A Framework to Enhance Privacy-Awareness in Mobile Web Systems

By

Nahier Aldhafferi

BCS (DTC), MIT (UOW)

Submitted in fulfilment of the requirements of the degree of Doctor of Philosophy

Principal Supervisor: Dr. David Miron
Co-Supervisor: Professor Aron Murphy
Co-Supervisor: Professor Trevor Brown

School of Science and Technology
University of New England
Armidale, Australia

Aug 2014
Declaration

Regarding the ideas, investigation, analysis, discussion and conclusions reported in this thesis, I certify that all these are entirely my own work. I also certify that the content of the study is original and has not been previously submitted.

Signature: 

Nahier Aldhaferi

Date: 06-08-2014
Abstract

In the last decade, the use of online social network sites has dramatically increased and these sites have succeeded in attracting a large number of users. The social network site has become a daily tool people use to find out about the latest news and to share details of their personal information. Many people use Internet mobile devices to browse these sites. The widespread use of some technologies unnecessarily puts the privacy of users at risk, even when these users remain anonymous. This study examines the risks to privacy surrounding the misuse of users’ personal information, such as maintaining trustworthy sites, as well as privacy issues associated with sharing personal information with others. This study also develops a framework to enhance privacy awareness in mobile Web systems. A privacy framework is proposed that incorporates suitability in the design and flexibility in the use to suit different types of Web mobile devices, and provides simple ways of adjusting and creating different privacy policies. This framework allows the user to create different levels of privacy settings and to better manage the exchange of personal information with other sites.

The proposed conceptual model for this study is derived from a review of the literature and the current privacy models. It shows how online users are able to create different privacy policies and set different policies to access the data. It also explains how the centrality of personal information details in one server will limit the distribution of personal information over the Internet and will provide users with more authority to control the sharing of their information with other websites. The design of the proposed framework is derived from developing other privacy models and adding new ideas that enhance the security level of protecting the privacy of users' information.

The study consists of five main tasks that include two different qualitative methodologies, programming two applications and testing the framework. The data were collected by using two different languages, Arabic and English, and both programming languages (ASP.net and SQL Server 2008) were used to design the privacy framework to deal with databases and simulate real communication between users, in order to achieve the main goal of designing the privacy framework.
This study contributes to providing a security environment for protecting the privacy of personal information. The findings provide greater understanding of privacy concerns and trust and how the current privacy models can be deployed via Internet mobile devices to control different privacy settings for different social media networks.
List of publications during the PhD study period


Acknowledgements

First of all, I sincerely wish to thank the following people for their assistance and encouragement in all stages of my research.

I would like to thank God for everything, and I appreciate the grace He has bestowed upon us.

I would like to give special thanks to my mother and to my wife for their assistance and prayers.

I would also like to thank my wonderful family and friends for their steadfast support and encouragement for this thesis.

I also give thanks to my previous supervisors, Dr Charles Watson and Prof A S M Sajeev, and to my current supervisors, Dr David Miron, Prof Aron Murphy and Prof Trevor Brown, for their efforts and patience. Their professional advice and their faith in me steered me toward completing this thesis.

I also thank all those people who have contributed, directly or indirectly, to the successful completion of my thesis.

Nahier Aldhafferi
# Table of Contents

**Chapter 1: Introduction**

1.1 Background to the study .......................................................... 1  
1.2 Recent research ........................................................................ 3  
1.3 Statement of the problem ............................................................ 6  
1.4 Goal and research objectives ....................................................... 8  
1.5 Methodology ............................................................................. 9  
1.6 Outline of thesis ....................................................................... 9  
1.7 Conclusion .................................................................................. 11

