ET 01/98

LB/DON/86/2014

Enhancing Security of ICA-AtoM: The Web-Based Archival Description Software

LIBRARY
UNIVERSITY OF MORATUWA, SRI LANKA
MORATUWA

Karunarathne W K S

Registration No: 108563P

Index No: MSc/IT/09/011

University of Moratuwa
107127

Supervisor: Dr. Prasad Wimalarathne

004 "13"
004(043)

May 2013

107127

"This dissertation is submitted in partial fulfilment of the requirement of the Degree of MSc in Information Technology
of
the University of Moratuwa"

107127

Declaration

I certify that this dissertation does not incorporate, without acknowledgement, any material previously submitted for a Masters, Degree or Diploma in any University and to the best of my knowledge and belief. It does not contain any material previously published or written by another person except where due reference is made in the text. I also here by give consent for my dissertation, if accepted to be made available for photocopying and interlibrary loans and for the title and summary to be made available to outside organizations.

Signature of Candidate *Date:* 28·08·2013

……………………………

W K S Karunarathne

Signature of Supervisor *Date:* 28.08.2013

……………………………

Dr. Prasad Wimalarathne

Abstract

The internet put the rest of the world at the reach of personal computer. In the same way, it is also made personal computers reachable by the rest of the world. Good News and Bad News! Over the last decade, the internet has been subject to widespread of security attacks. Besides the classical terms, new ones had to be found in order to designate a large collection of threats: Worms, break-ins, hackers, crackers, hijacking, spoofing, man-in-the-middle, password-sniffing, denial of service and so on. With the sequence of cyber-attacks which were targeted various Government websites, during the recent past; it hampers the effectiveness of security research and practices carried out developing such websites.

This project focuses on security issues of the web application, which is being used by the Department of National Archives, which is the ICA-AtoM. The security features of ICA-AtoM are not adequate to withstand ongoing cyber threats and attacks. Being the last resort to find most of the valuable documents, papers or journals publish throughout the history, the online repositories at National Archives should be essentially safeguard against the malicious hackers. Moreover the focus of this project includes discussing in detail the ICA-AtoM related vulnerabilities and how they are exploited. This converge the definitions of various hacking practices, it's implication on the ICA-AtoM.

This paper aiming for a better understanding of the subject matter. In the paper we discuss some of the major actual known attacks. Besides the description of each attack and way they are carried on. We also discuss the related means of prevention, detection and/ or defense such attacks though various security techniques introducing to the system.

Acknowledgement

This project is a result of my effort with the continuous support of our Supervisor, Dr. Prasad Wimalarathne who guided me way throughout the project.

Also my heartfelt gratitude towards University of Moratuwa for this great opportunity extended for myself to seek, learn and apply.

I take this opportunity to thank my family who lent me their hands giving me freedom and peace of mind to a better working environment setting up priority on my effort to fulfil my effort of system designing and documentation. I'm grateful for my family and for my friends for their various efforts of cooperation and interest taken over on my studies.

Last but not least, I would like to thank the lecturers for cooperating with me and helping and being kind enough to devote their time for me.

Table of Contents

DECLERATION ii
ABSTRACT iii
ACKNOWLEDGEMENT iv
TABLE OF CONTENTS v
LIST OF TABLES x
LIST OF FIGURES xi
LIST OF ACRONYMS xiii

CHAPTER 1 – INTRODUCTION

1.1. INTRODUCTION 2
1.2. MOTIVATION 2
1.3. AIMS AND OBJECTIVES 3
1.4. SCOPE 4
1.5. STRUCTURE OF THE DISSERTATION 4

CHAPTER 2 – LITREATURE REVIEW

2.1. ARCHIVES 6
2.2. ARCHIVAL PROCESSING 6
2.3. ARCHIVAL WORKFLOW 7
2.3.1. Appraisal 7
2.3.2. Accession 7
2.3.3. Arrangement 8
2.3.4. Description 8
2.3.5. Preserve 8
2.3.6. Provide Access 9
2.3.7. Offer Reference Service 9
2.4. ARCHIVAL DESCRIPTION 11
2.4.1. Records 12
2.5. STANDARDS FOR ARCHIVAL DESCRIPTION 13
2.5.1. ISAD (G) 14
2.5.2. RAD – Rules for Archival Description 14
2.6. METADATA 16

