MITIGATION OF SHOULDER-SURFING ATTACK ON PICTURE-BASED PASSWORDS USING FALSIFYING AUTHENTICATION METHODS

POR LIP YEE

THESIS SUBMITTED IN FULFILMENT
OF THE REQUIREMENTS
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

FEB 2012

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: POR LIP YEE

I.C/Passport No: 770221-07-5907

Registration/Metric No: WHA 040007

Name of Degree: DOCTOR OF PHILOSOPHY

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"):
MITIGATION OF SHOULDER-SURFING ATTACK ON PICTURE-BASED PASSWORDS USING FALSIFYING AUTHENTICATION METHODS

Field of Study: INFORMATION SECURITY

I do solemnly and sincerely declare that:

1) I am the sole author/writer of this Work;
2) This Work is original;
3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature **Date**
Subscribed and solemnly declared before,

Witness's Signature **Date**
Name:
Designation:

Abstract

Over the years, various picture-based password systems were proposed to exploit the utility of pictures for user authentication. However, there are problems associated with these picture-based password authentication systems such as: vulnerability to security threats, and users' memorability of the passwords. This research was undertaken to develop methods to mitigate shoulder-surfing attack. Two falsifying authentication methods using: (i) penup event and neighbouring connectivity manipulation; and (ii) partial password selection and metaheuristic randomisation algorithm methods, were proposed. The first and second proposed methods were incorporated into the proposed Background Pass-Go (BPG) system and Visual Identification Protocol Professional (VIP Pro) system respectively. To improve the users' memorability, the upload background picture function and cued colour scheme were proposed for the BPG system; the grid line scaling function and the loose authentication method were proposed for the enhanced BPG system; and the chronological story-based cued recall technique was proposed for the VIP Pro system. Prototypes, simulations, observations and interviews were used as the data gathering methods. An offline FOA Java simulation was carried out to evaluate the capability of the MRA method in preventing FOA attack. Case studies were conducted to evaluate the capability of the proposed methods in mitigating shoulder-surfing attack. Kruskal Wallis test and calculation of the success rate in attacking were used to evaluate the capability of the proposed methods in mitigating shoulder-surfing attack. In general, the result of the case studies show that the two proposed falsifying authentication methods are able to mitigate shoulder-surfing attack regardless of the gender and competency levels of the shoulder-surfing attackers. Besides, the proposed MRA is effective in preventing FOA attack. A majority of the survey participants also stated that the proposed cued recall methods can aid users in memorising their password.

Acknowledgments

First of all, I would like to thank my current supervisors, Assoc. Prof. Dr. Abdullah Gani and Dr. Rosli Salleh for agreeing to take over as my supervisors, after I have been left for about a year without any supervisor.

I would also like to express my most sincere gratitude and utmost appreciation to Assoc. Prof. Dr. Diljit Singh for his encouragement, inspiration and support especially when I encountered difficulty in compromising with and fulfilling the requirements set by my new supervisor.

I would like to acknowledge and extend my heartfelt gratitude to Ms. Delina Beh Mei Yin and Ms. Ong Sim Ying for their support and blessing. I would like to thank my good friend, Dr. Goh Chong Tien, for proof-reading and providing constructive feedback on my publications and thesis. Special thanks to all my family members and friends for their good wishes and unwavering support for my success. Without your support, I know I will not be able to make it.

Last but not least, I would like to express my gratitude to the Ministry of Science, Technology and Innovation (MOSTI), Malaysia, and the University of Malaya (UM) for providing the research funds to make this project a success.