**Chapter 2: Literature Review**

2.1 Introduction .................................................................................. 12  
2.2 Social network sites .................................................................... 12  
  2.2.1 Web 2.0 and social network sites ......................................... 12  
  2.2.2 Background of social network sites ...................................... 14  
  2.2.3 Defining social networking sites .......................................... 15  
  2.2.4 User awareness in social network sites ................................. 16  
2.3 Privacy ......................................................................................... 17  
  2.3.1 Definition of privacy ............................................................. 18  
  2.3.2 Internet privacy ................................................................. 18  
  2.3.3 Privacy concerns ............................................................... 20  
  2.3.4 Trust .................................................................................. 25  
  2.3.5 Online privacy risks and protection ..................................... 26  
2.4 Centrality of personal information details in online systems ........ 28  
  2.4.1 Centrality of personal information in PayPal ....................... 29  
  2.4.2 How other websites access users’ personal details in PayPal . 32  
  2.4.3 Personal information security in PayPal ............................... 34  
  2.4.4 Challenges regarding centralised personal information in online systems ......................................................... 36  
  2.4.5 Security of personal information in centralised online systems .... 42  
  2.4.6 Advantages and disadvantages of centralised personal information details in online systems .............................. 46  
2.5 Mobile web systems .................................................................. 48  
  2.5.1 Mobile web ......................................................................... 49
4.7.1 General code structure ................................................................. 106
4.7.2 A scenario for selecting privacy settings using the Smart Wizard System ...... 110
4.7.3 Description of structures used in the Smart Wizard System ......................... 112
4.7.4 Smart Wizard System test code ..................................................... 116
4.8 Testing the Smart Wizard System ..................................................... 122
4.8.1 Data collection and sample size .................................................... 123
4.8.2 Ethical considerations .................................................................. 124
4.8.3 Data analysis and reliability .......................................................... 125
4.9 Developing the Proposed Privacy System ............................................. 125
4.9.1 Algorithm description ................................................................ 129
4.9.2 Programming method ................................................................. 133
4.9.3 Code description ....................................................................... 142
4.10 Testing the whole privacy system .................................................... 155
4.11 Conclusion .................................................................................... 165

Chapter 5: Results and Analysis .......................................................... 166
5.1 Introduction .................................................................................... 166
5.2 Questionnaire Results .................................................................... 166
5.2.1 Data quality and characteristics of respondents .................................. 166
5.2.2 Usage of online social network accounts and Internet mobile devices ....... 168
5.2.3 Awareness of privacy settings ....................................................... 170
5.2.4 Rating the importance of personal information ................................. 176
5.2.5 Comparing the findings with other research ...................................... 182
5.3 The Smart Wizard System ............................................................... 187
5.3.1 Implementation results ................................................................. 187
5.3.2 Concerns about hidden personal information items ............................ 190
5.4 The Proposed Privacy System .......................................................... 194
5.4.1 Implementation results of creating privacy policies in Server 1 (privacy system) .... 194
5.4.2 Implementation results of applying privacy policies in Servers 2, 3 and 4 ........ 196
5.5 Comparing the Whole Framework with Other Models ............................ 199
5.5 The Results of Implementing the Whole Privacy System ......................... 213
5.6 Conclusion ..................................................................................... 215

Chapter 6: Conclusion ......................................................................... 217
6.1 Introduction .................................................................................... 217
6.2 Summary of the Study .................................................................... 218
List of Figures

(All figures were designed by the researcher)