2.6.1. Recordkeeping Metadata 16
2.7. ARCHIVAL DESCRIPTION SOFTWARE 17
2.7.1. Need for Archival Description Software 17
2.8. ICA-AtoM 18
2.8.1. The Origin of ICA-AtoM® 19
2.8.2. The Driving Factor of ICA-AtoM® Project 19
2.8.3. Architecture and Technical Overview of ICA-AtoM® 19
2.8.4. Entity types of ICA-AtoM® 23
2.8.5. Usage of ICA-AtoM® 23
2.8.6. Version History and Added Features of ICA-AtoM® 25
2.8.7. The Future of ICA-AtoM® 26
2.8.8. Limitations of ICA-AtoM® 27
2.9. SIMILAR PROJECTS 28
2.9.1. Limitations Similar Projects 32
2.10. DEPARTMENT OF NATIONAL ARCHIVES 34
2.10.1. National Archives –Objectives 34
2.10.2. Services Provided by National Archives 35
2.10.3. The Role of ICA-AtoM® at National Archives 35
2.11. WEB SECURITY 36
2.11.1. Online Challengers for Sri Lanka 36
2.11.2. Online Threats vs. Department of National Archives 40
2.12. HACKING WEB SERVERS 40
2.12.1. Why the Web servers are compromised? 41
2.12.2. Impact of Web server Attack 42
2.12.3. Attack Methodology 42
2.12.4. Web server Security Tools 46
2.12.5. Patch Management 46
2.12.6. Defend Against Web server Attacks 47
2.13. HACKING WEB APPLICATIONS 48
2.13.1. Vulnerability Stack 49
2.13.2. Web Application Threats 49
2.13.3. Counter Measures 53
2.13.4. Security & Pen Testing Tools 54
2.14. LITERATURE REVIEW – SUMMARY 57

CHAPTER 3 – ANALYSIS

3.1. FEASIBILITY STUDY 59
3.1.1. Economic Feasibility 61
3.1.2. Technical Feasibility 61
3.1.3. Operational Feasibility 62
3.1.4. Schedule Feasibility 63
3.1.5. Organizational Feasibility 63
3.1.6. Legal Feasibility 64
3.1.7. Marketing Feasibility 64
3.2. REQUIREMENT FOR ENHANCING SECURITY OF ICA-AtoM® 65
3.2.1. Objective 65
3.2.2. Requirement Collection Methods 65
3.2.3. Analysis and Review of Gathered Requirements 67
3.2.4. Non-Functional Requirements 68
3.2.5. Functional Requirements 71
3.2.6. Requirement validation and Management 75
3.3. SYSTEM REQUIREMENTS 76
3.4. USER REQUIREMENTS 76
3.5. LIMITATION FOR ENHANCING SECURITY FOR ICA-AtoM® 77
3.6. ANALYSIS – SUMMARY 78

CHAPTER 4 – DESIGN

4.1. SOLUTION 80
4.2. DESIGN THE SECURITY ENHANCEMENT 80
4.3. VALIDATE DATA INTEGRITY 81
4.3.1. Integrity Validation feature of Existing System 82
4.3.2. Integrity Validation feature of Proposed System 83
4.4. SECURING USER LOGIN CREDENTIALS 84
4.5. SECURING THE CLIENT THROUGH SSL 85
4.6. CHANGE MANAGEMENT – REPORTS 86
4.7. SESSION MANAGEMENT 87
4.8. ENFORCE PASSWORD POLICY 88

4.9. SECURING ICA-AtoM FROM PHISHING ATTACKS........................ 89
4.10. SECURING ICA-AtoM FROM DoS ATTACKS.............................. 90
4.11. SECURING THE PHP CONFIGURATION.................................. 90
4.12. SECURING MySQL.. 91
4.13. SECURING THE OPERATING SYSTEM – CentOS.......................... 91
4.14. DESIGN – SUMMARY.. 92

CHAPTER 5 – IMPLEMENTATION

5.1. IMPLEMENTATION OF SECURED ICA-AtoM SYSTEM......................... 94
5.2. SECURED ICA-AtoM SYSTEM – DEVELOPMENT TOOLS....................... 94
5.2.1. Software Used for Development.................................... 94
5.2.2. Software Used for the security testing............................ 96
5.3. DEVELOPMENT TECHNOLOGY – SECURED ICA-AtoM SYSTEM.... 99
5.3.1. Key Tool – Key and Certificate management Tool.................. 99
5.3.2. Validating integrity of the uploaded image using checksum.......... 102
5.3.3. Storing the Password under SHA-512 Encryption...................... 102
5.4. IMPLEMENTATION ENVIRONMENT – SECURED ICA-AtoM.......... 105
5.5. IMPLEMENTATION – SUMMARY.. 105

