PROTECT – An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks

Ludger Goeke[1], Alejandro Quintanar[1], Kristian Beckers[1], and Sebastian Pape[1,2](✉)[0000−0002−0893−7856]

[1] Social Engineering Academy (SEA) GmbH
Eschersheimer Landstrasse 42, 60322 Frankfurt am Main, Germany
[2] Goethe University Frankfurt, Faculty of Economics and Business Administration
Theodor-W.-Adorno-Platz 4, 60323 Frankfurt am Main, Germany

Abstract. Social engineering is the clever manipulation of human trust. While most security protection focuses on technical aspects, organisations remain vulnerable to social engineers. Approaches employed in social engineering do not differ significantly from the ones used in common fraud. This implies defence mechanisms against the fraud are useful to prevent social engineering, as well. We tackle this problem using and enhancing an existing online serious game to train employees to use defence mechanisms of social psychology. The game has shown promising tendencies towards raising awareness for social engineering in an entertaining way. Training is highly effective when it is adapted to the players context. Our contribution focuses on enhancing the game with highly configurable game settings and content to allow the adaption to the player's context as well as the integration into training platforms. We discuss the resulting game with practitioners in the field of security awareness to gather some qualitative feedback.

Keywords: security controls · social psychology · serious games · fraud prevention · security training

1 Introduction

Kevin Mitnick a most famous social engineer was interviewed over 15 years ago and stated the following. "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." [3]. Today this is as true as it was back than as various current studies confirm [15,6].

Serious games have established a reputation for getting employees of companies involved in security activities in an enjoyable and sustainable way. Moreover, serious games are designed for a primary purpose other than pure entertainment, e.g. education, awareness training or social change, but they preserve a playful

character. Williams et al. [20] introduced the protection poker game to prioritise risks in software engineering projects. Shostack [18] from Microsoft presented his Elevation of Privileges card game to practice threat analysis with software engineers. Furthermore, games are used as part of security awareness campaigns [8] and particularly as a part of social engineering threat analysis [4].

Another game called *PERSUADED* specifically trains people to withstand social engineering attacks [1]. The game works as follows. Employees get confronted with a possible social engineering threat and have to select a defence mechanism. This correct defence mechanism is a pattern of behaviour ensuring a secure outcome. For example, an employee gets a phishing mail and is asked to open its attachment. Afterwards the player selects a countermeasure: "Do not open the email and inform the information security department immediately". The player gets immediate feedback whether the chosen defence is correct. In this paper, we describe how we built on the concept of PERSUADED and developed a new family of games called *PROTECT*.

Our contribution in this paper is the serious game PROTECT, which entails the following novelties:

- The game contains new scenarios for automated shipping and electronic cancer register domains
- The game can be configured to serve various game settings to allow a progression between difficulty levels and various other challenges to keep the players playing.
- A discussion with five security practitioners to assess the potential of the game for security trainings.

Our paper is organised as follows. Section 2 presents background and related work, while Section 3 contains the design methodology applied for creating our game. Section 4 describes the serious game PROTECT in detail. Section 5 documents the feedback for the game from practitioners and Section 6 concludes.

2 Background and Related Work

As security is usually a secondary task, computer security training has often been perceived to be an uninteresting enforcement to users and managers. The approach of developing serious games has therefore been adopted to provide knowledge and training in that field.

CyberCIEGE is a role playing video game, where a player acts as an information security decision maker in an enterprise. Players' main responsibilities are to minimize the risk to the enterprise while allowing users to accomplish their goals. Similar to Persuaded, the game offers a simulation of the reality particularly portraying the need to maintain the balance between productivity and security. As decision makers, players get to make choices concerning users (i.e. How extensive will background checks be?), computers (i.e. How will computers be networked?) and physical security (i.e. Who is allowed to enter a zone?) while monitoring the consequences of their choices. When compared to Persuaded, we

recognized CyberCIEGE offered several advantages common to those offered by Persuaded. For instance, players are in a defensive mode and they get to make decisions and experience their consequences. CyberCIEGE even incorporates assets and resources in the game, which is a missing element in Protect. On the other hand, the game requires longer time to learn and to play [10].

PlayingSafe is a serious game in the domain of social engineering. It consists of multiple choice questions which are wrapped in typical mechanics of a board game. Since questions provided are exclusive to social engineering, the game is very similar to ours. The main difference lies however in the focus in the topic of social engineering. PlayingSafe asks questions in the fields of Phishing, advanced fee fraud, spam and others, being a category that covers less common attacks. Our game on the other hand covers a broader field without offering depth in each topic. Additionally, our game incorporates strategy favouring the entertainment element, in order to enhance the game experience the game provides [13].

