RISK-DET: ICT Security Awareness Aspect Combining Education and Cognitive Sciences

Guillaume Schaff, Carlo Harpes, Matthieu Aubigny
itrust consulting (Luxembourg)
{schaff, harpes, aubigny}@itrust.lu

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

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

***Abstract*— This paper explains the main innovation of a risk assessment tool, called RISK-DET, which will include an ICT risk awareness aspect supported by a specific application: Voozio 2.0. The design of the RISK-DET tool considers the implementation of the emergent ICT (Information and Communication Technology) Risk Detection Skill (IRDS) concept. Today, the users' inability to detect a risk situation is a real security problem and represents a societal challenge. According to the results of a security experiment based on a malicious smartphone application called Voozio 1.0, the main reason for this problem is the absence of effective ICT security awareness training programs adapted to users' needs. To prove and confirm this hypothesis, we aim to evolve the Voozio application in the 2.0 version. This new version will be able to determine the ability of ICT users to detect a risk situation and improve it by combining cognitive sciences and education technologies. We will describe here the specifications of the new version of Voozio. We also present the Voozio 2.0 implementation framework.**

Keywords-E-learning; ICT security awareness; social engineering; cyber-security; cognitive sciences; risk perception; education science; human-computer interaction.

I. INTRODUCTION

The rising use of new Information and Communication Technologies (e.g., smartphones, digital tablets, laptops, etc.) in our daily life has increased our vulnerability to new cyber-attacks [1][2][3]. With the cyber-criminal professionalization, the ICT threats (virus, phishing, scamming) are more sophisticated and their impact can be very significant on our lives [4][5] (personal data theft, ransomware). In parallel, the current security mechanisms are not yet sufficiently adapted to face these new types of ICT attacks. To limit their impacts, several researchers have developed anti-phishing training programs [6][7][8]. However, these programs are not sufficient to limit an ICT attack and that is why the ICT users' ability to detect a risk situation (ICT Risk Detection Skill (IRDS)) should be improved. To improve their ICT Risk Detection Skill (IRDS), users should be able to adopt good security practises when faced with cyber-threats. Here, an ICT risk is the probability that a threat exploits ICT vulnerabilities (e.g., malicious email, phishing link, etc.) which impacts the confidentiality, integrity or availability of information. To limit these impacts, we propose to develop a security awareness aspect to improve the users' ICT Risk Detection Skill level. Research has been done to develop, for instance, security awareness and education programs [9]. A few experiments have been executed. They show that, through training, ICT users develop new skills improving their ability to detect ICT attacks (detect false/malicious email, malicious spam). Still, a lot of work needs to be done in the field of cybercrime prevention, in particular ways to prevent users becoming victims of social engineering [10][11].

Accordingly, the present paper aims to present a new tool which has two aspects: firstly, a measurement aspect to determine the users' ability to detect a risk situation (IRDS); secondly, an ICT security awareness aspect to improve IRDS. This global ICT security awareness solution will not be an isolated solution, but will be integrated into a set of several tools, developed in the framework of the FP7 TREsPASS project [18]. This European project aims to combine technical and social sciences in order to develop methods and tools to analyse and visualise information security risks in dynamic organisations. The expected outcome of this project is an "attack navigator" indicating which attack opportunities are possible in a targeted organisation, which of them are the most critical, and which countermeasures are most effective. To identify potential attack opportunities, the RISK-DET tool contributors (who are also participants of the TREsPASS project) aim to develop an additional risk assessment tool focused on social sciences.

The present paper first explains the role of cognitive sciences in ICT security awareness. Secondly, it presents the security awareness aspect (represented by the Voozio 2.0 application) of the RISK-DET tool. Thirdly, it describes the implementation framework of the Voozio 2.0 application. Finally, we conclude by describing the next steps, the research hypothesis and expected results.

II. COGNITIVE SCIENCES IN ICT SECURITY AWARENESS

With a lack of ICT security awareness, users are strongly susceptible to social engineering and phishing attacks [13]. As part of our previous research [12], we created a malicious application on Google Play and used it to test the ability of a representative sample of informed users to detect a risk situation on their smartphones. Our results show that more than half of the targets submitted their personal information to our malicious smartphone application called Voozio. It seems feasible to conclude that the majority of ICT users are relatively susceptible to IT attacks. We concluded that the cognitive aspect has an impact on the ICT users' reaction when faced with risk situations.

