IET Software

Submission Template for IET Software Journal Special Issue

IET Journals
The Institution of Engineering and Technology

Improving Software Security Awareness Using A Serious Game

ISSN 1751-8644
doi: 0000000000
www.ietdl.org

Affan Yasin[1], *Lin Liu*[1] ✉, *Tong Li*[2], *Rubia Fatima*[1], *Wang Jianmin*[1]

[1] *School of Software, Tsinghua University, Beijing, China*
[2] *Beijing University of Technology, Beijing, China*
✉ *E-mail: linliu@tsinghua.edu.cn*

Abstract:
Context: Protecting people from cyber threats imposes great challenges, not only technically, but also socially. To achieve the intended level of awareness, software security principles need to be shown with concrete examples during security education. **Objective:** This study aims to design a serious game integrating software security knowledge and concepts into the processes to make it more engaging to learn while playing. **Method:** In this paper, we have: i) designed a serious game to compensate the deficiencies in the literature; ii) performed empirical evaluations including survey, brainstorming and observation to the proposed game. **Results:** Our study shows that: i) Cyber Security-Requirements Awareness Game (CSRAG) has a positive effect on players security learning outcomes, level of engagement and participation; ii) Game-based learning can be an effective way of teaching security related scenarios.

1 Introduction

The digital era of today is marked by proliferation of software systems across various platforms used in our daily lives. Examples include mobile phones, laptops, smart watches, etc. It is of utmost importance that the systems continuously provide us with their intended services. The importance of security and privacy protection of these systems has drastically increased due to their penetration in every walk of life. e.g., business, hospitals, education, etc. Software security emphasizes upon the matter which makes software work correctly even under malicious attacks. Attaining and sustaining security level impose complex and interdisciplinary challenges. To make software systems work as they are intended, the training, awareness, and education of the end users regarding system security is of great importance. Similarly, the security personnel of software systems need to understand not only the technical but also the social aspects of security to better defend against cyber-attacks.

Cybersecurity is of much importance as we enter the digital era. Our identity, property, reputation are all taking an electronic form, which can easily be extracted and manipulated, if not well protected. There are many technical security protection measures that have been developed and deployed in today's information systems. However, security protection still requires holistic understanding of human psychology and behavior. Since they are one of the most vulnerable targets in the loop. Thus, enhancing security knowledge of the system actors and improving their security awareness are of great importance.

Security education is no easy job. Security concepts and models are often abstract and technical, which makes them inaccessible to general system players. Among the many methods being developed and used to conduct security training, game based approaches are considered as potentially one of the most useful and effective ones. As in any game-based learning environment, learners have the freedom to explore multiple alternatives without any fear of failure or negative consequences. In this paper, we have designed a card based game named Cyber Security-Requirements Awareness Game (CSRAG). The primary goal of the game is to make aware the technology end-users regarding security related concepts, threats, and the possible ways to identify potential threats in operation environment. Understandably, playing one session of the game will only help them decipher the basics. For better understanding, players need to play multiple sessions of the game, so that maximum literature, which is embedded in the game design, can be unfolded and several valuable lessons can be learned from the game.

In our previous work [1], we have designed and evaluated a security awareness game. This paper follows the same line of research and extends the research direction of our study in several ways. The contribution of this study is as follows:

- Change the setting of game to software systems security protection from users perspective.
- To improve the challenge part of the game, we have introduced the game element of clue/spy card. To improve the physical security mechanism of hospital, security personals were placed on the map. Furthermore, to enhance the engagement of the participant we have updated the process, rules and map of the game.
- To strengthen the evaluation and engagement part of the activity, we have: i) adapted Pre-post questionnaire from the literature; ii) designed animated videos mimicking real-life social engineering attacks; iii) designed animated videos using attack scenarios adapted from USAHealthit.gov website.
- To overall improve the game, we have utilized previous results, feedback and observations to further polish the game rules and process.

2 Research Methodology

Firstly, in order to perform this study, we have performed a literature review to find the potential background and research gap. After that, we searched for the literature which focused on security challenges and their game-based solutions. After acquiring a better understanding of the area, the current trends and the challenges, we started designing the game using the security literature as the base. After its creation, the game was played as a pilot activity in the lab for initial feedback. After settling down with the rules and the process, we moved forward in planning an activity. The players filled pre-questionnaire before playing the game and, at the end, wrote hypothetical scenarios followed by suggestions on real-life attack scenarios across different countries.

