A Serious Game for Eliciting Social Engineering Security Requirements

Kristian Beckers
Technische Universität München,
Germany
Email: beckersk@in.tum.de

Sebastian Pape
Goethe-University Frankfurt
Germany
Email: sebastian.pape@m-chair.de

***Index Terms*—security requirements elicitation, requirements prioritisation, threat analysis, gamification**

***Abstract*—Social engineering is the acquisition of information about computer systems by methods that deeply include non-technical means. While technical security of most critical systems is high, the systems remain vulnerable to attacks from social engineers. Social engineering is a technique that: (i) does not require any (advanced) technical tools, (ii) can be used by anyone, (iii) is cheap.**

Traditional security requirements elicitation approaches often focus on vulnerabilities in network or software systems. Few approaches even consider the exploitation of humans via social engineering and none of them elicits personal behaviours of individual employees. While the amount of social engineering attacks and the damage they cause rise every year, the security awareness of these attacks and their consideration during requirements elicitation remains negligible.

We propose to use a card game to elicit these requirements, which all employees of a company can play to understand the threat and document security requirements. The game considers the individual context of a company and presents underlying principles of human behaviour that social engineers exploit, as well as concrete attack patterns. We evaluated our approach with several groups of researchers, IT administrators, and professionals from industry.

I. Introduction

"The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you [...] What I found personally to be true was that it's easier to manipulate people rather than technology [...] Most of the time organizations overlook that human element."[1] These words from Kevin Mitnick spoken in a BBC interview were made over a decade ago and are still of utmost importance today. A Dimensional Research study[2] with 853 IT professionals from United States, United Kingdom, Canada, Australia, New Zealand, and Germany about social engineering in 2011 confirmed Mitnick's statement. It revealed that 48% of large companies and 32% of small companies fell victim to 25 or more social engineering attacks in the past two years. The average cost per incident was over $25 000. 30% of large companies even cited a per incident cost of over $100 000. The SANS institute released a white paper[3] with even more severe numbers about social engineering. It states that cyber attacks cost U.S. companies $266 million every year and that 80% of all attacks are caused by authorized users. These users are either disgruntled employees or non-employees that have established trust within a company.

Eliciting security requirements for human threats is essential to consider the right defense mechanisms for concerns of socio-technical systems (STS). This elicitation is difficult for security engineers, because these are trained to focus mainly on other aspects of STS such as business processes, software applications, and hardware components. Additionally, external security engineers would have to gather relevant domain knowledge to understand the company, e.g. learn about processes, policies, employees' capabilities and attitudes. A common theme in security requirements engineering is modeling aspects of STS. For example, Lamsweerde [1] investigates security requirements for software, Mouratidis [2] and Liu [3] analyze organizational security issues, and Herrmann [4] focuses on business processes. The work of Li [5] considers all aspects of STS in one holistic model. These approaches have in common that they often assume the security requirements are known by the stakeholders and have only to be made explicit via modeling. This leads to a gap in the security analysis if the stakeholders are not aware of social engineering threats. Some approaches use patterns to identify threats [6], [7], which is generally a good idea, but for social engineering difficult, since the personality traits of individual persons such as *writes passwords on post-it notes* have to be known and described in a model. That is currently not done in security requirements engineering.

Several approaches focus on the elicitation of security requirements in different ways. Houmb [8] uses the Common Criteria as a basis for identifying security concerns in software documentation, Herrmann [9] relies on business risks for eliciting security requirements. These approaches build on existing software and business documentation as a source for security requirements, which does not focus on the behavior of humans in a company that might be exploited by a software engineer. Several works propose to use brainstorming as a

[1] news.bbc.co.uk/2/hi/technology/2320121.stm

[2] http://docplayer.net/11092603-The-risk-of-social-engineering-on-information-security.html

[3] http://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232

source for security requirements, e.g., Ionita [10]. These may result in social engineering security requirements, but again only if the stakeholders come up with the idea of social engineering, which requires them to know about it beforehand.

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 designed for a primary purpose other than pure entertainment, e.g. education, awareness training, social change. Williams et al. [11], [12] introduced the protection poker game to prioritize risks in software engineering projects. Shostack [13], [14] from Microsoft presented his Elevation of Privileges (EoP) card game to practice threat analysis with software engineers. We believe a serious game is relevant for social engineering, as well. Furthermore, games are used as part of security awareness campaigns [15]. For example, Denning [16], [17] provides with Control-Alt-Hack a game to raise security awareness by letting players become white hat hackers. Control-Alt-Hack does not focus on threat analysis or security requirements elicitation, but rather places emphasis on awareness. Therefore, it is set in a fictional scenario. In addition, the players use attacks that are predefined on the cards and do not need to elicit attacks on their own. The reason is the aim of awareness, which limits the game to increasing its players' knowledge about the existence and potential harm of hacking attacks.

We believe that there is a major benefit from eliciting security requirements using employees of a company in such a game for social engineering. In contrast to security engineers, common employers have the benefit of knowing their daily routine well. Namely, they are aware of business processes and their contexts, and especially deviations from provisions. Additionally, they know about their (and their co-workers') security knowledge, attitudes towards security rules and policies, and past behavior. In short, the employees are unconsciously aware of the human vulnerabilities in a company.

We propose to use a game (see Figs. 1 and 2) to make these threats explicit, which lets them play the role of a social engineering attacker. The game provides the required information about human behavior patterns such as the herd principle (if everyone is doing it, I do it as well) and attack scenarios that social engineers use such as phishing.

In order to provide the validity of these principles and attack scenarios, we took all of them from scientific publications. The game enables employees to learn about social engineering, while practicing immediately. This immediate application of learned knowledge has proven to have lasting effects [18].

The game works as follows. Employees propose social engineering threats and the other players rate their validity based on their knowledge of the context, e.g. employee Anton would fall for a phishing mail only if he is under time pressure for a deadline. This leads to a ranking of the proposed threats. Afterwards the threats are the basis for security requirements that shall prevent them.

