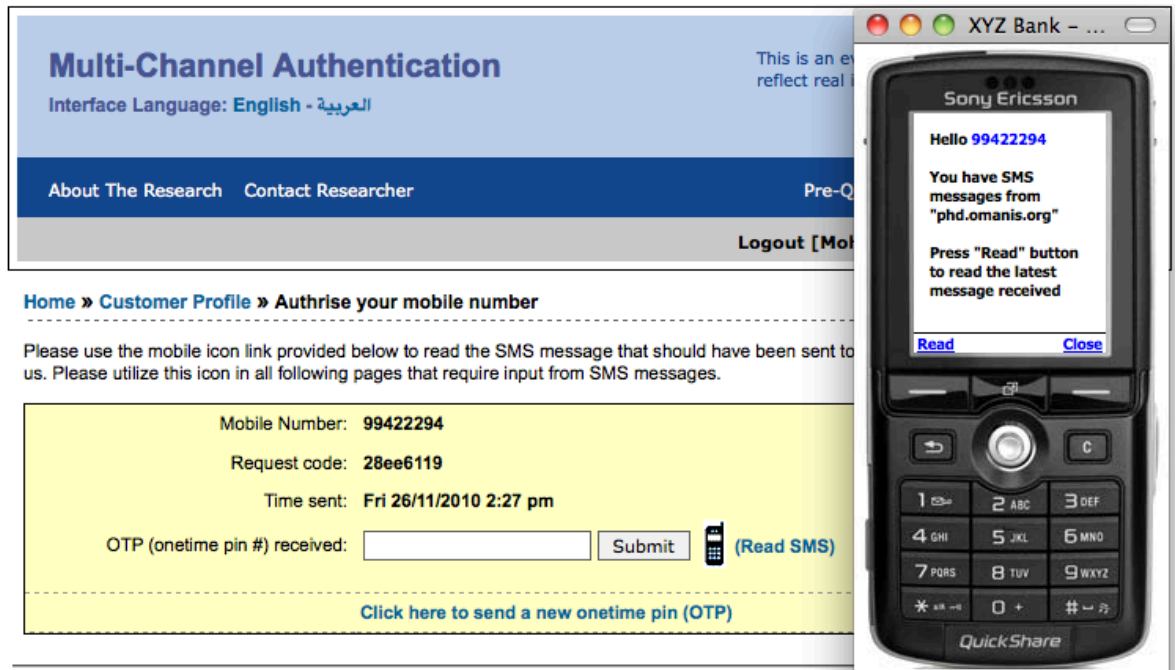


Figure 7-9: Registration task - stage 3 - implementation

The final stage of the registration task activates the primary mobile number. The user was redirected to the mobile activation page (see Figure 7-9). The application requested the user to open a mobile phone simulator to read the SMS message sent from the bank. This mobile simulator was used in the application to avoid any network interruptions while users are testing the prototype application. This implementation prevented SMS message delivery failure whether the user had submitted valid mobile numbers or not. In addition, the SMS gateway software license and the hardware needed to implement live SMS messages for all users without restrictions were expensive and exceeded this researcher's allocated budget.

For these reasons, the users were instructed to click on a mobile icon that appeared on the screen. This mobile icon opened an on-screen mobile phone that simulated a mobile phone the user could have in real life. Once the user clicked on the icon, a mobile phone appeared on the screen with a welcome message informing the user that he or she had received a SMS message from XYZ Bank. The user was to click on the "Read" button to read the message. The SMS message then appeared from the screen, representing the exact message that would be delivered to the user's mobile phone number if the SMS gateway were enabled by the system (see Figure 7-9). The user had to read the message and extract the OTP included somewhere within the message. This OTP was then to be used in the available text-box on the previous screen to activate the mobile number.

This process was important to teach the participant how the application and mobile phone interacted with each other. This 3rd stage does not exist in the real online banking applications as the customer's mobile numbers can be verified at enrolment.

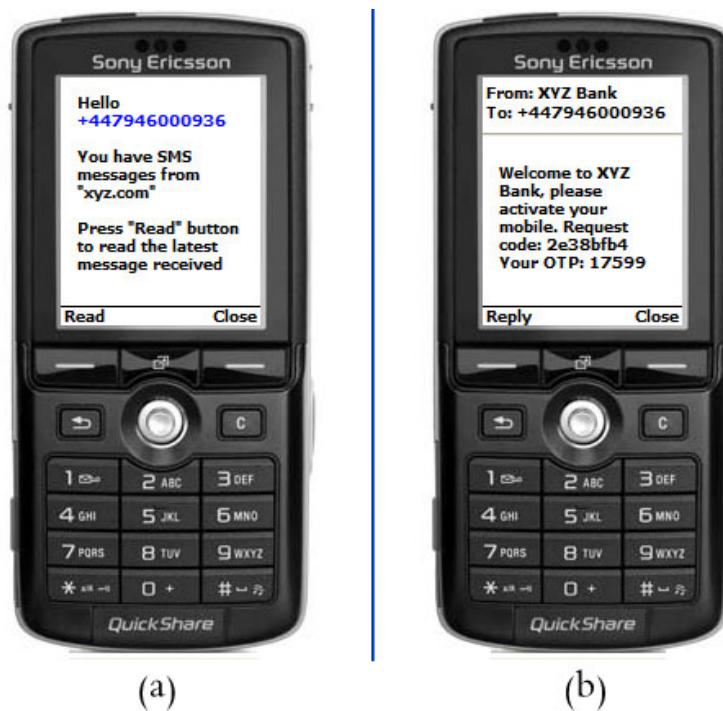


Figure 7-10: Mobile simulator - (a) Welcome message, (b) SMS message

Along with the OTP that sent to the user, the SMS message also contained a *request code* (as can be seen in Figure 7-10). This request code acted as a unique code to differentiate between different OTPs if the user requested more than one SMS message to be sent out. In real implementations, and for other authentication purposes where SMS messages were used to complement other authentication mechanisms, mobile networks sometimes encounter issues such as lagging. If this happened, and the user did not receive the SMS message within a specific time (60 seconds in the case of the prototype application), the system would allow him or her to request another SMS message with a new OTP and different request code. If the user received both SMS messages at the same time, only the SMS message with the request code that matched the one displayed on the screen would be used to validate the request. The same applied to all other SMS correspondences between the application and the user.

7.2.4.2 Task 2: Verification channel selection

After the user's mobile number had been successfully verified, the application asked the user to select the more convenient verification channel to use (see Figure 7-11). This verification channel defined how the user would verify the OTP received from the system.

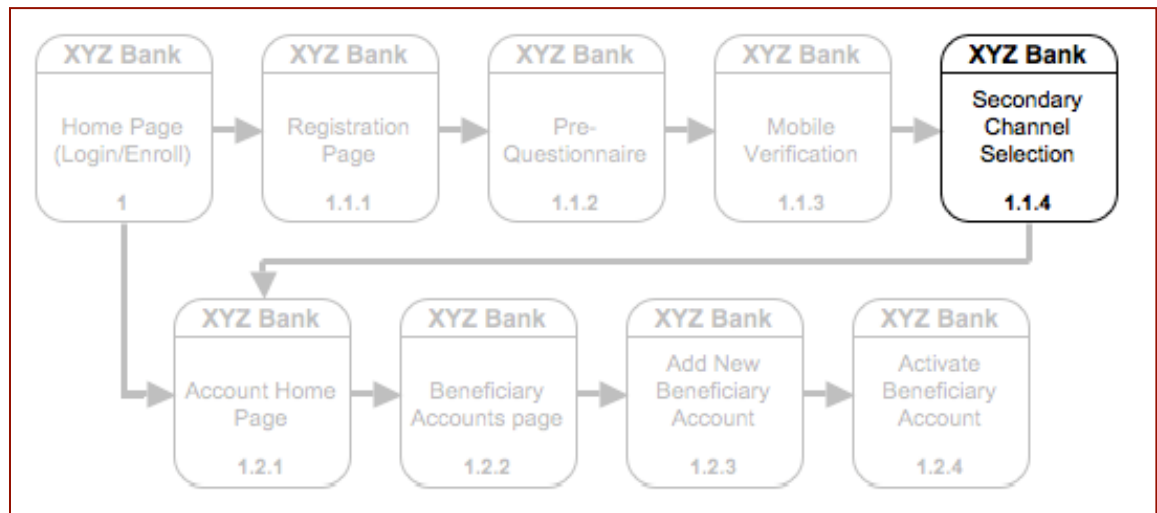


Figure 7-11: Task 2 - Storyboard

There are two methods available:

1. *Verifying OTP through the web channel* (see Figure 7-12): this approach suggested that the user would receive the OTP via a SMS message, and then that he or she would verify this OTP back to the system by entering it in a text field on the screen.

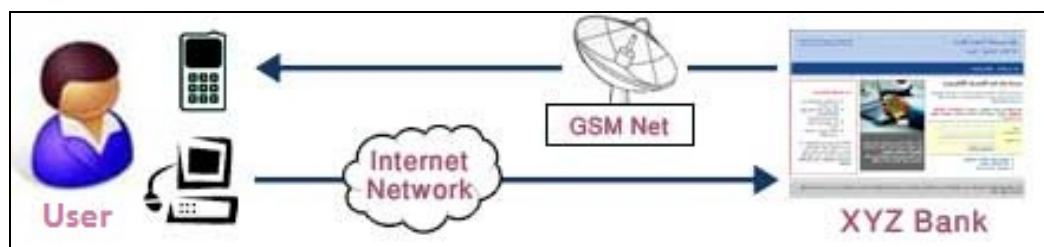


Figure 7-12: Verifying OTP through the web channel

2. *Verifying OTP through the mobile network channel* (see Figure 7-13): the user received the OTP by SMS as suggested by the previous method; however, here the user would verify the OTP by sending it back to the system using a mobile network (by SMS).



Figure 7-13: Verifying OTP through the mobile network channel

Once the user selected one of the available verification methods, the application created a test bank account and credited an amount of OMR 10,000 to be used in later tasks.

7.2.4.3 Task 3: Beneficiary accounts

The participants in this task were required to create beneficiary accounts to transfer money among them. There was no limit on the number of beneficiary accounts each user could create. However, the most important factor in this task was to introduce the MCA mechanism implementation for the user to test as suggested by section 6.4.2.

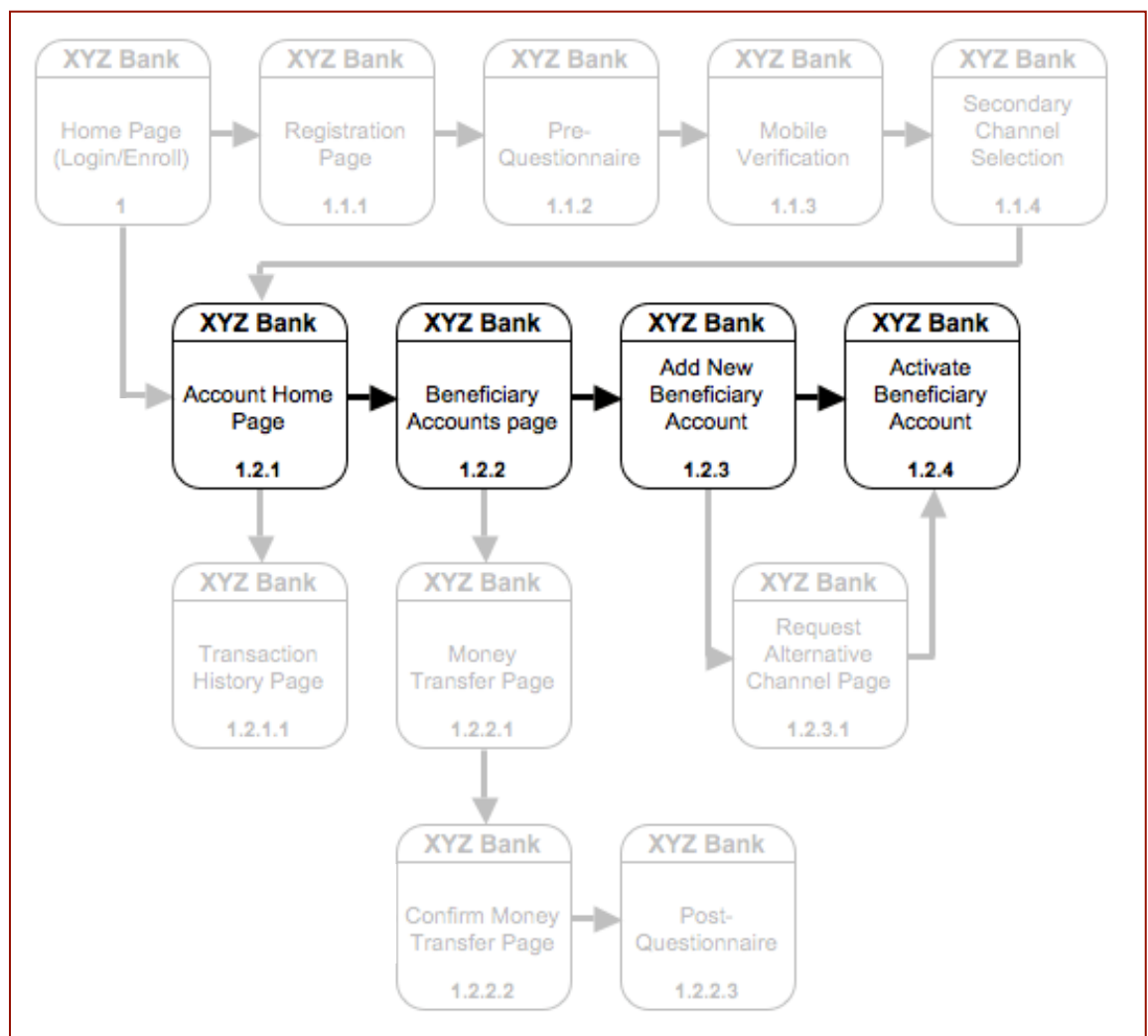


Figure 7-14: Task 3 - Storyboard

As illustrated in Figure 7-14, first the user needed to request to add a new beneficiary account from the beneficiary accounts page. The application then requested the user to enter the beneficiary account details as depicted in Figure 7-15.

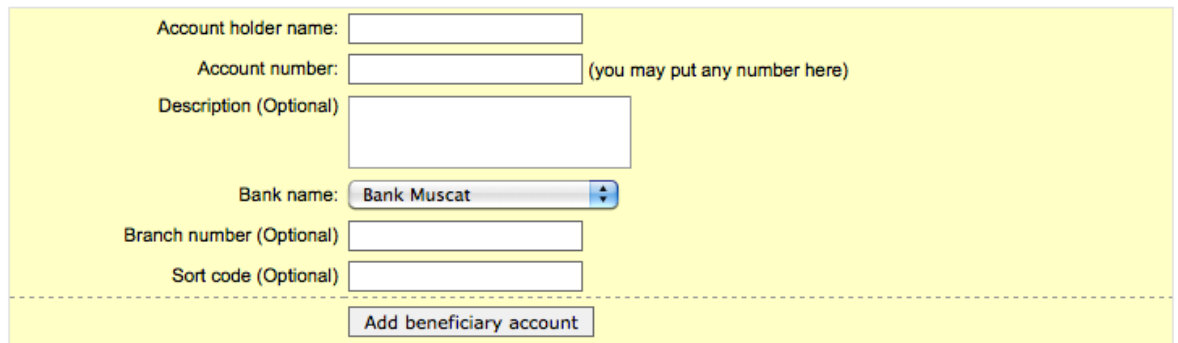
A screenshot of a web form titled 'Add new beneficiary account form'. The form is set against a light yellow background. It contains several input fields: 'Account holder name:' with a text box, 'Account number:' with a text box and a note '(you may put any number here)', 'Description (Optional)' with a larger text box, 'Bank name:' with a dropdown menu showing 'Bank Muscat', 'Branch number (Optional)' with a text box, and 'Sort code (Optional)' with a text box. At the bottom of the form is a blue button labeled 'Add beneficiary account'.

Figure 7-15: Add new beneficiary account form - implementation

After the user submitted these details, the application created a new beneficiary account, which was not yet active, and sent out an SMS message to the user to activate the account. The format of the message is shown in the Figure 7-16 below.

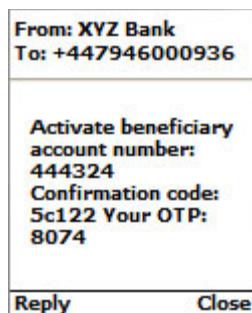
A screenshot of an SMS message interface. At the top, it shows 'From: XYZ Bank' and 'To: +447946000936'. The main body of the message contains the text: 'Activate beneficiary account number: 444324', 'Confirmation code: 5c122', and 'Your OTP: 8074'. At the bottom of the message box are two buttons: 'Reply' and 'Close'.

Figure 7-16: SMS message format for activating a beneficiary account

Three important variables were included in the SMS message body: *the beneficiary account number*, *the confirmation code*, and *the OTP*. The beneficiary account number helped the user to know if he or she were authenticating the beneficiary account that was originally created or another beneficiary account that had been created by an attacker. The confirmation code, on the other hand, was an identification code for the SMS message, which the user could match with the confirmation code displayed on the screen. If they matched, then the OTP sent in this message was the OTP to be entered on the screen (or to be replied back via SMS message to the bank system if the user selected to verify the OTP by SMS in Task 2). This feature served the same function as the request code covered earlier in Task 1.

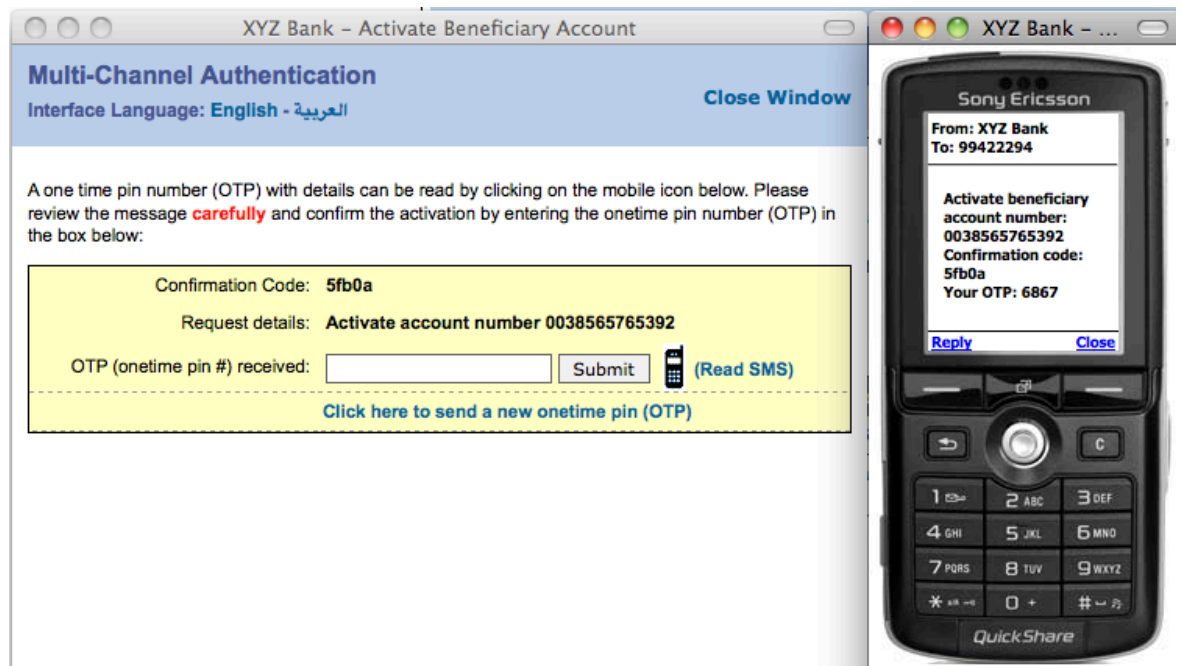


Figure 7-17: Activate beneficiary account - implementation

For the user to activate the new added beneficiary account, he or she had to open the activation window assigned to the beneficiary account (see Figure 7-17). After ensuring that the confirmation code from the screen and the SMS message matched, then the user could extract the OTP from the message and write it in the text-box available in the window.

Once the correct OTP was submitted, the beneficiary account was activated and the participant could then move to Task 4.

7.2.4.4 Task 4: Money transfer

Money transfer services and other financial services that involve moving money away from the user account belong to the transactional level of the system. All previous tasks dealt with the informational level only. Hence, Task 4 could not be completed without completing Task 3 that, in turn, required the MCA mechanism to complete. It is vital that transactional level services be restricted from access or manipulation unless they, or any services leading to them, are authenticated using the MCA mechanism.

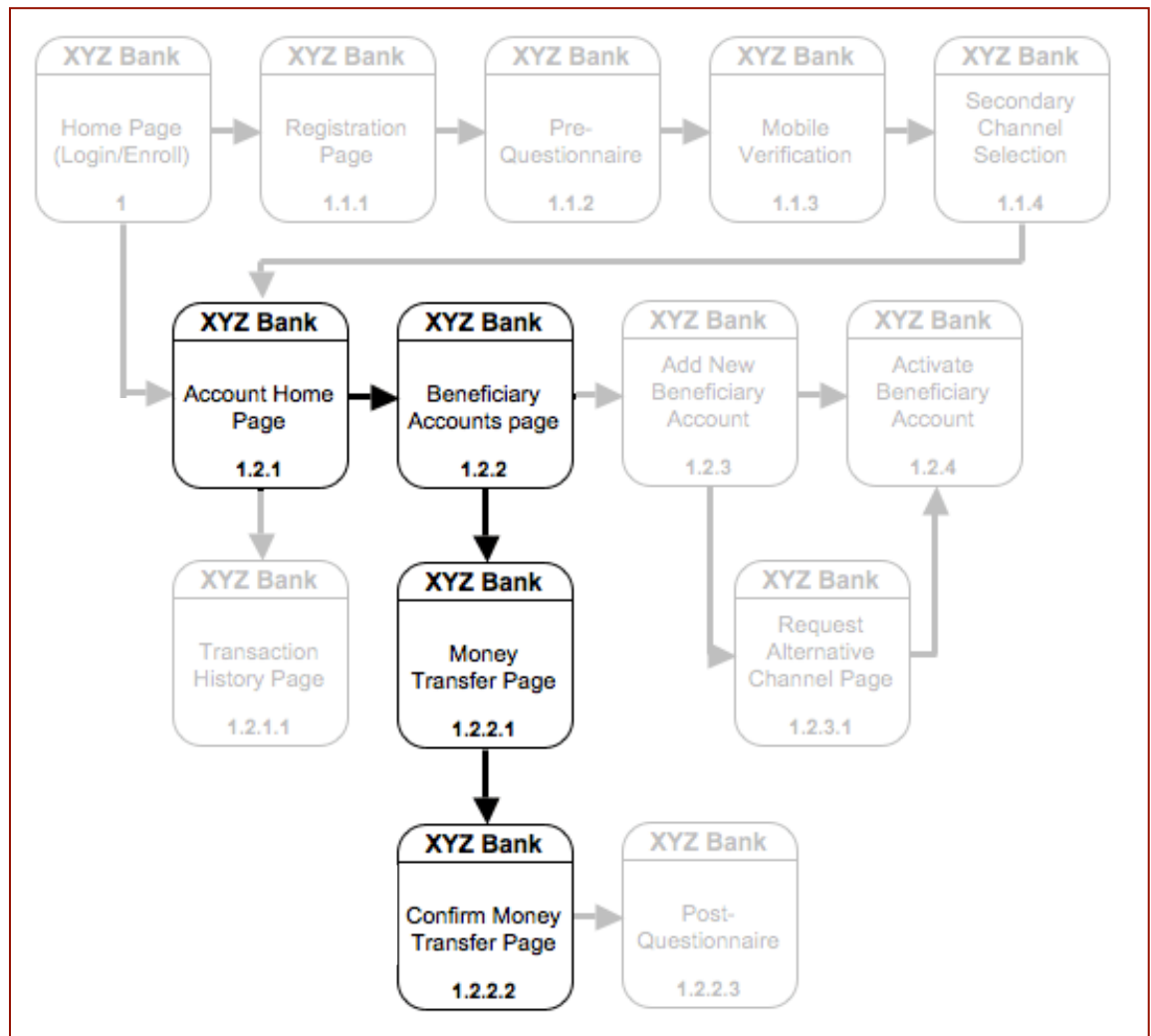


Figure 7-18: Task 4 – Storyboard

Task 4 was comprised of three steps, starting from the account home page (see Figure 7-18). To initiate a money transfer request, the user had to access the beneficiary accounts page shown in Figure 7-19. Any activated beneficiary account listed on this page had three options enabled in front of its record. A description of the role of each of these three options follows.

Multi-Channel Authentication

Interface Language: English - العربية

This is an evaluation application and does not reflect real information of real customers!

[About The Research](#)
[Contact Researcher](#)
[Show Help](#)
[Pre-Questionnaire](#)
[Post-Questionnaire](#)

[Logout \[Mohamed\]](#)
[Accounts](#)
[Edit Profile](#)

[Home](#) » [Transfer](#)

Your beneficiary account has been activated successfully!

In this page you can transfer money from your account number **38-983453616** to another account. Please provide details of beneficiary account / account intended to be credited:

[Add a new beneficiary account](#)

Beneficiary Name	Account #	Status			
Harib Al Busaidi	0038565765392	Active	Transfer	Delete	History

Activate*: the account is awaiting your response. Please click the link Activate for more details.

Figure 7-19: Beneficiary accounts page - implementation

- *Transfer*: this option allowed the user to transfer money to the beneficiary account associated with this option. It took the user to another page with a transfer form that had to be filled (see Figure 7-20).

Amount Available: **OMR 10,000**

Beneficiary Name: **Harib Al Busaidi**

Beneficiary account number: **0038565765392**

Amount to transfer: (max OMR 5,000.00 per transaction)

Description of Payment:

*use this to keep a record of your payment by describing the reason of payment

Figure 7-20: Money transfer form - implementation

- *Delete*: this option deleted the beneficiary account. Any additional beneficiary account required another OTP activation following a deletion.
- *History*: this allowed the user to view all transaction history for the selected beneficiary account.

The maximum transfer allowed was OMR 5,000 per *transaction*. This limitation ensured that the user could test the transfer process at least twice because the application initially credited the user account an amount of OMR 10,000 for testing purposes after the completion of Task 2).

Beneficiary Name: Harib Al Busaidi

Beneficiary account number: 0038565765392

Amount to transfer: OMR 1,500.00

Description of Payment: December rent

Exchange rate: 1.000

Transfer Charges: OMR 0.000

Enter your password: (password you selected at registration time)

Confirm || Modify Cancel

Figure 7-21: Money transfer confirmation page - implementation

Figure 7-21 shows the confirmation page displayed to the user after he or she had selected and submitted the amount and description in the transfer page. It confirmed the transaction details for the user to verify. The verification process was completed by submitting the account login password. Once the password was submitted and verified, the transaction took place.

7.2.4.5 Task 5: Emergency authentication mechanism

In this final task, the user was advised to test the 4th factor authentication approach suggested by [48] (see Figure 7-22). This works in real applications only in situations where the primary channel medium (user mobile number in this study) is not available. An alternative mobile number can be used to process the user transactions until the primary medium is available again. This can be done by creating a new beneficiary account just the way the user did in Task 3. However, this time the user saw the option “Switch to the alternative channel” in the beneficiary account, activation window (see Figure 7-23).

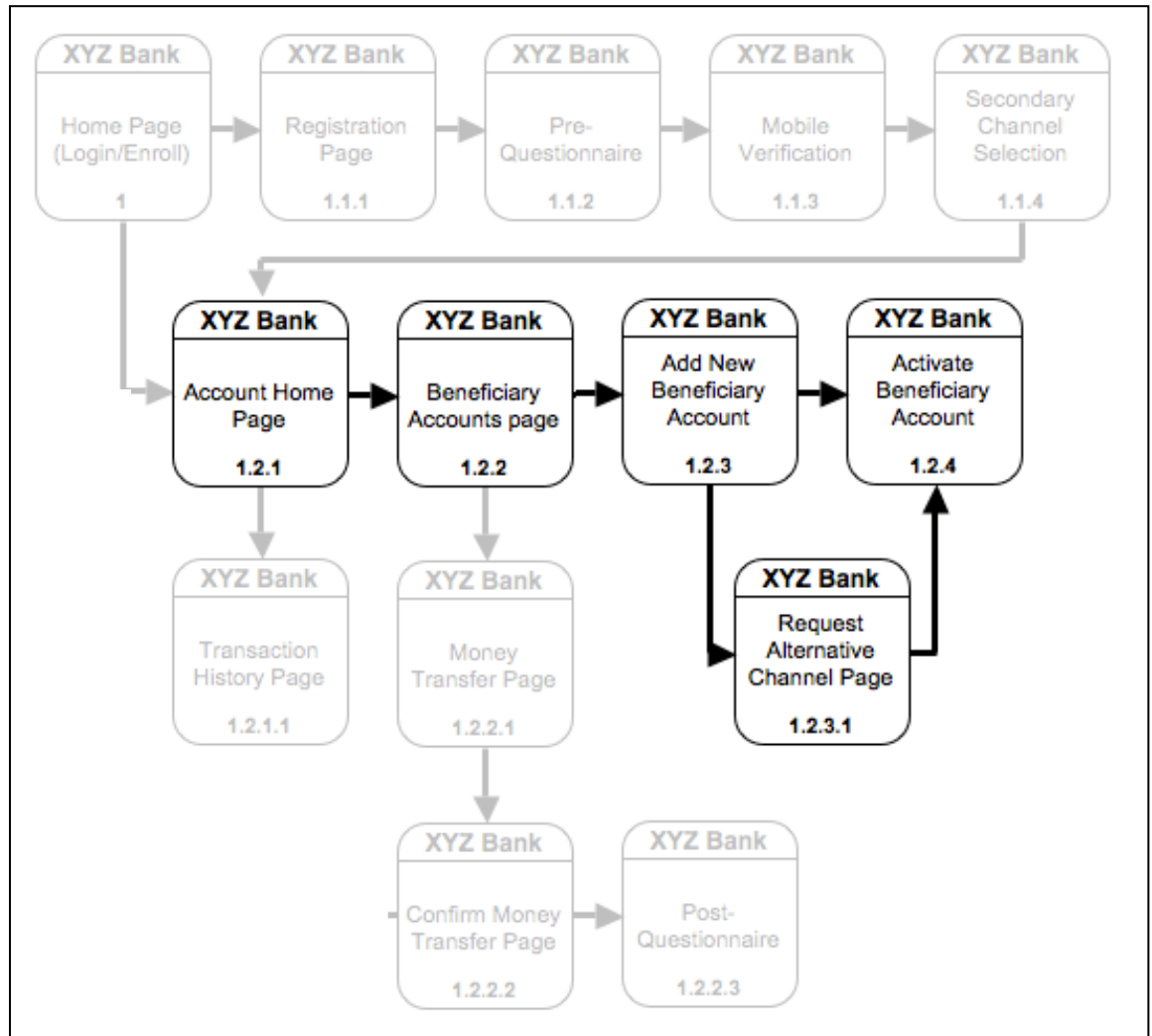


Figure 7-22: Task 5 - Storyboard

Multi-Channel Authentication

Interface Language: English - العربية

[Close Window](#)

A one time pin number (OTP) with details can be read by clicking on the mobile icon below. Please review the message **carefully** and confirm the activation by entering the onetime pin number (OTP) in the box below:

Confirmation Code: **fff96**

Request details: **Activate account number 0038565765393**

OTP (onetime pin #) received: [\(Read SMS\)](#)

Have you lost your mobile?: [Switch to the alternative channel](#)

Wait 152 seconds before sending new message

Figure 7-23: Beneficiary activation window - Task 5 - implementation

If the user selected this option, another page asking him or her to confirm the switch channels request appeared. Once the user confirmed the request, a one-time password was sent out via SMS message. However, this time, the SMS message was not delivered to the

user's mobile number; rather, it was sent to the alternative mobile number registered in the user's account. The SMS message sent in this case would look like the one depicted in Figure 7-24.

