PINEPULSE: A System to PINpoint and Educate Mobile Phone Users with Low Security

Iosif Androulidakis[1] and Gorazd Kandus[2]

[1] Jožef Stefan International Postgraduate School
Jamova 39, Ljubljana SI-1000, Slovenia
sandro@noc.uoi.gr
[2] Department of Communication Systems, Jožef Stefan Institute
Jamova 39, Ljubljana SI-1000, Slovenia
gorazd.kandus@ijs.si

Abstract. The threats mobile phone users face, are about to increase due to the rapid penetration of advanced smartphone devices and the growing Internet access using them. As such, reinforcing users' security has become a critical imperative. This paper refers to a system that pinpoints and informs mobile phone users that have a low security level, thus helping them protect themselves. The system consists of software-application, installed in mobile phones as well as of software and data bases, installed in the mobile telephony operators' servers. Mobile telephony providers (by adopting this application), as well as manufacturers (by pre-installing it in their phones), could help mitigate the increased security threats effectively protecting the end users.

Keywords: Mobile phones security, User Education, Security Enhancing Application, User Profiling, Behavior Modeling.

1 Introduction

Mobile devices are becoming a critical component of the digital economy, a style statement and useful communication device, a vital part of daily life for billions of people around the world. The threats mobile phone users face, are about to increase due to the rapid penetration of advanced smartphone devices and the growing Internet access using them [1]. Mobile ubiquitous services pose great security challenges [2] while mobile phones are used from both experienced and security savvy users as well as from people that do not pay that much attention to security issues. All of them must be protected from unauthorized third party access to their data and from economic frauds. Since users' alone can't cope with this task, operators and handset manufacturers have to take extra security measures and to educate users.. The best way to deal with the problem, however, is by educating users.

2 Related Work

As previous work has shown [3][4], users exhibit different levels of knowledge in regards to security. A study of mobile users focusing on their awareness and concerns

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 62–66, 2012.

related to security threats, from security vendor McAfee, indicated that more than three quarters of respondents don't have any security at all [5]. In other words, despite of acknowledging the wealth of threats - ranging from phishing scams to viruses - that could impact them (including concerns about losing or having their phone or personal data stolen [6][7][8]), users don't see security strengthening of their phone as a critical concern.

In addition to the above, mobile security is not considered a critical issue by companies. Cell phone security for enterprise devices is seriously lacking, and a little misunderstood as well [9], while the majority of companies do not have a security policy that addresses mobile devices [10]. However, some initiatives are taken in the direction of protecting mobile phones against threats like viruses policies, tools and recruiting technically skilled personnel [11]. In regards to awareness systems, there have been efforts to create a sense of accountability in a world of invisible services that we will be comfortable living in and interacting with [12] as well as mechanisms for managing security and privacy in pervasive computing environments [13] but they still focus mostly in privacy issues and not actual security enhancement through education. In any case there are also significant legal issues as presented in [14].

It is more than clear that the mobile security area is going to be the next battleground since mobile security is an emerging discipline within information security arena and security levels are not high enough [15]. While users are not receiving proper cyber security and training education from schools [16], they are lacking the security awareness and proper etiquette [17]. This presents a vast opportunity for carriers and service providers to play a proactive and strategic role in protecting their subscribers, both through education and also through the security software they deploy across their networks, as is the case presented in this paper. Indeed, thanks to the system described in the following sections, these specific user categories can easily be pinpointed and presented with the right amount of information and dialogs [18] to restore their security level.

3 System's Architecture and Functions

The system consists of an application, installed in mobile phones and software and data bases, installed in mobile operators' main servers. These applications communicate through the mobile telephony network in a ciphered way. The mobile phone installed application (with minor differences in the array of services offered) would be able to function in all kind of devices that have an advanced operating system (e.g. Windows Mobile, Symbian, Android, iOS). A lighter version could also be implemented for older and simple devices using J2ME (Java 2 Micro Edition).

Three main functions are performed by the system. The first function allows pinpointing users, who have a low security level in their mobile phone, for whatever reason. The second function automatically suggests the proper methods, actions and best practices the user has to follow in order to restore security in a higher level. Finally, the third function, allows the encrypted communication and data exchange, between mobile devices and provider's servers.

The device's security level evaluation function can be implemented automatically, manually or with a combination of the two. Using the automatic method, the application transparently examines device's settings and informs the user for those that are in a state possessing security risk. In addition, by addressing questions to the user, the manual method, can check aspects of his behavior that do not reflect directly to the device's settings. Furthermore, the user is asked for his subjective opinion on how secure he feels his mobile is. As it is proven in previous work [14][3][4] users can be grouped in specific security categories, based on demographical and other behavioral elements as well as on the way of using their mobile phones. Results from both the manual and the automatic method are transferred to the applications in the server, where using artificial neural networks and rules, conclusions are extracted for the specific combination of user – mobile phone. Respectively, the answers to proper questions that examine the security practices that users follow, can lead to a security behavioral prediction model of the users. It is also possible to record the hour where changes of security influencing settings take place, as to provide one more element that can help the security model.