CHAPTER 6 – TESTING

6.1. TESTING THE SYSTEM.. 108
6.2. TEST PLAN AND OBJECTIVES OF SECURED ICA-AtoM SYSTEM..... 108
6.3. TEST CASES... 110
6.3.1. Index Page – The Login.. 110
6.3.2. Digital Certificate Uploading – Changing the integrity.............. 112
6.3.3. Secure Login through SSH.. 113
6.3.4. Digital Signature – Validation...................................... 114
6.4. TEST – SUMMARY.. 114

CHAPTER 7 – EVALUATION

7.1. PROJECT EVALUATION.. 116
7.2. NEED FOR EVALUATION... 116

7.3. SECURITY ENHANCEMENT OF ICA-AtoM.. 116
7.3.1. Results of the Project.. 116
7.3.2. Barriers to Achieve Goals.. 117
7.4. DEVIATION FROM ORIGINAL PROJECT PLAN................................. 118

CHAPTER 8 – CONCLUSION

8.1. MAJOR ACHIEVEMENTS OF THE SYSTEM.. 120
8.2. IMPROVEMENTS OF THE SYSTEM.. 121
8.2.1. The Future Development path.. 121
8.3. PROBLEMS BEYOND CONTROL... 122

REFERENCE.. 123

APPENDIX A – SYSTEM DOCUMENTATION.. 132

APPENDIX B – USER DOCUMENTATION... 141

APPENDIX C – CODE LISTING.. 152

APPENDIX D – SECURING APACHE.. 163

APPENDIX E – INTERNATIONAL STANDARD FOR ARCHIVAL DESCRIPTION.. 168

APPENDIX F – TECHNICAL REQUIREMENTS OF ICA-AtoM............ 171

APPENDIX G – HARDENING CentOS... 174

APPENDIX H – SESSION HIJACKING... 183

APPENDIX I – SCANING AND VULNERABILITY ASSESMENT RESULTS.. 188

List of Tables

Table 2.1: Tabulation of Archival Description Software *(Part 1)* 32

Table 2.2: Tabulation of Archival Description Software *(Part 2)* 33

Table 3.1: Cost Benefit Analysis of the Project 60

Table 3.2: Major Vulnerabilities Observed During Assessment *(Part 1)* 67

Table 3.3: Major Vulnerabilities Observed During Assessment *(Part 2)* 68

Table 3.4: Hardware Configurations 76

Table 3.5: Software Configurations 76

Table 5.1: Server Requirements 105

Table 6.1: Login Test Case #001 110

Table 6.2: Login Test Case #002 111

Table 6.3: Login Test Case #003 111

Table 6.4: Login Test Case #004 111

Table 6.5: Login Test Case #005 112

Table 6.6: Login Test Case #006 112

Table 6.7: Image Upload Test Case #007 112

Table 6.8: Image Upload Test Case #008 113

Table 6.9: Secure Login through SSH Test Case #009 113

Table 6.10: Secure Login through SSH Test Case #010 113

Table 6.11: Digital Signature Validation Test Case #011 114

Table 6.12: Digital Signature Validation Test Case #012 114

LIBRARY

List of Figures

Figure 2.1: Archival Workflow.. 10

Figure 2.2: ICA-AtoM – A Screenshot... 18

Figure 2.4: ICA-AtoMArchitecture... 20

Figure 2.5: ICA-AtoM Multi-Repository Architecture...................................... 22

Figure 2.6: ICA-AtoM Entity Types and its Connectivity................................. 23

Figure 2.7: Technical resources of OAIS compliant Digital Preservation System.... 26

Figure 2.8: Website attack of *www.nationalsecurity.lk*.................................... 37

Figure 2.9: Website attack of *www.media.gov.lk*.. 37

Figure 2.10: Website attack of *deyatakirula.gov.lk* and *govtwhip.gov.lk*................. 38

Figure 2.11: Website attack of *www.slpa.lk*.. 39

Figure 2.12: Webserver market share of all sites... 40

Figure 2.13: Webserver market share of top million busiest sites...................... 41