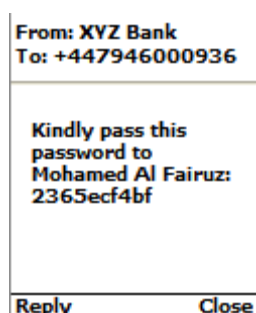


Figure 7-24: The SMS message format sent to the alternative mobile number

This message contained only one factor: the one-time password, a one-time random string that contains numbers and letters. The message asked the mobile holder to pass this password to the account owner so he or she could use it to authorize transactions. No further details needed to be passed along with this message for security reasons. The holder of this mobile number must not know what beneficiary account the account owner would like to activate nor would he or she know any other details related to the user account.

Figure 7-25 shows the window that appeared to the account owner once he or she tried to activate a beneficiary account while the account was switched to the alternative channel mode.

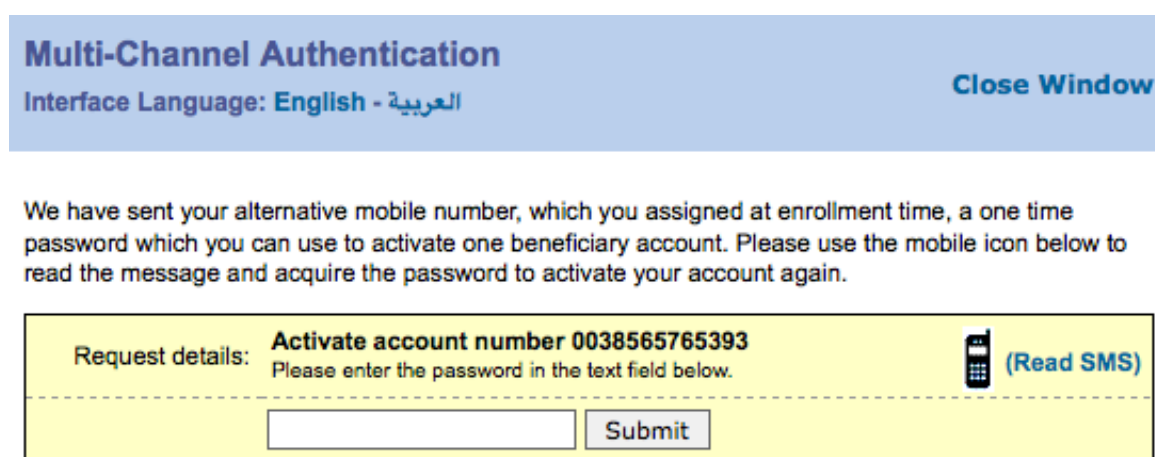


Figure 7-25: Beneficiary account activation window - alternative channel mode - implementation

If the valid password were entered, the beneficiary account would be activated and the user account would be switched back to the normal mode again.

After the user completed this final task, the application showed a link to the post-questionnaire, which collected user feedback about the MCA mechanism implemented in the prototype application.

7.2.5 Participants

Participants were contacted by electronic mails, SMS messages and by meeting them face-to-face. A total number of 188 people took part in the experiment.

Due to the tied social relationships between people in Oman, it was important to test the effects of these independent variables on the researcher friends and colleagues who participated in the study. The sample was divided into two groups: *friends and colleagues* and *other participants*. These two groups were assessed separately to spot any possible social relationship effects on the results in two different areas of the research:

1. Demographic profile and dropout rates (section 7.3.2).
2. Users' satisfaction testing of MCA (section 0).

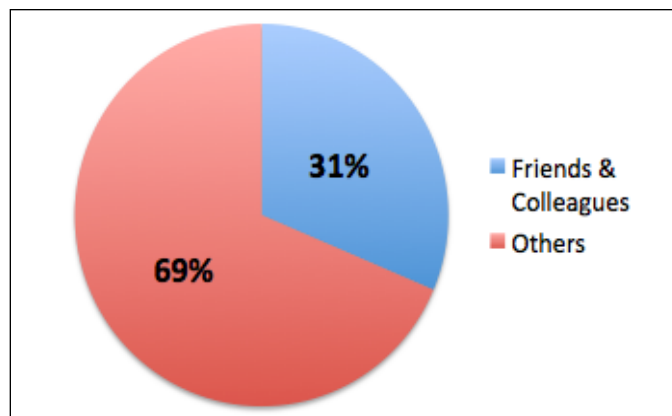


Figure 7-26: Percentage of friends and colleagues compared to other participants in the study

Initial frequency analysis revealed that the friends and colleagues comprised 31% of the total sample size of 188 participants (see Figure 7-26).

7.3 Demographic Profile of Participants

A total of 188 participants registered. Figure 7-27 depicts the demographic profile of all participants as well as the percentage of those who successfully completed all tasks.

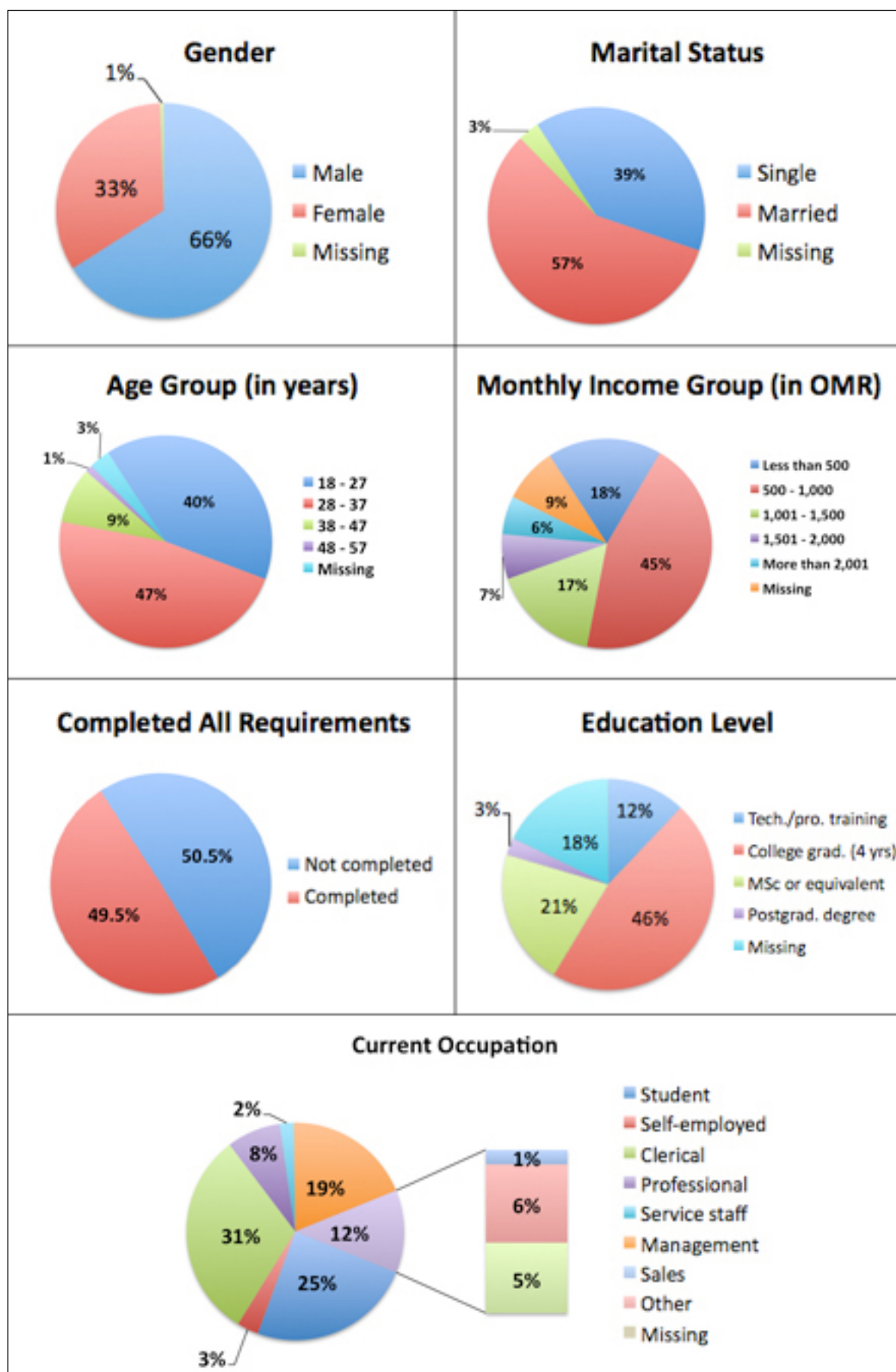


Figure 7-27: Demographic profile of all participants

These details are used in sections 7.3.1 and 7.5.2 to examine the relationship between the demographic characteristics (as independent variables) and the dependent variables (e.g., dropout rates and factors influencing online banking adoption).

It is also important to mention here that the recorded literacy rate in Oman (in 2007) for young males and females reached 99 and 98% respectively [241]. According to the same source, although there were almost 96% people with phones, only 10% people in Oman had an Internet connection in 2007. However, according to [242], Internet usage in Oman has increased radically to almost 41.7% as of June 2010.

7.3.1 Dropout Rates

A user who did not complete all tasks required in the study was considered as a “not completed case”, which meant that the user dropped out at some stage within the experiment. A total of 95 participants (50.5%) dropped out or did not complete all requirements (see Figure 7-27). These participants’ details were still valid and used to different analysis through this chapter since more than half of these participants completed the pre-questionnaire (more details presented in Table 7-16).

To examine the relationship between the participants’ demographic characteristics (independent variables), with the dropout rates (a dependent variable), a chi-square test for independence was used, as suggested by [155].

Variable	Value	df	Asymp. Sig. (2-sided)
Gender	0.605**	1	.437
Marital status	.023**	1	.880
Education level	15.342*	3	.002
Age group	2.131*	3	.546
Monthly income	5.080*	4	.279

* based on Pearson Chi-Square

** based on Continuity Correction (computed only for a 2x2 table)

Table 7-2: Chi-square test for independence summary results between demographic profile and dropout rates

The results in Table 7-2 show that only the education level scored significantly below 0.05. The relationship between education level and dropout rates is significant ($X^2(3) = 15.342$, $p < 0.05$). This suggests that the number of users who completed all tasks is affected by the level of education. To examine this fact, a close look to the chi-square test results produced

by SPSS 19 in Table 7-3 will help to clarify the relationship between education levels and the dropout rates.

Education Levels	Completed?		Total
	No (%)	Yes (%)	
Technical/Professional Training	19 (82.6%)	4 (17.4%)	23
College graduation (4 years)	43 (49.4%)	44 (50.6%)	87
Master degree or equivalent	17 (43.6%)	22 (56.4%)	39
Postgraduate degree	0 (0%)	5 (100%)	5
Total	79 (51.3%)	75 (48.7%)	154*

* Total participants reported their level of education was 154 (82%) out of 188 (see Figure 7-27)

Table 7-3: Cross tabulation between education level and dropout rates

The information depicted in Table 7-3 shows that users' failure rate to complete the tasks is very high (82.6%) for those who belong to the technical/professional training category. This rate decreases to 49.4% for users who have a college degree and to 43.6% for those with a Master degree or equivalent. Finally, the failure rate reached zero for those who had acquired a postgraduate degree.

Due to the small number of postgraduate degree participants who completed all tasks (5 cases only), the test was re-run after eliminating these cases to see if they influenced the relationship between education level and dropout rates. The outcome of the test was still significant ($X^2(2) = 9.928, p = 0.007$, see Appendix D1)

These figures reflect the fact that many of those who have not yet acquired a college degree may have not had the chance to try online banking prior to the pilot. In contrast, there is a high probability that those who completed a postgraduate degree have already started work with or are familiar with online banking. This can be further investigated by checking the relationship between users who have tried online banking before (online banking experienced users) and the dropout rate.

Figure 7-28 illustrates the relationship between experienced users and the dropout rates. The results show that only 39.5% of total users who had not tried online banking before completed all tasks, while 57.6% of users who had used online banking before were able to complete all tasks. The SPSS 19 results show that the relationship between online banking users (participants who have experience with online banking) and dropout rates is significant ($X^2(1) = 5.293, p < 0.05$, see Appendix D2)

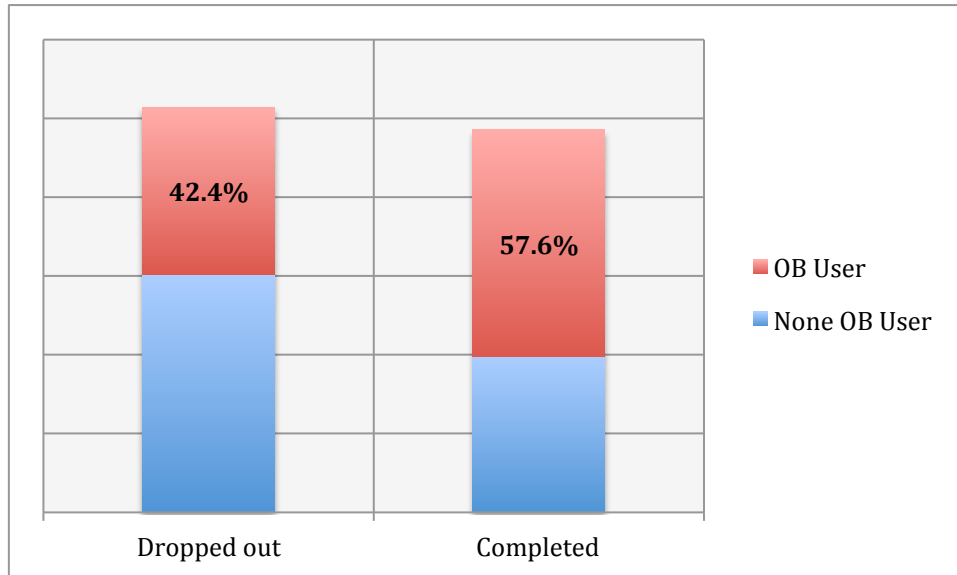


Figure 7-28: Relationship between online banking (OB) experienced users and dropout rates

7.3.2 Affects of Social Relationships on Dropout Rates

A crosstabulation analysis by SPSS 19 was used to check the affects of social relationships on dropout rates. Figure 7-29 illustrates the outcome of the analysis and shows that the number of participants from both groups, *friends and colleagues* and *others*, were almost similar. However, the number of people who dropped out was significantly different in both groups. While only 11 participants from friends and colleagues group dropped out, 84 participants dropped out from the other group.

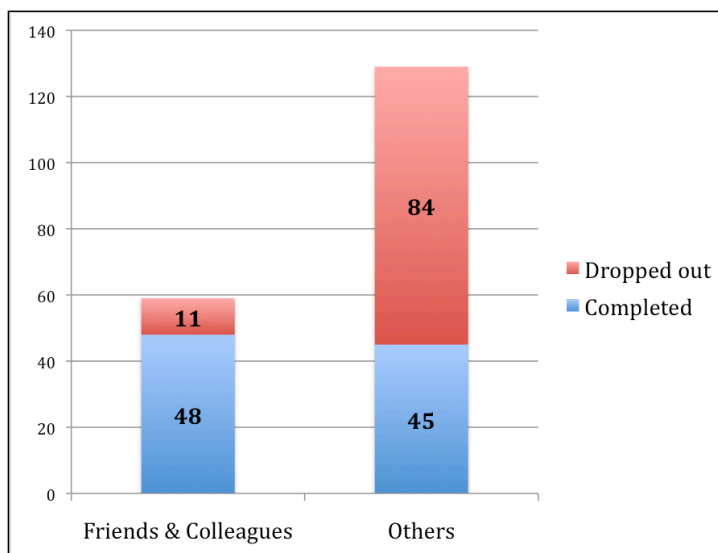


Figure 7-29: Relationship between social relationship and dropout rates

The chi-square test for independence indicated significant association between social relationships and dropout rates, $X^2(1, n=188) = 33.142, p < .001$, see Appendix D1.

7.4 Preliminary Test

Four preliminary tests were carried out in order to prepare the data for analysis. First, the questionnaire's variables were arranged into pre, post, and common. This was necessary to create data sets that could be processed by SPSS 19 for analysis and hypothesis testing. Second, the application logs were examined and arranged in data files. New variables, based on the existing variables, were introduced, and saved along with other variables on file. This process was important to prepare data for the subsequent data screening process.

After data were prepared in different files, they were checked for missing data. The process involved careful examination of each variable to determine how these missing data should be treated (i.e., ignore, replace, or delete). Finally, the data, especially the data from application logs, were checked for extreme scores (outliers). The process involved setting up some limitations to the formula to ensure that all extraneous extreme scores were omitted while maintaining the outliers that existed for valid reasons.

7.4.1 Data Preparation

Two sets of data were collected from the application database. The first set came from the online questionnaires and the other set came from the logs, which recorded the users' interactions with the application. The following subsections discuss how each of these sets was analyzed.

7.4.1.1 Questionnaires

Both pre and post-questionnaire data were analyzed. Data from these questionnaires were extracted and placed in separate files. Nevertheless, data that identified the personality and the background of the participant (e.g., gender, age, prior Internet banking experience, Internet usage frequency, education level, and monthly income groupings) were treated as common variables and were, therefore, included in both data files (see Figure 7-30).

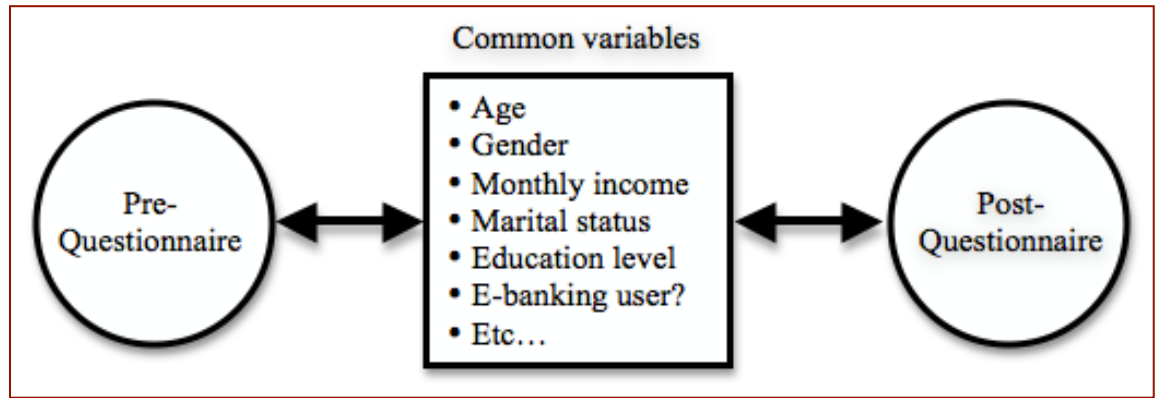


Figure 7-30: Common variables between the pre and post-questionnaire data files

7.4.1.2 Application logs

Application logs represented the interaction activities of the users and created a record for each link clicked on by the user. The row data in the logs table were recorded in a format that could not be used as variables in the analysis and, therefore, some transformation listed below was carried out to ensure data readiness for analysis.

To prepare the logs for analysis, first, a new variable was created to calculate the time each user spent on each page of the application (in seconds). The following formula was used to calculate these values:

$$TS_n = VT_{n+1} - VT_n$$

where TS is the time spent on each page (in seconds), VT is the page visit time (in Unix base time), and n is the record index in the logs table.

The formula calculated the time spent on any given page (TS_n) by subtracting the time the user visited this page (VT_n) from the time the user visited the next page (VT_{n+1}). There were 12,995 records in the log table and calculating TS_n manually was inefficient. Therefore, a script (see Appendix A) was designed to automate the calculation process and to store the TS_n values in a new field in the logs.

	Start task identifiers		Finish task identifiers		Intermediate pages
	Page	Query String	Page	Query String	
Task 1	profile.php	-	channels.php	mode=sent	2
Task 2	channels.php	-	account.php	mode=new	0
Task 3	transfer.php	-	transfer.php	activate=true	3
Task 4	transfer_page.php	bn_id=	account.php	acc_no=	1
Task 5	transfer.php	-	transfer.php	activate=true	6

Table 7-4: The 5 tasks identifiers

Next, a list of task identifiers was created to calculate the overall time a user spent on each task (see Table 7-4). This process was vital to determine how much time each user spent doing each task, which, in turn, could help identify the tasks that were not user friendly or that were hard to complete.

After these identifiers had been established, another script calculated the time each user spent on each task (see Appendix A). The following formula was used to calculate the time spent (TS) for each task and the total time spent (TS_t) for all 5 tasks per user:

$$\sum_{n=1}^i (TS_{n+1} - TS_n)$$

where *TS* is the time spent on each page (in seconds), *i* is the pages count for a given task, and *n* is the page index. When the outcome of this formula is equal to zero, the user did not complete the task.

7.4.2 Data Screening

SPSS 19 was used to check data accuracy and validity. This was an important phase before analyzing the data. The results of descriptive statistics showed no errors in the data gathered from questionnaires. The averages were normal for all variables of both questionnaires (i.e., the pre-questionnaire and post-questionnaire). The minimums and maximums were both within the expected range for each set of questions. The questionnaire data screening analysis is presented in Appendix C.

The data gathered from database logs' tables, however, showed some outliers and extreme points. The following subsections discuss these issues in more detail along with procedures followed to deal with the missing data values from both questionnaires and logs.

7.4.2.1 Missing data

Researchers [155, 243, 244] categorized missing data based on their characteristics into three categories: missing completely at random (MCAR), missing at random (MAR), and missing not at random (MNAR). MCAR happens when “subjects who have missing data are a random subset of the complete sample of subjects” [245]. Thus, the probability of an observation being missing does not depend on the information that is observed or not observed, and the cause of “missingness” is completely random. With data being MAR, the

“missingness” may depend on the information that is observed but it is independent of information that is not observed. MNAR, on the other hand, occurs when “missingness” depends on both observed and unobserved information. MCAR and MAR can be ignored while the MNAR cannot [155, 243, 244] because MNAR usually reflects a systematic pattern and data are not missing randomly. Tabachnick and Fidell argued that if the “missingness” rate is lower than 5%, then the missing data could be ignored without any further analysis [243]. Therefore, the SPSS 19 statistical software package was used to identify the percentage and pattern of the missing data for the pre-questionnaire and post-questionnaire (Appendix C).

Variables	N = 188		
	Valid	Missing	%
How often do you make use of Internet banking service?	119	69	36.7
With how many banks do you do your Internet banking services?	114	74	39.4
Which is your highest level of education?	154	34	18.1
What is your current occupation?	178	10	5.3
To which monthly income group you belong (in OMR)?	172	16	8.5

Table 7-5: Pre-questionnaire variables that incurred a “missingness” rate higher than 5%

The results showed that the “missingness” rate in the post-questionnaire was lower than 5% for all variables. By contrast, pre-questionnaire data revealed 5 variables that incurred a “missingness” rate higher than 5% (see Table 7-5). However, after a closer look at these variables, only two variables were truly missing.

The first 2 variables in Table 7-5 were related to question 3 in Section A of the pre-questionnaire (see Appendix B), which asked the users if they made use of an Internet banking facility. All participants who selected “No” for that question were asked to ignore the following two questions (i.e., represented by the first two variables in Table 7-5) and proceed to section B. The 69 participants who did not answer these questions were those users who participated in the study without having online banking experience. These users’ data will be discussed in the next section.

The missing rate in the second question is higher, which means there were 5 more participants (i.e., 74 who did not answer the 2nd question and 69 who did not answer the 1st question in Table 7-5) who used online banking but preferred not to answer the 2nd question. However, 5 participants out of 188 incurred only a 2.7% “missingness” rate, which therefore, can be treated as MCAR and ignored.

The education level, on the other hand, was a question to be answered by all participants (a total of 188) and the “missingness” rate was 18.1% (i.e., higher than 5%, and therefore, not able to be ignored). Thus this variable is further analysed in section 7.4.2.2.

After a close look to the data file created in SPSS 19, it was found that 4 participants have ignored many consecutive questions presented in section C of the pre-questionnaire and also dropped out at that point. When these 4 cases were ignored for the last two variables in Table 7-5, the missingness rate for the variable “current occupation” dropped below 5% and therefore can be ignored. However, the “monthly income” variable still incurred 6.5% missingness rate even after these 4 cases were dropped. Therefore, further analysis is required for this variable and is presented in section 7.4.2.3.

7.4.2.2 Missing data – Education Level

In order to examine whether this happened randomly, the SPSS 19 option “Missing Value Analysis (MVA)” with “Crosstabulations of categorical and indicator variables” was used as suggested in [246]. This method helps identify the differences in missing values among categories.

Table 7-6 shows how the education level values were affected by other common variables (e.g., gender, marital status, current occupation, organization business area, and monthly income). For example, the number of missing values in the gender variable appeared to vary between male and female. 87.1% of male respondents reported their educational level while only 74.2% of female respondents did.

A more drastic difference can be noticed in marital status. Those who were single were much less likely to report their level of education compared than those who were married. Only 73.0% of the single respondents reported their education level, while the percentage of those who were married and reported levels of education was 90.7%.

Likewise, the age group variable had the same effect as seen in marital status. 24.0% of respondents who were 18 to 27 years old did not report their education level, while fewer from the age groups of 28 – 37 and 38 – 47 did not report their level of education (10.1% and 6.3% respectively). The age group of 48 to 57 years did not contain enough available data to be included.

Looking at the table for organization or business area, the missing values among categories do not appear to vary much. Whether someone’s organization was a banking and financial

service, a communication and utilities organization, an educational facility, or a service industry, it did not seem to affect whether data were missing for the level of education variable. While the low count categories were ignored, most missing values were in the range from 12.3% to 16.7%. The difference was minimal and likely due to chance.

Variables	Missing	Education Level (N=188)			
Gender	2	Count	%	Missing	% Missing
Female		46	74.2	16	25.8
Male		108	87.1	16	12.9
Marital Status	6	Count	%	Missing	% Missing
Single		54	73.0	20	27.0
Married		98	90.7	10	9.3
Age Group	6	Count	%	Missing	% Missing
18 to 27		57	76.0	18	24.0
28 to 37		80	89.9	9	10.1
38 to 47		15	93.8	1	6.3
48 to 57		1	50.0	1	50.0
Current Occupation	10	Count	%	Missing	% Missing
Student		30	65.2	16	34.8
Self-employed		5	83.3	1	16.7
Clerical		51	87.9	7	12.1
Professional		15	100.0	0	0.0
Service staff		3	75.0	1	25.0
Management		34	94.4	2	5.6
Sales		2	100.0	0	0.0
Other		8	72.7	3	27.3
Organization Business Area	24	Count	%	Missing	% Missing
Banking and financial services		25	89.3	3	10.7
Transport and distribution		1	100.0	0	0.0
Communication and utilities		13	86.7	2	13.3
Trade and commerce		11	100.0	0	0.0
Education		50	87.7	7	12.3
Service industry		15	83.3	3	16.7
Farming and agriculture		1	100.0	0	0.0
Self-employed		0	0.0	0	0.0
Other		24	72.7	9	27.3
Monthly Income (in OMR)	16	Count	%	Missing	% Missing
Less than 500		21	63.6	12	36.4
500 to 1,000		71	84.5	13	15.5
1,001 to 1,500		30	96.8	1	3.2
1,501 to 2,000		12	92.3	1	7.7
More than 2,001		11	100.0	0	0.0

Table 7-6: Crosstabulations of education level verses other common variables

Finally, monthly income seems to be the highest influencing variable on reporting the level of education. If a respondent had an income less than OMR 500, then a response for

education level was more likely to be missing. At least 92.3% of the respondents whose income was more than OMR 1,501 reported level of education. Moreover, 96.8% of respondents who fell into the monthly income group of OMR 1,001 – 1,500 reported their education level. On the other hand, this rate decreased dramatically with lower monthly incomes. Only 84.5% of respondents from the monthly income group of OMR 500 – 1,000 reported their education level while the highest “missingness” rate of education level recorded among all categories was 36.4%, which fell in the monthly income group of OMR 500 or less.