The system maintains data bases from studies in large user categories that provide the proper body for the system's training. These data bases are constantly updated with the results and the metrics from the system's operations. Finally, a very important function is the comparison of automated metrics to the user's answers, through which can be determined whether the user actually knows and applies the security measures or not. For this purpose, we use two metrics as awareness and security indicators: The mean actual awareness value (MAAV) and the mean actual security value (MASV), as described in [19]. These two methods, the automatic detection of settings and the conclusions extraction based on user's answers, complete the first stage of evaluating the security level.

At the second stage, the system implements the functionality of informing the user. Examining the current state and user's profile, the application suggests proper methods, actions and best practices the user has to follow in order to restore (if needed) the security in a higher level. If the device allows it and if the user accepts it, device settings can automatically be changed. Depending on the device functionality, instructions are presented to the user, either as a simple text documents or as multimedia material. The user can also configure different graphical user interface and setup elements as customization is a critical issue for software acceptance [20].

For the proper operation of the system, encrypted communication and date exchange between the device's application and the servers of the provider's network takes place. This communication is essential for off-loading the resource intensive neural network classification to the servers, instead of running it in the mobile device. In that way, the mobile device only records settings and the whole process takes place in the servers. Moreover, this communication allows not only the disposal of new multimedia material whenever is available, but also the enrichment of the manual evaluation method with new questions when new scientific data are presented. It can also upgrade the application itself, so that it can examine and locate a greater array of mobile phone's settings that reflect to its security. In any case, the communication takes place in a ciphered way so that interception is not possible.

4 Conclusion

By using this simple to implement system and the powerful data mining and modeling techniques of the underlying scientific principles it is possible to achieve a high security level, minimizing the risk factor attributed to the users. Bad security practices and risky usage are immediately pinpointed. In addition, user profiling and behavior prediction models based on the data gathered allow to further focus security efforts to those users that mostly need them. In any case the educational aspect of the application, using multimedia material improves users' overall security level, leading to greater security feeling and as such increased mobile phone usage.

References

1. comScore M: Metrics: Smarter phones bring security risks: Study (2008)
2. Leung, A., Sheng, Y., Cruickshank, H.: The security challenges for mobile ubiquitous services. Information Security Technical Report 12(3), 162–171 (2007)
3. Androulidakis, I., Kandus, G.: A Survey on Saving Personal Data in the Mobile Phone. Proceedings of Sixth International Conference on Availability, Reliability and Security (ARES 2011), pp. 633–638 (2011)
4. Allam, S.: Model to measure the maturity of smartphone security at software consultancies. Thesis. University of Fort Hare (2009)
5. McAfee: Mobile Security Report 2008 (2008)
6. Trend Micro: Smartphone Users Oblivious to Security. Trend Micro survey (2009)
7. CPP: Mobile phone theft hotspots. CPP survey (2010)
8. ITwire: One-third of Aussies lose mobile phones: survey. ITwire article (2010)
9. ABI Research, Study: Enterprises Need to Address Cell Phone Security (2009)
10. TechRepublic: Survey respondents say companies are lax on mobile security. TechRepublic article (2007)
11. Darkreading: Survey: 54 Percent Of Organizations Plan To Add Smartphone Antivirus This Year. Darkreading article (2010)
12. Langheinrich, M.: A Privacy Awareness System for Ubiquitous Computing Environments. In: Borriello, G., Holmquist, L.E. (eds.) UbiComp 2002. LNCS, vol. 2498, pp. 237–245. Springer, Heidelberg (2002)
13. Cornwell, J., Fette, I., Hsieh, G., Prabaker, M., Rao, J., Tang, K., Vaniea, K., Bauer, L., Cranor, L., Hong, J., McLaren, B., Reiter, M., Sadeh, N.: User-Controllable Security and Privacy for Pervasive Computing. In: Eighth IEEE Workshop on Mobile Computing Systems and Applications, HotMobile 2007 (2007)
14. King, N.J., Jessen, P.W.: Profiling the mobile customer – Privacy concerns when behavioral advertisers target mobile phones. Computer Law & Security Review 26(5), 455–478 (2010)
15. Goode Intelligence: Mobile security the next battleground (2009)
16. National Cyber Security Alliance (NCSA): Schools Lacking Cyber Security and Safety Education (2009)
17. Cable & Wireless: Workers lack mobile phone etiquette (2009)

18. De Keukelaere, F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L., Zurko, M.E.: Adaptive Security Dialogs for Improved Security Behavior of Users. In: Gross, T., Gulliksen, J., Kotzé, P., Oestreicher, L., Palanque, P., Prates, R.O., Winckler, M. (eds.) INTERACT 2009. LNCS, vol. 5726, pp. 510–523. Springer, Heidelberg (2009)
19. Androulidakis, I., Kandus, G.: Feeling Secure vs. Being Secure the Mobile Phone User Case. In: Jahankhani, H., et al. (eds.) ICGS3/e-Democracy 2011. LNICST, vol. 99, pp. 212–219. Springer, Heidelberg (2012)
20. Hakila, J., Chatfield, C.: Personal customization of mobile phones: a case study. In: Proceedings of NordiCHI, pp. 409–412 (2006)