HATCH: Hack And Trick Capricious Humans – A Serious Game on Social Engineering

Kristian Beckers
Technische Universität München (TUM)
Institute of Informatics
Boltzmannstr. 3
85748 Garching, Germany
kristian.beckers@tum.de

Sebastian Pape
Goethe-University Frankfurt
Faculty of Economics
Theodor-W.-Adorno-Platz 4
60323 Frankfurt, Germany
sebastian.pape@m-chair.de

Veronika Fries
Technische Universität München (TUM)
Institute of Informatics
Boltzmannstr. 3
85748 Garching, Germany
veronika.fries@tum.de

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 in penetration tests, such systems remain highly vulnerable to attacks from social engineers that exploit human behavioural patterns to obtain information (e.g., phishing). To achieve resilience against these attacks, we need to train people to teach them how these attacks work and how to detect them. We propose a serious game that helps players to understand how social engineering attackers work. The game can be played based on the real scenario in the company/department or based on a generic office scenario with personas that can be attacked. Our game trains people in realising social engineering attacks in an entertaining way, which shall cause a lasting learning effect.

Security, Methods, Education, Social Engineering, Serious Gaming

1. INTRODUCTION

Traditional penetration testing approaches often focus on vulnerabilities in network or software systems (Mitnick and Simon (2009)). Few approaches even consider the exploitation of humans via social engineering. While the amount of social engineering attacks and the damage they cause rises yearly the awareness of these attacks by employees remains low (Hadnagy (2010, 2016); Proofpoint (2016)).
Recently, serious games have built reputation for getting employees of companies involved in security activities in an enjoyable and sustainable way. While still preserving a playful character, serious games are used for e.g. security education and threat analysis (Williams et al. (2009, 2010), Shostack (2012, 2014), Denning et al. (2013)). We believe that there is a major benefit for adapting serious games specifically for social engineering (Beckers and Pape (2016a)). Our game aims at enabling common employees to elicit social engineering threats for their companies (real world scenario). Additionally, we have developed a generic scenario for training and awareness rising, which provides a description of a fictional office scenario with personas. In this paper we present our game, the generic scenario and our preliminary results of its application with students, academics, and industry.

Figure 1: *Picture of a Game Session*

2. DESIGN OF THE GAME

In short, the rules of the game are as follows:

1. Each player draws a card from the deck of *human behavioral patterns* (principles), e.g. the *Need and Greed principle*. The game is designed based on existing published work (e.g. Stajano and Wilson (2011), c.f. Beckers and Pape (2016b)).
2. Each player draws three cards from the deck of the *social engineering attack techniques* (scenarios), e.g. phishing. The game is

designed based on existing published work (e.g. Gulati (2003); Peltier (2006), c.f. Beckers and Pape (2016b)).

3. The players decide if they are insiders or outsiders to the organization.
4. Each player presents an attack to the group and the others discuss if the attack is feasible.
5. The players get points based on how viable their attack is and if the attack was compliant to the drawn cards. The player with the most points wins the game.
6. As debriefing, the perceived threats are discussed and the players reflect their attacks. They may be supported by the company's security personal.

3. INDEPENDENT SCENARIO

We created a generic scenario that people can relate to with little effort. We came up with the ACME office company, a medium sized producing company for paper. Therefore, we described 10 employees, their roles in the company, familiarisation with computers and attitudes towards security and privacy (see Fig. 2 as an example).

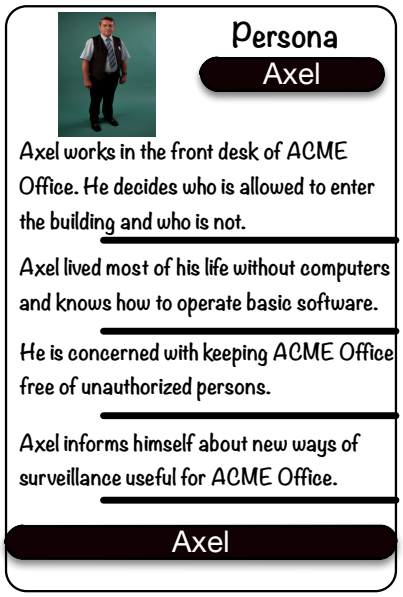

Figure 2: *A persona[1] within our ACME Office scenario*

4. PRELIMINARY RESULTS

To validate our research, we initially played the context-specific version with 25 full time employees of the Technical University Munich and Goethe-University Frankfurt with a university degree. We were initially interested if the players could elicit possible and context-specific threats for their respective environments. We played in total 49 turns of the game in which a player suggests a threat. The players deemed 42 of these threats possible and 7 were rated not possible by the players. The results suggest that the players were able to elicit threats with the game (c.f. Beckers and Pape (2016a)).