SEAG is a serious game designed to raise awareness of social engineering. The game utilizes levels that tackle different cognitive aspects and hence provide an effective learning experience. The first level consists of quiz-like questions to build a knowledge base for the players. The second level is a match game where players have to match social engineering terms with respective pictures. Finally, the players are presented real life scenarios to analyse pertaining to threat. This simulation of real life application of the learnt lesson should test players ability to detect attacks- an approach very similar to inoculation [14]. Due to the construction with the different levels, the game seems to be more suitable for a one-time approach. In contrast, our game is based on one basic principle, but the configuration allows to raise the game's difficulty.

HATCH is a serious game for teaching employees about social engineering attacks [4]. The employees are guided by the game to elicit social engineering threats for their context. An extension of the game provides various scenarios e.g. for energy providers and personas to allow players to understand attacks of other contexts [5]. HATCH is a physical table top game that requires at least three players and a game master. Our game does not need a game master, and thus can be played by individual players at any time alone.

3 Methodology

PROTECT is based on the game concept of PERSUADED [1]. In this paper, Aladawy et al. discuss design goals and game concepts for a serious card game for the sensitization of people against social engineering attacks. To evaluate PERSUADED, a prototype implementation of the game has been developed.

It realizes the following improvements:

In this section, we describe the concepts for building PROTECT.

3.1 New Implementation with Enhanced Configuration

PROTECT is a complete new implementation of the design goals and game concepts of PERSUADED. While taking the findings from the case study into

account, the focus was on the configuration of the game. By offering a lot of configuration options, i.e. for the game play, PROTECT can be seen as a family of games with PERSUADED just being a specific member of the game family. The aim is to allow an easy adaption to specific scenarios as well as to the player's skills. This can be particularly important if an employee changes the department and faces new threats in his/her new department.

By making the configuration options accessible via an application programming interface (API), PROTECT can not only serve as a stand-alone application but also be easily embedded into a training platform. In this case a training platform could control the difficulty of the game by changing the game configuration depending on the player's achievement in previous games. It would also be possible that the external training platform considers various other inputs such as the player's reaction to phishing mails, the results from other games or trainings.

In particular, we implemented an additional algorithm for the appearance of attacks in the game to make it easier for beginners to get started in the game. We introduced new cards that can defend any attack (jokers). We provided new algorithms for handling attacks which are not defended correctly and a special treatment for attacks that have not been defended correctly in previous games. The corresponding configuration parameters can be changed independently, allowing a number of (slightly) different games. The different configuration options are explained in detail in Sect. 4.2.

3.2 Game Concept

As for PERSUADED, the scientific foundation of this game are findings from Schaab et al. [16,17]. The authors analysed social psychology methods of training against persuasion and mapped them to trainings in IT security. One identified gap was the lack of using *inoculation*, the repeated confrontation of people with a challenging situation in order to trigger an appropriate response. In particular, inoculation is incorporated into the game mechanics to trigger resistance to social engineering attacks through exposing people to realistic attack scenarios. In order to provide the validity of the attack scenarios, we took all of them from scientific publications [19,15,11,7,2,12]. The game enables employees to learn about social engineering, while practising simultaneously. This immediate application of learned knowledge has proven to have lasting effects [9]. The enhanced configuration allows to adapt the game better to the player's needs. This is not only important to keep players motivated but also to adapt the game in a way that fits to the concept of inoculation. In versions for beginners the player's focus is mainly on matching different threats with the correct defences. In the more challenging versions for advanced players in order to be successful, the player is forced to think ahead. As a consequence, matching the different threats with the correct defences is still necessary but happens more unconsciously.

4 PROTECT

PROTECT is a serious card game that implements a training for the subject of social engineering. Its primary goal is the inoculation of people against social engineering attacks. This inoculation shall be achieved by confronting people repeatedly with social engineering scenarios in order to trigger an appropriate response.

PROTECT is implemented as an online game.

This chapter is divided into the following subsections:

- Section 4.1 describes game concepts and game mechanisms of PROTECT.
- Section 4.2 considers the configuration of PROTECT. In that respect, the configuration options regarding to (a) card decks, (b) instantiations of PROTECT and (c) properties for a game of PROTECT are discussed.
- Section 4.3 considers the implementation of PROTECT. It comprises the Graphical User Interface of PROTECT and its future provision as a web service.

4.1 Game Concepts and Game Mechanisms

This section considers the game concepts and mechanisms of PROTECT.

It is designed to achieve the following goals:

1. increasing awareness for social engineering,
2. training resistance to persuasion and
3. addressing the general population.