Figure 2.1. Personal information for opening a PayPal personal account ..................... 31
Figure 2.2. Information required for opening a PayPal business account ..................... 32
Figure 2.3. PayPal client/server architecture ............................................................... 33
Figure 2.4. Transaction flow for merchant websites using hosted pages ..................... 35
Figure 2.5. Email scam with link .................................................................................. 38
Figure 2.6. Email scam with a form .............................................................................. 39
Figure 2.7. A typical online transaction model ............................................................ 41
Figure 2.8. Vulnerable points in a typical online transaction network ......................... 41
Figure 2.9. Tools for achieving the security of information in online systems ............. 42
Figure 2.10. Iconix digital signature in Yahoo! Mail client .......................................... 44
Figure 2.11. Secure negotiated sessions using SSL ...................................................... 45
Figure 2.12. Privacy components and ramifications ..................................................... 59
Figure 2.13. A comparison of the structures of the rule wizard and the profile wizard ... 60
Figure 3.1. An example of using MAC in a military access control system ................. 67
Figure 3.2. Role-Based Access Control relationships ............................................... 68
Figure 3.3. UCON model components ....................................................................... 70
Figure 3.4. RADIUS authentication messages ......................................................... 71
Figure 3.5. Conceptual model – Key factors of the suggested design ......................... 74
Figure 3.6. Secure connection between the PDA device and the Server 1 application .... 76
Figure 3.7. Secure connection between the Server 1 application and the SQL server ... 78
Figure 3.8. Secure connection between the Server 1 application and the database ....... 79
3.9. An overview of the suggested access control system architecture .................... 80
Figure 3.10. Authentication processes in the suggested access control system ............ 80
Figure 4.1. The General Methodology of Research Design (Vaishnavi & Kuechler 2004) .............................................................................................................. 92
Figure 4.2. Stages of designing the proposed privacy framework ............................... 95
Figure 4.3. The basic functionality of the smart wizard .............................................. 100
Figure 4.4. General code structure for the Smart Wizard System ................................ 107
Figure 4.5. General code structure for the wizard’s window stage ............................... 108
Figure 4.6. General code structure for the suggested settings stage ........................... 109
Figure 4.7. An example of using pictures in the Smart Wizard System ....................... 110
Figure 4.8. Web pages of the Smart Wizard System ............................................... 113
Figure 4.9. An example of a question in the Smart Wizard System ......................... 113
Figure 4.10. An example of using the “viewstate” command ........................................... 114
Figure 4.11. An example of using an object in the Smart Wizard System .......................... 114
Figure 4.12. An example of how the SQL server sets privacy settings .............................. 115
Figure 4.13. An example of the suggested privacy settings .............................................. 115
Figure 4.14. An example of changing the suggested privacy settings .............................. 116
Figure 4.15. An example of the selection of privacy settings by using Smart Wizard System .......................................................... 117
Figure 4.16. An example of selecting custom privacy settings using the Smart Wizard System .......................................................... 120
Figure 4.17. Calculating the accuracy percentage of the Smart Wizard System ................. 121
Figure 4.18. General infrastructure for the suggested privacy system .............................. 126
Figure 4.19. General infrastructure for the suggested privacy system .............................. 127
Figure 4.20. Algorithm processing for the privacy system (server 1) ................................ 130
Figure 4.21. Algorithm processing for other websites (servers 2, 3 and 4) ......................... 132
Figure 4.22. The process of importing and saving privacy policies from server 1 .............. 141
Figure 4.23. View of the registration page for server 1 .................................................. 143
Figure 4.24. The code and store procedure for the registration page .............................. 144
Figure 4.25. Login page ............................................................................................... 144
Figure 4.26. The code and store procedure for the login page ...................................... 145
Figure 4.27. The code and store procedure for the personal information page ............... 146
Figure 4.28. Adding a new privacy policy ................................................................. 147
Figure 4.29. The code and store procedure for adding a new privacy policy ................. 148
Figure 4.30. View all created privacy policies ......................................................... 148
Figure 4.31. The code and store procedure for requesting the user’s privacy policies .... 149
Figure 4.32. Screenshot of a new user creation window for servers 2, 3 or 4 ............... 149
Figure 4.33. The code and store procedure for the registration process for servers 2, 3 and 4 ............................................................... 150
Figure 4.34. The code and store procedure for the login page for servers 2, 3 and 4 ....... 151
Figure 4.35. The code and store procedure for importing the current applied privacy policy ................................................................. 152
Figure 4.36. Selecting a privacy policy for the server 2 website .................................. 152
Figure 4.37. The code and store procedure for applying a privacy policy .................... 153
Figure 4.38. The code and store procedures for accessing personal information details ..... 154
Figure 4.39. Registration page, part 1 ................................................................. 155
Figure 4.40. Registration page, part 2 ................................................................. 156
Figure 4.41. Login page ............................................................................................... 156
Figure 4.42. Main page ............................................................................................... 157
Figure 4.43. View all created privacy policies ............................................................ 157
Figure 4.44. Creating a new privacy policy ................................................................. 157
Figure 4.45. Using the Smart Wizard System for adding and adjusting privacy policies.. 158
Figure 4.46. View all created privacy policies ............................................................. 158
Figure 4.47. Creating a new user on server 2, 3 or 4 .................................................. 160
Figure 4.48. Login process on servers 2, 3 or 4 ......................................................... 160
Figure 4.49. Alice’s account main page ................................................................. 160
Figure 4.50. Log into the server 1 database through server 2, 3 or 4 ............................. 161
Figure 4.51. Selecting one privacy policy from the list ............................................... 162
Figure 4.52. Saving a privacy policy ....................................................................... 162
Figure 4.53. An example of applying “high privacy level” to this website ...................... 163
Figure 4.54. Creating a new privacy policy through the websites of server 2, 3 or 4 ......... 164
Figure 4.55. The new privacy policy has been added to the list .................................. 165
Figure 5.1: Analysis of survey data ‘Section two’ ...................................................... 169
Figure 5.2: Analysis of use of mobile services ......................................................... 170
Figure 5.3: Mean values of the elements of personal information for males .................. 177
Figure 5.4: Mean values of the elements of personal information for females ............... 178
Figure 5.5: A comparison between Arabic and English cultures ............................... 186
Figure 5.6: A comparison, showing the disclosure of information in three different years . 184
Figure 5.7: A comparison between the years 2010 and 2012 ....................................... 186
Figure 5.8: Combined male and female views of personal information that should or must be hidden ................................................................. 192
Figure 5.9: Male views of personal information that should or must be hidden ............. 193
Figure 5.10: Female views of personal information that should or must be hidden ......... 194
Figure 5.11: A comparison between the default privacy settings in Facebook and in the proposed system for males ......................................................... 202
Figure 5.12: A comparison between selected default privacy settings in Facebook and in the proposed system for females ......................................................... 205
Figure 5.13: Profile Engine search page ................................................................. 206
Figure 5.14: The result from selecting one user .......................................................... 207
Figure 5.15: The results of searching for the user on the Facebook site ......................... 209
Figure 5.16: Percentage of items that can be accessed via a third party application ....... 213
List of tables