Currently companies focus on two options for addressing the social engineering problem.

Figure 1: The Cards of our Game

Firstly, companies can conduct *security awareness trainings* in which employees are told about the threat of social engineering. These trainings are often mandatory for employees and don't have a lasting effect[4]. As a cheaper variant, security awareness campaigns try to achieve the same goal, but face the same problems than trainings. In general, they are not well adapted to the employees' weaknesses.

Secondly, companies hire penetration testing companies that *attack* their clients and show weaknesses.These kind of penetrations tests are rarely done, because they come with a number of problems, e.g. a lot of effort needs to be invested beforehand to address legal issues [19]. At best, when those penetration tests are conducted, the tester finds flaws and companies can educate the affected employees. However, experiments have shown that these approaches are difficult, because humans are easily demotivated when confronted with the results [20].

We propose to solve this issue by playing our serious game for social engineering threat analysis. Our target audience consists of all employees of a company, security aware IT administrators and security engineers, as well as secretaries or sales persons. The reason why we even want security aware employees to play is, that these usually focus on technical threats and have currently little to no support for eliciting social engineering support.

The remainder of our paper is organized as follows. Section II reports on the goals of our project. Section III provides an overview of serious games in particular with regards to security and security requirements engineering approaches. Section IV describes the game and its design process. Sect. V reports on our evaluation of the game and shows resulting threats and security requirements. Section VI concludes and provides directions for future work.

II. Project Goals

A. Goals

As motivated by Sect. I our main goal is to provide structured means to elicit and prioritize social engineering security requirements. This includes:

[4]https://citadel-information.com/wp-content/uploads/2010/12/Beyond-Awareness-Training-Its-Time-to-Change-the-Culture-Stahl-0504.pdf

Figure 2: Our Serious Game for Social Engineering

- Considering a context specific to a company that shall be protected, which means considering personal traits of its employees, weaknesses in its processes, and lack of awareness or even misguided security attitudes and policies. If we do not provide essential support for **context-specific** threats the players run the risk to come up with generic and meaningless threats. This would be fine for raising awareness, but not for threat elicitation.
- Basing our game on **existing research**, which has been thoroughly evaluated by international researchers in the field of social engineering. We wanted to avoid bias by making up social engineering elements (behaviors and attack scenarios) by ourselves or external consultants and missing relevant fundamental elements.
- Keeping our game **simple** allows the players to focus on the threat analysis and spend as little effort as possible on learning and following the game's rules. This allows them to focus most of their cognitive powers on eliciting the threats.
- Making the game **entertaining** is of utmost importance. According to Klimmt [21, p. 256f] enjoyment during the game generates attention and interest. An external security engineer would need to understand the company (processes, policies, employees' capabilities and attitudes) and get domain knowledge in order to elicit threats. We believe it is easier and more cost-effective to train the people that know the context of their work really well in threat analysis. The highest danger of the participation of non security experts is the *looking out of the window*[5] effect, which describes the participants' boredom leads them to stop participating and spend their time looking out the window and thinking of other topics. Our aim is to avoid this effect by engaging the players in an enjoyable experience.

[5]This effect was introduced to the authors by Ketil Stølen.

B. Why a Game?

This section is mainly based on the argumentation of Denning [16] for their security awareness game. We extended Denning's argumentation with arguments from research on serious games. As a result, we believe that a serious game can fulfill our project goals. If designed properly, a serious game can be an appropriate tool for supporting context-specific threat analysis to different kinds of employees. In short:

- Games can be fun, which gets employees involved.
- Games provide a realm that encourages employees to be creative and try new ways of thinking
- Games are intended to be engaging and entertaining, which gets employees to play again and again.
- A game provides a realistic scenario, but the players do not need to fear consequences, because "playful action [...] is intentionally limited to a situational frame that blocks out further consequences of action results."(cf. Klimmt [21, p. 253]) Klimmt points out, that direct consequences are a reduction of complexity, because players do not even need to think about consequences. Another consequence is the accessibility of imagined contexts and activities; fantasy allows role-play in contexts that would not be feasible, appropriate or desirable otherwise. This mind-set exactly matches our aim to make players think like an attacker.

We could have designed this game as a computer game. Both formats have their benefits and limitations. We decided to design a physical tabletop game mainly, because the social setting of the game involves the physical presence of potential victims and the players are reminded of their vulnerabilities while playing. These victims or people that know them well can participate in the discussions about threats and may be reminded of their actual behavior by their presence. Furthermore, Denning's reasons apply in our case, as well.

- Physical games may be attractive to people who dislike computer games.
- Physical games require no hardware or digital resources, except for a table.
- Physical games allow to browse its components such as principles without playing.

C. Target Audience

When designing the game, we had to consider the trade-off between designing a very general and generic game and one specific for a certain target group. While a game appealing to as many people as possible may be broadly applicable, a more targeted version may benefit from domain knowledge and may be more helpful for the players. We decided to target the middle and design a game for employees without consideration of properties specific for certain industrial sectors.

a) Primary Audience: Our game addresses *company employees* that work with computers and information assets. In particular, we want to engage *security engineers* and *IT administrators* in social engineering threat analysis. We claim that these have initial security knowledge which makes it

easier for them to get introduced to the topic. On the other hand the human engagement necessary when dealing with social engineering is fairly new to many of these population and our game shall help with this task.

b) Secondary Audience: Persons in a company that work with information assets are the entire *Administration* staff. We welcome their engagement in the game in order to be motivated and encouraged to tackle social engineering. Ideally we mix this second audience with the first, so that knowledgeable security people can explain security concepts and procedures during the discussions of the game.

In the future, we plan to provide introductionary material and further examples to make the game appealing to a broader population.

III. Background and Related Work

We are not aware of a serious game for social engineering to elicit security requirements. We report on the following works relating to serious games in software planning and security engineering.

Serious games have demonstrated a significant potential in industrial education and training disciplines [22], [23], [24], given that organizations care for players' privacy and working atmosphere and especially do not use gaming data for appraisal or selection purposes, and clearly communicate this to employees [**?**].