Regarding its main game concepts, PROTECT is designed as a single player card game that realizes a patience and solitaire game approach. As usual with this type of card games, the cards can be contained in the card deck or on the player's hand. In every turn of the game, a player can either draw a card from the deck or play a card from his/her hand. The implementation of these easy rules by PROTECT keep the complexity of the game low. This leads to a quite low initial barrier for playing the game and a focus on the actual content of teaching. Because the deck of cards is always shuffled before a game starts, each game is different from the previous game(s) (cf. [1], chap. 3, p. 5). This fact shall motivate players to play the game repetitively. The solitary approach enables players to play the game at any time, independently from other persons.

During a game of PROTECT, a player is confronted with different social engineering attacks. The task of the player is to select an appropriate defense mechanism for an attack. In this context, a defense mechanism represents a pattern of behaviour that prevents a successful conduct of a social engineering attack (cf. [1], chap. 1, p. 2). For the implementation of this game concept, PROTECT provides the following types of cards:

1. *Attack cards* represent scenarios for social engineering attacks in textual form.

2. *Defense cards* describe a pattern of behaviour for preventing the success of a certain attack. For each Attack card exists one corresponding Defense card. The contents of Defense cards are also represented in textual form.
3. *See The Future cards* allow the player to take a look on the three upper cards on the top of the card deck.
4. *Skip turn cards* allow the player to skip the top card of the deck and put this card to the bottom of the deck. It is only allowed to play a Skip turn card at the beginning of a turn when the top card of the deck is still hidden (cf. [1], Chap. 1, p. 4).
5. *Joker cards* are wildcards that can be selected by the player as a defence mechanism for every Attack card.

At the beginning of a game all cards are contained in the shuffled card deck. The game starts when the player draws the first card from the deck.

In the following, the game mechanisms of PROTECT are described.

At the beginning of a turn, a player can perform ONE of the following actions:

1. Draw a card from the top of the card deck.
2. Playing a See the future card or Skip turn card if such a card is on the players hand.

Any drawn card that is NOT an Attack card, is put to the hand of the player. After that, the turn is over.

When an Attack card has been drawn, the player has to select the appropriate Defense card. If he/she

1. selects the correct Defense card, the score is increased.
2. selects an incorrect Defense card, the score is decreased and the player loses a life.
3. has no Defense card on the hand, a life is lost.

A player can also play a Joker card to defend every Attack card. In this case, the score is also increased. By playing Joker cards, players can achieve a good score, even if they do not know the appropriate defenses for some attacks. This shall keep up the motivation of the players high, to play the game repeatedly.

When the card deck is empty, the game is won. The game is lost if

1. the game time is up before finishing the deck or
2. a player has lost all his/her lives.

The following description considers the special function of See the future and Skip turn cards. As previously mentioned, it may be the case that a player has no appropriate Defense card or no Defense card at all on the hand to defend a drawn Attack card. If the player's hand does also not include a Joker card, he/she has no direct chance to prevent the loss of a life. This fact shall encourage the player to use See the future and Skip turn cards in the following way.

The player can play a See the future card to peek the upper three cards on top of the card deck. If these cards include any Attack cards, he/she can check if the appropriate Defense cards are

– on his/her hand or
– contained in the future cards itself at the right position.

If the future cards should contain any Attack cards for which no corresponding Defense card is available, the player can remember the order of these Attack cards and play a Skip turn card to skip such an Attack card when it is on the top of the deck. In this way, the loss of a life can be prevented. The provision of this game strategy increases the learning effect because the player studies the content of any Attack cards included in the future cards more carefully. This also applies for the content of the current Defense cards on his/her hand. Furthermore, he/she matches Attack cards partly against defense mechanisms that are not represented by Defense cards on the players hand.

The provision of the strategy, mentioned before, requires an increased understanding of the game from the player. Additionally, it has a random factor because of the random order of the cards in the deck.

The study of [1] has shown that a considerable amount of players rated the above mentioned concept for the appearance of Attack cards on the top of the deck, as negative. Thus, PROTECT provides additionally a further concept for the appearance of Attack cards on the top of the deck. The implementation of this concept ensures that only such Attack cards can appear on the top of the deck for which an appropriate Defense card is currently on the player's hand. In this scenario the player can use the See the future cards and Skip turn cards to skip Attack cards for which he/she is not able to identify the appropriate Defense card on the hand. Because the additional concept for the appearance of Attack cards make the playing of PROTECT easier it shall be used for players on the beginner level.

PROTECT also provides two different concepts for the handling of Attack cards that have been solved incorrectly. In that regard, such an Attack card is

1. removed from the game or
2. is put back to the bottom of the card deck.

The second alternative represents the more easier variant because the player gets more chances to solve an attack correctly. Compared to the first variant, the player could still reach a good score, even with some incorrect solutions of attacks.