7.4.2.3 Missing data – Monthly Income Group

Missing Value Analysis (MVA) of SPSS 19 was used again to check the affects of the common variables on the monthly income group values. In this analysis, however, only 184 out of 188 participants records were used. The four records dropped represented the participants who failed to answer several consecutive questions from section C in the pre-questionnaire.

Table 7-7 presents the outcome of the MVA between monthly income groups and other common variables (e.g. gender, marital status, age group, and level of education). The results found matched the outcome from the MVA between education level the common variables. For example, male participants were more likely to report their monthly income than their female counterparts. That is, 96.0% of male respondents reported their monthly income while only 88.3% of female respondents did. Likewise, almost 98% of married respondents have reported their monthly income while only 86.5 of single respondents did.

Age group showed the most significant differences where younger participants were much less likely to report their monthly income than their older counterparts. For instance, 13.3% of respondents who belong to the age group 18 to 27 years did not report their monthly income group. This percentage has declined drastically to 2.2% for the participants who belong to the age group 28 to 37 years. Furthermore, all participants who are 38 years or more reported their monthly income group.

Looking at the table for current occupation, only students groups recorded missing values of 19.6% in the monthly income group variable. All other participants have reported the group of monthly income they belong to.

Finally, the missing values for both organization business area and education level did not show a specific pattern that can be reported and therefore the missingness incurred can be treated as MCAR.

Variables	Missing	Monthly Income Group (N=184*)			
Gender	0	Count	%	Missing	% Missing
Female		53	88.3	7	11.7
Male		119	96.0	5	4.0
Marital Status	2	Count	%	Missing	% Missing
Single		64	86.5	10	13.5
Married		106	98.1	2	1.9
Age Group	2	Count	%	Missing	% Missing
18 to 27		65	86.7	10	13.3
28 to 37		87	97.8	2	2.2
38 to 47		16	100.0	0	0.0
48 to 57		2	100.0	0	0.0
Current Occupation	6	Count	%	Missing	% Missing
Student		37	80.4	9	19.6
Self-employed		6	100.0	0	0.0
Clerical		58	100.0	0	0.0
Professional		15	100.0	0	0.0
Service staff		4	100.0	0	0.0
Management		36	100.0	0	0.0
Sales		2	100.0	0	0.0
Other		11	100.0	0	0.0
Organization Business Area	20	Count	%	Missing	% Missing
Banking and financial services		25	89.3	3	10.7
Transport and distribution		1	100.0	0	0.0
Communication and utilities		13	86.7	2	13.3
Trade and commerce		11	100.0	0	0.0
Education		50	87.7	7	12.3
Service industry		15	83.3	3	16.7
Farming and agriculture		1	100.0	0	0.0
Self-employed		0	0.0	0	0.0
Other		24	72.7	9	27.3
Level of Education	30	Count	%	Missing	% Missing
Technical/professional training		23	100.0	0	0.0
College graduate (4 years)		79	90.8	8	9.2
Master degree or equivalent		38	97.4	1	2.6
Postgraduate degree		5	100.0	0	0.0

* Four cases (participants) were dropped from the total number because they did not complete the whole section of the pre-questionnaire that has these variables

Table 7-7: Crosstabulations of monthly income group verses other common variables

7.4.2.4 Outliers

According to [247], an outlier is an observation that is numerically distant from the rest of the observations. It is also simply referred to as “the values within the data that are well above or well below the majority of other cases” [155]. Outliers can be identified using different techniques. Assessing normality of a distribution is one way to identify outliers. Gravetter [248] defined normal distribution as a symmetrical, bell-shaped curve, which has the greatest frequency of scores in the middle, with smaller frequencies towards the extremes.

The data that could be checked for normality in this study were the data retrieved from the log table since they comprised the only data set that contained continuous variables (e.g., the time the user spent on each task in seconds). The rest of the data collected from the questionnaires could not be tested for normality, as all variables involved were discrete rather than continuous.

In order to test the normality and to check for outliers, the option “Explore” in SPSS 19 was used. The results revealed some extreme points and abnormal figures (see Table 7-8).

Tasks	Time Spent (in seconds), n=87				
Task 1: Registration & mobile auth.	M	5% Trim. M	Median	Min.	Max.
a. Create a profile	7978.74	1594.9	80.00	18	221401
b. Authenticate mobile number	3453.75	138.72	96.00	18	284876
Task 2: Auth. channel	M	TM*	Median	Min.	Max.
a. Select an auth. channel	66.25	55.60	41.00	8	380
Task 3: Beneficiary account	M	TM*	Median	Min.	Max.
a. Open accounts page	3980.15	72.42	40.00	6	333428
b. Create an account	71.66	57.16	44.00	14	766
c. Activate the account	266.02	162.50	103.00	21	5775
Task 4: Money transfer	M	TM*	Median	Min.	Max.
a. Fill transfer details	6940.79	38.48	29.00	7	577486
b. Confirm the transfer	5923.29	24.48	20.00	8	512243
Task 5: Alternative channel	M	TM*	Median	Min.	Max.
a. Open accounts page	37886.68	108.15	63.00	5	3280413
b. Create a new account	67.78	60.63	53.00	0	399
c. Open activation page	966.97	27.21	16.00	3	80939
d. Switch to alternative channel	12.44	11.13	7.00	2	74
e. Activate the account	5691.41	82.77	62.00	19	318568

Table 7-8: Descriptive statistics for the raw data from logs

Table 7-8 shows how the data are distributed randomly without forming a specific pattern. This is usually caused by high numbers of extreme scores in the data and this can be noted

well in the table. For example, the maximum time one user spent doing the sub-task 5-a was 3,280,413 seconds (about one month and a week's time). This is clearly not a realistic figure. The reason behind such an extreme score could have been that the user left the application in the middle of Task 5 and returned after almost 5 weeks to complete the work. This outlier negatively affected the means of all task scores.

Similarly, the 5% trimmed mean (TM) on the table, in most of the tasks, shows significant differences, compared to the normal means (M). This is because the 5% trimmed mean ignores 5% of the data from each side. The significant change in the TM means that those dropped data were extreme and had a major influence on the normal data means.

Although the extreme outliers that influenced the normal means (M) in this study could be removed to correct the analysis, other outliers were valid and existed for a reason. A user might have been working on a specific task and suddenly got lost and was unable to continue fulfilling the requirements of that task. The user would then try to redo the task. A third and fourth try, which required extra time, might have been needed to go back to the task guide to read the instructions more carefully before the user was finally able to finish the task. The application, in this case, would count the time from the first try until the user successfully completed the requirements of that task.

Another user might have a very slow Internet connection. It would take more time to load pages, which would contribute towards the total time spent in each task. If the time the user needed to load each page exceeded a few seconds (e.g., more than 4 to 6 seconds per page), this could cumulatively have added up to more than a minute to complete one task, such as task 5 (i.e., with about 6 pages that needed to load several times in some cases).

Accordingly, to correct the data for further analysis, a number of seconds equal to 120 (2 minutes) was accepted as a maximum time needed to fulfil the requirements of each page. Thus, if the application recorded a time of less than 120 seconds, then this data was considered valid; otherwise, it was rejected and replaced with 0. Naturally, a user would not spend more than 2 minutes on a web page unless it was intensively asking for input with complex client-side validations. In this study, the most time-consuming page among the 5 tasks was the "profile.php" page at Task 1-a, which required the user to input the full name, primary mobile number, and alternative mobile number. Under normal conditions, this could be done in less than 15 to 20 seconds. The researcher believed that 120 seconds was sufficient for fulfilling the requirements of any page, taking into consideration unusual factors that might increase the average time needed for each page such as Internet

connection slowness, slow user typing, time taken to read information from the task guide, and validation errors.

After removal of the extreme scores, the “Explore” test of SPSS 19 was rerun accordingly. The results revealed better normality with minor outliers that were not considered extreme. The TM and M were close to each other in almost all tasks (see Table 7-9).

Tasks	Time Spent (in seconds), n=87				
Task 1: Registration & mobile auth.	M	TM*	Median	Min.	Max.
a. Create a profile	67.40	63.73	58.00	0	215
b. Authenticate mobile number	83.43	82.07	74.00	1	197
Task 2: Authentication channel	M	TM*	Median	Min.	Max.
a. Select an authentication channel	44.85	42.61	36.00	0	147
Task 3: Beneficiary account	M	TM*	Median	Min.	Max.
a. Open accounts page	43.31	39.95	37.00	6	217
b. Create an account	40.36	38.27	39.00	1	139
c. Activate the account	87.89	83.69	69.00	21	248
Task 4: Money transfer	M	TM*	Median	Min.	Max.
a. Fill transfer details	36.16	33.35	26.00	0	139
b. Confirm the transfer	23.95	20.80	19.00	8	124
Task 5: Alternative channel	M	TM*	Median	Min.	Max.
a. Open accounts page	67.57	61.50	46.00	4	249
b. Create a new account	61.80	57.37	52.00	0	230
c. Open activation page	24.85	20.60	14.00	0	202
d. Switch to alternative channel	12.44	11.13	7.00	2	74
e. Activate the account	74.17	69.55	59.50	19	238

* 5% Trimmed Mean

Table 7-9: Descriptive statistics of a clean version of logs data

The 0s that replaced the extreme scores recorded per web-page has caused the results in Table 7-9 to show 0 as the minimum completion-time for several sub-tasks. These 0s do not represent actual completion-time for these sub-tasks, but rather represent that there were extreme outliers that were rejected and replaced with 0s.

The only one 0 minimum completion-time represented in Table 7-8 (sub-task 5-b) might be due to one participant or more who started the task but did not complete it and closed the web-page. Such behaviour caused a missing task end-time and therefore is represented by 0.

Some of the tasks, in Table 7-9, comprised more than one web page that the user needed to visit in order to complete the whole task. For example, to complete task 1-b (i.e., authenticate mobile number), the user had to open the authentication page followed by

another window, which simulated a mobile phone that the user used to “read” or “send” SMS messages. Once the user read the message and copied the One Time Pin (OTP), that window could be closed and the user returned to the authentication page to submit the OTP. This, accordingly, increased the total time the user needed to complete a sub-task (i.e., given that each web page was allowed a maximum of 120 seconds of time, which made the total equal to the number of web pages multiplied by 120). Therefore, another condition was applied to eliminate extreme outliers that might not have been cleared in the first cleaning cycle. This condition was implemented by defining “missing values” in SPSS 19 for all variables that represented the sub-tasks. These definitions dropped any sub-task score that was more than 250 (i.e., the total time the user spent on each sub-task should not have been more than 250 seconds). Since all sub-tasks involved, at most, two web pages, no more than 240 seconds should have been spent for each sub-task per user (maximum value should not exceed 240). However, due to some unexpected behaviours noted from the logs, some users tended to open more than one version of the web page, which duplicated the entries in the log files, and therefore, doubled the calculated time spent for each sub-task. The 250-second limit per sub-task dropped all scores that were affected by such behaviour and, at the same time, ensured that people who suffered from slow Internet connections were still allowed a further 10 seconds on top of the given 240s for both pages.

7.4.3 Summary

The preliminary test carried out in this section was important to screen and prepare data for the analysis. Two sets of data were prepared: those that came from the questionnaires and the ones came from the application logs table. The former dataset was first divided into three categories: pre, post, and common. A data screening process using SPSS 19 was used to check these data for validity; making sure they were transferred into SPSS correctly for further analysis.

The application logs were then prepared and arranged into different variables to make the analysis feasible. SPSS 19 was used again to screen the data and eliminate possible extreme figures. Different formulae were used in section 7.4.1.2 to ensure data validity for usability analysis covered in section 7.6.1.

7.5 Factors Influencing Adoption of Online Banking

7.5.1 Demographic Variables Hypotheses

To investigate whether or not the demographic characteristics influenced the adoption of online banking in Oman, these characteristics were hypothesized as follows:

H_{1a}: Gender significantly influences customers' usage of online banking

H_{1b}: Marital status significantly influences customers' usage of online banking

H_{1c}: Education level significantly influences customers' usage of online banking

H_{1d}: Age significantly influences customers' usage of online banking

H_{1e}: Income significantly influences customers' usage of online banking

7.5.2 Hypotheses Testing – Demographic Variables

To investigate the effects of demographic characteristics on the adoption of online banking, the demographic variables (gender, marital status, education level, age group, and monthly income group) were compared between the online banking users and non-users. SPSS 19 was used to test the hypotheses drawn in section 7.5.1 for demographic variables (H_{1n}, n=a to e). Table 7-10 shows a brief summary of the chi-square test results.

Variable	Value	df	Asymp. Sig. (2-sided)	Hypothesis test result (<i>p-value</i> =0.05)
H _{1a} : Gender	8.015**	1	.005	Support H _{1a}
H _{1b} : Marital status	7.574**	1	.006	Support H _{1b}
H _{1c} : Education level	21.511*	3	.000	Support H _{1c}
H _{1d} : Age group	12.125*	3	.007	Support H _{1d}
H _{1e} : Monthly income	23.399*	4	.000	Support H _{1e}

* based on Pearson Chi-Square

** based on Continuity Correction (computed only for a 2x2 table)

Table 7-10: Chi-square test for independence summary results between demographic profile and attitude towards adopting online banking

Further analysis was conducted using cross tabulations to provide greater insight than single statistics of chi-square. Cross tabulations allow the display of joint distribution of two or more variables, and thus, to describe the distribution of two or more variables,

simultaneously [232]. The results from cross tabulation analysis are presented and briefly discussed in the following subsections.

7.5.2.1 Gender

In literature, there are many different arguments on gender and its direct impact on technology adoption. For example, [249] found men to be more concerned with achievement than women. Another study [250] stated that men may be more task-oriented (i.e., the accomplishment of a task that requires the use of technology [251]) than women. Other factors such as characteristics of system design, training, and documentation may also affect technology usage [151], which may manifest in differences among men and women's experiences [252].

Concerning this study, it can be noted from Figure 7-31 that 37% of female respondents used online banking services. This figure increased to 63% when considering male respondents. This confirms that males are more likely to adopt online banking than females. As chi-square test results suggested in Table 7-10, gender significantly impacted the adoption of online banking ($X^2(1) = 8.015, p < 0.01$) and these results confirmed the outcomes drawn by [253] and [254].

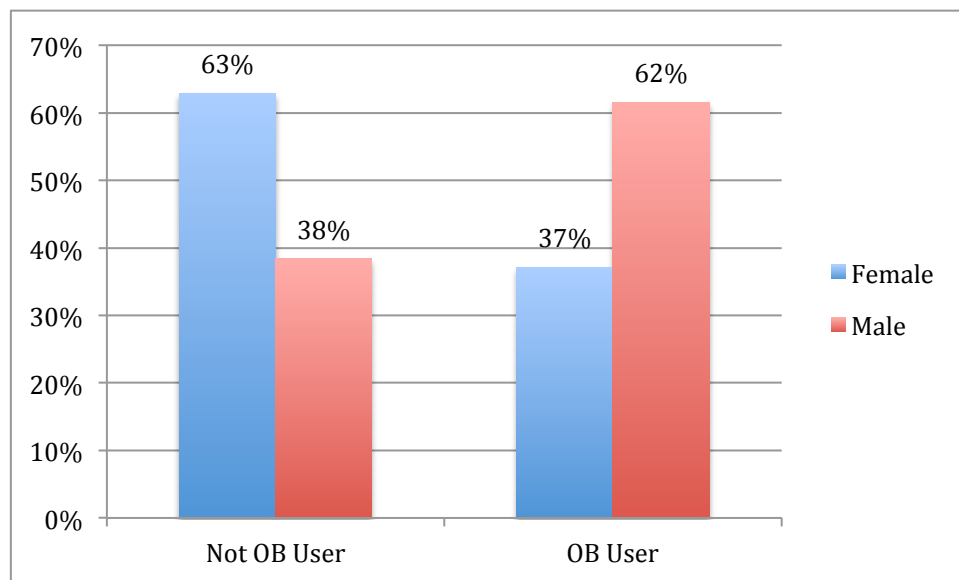


Figure 7-31: Relationship between gender and percentage of online banking (OB) experience

In Oman, the significant relationship between gender and online banking could also be attributed to the dominating Arabic and Islamic cultures. These cultures specify different roles for male and female in the society. For example, despite the public equality of rights and duties, males are primarily responsible for family's external and financial affairs, while

females are expected to take care of home and children. It is also socially unacceptable in Oman for females to attend Internet cafés. Hence, it is more appropriate for females in Oman to use the Internet only from home or work [255].

These results confirm the argument made by [256, 257] that gender is affected by social and cultural factors in the context of technology adoption.

7.5.2.2 Marital Status

Figure 7-32 shows that the adoption of online banking is significantly affected by the marital status of users ($X^2(1) = 7.574, p < 0.01$, see Table 7-10). While only 41% of single respondents used online banking, 63% of married respondents adopted online banking. This may have been a consequence of the fact that people in Oman get married in their 20s (i.e., based on 2003 figures: mean age at marriage in Oman is 24.8 for men and 28.1 for women [258]).

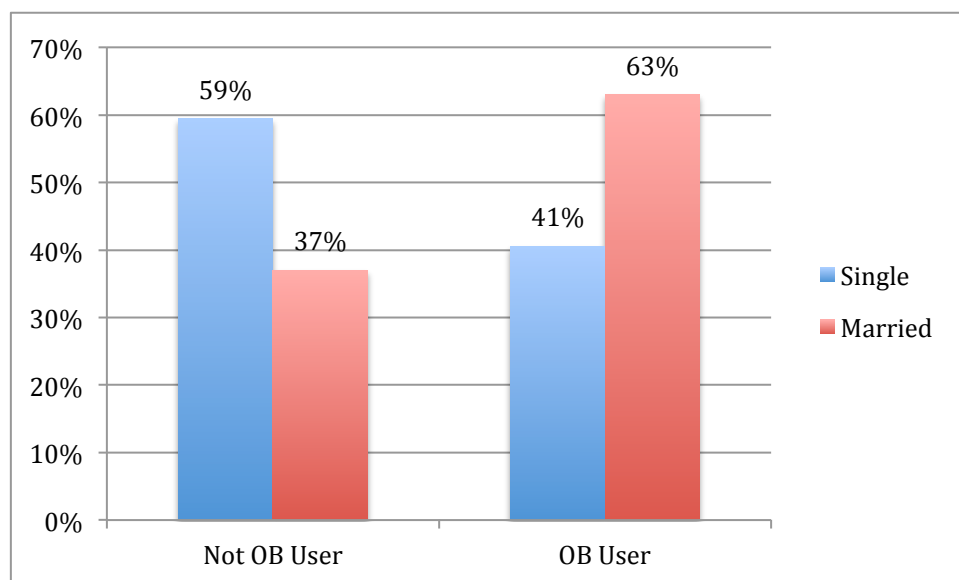


Figure 7-32: Relationship between marital status and percentage of online banking (OB)

It is common in Oman that people do not open bank accounts until they start paid employment. This leaves an average of 3 to 4 years for high-school diploma graduates or 1 to 2 years for college degree (4 years) graduates to have worked, and maybe utilized online banking services, before getting married.

7.5.2.3 Education level

Education level results depicted in Figure 7-33 show that the higher the education level achieved the greater the probability of the user adopting online banking. While only 36%

of technical/professional training graduates adopted online banking, 50% of college graduates had used online banking before. This percentage increased to 100% for those who had acquired a postgraduate degree. Thus a highly significant relationship existed between education level and adoption of online banking ($X^2(3) = 21.511, p < 0.001$, see Table 7-10).

The crosstab analysis was re-run to test the relationship significance without including the *Postgraduate degree* group since there is only a small number of participants recorded in this group (5 cases). The results again revealed a highly significant relationship between education level and adoption of online banking ($X^2(2) = 18.406, p < 0.001$, see Appendix D2).

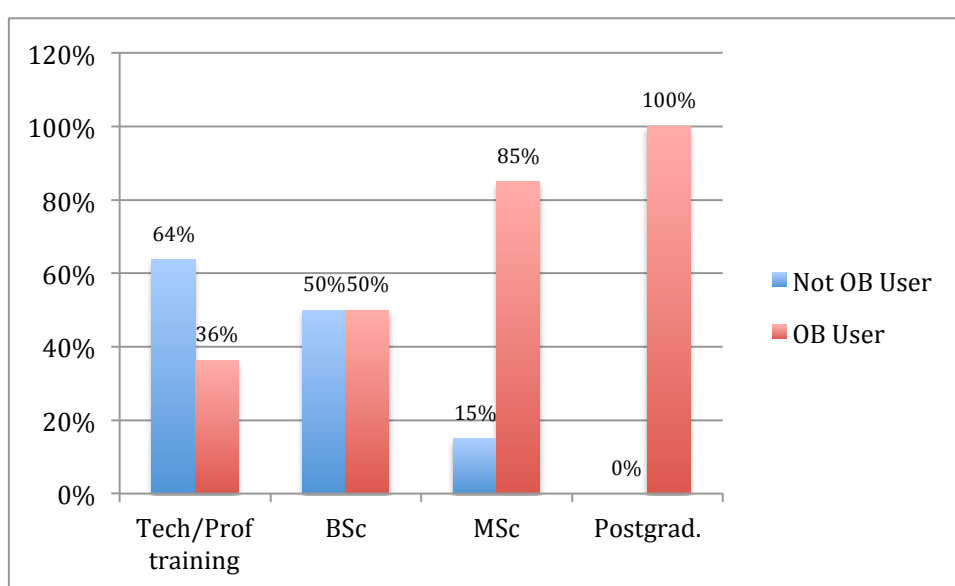


Figure 7-33: Relationship between education level and percentage of online banking (OB) users

These results were not surprising as online banking adoption usually increases with education level [259]. High-educated users are more likely to utilize online banking than their low-educated counterparts. They are usually more Internet literate [254] and involved with online services than uneducated people. This is especially true in Oman since computer literacy was first introduced to the primary education system in the academic year 1998/1999 [255]. This means that the first cohort of these students were in their final year of the higher education certificates by the time this experiment was conducted (therefore excluded).

7.5.2.4 Age group

Age group, like other demographic characteristics, showed significant impacts on the adoption of online banking ($X^2(3) = 12.125, p < 0.01$, see Table 7-10). The column chart results in Figure 7-34 justify this outcome.

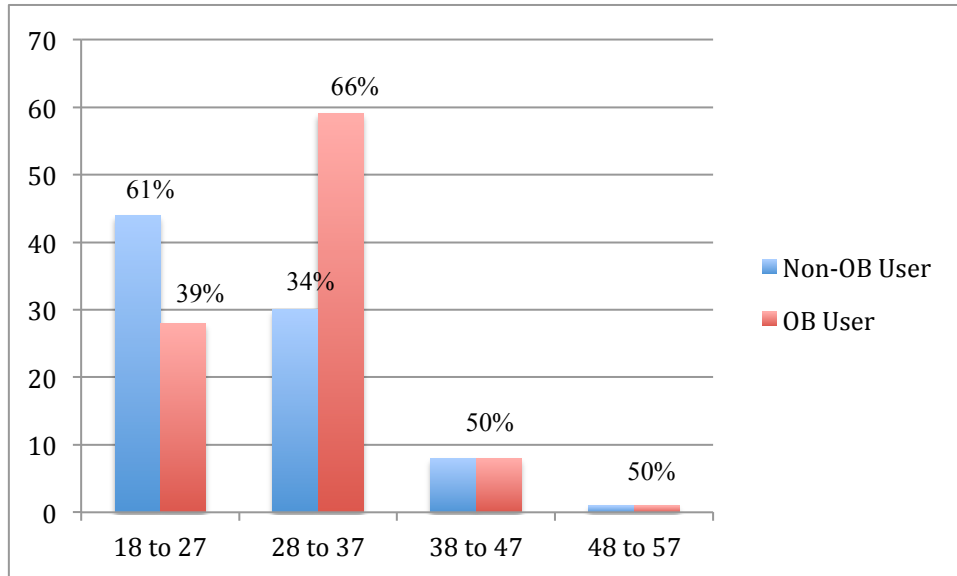


Figure 7-34: Relationship between age group and online banking (OB) users

Although the percentage of respondents who adopted online banking was the same (50%) for both age groups 38 to 47 and 48 to 57, the small number of respondents in both these groups (see Table 7-11) did not impact the overall relationship between age group and online banking experience. The percentage of online banking users increased from 39% for the age group between 18 to 27 years to 66% for the age group between 28 to 37 years, the same figure decreased to 50% for both age groups between 38 and 47 years and between 48 and 57 years (inclusive).

Age Group (in years)	Online banking user?		Total
	No	Yes	
18 to 27	44	28	72
28 to 37	30	59	89
38 to 47	8	8	16
48 to 57	1	1	2
Total	83	96	179

Table 7-11: Cross tabulation between age group and users with online banking (OB) experience

To test the effects of the small number of respondents who belong to the age groups 38 to 47 and 48 to 57, the test was re-run excluding these two groups. The results revealed an even higher significant relationship ($X^2(1) = 10.956, p = 0.001$, see Appendix D2).

The results revealed that younger people in Oman are less likely to adopt online banking than their older counterparts. This does not confirm the findings reported in [147] where there was no significant link between age and users' decision to adopt online banking in Saudi Arabia.

7.5.2.5 Monthly Income Group

Monthly income group was another demographic characteristic that showed a highly significant impact on online banking adoption ($X^2(4) = 23.399, p < 0.001$, see Table 7-10). Individuals with higher monthly income were more likely to adopt online banking.

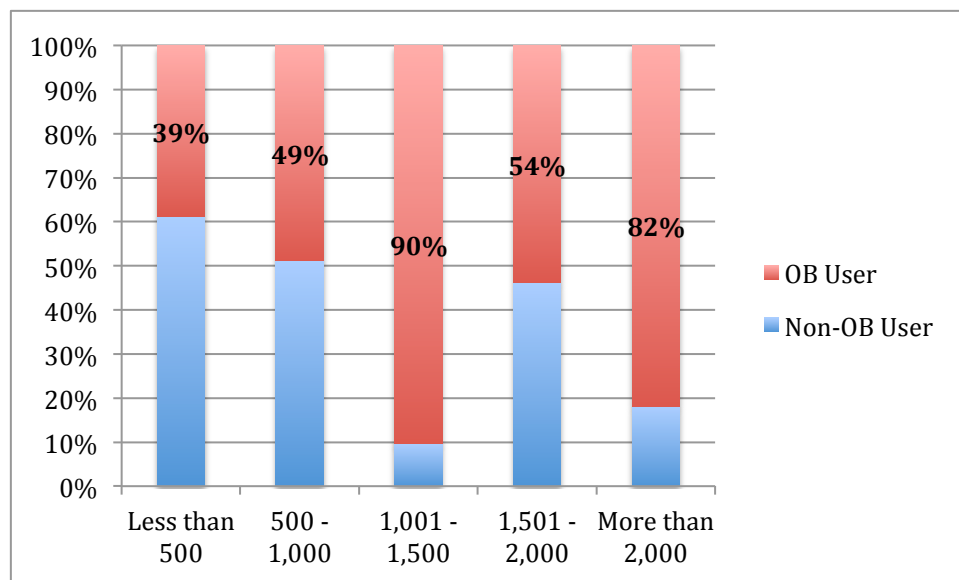


Figure 7-35: Relationship between monthly income group (in OMR) and percentage of online banking (OB) users

The stacked column chart in Figure 7-35 illustrates the positive relationship between the two variables. Only 39% of participants whose income was less than OMR 500 adopted online banking. This figure increased dramatically to the highest figure of 90% for participants who incurred a monthly income rate of more than OMR 1,000. The rate decreased to 54% for those receiving a monthly income between OMR 1,501 and 2,000 and increased again to 82% for the last group of those who have income of more than OMR 2,000.

The relatively small number of participants who belong to the last two monthly income groups might be the reason behind maintaining a highly significant relationship between monthly income group variable and online banking adoption. The first three groups that reflected a steady increase of adoption pattern were seen to be the ones that affected the

relationship because of the number of participants involved in these groups (see Table 7-12).

Monthly Income Group (in OMR)	Online banking user?		Total
	No	Yes	
Less than 500	19	12	31
500 – 1,000	43	41	84
1,001 – 1,500	3	28	31
1,501 – 2,000	6	7	13
More than 2,000	2	9	11
<i>Total</i>	73	97	170

Table 7-12: Cross tabulation between monthly income group and users with online banking (OB) experience

These results can be attributed to different reasons. Low-income people might have difficulties affording the cost of home computers and Internet services. In Oman, banks also charge monthly fees on accounts with balance less than OMR 100. Thus, low-income people might only maintain one account and not see any benefits managing it online.

There is a correlation between age and adoption, and also between income and adoption. Since income tends to rise the longer we work it could well be that these two factors are related in some way, but we do not have the data to confirm this.

7.5.3 External TAM Variables Hypotheses

The TAM variables used in this research are based on questions proposed in similar studies carried out by Padachi [153] and Sohail [154]. These questions were analysed and grouped into different related questions as mentioned in section 3.5.2. It was, therefore, important in this research to carry out a factor analysis to identify the interrelationship between these questions and to identify the most suitable related groupings possible. In this sense, and based on factor analysis reporting guidelines suggested by Pallant [155], the 14 items in Table 7-13 were subjected to principal components analysis (PCA) using SPSS 19. Prior to performing PCA, the suitability of data for factor analysis was assessed. Inspection of the correlation matrix revealed the presence of many coefficients of .3 and above. The Kaiser-Meyer-Olkin value was .9, which exceeds the recommended value of .6 [260], and Bartlett's Test of Sphericity [261] reached statistical significance ($p=.000$), supporting the factorability of the correlation matrix (more details in Table 7-13).

The principal components analysis shown in Table 7-13 revealed the presence of four components, explaining 50.9%, 9.5%, 6.3%, and 5.4% of the variance, respectively. These

results were initially rotated, using varimax rotation, to isolate more meaningful dimensions. The percentage of variance was reflected by a clear break after the second component in the screeplot (available along with Component Matrix table in Appendix D). All variables reported loadings scores more than 0.5.