The objectives of the study are further converted into following research questions:

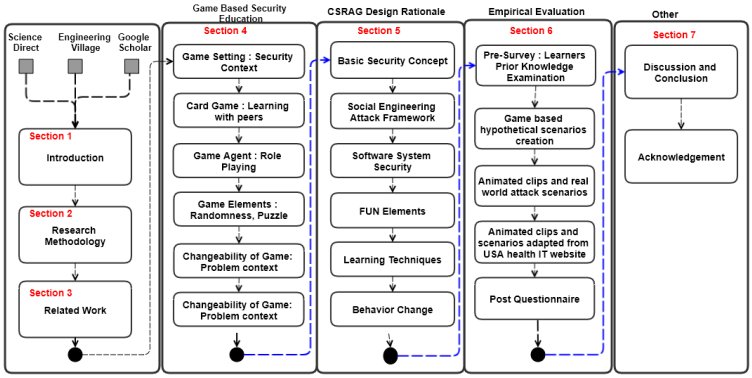

Fig. 1: Research Protocol

RQ1: How to design a serious game using game design principles which integrate security requirements knowledge and concepts into the processes?

Rationale: The motivation behind this research question is to devise a method which can be used to design a game. The primary challenge is to embed the concepts of cybersecurity and game design principles while designing a serious game for cybersecurity awareness.

RQ2: Does playing security card game CSRAG help participants to identify potential security attacks in a given situation?

Rationale: This research question aims to analyze the effectiveness of the proposed game in cybersecurity concepts learning using empirical methods.

The detailed flow of the paper is as follows: Section 1 introduces and motivates the problem by discussing recent cyber attack events and importance of socio-technical awareness of people. Section 2 explains the research methodology used inorder to answer the research questions. Section 3 shows the important existing work on the topic while Section 4 explains the design of the game: in particular, design rationales, an overview of the game map, and the process for playing the game. Section 5 describes definitions of security related concepts, game ontology, and attack framework used for game design. Section 6 discusses the results of the empirical evaluation performed, possible validity threats for the study and the overall findings. Section 7, discusses the findings and Section 8, finally concludes the paper. The research protocol of this study can be seen in Figure 1.

3 Related Work

Game-based learning are nowadays taken as a hot topic of research with applications in the field of marketing, business, software, medical applications and education to name a few. Many studies [2–4] have been conducted to analyze the effects of game design on training, education and learning of the participants. The majority of the studies concluded that game-based learning does bring about a positive effect on the learning of the students [5, 6].

Games engage students and bring better learning outcomes. An experiment was designed and conducted on 254 students and suggested that collaborative game-based learning has a positive effect on student learning, engagement, and motivation [7, 8]. Furthermore, students learning processes not only depend on game-based learning but also on the process itself. To verify, the researchers created a digital game to teach the English language. The results of the experiment clearly showed that students, while using game-based learning, are more engaged in learning and participation. Furthermore, participants think that game-based learning process and method trigger curiosity [9]. Moreover, researcher analyzes which method for cyber security awareness is better. Whether to use a text based method or video based training or simply use game-based technique? The study concluded that use of combined method for training and awareness make the goal easy to achieve [10]. Moreover, researchers analyzed that game-based learning effect has been observed in nearly all fields such as education (security), games, health, etc. However, industry and organizations are hesitant to adopt games for teaching possibly due to the reason that games are generally expected to contribute negatively in any serious learning process. The author suggested guidelines for corporate usage of games for learning processes that were validated by experts in a workshop. The author also suggested that games must be used for vocational work based learning to get better results [11]. Researchers around the globe are working on game-based security education from different perspective. Some of the important works in the same field are given below.

Control-Alt-Hack [12] is a white hacking themed strategy and board card game developed by the University of Washington students. This game can be played by 3 to 6 players at a time. The playing time of the game for one round is about 1 hour. The primary purpose of the designer for designing the game is to enhance the awareness and interest of the students towards security related field. By playing the game player can be appraised of any potential attacker's imagination, skills, and issues being faced. The game is more focused on game design principles with major security terms used in cards for knowledge.

Another commercial game designed and developed on cyber security awareness topic is **d0x3d!**[*].This game can be played by 2-4 players at a time. In this game, players act like hackers. Their mission includes penetrating a network system. Furthermore, with team effort, the players need to use shares of digital assets provided to them and employ these resources to get stolen digital assets. After collection of all four of digital assets, the players need to exit the network. Within each round, the player's intrusion might be detected by patched networks set by admins. On any suspicion of penetration, admins ask for a forensic investigation and may increase the network threat level.