Example Scenario We have extended the game PROTECT with various real scenarios from the EU project Threat Arrest[3]. One of these scenarios concerns automatic shipping. Digitalisation has increased the use of industrial control systems in the shipping domain. The increased use of computers and their interface exposes the systems that control vital systems and steer the ship itself to the risk of cyberattacks. The captain and crew are on their ship, while a back office provides IT-support. We elicited possible attacks that could be mitigated with awareness training such as the following. The crew is in contact with the back

[3] Threat Arrest homepage: https://www.threat-arrest.eu

office on land in some intervals. If there is a problem with the onboard computer system the back office provides advice for maintenance to the crew. A social engineer pretends to be a back office employee and asks them to provide their credentials for maintenance. Another possible scenario would be that the crew is in ports all over the world. Maintenance is done on ports during stays outside of the home harbour. A social engineer pretends to be a maintenance worker and distributes usb sticks on the harbour with the hope that one of the crews picks one up and connects it to the computer system of the ship. We elicited totally over 20 plausible attacks for the game PROTECT.

4.2 Configuration Options

In this Section the options for the configuration of PROTECT are discussed. This discussion considers the following configuration aspects:

1. Configurations of card decks
2. Configurations during an instantiation of PROTECT
3. Internal configuration parameters of PROTECT

Configuration of Card Decks Within PROTECT, the content of the cards of a deck are defined in a JSON format. Each card is defined by a single JSON file. The graphical representation of a drawn card in the GUI is generated on the fly during a game, based on the content of the corresponding JSON file. The definition of cards based on JSON files enables easy and fast

- creations of new card decks and
- modifications of existing card decks

to cover more specific social engineering scenarios.

Each card deck in PROTECT is identified by an unique identifier. These identifiers are used to configure which card deck shall be played within an instantiation of PROTECT (see Section 4.2).

Standard Card Decks The standard card deck of PROTECT contains pairs of Attack and Defense cards for typical social engineering scenarios. It includes the following types off attacks (cf. [1], chap. 1, p. 4):

- baiting,
- phishing,
- tailgating
- mail attachment,
- physical impersonation,
- virtual impersonation,
- voice of Authority and
- popup window

Additionally, the standard card deck contains action cards in form of Joker, See the future and Skip turn cards. The number of action cards of each type in the card deck can be configured when PROTECT is instantiated. (see 4.2).

Adapted Card Decks The game PROTECT can be also used to verify that a company's security policy is understood and followed by its employees. This works by describing the possible attacks against a company that the rules of the policies try to prevent. For example, the policy might contain a rule to shredder all confidential documents. We provide a card in which a person takes the shredder for maintenance and tells the staff that in the absence of the shredder they should throw the documents in the regular trash bin and that is not necessary to use the shredder on the next floor. The right behaviour would be to object and use the other shredder and inform the security staff of this incident.

Instantiation Parameters PROTECT provides the hand over of information that is necessary for a game, during its instantiation. This information is represented by so-called *instantiation parameters* that are listed in Table 1.

The instantiation parameters *player ID* and *player name* provide information about the player of the game. The time that a game can take the longest is represented by the parameter *game time*. Because of their logical connection the instantiation parameters *card deck ID* and *difficulty level* shall be considered in more detail. The *card deck ID* and *difficulty level* enable the definition which card deck shall be played with which level of difficulty. Within PROTECT, a value for a difficulty level is mapped to a certain configuration of PROTECT regarding the selected card deck. This means, that a level of difficulty results from the particular values of the configuration parameters. These configuration parameters are specified in Table 2.

The parameter *special practice* defines if Attack cards that have been solved incorrectly in previous rounds of the game and there corresponding Defense cards shall be included multiple times in the card deck. If this is the case, the number of occurrences for such pairs of cards is defined by the appropriate configuration parameter (see Table 2).

Table 1: Instantiation parameters of PROTECT

Parameter	**Description**
player ID	Unique identifier of the player
player name	Name of the player
game time	Game time in minutes
card deck ID	Unique identifier of the card deck that shall be played.
difficulty level	Level of difficulty with which the game shall be played. The value of the difficulty level corresponds to a certain internal configuration of PROTECT.
special practice	Defines if Attack cards that have been solved incorrectly in previous games of PROTECT and the appropriate Defense cards shall occur multiple times in the card deck.

Internal Configuration Parameters *Internal configuration parameters* enable a configuration of properties for a game of PROTECT. The different internal configuration parameters are described in Table 2. A set of internal configuration parameters with the appropriate value is contained in a *configuration*. Configurations specify certain levels of difficulty for a game of PROTECT by the values of their parameters. For example, the level of difficulty decreases

- the more Joker cards a card deck includes,
- the more lives a player has,
- when only such Attack cards can be drawn for which the corresponding Defense card is on the player's hand,
- when incorrectly solved Attack cards are put back into the card deck and
- when the score can not have a value less than zero.