In particular, games for IT security preparedness in the electricity industry in Norway [25] have helped to determine the right composition of response teams in terms of competencies. These exercises have the potential to optimize current emergency practices and they offer the possibility to evaluate new practices in a realistic setting.

The *planning poker* game [26], [27] provides a collaborative method for estimating efforts for software engineering. The players take turns to estimate the efforts of a task in the first round, discuss the reasoning for their estimations and estimate again in a second round. The results are well agreed upon resource estimates. The variant of planning poker for software security called *protection poker* [11], [12] provides a way for understanding and prioritizing risks. The game lets software engineers estimate the value of assets and the potential damage of threats towards these assets. The players suggest and discuss estimates for these values similar to planning poker. Finally the players quantify the risk for each asset and threat pair by multiplying their values. These pairs are placed in descending order by their risk values, which results in a prioritized list of risks. The game has also the benefit that software engineers have a simple way to discuss and learn about security concerns and measures. The authors found reasonable indication for this statement based on their empirical evaluations with academics [11] and practitioners [12]. In contrast to our work, this game does not use cards, but estimates on paper or boards and does not focus on social engineering. In the future, we can combine our games as follows. Our threats can be input for protection poker, which adds risk assessment to our threats.

Shostack [13], [14] argues as well that teaching software engineers about security is more favorable than using security engineers to conduct the threat analysis, because security engineers have to invest a lot of time to understand the work of the software engineers. This understanding is essential to discover vulnerabilities. In contrast, software engineers are more familiar with possible vulnerabilities of their systems, if they are taught about threat analysis. Thus, the author developed a card game called *Elevation of Privileges*. In contrast to the games described before it is a physical card game[6]. Each player draws several threats. In turns, the players then explain how these threats could manifest with regard to the software they are currently engineering. If a player can convince the other players that her threat is worth a bug investigation, a request for an additional feature or even a design change, she gets a point. The player with the most points by the end of the game wins. In contrast to our work, Shostack focuses on software security and software engineers as a target audience, while our game is for any kind of employees that work with information assets.

Games are also effective in security awareness campaigns [15], which aim to make people aware of IT security threats. The serious game Control-Alt-Hack from Denning [16], [17] is a tabletop game that lets players take the role of managers of a security penetration testing company. The company attacks its customers with their consent and the player that achieves the most successful attacks and earns subsequently the most money wins. The success of the attacks is decided by a roll of the dice. The players learn about existing attacks and the damage they can cause within the fictional setting. In contrast to our work, the game has a focus on awareness, and therefore no context-specific threats are elicited or security requirements documented.

The security cards[7] is a deck of cards that contains cards of the types impact on humans, adversary motives, adversary resources, and adversary methods. The aim of this game is to brainstorm about threats. In contrast to our work these cards do not come with a clear set of rules and are not based on literature, but are more vague. For example, an adversary's method is processes and asks the players to come up with a bureaucratic process for an attack. This level of abstraction provides less guidance than our card games.

Further available games are [d0x3d!][8] a tabletop game designed to raise awareness to network security terminology and attacker models. The card game *Exploit!*[9] is an entertainment game for security engineers. OWASP Cornucopia[10] trains threat modeling and risk assessment for software applications. However, none of these games addresses social engineering threat elicitation with employees.

[6]The Elevation of Privileges (EoP) Card Game: https://www.microsoft.com/en-us/SDL/adopt/eop.aspx

[7]The security cards: http://securitycards.cs.washington.edu

[8]The [d0x3d!] game: http://www.d0x3d.com

[9]Core Impact: Exploit! http://www.coresecurity.com

[10]Cornucopia https://www.owasp.org/index.php/OWASP_Cornucopia

Capture-the-Flag[11] games make the players compete in simulated security attacks. These have been extended to the realm of social engineering[12]. These competitions select social engineers that attack existing companies, but these are not employees of these companies and limit themselves to telephone based attacks. The companies are informed of the results, but these often do not volunteer to be attacked and as unwilling participants the positive impact these studies can have seem rather limited. In any case, Social Engineering Capture the Flag are more a kind of social penetration testing than threat elicitation. From the companies' perspective, they therefore come with the problems already mentioned in Sect. I.

IV. Designing the Game

We could not identify a game that provides structured context-specific threat analysis, is based on existing research, is simple and engaging (see Sect. III). Thus, we decided to create our own game mechanics and improved them over a number of feedback rounds. Our game on social engineering consists of three sections: *Preparation* the game considering the players' context, *Playing* the game and eliciting threats and *Debriefing* the players including prioritizing threats. Each of the sections may consist of several phases. In this Section, we present the game rules along with our design rationales.

Section 1: Preparation

1. Create an Overview Plan Provide an *overview plan* of the department by using the fire escape plan. This plan has to be augmented with the assets of the company, the people working in that department, and their locations, as well as communication channels e.g. VoIP, Email, etc (cf. Fig. 3). All players should be involved in the creation or have to check the plan for completeness.

Reasoning: We base this step on the fire escape plan of the department, because it is easily available since it often is publicly hung out to show escape routes. Additionally, the plan shows fire-extinguishers, fire alarm buttons, and escape ways, which may be used by the players in an attack. Lastly, the natural consequence of the players checking it for flaws is that they are familiar with it at the beginning of the game and further discussion in the game is focused on the attacks and not the setup.