Afterwards, we were interested to measure if playing the game raises the security awareness of the players. Kruger and Kearny (Kruger and Kearney (2006)) measure security awareness in terms of knowledge (what an employee knows), attitude (what an employee thinks), and behaviour (what an employee does). We created a set of 14 questions that measured security awareness with relation to the attack scenarios in our game on a 5-point Likert scale. The answers range from *totally disagree* to *totally agree*. We assessed the questionnaires with games played with 10 full time employees from academia and 4 senior employees of an organisation A. The academics used our ACME office scenario and the senior employees the context-specific version of the game. We could measure on average between 0.5 and 1 point increase in security awareness with the players after they played HATCH. There was no statistical significant difference in persons who worked with ACME office scenario and the ones with the context-specific version of the game.

In future, we will try both versions of the game with a larger sample of participants and we are planning to measure the flow construct (Csikszentmihalyi (2000)) in relation to playing the game. In particular, we are planning to use the Flow Kurz Skala (Rheinberg et al. (2016)) to measure how intensive the player emerge in the game and correlate this to the difference in security awareness before and after the game. We assume that the flow experience is positively correlated to an increased security awareness. Additionally, we will create more generic scenarios to allow players with different background an easier access to the game.

5. ACKNOWLEDGEMENTS

We thank all the players of our game that provided us with invaluable feedback and spend their precious time with us improving the game. This research has been partially supported by Federal Ministry of Education and Research Germany (BMBF) within the focal point "IT-Security for Critical Infrastructures" (grant number 16KIS0240) and the TUM Living Lab Connected Mobility (TUM LLCM) project funded by the Bayerisches Staatsministerium für Wirtschaft und Medien, Energie und Technologie (StMWi).

[1] Picture is taken from Flickr `https://flic.kr/p/Ch2gjk`

REFERENCES

Beckers, K. and S. Pape (2016a). A serious game for eliciting social engineering security requirements. In *Proceedings of the 24th IEEE International Conference on Requirements Engineering*, RE 16, pp. To Appear. IEEE Computer Society.

Beckers, K. and S. Pape (2016b). Theoretical foundation for: A serious game for social engineering. Technical report, Technical University Munich (TUM) and Goethe-University Frankfurt. http://pape.science/social-engineering/.

Csikszentmihalyi, M. (2000). *Beyond Boredom and Anxiety: Experiencing Flow in Work and Play* (25th Anniversary edition ed.). Jossey-Bass.

Denning, T., A. Lerner, A. Shostack, and T. Kohno (2013). Control-alt-hack: The design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, New York, NY, USA, pp. 915–928. ACM.

Gulati, R. (2003). The threat of social engineering and your defense against it. *SANS Reading Room*.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. Indianapolis: John Wiley & Sons.

Hadnagy, C. (2016). The social engineering infographic. Technical report, Social Engineer, Inc. http://www.social-engineer.org/social-engineering/social-engineering-infographic/.

Kruger, H. A. and W. D. Kearney (2006). A prototype for assessing information security awareness. *Comput. Secur. 25*(4), 289–296.

Mitnick, K. D. and W. L. Simon (2009). *The Art of Deception*. Wiley.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Systems Security 15*(5), 13–21.

Proofpoint (2016). The human factor report 2016. https://www.proofpoint.com/us/human-factor-report-2016.

Rheinberg, F., R. Vollmeyer, and S. Engeser (2016). Flow kurz skala. Technical report. http://www.psych.uni-potsdam.de/people/rheinberg/messverfahren/FKS-englisch.pdf.

Shostack, A. (2012). Elevation of privilege: Drawing developers into threat modeling. Technical report, Microsoft, Redmond, U.S. http://download.microsoft.com/download/F/A/E/FAE1434F-6D22-4581-9804-8B60C04354E4/EoP_Whitepaper.pdf.

Shostack, A. (2014). *Threat Modeling: Designing for Security* (1st ed.). John Wiley & Sons Inc.

Stajano, F. and P. Wilson (2011, March). Understanding scam victims: Seven principles for systems security. *Commun. ACM 54*(3), 70–75.

Williams, L., M. Gegick, and A. Meneely (2009). Protection poker: Structuring software security risk assessment and knowledge transfer. In *Proceedings of International Symposium on Engineering Secure Software and Systems*, pp. 122–134. Springer.

Williams, L., A. Meneely, and G. Shipley (2010, May). Protection poker: The new software security "game". *Security Privacy, IEEE 8*(3), 14–20.