In general, cognitive sciences are based on the study and modelling of users' perception and particularly the risk perception. That is why we have decided to integrate cognitive sciences a.o. in Voozio 2.0, to obtain more in-depth results. In general, scholars have argued that ICT users have a major role to play in enhancing global ICT security [14]. The purpose of the present study is to present an evolved version of Voozio that will integrate cognitive, social and education sciences. As users are one key element to avoid ICT attacks, the cognitive aspect of the ICT users should be strongly developed thanks to efficient security awareness solutions. The development of Voozio 2.0 will be based on the cognitive sciences, in line with our IRDS concept. What do we mean when we use the term "cognitive

 ISBN: 978-1-61208-346-9

sciences"? Cognitive sciences are a set of scientific disciplines dedicated to the description, explanation, and appropriate simulation mechanisms of human thought [13]. Based on the approach of cognitive sciences applied to ICT, the design of Voozio 2.0 should include two following properties: firstly, a function for evaluating the IRDS of the users whilst considering several psychological factors (character, personality, reason ability), and secondly, a function for generating a relevant training program in line with users' needs. Cognitive science is tied with Educational Technology, and we believe that this discipline should be integrated into the new version of our application by incorporating an education program which can be adapted for individual users. For Voozio 2.0, the cognitive science integration will consist of collecting test subjects' psychological factors (character, personality, reason ability) with a dedicated questionnaire, validated by an expert panel. The psychological factors will allow the Voozio 2.0 administrator to establish subjects' psychological profile. This profile will be used in the IRDS measurement phase and refined continuously in the next phase.

III. ICT SECUTIRY AWARENESS ASPECT PRESENTATION

The Voozio 2.0 application is composed of a Computer Assisted Test (CAT) based on identified ICT risk situations, e.g., malicious email and/or website. The risk situations will be presented to the tested users through short videos, pictures, or games. The users' aim is to identify what level of risk the ICT situation presents. During this CAT, the researchers will analyse the users' behaviour based on several factors, such as time taken to answer, uncertainty, etc. In order to obtain an accurate way of scoring, the risk situations will follow a precise graduation depending on the level of danger based on their impacts. The analysis of users' reactions when faced with an ICT risk scenario will be scored and analysed according to a pre-defined scale. After the IRDS measurement phase, Voozio 2.0 will introduce an educational program composed of e-learning modules. The e-learning modules will be adapted to the users' risk perception ability and reactions. Here, we aim to improve the IRDS level of the users. As shown in Figure 1, the increase in IRDS level is supported by six disciplines.

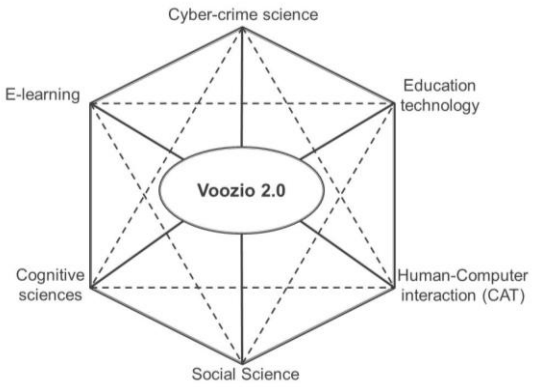

Figure 1. Disciplines of the IRDS increase phase

A sustainable improvement of the IRDS requires as many interactions as possible between these six disciplines. Therefore, Voozio 2.0 will integrate the Cognitive and Social sciences, as well as Human-Computer interaction in the IRDS level measurement phase. These disciplines will consider test subjects' psychological profiles in the IRDS measurement. Moreover, the researchers aim to include E-learning, Education and Cyber-crime science [14] in Voozio 2.0 conception to increase the users' IRDS level. Furthermore, the ICT security awareness aspect will allow Voozio 2.0 administrators to provide training programs adapted to users' training needs depending on the IRDS test results and subjects' reactions (user behaviour). The social sciences play an important part in the Voozio 2.0 general process by bringing an additional precision level to the IRDS measurement.

IV. VOOZIO 2.0 IMPLEMENTATION

An adapted IRDS measurement test should be integrated in Voozio 2.0 to determine users' training needs. This test is intended for a group of users and necessitates a preliminary requirement; the agreement between "the trainer" and the management team of the organisation (e.g., Managing Director, IT Manager, etc.). Here, the trainer corresponds to the Voozio 2.0 administrator who will submit the IRDS measurement and the training program to the targeted staff. The test will consist of sending an email which proposes to install the Voozio 2.0 application to the entire staff of a private/public organisation. After installation, Voozio 2.0 will generate several risk situations (e.g., malicious email and spam). We stress that the risk situations generated will not present any danger for the users' devices. The test will only measure how many of the users are unaware of the threat and "fall into the trap". Once the data has been collected and interpreted, the trainer will be able to establish a first IRDS level evaluation for all staff. After the test, Voozio 2.0 will send a training program composed of e-learning modules focusing on good ICT security practices to all the employees. A short time (one or two weeks) after the ICT security awareness program, an additional risk situation will be generated by the Voozio 2.0 application to evaluate the reliability of the provided training programs. A comparison study will be performed by the trainer to note the difference between the IRDS test results obtained before and after training program. Thanks to this test, we will be able to measure the efficiency of the ICT security awareness aspect based on any improvements. To have relevant results, application implementation will be on a large organisation to measure and improve the ICT Risk Detection Skill level of their employees (pool of testers).

If we succeed to reach the critical mass for the test pool, we will be able to collect relevant results needed to establish a statistical study. According to a precise and automatic analysis of the results, the solution will create a user classification depending on their ICT attack vulnerability and will generate dedicated ICT training programs specific to different user groups to enhance ICT Risk Detection Skill. As in our previous research, no personal data will be retained during this test and test subjects' privacy will be strictly respected.