Figure 2.14: Impact of Web Server Attacks.. 42

Figure 2.15: Nessus Vulnerability Scanner.. 43

Figure 2.16: HTTP Response Hijacking.. 45

Figure 2.17: Top 10 Vulnerability Classes 2011.. 48

Figure 2.18: The Vulnerability Stack... 49

Figure 2.19: Acunetix Web Vulnerability Scanner.. 54

Figure 2.20: Netsparker Web Vulnerability Scanner... 55

Figure 2.21: N-Stalker Web Application Security Scanner................................ 55

Figure 3.1: Requirement validation Process.. 75

Figure 4.1: Evolutionary Prototyping Method.. 81

Figure 4.2: Interface of Importing Multiple Digital Objects.................................... 82

Figure 4.3: USE CASE: Digital object upload and retrieval...................................... 82

Figure 4.4: Activity Diagram for Uploading and Viewing Image.............................. 83

Figure 4.5: USE CASE: Validating Digital Objects.. 83

Figure 4.6: Activity Diagram for Image validation.. 84

Figure 4.7: Securing the connectivity through SSL... 86

Figure 4.8: Current Description Update Searching Interface.................................... 86

Figure 4.9: Activity Diagram for Session Timeout.. 87

Figure 4.10: Password Policy Implementation... 88

Figure 4.11: Login interface of ICA-AtoM... 89

Figure 4.12: New Login Interface Activity Diagram.. 89

Figure 5.1: Basic Architecture of LAMP.. 95

Figure 5.2: Nessus Web Interface.. 97

Figure 5.3: Metasploit Interface.. 98

Figure 6.1: Unit Testing Process.. 109

Figure A.1: Boot up Screen of CentOS 6.3.. 133

Figure A.2: Skip Media Test.. 133

Figure A.3: Select Installation Media... 133

Figure A.4: Network Configuration... 134

Figure A.5: Begin of GUI Installation Screens.. 134

Figure A.6: Write Storage Configuration to Disk.. 135

Figure A.7: CentOS 6.3 Installation Progress.. 135

Figure A.8: CentOS Rebooting Process... 136

Figure A.9: CentOS Start-up.. 136

Figure A.10: CentOS 6.3 Log-in Prompt... 136

Figure A.11: ICA-AtoM Web Installation start Screen... 139

Figure A.12: ICA-AtoM Database configuration.. 140

Figure A.13: ICA-AtoM Site configuration.. 140

Figure B.1: ICA-AtoM Index Page... 142

Figure B.2: ICA-AtoM Login Page... 143

Figure B.3: ICA-AtoM Password Prompt.. 143

Figure B.4: ICA-AtoM Home Page... 144

Figure B.5: View User Profile of ICA-AtoM.. 144

Figure B.6: Change Secure Image... 145

Figure B.7: Browse Digital Objects.. 146

Figure B.8: Comparison of Checksum... 146

Figure B.9: Sign PDF Toolkit... 147

Figure B.10: Unsigned Document.. 147

Figure B.11: Signed Document.. 147

Figure B.12: Signed PDF with Trusted signature panel... 148

Figure B.13: Signed but Unrecognized PDF with untrusted signature panel......... 148

Figure B.14: Create a Key File... 148

Figure B.15: Create Export Certificate... 149

Figure B.16: pair of Generated Keystore and Export Certificate........................... 149

Figure B.17: Validating Untrusted Identity... 150

Figure B.18: Validated Identity.. 151

Figure H.1: Session Hijacking Initiation Pattern.. 143

Figure H.2: Spoofing Attack Initiation Pattern... 144

Figure H.3: Session Hijacking on OSI Model.. 145

Figure H.4: Defend Against Session Hijacking... 146

List of Acronyms

LAMP	-	Linux, Apache, MySQL, PHP
ICA-AtoM	-	International Council for Archives – Access to Memory
DMS	-	Document Management System
DBMS	-	Database Management System
EAD	-	Encoded Archival Description
ISAD (G)	-	International Standard Archival Description (General)
IDS	-	Intrusion Detection System
IPS	-	Intrusion Prevention System
ICMP	-	Internet Control Message Protocol
RAD	-	Rules for Archival Description
OAIS	-	Open Archival Reference Model
OSARIS	-	Open Source Archival Resource Information System
VA	-	Vulnerability Assessment
PT	-	Penetration Testing
WAF	-	Web Application Firewall
OWASP	-	Open Web Application Security Project
WASC	-	Web Application Security Consortium