An application to estimate the Cyber-risk Detection Skill of mobile device users.

(Novel idea presentation)

Guillaume Schaff
itrust consulting (Luxembourg)
schaff@itrust.lu

Romain Martin
University of Luxembourg
romain.martin@uni.lu

Carlo Harpes
itrust consulting (Luxembourg)
harpes@itrust.lu

Marianne Junger
University of Twente
m.junger@junger.nl

***Abstract*— According to experts' predictions, mobile devices (smartphones, tablet computers) will replace the widespread personal computer by 2017 for personal and work tasks (emergence of BYOD). In parallel, the expert community has observed an increase of cyber-attacks against mobile devices. Mobile device users are increasingly required to develop new skills to manage their equipment correctly. Towards this goal, the 21st Century Skills framework redefines the essential knowledge and skills, which people should acquire during the education process in order to meet the new requirements of the "computing society". However, the lack of IT security awareness on mobile devices clearly shows that the 21st Century Skills is not yet assimilated by the users. To measure and improve the assimilation of such skills, we propose to define a new psychological concept; Cyber-risk Detection Skill (CDS), inspired by the 21st Century Skills framework. In this, paper we present the concept and design of a user behaviour test based on a cyber-attack scenario in order to measure user awareness. In a later phase we propose to develop a psychological tool (such as a specific methodology), which will measure the Risk Detection Skill of mobile device users in a more comprehensive way.**

Keywords: Security awareness, social engineering risks, behaviour analysis and measurement, risk detection, IT risks, Smartphone and IT users.

I. INTRODUCTION

The emergence of the mobile technologies has changed our lifestyle and our environment over the last ten years. The complexity of mobile devices (smartphones, computers, etc.) has encouraged the development of new skills by the users and requires them to adapt to new technologies. However, technology often evolves faster than people can adapt to it and currently only a small part of the population is aware of the IT security risks. During the last two years, the number of malware developed to exploit weaknesses in mobile devices (SMS Zombie, Fakelnt, Marketpay) has strongly increased (3069 in 2012) [1], [2]. The cybercriminal motivation to hack mobile devices is usually to embezzle money from victims. For example, mobile devices generally include insecure billing systems, which is supported by the telecommunication operators [3], [4] and present several flaws. This insecure system can be exploited by cybercriminals to swindle money out of the victims (surtaxed SMS/calls) [5]. There are also other threats aiming at mobile device users such as hacking or mobile viruses [6], [7]. Besides technical weaknesses, users have characteristics that make them vulnerable to manipulations by attackers in many circumstances. This has been labelled 'social engineering' [8], [9]. Research shows that humans are easily fooled and tend to be gullible [10], [11]. They tend not to see the cyber risks that confront them. This shows that mobile device users' skills are in urgent need of improvement [12], [13]. With that goal in mind, we propose the development of a new concept called Cyber-risk Detection Skill (CDS). Below, we first explain the concept of CDS. Then, we present the attack scenario, which allows us to present the general context of the IT awareness level of mobile device users. In future work, the concept of CDS will be elaborated further and its emotional, cognitive and behavioural aspects will be explored in more depth.

II. THE CYBER-RISK DETECTION SKILL (CBS)

In order to adapt to the current "ICT society", people are required to master essential new skills. We define the Cyber-risk Detection Skill (CDS) concept to evaluate the capacity of people to detect a risk situation in their daily life. The CDS concept is inspired by the "21st Century Skills" developed by Bernie Trilling and Charles Fadell, which redefines the education objectives according to 21st century requirements. One of our project objectives consists in increasing the knowledge of mobile device users with regards to cyber-risk detection. In our study we will focus on cyber risks; specifically on the mobile device users' risk detection ability.

We created the new psychological CDS concept mainly to evaluate the specific skill assimilation, which consists of detecting a mobile device attack (malicious email, application, etc.) and avoiding virus infection on a mobile device. Thanks to this concept we will be able to measure the ability of mobile device users in detecting an IT attack. The measurement results will help us identifying several user groups, which could be potential victims of IT attacks. The mobile user groups' classification will be useful for adapting IT security awareness according to specific users.

This idea is part of the panel of new tools developed in the framework of the FP7 TREsPASS project. The TREsPASS project aims at developing methods and tools to analyse and visualise information security risks in dynamic organisations. It combines knowledge from technical and social sciences (e.g., social engineering, behavioural study). The results of our experience will contribute to the TREsPASS project by the means of an experimental tool

based on the mobile device users' behaviour analysis regarding social factors (age, socio-economic background, personality, general cognitive abilities). This tool will include these social factors in a model in order to predict a successful social engineering attack on a dynamic organisation.

III. THE CDS ATTACK SCENARIO

The most typical attack scenario against mobile devices consists of implementing a Trojan in an official application available on the application markets (2) (Google Play) and inviting the victims to download the infected application.

After installation the malicious application has access to the whole phone database and can be used for criminal purposes. For example, the most skilled attackers can secretly listen to phone conversations, track a device, install malicious mobile device applications via a link, take photos, or even make online purchases without the owner's consent. Below we present an experimental attack scenario that will be used to test user's CDS.