Factors	Rotated factor loading	Percentage of variance
Ease of use		50.9%
a. Convenient way of doing bank transactions	.899	
b. Time saving	.851	
c. Ease of performing e-transaction	.789	
d. User friendly web site	.694	
e. Range of electronic services offered	.665	
Trust and relationship		9.5%
a. Bank response rate to queries	.821	
b. Ethical and professional conduct	.780	
c. Bank's policy to compensate for losses	.775	
d. Reliability of your banker	.584	
Ease of access		6.3%
a. Connection speed	.892	
b. Convenience to access the service	.716	
Security		5.4%
a. Length of Internet experience	.849	
b. Security of Internet transaction	.677	
c. Clear and understandable instructions	.519	
KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy	.900	
Bartlett's Test of Sphericity	Sig. .000	

Table 7-13: Summary of the 'Factor Analysis' for factors influencing adoption of online banking

The most significant factor was *ease of use*. The other influencing factors were *trust and relationship*, *ease of access*, and *security* (consistent with research reported in [153, 154] where trust and relationship and security were treated as external variables). The only differences between these results and the previous two studies were that the analysis carried out in this research found a significant relationship between *convenience* and *ease of use* variables and that these, therefore, were combined in one component, named 'perceived ease of use'.

Based on the preceding factor analysis, the three factors selected as external variables were *trust and relationship*, *ease of access*, and *security*. The TAM internal variables relationships such as $PEU \rightarrow PU$, $PEU/PU \rightarrow Attitudes$, $Attitudes/PU \rightarrow Intention$, were not addressed as they are out of the scope of this research. However, the results of other similar studies were reported instead.

Based on the literature review of studies on the same area (see sections 3.5.2.1, 3.5.2.1 and 3.5.2.3), it becomes necessary to formulate the research hypotheses for external variables as follow:

H_{1f}: Trust and relationship has a positive effect on Perceived Ease of Use (PEU)

H_{1g}: Ease of access has a positive effect on Perceived Ease of Use (PEU)

H_{1h}: Security has a positive effect on Perceived Ease of Use (PEU)

The measurement model for this study based on TAM can therefore be represented by Figure 7-36 below:

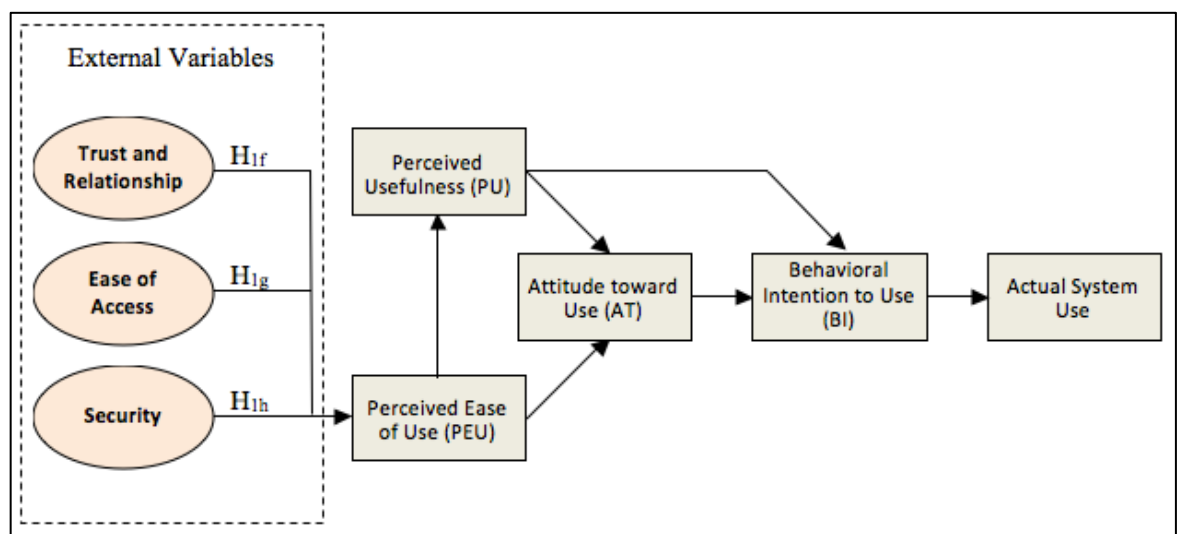


Figure 7-36: The measurement model of the study based on TAM

7.5.4 Hypotheses Testing – TAM External Variables

There are three non-demographic hypotheses (drawn in section 7.5.3):

H_{1f}: Trust and relationship has a positive effect on Perceived Ease of Use (PEU)

H_{1g}: Ease of access has a positive effect on Perceived Ease of Use (PEU)

H_{1h}: Security has a positive effect on Perceived Ease of Use (PEU)

According to Pallant [155], correlation analysis can be used to describe the strength and direction of the relationship between two variables (e.g. Security → PEU).

Based on the summary results of factor analysis in Table 7-13, four components were found to represent all 14 questions presented in section B of the pre-questionnaire: ease of

use, trust and relationship, ease of access, and security. Therefore, the mean scores for each of these components have to be calculated separately for each participant so it can be used in the correlation analysis.

To achieve this, SPSS 19 was used to compute the mean scores of all cases and put the results in a new four variables, which represents the four components identified by the factor analysis. These new variables data were then used to test the hypotheses using correlation technique in the following sections.

7.5.4.1 Correlation analysis

This section discusses the results relative to the correlation analysis of the hypothesis formed for the external variables of the proposed TAM. The relation of these variables with the PEU can be assessed by examining the correlation, which illustrates how strong is the relationships between the dependent and independent variables, and the (R^2) value, which shows the amount of variance explained by independent variables. SPSS 19 was used to test the correlation between the forgoing external variables of TAM and results of correlation are shown in Table 7-14.

		PEU	T&R	EoA	Security
Perceived ease of use	Pearson Correlation	1			
	Sig. (2-tailed)				
Trust and relationship	Pearson Correlation	.638**	1		
	Sig. (2-tailed)	.000			
Ease of access	Pearson Correlation	.690**	.508**	1	
	Sig. (2-tailed)	.000	.000		
Security	Pearson Correlation	.676**	.649**	.510**	1
	Sig. (2-tailed)	.000	.000	.000	

** Correlation is significant at the 0.01 level (2-tailed), $n=184$

Table 7-14: Correlation analysis results

All three variables showed significant statistical support. Trust and relationship, ease of access, and security were correlated significantly (i.e. correlation $> .6$) with the PEU. All relationships between these variables and PEU were investigated using the Pearson product-moment correlation coefficient. There was a strong, positive correlation between trust and relationship and PEU, $r = .638$, $n = 148$, $p < .001$ ($R^2 = 0.407$, Table 7-15), with high levels of trust and relationship associated with high levels of PEU. The highest correlated variable with the PEU was *ease of access* which $r = .690$, $n = 148$, $p < .001$ ($R^2 = 0.476$, Table 7-15).

Hypothesis	Relationship	R ²	Correlation	p-Value	Supported?
H _{1f}	T&R → PEU	0.407	0.638	0.000	Yes
H _{1g}	EoA → PEU	0.476	0.690	0.000	Yes
H _{1h}	Sec → PEU	0.457	0.676	0.000	Yes

Table 7-15: Assessment of the TAM external variables

The second highest correlated variable with the PEU was *security* $r = .676$, $n = 148$, $p < .001$ ($R^2 = 0.457$, Table 7-15). Thus, high levels of perceived security are associated with high levels of PEU.

The hypotheses were tested against the results in Table 7-15. All hypotheses proposed for the TAM external variables were supported.

7.5.5 Research Model

Based on the earlier results that cover theoretical background and analyses of different determinants of customer attitudes toward online banking acceptance, an extended TAM model for online banking acceptance in Oman was derived. Figure 7-37 illustrates this research model and the extended variables.

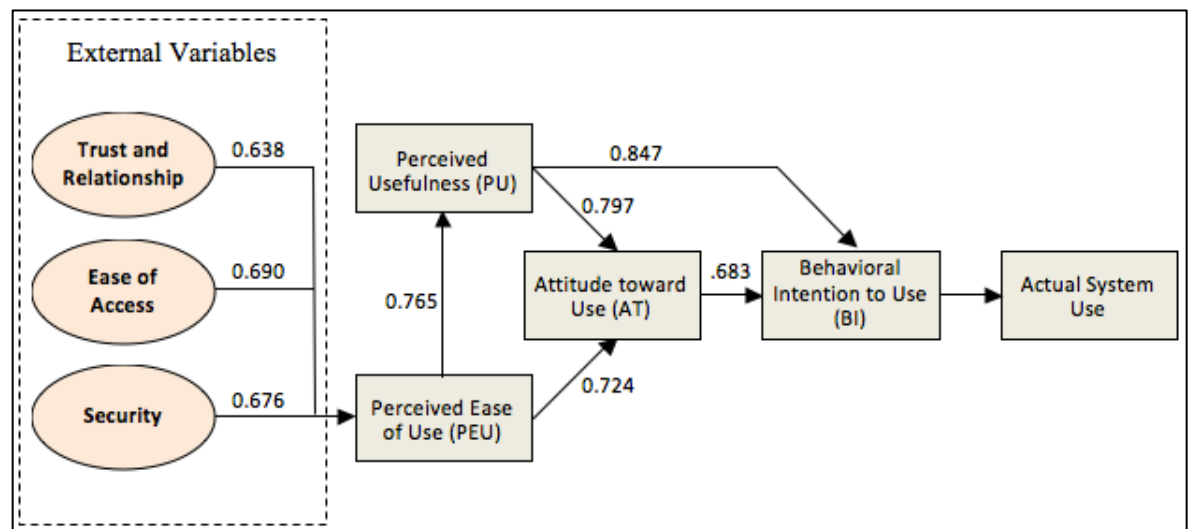


Figure 7-37: Extended TAM for online banking in Oman (Note: the results shown for internal TAM constructs were extracted from [147])

To summarize, all extended variables tested in the TAM model scored significant relationship with PEU (see Figure 7-37). These results confirm with a similar recent study conducted in Saudi Arabia by Al-Somali [147].

7.6 MCA – Usability and Acceptability

It is vital to mention that this study is concerned with the usability and acceptability of the multi-channel authentication (MCA) mechanism and is not concerned with the usability and acceptability of the prototype web-application. Therefore, the variables covered may well not be the same as the variables found in the literature for testing websites' overall usability and acceptability. Also it is important to mention that in some cases, where appropriate, only data from existing online banking users was used since participants who did not use conventional online banking could not meaningfully compare the two systems and were, therefore, unable to tell whether MCA was a better alternative or not.

The following subsections address the measurement of both usability and acceptability of the multi-channel authentication mechanism.

7.6.1 Measuring Usability of MCA

Usability in this research is measured using the three ISO metrics suggested by The International Organization for Standardization (ISO): *effectiveness*, *efficiency* and *satisfaction* [101] (defined in section 3.2). Effectiveness and efficiency of MCA were measured, in this study, using dependent variables such as completion-time and dropout rates that were collected from the application logs. Satisfaction, on the other hand, was measured based on respondents' feedback on a set of 5-option Likert scales in the online-questionnaire. Hence, the following hypotheses were tested:

H_{2a}: Multi-channel authentication mechanism is effective

H_{2b}: Multi-channel authentication mechanism is efficient

H_{2c}: Multi-channel authentication mechanism is satisfactory

The following subsections report on the tests of these three hypotheses individually, based on the three ISO usability metrics.

7.6.1.1 Effectiveness

Effectiveness, in the context of MCA usability evaluation, meant that the participants were able to complete all tasks effectively without dropping out at any point. The application logs maintained detailed information about all participants who registered in the

experiment. This information was useful to determine the completion rates for each of the 5 requested tasks.

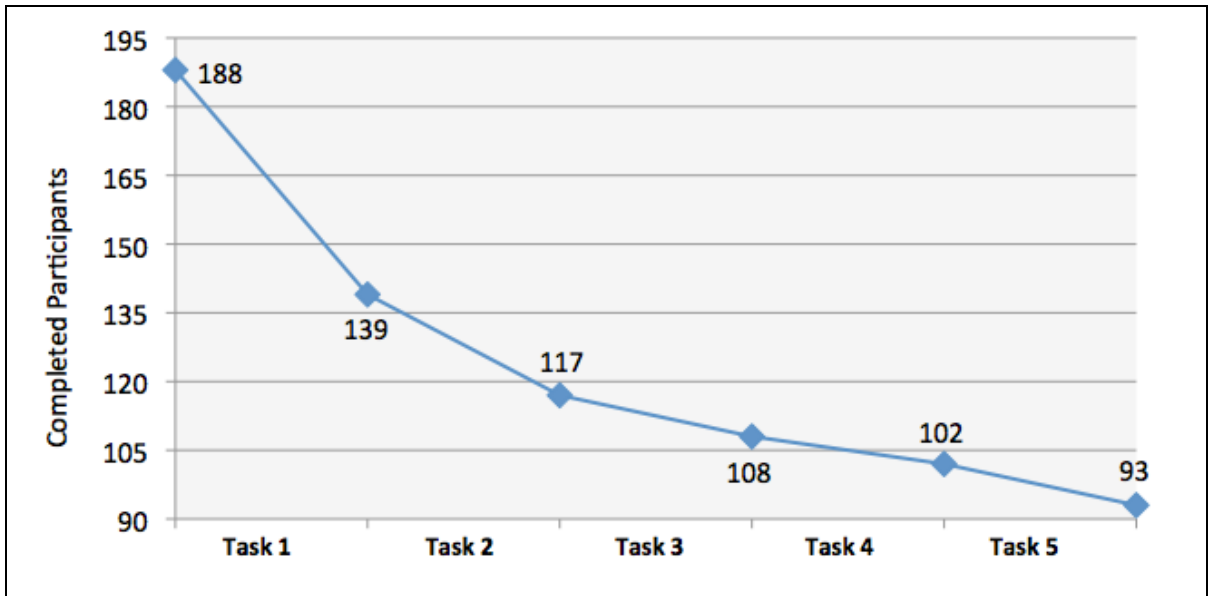


Figure 7-38: Completion task rate for all participants

Figure 7-38 illustrates the completion task rate for the 188 participants who tested the application. It can be noted that the major dropout happened in task 1 (registration and mobile authentication). This task consisted of two sub-tasks: creating a profile (T1_a) and authenticating the registered mobile number (T1_b). Based on the statistical frequency analysis of the application logs using SPSS 19, which is depicted in Table 7-16, 43 participants dropped out while creating their profile (i.e., entering their name and mobile number directly after they finished filling in the pre-questionnaire) and another 6 participants dropped out before they successfully authenticated their registered mobile number. The cumulative number of participants who dropped out before completing task 1 was 49 and this figure was the highest recorded drop out and accounted for 22.9% of the total participants of this study. These participants had not, at that point, tested the multi-channel authentication (MCA) mechanism, which entered the process after the user created and authenticated a beneficiary account using a mobile (task 3). Therefore, completion and dropout rates were ignored for the first two tasks. The independent variables that might have caused high dropout rates in these tasks were analyzed and discussed earlier in section 7.3.1.

Based on Table 7-16 figures, although the cumulative dropout rate was 37.8% for the first two tasks, the subsequent MCA related tasks (tasks 3, 4, and 5) recorded only a 12.7% dropout (T5_e cumulative dropout rate – T2_a cumulative dropout rate). Furthermore, there

was 2.7% to 3.1% dropout rate for sub-tasks T3_b, T4_a, and T5_b. These tasks were basic functions that did not directly involve MCA to accomplish.

Tasks	Completed N = 188		Dropped out		
Task 1: Registration & mobile authentication	N	%	N	%	C. ≈ %*
T1 _a . Create a profile	145	77.1	43	22.9	22.9
T1 _b . Authenticate mobile number	139	73.9	6	3.2	26.1
Task 2: Authentication channel	N	%	N	%	C. ≈ %*
T2 _a . Select an authentication channel	117	62.2	22	11.7	37.8
Task 3: Beneficiary account creation	N	%	N	%	C. ≈ %*
T3 _a . Open accounts page	115	61.2	2	1.1	38.8
T3 _b . Create an account	109	58.0	6	3.2	42.0
T3 _c . Activate the account	108	57.4	1	0.5	42.6
Task 4: Money transfer	N	%	N	%	C. ≈ %*
T4 _a . Fill transfer details	102	54.3	6	3.2	45.7
T4 _b . Confirm the transfer	102	54.3	0	0.0	45.7
Task 5: Alternative channel	N	%	N	%	C. ≈ %*
T5 _a . Open accounts page	100	53.2	2	1.1	46.8
T5 _b . Create a new account	95	50.5	5	2.7	49.5
T5 _c . Open activation page	93	49.5	2	1.1	50.5
T5 _d . Switch to alternative channel	93	49.5	0	0.0	50.5
T5 _e . Activate the account	93	49.5	0	0.0	50.5

* Rounded cumulative dropout percentage

Table 7-16: Sub-tasks completion and dropout rates

T3_b and T5_b were identical and requested users to create a beneficiary account by submitting a name and an account number using a basic form with text boxes and drop-down menus. T4_a, likewise, requested users to submit the amount of money they would like to transfer using a form with only two text boxes and a submit button. Therefore, it is unlikely that these users encountered usability issues or even made an effort to try to accomplish these simple tasks. The dropout rate of these sub-tasks (total of 8.9% dropout rate) could have been caused by other unknown external factors. This decreases the total dropout rates that were more likely to be caused by the MCA mechanism to 3.8% (12.7% - 8.9%). According to [262], a technology is effective as long as only less than 5% of its users will have technical issues. These technical issues could lead them to request support or to abandon the system, or hence, to dropout in the context of this study's experiment.

Since the analysis revealed that only 3.8% (less than 5%) of total participants dropped out before completing all tasks because of usability issues related to the MCA mechanism, the effectiveness hypothesis of MCA, therefore, was supported.

7.6.1.2 Efficiency

Efficiency is another usability metric defined by ISO. It can be evaluated by measuring the completion time of each task and sub-task separately. A system is considered efficient if users are able to accomplish tasks such as registration within a reasonable time. The response and loading time variables were neglected here since this study was testing the usability of the MCA mechanism rather than the web application design itself, as stated earlier in this section.

This study was comprised of 5 tasks, each of which had one to five sub-tasks. A sub-task, most of the time, is represented by one web document where users are instructed to enter details in a form provided within that page or extract useful information (e.g., OTP, SMS message, or password) that the user might need in other subsequent tasks. Nevertheless, there are few sub-tasks that request users to access more than one page at a time to fulfil the requirements. For example, T1_b (Task 1, sub-task b) was part of the registration and mobile authentication task. The main requirement of this sub-task was to authenticate the mobile number the user had to submit at T1_a (creating a profile). The user was instructed by the application to open a web page that showed a mobile phone icon. Next, the user was advised to click on the mobile phone icon to read the SMS message, which contained the OTP, in a new web page that simulated a mobile phone. Finally, the user would have to navigate through the simulator and copy the OTP, after which the simulator would be closed and the OTP would be entered in the text field that would automatically appear in the previous web page (the page that originally has the mobile phone icon).

To investigate the completion time for each sub-task, statistical frequency analysis in SPSS 19 was used to extract the mean and median of the time-spent variable. The results are depicted in Table 7-17.

The mean scores provided in Table 7-17 clearly show that most of the sub-tasks completion times were below one minute. The highest completion times recorded were for the three tasks T1_b, T3_c and T5_e which incurred mean scores of 83.4, 87.9 and 74.2 seconds respectively. This could be a result of the fact that the users are requested to open the mobile simulator in all these three tasks to read the SMS message, extract the OTP and then entering it into the screen for final submission. The change in mean score between the similar sub-tasks cannot be attributed to learning effects because both 2nd and 3rd tasks were similar, as mentioned, to the first task T1_b (task 1, sub-task b: authenticating mobile number). The only difference between T1_b and the other tasks was that the first task's OTP

was used to authenticate the mobile number, while the OTP of T3_c and T5_e was used to activate a beneficiary account. Therefore, if learning effect were the reason behind the decrease in the completion time mean score between T3_c and T5_e, then it would make more sense that T1_b would incur a longer completion time mean than both T3_c and T5_e, while it incurred only 83.4 seconds as shown in Table 7-17.

Tasks	Completion time (in seconds)	
	Mean	Median
Task 1: Registration & mobile authentication <i>Total</i>	168.32	132
T1 _a . Create a profile	67.4	58
T1 _b . Authenticate mobile number	83.43	74
Task 2: Authentication channel <i>Total</i>	44.85	36
T2 _a . Select an authentication channel	44.85	36
Task 3: Beneficiary account creation <i>Total</i>	209.36	175
T3 _a . Open accounts page	43.31	37
T3 _b . Create an account	40.36	39
T3 _c . Activate the account	87.89	69
Task 4: Money transfer <i>Total</i>	66.11	49
T4 _a . Fill transfer details	36.16	26
T4 _b . Confirm the transfer	23.95	19
Task 5: Alternative channel <i>Total</i>	160.21	122
T5 _a . Open accounts page	67.57	46
T5 _b . Create a new account	61.8	52
T5 _c . Open activation page	24.85	14
T5 _d . Switch to alternative channel	12.44	7
T5 _e . Activate the account	74.17	59.5

Table 7-17: Completion time of experiment tasks

Although completion-time in online-based experiments is not as reliable as other measurements used to test other hypotheses due to unforeseen environmental and personal factors (e.g., answering a phone call, discussing prompt issue with a colleague, sudden power shut-down, having a cup of coffee, etc...) which can intervene and affect the time spent on each task, it can still be made more reliable with the support of qualitative scales. For example, a supportive qualitative measurement of MCA efficiency was the mean score recorded for one of the post-questionnaire statements that asked the user to state how much he or she agrees or disagrees with the following statement (using 5-option Likert scale, 1 strong disagree to 5 strong agree):

I feel that MCA has just made things complicated and time-consuming

Based on the analysis results illustrated in Table 7-19, the mean score for this statement was 2.4 (Median = 2, Mode = 1). This mean score was the lowest score recorded among

other statements and it clearly shows that most of the users did not find MCA a time-consuming technology overall. However, the implementation of an on-screen simulated mobile phone could have affected these results where delivery delay of SMS messages and mobile network signal have been neglected.

For all the reasons covered in this section, the efficiency hypothesis of MCA was supported.

7.6.1.3 Effects of experience, gender and age on usability (efficiency)

The effects of participants' grouping existed in the independent variables such as experience (experienced users and inexperienced users), gender (male and female) and age (18-27, 28-37, 38-47, 48-57 and more than 57 years) was investigated to test for differences between these groups on overall tasks completion time.

Mann-Whitney U Test was used to test all variables where independent-sample t-test was used to confirm these results. The data in each variable had enough participants to ignore the normality distribution assumption of t-test except for gender which had lower than 30 female users (was ignored therefore).

The Mann-Whitney U Test results in Table 7-18 revealed no significant difference in the overall tasks completion time of all groups of variables tested (experience, gender and age group). All probability values (p) were higher than the significance level (.05). The results of the variables experience and age group were also confirmed by the outcome of the independent-sample t-test.

Variables	Groups	N	<i>p</i>	
			U Test	t-test
Experience	Online banking users	52	.552	.503
	Non-online banking users	33		
Gender	Female	28	.813	-
	Male	59		
Age Group (years)	18 to 27	34	.707	.681
	28 to 37	42		

Table 7-18: Results of Mann-Whitney U Test and independent-sample t-test for differences between experience, gender and age group on overall tasks completion time.

7.6.1.4 Satisfaction

Satisfaction is the most subjective part of usability [263] and it is necessary to ensure that users will continue to use the technology. In the context of this study, satisfaction was tested based on a set of Likert scales. These questions aligned with [98]’s model of the attributes of system acceptability (usability part of the model) as well as with the system usability scale (SUS), a usability scale by [233] that can be used for global assessments of systems usability.

To evaluate users’ satisfaction based on the questions asked in the questionnaire, it is first necessary to describe the mean scores for each of these questions.

Variables, scale: [Strong Disagree (1) to Strong Agree (5)]	Mean	Median	Mode
If multi-channel authentication (MCA) service is implemented by your bank, I would recommend it to others	4.3	5	5
I expected the MCA to work the way it did	4.2	4	4
I trust that MCA would protect me from Internet fraud and attacks	4.0	4	5
I feel that MCA has just made things complicated and time-consuming	2.4	2	1
With MCA, I am not worried about using public computers for Internet banking services	3.6	4	3
I would imagine that most people would learn to use this system very quickly	3.8	4	4
I found the alternative channel feature convenient when (in case) my primary channel (for example your mobile phone) is unavailable	4.3	5	5
I would prefer to use the alternative channel option than making a call-center/help-desk call	4.1	4	5

Table 7-19: Descriptive statistics of usability questions

Table 7-19 provides a descriptive analysis of the user usability questions. It can be noted that the lowest mean score was for the only negative-type question about MCA, ‘I feel that MCA has just made things complicated and time-consuming’ with an average mean score of 2.4 (median = 2, mode = 1). This indicates that participants found MCA to be effective and efficient to use; supporting the results drawn in sections 7.6.1.1 and 7.6.1.2.

In terms of security, although most of participants were neutral when answered the question ‘With MCA, I am not worried about using public computers for Internet banking services’ (mode = 3), they gave very positive responses to the question ‘I trust that MCA would protect me from Internet fraud and attacks’ with mean score of 4.0 (median = 4, mode = 5).

It is also clear that the top two variables that scored the highest mean of 4.3 were ‘If multi-channel authentication (MCA) service is implemented by your bank, I would recommend it

to others’ and ‘I found the alternative channel feature convenient when (in case) my primary channel is unavailable’. These figures indicate that online users found both the *multi-channel authentication mechanism* and the *emergency alternative authentication channel feature* usable and were satisfied. Moreover, the fact that users were prepared to market the idea and recommend it to their friends was an indication of their overall satisfaction and willingness to accept and adopt the MCA technology. Therefore, the satisfaction hypothesis of MCA was supported.

7.6.1.5 Effects of social relationships on usability (satisfaction)

To further validate this outcome, the effects of social relationships on satisfaction were also analyzed using the Mann-Whitney U Test.

Factors	F&C?*		Md**		Z	p	r***
	Yes	No	F&C	Oth.			
If MCA service is implemented by your bank, I would recommend it to others	43	36	5.0	4.0	-0.981	0.33	0.11
I expected the MCA to work the way it did	43	36	4.0	4.0	-0.363	0.72	0.04
I trust that MCA would protect me from Internet fraud and attacks	43	35	4.0	4.0	-0.293	0.77	0.03
I feel that MCA has just made things complicated and time-consuming	43	36	2.0	2.5	-1.172	0.24	0.13
With MCA, I am not worried about using public computers for Internet banking services	42	36	4.0	3.0	-0.545	0.59	0.06
I would imagine that most people would learn to use this system very quickly	43	36	4.0	4.0	-0.727	0.47	0.08
I found the alternative channel feature convenient when (in case) my primary channel (for example your mobile phone) is unavailable	41	36	5.0	4.5	-0.290	0.77	0.03
I would prefer to use the alternative channel option than making a call-center/help-desk call	43	36	4.0	4.0	-0.100	0.92	0.01

* Friends and colleagues?, ** Median

*** effect size was calculated manually based on the outcome of Mann-Whitney U Test. The formula used was: $r = |z| / \text{square root of } N [155]$ (N: total number of cases for both OB and non-OB users)

Table 7-20: Comparative evaluation of social relationships on satisfaction using Mann-W. U Test

Table 7-20 illustrates the outcome of the test. It can be clearly noticed that the *p* values are larger than .05, which indicates that there is no statistically significant difference in the satisfaction scores of friends and colleagues and other participants.

7.6.1.6 Effects of experience, gender and age on usability (satisfaction)

The outcome drawn in section 0 represented the results for all participants who completed all tasks and did the post-questionnaire. This includes experienced users who already adopted online banking services and the inexperienced users who are unfamiliar with online banking services. To investigate the effects of experience on users’ satisfaction

measured earlier in section 0, a Mann-Whitney U Test technique is used to compare the mean scores of usability variables for experienced and inexperienced online banking users. The same test was carried out to also check for effects of gender and age on usability (satisfaction). The alternative independent-sample t-test was not a suitable technique because the data violated some general assumptions for this test such as homogeneity of variance and normal distribution of sample (cannot be ignored since total number of inexperienced users were less than 30). The results of Mann-Whitney U Test are shown in Table 7-21.

Factors	N, Exp.?*		p	N, Gender		p	N, Age Group		p
	Yes	No		M	F		18-27	28-37	
If multi-channel authentication (MCA) service is implemented by your bank, I would recommend it to others	52	25	0.69	55	24	0.70	32	38	0.18
I expected the MCA to work the way it did	52	25	0.62	55	24	0.78	32	38	0.73
I trust that MCA would protect me from Internet fraud and attacks	52	24	0.15	54	24	0.57	32	38	0.90
I feel that MCA has just made things complicated and time-consuming	52	25	0.69	55	24	0.07	32	38	0.32
With MCA, I am not worried about using public computers for Internet banking services	51	25	0.72	54	24	0.18	32	37	0.72
I would imagine that most people would learn to use this system very quickly	52	25	0.41	55	24	0.61	32	38	0.94
I found the alternative channel feature convenient when (in case) my primary channel (for example your mobile phone) is unavailable	51	24	0.84	53	24	0.44	31	37	0.70
I would prefer to use the alternative channel option than making a call-center/help-desk call	52	25	0.15	55	24	0.84	32	38	0.91

* Experienced user?

Table 7-21: Comparative evaluation of experience, gender, and age on users' satisfaction (MCA) using Mann-Whitney U Test

All probability values (p) shown in Table 7-21 in the experience column were not less than or equal to .05, so the results were not significant. There were no statistically significant differences in the satisfaction scores of experienced users and non-experienced users.

The same results apply for gender and age group. None of these independent variables found to have significant differences in the satisfaction scores among their groups (male/female and 18-27/28-37 years). All probability values (p) for both gender and age were greater than the significance level of .05. Therefore, no further investigation of effect size was needed.

7.6.2 Measuring Acceptability of MCA

Acceptance of online banking technology was covered thoroughly in section 7.5. Both online users with and without online banking experience were involved in the study and all data was used to test the hypotheses. However, to investigate the user acceptability of the multi-channel authentication (MCA) mechanism, only participants with online banking experience were considered. It was not feasible to ask customers who had not utilized or tested online banking services before to give feedback on a new online banking technology. They did not have the required background experience on the existing technology on which to base their decisions and opinions on a new one.