Contents

Abstract i

Acknowledgments ii

List of Figures ix

List of Tables xv

Acronyms and Abbreviations xvii

Chapter 1 Introduction 1

1.1 Background 1

1.2 Motivation 2

1.3 Statement of Problem 4

1.4 Statement of Objective 8

1.5 Scope of the Research 9

1.6 Significance of the Research 10

1.7 Organisation of Thesis 11

Chapter 2 Literature Review 14

2.1 Introduction 14

2.2 Security Threats in Picture-Based Password 14

2.2.1 Surveillance Approach 15

2.2.2 Malware Attack 16

2.2.3 Password Guessing and Cracking 16

2.2.4 Social Engineering Attack 17

2.3 Password Authentication 19

2.4 Related Work 22

2.4.1 Locimetrics Authentication System 22

2.4.2 Drawmetrics Authentication System 32

2.4.3 Locimetrics and Drawmetrics Hybrid Authentication System 40

2.4.4 Searchmetrics and Its Hybrid Authentication Systems 44

2.5 Summary 66

Chapter 3 Methodology 68

3.1 Introduction 68

3.2 Approaches to Research 68

3.2.1 Proposed Falsifying Authentication Methods and Cued Recall Methods..... 69

3.2.2 System Design and Implementation.. 71

3.2.3 Testing and Evaluation 72

3.2.3.1 Shoulder-Surfing Attack I.. 73

3.2.3.2 Shoulder-Surfing Attack II... 76

3.2.3.3 Survey on Colour Usage 81

3.2.3.4 Sensitive Area Testing 82

3.2.3.5 Survey on Usability Part I.. 83

3.2.3.6 Survey on Usability Part II... 85

3.2.4 Documentation... 86

3.3 Summary 87

Chapter 4 Design and Implementation of Background Pass-Go.................................. 88

4.1 Introduction 88

4.2 BPG System Architecture 88

4.3 BPG Use Case Diagram 89

4.3.1 Enrollment Process... 90

4.3.1.1 Draw Password.. 90

4.3.1.1.1 Change the Colour of the Indicators 97

4.3.1.1.2 Load/Unload Background Picture 99

4.3.1.1.3 Show/Hide Sensitive Area 100

4.3.1.1.4 Show/Hide Indicators.. 101

4.3.1.2 Register Password ... 102

4.3.1.3 Clear Password ... 104

4.3.1.4 Back to Main Menu ... 105

4.3.1.5 System Flow of the Enrollment Process ... 105

4.3.2 Verification Process ... 107

4.3.2.1 Login ... 107

4.3.2.2 System Flow of the Verification Process ... 109

4.4 Database Design ... 111

4.5 Summary ... 112

Chapter 5 Design and Implementation of Enhanced Background Pass-Go ... 113

5.1 Introduction ... 113

5.2 Enhanced BPG System Architecture ... 113

5.3 Enhanced BPG Use Case Diagram ... 114

5.3.1 Enrollment Process ... 114

5.3.1.1 Draw Password ... 115

5.3.1.1.1 Grid Line Scaling Function ... 115

5.3.1.2 Register Password ... 117

5.3.1.2.1 Loose Authentication ... 118

5.3.1.3 System Flow of the Enrollment Process ... 121

5.3.2 Verification Process ... 123

5.3.2.1 Login ... 123

5.3.2.2 System Flow for Verification Process ... 124

5.4 Database Design ... 126

5.5 Summary ... 126

Chapter 6 Design and Implementation of Visual Identification Protocol Professional 128