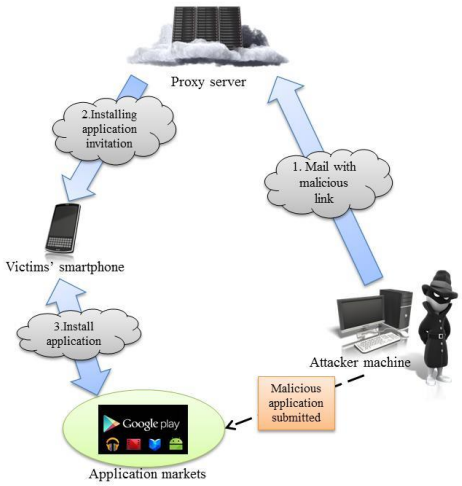

Figure 1: Presentation of attack scenario steps

This experimental attack scenario consists of six steps. 1) The researchers will send a false email to a small organisation mailing list (private company or public organisation). This false email will invite the user to download a gaming application on Google Play. 2) We will submit a malicious application, which contains a "Pass" on Google Play to access to the users mobile devices. 3) After downloading and installing the application on the mobile device, the application will generate an automatic message that promises to be more effective if allowed access to the mobile device's geo-localisation, contacts and database. 4) In case of acceptance by the user the researchers/attackers succeeded in having a theoretical access to the mobile devices' database. 5) After the user has given the application full access rights, they will then be asked by the researchers to create a "gaming profile" by completing a questionnaire, which includes relevant personal information. 6) After the questionnaire has been validated by the user an automatic message will appear on the screen and inform the user that they have given a malicious application access to their mobile device's database.

This experimental attack scenario exploits one of the flaws of Google Play: This experiment is feasible because Google Play does not yet use an effective application checking system that can detect malicious applications. It is important to stress that the type of information obtained during the attack could be used by a hacker to guess the victim's password and username for social networking accounts (Facebook, twitter), professional networks (Viadeo, LinkedIn), banking interfaces or company intranet accounts (VPN, SVN). However, the main goal of the experimental attack is not to steal personal information from the users/potential victims but to evaluate their ability to detect an attack. To be sure to reach the maximum amount of potential survey victims, this "fake gaming application" will be submitted to Google Play, which is the most used application market. We stress that this experience is a real social engineering attack and all the information collected during this test will be anonymously exploited and then stored for analysing and interpretation.

After analysing and interpretation of the first results, we propose to establish other relevant CDS attack scenarios, which correspond to common risk situations. These other CDS attack scenarios will have various scopes like false pop-up message interpretation and social engineering phone attack detection at a helpdesk. The results of these experiences will allow us to measure the ability of mobile device users in detecting an IT risk situation depending on social factors (age, socio-economic background, personality, general cognitive abilities).

IV. CONCLUSION

The attack on mobile devices with an infected "fail gaming application" will be used to determine the general ability of the mobile device users in detecting an attack, which could have serious consequences (e.g., personal information theft). The results of this experiment will also be used to illustrate our new CDS concept by presenting the current users' IT security awareness. The results will be gradually analysed depending on the users' reaction (application downloaded, questionnaire completed) and analysed to see if the user is able to detect an IT risk situation. This will allow us to establish the usefulness of the Risk Detection Skill concept. In the continuity of our project, we will develop and improve our test scenario with other approaches. After analysing the results of this first experience we expect to establish at least two other test scenarios. Presently, the researchers will develop the prototype application and submit it on Google Play to test on a dozen smartphones. After the pilot phase, the next step of this experience will consist of attacking smartphone users of targeted organisations. The publication of the results and conclusions is planned for the third quarter of 2014.

REFERENCES

[1] X. Jiang, A. Bhattacharya, P. Dasgupta, W. Enck. A survey of mobile malware in the wild. Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. University of California, Berkeley. Pages 3-14. 2011.

[2] A. Derrick Schmidt, S. Albayrak. Malicious Software for Smartphone., Technical Report: TUB- DAI 02/08-0. Technische Universitat Berlin/ DAI-Labor. 2008.

[3] Bose, Abhijit, and Kang G. Shin. "On mobile viruses exploiting messaging and Bluetooth services." Securecomm and Workshops, 2006. IEEE, 2006.

[4] D. Shih, H. Lin, H. S Chiang, M. H. Shih, (2008). "Security aspects of mobile phone virus: a critical survey. Industrial Management & Data Systems", 108(4), pages 478-494, 2008..

[5] W. Jeon, J. Kim, Y. Lee, D. Won. "A practical analysis of smartphone security." Human Interface and the Management of Information. Interacting with Information. Springer Berlin Heidelberg, 2011..

[6] T. Dimkov, W. Pieters, P.Hartel. Scenarios Spanning through the Physical, Digital and Social Domain, Distributed and Embedded Security Group, University of Twente {trajce.dimkov,wolter.pieters,pieter.hartel}@utwente.nl}. 2010..

[7] Ostrovsky, Rafail, and Moti Yung. "How to withstand mobile virus attacks." Proceedings of the tenth annual ACM symposium on Principles of distributed computing. ACM, 1991.

[8] P. Hartel, M. Junger, M. Klaver, E.Luiijf, R. Wieringa. Towards quantitative cybercrime analysis. Position paper, version 30 March 2013.

[9] A. Herzberg, R. Margulies, "Long-term user study of forcing and training login mechanisms against phishing". Tech. rep, Bar Ilan University, March 2011.

[10] C. Fleizach, M. Lijienstam, P. Johansson, G. Voekler, A. Méhes. Can you Infect Me Now? Malware Propagation in Mobile Phone Network. WORM conference. University of California, San Diego. 2007.

[11] C. Hale. "Fear of crime : a review of the literature" International Review of Victimology. Volume 4, Pages 79-150, 1996.

[12] B. Trilling, C. Fadel, 21st century skills: learning for life in our times. San Francisco, CA: Jossey-Bass. http://www.21stcenturyskillsbook.com/index.php. 2009. C. Fadel,

[13] B. Trilling. "Encyclopaedia of the Science of Learning", Springer Science + Business media, LCC 2012.