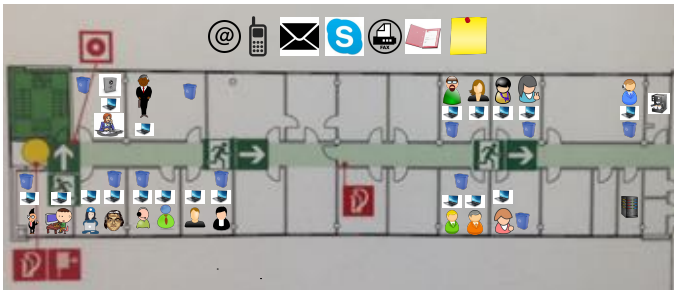

Figure 3: Overview Plan

[11]Capture the Flag: https://www.defcon.org/html/links/dc-ctf.html
[12]Social Engineering CTF: http://www.social-engineer.org/category/ctf/

Section 2: Playing

In the Playing section, the players take the role of the attacker. It consists of the following phases:

1. Draw Human Behavioral Pattern Card Each player draws a card from the deck of *human behavioral patterns* (principles). Users behaving according to one of the principles can be exploited by social engineers. One example for the patterns is the so-called *Need and Greed principle* that states "Your needs and desires make you vulnerable. Once hustlers know what you really want, they can easily manipulate you. "A sample card is shown in Fig. 4.

Reasoning: The human behavioral patterns are based on the work of Stajano and Wilson [28], who describe why attacks on scam victims may succeed. We extended the set of behavioral patterns[13] by patterns found in work on social engineering from Gulati [29] and Peltier [30].

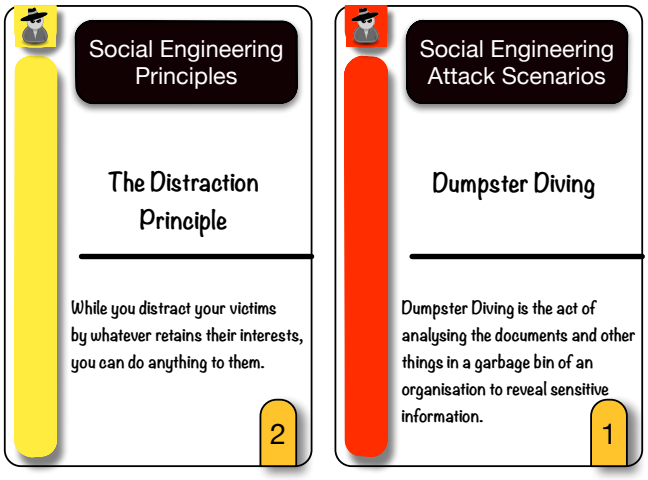

Figure 4: Principle (Left), Attack Technique (Right)

2. Draw Attack Scenario Cards The next step is that each player draws three cards from the deck of the *social engineering attack techniques* (scenarios). For example, reverse social engineering comprises creating a problem for the selected person and solving it for him. The gained trust is used to ask the victim for a favor. A sample card is shown in Fig. 4.

Reasoning: The used attack techniques are mostly based on the work of Krombholz et al. [31]. We also extended the set of attack techniques[14] adapted from the work of Gulati [29], Peltier [30], and Chitrey et al. [32]. Since most attacks are only related to a subset of the behavioral patterns in an appropriate manner, we allow the players to take three cards.

3. Choose Attacker Type Each player gets one *attacker type* card. The card has two sides shown in Fig. 5. One for an inside attacker, who is a well known member of the organization. And one for an outside attacker, who is unknown to the members of the organization.

[13]A full list of all human behavioral patterns along with the corresponding reference may be retrieved on http://pape.science/social-engineering/.
[14]A full list of all attack techniques along with the corresponding reference may be retrieved on http://pape.science/social-engineering/.

Reasoning: Insiders have already established trust in the organizations, which leads to an easier starting point for an attack. Outsiders have to establish trust in the organization first before conducting the attack. The players should think about what kind of attacker they are and plan their attack accordingly. For example, an insider might need to cover his tracks more carefully or pass the buck to co-workers while an outsider has to provide a reason for being in the building.

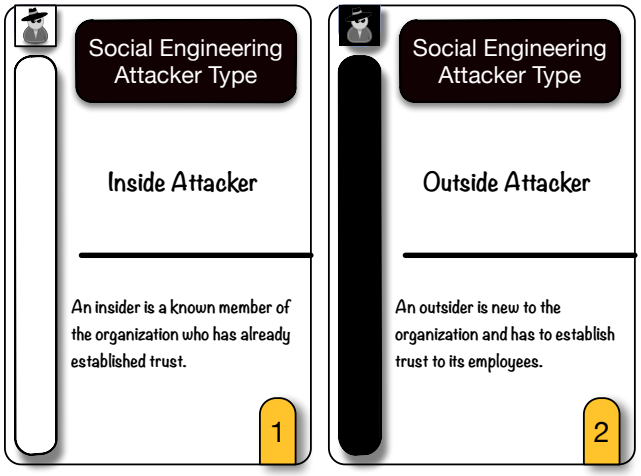

Figure 5: Attacker Card (Front- and Backside)

4. Brainstorming In the brainstorming phase the players take the role of the attacker. Each player thinks of how to conduct one of the three attacks to exploit the behavioral pattern of an employee. The exploit targets one person in the overview diagram and an asset. Moreover, the player has to choose if she is an insider or outsider of the organization. The players get five minutes to think about and elaborate their attacks.

Reasoning: We experimented with different time frames for the brainstorming in feedback sessions and discovered in 4 sessions (n=3,n=2,n=4,n=4) that players need on average between 4 to 5 minutes to elicit a threat. A too short time frame showed to annoy the players while too much time got them easily distracted.

Rounds of the game: Each player proposes an attack in the fashion explained below. This iterates until all persons iterated at least twice. We denote a *turn* as one player presenting an attack along with the discussion and getting points. A *round* consists of turns of all players. After each round, the players restock their cards. The brainstorming phase in the iterations may be shortened as needed by the players.

5. Attack The active player presents his attack to the group. Each attack consists of a principle, an attack scenario, an attacker, a victim, a communication channel and a targeted asset (c.f. Tab. I). Note that once a player has proposed an attack it is finalized and cannot be changed anymore by the player.

Reasoning: The players should finalize their attack, because otherwise the players could always adapt their attack to address any concerns that may arise and gain full points. While this has still lead to lively discussions, it showed that players were dissatisfied because the awarding of points did not reflect the players effort. As discussed in Sect. II-B it is important to retain the playful character of the players' actions.