6.1 Introduction ... 128

6.2 VIP Pro System Architecture 128

6.3 VIP Pro Use Case Diagram 129

6.3.1 Enrollment Process.. 129

6.3.1.1 Identify Username 130

6.3.1.2 Identify Password 130

6.3.1.2.1 Select Picture from Predefined Category.................................... 131

6.3.1.2.1.1 Reset Selection.. 132

6.3.1.2.2 Arrange Password Sequence 133

6.3.1.2.2.1 Reset Password Sequence... 134

6.3.1.3 Register Password 134

6.3.1.4 System Flow for Enrollment Process 135

6.3.2 Verification Process 136

6.3.2.1 Login... 137

6.3.2.2 System Flow for Verification Process 142

6.4 Database Design 143

6.5 Summary 146

Chapter 7 Analysis and Testing.. 147

7.1 Introduction 147

7.2 Analysis and Testing of the BPG System 147

7.2.1 Shoulder-Surfing Mitigation... 147

7.2.2 Sensitive Area 155

7.2.3 Colour Scheme.. 157

7.2.4 Upload Background Picture Feature 159

7.3 Analysis and Testing of the Enhanced BPG System 161

7.3.1 Grid Line Scaling Feature... 161

7.3.2 Loose Authentication Feature 163

7.4 Analysis and Testing of the VIP Pro System 166

7.4.1 |*X*| Password Interval.. 166

7.4.2 |*J*| Partial Password Interval.. 167

7.4.3 MRA Distribution Range.. 170

7.4.4 Mitigate Shoulder-Surfing Testing... 172

7.4.5 Chronological Story-Based Cued Recall Technique................................. 174

7.5 Summary 176

Chapter 8 Result and Discussion.. 178

8.1 Introduction 178

8.2 Results of the BPG System... 178

8.3 Results of the Enhanced BPG System 183

8.4 Results of the VIP Pro System.. 186

8.5 Summary 189

Chapter 9 Conclusion.. 190

9.1 Introduction 190

9.2 Achievement of the Objectives.. 190

9.3 Contributions 192

9.4 Limitations of the current study.. 195

9.5 Future Directions 196

9.6 Final Remarks... 197

Reference 199

Appendix A 209

Appendix B 211

Appendix C 213

Appendix C 216

Appendix D 218

Appendix E 248

Appendix F 256

Appendix G 288

List of Figures

Figure 1.1: Number of Different Passwords Frequently Used for Accessing All Services 3

Figure 1.2: Alphanumeric Passwords Change Frequency 3

Figure 1.3: An Off-line FOA Attack Simulation and Its Observation Result........ 7

Figure 2.1: Picture-Based Password Security Threats Classification........ 15

Figure 2.2: Authentication System Classification Tree 21

Figure 2.3: Blonder System........ 23

Figure 2.4: visKey System 23

Figure 2.5: Passlogix V-Go System 25

Figure 2.6: PassPoints System 26

Figure 2.7: Cued Click-Points System........ 27

Figure 2.8: Persuasive Cued Click-Points System 28

Figure 2.9: Organisation Chart of Locimetrics Authentication Systems........ 30

Figure 2.10: Draw A Secret System 32

Figure 2.11: Multi-Grid DAS System 34

Figure 2.12: DAS with Rotation System 35

Figure 2.13: Background Draw a Secret System 36

Figure 2.14: Qualitative Draw A Secret System 38

Figure 2.15: Organisation Chart of Drawmetrics Authentication Systems 39

Figure 2.16: Pass-Go System 41

Figure 2.17: Hybrid Authentication System Organisation Chart for Locimetrics and Drawmetrics Systems 42

Figure 2.18: Passfaces™ System 44

Figure 2.19: Déjà Vu System 46

Figure 2.20: Triangle System 47

Figure 2.21: Movable Frame System 48

Figure 2.22: Special Geometric Configuration System 49

Figure 2.23: Picture Password System 50

Figure 2.24: Where Is Waldo (WIW) System 51

Figure 2.25: Visual Identification Protocol (VIP) Systems 53

Figure 2.26: Story System 55

Figure 2.27: Pict-O-Lock System 55

Figure 2.28: Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS) System 56

Figure 2.29: S3PAS Session Password Determination 57

Figure 2.30: Use Your Illusion System 59

Figure 2.31: Temporal Indirect Image-Based Authentication (TI-IBA) 60

Figure 2.32: Organisation Chart of Searchmetrics and Its Hybrid Authentication Systems 62

Figure 3.1: Research Methodology Framework 69

Figure 3.2: A Password Created Using the Predefined Password Encoding Technique 73