Table 3.1. An example of using an access control list .......................................................... 65
Table 3.2. An example of using a list to identify a privacy policy for the user ......................... 88
Table 4.1. The personal information items used in this study .............................................. 104
Table 4.2. Description of the Smart Wizard System’s database ........................................... 112
Table 4.3. The design of the wizard_user table. ................................................................... 135
Table 4.4. The design of the permission table. ...................................................................... 136
Table 4.5. The design of the wizard_user table. ................................................................... 137
Table 4.6. The design of the wizard_favorite_setting table. ............................................. 137
Table 4.7. Alice’s privacy policies. ....................................................................................... 139
Table 4.8. The status of sharing personal information items based on different privacy policies. ................................................................. 159
Table 5.1: Using the Alpha scale to calculate the reliability of the survey ............................. 167
Table 5.2: Analysis of the survey data for ‘Section one’ ....................................................... 168
Table 5.3: Analysis of survey data for ‘Section four A’ ........................................................ 171
Table 5.4: Analysis of survey data for ‘section four B’ ....................................................... 172
Table 5.5: Analysis of survey data for ‘section four C’ ....................................................... 172
Table 5.6: Comparison between Arabic and English participants. ....................................... 175
Table 5.7: Analysis identifying the important elements in a user’s personal information ....... 176
Table 5.8: Comparison between males and females for each element of personal information ................................................................................................................................. 179
Table 5.9: Distribution of privacy levels for both genders .................................................... 180
Table 5.10: Percentages of disclosure of personal information items in years 2005 and 2013. 183
Table 5.11: The relative importance of privacy ................................................................. 189
Table 5.12: Personal information items that concerned both genders and that were hidden. 192
Table 5.13: Create accounts in Server 1 ............................................................................. 195
Table 5.14: The created privacy policies .............................................................................. 196
Table 5.15: Login details and the applied privacy policies for each server ......................... 197
Table 5.16: The current applied privacy policy on each server for all users ....................... 198
Table 5.17: The applied privacy policies on server 3 and 4 .............................................. 199
Table 5.18: Default privacy settings for males. .................................................................. 201
Table 5.19: Percentage of hidden items, for males. ......................................................... 202
Table 5.20: Default privacy settings for females. .............................................................. 204
Table 5.21: Percentage of hidden items for females. ....................................................... 204
Table 5.22: A comparison between the implementation of the proposed system and other applications. ............................................................................................................. 211
List of Appendices

Appendix A: Task 1: Participant Information Sheet .............................................................. 257
Appendix B: Task 1: Ethics Approval ................................................................. 261
Appendix C: Task 1: Survey ......................................................................................... 262
Appendix D: Task 1: Statistical Data Analysis ................................................................. 268
Appendix E: Task 2: Participant Information Sheet .......................................................... 271
Appendix F: Task 2: Ethics Approval ............................................................................... 273
Appendix G: Task 2: Online Implied Consent for Participants .......................................... 274
Appendix H: Task 2: Online Survey ............................................................................... 276
Appendix I: Task 2: A scenario for selecting privacy settings using the Smart Wizard System ......................................................................................................................... 278
Appendix J: Results of applying different privacy policies for different users .............. 286
Appendix K: Application source code ............................................................................. 286