6. Discussion The discussion starts with a feasibility reasoning of the proposed threat. The players discuss first, if the attack is feasible, in which case the player gets 2 points. If the player received help when describing the attack or the attack is plausible, but infeasible (e.g. because the attacked person has a special training to resists the described attack), the player gets 1 point. If the proposed attack is not plausible the turn ends immediately and the player gets no points.

In case the player received more than one point, a compliance discussion follows. *Principle:* If the attack described by the player is a perfect match, the player gets 2 points, if it matches only somehow, he gets 1 point. *Scenario:* If the attack described matches the presented attack technique card, the player scores 1 point. *Attacker:* Finally, the players discuss if the inside attacker (1 point) and outside attackers (2 points) card matches the attacker type in the proposed threat.

Reasoning: We first want to establish if the attack is intuitively working in the minds of the players or if reasonable doubts exist. If the doubts are so strong that no players believes this attack can work we have a punishment installed in the game (0 points and end of turn). Afterwards, we would like to reward the players to think about the behaviors and attack scenarios on their cards, as well as the different approaches of inside and outside attackers.

7. Improvements In addition, the other players can also propose improved versions of an attack and gain 2 points for a major improvement or 1 point for a minor improvement. The points are granted by the other players.

Reasoning: We want to get the other players variations of the threat in order to explore their variations. Any missing threat during a security analysis presents a risk that is not considered and subsequently not protected against.

Section 3: Debriefing

In the debriefing phase, the players reflect their attacks. They may be supported by the company's security personnel.

Prioritize Threats We propose the following activities: (1) identify the most relevant threats of social engineers in your organization (e.g. based on likelihood to succeed and damage they potentially cause), (2) try to figure out why some people were attacked more often and (maybe) others not at all, (3) analyze why some communication channels were used more often than others, and (4) determine which assets were attacked more often than others.

Reasoning We aim to foster discussions about how severe social engineering attacks can be for an organization and find out which are the main security concerns for social engineering respectively.

Document Security Requirements We use a similar approach than Misuse Cases [33] to map threats to security requirements that specify the underlying security problem.

Reasoning We want this step to be simple and based on some well established work. The misuse case fulfills that criteria.

V. Evaluation

A. Sampling

We evaluated the game in practical experiments at the University Frankfurt and the Technical University Munich. We played the game with 27 players that are full time employed and 3 senior researchers have participated in the game in the role of a game master. The distribution of the players is the following (see Fig. 6): 5 players are employed at the University Frankfurt, 19 at the Technical University Munich and 1 is employed at a telecommunications company. Among the players were 2 senior researchers, 19 researchers, 4 members of the IT administration staff, 1 secretary and 1 professor. In particular, the players held masters' degrees in computer science (18), business information systems (4), economics (1), and IT security (1). In addition, 3 players have a PhD in computer science, while 4 players do not have academic degrees (see Fig. 7). We did not use students in our evaluations, but scientific employees and members of the administrative staff. The reason for this is that the target audience of the game consists of company employees and we identified a sample set that reflects our target audience.

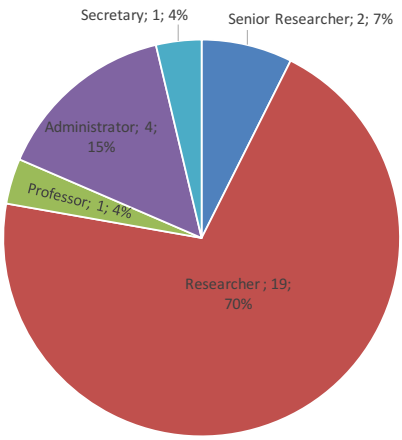

Figure 6: Player's Professions

B. Operation

We played the game in 7 individual sessions with 3 to 4 players and 1 game master in each round. In total, 49 turns of the game were played and 17 hours of playing time. Note that the time of playing the game varied depending on the length of the discussions of the feasibility of a proposed attack.

For the first two sessions we introduced social engineering and the rules of the game in a 15 minute presentation. Afterwards, we decided to shorten the introduction in order to get the players involved with the game sooner. Hence, sessions 3 to 7 are just introduced with a 5 minute introduction. We

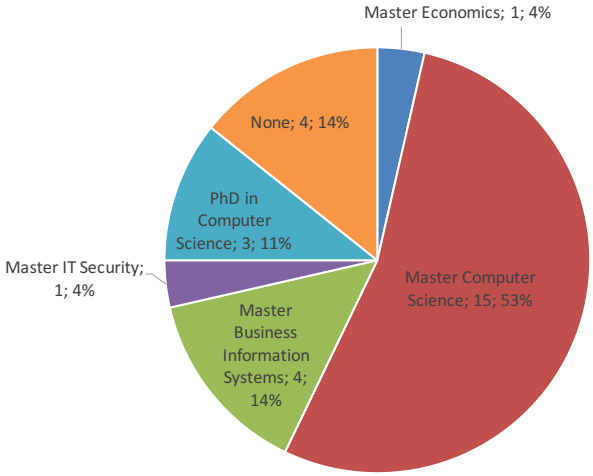

Figure 7: Player's Academic Degrees

devised a handout[15]. for the players in order to gain easy access to the rules at any time and handed it to them before starting a round. We played the game in a closed room so the players would not be distracted by any outside influence. Some of the players mentioned that our instructions on an A4 paper are too long for reading while playing. Therefore, we also provided a short version of the rules.

The game masters initiated the game with issuing the cards and just motivated the participants to elicit and discuss social engineering threats. They ensured that everyone's opinion is heard. The game masters did not voice any opinions during the discussions, they just documented the choices regarding points of the participants. Afterwards the game masters conducted the debriefing of the players of the game. The results of the debriefing is reported as part of the data analysis (c.f. Tab. I).