Figure 4.1: BPG System Architecture 89

Figure 4.2: Background Pass-Go Use Case Diagram 89

Figure 4.3: Intersection Points and Indicators Design 91

Figure 4.4: Pseudocode for Intersection Points Implementation 91

Figure 4.5: Pseudocode for Indicators Implementation 92

Figure 4.6: Eight-Nearest-Neighbour Connectivity 92

Figure 4.7: Proposed Neighbour Connectivity 93

Figure 4.8: Neighbour Connectivity Comparisons 93

Figure 4.9: Penup Event Demonstrations 94

Figure 4.10: Draw a Line with One Penup Event 94

Figure 4.11: Draw a Line with Two Penup Events 95

Figure 4.12: Draw a Line with Three Penup Events 95

Figure 4.13: Penup Event and Neighbouring Connectivity Manipulation 96

Figure 4.14: Visualisation Effect.. 96

Figure 4.15: Overlapped Penups 97

Figure 4.16: A BPG Password Instance Using Colours as a Cue 98

Figure 4.17: Pseudocode for Colour Scheme Implementation 98

Figure 4.18: Load/Unload Background Picture Function.. 99

Figure 4.19: Pseudocode for Load/Unload Background Picture Implementation 99

Figure 4.20: Show/Hide Sensitive Area Function... 100

Figure 4.21: Pseudocode for Show/Hide Sensitive Area Implementation 100

Figure 4.22: An Instant of a Login Process Using the “Show/Hide Indicators” Function

.... 101

Figure 4.23: Pseudocode for “Show/Hide Indicators” Implementation 102

Figure 4.24: Example of a Password Encoding Generated by the BPG System 103

Figure 4.25: Pseudocode for BPG Encoding Scheme Implementation...................... 103

Figure 4.26: Password Hashing Feature 104

Figure 4.27: Pseudocode for Password Hashing Implementation.............................. 104

Figure 4.28: Clear Password Function... 104

Figure 4.29: Pseudocode for Clear Password Implementation 105

Figure 4.30: Back Function GUI 105

Figure 4.31: Pseudocode for Back Function Implementation................................... 105

Figure 4.32: System Flow of the Enrollment Process 106

Figure 4.33: Login using Show/Hide Indicator Function.. 108

Figure 4.34: Pseudocode for Login Function... 108

Figure 4.35: Sample Login Data 109

Figure 4.36: System Flow of the Verification Process 110

Figure 5.1: Enhanced BPG System Architecture 113

Figure 5.2: Enhanced BPG Use Case Diagram.. 114

Figure 5.3: Grid Line Scaling Feature 116

Figure 5.4: Maximum Scaling Feature 116

Figure 5.5: The Usability of the Grid Line Scaling Function 117

Figure 5.6: Pseudocode for Grid Line Scaling Implementation................................. 117

Figure 5.7: A Sample Password and the Encoding Generated of the Enhanced BPG System.. 118

Figure 5.8: Loose Authentication Password and its Encoding: Example I................. 120

Figure 5.9: Loose Authentication Password and its Encoding: Example II 120

Figure 5.10: Pseudocode for Loose Authentication Implementation.......................... 121

Figure 5.11: System Flow of the Enrollment Process 122

Figure 5.12: System Flow of the Verification Process 125

Figure 6.1: VIP Pro System Architecture 129

Figure 6.2: VIP Pro System Use Case Diagram.. 129

Figure 6.3: Identify Username GUI.. 130

Figure 6.4: Pseudocode for the Identify Username Implementation.......................... 130

Figure 6.5: Select Picture from Predefined Category... 131

Figure 6.6: Pseudocode for Select Picture from Predefined Category Function and Its Respective Pictures Implementation.. 132

Figure 6.7: Reset Selection Feature.. 132

Figure 6.8: Pseudocode for Reset Selection Implementation 133

Figure 6.9: Identify Password Sequence.. 133

Figure 6.10: Pseudocode for Identify Password Sequence Implementation............... 133