Moving forward, **Elevation of Privileges (EoP)**[†], a card game on threat modeling, was designed by Microsoft based on STRIDE model. Threat modeling is a design phase of Security Development Lifecycle (SDL). The EoP card game explores threats in software and computer systems through the details of threat modeling. This game is designed for various categories of people i.e. developers, architects, and engineers to check their projects for various threats.

[*] *http://d0x3d.com/d0x3d/welcome.html*
[†] *https://www.microsoft.com/en-us/sdl/adopt/eop.aspx*

Table 1 CSRAG Comparison with other Games adapted from [1]

Aspects	Characteristics	CSRAG	Ctrl-ALt-Hack [12]	Social Engineering [13]	Dox3d
Role Playing	(Attack) Characters in game	✓	✓	x	✓
Security Context	Story line of the Game	✓	✓	x	✓
	Dynamic Nature of Map (Changeability)	some+	x	x	✓
	Map Used in the game for reference	✓	x	✓	✓
	Players play by moving on the Map	✓	x	x	✓
Security Mechanism	Attack Mechanics	✓	✓	✓	✓
	Defence Mechanics	x	x	x	✓
	Making Scenario	✓	x	✓	x
Game Element	Different type of Attack Cards	✓	some+	✓	x
	Dice for Randomness	✓	✓	x	x
Security Knowledge Area	Social Engineering Issues	✓	some+	✓	some+
	Network Security Related Issues	✓	some+	x	✓
	Physical Security Related Issues	✓	some+	x	some+
Security Protection Target	Mission for the Team and Player	✓	✓	x	✓
Team-based Learning	Discussion Session (Knowledge/Experience sharing)	✓	some+	✓	some+
Evaluation Design	Different Methods for Evaluation	✓	x	x	x

Finally, this **Social Engineering** game [13] aims to understand the threats associated with human assets working in the organization. The game contains a combination of attack card and psychology cards. The players work as an individual. The players have to suggest the most suitable attack card with the psychology to attack the human asset present on the given floor plan. Besides this, players have to create scenarios with respect to the situation to better understand the security concepts.

Our CSRAG game covers various aspects relating to role playing, security context, security mechanism, team-based learning etc. Moreover, it extends various new concepts in design and evaluation. The detailed comparison can be seen in Table 1 which is adapted from [1]. In Table 1, 'Some+' identifies that a particular phase is present to a good extent in the game. '✓' represents the complete presence of that phase in the game and 'X' represents the absence of that phase in the game. Type of attack, vulnerability associated with assets, psychology attack, attack framework, type of an attacker, dynamic nature of map etc. are a few important features of our game. In this version of the game, besides introducing new cards, updated game process, and new evaluation methods, we are using some of the game cards from its previous version. Some of the examples are vulnerability cards, attacker position cards, asset cards, puzzle cards and attacker role cards. Furthermore, process of developing hypothetical attack scenarios in game process is the same as that of the previous version. Moreover, the previous edition focused more on organizational security; however, this version focuses primarily on software security.

4 Game-Based Security Education

Section 4, explains the game context, motivation for card game, peer learning, game roles, changeability, game elements and game process of the CSRAG game.

Software security concerns with protecting information as well as systems assets of a target organization. As shown in Figure 2, we use a game map to provide the context of the software system, which includes the physical layout of the system components, and the operators of the system functionalities. Based on the information provided in the game map, we ask players to play the role of an organization security protection team who will identify the potential risks, including cybersecurity threats, the human vulnerabilities, and possible countermeasures. We will also ask the players take a "negative" viewpoints as ethical hackers do. Thus, security requirements can be derived as "anti-requirements" of the normal functional and non-functional requirements in a given organization and systematical setting. The concepts such as security context, vulnerabilities, processes, attack measures, and countermeasures are already embedded into the game design. The security context is mimicking a hypothetical organization with floor plan and the potential assets to be protected.

One of the primary challenges for the team players is that they have limited knowledge and certain constraints on resources. For example, the life bar of the player in the game drains if a player disguised as spies, get exposed. If all of the lifebar is used up, the ransomware attackers may get vigilant, and the secret agent team may not be able to get the spy person and, eventually, will not be able to save the organization from this cyber attack. Besides this, the failed mission will finally bring a bad name to the agency as well as to the government offices. So, stopping this attack and bringing the people behind this plan to light is the critical and most important task given to the team.