C. Data Analysis

We present the resulting statistics of the game in the following. We played 49 turns of the game resulting in 33 plausible attacks, 9 feasible attacks, and 7 non feasible attacks (see Fig. 8). Hence, the majority of the elicited attacks were plausible. Note that the following statistics focus only on the 42 plausible and feasible attacks. We exclude the non feasible attacks for the following analysis. We categorized the victims attacked in our threats to the following types: secretary, employee, and IT administrator (see Fig. 9). Our analysis revealed that employees are the most often attacked victims. We assumed before playing the game that this would be the secretaries, because they are assumed to be the weakest spot. The reason for this is that they have the least amount of university education and the most contact with people. Moreover, they are doorkeepers of the department heads and

[15]The handout is available at: http://pape.science/social-engineering/

Table I: Social Engineering Threats Elicited during our Evaluation

Nr.	Context Knowledge	Attack	Asset	Principle	Attack Scenario
1	Tim is seeking for attention and likes to be admired for his achievements.	A member of an intranet security discussion board invites Tim to participate in an honorary event and asks the Tim to log in with his credentials to the intranet side using a specific link.	Credentials	Distraction	Waterholing
2	Jim flies to the United States from Germany with Lufthansa and they just announced a strike. Jim is watching his email closely to get any information about delays quick and deal with them.	The attacker fakes a Lufthansa email with an updated travel itinerary and attaches some malware to this email. The malware would gain him access to the Jim's PC and all digital assets on it.	Notebook Data	Time Pressure	Mail Attachment
3	Bob is using Yahoo Mail, which forces him to re-enter his credentials after 2 weeks continuously being logged in.	Bob proposes to attack himself using the outlined weakness in Yahoo Mail. If an attacker would fake the popup, he would probably (re-)enter his credentials	Email Data	Ignorance and Carelessness	Popup Window
4	Steve always leaves his office door and computer unlocked. The cleaning guy is quite dominant when cleaning the rooms.	An attacker can just enter his office pretending to be a (new) cleaning guy, so he can just enter and send an email using his computer and open an attachment with a Trojan.	Notebook Data	Laziness	Support Staff
5	Robert's family is about to arrive in the city to celebrate his PhD submission. He also is printing his Phd-thesis at the moment. Robert gets a call from his family who arrives by train.	The attacker would be around and offer him to finish copying his dissertation. Due to Robert's stress with his dissertation and family arriving he would welcome help. The attacker would then steal data from his dissertation.	Dissertation	Trust Principle	Direct Approach
6	Claudia is a new employee and worried about her reputation. She is using the local WiFi access and the company is communicating with a chat tool.	The attacker would send her some links that turn out to be pornography in the chat tool, after that the attacker will call her and pretend to be a system administrator and pressure her to reveal confidential information for not letting anybody know about the pornography.	Confidential information	Trust Principle	Direct Approach
7	Bernhard needs a lot of computational power to run experiments. He does not have sufficient resources and a tight deadline to deliver results. He just ordered more IT resources.	The attacker spoofs the email of the IT administration and sends him an email pretending to be the administration. The email asks to open an email attachment that contains a new form he has to fill in if he wants to get the resources he previously ordered. The attachment contains a malware.	PC data	Need and Greet	Email Attachment
8	Jean has to work a lot with the financial administration due to project billing issues for a European research project she is working on.	The attacker pretends to be from the finance administration and gain her credentials for the website the European Project is used for billing. By telling that some issues need to be resolved and proposing to take care of them for her she would gladly give the attacker her credentials.	Credentials	Guilt (No points)	Direct Approach
9	Torben googles himself regularly to check his reputation in the web.	The attacker prepares a site with information about him and with exploits. The attackers would try to get it in the google ranking and wait for him to google himself. If he checks the results and notices the new page, he'll browse it.	PC data	Guilt (No points)	Direct Approach (No points)
10	Recently, there has been a bomb threat and the administration asked everyone to leave the building for "technical reasons". Further information was promised the next days.	Impersonate someone from the health department and claim that all people have to leave the building due to recently discovered asbestos or start a fake fire alarm to access the boss's office for a couple of minutes.	Data in Office	Fear of the Unknown	Third Party Authorization

often hold a lot of access privileges. However, this assumption turned out to be wrong. Moreover, we did not expect more than 10% of the attacks directed towards the IT administration, because these are supposedly the most well trained employees with regard to social engineering. Furthermore, we present the distribution of attacks towards employees in detail in Fig. 10 right. The blue employees are secretaries, the green ones are administrators and the red ones are scientific employees. The number following the name is the number of times that person was attacked. All of the names are pseudonyms for real people. The person that suffered the most attacks is Monja a secretary with overall 8 attacks. In contrast, all other victims suffered between 1 and 3 attacks.

The ratio between insider and outsider attackers is 22 outsider attacks to 20 insider attacks (see Fig. 8). We expected a large ratio of insider attacks, because these are easier to elicit, due to the fact that inside attackers have already established trust. In particular, the players can attack as themselves. However, the statistics show that these numbers are almost even and we could not reveal a significant preference for either attacker type.

Table II: From Threats to Requirements

Nr.	Threat	Security Requirement
1	A member of an intranet security discussion board invites Tim to participate in an honorary event and asks the boss to log in with his credentials to the intranet side using a specific link.	A security awareness training has to teach Tim and other employees to investigate links from unknown sources, even when under time pressure. These investigations can be delegated, e.g., to the IT security team.

We present an excerpt of the threats we elicited in our evaluation in Tab. I and show the domain knowledge these contain. The table outlines the drawn cards and targeted assets, as well. Note that even if these attacks are plausible, in some cases the players did not receive the points for principles or attacks, because her attack did not match the received cards.

