School of Computing

MSc Project Specification

Student type: Part Time Cohort: Management

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Surname :** | Corchero | |  | **Forename(s) :** | Mario |
|  |  | |  |  |  |
| **Address** : | 19, Avennue docteur Dautheville. Antibes. 06160 (France) | |  | **ID No.:** | B00228364 |
|  |  |  |  |
|  |  | **Email** : | B00228364@studentmail.uws.ac.uk |
|  |  |  |  |
|  | | | | | |
| **Project Title :** | | | | | |
| Smartphone Messaging Applications – How secure are they? | | | | | |
|  | | | | | |
| **Research Question :** | | | | | |
| Are the applications that we use for messaging on our mobile devices secure and is the data that we share safe? | | | | | |
|  | | | | | |
| **Outline (Overview) :** | | | | | |
| A variety of messaging applications have been released for mobile devices, including mobile phones and tablets, over the past few years. These applications have been widely adopted, not least because they enable users to leverage the Internet to exchange messages for free both nationally and internationally.  There appear to be two main routes to market: 1) applications developed directly for mobile devices (e.g. WhatsApp) and; 2) migration of applications that are already well established on desktop computers (e.g. Facebook Messenger and Google Talk). The same applications are found in different devices including smartphones and tablets and across virtually all mobile platforms including: Android, iOS, Windows Mobile, Symbian, etc.  However in the rush to bring these applications to market, enough attention has not been given to important considerations such as data security. As is the case with many mobile applications, building in robust security features has not been a primary development objective. Consequently, personal data is being exposed and given that the data that we typically share in a messaging application is of a sensitive nature, it is the author’s view that this warrants further investigation.  Research will involve distributing questionnaires to check how such messaging applications are currently being used and to identify users’ security expectations. The underlying security of existing applications will be studied and attempts will be made to bypass existing security mechanisms. Practical exploits will be underpinned by a wide ranging study of the literature pertaining to mobile security, network security techniques, and other relevant fields of research. | | | | | |
|  | | | | | |
| **Objectives (*The Project will)* :** | | | | | |
| 1. To determine how users utilize messaging applications.  2. To determine the security expectations users have about messaging applications.  3. To research and identify the security vulnerabilities of messaging applications.  4. To try to bypass the security that such applications provide. | | | | | |
|  | | | | | |
| **Relationship to Course (and Stream) :** | | | | | |
| This project draws on knowledge gathered from subjects including Mobile Business, Managing Projects and Information Security and Ethics for the Information Technology Professional.  Security in mobile devices may need to be improved and this study aims to highlight any security problems affecting messaging applications. | | | | | |
|  | | | | | |
| **Resources (including Reading List) :** | | | | | |
| 1. Bønes, E., Hasvold, P., Henriksen, E., Strandenæs, T., 2007. Risk analysis of information security in a mobile instant messaging and presence system for healthcare. International Journal of Medical Informatics 76, 677–687. 2. Cortjens, D., Spruyt, A., Wieringa, W.F.C., n.d. WhatsApp Database Encryption Project Report. 3. De Cristofaro, E., Durussel, A., Aad, I., 2011. Reclaiming privacy for smartphone applications, in: 2011 IEEE International Conference on Pervasive Computing and Communications (PerCom). Presented at the 2011 IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 84 –92. 4. Lane, D., 2003. Instant Messaging Security. 5. Nardi, B.A., Whittaker, S., Bradner, E., 2000. Interaction and outeraction: instant messaging in action, in: Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work, CSCW ’00. ACM, New York, NY, USA, pp. 79–88. 6. Reddy, N., Jeon, J., Vaughan, J., Millstein, T., Foster, J., 2011. Application-centric security policies on unmodified android. UCLA Computer Science Department, Tech. Rep 110017. 7. Schrittwieser, S., Frühwirt, P., Kieseberg, P., Leithner, M., Mulazzani, M., Huber, M., Weippl, E., 2012. Guess Who’s Texting You? Evaluating the Security of Smartphone Messaging Applications, in: Proceedings of the 19th Annual Symposium on Network and Distributed System Security. 8. Shanda Hong, Sun-Jen Huang, Chia-Sjemg Chang, 2012. CityGIM: A Mobile Multimedia IM System for Collaboration of Government Organizations [WWW Document]. URL http://student2.ntust.edu.tw/ezfiles/21/1021/img/326/hong.pdf (accessed 1.15.13). | | | | | |
|  | | | | | |
| **Marking Scheme :** | | | | | |
| Introduction 10%  Research Method 20%  Literature Review 25%  Data Analysis 20%  Critical Evaluation 10%  Conclusion and Further work 15% | | | | | |
|  | | | | | |
|  | | | | | |
| **Date (specification submitted) :** | | 16 January 2013 | | | |
|  | | | | | |
| **If a member of staff has agreed to supervise your project, please indicate their name below. We will also need an email from this person to confirm their agreement:** | | | | | |
|  |  | | | | |
| Supervisor: | **Andrew Rae** | | | | |