A configuration is associated to a certain difficulty level for a play of PROTECT with a particular card deck. The information according to the card deck and difficulty level are passed during the instantiation of PROTECT (see Table 1).

Table 2: Internal configuration parameters of PROTECT

Parameter	**Description**
number of lives	Defines the numbers of lives that a player has.
number Joker cards	Defines the number of Joker cards in the card deck.
number See the future cards	Specifies the number of See the future cards in the card deck.
number Skip turn cards	Defines the number of Skip turn cards in the card deck.
score increase	Defines the number of points added to the score when the CORRECT Defense card or a Joker card has been selected for an Attack card.
score decrease	Defines the number of points removed from the score when an INCORRECT Defense card has been selected for an Attack card.
range of score	Specifies if the score can be less than zero or if the lowest score is zero.
appearance of Attack cards	Defines if (a) ANY Attack card can appear on the top of the deck, even if the corresponding Defense card is not on the hand of the player. (b) ONLY those Attack cards can appear on the top of the card deck for which the corresponding Defense card is on the player's hand.
handling of incorrectly solved Attack cards	Specifies if an Attack card that has been solved incorrectly is (a) put back to the bottom of the card deck or (b) removed from the game.

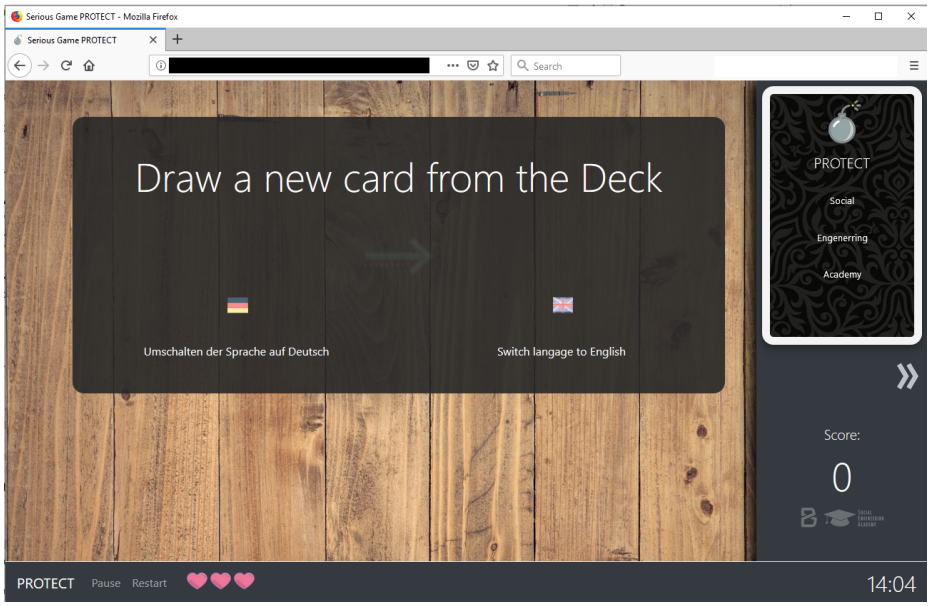


Fig. 1: GUI of PROTECT at the beginning of a game

4.3 Implementation

This Section discusses the implementation of game concepts and mechanisms that are described in Section 4.1 by PROTECT. The discussion considers the Graphical User Interface of PROTECT and a concept for its future provision as a web service.

Graphical User Interface The Graphical User Interface (GUI) of PROTECT is executed in a web browser. It is implemented in JavaScript by using the JavaScript library *jQuery* and the framework *Bootstrap*. The GUI is especially designed to be displayed on mobile devices. Nonetheless, it can be displayed on PC monitors and laptop screens without any problems.

The Figure 1 shows an execution of the PROTECT GUI in a web browser at the beginning of a game. The dialog for changing the language of the game is displayed. The card deck, including the Attack, Defense and action cards (e.g See the future cards), is positioned in the top right corner. It is shuffled automatically before each game. A player can draw a card by double-clicking on the card deck. The game score and the remaining game time are represented in the bottom right corner. It is also possible to pause a game with help of the *Pause*-button in the bottom left corner of the GUI. A game can also be cancelled and restarted. The corresponding *Restart*-button is positioned next to the *Pause*-button. The remaining lives of a player during a game are displayed by the pink heart symbols.