Participants were asked to indicate how likely they would be to use different online banking services on an online banking system with and without multi-channel authentication (based on their existing experience with conventional online banking). To analyze these data, two statistical techniques available as suggested by [155]: paired-samples t-test and Wilcoxon Signed Rank Test. Both techniques are used when comparing the mean scores for one group of people based on two different conditions. In this case, the study compared the mean scores for online banking users' preferences when using a conventional online banking system and when using an online banking system with a multi-channel authentication mechanism. The same assumptions drawn for the independent-sample t-test and Mann-Whitney U Test discussed earlier in section 7.5.4 applied here for both techniques. While considering the violation of the normally distributed assumption due to the large sample size, this study tested the data using paired-samples t-test first and then confirmed the results with the Wilcoxon Signed Rank Test as presented in the subsequent sub-sections.

7.6.2.1 Paired-samples t-test

Table 7-22 shows a brief summary of the results of paired-samples t-test analysis by SPSS 19 for online users when using online banking systems with multi-channel authentication (OBMCA) and when using conventional online banking systems (COB) (more detailed results are provided in Appendix D).

Variables	<i>M*</i>		<i>t</i>	Sig. (2-tailed)	eta** squared
	OBMCA	COB			
1. Do inter account funds transfer	4.06	3.36	3.600	0.001	.146
2. Make payment to other personal account	4.18	2.89	6.424	0.000	.355
3. Make payment to other local bank account	4.17	2.99	6.434	0.000	.353
4. Transfer funds to credit card account	4.05	3.19	5.553	0.000	.289
5. Do foreign transfer	3.82	2.38	7.532	0.000	.431
6. Top-up mobile phones	4.07	2.61	8.291	0.000	.478
7. Order cheque books	3.79	3.32	2.509	0.014	.076
8. Stop lost ATM cards	3.99	3.42	2.626	0.010	.082
9. Stop lost credit cards	3.93	3.45	2.302	0.024	.066
10. Apply for a credit card limit change	3.87	2.97	4.489	0.000	.210
11. Request the issue of current acct. state.	4.39	3.73	3.872	0.000	.165
12. Setup standing order transactions	4.08	2.88	6.739	0.000	.380
13. Setup new account	3.81	2.73	4.871	0.000	.236
14. Apply for foreign currency accounts	3.59	2.88	3.233	0.002	.125
15. Apply for debit/credit card	3.86	2.83	5.373	0.000	.278
16. Apply for a loan	3.43	2.53	4.027	0.000	.180
17. Request telephone banking	3.86	2.84	4.809	0.000	.236

* *M*: Mean scores; OBMCA: Online banking with MC; COB: Conventional online banking (without MCA)

** eta squared was calculated manually based on the outcome of paired-samples *t*-test in Appendix D.

The formula used was: $t^2 / (t^2 + (N - 1))$

Table 7-22: Paired-samples *t*-test comparing online users' preferences for using online banking services on systems with MCA and without MCA

7.6.2.2 Discussion

The results show significant differences in users' preferences between OBMCA and COB in all of the services offered. The top five services which scored the highest magnitude of the MCA's effect were *make payment to other personal account*, *make payment to other local bank account*, *do foreign transfer*, *paying to top-up mobile phones* and *setup standing order transactions* with eta squared of .355, .353, .431, .478 and .380 respectively. These scores represent a substantial difference in users' preferences between OBMCA and COB (i.e., based on [264] guidelines that state an eta squared score above .14 represents a large effect). These five services were services that either participants might use on a daily basis or have security concerns using them via conventional online banking, unlike other services, such as ordering a chequebook, stopping a lost ATM card, applying for a loan, or requesting telephone banking. This indicates that participants were concerned about the services they required more frequently or those that involves money transfer to a foreign accounts or countries. This can also be supported by the fact that the least mean scored among all services was the 'Do foreign transfer' service. The lowest mean scores of this service in conventional online banking reflects the unwillingness of bank customers to utilize such service without improved authentication technology such as MCA.

7.6.2.3 Wilcoxon Signed Rank Test

Wilcoxon Signed Rank Test is a non-parametric alternative statistical technique to the paired-samples t-test and especially used for the data that are measured only at the ordinal (ranked) level. Similarly to the Mann-Whitney U Test, the normal distribution assumption is not required for this technique.

Variables	Z	Sig. (2-tailed)	Effect size r *
1. Do inter account funds transfer	-3.310	0.001	0.26
2. Make payment to other personal account	-5.144	0.000	0.41
3. Make payment to other local bank account	-5.049	0.000	0.40
4. Transfer funds to credit card account	-4.691	0.000	0.37
5. Do foreign transfer	-5.684	0.000	0.46
6. Top-up mobile phones	-5.849	0.000	0.47
7. Order cheque books	-2.401	0.016	0.19
8. Stop lost ATM cards	-2.216	0.027	0.18
9. Stop lost credit cards	-2.177	0.029	0.17
10. Apply for a credit card limit change	-4.063	0.000	0.32
11. Request the issue of current account statement	-3.479	0.001	0.28
12. Setup standing order transactions	-5.337	0.000	0.43
13. Setup new account	-4.163	0.000	0.33
14. Apply for foreign currency accounts	-3.043	0.002	0.24
15. Apply for debit/credit card	-4.320	0.000	0.35
16. Apply for a loan	-3.564	0.000	0.29
17. Request telephone banking	-4.214	0.000	0.34

* Effect size was calculated manually based on the outcome of Wilcoxon Signed Rank Test. The formula used was: $r = |z| / \text{square root of } N$ [155] (N: total number of cases for both OB and none-OB users)

Table 7-23: Wilcoxon Signed Rank Test comparing online users' preferences for using online banking services on systems with MCA and without MCA

7.6.2.4 Discussion

The results from Table 7-23 show significant differences in all users' preferences between OBMCA and COB in most of the services offered. This was identical to the results from the paired-samples t-test presented in Table 7-22. The top five variables that scored highest effect size (r) were *Make payment to other personal account*, *Make payment to other local bank account*, *Do foreign transfer*, *Top-up mobile phones* and *Setup standing order transactions* with effect size values of 0.41, 0.40, 0.46, 0.47 and 0.43 respectively. These results confirmed the results found earlier from paired-samples t-test.

The variables *Stop lost ATM cards* and *Stop lost credit cards* were among the variables that scored the lowest significance rates in both tests and this can be attributed to the fact that both of these services do not pose high risk to the account holder. They do not involve money transactions and therefore the majority of the participants did not mind using either

online banking with MCA or conventional online banking technologies to utilize such services online.

Overall, both tests confirmed that the participants in this study accepted and preferred to use online banking web-application with MCA than other conventional online banking authentication techniques for all 17 banking services listed in section B of the post-questionnaire (see Appendix B4).

7.6.3 Comparison with Other Studies

Table 7-24 summarizes the differences and matches between this research and Weir's study discussed in section 3.3.1.

	Weir's study 2010 [122]	This research
Demographics	<ul style="list-style-type: none"> • 141 participants from UK • 77 female and 64 male • 93 online banking users and 48 non-OB users 	<ul style="list-style-type: none"> • 188 participants from Oman • 62 female, 124 male and 2 missing • 99 online banking users, 86 non-OB users and 3 missing
Research methodology	<ul style="list-style-type: none"> • Controlled environment • OTPs were delivered to physical mobile phones given to users (Sony Ericsson K-700 model) via SMS 	<ul style="list-style-type: none"> • Uncontrolled environment • OTPs were delivered to a simulated on-screen mobile phone (Sony Ericsson 7-750 model) via SMS
Statistical techniques	<ul style="list-style-type: none"> • Parametric 	<ul style="list-style-type: none"> • Parametric confirmed by non-parametric
Findings		
Effectiveness	<ul style="list-style-type: none"> • Multi-channel authentication was the most effective (without no problems facing the participants) authentication method compared to other 2-factor authentication mechanisms 	<ul style="list-style-type: none"> • Multi-channel authentication was effective with a 3.8% dropout rate (<i>section 7.6.1.1</i>)
Efficiency	<ul style="list-style-type: none"> • Not measured 	<ul style="list-style-type: none"> • MCA was found efficient based on time-completion rates and usability questionnaire (<i>section 7.6.1.2</i>)
Satisfaction	<ul style="list-style-type: none"> • 2-factor authentication methods scored significantly higher than the 1-factor method for online banking authentication usability metrics used in the questionnaire overall 	<ul style="list-style-type: none"> • Multi-channel authentication method scored significantly higher than the conventional 1-factor/2-factors authentication methods for online banking (<i>section 0</i>)
Security	<ul style="list-style-type: none"> • The majority of participants were interested in the security benefits of OTP via secondary device or channel 	<ul style="list-style-type: none"> • The majority of participants trusted that MCA method would protect them from online fraud and attacks (<i>section 0</i>)
Age * Usability	<ul style="list-style-type: none"> • Younger participants scored significantly higher in terms of usability than their older counterparts 	<ul style="list-style-type: none"> • No significant differences found in the satisfaction scores among different age groups (<i>section 7.6.1.6</i>)
Experience effects	<ul style="list-style-type: none"> • Previous experience effected usability scores awarded to each authentication method tested 	<ul style="list-style-type: none"> • Previous experience had no effects on satisfaction of users towards MCA method (<i>section 7.6.1.6</i>) • Previous experience had no effects on efficiency of MCA method (<i>section 7.6.1.3</i>)

Table 7-24: Comparison of findings between this research and another study in the same area

7.7 Chapter Summary

This chapter has outlined the survey design and data collection techniques used in this study. It explained different preliminary analyses including data preparation and screening, which were necessary to provide valid and clean data for the hypothesis testing and analysis. More importantly, this chapter provided empirical results that support the theoretical evaluation of multi-channel authentication covered in section 5.4 of Chapter 5. The results supported all hypotheses. Details of the hypotheses testing results are illustrated in Table 7-25 below.

Hypotheses	Results
Online banking is acceptable to users in Oman	
H _{1a} : Gender significantly influences customers' usage of online banking	Supported
H _{1b} : Marital status significantly influences customers' usage of online banking	Supported
H _{1c} : Education level significantly influences customers' usage of online banking	Supported
H _{1d} : Age significantly influences customers' usage of online banking	Supported
H _{1e} : Income significantly influences customers' usage of online banking	Supported
H _{1f} : Trust & relationship has a positive effect on Perceived Ease of Use (PEU)	Supported
H _{1g} : Ease of access has a positive effect on Perceived Ease of Use (PEU)	Supported
H _{1h} : Security has a positive effect on Perceived Ease of Use (PEU)	Supported
Multi-channel Authentication is usable and acceptable to users in Oman	
H _{2a} : Multi-channel authentication is effective	Supported
H _{2b} : Multi-channel authentication is efficient	Supported
H _{2c} : Multi-channel authentication is satisfactory	Supported
H _{2d} : Multi-channel authentication is acceptable to users	Supported

Table 7-25: Hypotheses testing results

The adoption of online banking in Oman was found to be influenced by different demographic factors such as gender, marital status, education level, and income level as well as other external variables such as trust and relationship, ease of access, and security. All these factors had an impact on customers' decisions about whether or not to accept and adopt online banking in Oman. These results were found to be consistent with the results of similar studies by [5] and [4]. The former found that security is the major factor that affects people' decisions to adopt online banking in Oman. The latter, likewise, found security and other factors such as ease of access, and trust and relationship to be among the main drivers of online banking adoption. Both of these results were confirmed by the outcomes of this study.

The second set of hypotheses was proved by testing the usability and acceptability of the multi-channel authentication mechanism. Usability was tested based on the three usability metrics defined by the ISO standards: *effectiveness*, *efficiency* and *satisfaction*. For the MCA to be effective, at least 95% of the online banking customers should have been able to complete the tasks without making mistakes. Efficiency in the context of MCA meant that online banking customers were able to accomplish online banking transactions using the MCA mechanism in a reasonable time and with reasonable effort. Satisfaction, on the other hand, meant the customers felt satisfied about MCA, and therefore, the continuity of their usage of online banking with MCA and their willingness to recommend this service to others were ensured.

Acceptability of the MCA mechanism was the final factor to be evaluated in this chapter. It was necessary to narrow the data used to test acceptability to only those customers who had already experienced conventional online banking. This was important to eliminate any biased results that could have resulted if non-online banking customers were involved in the test to show their acceptance of the MCA mechanism without prior experience with online banking services. All the usability and acceptability hypotheses enumerated at the beginning of this chapter were supported.

The findings from usability measures were compared with another study published by Weir in 2010. The comparison revealed the areas where the two populations of UK and Oman differs or matches in terms of their perceptions of usability and security for online banking authentication methods.

Chapter 8

Conclusion

8.1 Introduction

The recent advances in communication and Internet technology have made online services more widely accessible. This has encouraged companies around the world, including the banking sector, to utilize online services for new business opportunities. Included in these new services were online banking services offered by banks. Online banking offered customers usable and accessible ways of doing banking from home or work. More recent technologies, such as 3G networks, have allowed customers to access their bank accounts and accomplish transaction requests using portable devices like PDAs, mobile phones, and notebooks.

On the other hand, these technological advances, along with the rich and sensitive information exchanged between the clients and their service providers have attracted Internet users with other agendas, honing their skills and developing new techniques to compromise other customers' accounts. Online banking services, as one of the targeted financial services, have implemented a number of different authentication mechanisms to withstand these attacks. The most recent authentication mechanisms utilize three basic authentication approaches: multilevel authentication, multi-channel authentication, and multi-factor authentication. None of these offers protection against more sophisticated attacks such as phishing and man-in-the-browser (MITB) attacks.

This study proposed a multi-channel authentication (MCA) mechanism that combines the strength of the three popular authentication approaches: multilevel, multi-channel, and multi-factor. These three authentication approaches were amalgamated to form an authentication mechanism that can better protect customers' accounts against most known attacks including phishing and MITB. A prototype web-application using MCA was designed and implemented to support the evaluation of the first part of the thesis statement: *"It is possible to design an authentication mechanism that uses multiple channels to resist attacks more effectively than most commonly used mechanisms"*. Different users were

asked to participate in the experiment to test the second part of the thesis statement: *“Such a mechanism will also be both usable and acceptable to users in Oman.”*

The following hypotheses in Table 8-1 were tested:

Hypotheses
Online banking is acceptable to users in Oman
H _{1a} : Gender significantly influences customers’ usage of online banking
H _{1b} : Marital status significantly influences customers’ usage of online banking
H _{1c} : Education level significantly influences customers’ usage of online banking
H _{1d} : Age significantly influences customers’ usage of online banking
H _{1e} : Income significantly influences customers’ usage of online banking
H _{1f} : Trust & relationship has a positive effect on Perceived Ease of Use (PEU)
H _{1g} : Ease of access has a positive effect on Perceived Ease of Use (PEU)
H _{1h} : Security has a positive effect on Perceived Ease of Use (PEU)
Multi-channel Authentication is usable and acceptable to users in Oman
H _{2a} : Multi-channel authentication is effective
H _{2b} : Multi-channel authentication is efficient
H _{2c} : Multi-channel authentication is satisfactory
H _{2d} : Multi-channel authentication is acceptable to users

Table 8-1: Hypotheses tested in this study

8.2 Research Objectives and Contributions

The general research topic addressed by this thesis was whether security of online banking users’ accounts could be increased while maintaining or also increasing usability. The specific thesis statement was *“It is possible to design an authentication mechanism that uses multiple channels to resist attacks more effectively than most commonly used mechanisms. Furthermore, such a mechanism will also be both usable and acceptable to users in Oman”*. The main research objectives defined in this thesis were as follows:

- Objective 1.** Review the most commonly used authentication classes, authentication mechanisms, and authentication attacks.
- Objective 2.** Review the usability and acceptability aspects of authentication mechanisms and the evaluation techniques used to assess them for new information technologies.
- Objective 3.** With respect to online banking, discuss some of the currently used authentication mechanisms and identify their weaknesses, showing how

they fail to protect customers' accounts against different attacks identified in objective 1.

Objective 4. Propose an authentication mechanism solution that addresses the security and usability problems identified and listed in objective 2. Theoretically evaluate the security of this solution and identify all features needed for implementation.

Objective 5. Empirically evaluate the new proposed mechanism with respect to usability and acceptability.

To meet the first objective, a thorough review of literature was undertaken. Six authentication classes were identified: knowledge-based, token-based, biometric-based, relationship-based, process-based, and location-based. These classes were compared to identify the advantages and disadvantages of each. They were then categorized with respect to implementation into four categories: single-factor, multi-factor, multilevel, and multilevel multi-channel authentication mechanisms. Finally, various attack methods that target these authentication mechanisms were discussed based on the communication component they target. These core communication components are the online service provider (OSP), the communication channel (CC), and the end user (EU).

To address the second objective, the current status of online banking applications (OBAs) was discussed. These applications were categorized, according to the service types offered to customers, into three categories: informational, local-transactional, and transactional. Each category needs a different authentication mechanism setup depending on the risk associated with the services offered. In order to evaluate mechanisms implemented in these categories, three case studies were discussed based on real OBAs. Further discussions identified the points of failure.

The third objective was met by proposing a new multilevel, multi-channel, and multi-factor authentication mechanism. Three design recommendations were suggested: user-defined secret keys, multi-language support, and key delivery encryption. These were intended to increase security and usability of the proposed solution. Security was evaluated based on threat-model analysis. Firstly, the attacks of the application were identified and categorized according to the STRIDE process by Microsoft into six categories: *spoofing*, *tampering*, *repudiation*, *information disclosure*, *denial of service*, *elevation of privilege*, and *DREAD*. An attack tree for the identified threats was constructed and the threats were evaluated

using a scenario-based evaluation process. Finally, risk mitigation and security controls were identified.

As part of the third objective, a prototype application was designed to test the proposed authentication mechanism empirically. This application simulated a real OBA and met the proposed solution guidelines. It further utilized an emergency authentication mechanism based on the relationship authentication class that can be triggered in case the secondary channel device (the mobile phone) is unavailable to complete the transaction. Finally, a list of other features and guidelines were included to complement and facilitate the actual implementation of the proposed multi-channel authentication (MCA) mechanism.

To meet the fourth objective, the usability and acceptability of the proposed solution were evaluated empirically by inviting users to test the prototype application. Two sets of online questionnaires and an indirect observation survey technique were used to collect feedback from the participants. The users were asked to complete 5 different tasks that provided data to support analysis. These data were analyzed to identify the factors affecting the adoption of online banking in Oman and to measure the usability and acceptability of the proposed MCA mechanism.

To conclude, the outcome of these analyses according to the hypotheses testing results are shown in Table 8-2:

Hypotheses	Results
Online banking is acceptable to users in Oman	
H _{1a} : Gender significantly influences customers' usage of online banking	Supported
H _{1b} : Marital status significantly influences customers' usage of online banking	Supported
H _{1c} : Education level significantly influences customers' usage of online banking	Supported
H _{1d} : Age significantly influences customers' usage of online banking	Supported
H _{1e} : Income significantly influences customers' usage of online banking	Supported
H _{1f} : Trust & relationship has a positive effect on Perceived Ease of Use (PEU)	Supported
H _{1g} : Ease of access has a positive effect on Perceived Ease of Use (PEU)	Supported
H _{1h} : Security has a positive effect on Perceived Ease of Use (PEU)	Supported
Multi-channel Authentication is usable and acceptable to users in Oman	
H _{2a} : Multi-channel authentication is effective	Supported
H _{2b} : Multi-channel authentication is efficient	Supported
H _{2c} : Multi-channel authentication is satisfactory	Supported
H _{2d} : Multi-channel authentication is acceptable to users	Supported

Table 8-2: Hypotheses testing results

8.3 Future Work

This thesis has contributed to usable, improved security by contributing both knowledge and practical applications of a MCA mechanism for users' authentication in online-distributed systems, specifically the online banking systems. However, it also raised new research directions. The following sections discuss these research opportunities in more detail.

8.3.1 More Usable Channels

Mobile devices have proved to be a usable complementary channel for online authentication. Other possible usable communication channels can also be used to support the MCA mechanism. These channels need to be tested for usability and security when used with other conventional authentication mechanisms.

SMS messages, on the other hand, can also be substituted with other services currently supported by mobile phones. Chatting software, in particular, such as What's Up for iPhones and BlackBerry's messenger are among most popular live messaging software nowadays. People can be allowed to set preferences on which these services (or any future live contact services) they prefer to receive their OTPs.

8.3.2 MCA for the Disabled

Although MCA proved usable and acceptable by users in Oman, disabled users might find it difficult to utilize it for their day-to-day financial transactions. The proposed MCA mechanism added another layer (mobile channel) of interactivity between users and online banking. This layer, in the context of online banking, needs further investigation alone and when combined with web-channel to see how it can be improved to meet the requirements of different disabilities. In this study, only people without disabilities were involved in testing the MCA solution.

8.3.3 MCA for Corporate Banking

The study has shown the MCA mechanism to address many of the current shortcomings of online banking. MCA can be extended to offer better usability and security to corporate online banking as well. For instance, involving multiple OTPs from different users to

authorize one transaction. This area has rarely been covered in the literature and investigating it would provide novel authentication solutions.

8.4 A Final Word

This research proposed a multi-channel authentication (MCA) mechanism that improves security of online banking systems while maintaining usability. The threat-analysis testing showed how the proposed MCA could protect users' accounts from most known attacks that other authentication mechanisms fail to address. A prototype online banking system using MCA was designed to test MCA's usability and acceptability. The majority of users who participated in the study felt that the MCA improved security. They also found the system usable and acceptable and indicated that they would use it and recommend it to others. These findings should be interesting to the banking sector if they want to improve their online banking systems. Too often banks focus on security while degrading usability. The guidelines and recommendations provided in this research will provide guidelines to banks wishing to offer more secure yet usable online banking.

Bibliography

- [1] "The Impact of Strong Authentication on Usability," RSA Security Inc. 2009 2009.
- [2] D. Chaffey, *Internet marketing : strategy, implementation and practice*. London: Financial Times, Prentice Hall, 2000.
- [3] S. Gaw and E. W. Felten, "Password management strategies for online accounts," presented at the Proceedings of the second symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2006.
- [4] I. Al-Sabbagh and A. Molla, "Adoption and Use of Internet Banking in the Sultanate of Oman: An Exploratory Study," *Journal of Internet Banking and Commerce*, vol. 9, 2004.
- [5] A. M. S. Khalfan, Y. S. Y. AlRefaei, and M. Al-Hajery, "Factors influencing the adoption of internet banking in Oman: a descriptive case study analysis," *Int. J. Financial Services Management*, vol. 1, p. 17, 2006.
- [6] (2009), *Electronic banking in the Sultanate of Oman*. Available: http://ecommercejournal.com/articles/15282_electronic_banking_in_the_sultanate_of_oman (2009, 09 December)
- [7] (2011), *Bank Muscat, About Us*. Available: <http://www.bankmuscat.com/en-us/AboutUs/Pages/default.aspx> (2011, 23 May)
- [8] K. Renaud, R. Cooper, and M. Al-Fairuz, "Support Architecture for Multi-Channel, Multi-Factor Authentication," presented at the IADIS International Conference, Algrave, Portugal, 2007.
- [9] D. Salomon, *Foundations of Computer Security*: Springer-Verlag, 2006.
- [10] (2010), *Internet 2009 in numbers*. Available: <http://royal.pingdom.com/2010/01/22/internet-2009-in-numbers/> (2010, May 24)
- [11] "Online Trends 2010," Centre for Retail Research, Research Report 2010.
- [12] M. E. Porter, "Strategy and the Internet," *Harv Bus Rev*, vol. 79, pp. 62-78, 164, Mar 2001.
- [13] , *CERT Statistics (Historical)*. Available: <http://www.cert.org/stats/> (2010, May 24)
- [14] W. Stallings, *Data and Computer Communications*, 8th ed.: Pearson Education International 2009.
- [15] W.-H. Yang and S.-P. Shieh, "Password authentication schemes with smart cards," *Computers & Security*, vol. 18, pp. 727-733, 1999.
- [16] K. Renaud, "Evaluating authentication mechanisms," in *Security and Usability: Designing Secure Systems That People Can Use*, ed: O'Reilly Media, 2005, pp. 103-128.
- [17] D. G. Firesmith and F. Consulting, "Engineering Security Requirements," *Journal of Object Technology*, vol. 2, pp. 53-68, 2003.
- [18] P. T. Leeson and C. J. Coyne, "The Economics of Computer Hacking," *Journal of Law, Economics, and Policy*, 2006.
- [19] "14th Annual CSI Computer Crime and Security Survey," *General Dynamics Advanced Information Systems*, December 2009.
- [20] B. Cashell, W. Jackson, M. Jickling, and B. Webel, "The Economic Impact of Cyber-Attacks," CRS Report for Congress 2004.
- [21] Entrust. *Risk-Based Authentication*. Available: <http://www.entrust.com/risk-based-authentication.htm> (2010, 11th April)

- [22] N. E. Hastings and D. F. Dodson, "Quantifying assurance of knowledge based authentication," in *ECIW 2004: The 3rd European Conference on Information Warfare and Security*, 2004.
- [23] Y. Chen and D. Liginlal, "A maximum entropy approach to feature selection in knowledge-based authentication," *Decis. Support Syst.*, vol. 46, pp. 388-398, 2008.
- [24] I. Jørstad and D. V. Thanh, "The Mobile Phone as Authentication Token," *Telenor ASA*, 2007 2007.
- [25] F. Piper, M. J. B. Robshaw, and S. Schwiderski-Grosche, *Identities and authentication*. Cheltenham: Edward Elgar, 2005.
- [26] "Password Management," T. G. o. t. H. K. S. A. Region, Ed., ed, 2008.
- [27] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*. CRC Press, Inc., 1996.
- [28] B. Schneier, "Customers, Passwords, and Web Sites," *IEEE Security and Privacy*, vol. 2, p. 88, 2004.
- [29] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords - Some Empirical Results," Computer Laboratory University of Cambridge 2001.
- [30] R. Sandhu and P. Samarati, "Authentication, access control, and audit," *ACM Comput. Surv.*, vol. 28, pp. 241-243, 1996.
- [31] C. Freund and D. Weinhold, "The Internet and International Trade in Services," *American Economic Review*, pp. 236 - 240, 2002.
- [32] ISO, "Identification cards -- Physical characteristics," vol. 7810, ed, 2003.
- [33] ISO, "Identification cards -- Recording technique," in *Tactile identifier mark* vol. 7811, ed, 2009.
- [34] ISO, "Information technology -- Identification cards -- Financial transaction cards," vol. 7813, ed, 2006.
- [35] ISO, "Identification cards -- Financial transaction cards -- Magnetic stripe data content for track 3," vol. 4909, ed, 2006.
- [36] G. Hancke, "A practical relay attack on ISO 14443 proximity cards," University of Cambridge Computer Laboratory 2005.
- [37] "HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements," Smart Card Alliance 2003.
- [38] ISO, "Identification cards -- Integrated circuit(s) cards with contacts," in *Physical characteristics* vol. 7816, ed, 1998.
- [39] R. Bolle and S. Pankanti, *Biometrics, Personal Identification in Networked Society: Personal Identification in Networked Society*. Kluwer Academic Publishers, 1998.
- [40] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, pp. 614-634, 2001.
- [41] K. Renaud, "Quantifying the quality of web authentication mechanisms: a usability perspective," *Journal of Web Engineering*, vol. 3, pp. 95-123, 2004.
- [42] S. T. Kent and L. I. Millett, *Who Goes There?: Authentication Technologies Through the Lens of Privacy*. National Academies Press, 2003.
- [43] J. D. Pierce, J. G. Wells, M. J. Warren, and D. R. Mackay, "A conceptual model for graphical authentication," in *1st Australian Information Security Management Conference*, Perth, Western Australia, 2003.
- [44] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 14, pp. 4-20, 2004.
- [45] C. Mills, *Biometrics: Back to Security Basics*. Book News Inc., 2002.
- [46] D. E. Denning and P. F. MacDoran, "Location-based authentication: Grounding cyberspace for better security," *Computer Fraud & Security*, vol. 1996, pp. 12-16, 1996.

- [47] J. Zhan and X. Fang, "Authentication Using Multi-level Social Networks," in *Knowledge Discovery, Knowledge Engineering and Knowledge Management*. vol. 128, A. Fred, J. L. G. Dietz, K. Liu, and J. Filipe, Eds., ed: Springer Berlin Heidelberg, 2011, pp. 35-49.
- [48] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: somebody you know," presented at the Proceedings of the 13th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2006.
- [49] S. U. Shah, Fazl-e-Hadi, and A. A. Minhas, "New Factor of Authentication: Something You Process," presented at the Proceedings of the 2009 International Conference on Future Computer and Communication, 2009.
- [50] J. Ashfield, D. Shroyer, and D. Brown, "Location-based Authentication of Mobile Device Transaction," US Patent, 2010.
- [51] (2010), *Open Proxy Server Statistics*. Available: <http://www.cert-in.org.in/open-proxy.htm> (2010, 14th April)
- [52] "X-Force 2009 Trend and Risk Report: Annual Review of 2009," IBM Security SolutionsFeb. 2010.
- [53] A. Kleusberg and R. B. Langley, "The Limitations of GPS," March/April 1990.
- [54] S. Goldthwaite, G. Crellin, and W. Graylin, "System and method for payment transaction authentication," US Patent US 2004/0019564 A1, Jan. 29, 2004, 2002.
- [55] M. J. Yates, S. M. Thompson, N. H. Edwards, M. M. Gifford, and D. J. McCartney, "Transaction Authentication," USA Patent, Apr. 1, 2004, 2003.
- [56] (2010), *identrica 2 factor authentication*. Available: <http://www.identrica.com/> (2010, 17 Jun)
- [57] (2003), *CellPhone Users Validation made easy*. Available: <http://www.saintlogin.com/html/cosa.html> (2010, 17 June)
- [58] (2011), *Security Procedure*. Available: http://www.lloydstsb.com/security/authentication_procedure.asp (2011, 16 May)
- [59] B. Schneier, "Attack trees," *Dr Dobbs Journal*, vol. 24, pp. 21-+, Dec 1999.
- [60] , *Hacking Attacks - How and Why*. Available: <http://www.crucialp.com/resources/tutorials/website-web-page-site-optimization/hacking-attacks-how-and-why.php> (2010, 15 April)
- [61] (2003), *Hackers Attack Al-Jazeera Website*. Available: <http://www.globalpolicy.org/component/content/article/168/36591.html> (2010, 15 April)
- [62] (2008), *Militants Attack Al-Arabiya Website*. Available: <http://www.ciol.com/News/News-Reports/Militants-attack-Al-Arabiya-website/131008111371/0/> (2010, 15 April)
- [63] R. Puri, "Bots & botnet: An overview," SANS InstituteAugust 08 2003.
- [64] R. Wash and J. K. MacKie-Mason, "Security when people matter: structuring incentives for user behavior," presented at the Proceedings of the ninth international conference on Electronic commerce, Minneapolis, MN, USA, 2007.
- [65] C. Patrikakis, M. Masikos, and O. Zouraraki, "Distributed Denial of Service Attacks," *The Internet Protocol Journal*, vol. 7, December 2004 2004.
- [66] (1996), *Panix Under Attack*. Available: <http://www.panix.com/press/synattack.html> (2010, April 15)
- [67] (2010), *Spanish police arrest masterminds of 'massive' botnet*. Available: <http://news.bbc.co.uk/1/hi/technology/8547453.stm> (2010, April 17)
- [68] C. K. Dimitriadis, "Analyzing the Security of Internet Banking Authentication Mechanisms," *Information Systems Control Journal*, vol. 3, 2007.
- [69] "10th CSI/FBI survey shows dramatic increase in unauthorized access," *IT Professional*, vol. 7, p. 5, 2005.

