Creativity Techniques for Social Engineering Threat Elicitation: A Controlled Experiment

Kristian Beckers[1], Veronika Fries[2], Eduard C. Groen[3], and Sebastian Pape[1,4]

[1] Social Engineering Academy
kristian.beckers,sebastian.pape@social-engineering.academy
[2] Technical University of Munich
veronika.fries@in.tum.de
[3] Fraunhofer IESE
eduard.groen@iese.fraunhofer.de
[4] Goethe University Frankfurt
sebastian.pape@m-chair.de

Abstract. We propose a controlled experiment to assess how well creativity techniques can support social engineering threat assessment. Social engineering threats form the basis for the elicitation of security requirements, a type of quality requirement, which state what threat should be prevented or mitigated. The proposed experiment compares a serious game and the Morphological Forced Connections technique with regard to their productivity, as well as completeness and precision.

Social engineering is the illicit acquisition of information about computer systems by primarily non-technical means. Although the technical security of most critical systems is usually being regarded, such systems remain highly vulnerable to attacks from social engineers that exploit humans to obtain information (e.g., phishing) [3, 4]. To develop systems that are more resilient to threats from social engineering, the security requirements should specifically address such threats.

Moreover, performing a threat assessment of social engineering is hard, because an attacker (a) does not need any (advanced) technical skills, and (b) can conduct an attack without advanced equipment. Hence, anyone can inflict significant damage through social engineering[5]. We have developed a serious game for social engineering [1, 2] (see Fig. 1), which is suitable for educating non-security experts about the threats of social engineering, as well as for eliciting security requirements to prevent and mitigate social engineering threats. The empirical elicitation and assessment of security requirements concerning social engineering is difficult, as it is not the system's security measures themselves that are causing the security threat, but unpredictability of humans with system knowledge. For example, humans can give away passwords. In the business context, these techniques additionally rely on the participation of common employees, who posses the required practical and domain knowledge.

[5] http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf

Figure 1: Game on Social Engineering

This makes foreseeing possible social engineering threats the main challenge. The elicitation of requirements to this end draws on the stakeholders' ability to make new associations, and therefore requires creativity techniques for the combination of existing (work) practices and potential threats.

In order to validate the suitability and effectiveness of our game (cf. [1, 2]) for eliciting security requirements concerning social engineering, we propose to conduct an experiment of 90 minutes in which we compare its yield for social engineering threat elicitation with that of the Morphological Forced Connections technique [5]. This established creativity technique was chosen because of its suitability to transform a combination of preexisting (work) aspects into new conceptual combinations (i.e., a threat) through inference.

The *context* of our experiment is the CreaRE workshop. Social engineering threats for a predefined scenario are elicited from the participants in either of two conditions. Our *hypothesis* concerns the productivity and precision of both approaches. We hypothesise that the serious game is more productive and precise than the creativity technique. We define true positives (TP) as correctly identified threats (i.e., correct result that experts have previously found or or that they verify during the experiment). False positives (FP) are threats reported by participants but not verified by expert review. We measure productivity in the number of TP discovered during a limited time frame and precision as the percentage of TP of the overall discovered threats. The *independent variable* is the technique used for the social engineering threat assessment, with two levels: "social engineering game" and "Morphological Forced Connections technique". The *dependent variables* are the total number of threats elicited with each method, the number of threats that are identified to be correct, and the time required to identify these threats. The correctness is validated by security experts reviewing the elicited threats and an assessment of the participants during the experiment.

The results of our experiment should provide an indication of how suitable the two creativity techniques are for performing social engineering threat elicitation. We need additional research to address the fundamental threat of social engineering to security.

References

1. Beckers K., Pape S. A Serious Game for Eliciting Social Engineering Security Requirements, Proceedings of RE, IEEE Computer Society, pp. 16-25, 2016
2. Beckers K., Pape S., Fries V. HATCH: Hack And Trick Capricious Humans - A Serious Game on Social Engineering, Proceedings of BHCI, ACM, pp. 1-3, 2016
3. Mitnick, K.D., Simon, W.L.: The Art of Deception. Wiley (2009)
4. Hadnagy. C.: Social Engineering - The Art of Human Hacking. Wiley (2011)
5. Boden. M.A.: The Creative Mind: Myths & Mechanisms (2nd Ed), Routledge (2004)