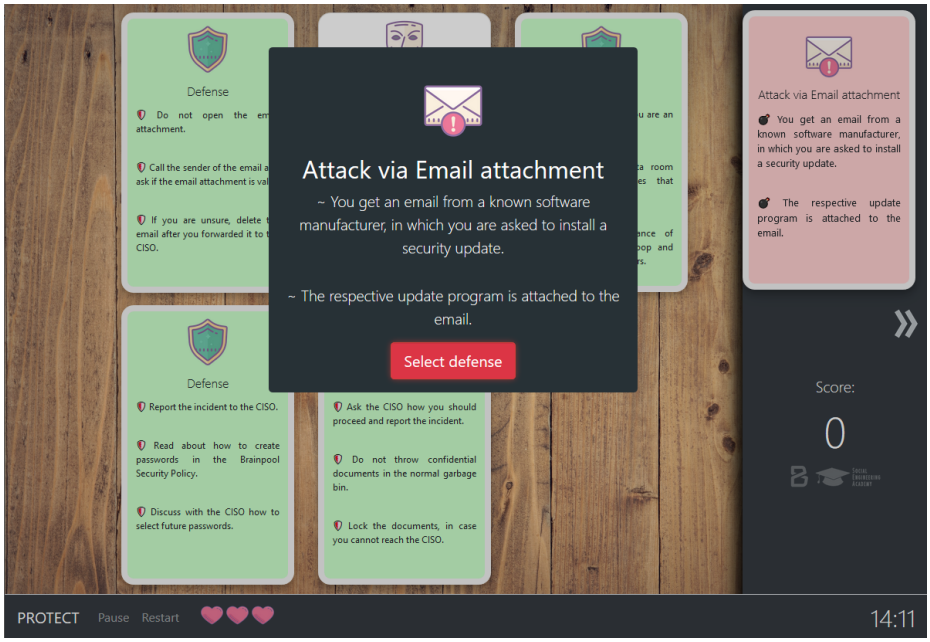
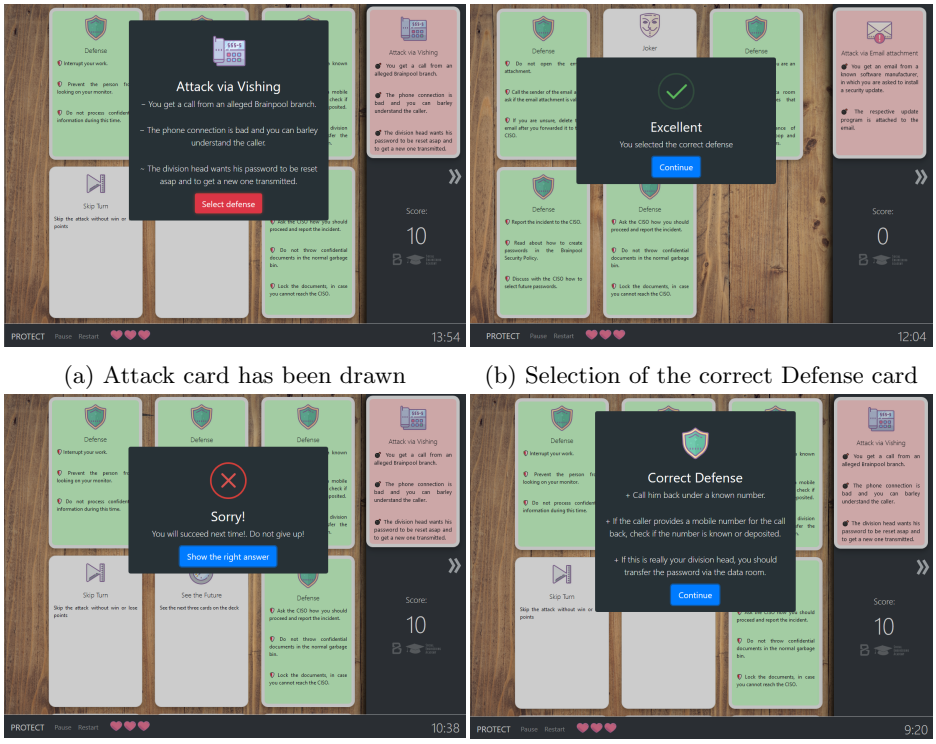


Fig. 2: Dialog after an Attack card has been drawn

The GUI supports the player in the game flow with appropriate dialogs. For example, the dialog in Figure 2 is shown after the player has drawn an Attack card. It requests the player to select a defense card after clicking on the *Select defense*-button. The Figure 3b displays the dialog after the selection of the correct Defense card. The game continues, after the player has pressed the *Continue*-button.

For example, the dialog in Figure 3a is shown after the player has drawn an Attack card. It requests the player to select a defense card after clicking on the *Select defense*-button. The Figure 3c displays the dialog after the selection of an incorrect Defense card. When the player clicks on the *Show the right answer*-button, the subsequent dialog represents the correct defense mechanism for the drawn Attack card (see Figure 3d). The game continues, after the player has pressed the *Continue*-button.