- [70] R. Saltzman and A. Sharabani, "Active Man in the Middle Attacks," IBM, Whitepaper February 27 2009.
- [71] (1999), *HTML Frames*. Available: <http://www.w3.org/TR/html4/present/frames.html> (2011, 28 April)
- [72] B. Glick. (2010), *Users remain the weakest link in the IT security chain*. Available: <http://www.computerweekly.com/blogs/editors-blog/2010/03/users-remain-the-weakest-link.html> (2010, April 17)
- [73] "Emerging Cyber Threats Report for 2009," GTISC, Georgia, US2009.
- [74] "Protection against Pharming and Phishing attacks," EasySolutions2009.
- [75] K. Poulsen. (2000), *Mitnick to lawmakers: People, phones and weakest links*. Available: <http://www.politechbot.com/p-00969.html>)
- [76] B. Schneier, *Secrets and Lies: Digital Security in a Networked World*: John Wiley & Sons, 2004.
- [77] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal*, vol. 19, pp. 122-131, 2001.
- [78] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, pp. 40-46, 1999.
- [79] B.-Y. Ng, A. Kankanhalli, and Y. Xu, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, vol. 46, pp. 815-825, 2009.
- [80] J. Grossklags, N. Christin, and J. Chuang, "Predicted and observed user behavior in the weakest-link security game," presented at the Proceedings of the 1st Conference on Usability, Psychology, and Security, San Francisco, California, 2008.
- [81] W. C. Summers and E. Bosworth, "Password policy: the good, the bad, and the ugly," presented at the Proceedings of the winter international symposium on Information and communication technologies, Cancun, Mexico, 2004.
- [82] "Phishing Activity Trends Report: 4th Quarter 2009," APWG2009.
- [83] A. Litan, "The War on Phishing Is Far From Over," Gartner Group2009.
- [84] , *The Pharming Guide - Whitepapers*. Available: <http://www.technicalinfo.net/papers/Pharming2.html> (2010, 17 May)
- [85] R. McMillan. (2008), *At Adobe's request, hackers nix 'clickjacking' talk*. Available: http://www.pcworld.idg.com.au/article/260609/adobe_request_hackers_nix_clickjacking_talk/ (2010, June 2)
- [86] "Making Sense Of Man-In-The-Browser," RSA, Whitepaper2009.
- [87] (2011), *Facebook f8 Changes Raise Five Serious Security and Privacy Concerns* Available: <http://www.bitdefender.com/news/facebook-f8-changes-raise-five-serious-security-and-privacy-concerns-2216.html> (2011, Oct 17)
- [88] C. Lorentzen, "User Perception and Performance of Authentication Procedures," Ph.D., School of Computing, Blekinge Institute of Technology, Karlskrona, 2011.
- [89] L. A. Jones, A. I. Ant, \#243, and J. B. Earp, "Towards understanding user perceptions of authentication technologies," presented at the Proceedings of the 2007 ACM workshop on Privacy in electronic society, Alexandria, Virginia, USA, 2007.
- [90] Nokia, "White Paper: Quality of Experience (QoE) of mobile services: Can it be measured and improved?," Nokia2004.
- [91] C. S. Weir, G. Douglas, M. Carruthers, and M. Jack, "User perceptions of security, convenience and usability for ebanking authentication tokens," *Computers & Security*, vol. 28, pp. 47-62, 2009.
- [92] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Computers & Security*, vol. 30, pp. 208-220, 2011.
- [93] B. Nanus and L. Farr, "Some cost contributors to large-scale programs," in *The Spring Joint Computer Conference*, 1964, p. 239.

- [94] N. Bevan, J. Kirakowski, and J. Maissel, "What is Usability?," in *The Fourth International Conference on Human-Computer Interaction (HCI International 1991)*, Stuttgart, Germany, 1991.
- [95] P. Kamthan, *Understanding Usability*, 2011.
- [96] D. A. Garvin, "What does Product Quality Really Mean?," *MIT Sloan Management Review*, vol. 26, p. 18, 1984.
- [97] C. Wilson, *User Experience Re-Mastered*: Morgan Kaufmann, 2009.
- [98] J. Nielsen, *Usability engineering*. Boston: Academic Press, 1993.
- [99] W. Quesenbery, *Storytelling for User Experience: Crafting Stories for Better Design*, 1 ed.: Rosenfeld Media, 2010.
- [100] C. M. Barnum, *Usability Testing Essentials: Ready, Set... Test!*, 1 ed.: Morgan Kaufmann, 2010.
- [101] ISO, "Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability," vol. 9241-11, ed, 1998.
- [102] B. Schneiderman, "Designing the User Interface," USA, 1998.
- [103] A. B. Pedersen, "Usability of authentication in web applications - a literature review," p. 31, July 8 2010.
- [104] B. Prince. (2011), *IT Security & Network Security News & Reviews: Security Spending Priorities for 2011 to Include Firewalls, Blocking Tools*. Available: <http://www.eweek.com/c/a/Security/Security-Spending-Priorities-for-2011-to-Include-Firewalls-Blocking-Tools-650650/> (2011, 21 Oct)
- [105] (2010), *2010 Information Security Breaches Survey results*. Available: <http://www.continuitycentral.com/news05117.html> (2011, 21 Oct)
- [106] P. Olson. (2011), *Sony Freezes 93,000 Online Accounts After Security Breach*. Available: <http://www.forbes.com/sites/parmyolson/2011/10/12/sony-freezes-93000-online-accounts-after-security-breach/> (2011, 21 Oct)
- [107] M. Liebowitz. (2011), *2011 Set to Be Worst Year Ever for Security Breaches* Available: <http://www.securitynewsdaily.com/2011-worst-year-ever-security-breaches-0857/> (2011, Oct 21)
- [108] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: a usability evaluation of PGP 5.0," presented at the Proceedings of the 8th conference on USENIX Security Symposium - Volume 8, Washington, D.C., 1999.
- [109] P. Cuthbert. (2009), *The importance of usable security*. Available: <http://www.castelain.com.au/blog/the-importance-of-usable-security> (2011, Oct 21)
- [110] Y. Ka-Ping, "Aligning security and usability," *Security & Privacy, IEEE*, vol. 2, pp. 48-55, 2004.
- [111] M. Mannan and P. C. v. Oorschot, "Security and usability: the gap in real-world online banking," presented at the Proceedings of the 2007 Workshop on New Security Paradigms, New Hampshire, 2008.
- [112] K. Lane, "Don't make me think: A common sense approach to Web usability," *Technical Communication*, vol. 53, pp. 365-366, Aug 2006.
- [113] C. Herley, "So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," presented at the NSPW, Oxford, United Kingdom, 2009.
- [114] L. F. Cranor and S. Garfinkel, *Security and usability : designing secure systems that people can use*. Beijing Farnham: O'Reilly, 2005.
- [115] C. Braz and J.-M. Robert, "Security and usability: the case of the user authentication methods," in *18th International Conference of the Association Francophone d'Interaction Homme-Machine*, Montreal, Canada, 2006, pp. 199-203.
- [116] E. Dustin, J. Rashka, and D. McDiarmid, *Quality web systems : performance, security, and usability*. Boston ; London: Addison Wesley, 2002.

- [117] M. D. Raimondo and R. Gennaro, "New approaches for deniable authentication," in *12th ACM conference on Computer and communications security*, Alexandria, VA, USA, 2005.
- [118] S. Culp. (2000), *10 Immutable Laws of Security Administration*. Available: <http://technet.microsoft.com/en-us/library/cc722488.aspx> (2011, 14 Aug)
- [119] A. D. Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," *Int. J. Hum.-Comput. Stud.*, vol. 63, pp. 128-152, 2005.
- [120] S. P. Everett, M. D. Byrne, and K. K. Greene, "Measuring the Usability of Paper Ballots: Efficiency, Effectiveness, and Satisfaction," in *Human Factors and Ergonomics Society 50th Annual Meeting*, 2006.
- [121] U. Piazzalunga, P. Savaneschi, and P. Coffetti, "The usability of security devices," in *Security and usability: Designing secure systems that People can use*, L. Cranor and S. Garfinkel, Eds., ed: O'Reilly Media, 2005, pp. 221-263.
- [122] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authentication methods in eBanking and the effects of experience," *Interacting with Computers*, vol. 22, pp. 153-164, 2010.
- [123] T. Acton, W. Golden, S. Gudea, and M. Scott, "Usability and Acceptance in Small-Screen Information Systems," in *eCollector 2004*, 2004.
- [124] V. Bordo. (2010), *Overview of User Acceptance Testing (UAT) for Business Analysts (BAs)*. Available: <http://www.develop.com/useracceptancetests> (2011, 3 Oct 2011)
- [125] T. Kunert, "User-Centered Interaction Design Patterns for Interactive Digital Television Applications," *Springer-Verlag*, 2009.
- [126] M. Zviran, C. Glezer, and I. Avni, "User satisfaction from commercial web sites: The effect of design and use," *Information & Management*, 2006.
- [127] A. Dillon and M. Morris, "Power perception and performance: From usability engineering to technology acceptance with the P3 model of user response," in *The 43rd Annual Conference of the Human Factors and Ergonomics Society*, Santa Monica, CA, 1999, pp. 1017-1021.
- [128] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, vol. 27, p. 53, September 2003.
- [129] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, 1989.
- [130] V. Venkatesh and F. D. Davis, "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science*, vol. 46, p. 19, Feb. 2000.
- [131] Y.-S. Wang and H.-H. Lin, "Determinants of user acceptance of Internet banking: an empirical study," *Journal of Service Industry*, vol. 14, p. 18, 2003.
- [132] D. Gefen, E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model," *MIS Quarterly*, vol. 27, p. 51, Mar 2003 2003.
- [133] S. A. Al-Somali, R. Gholami, and B. Clegg, "An investigation into the acceptance of online banking in Saudi Arabia," *Technovation*, vol. 29, p. 11, 2009.
- [134] M. Fishbein and I. Ajzen, *Belief, attitude, intention, and behavior : an introduction to theory and research*. Reading, Mass.: Addison-Wesley Pub. Co., 1975.
- [135] J. van Biljon and K. Renaud, "A Qualitative Study of the Applicability of Technology Acceptance Models to Senior Mobile Phone Users," in *Advances in Conceptual Modeling – Challenges and Opportunities*. vol. 5232, I.-Y. Song, M. Piattini, Y.-P. Chen, S. Hartmann, F. Grandi, J. Trujillo, A. Opdahl, F. Ferri, P. Grifoni, M. Caschera, C. Rolland, C. Woo, C. Salinesi, E. Zimányi, C. Claramunt, F. Frasinicar, G.-J. Houben, and P. Thiran, Eds., ed: Springer Berlin / Heidelberg, 2008, pp. 228-237.

- [136] Y. Malhotra and D. F. Galletta, "Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation," in *32nd Hawaii International Conference on System Sciences*, 1999.
- [137] F. H. Chandio, "Title," unpublished.
- [138] R. P. Bagozzi, "The legacy of the technology acceptance model and a proposal for a paradigm shift," *Journal of the Academy of Marketing Science*, vol. 8, 2007.
- [139] W. R. King and J. He, "A meta-analysis of the technology acceptance model," *Information and Management*, vol. 43, p. 15, 2006.
- [140] N. Z. Hosein, "Internet banking: Understanding consumer adoption rates among community banks," in *Academic and Business Research Institute Conference*, Las Vegas, 2010.
- [141] J.-H. Wu and S.-C. Wang, "What drives mobile commerce? An empirical evaluation of the revised technology acceptance model," *Inf. Manage.*, vol. 42, pp. 719-729, 2005.
- [142] F. D. Davis, "User acceptance of information technology: system characteristics, user perceptions and behavioral impacts," *Int. J. Man-Mach. Stud.*, vol. 38, pp. 475-487, 1993.
- [143] P. J. Hu, P. Y. K. Chau, O. R. L. Sheng, and K. Y. Tam, "Examining the technology acceptance model using physician acceptance of telemedicine technology," *J. Manage. Inf. Syst.*, vol. 16, pp. 91-112, 1999.
- [144] P. Legris, J. Ingham, and P. Collette, "Why do people use information technology? A critical review of the Technology Acceptance Model," *Information & Management*, vol. 40, pp. 191-204, 2003.
- [145] K. Renaud and J. v. Biljon, "Predicting technology acceptance and adoption by the elderly: a qualitative study," presented at the Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries: riding the wave of technology, Wilderness, South Africa, 2008.
- [146] K. M. Nor and J. M. Pearson, "The influence of trust on internet banking acceptance," *Journal of Internet Banking and Commerce*, vol. 12, 2007.
- [147] S. A. Al-Somali, R. Gholami, and B. Clegg, "Internet Banking Acceptance in the Context of Developing Countries: An Extension of the Technology Acceptance Model," 2008.
- [148] E.-J. Lee and J. Lee, "CONSUMER ADOPTION OF INTERNET BANKING: NEED-BASED AND/OR SKILL BASED?," *Marketing Management Journal*, vol. 11, p. 13, 2001.
- [149] B. Jaruwachirathanakul and D. Fink, "Internet banking adoption strategies for a developing country: the case of Thailand," *Internet Research*, vol. 15, p. 16, 2005.
- [150] Y. T. Chang, "Banking Structure and Governance: Changes in Regulation and Technology," Ph.D in Economics, Department of Economics, The University of Warwick, 2005.
- [151] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User Acceptance of Computer Technology: Comparison of Two Theoretical Models," *Management Science*, vol. 34, p. 22, 1989.
- [152] J. Yu, I. Ha, M. Choi, and J. Rho, "Extending the TAM for a t-commerce," *Information & Management*, vol. 42, pp. 965-976, 2005.
- [153] K. Padachi, B. Seetanah, and S. Rojid, "Investigating into the factors that influence the adoption of Internet banking in Mauritius," *Journal of Internet Business*, 2008.
- [154] M. S. Sohail and B. Shanmugham, "E-banking and customer preferences in Malaysia: an empirical investigation," *Inf. Sci. Inf. Comput. Sci.*, vol. 150, pp. 207-217, 2003.

- [155] J. Pallant, *SPSS survival manual : a step by step guide to data analysis using SPSS (version 15)*, 3rd ed. Sydney, Australia: Ligare Book Printer, 2007.
- [156] S. Li and A. Worthington, "The relationship between the adoption of Internet banking and electronic connectivity: - An international comparison," 2004.
- [157] K. J. Stewart, "Transference as a means of building trust in World Wide Web sites," presented at the Proceedings of the 20th international conference on Information Systems, Charlotte, North Carolina, United States, 1999.
- [158] M. Sathye, "Adoption of Internet banking by Australian consumers: an empirical investigation," *International Journal of Bank Marketing*, vol. 17, p. 10, 1999.
- [159] H. Karjaluoto, M. Mattila, and T. Pento, "Electronic banking in Finland: Consumer beliefs and reactions to a new delivery channel " *Journal of Financial Services Marketing*, vol. 6, p. 16, 1 June 2002.
- [160] B. Suh and I. Han, "Effect of trust on customer acceptance of Internet banking," *Electronic Commerce Research and Applications*, vol. 1, pp. 247-263, 2002.
- [161] S. Rotchanakitumnuai and M. Speece, "Barriers to internet banking adoption: a qualitative study among corporate customers in Thailand," *International Journal of Bank Marketing*, p. 11, 2003.
- [162] D. Tomiuk and A. Pinsonneault, "Customer loyalty and electronic-banking," *Journal of Global Information Management*, 2001.
- [163] T. Pikkarainen, "Consumer acceptance of online banking: an extension of the technology acceptance model," *Internet Research*, vol. 14, 2004.
- [164] C. Jayawardhena and P. Foley, "Changes in the banking sector - the case of Internet banking in the UK," *Internet Research*, vol. 10, pp. 19-31, 2000.
- [165] A. Almogbil, "Title," unpublished.
- [166] A. Mattila and M. Mattila, "How perceived security appears in the commercialisation of internet banking," *International Journal of Financial Services Management*, vol. 1, p. 13, 2005.
- [167] M. Nilsson, A. Adams, and S. Herd, "Building Security and Trust in Online Banking," presented at the CHI, Portland, Oregon, USA, 2005.
- [168] C. Ranganathan and S. Ganapathy, "Ky dimensions of business-to-consumer web sites," *Information & Management*, vol. 39, p. 8, 2002.
- [169] M. Tan and T. S. H. Teo, "Factors influencing the adoption of Internet banking," *J. AIS*, vol. 1, p. 5, 2000.
- [170] T. C. E. Cheng, D. Y. C. Lam, and A. C. L. Yeung, "Adoption of internet banking: An empirical study in Hong Kong," *Decision Support Systems*, vol. 42, pp. 1558-1572, 2006.
- [171] B. Howcroft, R. Hamilton, and P. Hower, "Consumer attitude and the usage and adoption of home-based banking in the United Kingdom," *International Journal of Bank Marketing*, vol. 20, p. 11, 2002.
- [172] W. D. Salisbury, R. A. Pearson, A. W. Pearson, and D. W. Miller, "Perceived security and World Wide Web purchase intention," *Industrial Management & Data Systems*, vol. 101, p. 11, 2001.
- [173] F. Greitzer, "Situating Usability Testing for Security Systems," The U.S. Department of Energy, Richland, Washington 2011.
- [174] H. Coolican, *Research methods and Statistics in Psychology*, vi ed. London, England: Hodder & Stoughton, 1990.
- [175] U. N. C. o. T. a. Development, "E-Commerce and Development Report 2002," United Nations, New York & Geneva 2002.
- [176] Girish. (2009), *Online banking security tips, dos and don'ts, avoid email phishing and fraudsters*. Available: <http://dotgiri.com/2009/11/09/online-banking-security-tips-dos-and-dont-avoid-email-phishing-and-fraudsters/-more-1873> (2010, 30 May)

- [177] P. Key, "Assessment of Today's Mobile Banking Applications from the View of Customer Requirements," 2004, pp. 70184a-70184a.
- [178] B. Burnham. (1996), *The Internet's Impact on Retail Banking*. Available: <http://www.strategy-business.com/article/17575?gko=93c98> (2010, 17 May)
- [179] C. Liao, P.-L. To, T.-H. Hsleh, and C.-C. Llu, "An Empirical Study of Factors Influencing the Adoption of Internet Banking," in *AMCIS 2009*, San Francisco, USA, 2009.
- [180] T. Kuisma, T. Laukkanen, and M. Hiltunen, "Mapping the reasons for resistance to Internet banking: A means-end approach," *International Journal of Information Management*, vol. 27, pp. 75-85, 2007.
- [181] S. L. Jarvenpaa, N. Tractinsky, and M. Vitale, "Consumer trust in an Internet store," *Information Technology and Management*, vol. 1, pp. 45-71, Oct 30 2004.
- [182] K. Kim and B. Prabhakar, "Initial trust, perceived risk, and the adoption of internet banking," presented at the Proceedings of the twenty first international conference on Information systems, Brisbane, Queensland, Australia, 2000.
- [183] D. J. Kim, D. L. Ferrin, and H. R. Rao, "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," *Decision Support Systems*, vol. 44, pp. 544-564, 2008.
- [184] T. Shiffrin. (2007), *Human Error Causes Most Data Loss, Study Says*. Available: http://www.pcworld.com/article/129736/human_error_causes_most_data_loss_study_says.html (2010, 10 June)
- [185] Z. Liao and M. T. Cheung, "Challenges to Internet e-banking," *Commun. ACM*, vol. 46, pp. 248-250, 2003.
- [186] M.-C. Lee, "Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit," *Electronic Commerce Research and Applications*, vol. 8, pp. 130-141, 2009.
- [187] (2006), *Online Banking Fees: Look for the Lowest Rates*. Available: <http://www.msmonney.com/mm/banking/onlinebk/fees.htm> (2010, 10 June)
- [188] I. Thomson. (2009), *Online attacks cost Pentagon US\$100 million*. Available: <http://www.securecomputing.net.au/News/142019,online-attacks-cost-pentagon-us100-million.aspx> (2010, 10 June)
- [189] J. Vijayan. (2010), *Cyberattacks raise e-banking security fears*. Available: http://www.computerworld.com/s/article/9168458/Cyberattacks_raise_e_banking_security_fears (2010, 11 June)
- [190] J. Vijayan. (2010), *Texas firm countersues bank in connection with \$800,000 cyber theft*. Available: http://www.computerworld.com/s/article/9160798/Texas_firm_countersues_bank_in_connection_with_800_000_cyber_theft (2010, 11 June)
- [191] J. Vijayan. (2010), *Michigan firm sues bank over theft of \$560,000*. Available: http://www.computerworld.com/s/article/9156558/Michigan_firm_sues_bank_over_theft_of_560_000 (2010, 11 June)
- [192] R. McMillan. (2010), *FDIC: Hackers stole more than \$120M in three months from small businesses*. Available: http://www.computerworld.com/s/article/9167898/FDIC_Hackers_stole_more_than_120M_in_three_months_from_small_businesses (2010, 11 June)
- [193] J. Vijayan and E. Lai. (2005), *Banks get new online authentication guidelines*. Available: http://www.computerworld.com/s/article/105599/Banks_get_new_online_authentication_guidelines (2010, 11 June)
- [194] D. E. McCorkle, "The role of perceived risk in mail order catalog shopping," *Journal of Direct Marketing*, vol. 4, pp. 26-35, 1990.

- [195] "Cybercriminals use Trojans & money mules to rob online banking accounts," Finjan Malicious Code Research Center2009.
- [196] K. A. Olsen, "A \$100,000 keying error," *IEEE Computer*, April 2008.
- [197] S. Denny. *The Electronic Commerce Challenge*. Available: <http://www.arraydev.com/commerce/JIBC/9811-06.htm> (2010, 18 May)
- [198] R. Dhamija and J. D. Tygar, "The battle against phishing: Dynamic Security Skins," presented at the Proceedings of the 2005 symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2005.
- [199] S. Brunswick, "eCommerce fraud - time to act?," *Card Technology Today*, vol. 21, pp. 12-13, 2009.
- [200] P. Kinsella. (2004), *Zinek Upgrades SMS Engine with Secure SMS Banking*. Available: <http://econsultancy.com/press-releases/211-press-release-zinek-upgrades-sms-engine-with-secure-sms-banking> (2010, 11 April)
- [201] (2009), *International Telecommunication Union*. Available: <http://datafinder.worldbank.org/> (2010, 10 Mar)
- [202] (2010), *Internet Usage Statistics: The Internet Big Picture*. Available: <http://www.internetworldstats.com/> (2010, 1 May 2010)
- [203] A. Kemshall, "Why mobile two-factor authentication makes sense," *Network Security*, vol. 2011, pp. 9-12, 2011.
- [204] "Wireless Short Message Service (SMS)," International Engineering Consortium1999.
- [205] M. Becker and M. Hanley, "Mobile Marketing Research Priorities: Roadmap to Engaging the "Connected Customer," Global Mobile Marketing Association2006.
- [206] S. O. R. GmbH, "mBanking - The Future of Personal Financial Transaction?," Frankfurt, 2001.
- [207] M. Odell. (2005), *Use of mobile helped police keep tabs on suspect and brother*. Available: <http://www.ft.com/cms/s/0/4239e29e-02f2-11da-84e5-00000e2511c8.html> (2010, 20 June)
- [208] G. Gupta. (2009), *Mobile phone security cracked, says German hacker*. Available: <http://www.guardian.co.uk/technology/2009/dec/29/gsm-mobile-algorithm-cracked-nohl> (2010, 20 June)
- [209] N. Stanley. (2010), *Mobile Phone Hacking for £1000*. Available: <http://www.computerweekly.com/blogs/Bloor-on-IT-security/2010/04/mobile-phone-hacking-for-1000.html> (2010, 20 June)
- [210] "SMS Spoofing: Prevent Revenue Loss by Securing The Network Against Fraudulent Attack," Openmind networks messaging experts, Whitepaper2008.
- [211] A. Fendelman. *How Are Cell Phones Different From Smartphones?* Available: <http://cellphones.about.com/od/coveringthebasics/qt/cellphonesvssmartphones.htm> (2010, 20 June)
- [212] A. Fendelman. (2010), *Mobile Security: Can You Trust Your Bank Account to Your Phone's Mobile Web?* Available: <http://cellphones.about.com/od/mobilewebtips/a/mobilesecurity.htm> (2010, 20 June)
- [213] ISO, "Ergonomic requirements for office work with visual display terminals (VDTs)," in *Guidance on usability* vol. 9241, ed, 1998.
- [214] J. Nielsen. (1994), *Ten Usability Heuristics*. Available: http://www.useit.com/papers/heuristic/heuristic_list.html (2010, 10 Sep)
- [215] M. M. Gardiner and B. Christie, Eds., *Applying cognitive psychology to user-interface design*. John Wiley & Sons, Inc., 1987, p.^pp. Pages.
- [216] K. Renaud and R. Cooper, "Feedback in Human-Computer Interaction - Characteristics and Recommendations," presented at the Annual Research Conference, South Africa, 2000.

- [217] F. L. Wong and F. Stajano, "Multichannel Security Protocols," *Pervasive Computing*, 2007.
- [218] M. Castells, M. Fernandez-Ardevol, J. L. Qiu, and A. Sey, *Mobile Communication and Society: A Global Perspective*: Massachusetts Institute of Technology, 2007.
- [219] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack. *Uncover Security Design Flaws Using the STRIDE Approach*. Available: <http://msdn.microsoft.com/en-us/magazine/cc163519.aspx> (2010, 22 Oct.)
- [220] R. L. Jones and A. Rastogi, "Secure Coding: Building Security into the Software Development Life Cycle," *Information Security Journal: A Global Perspective*, vol. 13, pp. 29 - 39, 2004.
- [221] R. Kazman, G. Abowd, L. Bass, and P. Clements, "Scenario-Based Analysis of Software Architecture," *IEEE Softw.*, vol. 13, pp. 47-55, 1996.
- [222] V. Prasath, "Modeling the Evaluation Criteria for Security Patterns in Web Service Discovery," *International Journal of Computer Applications*, vol. 1, pp. 53-60, February 2010.
- [223] D. F. Cooper, "The Australian and New Zealand Standard on Risk Management, AS/NZS 4360:2004," Broadleaf Capital International PTY LTD, NSW, Australia 2007.
- [224] P. Mell, K. Scarfone, and S. Romanosky. (2007), *A Complete Guide to the Common Vulnerability Scoring System*. Available: <http://www.first.org/cvss/cvss-guide.html> (2011, 23 May)
- [225] C. Alberts and A. Dorofee. (2001), *An Introduction to the OCTAVE Method*. Available: <http://www.cert.org/octave/methodintro.html> (2011, 23 May)
- [226] OWASP. *Threat Risk Modeling*. Available: https://http://www.owasp.org/index.php/Threat_Risk_Modeling_-_Performing_threat_risk_modeling_using_the_Microsoft_Threat_Modeling_Process (2011, 23 May)
- [227] J. D. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla, and A. Murukan. (2003), *.NET Framework Security: Threat Modeling*. Available: <http://msdn.microsoft.com/en-au/library/ff648644.aspx> (2011, 3 Dec)
- [228] P. Koutsabasis, E. Vlachogiannis, and J. S. Darzentas, "Beyond Specifications: Towards a Practical Methodology for Evaluating Web Accessibility," *Journal of Usability Studies*, vol. 5, p. 14, August 2010.
- [229] , *Layered Performance Architecture*. Available: <http://www.nothingbutyellow.com/articles/layered-performance-architecture.html> (2010, Nov. 25th)
- [230] M. Agoyi and D. Seral, "The use of SMS encrypted message to secure automatic teller machine," *Procedia Computer Science*, vol. 3, pp. 1310-1314, 2011.
- [231] (2011), *Multi-channel authentication is an alternative to tokens*. Available: <http://www.threatchaos.com/home-mainmenu-1/16-blog/577-multi-channel-authentication-is-an-alternative-to-tokens> (2011, 16 May)
- [232] K. Padachi, S. Rojid, and B. Seetanah, "Analyzing the Factors that Influence the Adoption of Internet Banking in Mauritius," in *Computer Science and IT Education Conference*, 2007.
- [233] J. Brooke, "SUS: a quick and dirty usability scale," in *Usability evaluation in industry*, ed London ; Bristol, Pa.: Taylor & Francis, 1996, pp. xvii, 252 p.
- [234] N. Schmitt, R. J. Klimoski, G. R. Ferris, and K. M. Rowland, *Research methods in human resources management*. Cincinnati: South-Western Pub. Co., 1991.
- [235] H. Sharp, Y. Rogers, and J. Preece, *Interaction Design: Beyond Human-computer Interaction*, 2nd edition ed.: John Wiley & Sons, 2007.