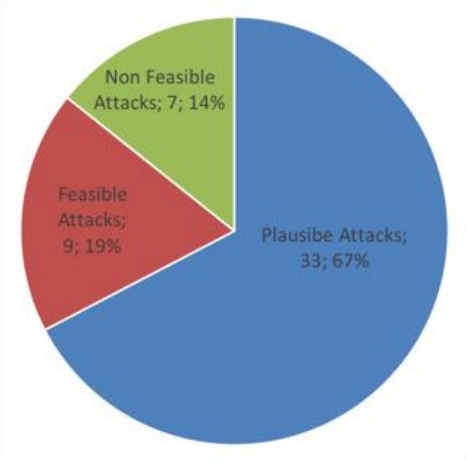

Figure 8: Attack Rating

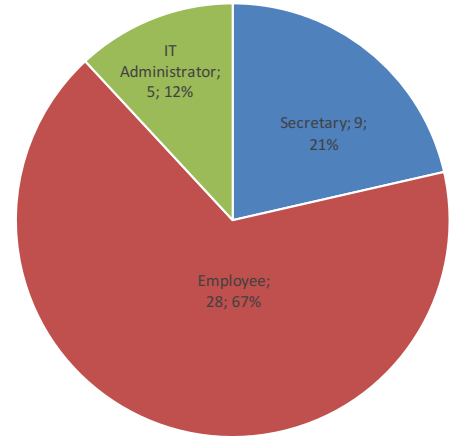

Figure 9: Victim Type

The final step of our approach is to formulate security requirements based on these threats. We provide an exemplary threat and requirement pair in Tab. II. The requirements shall contain a constructive procedure to support the possible victims in evading the elicited threats. In the future, we will look into how to do a reconciliation of multiple social engineering security requirements to derive an entire awareness training from it.

In addition, we deem it important that the employees understand that they will not be punished if they fell for a social engineering attack, but limit the damage in informing the security incident management team. The person that does this debriefing has to ensure that employees understand that they can resist this attack with proper training and motivate them to do so. The understanding of the social engineering attacker due to the precise attack presented should help employees to gain confidence that they can adopt a resistance strategy.

VI. Conclusion and Future Work

Social engineering attacks are a significant problem for IT security. Even for IT security professionals it is challenging to elicit security requirements for social engineering threats.

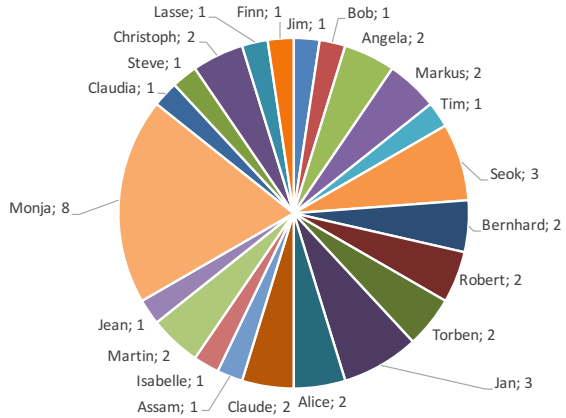

Figure 10: Victim Type Detail

Commonly, social engineering threat assessment involves penetration testers that execute attacks on their customers and report security requirements to them afterwards. This involves the deception of people and a possible violation of their privacy rights and provides only a small fraction of all attack vectors. We propose an alternative to these techniques that does not involve the lying to people, does not require external security consultants, carries less risk of privacy violations, and utilizes domain knowledge of the employees of these companies. These employees have due to their work experience in the company the most relevant information to assess social engineering vulnerabilities in themselves and their colleagues.

Our proposed solution utilizes a card game that employees of a company play to elicit social engineering threats and subsequent security requirements. These know the domain well and learn about social engineering in a structured way while playing the game. Security consultants are more familiar with social engineering, but they have to learn about the domain to elicit relevant context-specific threats. We argue that employees can be taught this knowledge with our game and at least contribute to the threat analysis and security requirements elicitation effort.

Our main contributions are listed in the following:

- Employees learn about different facets of social engineering acts e.g. how social engineering attacks are composed. They learn by applying the knowledge when becoming an attacker in the game. The learning and application of social engineering while having fun playing creates lasting knowledge on the subject.
- The domain knowledge of the players and in particular their observations during their daily work allows them to elicit context-specific attacks.
- The plausibility of the proposed attacks are rated by the employees, again by applying valuable insights of the domain in their argumentation. Hence, not plausible attacks in this specific context are eliminated quickly. It also leads to a prioritization of threats and their respective security requirements into plausible attacks and only feasible ones.

- The employees are warned about threats they may face in their daily lives and develop a sense of suspicion when being attacked. Threats being elicited with our game have domain specific information, which makes them realistic.

In the future, we are planning to create a context-independent version of the game that can be used without preparation in security awareness campaigns.

VII. 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 the Federal Ministry of Education and Research Germany (BMBF) via the project SIDATE (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).

References

[1] A. van Lamsweerde and E. Letier, "Handling obstacles in goal-oriented requirements engineering," *IEEE Trans. Softw. Eng.*, vol. 26, no. 10, pp. 978–1005, Oct. 2000. [Online]. Available: http://dx.doi.org/10.1109/32.879820

[2] H. Mouratidis and P. Giorgini, "Secure tropos: A security-oriented extension of the tropos methodology." *Journal of Autonomous Agents and Mult-Agent Systems*, 2005.

[3] L. Liu, E. Yu, and J. Mylopoulos, "Security and privacy requirements analysis within a social setting," in *Proceedings of the 11th IEEE International Conference on Requirements Engineering*, ser. RE '03. Washington, DC, USA: IEEE Computer Society, 2003, pp. 151–. [Online]. Available: http://dl.acm.org/citation.cfm?id=942807.943910

[4] P. Herrmann and G. Herrmann, "Security requirement analysis of business processes," *Electronic Commerce Research*, vol. 6, no. 3, pp. 305–335, 2006.

[5] T. Li and J. Horkoff, *Advanced Information Systems Engineering: 26th International Conference, CAiSE 2014, Thessaloniki, Greece, June 16-20, 2014. Proceedings*. Cham: Springer International Publishing, 2014, ch. Dealing with Security Requirements for Socio-Technical Systems: A Holistic Approach, pp. 285–300.