(a) Attack card has been drawn

(b) Selection of the correct Defense card

(c) Selection of an incorrect defense card

(d) Correct defense mechanism

Fig. 3: Different Dialogs within the Game

Provision of PROTECT as a Web Service The content of this section describes a concept for the provision of PROTECT as a web service. This type of provision has the following advantages:

1. Companies that want to use PROTECT for training their employees do not need to set up an own infrastructure for the deployment of PROTECT.
2. PROTECT can be integrated easily into other training platforms. This is achieved by the use of standardized application protocols that enable a loose coupling between different systems. Such an approach will be realized within the research project *Threat-Arrest*[4], where PROTECT will be integrated into the *Threat-Arrest training platform*.

PROTECT shall be provided as a cloud computing service in form of *Software as a Service (SaaS)*. For the deployment of PROTECT, an appropriate cloud infrastructure, deployment environment and database shall be used in form of cloud services. The usage of these services shall be supplied by a third party cloud service provider.

[4] https://www.threat-arrest.eu/

The architecture of the PROTECT web service is represented in Figure 4 in an abstract way. It shows that the PROTECT web service will use

- a deployment environment for the deployment of PROTECT and
- a data base service for storing data that is related to played games of PROTECT.

The selection of a certain deployment environment (e.g. virtual server, container service) is currently in the state of development.

The external functionality of the PROTECT web service is provided via a REST API (see Figure 4). A client can use a certain function by sending the appropriate HTTP request to the PROTECT web service. The web service sends the result of the function back to the client via an HTTP response. In the following, the basic functionality of the PROTECT REST API will be considered:

1. Instantiation of PROTECT with the specified instantiation parameters (see Table 1). The PROTECT web service returns the created PROTECT instance to the client.
2. Query of results regarding to games of PROTECT. The set of the returned results can be defined by filter parameters that are contained in the content data of the appropriate HTTP requests.

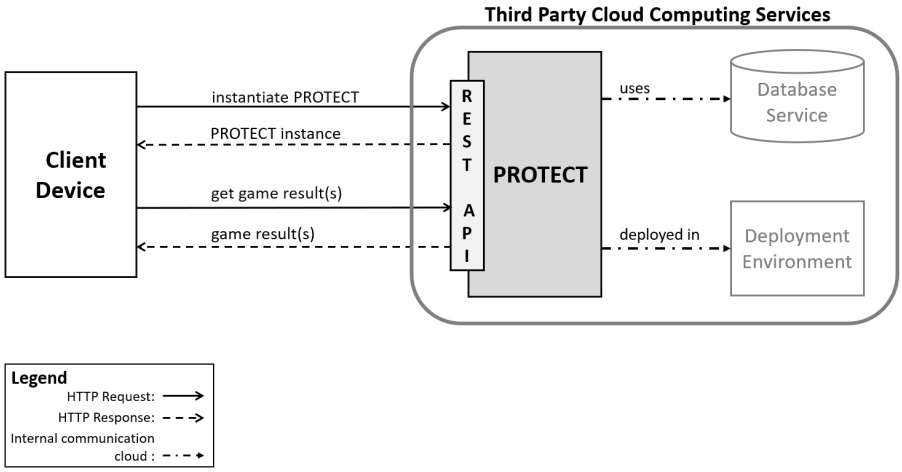


Fig. 4: Abstract architecture of the PROTECT web service

5 Discussion

We showed our game to 5 practitioners from different domains (from the information technology, cybersecurity, smart homes, and automotive) and gathered

the following feedback. The general perceptions during game play provided feedback that conforms with our design goals. One participant stated, that for them the game simulates the reality. The player further explained, that in real life, it is rather difficult to expect social engineering attacks and always be ready for them, which they found was mapped through the random factor. Furthermore, the player mentioned that usually even the most cautious people might fall victim for social engineering when not constantly reminded of this threat. The player stated that the game does a good of job of doing that. Moreover, being able to defend themselves against social engineering in the game gave confidence the same could be achieved in real life. Another participant provided feedback on the challenge level in the game saying that "one has to think". For this player, the game was also "easy to understand", reflecting the modesty of the trade-off between those two conflicting elements. Finally, the player emphasised the importance of the game being single player for the replay value, saying that he can "play the game another 3 times just right now".

6 Conclusion

We designed, implemented and evaluated a serious game family for training social engineering defence mechanisms, called PROTECT. Since the basic concept of the game has already been evaluated for PERSUADED [1], we focused on the evaluation of the enhanced configuration.