- [236] V. Vehovar and K. L. Manfreda, "Overview: Online surveys," in *The SAGE handbook of online research methods*, N. Fielding, R. M. Lee, and G. Blank, Eds., ed Los Angeles ; London : SAGE, 2008, pp. 175 - 254.
- [237] D. Andrews, B. Nonnecke, and J. Preece, "Electronic Survey Methodology: A Case Study in Reaching Hard-to-Involve Internet Users," *International Journal of Human-Computer Interaction*, vol. 16, pp. 185 - 210, 2003.
- [238] K. Finstad, "The System Usability Scale and Non-Native English Speakers," *Journal of Usability Studies*, vol. 1, p. 3, August 2006 2006.
- [239] M. Al-Fairuz and K. Renaud, "Multi-channel, Multi-level Authentication for More Secure eBanking," in *ISSA*, Johannesburg, South Africa, 2010.
- [240] H. T. Reis and C. M. Judd, *Handbook of Research Methods in Social and Personality Psychology*: Cambridge University Press, 2000.
- [241] (2007), *At a glance: Oman, Education*. Available: http://www.unicef.org/infobycountry/oman_statistics.html - 67 (2010, 30 Aug.)
- [242] (2010), *Oman: Internet Usage and Marketing Report*. Available: <http://www.internetworldstats.com/me/om.htm> (2010, 30 Aug.)
- [243] B. G. Tabachnick and L. S. Fidell, *Using multivariate statistics*, 5th ed. Boston: Pearson/Allyn & Bacon, 2007.
- [244] W. Outhwaite and S. P. Turner, *The SAGE handbook of social science methodology*. Los Angeles ; London: SAGE, 2007.
- [245] A. R. Donders, G. J. van der Heijden, T. Stijnen, and K. G. Moons, "Review: a gentle introduction to imputation of missing values," *J Clin Epidemiol*, vol. 59, pp. 1087-91, Oct 2006.
- [246] "SPSS Missing Values 17.0," 2007.
- [247] V. Barnett and T. Lewis, *Outliers in statistical data*, 3rd ed. Chichester ; New York: Wiley, 1994.
- [248] F. J. Gravetter and L. B. Wallnau, *Statistics for the behavioral sciences*, 6th ed. Belmont, CA: Wadsworth, 2004.
- [249] G. Hofstede, *Cultures and Organizations: Software of the Mind*: McGraw-Hill, 1997.
- [250] H. L. Minton and F. W. Schneider, *Differential Psychology, Prospect Heights. IL*: Waveland Press, 1971.
- [251] F. Wahid, "USING THE TECHNOLOGY ADOPTION MODEL TO ANALYZE INTERNET ADOPTION AND USE AMONG MEN AND WOMEN IN INDONESIA," *The Electronic Journal of Information Systems in Developing Countries*, vol. 32, 2007.
- [252] P. Legris, J. Ingham, and P. Collette, "Why do people use information technology?: a critical review of the technology acceptance model," *Inf. Manage.*, vol. 40, pp. 191-204, 2003.
- [253] G. Zhou and J. Xu, "Adoption of Educational Technology: How Does Gender Matter?," *International Journal of Teaching and Learning in Higher Education*, vol. 19, p. 13, 2007.
- [254] R. R. Burke, "Technology and the customer interface: what consumers want in the physical and virtual store?," *Journal of the Academy of Marketing Science*, vol. 30, p. 21, 2002.
- [255] A. Al-Hajri, "Computer Assisted Assessment in Oman: Factors Affecting Student Performance," Doctorate, Faculty of Science and Technology, University of Plymouth, 2011.
- [256] A. Scott, L. Semmens, and L. Willoughby, "WOMEN AND THE INTERNET The natural history of a research project," *Information, Communication & Society*, vol. 2, pp. 541 - 565, 1999.

- [257] C. L. Ferle, S. Edwards, and Y. Minzuno, "Internet Diffusion in Japan: Cultural Considerations," *Journal of Advertising Research*, 2002.
- [258] "World Marriage Data 2008," United Nations 2008.
- [259] T. Meyer, "Online banking: The young and well-educated extend their lead until 2010," Deutsche Bank Research, Frankfurt, Germany 2008.
- [260] H. Kaiser, "An index of factorial simplicity," *Psychometrika*, vol. 39, pp. 31-36, 1974.
- [261] M. Bartlett, "A note on the multiplying factors for various chi square approximations," *Journal of the Royal Statistical Society*, 1954.
- [262] W. Quesenbery, "What Does Usability Mean: Looking Beyond 'Ease of Use'," in *48th Annual Conference, Society for Technical Communication*, 2001.
- [263] Dan. (2007), *Usability Components: Memorability and Satisfaction*. Available: <http://www.doublespark.co.uk/blog/usability-components-memorability/> (2010, 2 Sept)
- [264] J. Cohen, *Statistical power analysis for the behavioral sciences*, 2nd ed. Hillsdale, N.J.: L. Erlbaum Associates, 1988.

Appendix A

Web-application Codes/Scripts

A1: PHP page to automate the process of calculating the time spent variable (TS_n)

```
<?php require_once('Connections/ev_conn.php'); ?>
<?php
if (!function_exists("GetSQLValueString")) {
function GetSQLValueString($theValue, $theType, $theDefinedValue = "",
$theNotDefinedValue = "")
{
    if (PHP_VERSION < 6) {
        $theValue = get_magic_quotes_gpc() ? stripslashes($theValue) : $theValue;
    }

    $theValue = function_exists("mysql_real_escape_string") ?
mysql_real_escape_string($theValue) : mysql_escape_string($theValue);

    switch ($theType) {
        case "text":
            $theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";
            break;
        case "long":
        case "int":
            $theValue = ($theValue != "") ? intval($theValue) : "NULL";
            break;
        case "double":
            $theValue = ($theValue != "") ? doubleval($theValue) : "NULL";
            break;
        case "date":
            $theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";
            break;
        case "defined":
            $theValue = ($theValue != "") ? $theDefinedValue : $theNotDefinedValue;
            break;
    }
    return $theValue;
}

mysql_select_db($database_ev_conn, $ev_conn);
$query_rsData = "SELECT users.username, logs.acctnum, logs.log_id, logs.ipaddress,
logs.visit_time, logs.visit_page, logs.user_agent, logs.get_vars, logs.post_vars
FROM users INNER JOIN logs ON users.username = logs.username WHERE (users.level=0)
ORDER BY logs.username, logs.log_id;";
$rsData = mysql_query($query_rsData, $ev_conn) or die(mysql_error());
$row_rsData = mysql_fetch_assoc($rsData);
$totalRows_rsData = mysql_num_rows($rsData);
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Data Analysis</title>
</head>
<body>
<p><strong>Logs records - DATA</strong></p>
<table width="100%" border="1">
```

```

<tr>
  <th>#</th>
  <th>Username</th>
  <th>Acct</th>
  <th>logid</th>
  <th>ipaddress</th>
  <th>page</th>
  <th>visit_time</th>
  <th>time_spent</th>
  <th>user_agent</th>
  <th>get_vars</th>
  <th>post_vars</th>
</tr>
<?php $x = 0; ?>
<?php do { ?>
<?php $x++;
  if($x > 1) {
    ?>
    <tr>
      <td><?php echo $x; ?></td>
      <td><?php echo $username; ?></td>
      <td><?php echo $acctnum; ?></td>
      <td><?php echo $log_id; ?></td>
      <td><?php echo $ipaddress; ?></td>
      <td><?php echo $visit_page; ?></td>
      <td><?php echo $visit_time; ?></td>
      <td><?php if($username == $row_rsData['username']) echo
($row_rsData['visit_time'] - $visit_time); ?></td>
      <td><?php echo $user_agent; ?></td>
      <td><?php echo $get_vars; ?></td>
      <td><?php echo $post_vars; ?></td>
    </tr>
  <?php
  }
  $username = $row_rsData['username'];
  $acctnum = $row_rsData['acctnum'];
  $log_id = $row_rsData['log_id'];
  $ipaddress = $row_rsData['ipaddress'];
  $visit_page = $row_rsData['visit_page'];
  $visit_time = $row_rsData['visit_time'];
  $user_agent = $row_rsData['user_agent'];
  $get_vars = str_replace('alert','',$row_rsData['get_vars']);
  $post_vars = str_replace('alert','',$row_rsData['post_vars']);
  ?>
<?php } while ($row_rsData = mysql_fetch_assoc($rsData)); ?>
<tr>
  <td>&nbsp;</td>
  <td>&nbsp;</td>
  <td>&nbsp;</td>
  <td>&nbsp;</td>
  <td>&nbsp;</td>
  <td>&nbsp;</td>
  <td>&nbsp;</td>
  <td>&nbsp;</td>
  <td>&nbsp;</td>
  <td>&nbsp;</td>
  <td>&nbsp;</td>
</tr>
</table>
</body>
</html>
<?php
mysql_free_result($rsData);
?>

```

A2: PHP page to automate the process of calculating the time spent variable (TSn) per each task

```
<?php require_once('Connections/ev_conn.php'); ?>
<?php
if (!function_exists("GetSQLValueString")) {
function GetSQLValueString($theValue, $theType, $theDefinedValue = "",
$theNotDefinedValue = "")
{
    if (PHP_VERSION < 6) {
        $theValue = get_magic_quotes_gpc() ? stripslashes($theValue) : $theValue;
    }

    $theValue = function_exists("mysql_real_escape_string") ?
mysql_real_escape_string($theValue) : mysql_escape_string($theValue);

    switch ($theType) {
        case "text":
            $theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";
            break;
        case "long":
        case "int":
            $theValue = ($theValue != "") ? intval($theValue) : "NULL";
            break;
        case "double":
            $theValue = ($theValue != "") ? doubleval($theValue) : "NULL";
            break;
        case "date":
            $theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";
            break;
        case "defined":
            $theValue = ($theValue != "") ? $theDefinedValue : $theNotDefinedValue;
            break;
    }
    return $theValue;
}
}

mysql_select_db($database_ev_conn, $ev_conn);
$query_rsData = "SELECT users.username, logs.acctnum, logs.log_id, logs.ipaddress,
logs.visit_time, logs.visit_page, logs.user_agent, logs.get_vars, logs.post_vars
FROM users INNER JOIN logs ON users.username = logs.username WHERE (users.level=0)
ORDER BY logs.username, logs.log_id";
$rsData = mysql_query($query_rsData, $ev_conn) or die(mysql_error());
$row_rsData = mysql_fetch_assoc($rsData);
$totalRows_rsData = mysql_num_rows($rsData);
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Data Analysis</title>
</head>

<body>
<p><strong>Logs records per tasks</strong></p>

<p>&nbsp;</p>
<table width="100%" border="1">
    <tr>
        <th>#</th>
        <th>Username</th>
        <th>Last logid</th>
        <th>Acct</th>
        <th>Task 1</th>
        <th>Task 2</th>
        <th>Task 3</th>
        <th>Task 4</th>
```

```

        <th>Task 5</th>
        <th>Total</th>
    </tr>
    <?php $x = 0; $ts = 0;

        $ts1start = false; $ts1finalize = false; $ts1done = false;
        $ts2start = false; $ts2finalize = false; $ts2done = false;
        $ts3start = false; $ts3finalize = false; $ts3done = false;
        $ts4start = false; $ts4finalize = false; $ts4done = false;
        $ts5start = false; $ts5finalize = false; $ts5check = false; $ts5done =
false;
    ?>
    <?php do { ?>
    <?php $x++;
    if($x > 1) {
        if($ts1finalize == true && $ts1done == false) $t1=($ts1 +
($row_rsData['visit_time'] - $visit_time));
        if($ts2finalize == true && $ts2done == false) $t2=($ts2 +
($row_rsData['visit_time'] - $visit_time));
        if($ts3finalize == true && $ts3done == false) $t3=($ts3 +
($row_rsData['visit_time'] - $visit_time));
        if($ts4finalize == true && $ts4done == false) $t4=($ts4 +
($row_rsData['visit_time'] - $visit_time));
        if($ts5finalize == true && $ts5done == false) $t5=($ts5 +
($row_rsData['visit_time'] - $visit_time));
    ?>
    <?php
    }
    $ts = $row_rsData['visit_time'] - $visit_time;
    // do the process of calculating the total time spent for each task
    if($row_rsData['username'] == $username) { // make sure we are dealing with
the same user
        // do a check for task 5 (check the intermediary page)
        if($row_rsData['visit_page'] == '/transfer.php' &&
substr($row_rsData['get_vars'],0,17) == 'mode=alt_activate') {
            $ts5check = true; // trigger the task5 check intermediary
page flag to true
        }
        // now we start with task 1
        if($ts1done == false) {
            if($ts1start == true) {
                $ts1 = $ts1 + $ts; // calculate task1 commulative TS
            }
            if($row_rsData['visit_page'] == '/profile.php' && $ts1start ==
false && $ts1done == false) {
                $ts1 = 0;
                $ts1start = true; // trigger the task1 start
flag to true
            }
            if($ts1finalize == true) { $ts1done = true; $ts1start = false;
}
            if($row_rsData['visit_page'] == '/channels.php') { // if
finish page is reached, set flag finalize to true
                $ts=0;
                $ts1finalize = true;
            }
        }

        // we start with task 2
        if($ts1done == true && $ts2done == false) {
            if($ts2start == true && $ts2done == false) {
                $ts2 = $ts2 + $ts; // calculate task2 commulative TS
            }
            if($row_rsData['visit_page'] == '/channels.php' && $ts2start
== false && $ts2done == false) {
                $ts2 = 0;
                $ts2start = true; // trigger the task1 start
flag to true
            }
        }
    }
}

```



```

        if($ts2finalize == true) { $ts2done = true; $ts2start = false;
    }

    if($row_rsData['visit_page'] == '/account.php') { // if finish
page is reached, set flag finish to true
        $ts=0;
        $ts2finalize = true;
    }
}

// we start with task 3
if($ts2done == true && $ts3done == false) {
    if(($ts3start == true && $ts3done == false) && $ts2done ==
true) {
        $ts3 = $ts3 + $ts; // calculate task3 commulative TS
    }
    if($row_rsData['visit_page'] == '/addbeneficiary.php' &&
$ts3start == false && $ts3done == false) {
        $ts3 = 0;
        $ts3start = true; // trigger the task1 start
flag to true
    }
    if($ts3finalize == true) { $ts3done = true; $ts3start = false;
}

    if(($row_rsData['visit_page'] == '/transfer.php' &&
$row_rsData['get_vars'] == 'activate=true') || ($row_rsData['visit_page'] ==
'/scripts/checksms.php' && $row_rsData['get_vars'] == 'chktype=1')) { // if
finish page is reached, set flag finish to true
        $ts=0;
        $ts3finalize = true;
    }
}

// we start with task 4
if($ts3done == true && $ts4done == false) {
    if($ts4start == true && $ts4done == false) {
        $ts4 = $ts4 + $ts; // calculate task4 commulative TS
    }
    if(($row_rsData['visit_page'] == '/transfer_page.php' &&
substr($row_rsData['get_vars'],0,6) == 'bn_id=') && $ts4start == false && $ts4done
== false) {
        $ts4 = 0;
        $ts4start = true; // trigger the task1 start
flag to true
    }
    if($ts4finalize == true) { $ts4done = true; $ts4start = false;
}

    if($row_rsData['visit_page'] == '/account.php' &&
substr($row_rsData['get_vars'],0,7) == 'acc_no=') { // if finish page is reached,
set flag finish to true
        $ts=0;
        $ts4finalize = true;
    }
}

// we start with task 5 ONLY IF all previous tasks are DONE
if($ts1done == true && $ts2done == true && $ts3done == true &&
$ts4done == true && $ts5done == false) {
    if($ts5start == true) {
        $ts5 = $ts5 + $ts; // calculate task5 commulative TS
    }
    if($row_rsData['visit_page'] == '/addbeneficiary.php' &&
$ts5start == false && $ts5done == false && $ts4done == true) {
        $ts5 = 0;
        $ts5start = true; // trigger the task5 start
flag to true
    }
    if($ts5check == true) {

```

```

        if($ts5finalize == true) { $ts5done = true; $ts5start =
false; }

        if($row_rsData['visit_page'] == '/transfer.php' &&
$row_rsData['get_vars'] == 'activate=true') { // if finish page is reached, set
flag finish to true

                $ts=0;
                $ts5finalize = true;

        }

    }
} else {
// if username is changed, reset all variables for a new cycle
$ts1start = false; $ts1finalize = false; $ts1done = false;
$ts2start = false; $ts2finalize = false; $ts2done = false;
$ts3start = false; $ts3finalize = false; $ts3done = false;
$ts4start = false; $ts4finalize = false; $ts4done = false;
$ts5start = false; $ts5finalize = false; $ts5check = false; $ts5done =
false;
$tsout = '';
}
?>
<?php
// output the results before moving to a new user
if($username != $row_rsData['username']) { ?>
    <tr>
        <td><?php echo $x; ?></td>
        <td><?php echo $username; ?></td>
        <td><?php echo $log_id; ?></td>
        <td><?php echo $acctnum; ?></td>
        <td><?php if($t1==0) { echo '<font color=red>'.$t1.'</font>'; } else { echo
$t1; } ?></td>
        <td><?php if($t2==0) { echo '<font color=red>'.$t2.'</font>'; } else { echo
$t2; } ?></td>
        <td><?php if($t3==0) { echo '<font color=red>'.$t3.'</font>'; } else { echo
$t3; } ?></td>
        <td><?php if($t4==0) { echo '<font color=red>'.$t4.'</font>'; } else { echo
$t4; } ?></td>
        <td><?php if($t5==0) { echo '<font color=red>'.$t5.'</font>'; } else { echo
$t5; } ?></td>
        <td><?php echo ($t1+$t2+$t3+$t4+$t5); $t1=0; $t2=0; $t3=0; $t4=0; $t5=0;
?></td>
    </tr>
<?php } ?>
<?
    $username = $row_rsData['username'];
    $acctnum = $row_rsData['acctnum'];
    $log_id = $row_rsData['log_id'];
    $ipaddress = $row_rsData['ipaddress'];
    $visit_page = $row_rsData['visit_page'];
    $visit_time = $row_rsData['visit_time'];
    $user_agent = $row_rsData['user_agent'];
    $get_vars = str_replace('alert','', $row_rsData['get_vars']);
    $post_vars = str_replace('alert','', $row_rsData['post_vars']);
?>
    <?php } while ($row_rsData = mysql_fetch_assoc($rsData)); ?>
</table>
</body>
</html>
<?php
mysql_free_result($rsData);
?>

```

Appendix B

Online Questionnaires

B1: Pre-questionnaire – Section A (English)



Section A: Internet and Banking Facilities

1. How frequently do you access the Internet from the following places?

	Daily	Weekly	Monthly	Never
Home	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Work	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
School	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Public (Library, Cybercafe, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile (including GPRS, 3G, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other, please specify <input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2. If you access the Internet daily, how many minutes/hours in total do you usually spend on it each day?

Up to 30 minutes	1 to 2 hours	2 to 3 hours	3 to 4 hours	Above 4 hours
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. Do you make use of Internet banking facility?

Yes	No	
<input type="radio"/>	<input type="radio"/>	<i>If the answer is no, save and proceed to Section B</i>

4. With how many banks do you do your Internet banking services?

One	Two	Three	Four	Five
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. How often do you make use of this service?

<input type="radio"/>	Every day
<input type="radio"/>	Several times a week
<input type="radio"/>	About once a week
<input type="radio"/>	Several times a month
<input type="radio"/>	About once a month
<input type="radio"/>	Less than once a month

B2: Pre-questionnaire – Section B (English)

Section A

Section B

Section C

Section B: Factors affecting the adoption of E-Banking

The following table lists factors that may motivate users to use internet banking and make Internet banking transactions. Using the scale 1 (not at all important) to 5 (very important), please rate how important each of the factors is/would be, in motivating you to use Internet banking.

1. Accessibility	1	2	3	4	5
Convenience to access the service	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Connection speed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. Trust and relationship	1	2	3	4	5
Reliability of your banker (A scale of 5 for highly reliable to a scale of 1 for not at all reliable)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bank response rate to queries	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ethical and professional conduct	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bank's policy to compensate for losses	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. Reluctance	1	2	3	4	5
The bank willingness to adopt technology	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The bank level of awareness of the Internet banking service	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. Security	1	2	3	4	5
Clear and understandable instructions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Security of Internet transaction	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Length of Internet experience	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. Convenience	1	2	3	4	5
Range of electronic services offered	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Convenient way of doing bank transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Time saving	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6. Ease of use	1	2	3	4	5
User friendly web site	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ease of performing E-Transaction	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

B3: Pre-questionnaire – Section C (English)

Section A

Section B

Section C

Section C: Participant Profile

1. Please state your gender:

Male	Female
<input type="radio"/>	<input type="radio"/>

2. What is your marital status?

Single	Married	Divorced	Other
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. Please indicate your age group (in years)?

18 - 27	28 - 37	38 - 47	48 - 57	58 - 67	68 or more
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4. Which is your highest level of education

<input type="radio"/>	High school or equivalent
<input type="radio"/>	Technical/professional training
<input type="radio"/>	College graduate (4 years)
<input type="radio"/>	Master degree or equivalent
<input type="radio"/>	Postgraduate degree

5. What is your current occupation?

Student	Self-employed	Clerical	Professional	Service Staff
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Management	Sales	Retired	Not Employed	Other (Specify)
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> <input type="text"/>

6. What type of business area best describes your organisation?

<input type="radio"/>	Banking and Financial Services (Finance, insurance and real estate)
<input type="radio"/>	Transport and distribution (including Aviation and Port)
<input type="radio"/>	Communication and Utilities
<input type="radio"/>	Trade and Commerce
<input type="radio"/>	Education
<input type="radio"/>	Service Industry (including Hotels/restaurants)
<input type="radio"/>	Farming and Agriculture
<input type="radio"/>	Self-employed, please specify: <input type="text"/>
<input type="radio"/>	Other, please specify: <input type="text"/>

7. To which monthly Income group you belong (in OMR)?

Less than 500	500 - 1,000	1,001 - 1,500	1,501 - 2,000	More than 2,001
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8. If you don't mind that the researcher contacts you for follow up, please provide your details below (Optional)

Name	<input type="text"/>
Contact Number	<input type="text"/>
E-mail Address	<input type="text"/>

B4: Post-questionnaire – Section A (English)

Section A

Section B

Section A: Internet and Banking Facilities

Listed below is a range of services offered via Internet banking. Please indicate how likely it is that you would use each of these services a) using the current system; b) if Multi-channel Authentication (MCA) is implemented by the e-banking system. Rate your answers on the scale (very unlikely) to 5 (very likely) .

	Current System ?					With MCA ?				
Services	1	2	3	4	5	1	2	3	4	5
<i>Payments</i>										
Do inter account funds transfer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Make payment to other personal account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Make payment to other local bank account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transfer funds to credit card account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Do foreign transfer: draft or SWIFT	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Top-up mobile phones	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<i>Requests/Applications</i>										
Order cheque books	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Stop lost ATM cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Stop lost credit cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Apply for a credit card limit change	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Request the issue of a current account statement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Setup standing order transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Setup new account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Apply for foreign currency accounts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Apply for debit/credit card	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Apply for a loan	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Request telephone banking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

B5: Post-questionnaire – Section B (English)

Section A

Section B

Section B: Internet Banking with Multi-Channel Authentication

1. Overall, please indicate how satisfied are you with the following
[Very dissatisfied (1) to Very satisfied (5)]

	1	2	3	4	5
Amount of SMS communication with the site	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ease of performing transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Level of security measures implemented	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2. Please indicate to what extent you agree with the following statements
[Strong Disagree (1) to Strong Agree (5)]

	1	2	3	4	5
If multi-channel authentication (MCA) service is implemented by your bank, I would recommend it to others	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I found MCA easy to use overall	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I expected the MCA to work the way it did	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I trust that MCA would protect me from Internet fraud and attacks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel that MCA has just made things complicated and time-consuming	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
With MCA, I am not worried about using public computers for Internet banking services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I would imagine that most people would learn to use this system very quickly	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I found the alternative channel feature convenient when (in case) my primary channel (for example your mobile phone) is unavailable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I would prefer to use the alternative channel option than making a call-center/help-desk call	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. What changes or additional features would you suggest for Multi-channel authentication?

4. Did you experience any difficulties trying to request a transaction? If Yes, please explain what are these difficulties?

5. Which way did you find most suitable/secure for you to authorise new beneficiary accounts? Entering the OTP (One Time Pin) by a) Web or by b) SMS

Please explain why?

6. If you have other comments/suggestions, please provide them below

B6: Pre-questionnaire – Section A (Arabic)

القسم 1 القسم ب القسم ج

القسم 1: تسهيلات القطاع المصرفي وشبكة الإنترنت

1. أستخدم الإنترنت من الأماكن الآتية:

لا يوجد	يوميًا	أسبوعيًا	شهريًا	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	المنزل
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	العمل
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	المدرسة
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	أماكن عامة (المكتبات، مقاهي الإنترنت، ...)
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	الجهاز النقال (متضمنًا شبكات 3G، GPRS، ...)
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	أخرى: برجاء التحديد

2. إذا كنت تتصل بشبكة الإنترنت يوميًا، ما هو مجموع الدقائق/الساعات التي تقضيها في الشبكة يوميًا؟

حتى 30 دقيقة	ساعة إلى ساعتين	ساعتين إلى 3 ساعات	3 إلى 4 ساعات	أكثر من 4 ساعات
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. هل تستخدم التسهيلات المصرفية عبر شبكة الإنترنت؟

نعم	لا	
<input type="radio"/>	<input type="radio"/>	إن كانت إجابتك "لا"، قم بحفظ الأجوبة وانتقل إلى القسم التالي

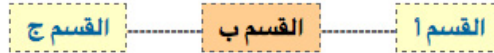
4. ما عدد المصارف التي تستخدم من خلالها خدمة التسهيلات عبر شبكة الإنترنت؟

واحد	إثنان	ثلاثة	أربعة	خمس
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. ما مقدار استخدامك لهذه الخدمة؟

<input type="radio"/>	بشكل يومي
<input type="radio"/>	عدة مرات أسبوعيًا
<input type="radio"/>	مرة واحدة أسبوعيًا
<input type="radio"/>	عدة مرات شهريًا
<input type="radio"/>	مرة واحدة شهريًا
<input type="radio"/>	غير ذلك

B7: Pre-questionnaire – Section B (Arabic)



القسم ب: العوامل المؤثرة في تطبيق خدمة المصرف الإلكتروني

الجدول التالي يعرض قائمة من العوامل المحفزة لاستخدام المصرف الإلكتروني. باستخدام المقياس 1 (عامل غير مؤثر بتاتا) إلى 5 (عامل مؤثر جدا) ، الرجاء تقدير أهمية كل عامل من هذه العوامل في تأثيره عليك لاستخدام المصرف الإلكتروني.

5	4	3	2	1	1. سهولة الوصول
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	أريحية الوصول إلى الخدمة
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	سرعة الاتصال
5	4	3	2	1	2. الثقة بالمصرف وعلاقته مع الزبون
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	مصادقية مصرفك (5 مصادقية عالية إلى 1 مصادقية معدومة)
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	مستوى سرعة الرد على الإستفسارات
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	الأخلاقيات المهنية
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	سياسة المصرف في تعويض الخسائر
5	4	3	2	1	3. التردد
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	رغبة المصرف في التكيف مع التقنية الحديثة
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	مستوى وعي المصرف بخدمة الصرافة الإلكترونية
5	4	3	2	1	4. الأمن
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	وضوح التعليمات
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	أمن المعاملات عبر شبكة الإنترنت
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	طول الخبرة الزمنية في مجال الإنترنت
5	4	3	2	1	5. الرضى والارتياح
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	تعدد الخدمات الإلكترونية المعروضة
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	الطريقة الأنسب لاستخدام المعاملات المصرفية
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	توفير الوقت
5	4	3	2	1	6. سهولة الاستخدام
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	سلاسة استخدام الموقع الإلكتروني
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	سهولة إنجاز المعاملات الإلكترونية

B8: Pre-questionnaire – Section C (Arabic)

القسم ج

القسم ب

القسم أ

القسم ج: سجل المشارك

1. الجنس؟

ذكر	أنثى
<input type="radio"/>	<input type="radio"/>

2. الحالة الاجتماعية؟

أعزب	متزوج	مطلق	أخرى
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. لأي المجموعات العمرية تنتمي (بالسنوات)؟

27 - 18	37 - 28	47 - 38	57 - 48	67 - 58	أكثر من 67
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4. ما أعلى شهادة علمية حصلت عليها

<input type="radio"/>	شهادة عامة أو ما يعادلها
<input type="radio"/>	دبلوم فني / مهني
<input type="radio"/>	شهادة جامعية (4 سنوات دراسية)
<input type="radio"/>	شهادة ماجستير أو ما يعادلها
<input type="radio"/>	شهادة دكتوراه

5. ما وظيفتك الحالية؟

طالب	أعمال حرّة	موظف حكومي	فني	موظف خدمات
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
موظف قطاع خاص	موظف مبيعات	متقاعد	باحث عن عمل	أخرى (الرجاء ذكر المهنة)
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

6. ما المجال التجاري الذي تنتمي إليه المؤسسة التي تعمل بها؟

<input type="radio"/>	الخدمات المصرفية والمالية (المؤسسات المالية، التأمين، والسمسة)
<input type="radio"/>	النقل والتوزيع
<input type="radio"/>	خدمية واتصالات
<input type="radio"/>	تجارية
<input type="radio"/>	تعليمية
<input type="radio"/>	القطاع الخدمي (إضافة إلى الفنادق والمطاعم)
<input type="radio"/>	القطاع الزراعي
<input type="radio"/>	أعمال حرّة، الرجاء التفصيل: <input type="text"/>
<input type="radio"/>	غير ذلك، الرجاء التفصيل: <input type="text"/>

7. لأي مجموعة دخل شهري تنتمي (بالريال العماني)؟

أقل من 500	500 - 1000	1001 - 1500	1501 - 2000	أكثر من 2000
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8. إذا لم يكن لديك مانع من تواصل الباحث معكم بخصوص هذه الدراسة في وقت لاحق، برجاء إضافة التفاصيل الآتية: (اختياري)

<input type="text"/>	الاسم
<input type="text"/>	رقم الهاتف
<input type="text"/>	عنوان البريد الإلكتروني

B9: Post-questionnaire – Section A (Arabic)

القسم ب

القسم أ

القسم أ: التسهيلات الشبكية (الإنترنت) والمصرفية

المدرجة أدناه مجموعة من الخدمات المصرفية المقدمة عبر الإنترنت. يرجى بيان مدى احتمالية استخدامك لكل خدمة من هذه الخدمات (أ) من خلال النظام التقليدي؛ (ب) من خلال نظام المصادقة المتعددة القنوات. استخدم المقياس من 1 (مستبعد جداً) إلى 5 (مرجح جداً).

