

THE USABILITY AND SECURITY OF ENCRYPTION APPLICATIONS USING TOKEN-BASED AUTHENTICATION

A thesis submitted in partial fulfilment of the requirements for the degree of
Master of Science in Information Security

By:

Riham AlMahawes

Under Supervision of:

Dr. Fahad Al- Harby

Submitted to:

Department of Information Security, Computer and Information Security College
Naïf Arab University for Security Sciences

April 2019

Table of Contents

Abstract	ii
Acknowledgment	iv
Statement of Original Authorship	v
Table of Contents	vi
List of Figures	vii
List of Tables.....	ix
List of Abbreviations.....	x
Chapter 1: Introduction	1
1.1 Overview.....	1
1.2 objectives	2
1.3 Problem statement.....	3
1.4 contribution	4
1.5 Motivation.....	4
1.6 Scope.....	4
1.7 Thesis organization	5
Chapter 2: Background and Literature Review	7
2.1 Background	7
2.2 Related works.....	33
2.3 Summary	50
Chapter 3: Methodology.....	53
3.1 Methodology	54
3.2 Ethical considerations	72
Chapter 4: Results and Discussions.....	75
4.1 Usability Evaluation.....	75
4.2 Security Evaluation	107
Chapter 5: Conclusion and Future Work.....	123
5.1 Conclusion	123
5.2 limitations.....	123
5.3 Future Work	124
References	125
Appendices	135
Arabic Summary	143

List of Figures

Figure 2. 1 Public Key Infrastructure Components	8
Figure 2. 7 The Penetration Testing Phases by NIST (Scarfone et al., 2008).	25
Figure 3.1 High-Level architecture of Entrust Managed Services PKI™ application.....	67
Figure 3.2 The Penetration Testing Process	71
Figure 4. 2 Workflow Diagram of Task# 1: Logging into WebRA Administration Application.	76
Figure 4. 3 Workflow Diagram of Task#2: Issuing a Digital Name Certificate for a User	77
Figure 4. 4 Workflow Diagram of Task#3: Issuing a Digital Email Certificate for a User.	78
Figure 4. 5 Workflow Diagram of Task#4: Approve Pending Requests.....	79
Figure 4. 6 Workflow Diagram of Task#5: Revoke Digital Certificate for a User.....	81
Figure 4. 7 Workflow Diagram of Task#6: Recover Digital Certificate for a User.....	82
Figure 4. 8 Workflow Diagram of Task#7: Personalization of SafeNet token	83
Figure 4. 9 Workflow Diagram of Task #8: Enrolment a Digital ID on SafeNet Token	84
Figure 4. 10 Workflow Diagram of Task #9: Change PIN Password of A Token.....	85
Figure 4. 11 Workflow Diagram of Task #10: Digitally Sign an Email Message	86
Figure 4. 12 Workflow Diagram of Task #11: Verify a Digitally Signed Email Message.....	87
Figure 4. 13 Workflow Diagram of Task #12: Encrypt Email Message	88
Figure 4. 14 Workflow Diagram of Task #13: Decrypt an Encrypted Email Message	89
Figure 4. 15 Workflow Diagram of Task #14: Digitally Sign a Document	90
Figure 4. 16 Workflow Diagram of Task #15: Verify a Digitally Signed Document.	91
Figure 4. 17 Workflow Diagram of Task #16: Encrypt A Document.	92
Figure 4. 18 Workflow Diagram of Task #17: Decrypt an Encrypted Document	93
Figure 4. 19 The Average of Effectiveness score of Each Task.....	94

Figure 4. 20 The Average Efficiency Score Per Task.....	95
Figure 4. 21 Average Satisfaction Score per Tasks	96
Figure 4. 23 The Usability Rate of Enrollment a Digital ID on a Token By RA and End Users.....	99
Figure 4. 24 Usability Attributes of Encrypting a Document	100
Figure 4. 25 The Usability Attributes of Digitally Signing a Document.....	101
Figure 4. 26 The Usability Attributes of Logging into WebRA Administration	102
Figure 4. 27 The difference of usability attributes between RA and end users for Task #18	102
Figure 4. 28 To-Be Business Process Modelling of Enrolment a Digital ID on a Token.....	104
Figure 4. 29 To-Be Business Process Modelling of Encrypting a Document	105
Figure 4. 30 To-Be Business Process Modelling of digitally signing a document.....	106
Figure 4. 31 VBA code of the used macro virus	112
Figure 4. 32 The warning message of the application	113
Figure 4. 33 Likelihood of Threat Agent Factors	115
Figure 4. 34 Likelihood of the Vulnerability Factors.....	116
Figure 4. 35 The Overall Estimated Likelihood for each Vulnerability	117
Figure 4. 36 The Factors of Technical Impact.....	118
Figure 4. 37 Factors of Business Impacts	119
Figure 4. 38 The Overall Estimated Impact	120

List of Tables

Table 2-1 Measures of effectiveness, efficiency, and satisfaction (Bevan, 2016)	15
Table 2-2 The CIS Security Metrics (Houngbo and Hounsou, 2015)	17
Table 2-3 Severity Levels	33
Table 2-4 Comparison of Vulnerability Assessment and Penetration testing (Doshi and Trivedi, 2015)	45
Table 3-1 The Demographic Characteristics of the Participants	57
Table 3-2 Comparison between the Most Common Security Standards	70
Table 4-1 Usability Score for Each Task	97
Table 4-2 Threat Agent Factors	114
Table 4-3 Likelihood of the Vulnerability Factors	116
Table 4-4 The Overall Estimated Likelihood	117
Table 4-5 The Factors of Technical Impact	118
Table 4-6 Factors of Business Impacts	119
Table 4-7 The Overall Estimated Impacts	119
Table 4-8 The Estimated Likelihood and Impacts with the Severity Level	120

List of Abbreviations

Abbreviations	Explanations
3DES	Triple DES
AES	Advanced Encryption Standard
API	Application programming interface
ASQ	Ages and Stages Questionnaires
ASVS	The OWASP Application Security Verification Standard
CA	Certificate Authority
CBS	Crypto-Biometric System
CC	Common Criteria
CERT	A Computer Emergency Response Team
CIF	Common Industry Format Standards
CIS	Centre for Internet Security
CMA	Crypto Misuse Analyzer
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certification Revocation List
DES	Data Encryption Standard
DMAIC	Define, Measure, Analyse, Improve and Control
ESP	Entrust Intelligence Security Provider
GLBA	Gramm-Leach-Bliley Act
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
ID	Identification Number
IP	Internet Protocol
ISO	International Standards Organization
ISSAF	Information Systems Security Assessment Framework
KKESH	King Khaled Eye Specialist Hospital
NIST	US National Institute of Standard and Technology
OSSTMM	Open Source Security Testing Methodology
OWASP	Open Web Application Security Project

PA	Policy Administrator
PACMAD	People at the Centre of Mobile Application Development
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PTES	Penetration Testing Execution Standard
RA	Registration Authority
SAC	SafeNet Authentication Client
SCR	Certificate Signing Request
SDLC	Software Development Life Cycle
SEQ	Single Ease Question
SMEQ	Subjective Mental Effort Questionnaire
UME	Usability Magnitude Estimation
USB	Uniform Resource Locator.
VA	Validation Authority
VBA	Visual Basic for Applications
VPN	Virtual private network
WWW	World Wide Web