[6] T. Li, E. Paja, J. Mylopoulos, J. Horkoff, and K. Beckers, "Holistic security requirements analysis: An attacker's perspective," in *Requirements Engineering Conference (RE), 2015 IEEE 23rd International*, 2015, pp. 282–283.

[7] T. Li, J. Horkoff, E. Paja, K. Beckers, and J. Mylopoulos, *The Practice of Enterprise Modeling: 8th IFIP WG 8.1. Working Conference, PoEM 2015, Valencia, Spain, November 10-12, 2015, Proceedings*. Springer International Publishing, 2015, ch. Analyzing Attack Strategies Through Anti-goal Refinement, pp. 75–90.

[8] S. H. Houmb, S. Islam, E. Knauss, J. Jürjens, and K. Schneider, "Eliciting security requirements and tracing them to design: An integration of common criteria, heuristics, and umlsec," *Requir. Eng.*, vol. 15, no. 1, pp. 63–93, 2010.

[9] A. Herrmann, A. Morali, S. Etalle, and R. Wieringa, "Riskrep: Risk-based security requirements elicitation and prioritization," in *1st International Workshop on Alignment of Business Process and Security Modelling, ABPSM 2011*, ser. Lecture Notes in Business Information Processing. Berlin, Germany: Springer Verlag, October 2011, pp. 1–8. [Online]. Available: http://doc.utwente.nl/78045/

[10] D. Ionita, J. W. Bullee, and R. J. Wieringa, "Argumentation-based security requirements elicitation: The next round," in *Evolving Security and Privacy Requirements Engineering (ESPRE), 2014 IEEE 1st Workshop on*, Aug 2014, pp. 7–12.

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

[12] L. Williams, A. Meneely, and G. Shipley, "Protection poker: The new software security "game"," *Security Privacy, IEEE*, vol. 8, no. 3, pp. 14–20, May 2010.

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

[14] ——, "Elevation of privilege: Drawing developers into threat modeling," Microsoft, Redmond, U.S., Tech. Rep., 2012, http://download.microsoft.com/download/F/A/E/FAE1434F-6D22-4581-9804-8B60C04354E4/EoP_Whitepaper.pdf.

[15] M. Gondree, Z. N. J. Peterson, and T. Denning, "Security through play," *IEEE Security and Privacy*, vol. 11, no. 3, pp. 64–67, 2013.

[16] T. Denning, A. Lerner, A. Shostack, and T. Kohno, "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*, ser. CCS '13. ACM, 2013, pp. 915–928.

[17] T. Denning, T. Kohno, and A. Shostack, "Control-alt-hack™: A card game for computer security outreach and education (abstract only)," in *Proceeding of the 44th ACM Technical Symposium on Computer Science Education*, ser. SIGCSE '13. ACM, 2013, pp. 729–729.

[18] F. L. Greitzer, O. A. Kuchar, and K. Huston, "Cognitive science implications for enhancing training effectiveness in a serious gaming context," *J. Educ. Resour. Comput.*, vol. 7, no. 3, 2007.

[19] G. Watson, A. Mason, and R. Ackroyd, *Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense*. Syngress, 2011.

[20] T. Dimkov, A. van Cleeff, W. Pieters, and P. Hartel, "Two methodologies for physical penetration testing using social engineering," in *Proceedings of the 26th Annual Computer Security Applications Conference*, ser. ACSAC '10. ACM, 2010, pp. 399–408.

[21] C. Klimmt, "Serious games and social change: Why they (should) work," in *Serious games: Mechanisms and effects*, U. Ritterfeld, M. Cody, and P. Vorderer, Eds. Routledge, 2009.

[22] P. Petridis, K. Hadjicosta, V. S. Guang, I. Dunwell, T. Baines, A. Bigdeli, O. F. Bustinza, and V. Uren, "State-of-the-art in business games," *International Journal of Serious Games*, vol. 2, no. 1, pp. 55–69, 2015.

[23] J. Riedel and J. Hauge, "State of the art of serious games for business and industry," in *Proceedings of Concurrent Enterprising (ICE)*, 2011, pp. 1–8.

[24] C. E. Catalano, A. M. Luccini, and M. Mortara, "Best practices for an effective design and evaluation of serious games," *International Journal of Serious Games*, vol. 1, no. 1, pp. 12–25, 2014.

[25] M. Line and N. Moe, "Understanding collaborative challenges in it security preparedness exercises," in *ICT Systems Security and Privacy Protection*, ser. IFIP Advances in Information and Communication Technology, H. Federrath and D. Gollmann, Eds. Springer International Publishing, 2015, vol. 455, pp. 311–324. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-18467-8_21

[26] J. Grenning, "Planning poker or how to avoid analysis paralysis while release planning," Object Mentor, Tech. Rep., 2002, https://renaissancesoftware.net/files/articles/PlanningPoker-v1.1.pdf.

[27] K. Molokken-Ostvold and N. Haugen, "Combining estimates with planning poker–an empirical study," in *Software Engineering Conference, 2007. ASWEC 2007. 18th Australian*, April 2007, pp. 349–358.

[28] F. Stajano and P. Wilson, "Understanding scam victims: Seven principles for systems security," *Commun. ACM*, vol. 54, no. 3, pp. 70–75, Mar. 2011. [Online]. Available: http://doi.acm.org/10.1145/1897852.1897872

[29] R. Gulati, "The threat of social engineering and your defense against it," *SANS Reading Room*, 2003.

[30] T. R. Peltier, "Social engineering: Concepts and solutions," *Information Systems Security*, vol. 15, no. 5, pp. 13–21, 2006.

[31] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Social engineering attacks on the knowledge worker," in *Proceedings of Security of Information and Networks*, ser. SIN '13. ACM, 2013, pp. 28–35.

[32] A. Chitrey, D. Singh, and V. Singh, "A comprehensive study of social engineering based attacks in india to develop a conceptual model," *International Journal of Information and Network Security (IJINS)*, vol. 1, no. 2, pp. 45–53, 2012.

[33] G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," *Requir. Eng.*, vol. 10, no. 1, pp. 34–44, 2005.