Figure 6.11: Reset Password Sequence Function... 134

Figure 6.12: Pseudocode for Reset Password Sequence Implementation 134

Figure 6.13: Registration Password Completion GUI 135

Figure 6.14: Pseudocode for Registration Password Implementation........................ 135

Figure 6.15: System Flow of the Enrollment Process 136

Figure 6.16: Challenge Set Generation GUI 137

Figure 6.17: Sample Password 138

Figure 6.18: Initial Challenge and Its Generated Pictures 139

Figure 6.19: Second Attempt and Its Generated Pictures 139

Figure 6.20: Final Attempt and the Pictures Generated by the Proposed System 140

Figure 6.21: Pseudocode for the Proposed Falsifying Authentication Method (Partial Password Selection and Metaheuristic Randomisation Algorithm) 141

Figure 6.22: Block Function 142

Figure 6.23: Pseudocode for Block Function.. 142

Figure 6.24: System Flow of Verification Process.. 143

Figure 6.25: VIP Pro Relational Database Diagram.. 143

Figure 7.1: A Password Created from the Predefined Password Encoding................ 148

Figure 7.2: Percentage Password Matching Results.. 150

Figure 7.3: Incorrect Password Encoding Produced by the Attackers 150

Figure 7.4: Distribution Testing Result 151

Figure 7.5: Sensitive Area Design... 155

Figure 7.6: Successful Access Rate Results... 157

Figure 7.7: Proposed Sensitive Area with the Radius Size of 0.30×d........................ 157

Figure 7.8: Colour Scheme Adopted from Microsoft Office Word 2003 158

Figure 7.9: Survey Result on Colour Usage 159

Figure 7.10: Survey on Participants’ Knowledge of Picture-based Password Authentication 161

Figure 7.11: Example of an Enhanced BPG Password 162

Figure 7.12: Loose Authentication Demonstration 164

Figure 7.13: Empirical Analysis of the |*X*| Password Interval 167

Figure 7.14: Analysis and Observation Result for $R_1^{j_{4..4}}$ 169

Figure 7.15: Analysis and Observation Result for $R_1^{j_{4..6}}$ 170

Figure 7.16: Population Pyramid Graph 173

Figure 7.17: A Sample Story 175

Figure 8.1: A Non-Centred and Asymmetrical Password 178

Figure 8.2: Example of a Password 180

Figure 8.3: Example of a Password Created Using the Upload Background Picture Function 181

Figure 8.4: Attackers' Attempt 181

Figure 8.5: Lines and Shapes Samples That Cannot be Drawn Using Pass-Go System 182

Figure 8.6: BPG Password Length 183

Figure 8.7: Password Length Comparison 186

Figure 9.1: Potential Security Threats for Web-Based Picture-Based Password Authentication System 196

List of Tables

Table 1.1: Usage of the Different Categories of Alphanumeric Passwords 3

Table 2.1: Synthesis of Locimetrics Authentication Systems..................................... 31

Table 2.2: Synthesis of Drawmetrics Authentication Systems 40

Table 2.3: Synthesis of Locimetrics and Drawmetrics Hybrid Authentication System . 43

Table 2.4: Synthesis of Searchmetric Authentication Systems.................................... 64

Table 3.1: Data Gathering Techniques Used to Evaluate the Capability of the Proposed Techniques in Mitigating Shoulder-Surfing Attack 72

Table 3.2: Data Analysis Techniques Used to Evaluate the First Proposed Method (Penup Event and Neighbouring Connectivity Manipulation)..................................... 75

Table 3.3: Data Analysis Techniques Used to Evaluate the Second Proposed Method (Partial Password Selection and Metaheuristic Randomisation Algorithm)................. 77

Table 3.4: Data Analysis Techniques Used to Evaluate the Capability of the Proposed Method in Preventing FOA Attack.. 78