نظام المصادقة المتعددة القنوات ؟					النظام التقليدي ؟						
5	4	3	2	1	5	4	3	2	1	الخدمات	
										المدفوعات	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	تحويل ضمن نطاق حساباتك الشخصية	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	تحويل لحساب شخصي آخر	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	تحويل لحساب آخر في نفس المصرف	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	تحويل لحساب بطاقة الائتمان	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	تحويل دولي	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	تعبئة رصيد أجهزة النقال	
										طلبات/مميزات	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	طلب دفاتر الشيكات	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	إيقاف بطاقات السحب الآلي المفقودة	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	إيقاف بطاقات الائتمان المفقودة	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	تغيير سقف بطاقة الائتمان	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	إصدار كشف الحساب الحالي	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	إنشاء حوالة دورية	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	إنشاء حساب مصرفي جديد	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	طلب حساب عملات أجنبية	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	تقديم طلب بطاقة التمان/صرف	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	تقديم طلب قرض	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	طلب خدمة الصرافة الهاتفية	

B10: Post-questionnaire – Section B (Arabic)

القسم ب

القسم 1

القسم ب: المصرف الإلكتروني من خلال نظام المصادقة المتعددة القنوات

1. بشكل عام، ما مدى رضاك عن ما يلي [غير راضٍ تماماً. (1) إلى راضٍ تماماً. (5)]

5	4	3	2	1	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	عدد الرسائل النصية المستخدمة لإنجاز المعاملات في الموقع
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	سهولة إنجاز المعاملات
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	مستوى مقاييس الأمان المستخدمة

2. ما مدى اتفاقك مع ما يلي [غير موافق تماماً. (1) إلى موافق تماماً. (5)]

5	4	3	2	1	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	إذا تم تفعيل نظام المصادقة المتعددة القنوات في مصرفي، سأقوم بإقناع الآخرين لاستخدامه
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	نظام المصادقة المتعددة القنوات سهل الاستخدام بشكل عام
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	أتصور أن يعمل نظام المصادقة المتعددة القنوات حسب ما تم تصميمه من أجله
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	أثق في أن نظام المصادقة المتعددة القنوات سيحمي حسابي المصرفي من الإختراقات والسرقات عبر الإنترنت
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	أعتقد أن نظام المصادقة المتعددة القنوات هو نظام معقد ويستهلك الوقت
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	لم أجد أشعر بالخوف الأمني حين استخدام خدمة المصرف الإلكتروني عبر الأجهزة العامة (مقاهي الإنترنت مثلاً) مع وجود نظام المصادقة المتعددة القنوات.
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	أعتقد أن معظم المستخدمين سيتعلمون استخدام هذا النظام بشكل سريع
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	وجدت أن خدمة القناة البديلة مناسبة لي في حالة غياب هاتفي النقال
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	أفضل استخدام خيار القناة البديلة عوضاً عن الاتصال لمركز الاتصال أو قسم المساعدة الخاص بالمصرف.

3. ما هي الخصائص الإضافية التي تود أن تراها في نظام المصادقة المتعددة القنوات؟

4. هل واجهت أي مشاكل حين إجراء أي معاملات؟ إن كانت الإجابة بنعم، الرجاء تفصيل هذه المشاكل.

5. أي الطرق المستخدمة في تفعيل حسابات المستخدمين وجدتها أفضل وأمن؟ إدخال الرقم السري عبر (1) الإنترنت أو عبر ب) إرسالها عن طريق رسالة نصية قصيرة SMS

الرجاء تفصيل السبب.

6. إذا كانت لديك أي إضافات أخرى، نرجو تزويدنا بها من خلال الصندوق التالي

Appendix C

Data Screening Results

C1: Pre-questionnaire data frequency and missing details (all participants)

Variables	N = 188			Mean	Min.	Max.
	Valid	Missing	%			
Do you make use of Internet banking facility?	185	3	1.6	0.54	0	1
Please state your gender	186	2	1.1	0.67	0	1

Based on two options (0 and 1)

Variables	N = 188			Mean	Min.	Max.
	Valid	Missing	%			
How frequently do you access the Internet from Home?	182	6	3.2	1.55	1	4
How frequently do you access the Internet from Work?	181	7	3.7	1.73	1	4
How frequently do you access the Internet from School?	159	29	15.4	3.16	1	4
How frequently do you access the Internet from Public?	166	22	11.7	3.36	1	4
How frequently do you access the Internet from Mobile?	173	15	8.0	2.55	1	4
How frequently do you access the Internet from other places?	85	103	54.8	3.81	1	4
What is your marital status?	182	6	3.2	1.59	1	2

Based on four options (1 to 4)

Variables	N = 188			Mean	Min.	Max.
	Valid	Missing	%			
How often do you make use of Internet banking service?	119	69	36.7	3.39	1	6
Please indicate your age group (in years)	182	6	3.2	1.70	1	4

Based on six options (1 to 6)

Variables	N = 188			Mean	Min.	Max.
	Valid	Missing	%			
What type of business area best describes your organization?	164	24	12.8	4.98	1	9

Based on nine options (1 to 9)

Variables	N = 188			Mean	Min.	Max.
	Valid	Missing	%			
If you access the Internet daily, how many minutes/hours in total do you usually spend on it each day?	181	7	3.7	3.36	1	5
With how many banks do you do your Internet banking services?	114	74	39.4	1.65	1	5
To which monthly income group you belong (in OMR)?	172	16	8.5	2.33	1	5
Which is your highest level of education?	154	34	18.1	3.17	2	5
Accessibility: convenience to access the service	181	7	3.7	3.95	1	5
Accessibility: connection speed	182	6	3.2	3.94	1	5
T&R*: reliability of your banker	179	9	4.8	3.99	1	5
T&R*: bank response rate to queries	183	5	2.7	3.67	1	5
T&R*: Ethical and professional conduct	179	9	4.8	3.89	1	5
T&R*: bank's policy to compensate for losses	178	10	5.3	3.62	1	5
Reluctance: the bank willingness to adopt technology	181	7	3.7	3.89	1	5
Reluctance: the bank level of awareness of the Internet banking service	177	11	5.9	3.99	1	5
Security: clear and understandable instructions	182	6	3.2	4.12	1	5
Security: security of Internet transaction	179	9	4.8	4.04	1	5
Security: length of Internet experience	179	9	4.8	3.72	1	5
Convenience: range of electronic services offered	180	8	4.3	3.77	1	5
Convenience: convenient way of doing bank transactions	180	8	4.3	3.84	1	5
Convenience: time saving	179	9	4.8	4.16	1	5
Ease of use: user friendly web site	182	6	3.2	4.03	1	5
Ease of use: ease of performing e-transaction	180	8	4.3	4.07	1	5

* Trust and relationship

Based on five options (1 to 5)

Variables	N = 188			Mean	Min.	Max.
	Valid	Missing	%			
What is your current occupation?	178	10	5.3	3.66	1	10

Based on ten options (1 to 10)

C2: Post-questionnaire data frequency and missing details (participants who completed all tasks)

Variables	N = 90			Mean	Min.	Max.
	Valid	Missing	%			
<i>Current Systems</i>						
Payments: Do inter account funds transfer	88	2	2.2	3.3	1	5
Payments: Make payment to other personal account	89	1	1.1	2.84	1	5
Payments: Make payment to other local bank acct.	89	1	1.1	2.94	1	5
Payments: Transfer funds to credit card account	88	2	2.2	3.16	1	5
Payments: Do foreign transfer: draft or SWIFT	87	3	3.3	2.47	1	5
Payments: Top-up mobile phones	87	3	3.3	2.61	1	5
Requests: Order cheque books	89	1	1.1	3.3	1	5
Requests: Stop lost ATM cards	89	1	1.1	3.35	1	5
Requests: Stop lost credit cards	88	2	2.2	3.32	1	5
Requests: Apply for a credit card limit change	88	2	2.2	2.98	1	5
Requests: Request the issue of a current account statement	89	1	1.1	3.73	1	5
Requests: Setup standing order transactions	86	4	4.4	2.93	1	5
Requests: Setup new account	90	0	0	2.84	1	5
Requests: Apply for foreign currency accounts	87	3	3.3	2.95	1	5
Requests: Apply for debit/credit card	87	3	3.3	2.86	1	5
Requests: Apply for a loan	86	4	4.4	2.63	1	5
Requests: Request telephone banking	87	3	3.3	2.84	1	5
<i>Multichannel Authentication (MCA)</i>						
Payments: Do inter account funds transfer	88	2	2.2	4.1	1	5
Payments: Make payment to other personal account	87	3	3.3	4.22	1	5
Payments: Make payment to other local bank acct.	88	2	2.2	4.24	1	5
Payments: Transfer funds to credit card account	89	1	1.1	4.07	1	5
Payments: Do foreign transfer: draft or SWIFT	87	3	3.3	3.8	1	5
Payments: Top-up mobile phones	87	3	3.3	4.08	1	5
Requests: Order cheque books	88	2	2.2	3.78	1	5
Requests: Stop lost ATM cards	89	1	1.1	4.04	1	5
Requests: Stop lost credit cards	87	3	3.3	4	1	5
Requests: Apply for a credit card limit change	89	1	1.1	3.85	1	5
Requests: Request the issue of a current account statement	87	3	3.3	4.43	1	5
Requests: Setup standing order transactions	86	4	4.4	4.05	1	5
Requests: Setup new account	88	2	2.2	3.77	1	5
Requests: Apply for foreign currency accounts	86	4	4.4	3.59	1	5
Requests: Apply for debit/credit card	88	2	2.2	3.91	1	5
Requests: Apply for a loan	89	1	1.1	3.43	1	5
Requests: Request telephone banking	89	1	1.1	3.93	1	5

Post-questionnaire: section A questions

Variables	N = 90			Mean	Min.	Max.
	Valid	Missing	%			
Question 1						
Amount of SMS communication with the site	89	1	1.1	4.26	2	5
Ease of performing transactions	89	1	1.1	4.31	2	5
Level of security measures implemented	89	1	1.1	4.28	1	5
Question 2						
If multi-channel authentication (MCA) service is implemented by your bank, I would recommend it to others	89	1	1.1	4.36	3	5
I found MCA easy to use overall	89	1	1.1	4.3	2	5
I expected the MCA to work the way it did	89	1	1.1	4.16	3	5
I trust that MCA would protect me from Internet fraud and attacks	88	2	2.2	4.03	1	5
I feel that MCA has just made things complicated and time-consuming	89	1	1.1	2.28	1	5
With MCA, I am not worried about using public computers for Internet banking services	88	2	2.2	3.59	1	5
I would imagine that most people would learn to use this system very quickly	89	1	1.1	3.84	1	5
I found the alternative channel feature convenient when (in case) my primary channel (for example your mobile phone) is unavailable	87	3	3.3	4.28	1	5
I would prefer to use the alternative channel option than making a call-center/help-desk call	88	2	2.2	4.19	1	5

Post-questionnaire: section B questions

Appendix D

Demographics Characteristics

D1: Relationship between Demographic Profile of Participants and Dropout Rates

Gender and Completed Crosstabulations					Completed?			
Value	df	Sig.	Missing		No	Yes	Total	
0.605**	1	.437	2	Female	Count	34	28	62
					% within Gender	54.8%	45.2%	100.0%
					% within Completed?	36.6%	30.1%	33.3%
					% of Total	18.3%	15.1%	33.3%
				Male	Count	59	65	124
					% within Gender	47.6%	52.4%	100.0%
					% within Completed?	63.4%	69.9%	66.7%
					% of Total	31.7%	34.9%	66.7%
				Total	Count	93	93	186
					% within Gender	50.0%	50.0%	100.0%
					% within Completed?	100.0%	100.0%	100.0%
					% of Total	50.0%	50.0%	100.0%

* based on Pearson Chi-Square

** based on Continuity Correction (computed only for a 2x2 table)

Relationship between Gender and Dropout Rates

Marital Status and Completed Crosstabulations						Completed?		
Value	df	Sig.	Missing			No	Yes	Total
.023**	1	.880	6	Single	Count	36	38	74
					% within M. Status	48.6%	51.4%	100.0%
					% within Completed?	39.6%	41.8%	40.7%
					% of Total	19.8%	20.9%	40.7%
				Married	Count	55	53	108
					% within M. Status	50.9%	49.1%	100.0%
					% within Completed?	60.4%	58.2%	59.3%
					% of Total	30.2%	29.1%	59.3%
				Total	Count	91	91	182
					% within M. Status	50.0%	50.0%	100.0%
					% within Completed?	100.0%	100.0%	100.0%
					% of Total	50.0%	50.0%	100.0%

* based on Pearson Chi-Square

** based on Continuity Correction (computed only for a 2x2 table)

Relationship between Marital Status and Dropout Rates

Education Level and Completed Crosstabulations					Completed?			
Value	df	Sig.	Missing			No	Yes	Total
19.607*	3	.000	34	Technical / Professional Training	Count	19	4	23
					% within Edu. Level	82.6%	17.4%	100.0%
					% within Completed?	24.1%	5.3%	14.9%
					% of Total	12.3%	2.6%	14.9%
				College grad. (4 years)	Count	43	44	87
					% within Edu. Level	49.4%	50.6%	100.0%
					% within Completed?	54.4%	58.7%	56.5%
					% of Total	27.9%	28.6%	56.5%
				Master deg. or equivalent	Count	17	22	39
					% within Edu. Level	43.6%	56.4%	100.0%
					% within Completed?	21.5%	29.3%	25.3%
					% of Total	11.0%	14.3%	25.3%
				Postgraduate degree	Count	0	5	5
					% within Edu. Level	0%	100.0%	100.0%
					% within Completed?	0%	6.7%	3.2%
					% of Total	0%	3.2%	3.2%
				Total	Count	79	75	154
					% within Edu. Level	51.3%	48.7%	100.0%
					% within Completed?	100.0%	100.0%	100.0%
					% of Total	51.3%	48.7%	100.0%

* based on Pearson Chi-Square

** based on Continuity Correction (computed only for a 2x2 table)

Relationship between Education Level and Dropout Rates

Education Level and Completed Crosstabulations					Completed?			
Value	df	Sig.	Missing			No	Yes	Total
9.928*	2	.007	39	Technical / Professional Training	Count	19	4	23
					% within Edu. Level	82.6%	17.4%	100.0%
					% within Completed?	24.1%	5.7%	15.4%
					% of Total	12.8%	2.7%	15.4%
				College grad. (4 years)	Count	43	44	87
					% within Edu. Level	49.4%	50.6%	100.0%
					% within Completed?	54.4%	62.9%	58.4%
					% of Total	28.9%	29.5%	58.4%
				Master deg. or equivalent	Count	17	22	39
					% within Edu. Level	43.6%	56.4%	100.0%
					% within Completed?	21.5%	31.4%	26.2%
					% of Total	11.4%	14.8%	26.2%
				Total	Count	79	70	149
					% within Edu. Level	53.0%	47.0%	100.0%
					% within Completed?	100.0%	100.0%	100.0%
					% of Total	53.0%	47.0%	100.0%

* based on Pearson Chi-Square

** based on Continuity Correction (computed only for a 2x2 table)

Relationship between Education Level and Dropout Rates (without the postgraduate degree group)

Age Group and Completed Crosstabulations					Completed?			
Value	df	Sig.	Missing		No	Yes	Total	
2.131*	3	.546	6	18 to 27	Count	39	36	75
					% within Age Group	52.0%	48.0%	100.0%
					% within Completed?	42.9%	39.6%	41.2%
					% of Total	21.4%	19.8%	41.2%
				28 to 37	Count	44	45	89
					% within Age Group	49.4%	50.6%	100.0%
					% within Completed?	48.4%	49.5%	48.9%
					% of Total	24.2%	24.7%	48.9%
				38 to 47	Count	8	8	16
					% within Age Group	50.0%	50.0%	100.0%
					% within Completed?	8.8%	8.8%	8.8%
					% of Total	4.4%	4.4%	8.8%
				48 to 57	Count	0	2	2
					% within Age Group	0.0%	100.0%	100.0%
					% within Completed?	0.0%	2.2%	1.1%
					% of Total	0.0%	1.1%	1.1%
				Total	Count	91	91	182
					% within Age Group	50.0%	50.0%	100.0%
					% within Completed?	100.0%	100.0%	100.0%
					% of Total	50.0%	50.0%	100.0%

* based on Pearson Chi-Square

Relationship between Age Group and Dropout Rates

Monthly Income Group (in OMR) and Completed Crosstabulations					Completed?			
Value	df	Sig.	Missing		No	Yes	Total	
5.080*	4	.279	16	Less than 500	Count	15	18	33
					% within Income Grp.	45.5%	54.5%	100.0%
					% within Completed?	18.1%	20.2%	19.2%
					% of Total	8.7%	10.5%	19.2%
				500 – 1,000	Count	43	41	84
					% within Income Grp.	51.2%	48.8%	100.0%
					% within Completed?	51.8%	46.1%	48.8%
					% of Total	25.0%	23.8%	48.8%
				1,001 – 1,500	Count	11	20	31
					% within Income Grp.	35.5%	64.5%	100.0%
					% within Completed?	13.3%	22.5%	18.0%
					% of Total	6.4%	11.6%	18.0%
				1,501 – 2,000	Count	6	7	13
					% within Income Grp.	46.2%	53.8%	100.0%
					% within Completed?	7.2%	7.9%	7.6%
					% of Total	3.5%	4.1%	7.6%
				More than 2,001	Count	8	3	11
					% within Income Grp.	72.7%	27.3%	100.0%
					% within Completed?	9.6%	3.4%	6.4%
					% of Total	4.7%	1.7%	6.4%
				Total	Count	83	89	172
					% within Income Grp.	48.3%	51.7%	100.0%
					% within Completed?	100.0%	100.0%	100.0%
					% of Total	48.3%	51.7%	100.0%

* based on Pearson Chi-Square

Relationship between Monthly Income and Dropout Rates

Social Relationship and Completed Crosstabulations						Completed?		
Value	df	Sig.	Missing			No	Yes	Total
33.142*	1	.000	0	Others	Count	84	11	95
					% within Completed the requirements?	88.4%	11.6%	100.0%
					% within Is Friend?	65.1%	18.6%	50.5%
					% of Total	44.7%	5.9%	50.5%
				Friends & Colleagues	Count	45	48	93
					% within Completed the requirements?	48.4%	51.6%	100.0%
					% within Is Friend?	34.9%	81.4%	49.5%
					% of Total	23.9%	25.5%	49.5%
				Total	Count	129	59	188
					% within Completed the requirements?	68.6%	31.4%	100.0%
					% within Is Friend?	100.0%	100.0%	100.0%
					% of Total	68.6%	31.4%	100.0%

* based on Continuity Correction (computed only for a 2x2 table)

Relationship between Social Relationship and Dropout Rates

D2: Relationship between Demographic Profile of Participants and Online Banking Experience

Have used online banking before?					Completed?		Total
Value	df	Sig.	Missing		No (%)	Yes (%)	
5.293*	1	.021	3	No	52 (60.5%)	34 (39.5%)	86
				Yes	42 (42.4%)	57 (57.6%)	99
				Total	94 (50.8%)	91 (49.2%)	185

* based on Continuity Correction (computed only for a 2x2 table)

Relationship between Tasks Completion and Online Banking Experience

Education Level and OB Experience Crosstabulations						OB User?		
Value	df	Sig.	Missing			No	Yes	Total
18.406*	2	.000	2	Technical / Professional Training	Count	14	8	22
					% within Edu. Level	64%	36%	100%
					% within OB User	22%	9%	15%
					% of Total	9%	5%	15%
				College grad. (4 years)	Count	44	44	88
					% within Edu. Level	50%	50%	100%
					% within OB User	69%	51%	59%
					% of Total	29%	29%	59%
				Master deg. or equivalent	Count	6	34	40
					% within Edu. Level	15%	85%	100%
					% within OB User	9%	40%	27%
					% of Total	4%	23%	27%
				Total	Count	64	86	150
					% within Edu. Level	43%	57%	100%
					% within OB User	100%	100%	100%
					% of Total	43%	57%	100%

* based on Pearson Chi-Square

Relationship between Education Level and OB Experience (without postgraduate degree group)

Age Group and Online Banking Experience Crosstabulations						OB User?		
Value	df	Sig.	Missing			No	Yes	Total
10.956*	1	.001	3	18 to 27	Count	44	28	72
					% within Age Group	61.1%	38.9%	100.0%
					% within OB User	59.5%	32.2%	44.7%
					% of Total	27.3%	17.4%	44.7%
				28 to 37	Count	30	59	89
					% within Age Group	33.7%	66.3%	100.0%
					% within OB User	40.5%	67.8%	55.3%
					% of Total	18.6%	36.6%	55.3%
				Total	Count	74	87	161
					% within Age Group	46.0%	54.0%	100.0%
					% within OB User	100.0%	100.0%	100.0%
					% of Total	46.0%	54.0%	100.0%

* based on Continuity Correction (computed only for a 2x2 table)

Relationship between Age Group and Online Banking Experience (without age groups 38 to 47 and 48 to 57)

D3: Factor Analysis – Component Matrix and Screeplot

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings ^a
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	7.125	50.890	50.890	7.125	50.890	50.890	5.881
2	1.325	9.467	60.357	1.325	9.467	60.357	4.720
3	.889	6.348	66.705	.889	6.348	66.705	3.810
4	.761	5.438	72.143	.761	5.438	72.143	3.498
5	.687	4.910	77.053				
6	.635	4.536	81.589				
7	.497	3.550	85.139				
8	.436	3.117	88.256				
9	.408	2.917	91.173				
10	.379	2.711	93.883				
11	.278	1.988	95.872				
12	.262	1.872	97.743				
13	.183	1.309	99.053				
14	.133	.947	100.000				

Extraction Method: Principal Component Analysis.

a. When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

Pattern Matrix^a

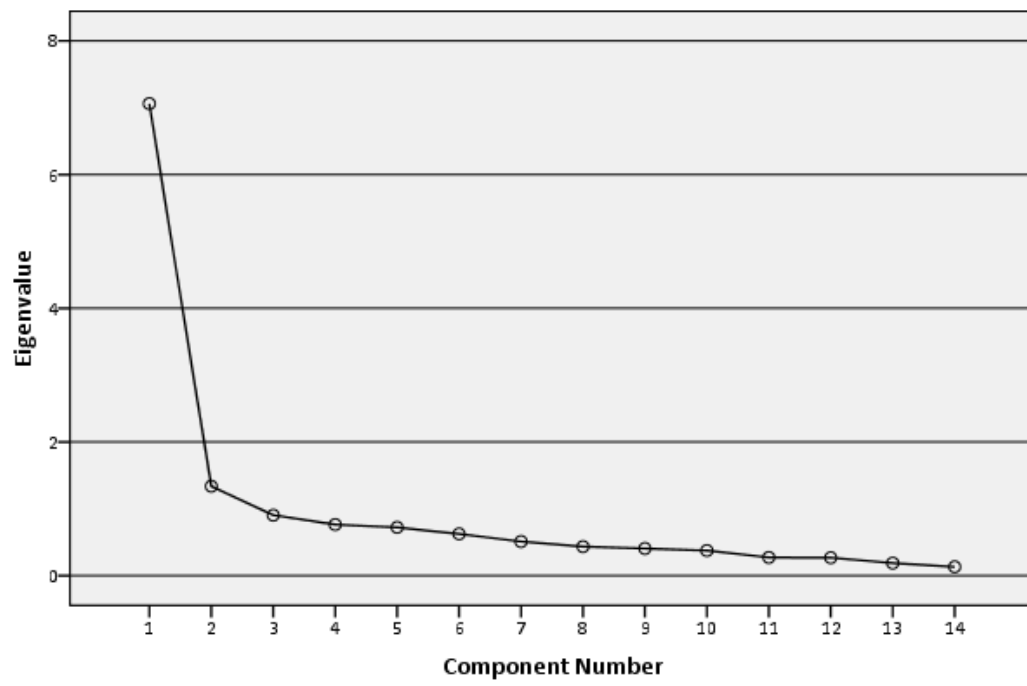
	Component			
	1	2	3	4
B5b	.899			
B5c	.851			
B6b	.789			
B6a	.694			
B5a	.665			
B2b		.821		
B2c		.780		
B2d		.775		
B2a		.584		
B4c			-.849	
B4b			-.677	
B4a			-.519	
B1b				.892
B1a				.716

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 8 iterations.

Scree Plot



D4: Independent-Sample T-Test – External Variables

	Online banking user?	N	Mean	Std. Deviation	Std. Error Mean
Trust and Relationship	No	88	3.50	.916	.098
	Yes	100	4.02	.792	.079
Accessibility	No	88	3.65	1.281	.137
	Yes	100	4.21	.998	.100
Security	No	88	3.70	1.054	.112
	Yes	100	4.10	.792	.079
Perceived ease of use	No	88	3.70	1.076	.115
	Yes	100	4.18	.794	.079

Group Statistics

Factors	Levene's Test for Equality of Variances		t-test for Equality of Means						
	F	Sig.	t	df	Sig. (2- tailed)	M Diff.	S. Err. Diff.	95% Conf. Inter. of the Diff.	
								Lower	Upper
Trust and relationship									
Equal variances assumed	4.323	.039	-4.198	186	.000	-.523	.125	-.769	-.277
Equal var. not assumed			-4.160	173.185	.000	-.523	.126	-.771	-.275
Accessibility									
Equal variances assumed	8.413	.004	-3.314	186	.001	-.552	.166	-.880	-.223
Equal var. not assumed			-3.262	163.715	.001	-.552	.169	-.885	-.218
Security									
Equal variances assumed	11.033	.001	-2.943	186	.004	-.398	.135	-.664	-.131
Equal var. not assumed			-2.891	160.227	.004	-.398	.138	-.669	-.126
Perceived ease of use									
Equal variances assumed	12.230	.001	-3.495	186	.001	-.478	.137	-.748	-.208
Equal var. not assumed			-3.430	158.377	.001	-.478	.139	-.754	-.203

Independent Samples Test

D4: Paried-Sample T-Test – Online Users’ Preferences on Services Usage between Online Banking Systems with MCA and without MCA

		Mean	N	Std. Deviation	Std. Error Mean
Q 1	With	4.18	62	1.064	.135
	Without	3.37	62	1.149	.146
Q 2	With	4.21	61	1.002	.128
	Without	2.79	61	1.318	.169
Q 3	With	4.26	62	.974	.124
	Without	2.82	62	1.248	.159
Q 4	With	4.10	61	.961	.123
	Without	3.25	61	1.234	.158
Q 5	With	3.70	60	1.253	.162
	Without	2.33	60	1.311	.169
Q 6	With	4.05	60	1.171	.151
	Without	2.60	60	1.210	.156
Q 7	With	3.75	61	1.337	.171
	Without	3.34	61	1.250	.160
Q 8	With	3.95	62	1.247	.158
	Without	3.44	62	1.288	.164
Q 9	With	3.95	61	1.217	.156
	Without	3.38	61	1.319	.169
Q 10	With	3.79	61	1.280	.164
	Without	2.97	61	1.224	.157
Q 11	With	4.36	61	1.065	.136
	Without	3.80	61	1.093	.140
Q 12	With	4.11	61	1.142	.146
	Without	2.89	61	1.185	.152
Q 13	With	3.68	62	1.352	.172
	Without	2.73	62	1.405	.178
Q 14	With	3.41	59	1.403	.183
	Without	2.98	59	1.383	.180
Q 15	With	3.89	61	1.199	.153
	Without	2.93	61	1.340	.172
Q 16	With	3.36	59	1.336	.174
	Without	2.59	59	1.301	.169
Q 17	With	3.77	60	1.320	.170
	Without	2.87	60	1.268	.164

Paired Samples Statistics

	Paired Differences					t	df	Sig. (2-tailed)
	Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
				Lower	Upper			
Q 1	.806	1.491	.189	.428	1.185	4.258	61	.000
Q 2	1.426	1.500	.192	1.042	1.810	7.428	60	.000
Q 3	1.435	1.543	.196	1.044	1.827	7.325	61	.000
Q 4	.852	1.314	.168	.516	1.189	5.065	60	.000
Q 5	1.367	1.775	.229	.908	1.825	5.963	59	.000
Q 6	1.450	1.466	.189	1.071	1.829	7.660	59	.000
Q 7	.410	1.564	.200	.009	.810	2.047	60	.045
Q 8	.516	1.734	.220	.076	.957	2.343	61	.022
Q 9	.574	1.756	.225	.124	1.023	2.553	60	.013
Q 10	.820	1.607	.206	.408	1.231	3.983	60	.000
Q 11	.557	1.467	.188	.182	.933	2.968	60	.004
Q 12	1.230	1.359	.174	.881	1.578	7.067	60	.000
Q 13	.952	1.928	.245	.462	1.441	3.886	61	.000
Q 14	.424	1.868	.243	-.063	.911	1.742	58	.087
Q 15	.951	1.755	.225	.501	1.400	4.231	60	.000
Q 16	.763	1.794	.234	.295	1.230	3.266	58	.002
Q 17	.900	1.674	.216	.467	1.333	4.164	59	.000

Paired Samples Test