Several goals were specified and refined to achieve the serious purpose of the game:

- Easier start into the game and increased replay probability.
- The game, i.e. game play, can be adapted to the player's skills and previous game results.
- The game attack scenarios can easily be adapted to the player's skills and environment.
- An integration into external training platforms is allowed, i.e. the platform can decide about the difficulty of the next games.

Our qualitative evaluation showed that with the enhanced configuration options, we could achieve our purpose. In future work, we aim to do a quantitative evaluation with a larger number of players.

Acknowledgements

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786890 (THREAT-ARREST).

References

1. Aladawy, D., Beckers, K., Pape, S.: PERSUADED: Fighting Social Engineering Attacks with a Serious Game. In: Furnell, S., Mouratidis, H., Pernul, G. (eds.) Trust, Privacy and Security in Digital Business - 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5-6, 2018, Proceedings. Lecture Notes in Computer Science, vol. 11033. Springer (2018). https://doi.org/10.1007/978-3-319-98385-1_8, https://doi.org/10.1007/978-3-319-98385-1_8, iSBN 978-3-319-98384-4
2. Bakhshi, T., Papadaki, M., Furnell, S.: A practical assessment of social engineering vulnerabilities. In: HAISA. pp. 12–23 (2008)
3. BBC: How to hack people (2002), news.bbc.co.uk/2/hi/technology/2320121.stm
4. Beckers, K., Pape, S.: A serious game for eliciting social engineering security requirements. In: Proceedings of the 24th IEEE International Conference on Requirements Engineering. RE '16, IEEE Computer Society (2016). https://doi.org/10.1109/RE.2016.39
5. Beckers, K., Pape, S., Fries, V.: HATCH: Hack and trick capricious humans – a serious game on social engineering. In: Proceedings of the 2016 British HCI Conference, Bournemouth, United Kingdom, July 11-15, 2016 (2016), http://ewic.bcs.org/content/ConWebDoc/56973
6. Dimensional Research: The Risk of Social Engineering on Information Security: A Survey of IT Profesionals (2011), http://docplayer.net/11092603-The-risk-of-social-engineering-on-information-security.html
7. Ferreira, A., Coventry, L., Lenzini, G.: Principles of persuasion in social engineering and their use in phishing. In: International Conference on Human Aspects of Information Security, Privacy, and Trust. pp. 36–47. Springer (2015)
8. Gondree, M., Peterson, Z.N.J., Denning, T.: Security through play. IEEE Security and Privacy **11**(3), 64–67 (2013)
9. Greitzer, F.L., Kuchar, O.A., Huston, K.: Cognitive science implications for enhancing training effectiveness in a serious gaming context. J. Educ. Resour. Comput. **7**(3) (2007)
10. Irvine, C.E., Thompson, M.F., Allen, K.: Cyberciege: gaming for information assurance. IEEE Security & Privacy **3**(3), 61–64 (2005)
11. Manske, K.: An introduction to social engineering. Information systems security **9**(5), 1–7 (2000)
12. Mitnick, K.D., Simon, W.L.: The art of deception: Controlling the human element of security. John Wiley & Sons (2011)
13. Newbould, M., Furnell, S.: Playing safe: A prototype game for raising awareness of social engineering. In: Australian Information Security Management Conference. p. 4 (2009)
14. Olanrewaju, A.S.T., Zakaria, N.H.: Social engineering awareness game (seag): An empirical evaluation of using game towards improving information security awareness. In: Proceedings of the 5th International Conference on Computing and Informatics, ICOCI 2015 (2015)
15. SANS: Social Engineering Threats (2003), http://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232
16. Schaab, P., Beckers, K., Pape, S.: A systematic gap analysis of social engineering defence mechanisms considering social psychology. In: 10th International Symposium on Human Aspects of Information Security & Assurance, HAISA 2016 ,Frankfurt, Germany, July 19-21, 2016, Proceedings. (2016), http://www.cscan.org/openaccess/?paperid=301

17. Schaab, P., Beckers, K., Pape, S.: Social engineering defence mechanisms and counteracting training strategies. Information and Computer Security **25**(2), 206–222 (2017). https://doi.org/10.1108/ICS-04-2017-0022, https://doi.org/10.1108/ICS-04-2017-0022
18. Shostack, A.: Threat Modeling: Designing for Security. John Wiley & Sons Inc., 1st edn. (2014)
19. Stajano, F., Wilson, P.: Understanding scam victims: Seven principles for systems security. Commun. ACM **54**(3), 70–75 (Mar 2011). https://doi.org/10.1145/1897852.1897872, http://doi.acm.org/10.1145/1897852.1897872
20. Williams, L., Meneely, A., Shipley, G.: Protection poker: The new software security "game". Security Privacy, IEEE **8**(3), 14–20 (May 2010)