V. MODEL ANALYSIS

The preliminary work of researchers consisted to identify related works [15][16][17] and establish a formal

 ISBN: 978-1-61208-346-9

state-of-the-art in risk perception domain. Before the experimental phase, we aim to submit Voozio 2.0 to an expert panel which have been worked on the same domain to analyse the proposed model and give their feedback on it. The expert panel feedback will allow us to refine the prototype to be adapted to users' needs. The expert panel will be selected by the Voozio 2.0 designers and will group experts from industrial and academic organisations.

VI. CONCLUSION

In the FP7 TREsPASS project framework, we aim to develop the RISK-DET risk assessment tool which will include an ICT security awareness aspect based on Cognitive and Education Sciences called Voozio 2.0 (based on the results of the previous experience conducted with the smartphone application Voozio 1.0). Analysis of similar works will allow us to define the Voozio 2.0 technical and functional specifications and implement our IRDS concept. After the Proof of Concept development phase (planned 3rd trimester 2014), we suggest that the Voozio 2.0 beta version could be validated by an expert panel and tested on an organisation of 1000 employees during an experimental phase. This phase will allow us to test our innovative IRDS measurement methodology and make our research work (results interpretation and model analysis). In the long term, Voozio 2.0 could provide a commercial ICT risk awareness solution. However, we should keep in mind that the effect of training can decrease over time. Due to this fact, the tool shall be based on a core system using versatile contents which will be set up over time, depending on the context of the ICT threat and on the security maturity of the organisation. Voozio 2.0 will enable us to propose a permanent IRDS measurement and security awareness solution. The first result of our work is the Voozio 2.0 technical and functional specifications document which will be published during the ICCGI 2014 conference.

AKCNOWLEDGEMENTS

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 318003 (TREsPASS). This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained herein.

REFERENCES

[1] K. Choo, "The cyber threats landscape:Challenges and future research directions", Computer & Security, vol. 30, iss. 8, 2011, pp. 719-731

[2] M. Yar, "The novelty of Cybercrime, an Assessment in Light of Routine Activity Theory", European Journal of Criminology, vol. 2, iss. 4, 2005, pp. 407-427

[3] P. Williams, "Organized Crime and Cybercrime: Synergies, Trends and Responses", Global Issues, vol. 6, iss. 2, 2011, pp. 22-26

[4] T. Jagatic, N. Johnson, M. Jakobsson, and, F. Menczer,, "Social phishing" Communication of the ACM, vol. 50, iss. 10, 2007, pp. 94-100

[5] A. Gazet, "Comparative analysis of various ransomware virii", Journal in Computer Virology, vol. 6, iss. 1, 2010, pp. 77-90

[6] S. Sheng, et al, "Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish", Proceedings of the 3rd symposium on Usable privacy and security, 2007, pp. 88-89, ISBN: 978-1-59593-801-5.

[7] P. Kumaraguru, et al, "School of phish: a real-world evaluation of anti-phishing training", Proceeding of the 5th Symposium on Usable Privacy and Security. Iss. 3, 2009, ISBN: 978-1-60558-736-3.

[8] X. Luo and, Q. Liao, "Awareness Education as the key to Ransomware Prevention", Publishing models and article dates explained, vol. 16, iss. 4, 2007, pp. 195-202.

[9] M.E. Thomson and, R. von Solms, "Information security awareness: educating your users effectively", Information Management & Computer Security, vol. 6 iss. 4, 1998, pp.167 – 173

[10] B. Claverie, "Cognitique, Science et pratique des relations à la machine à penser", Revue des sciences de l'éducation, vol. 34, iss. 1, 2005, pp. 227-228

[11] Hartel, P.H., Junger, M. and, Wieringa, R.J. "Cyber-crime Science = Crime Science + Information Security", Technical Report TR-CTIT-10-34, Centre for Telematics and Information Technology University of Twente, Enschede, 2010

[12] G. Schaff, C. Harpes, R. Martin and, M. Junger, "An application to estimate the cyber-risk detection skill of mobile device users". Sixth International Conference on Advances in Human oriented and Personalized Mechanisms, Technologies, and Services, CENTRIC 2013, November 2013, Venice, Italy.

[13] E. Albrechtsen. "A qualitative study of users' view on information security". Computer & Security, vol. 26, iss. 4, pp. 276-289

[14] T. Vidas, E. Owusu, S. Wang, C.Zeng, L. Faith and, N. Christin. "QRirshing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks" Financial Cryptographie and Data Security, 2013, pp. 52-69,.

[15] L. Sjoberg, B-E. Moen, and, T. Rundmo, "Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research"; Trondheim, 2004.

[16] N. Pidgeon, "Risk assessment, risk values and the social science programme: why we do need risk perception research". Reliability Engineering & System Safety, vol. 59, iss. 1, 1998, pp. 5-15.

[17] B. Fischhoff, et al. "Risk perception and communication". Oxford textbook of public health, vol. 2, iss. 5, 2009, pp. 940-953

[18] P. Hartel and, W. Pieter; "FP7 project TREsPASS press release", January 2013

 ISBN: 978-1-61208-346-9