Table 3.5: Data Analysis Techniques Used to Evaluate the Capability of the Proposed Methods in Helping Users to Improve the Memorability.. 80

Table 3.6: Colour Usage Survey Questions and the Data Type................................... 81

Table 3.7: Survey on Usability Part I: Questions and Their Data Type 84

Table 3.8: Survey on Usability Part II: Questions and Their Data Type....................... 86

Table 4.1: The Identified Colours and Their RGB Values 98

Table 4.2: BPG Metadata.. 111

Table 5.1: Enhanced BPG Metadata... 126

Table 6.1: VIP Pro Metadata... 144

Table 7.1: Comparison of the Kruskal Wallis Test Results between the Prosgraduate Student Group and the Undergraduate Student Group 152

Table 7.2: Comparison of the Kruskal Wallis Test Result Obtained by the Male and the Female Participants.. 154

Table 7.3: Comparison of the Kruskal Wallis Test Result Obtained by the Male and the Female Participants (for Postgraduate Students)... 154

Table 7.4: Comparison of the Kruskal Wallis Test Result Obtained by the Male and the Female Participants (for Undergraduate Students).. 154

Table 7.5: Top 10 Preferred Colours 159

Table 7.6: Results of Cross-Tabulation of the Responses to Q1 and Q2.................... 160

Table 7.7: Chi-Square Test for Q1 and Q2 161

Table 7.8: Chi-Square Test for Q3 and Q4 163

Table 7.9: Chi-Square Test for Q5 and Q6 165

Table 7.10: Chi-Square Test for Q7 and Q8 166

Table 7.11: MRA Interval with Minimum and Maximum *j*=4 168

Table 7.12: MRA Interval Classification.. 171

Table 7.13: MRA Interval with Minimum *j*=4 and Maximum *j*=5 172

Table 7.14: Cross-Tabulation of Q9 and Q10.. 175

Table 7.15: Chi-Square Test for Q9 and Q10 176

Table 8.1: Synthesis of the Results of the BPG System 179

Table 8.2: Password Space Comparison.. 183

Table 8.3: Synthesis of the Results of the Enhanced BPG System 184

Table 8.4: Enhanced BPG Password Space 185

Table 8.5 Synthesis of the Results of the VIP Pro System 187

Table 8.6: Password Space Comparison.. 188

Acronyms and Abbreviations

ASCII	American Standard Code for Information Interchange
ATM	Automatic Teller Machine
BCI	Brain-Computer Interface
BDAS	Background Draw a Secret
BMP	Bitmap
BPG	Background Pass-Go
CCP	Cued Click Points
CLDC	Connected Limited Device Configuration
COM	Component Object Model
DAS	Draw A Secret
DNS	Domain Name Services
FCSIT	Faculty of Computer Science and Information Technology
GIF	Graphic Interchange Format
GUI	Graphic User Interface
HVS	Human Visual Sensory
FOA	Frequency of Occurrence Analysis
ID	Identification/Identity/Identifier
IDE	Integrated Development Environment
IP	Internet Protocol
J2ME	Java 2 Micro Edition
JPEG	Joint Photographic Experts Group
JRE	Java Runtime Environment
MAC	Media Access Control
MD5	Message Digest 5
MITB	Man-in-the-Browser

MOSTI	Ministry of Science, Technology and Innovation
MRA	Metaheuristic Randomisation Algorithm
MySQL	My Structured Query Language
OLE	Object Linking and Embedding
PC	Personal Computer
PCCP	Persuasive Cued Click-Points
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PNG	Portable Network Graphics
PRI	Primary
Pro	Professional
QDAS	Qualitative Draw A Secret
R-DAS	DAS with Rotation
RFID	Radio Frequency Identification
RGB	Red, Green and Blue
S3PAS	Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme
TI-IBA	Temporal Indirect Image-Based Authentication
UNI	Unique
UM	University of Malaya
VIP	Visual Identification Protocol
WIW	Where Is Waldo