4.1 Game Setting : Security Context

The storyline shall introduce the organizational and systems setting, the potential threats, and the role of the players etc. For example, we assume that the team players belong to the undercover team of a Health IT systems security agency. The Agency has received Intelligence information that one particular hospital in the country is to become the potential target of a ransomware attack. The task of the team is to evaluate that particular hospital's organizational and informational setting, obtain vulnerability/weakness and, finally, uncover the people involved in this planning. The players are working as a team with a common goal to achieve. There is however, competition with other teams. The winner will be the one with the most feasible and innovative attack scenarios on asset description and vulnerability.

Initially, the teams will get two secret pieces of information to uncover the people working towards compromising the hospital system. First one is the floor plan/map of the organization, and the second information is the room number in which that particular person works.

4.2 Card Game : Learning with peers

We followed the design motivation of security awareness and threat modelling as in [12, 13]. Furthermore, the motivation for designing the card based game is to minimize communication barriers between team players as well as the competing teams. Besides this, the same geographical location helps to reduce many communication barriers while maximizing contribution and discussion between players in face-to-face communication. The review sessions at the end of the game also contributes to mutual peer-to-peer dissemination of information and game decision. The details of communication barriers in the distributed teams and the positive results of face-to-face communication can be seen in the study [14, 15].

4.3 Game Agents: role playing

Usually, the teams are divided into a group of three to four. The first player represents a character role of Network attacker, the second represents a role of Social Engineer Attacker, and the third poses a role of Physical Attacker. The primary motivation for this is that every team member may represent at least one particular type of character roles. If more than three players are on the team, then these others will help in selecting or making important decisions in game. The team uses a piece to represent their position on the map.

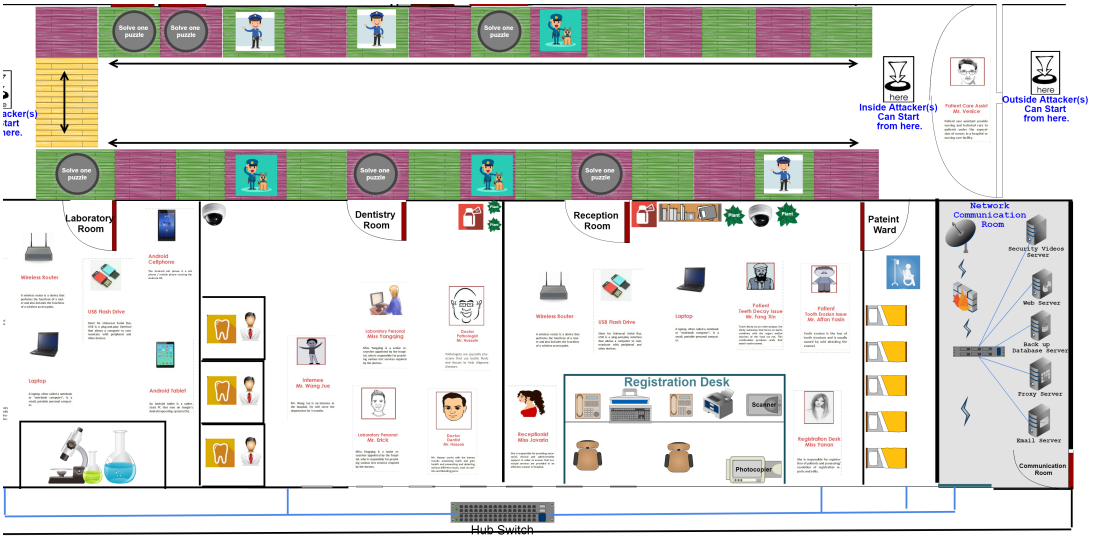

Fig. 2: Map of the Game (Partial): Hospital information systems setting

To create suspense, drama, and randomness, every room will have at least two undercover security personnel and two spy cards which will lead to infected the IT product. The players have to randomly select the human asset. If the secret agent emerges, the team loses one chance. Else, the team get the room number of the infected device.

To make the movement on the way the tiles will have security personnel randomly assigned to them. In reality, this represents the security within the hospital. If by rolling the dice the player gets his/her piece on the tile of the security personal, the player will lose a life.

4.4 *Game Elements : randomness, puzzle*

Initially, each team has a total of four chances. Before losing all the lives, the player has to access the infected device as indicated by the spy person in the organization. Generally, in the game, the player will lose a life by one if the player gets caught by the police or undercover security personnel. If the player loses all the lives before reaching and successfully compromising the infected device, the mission/game will be lost in totality.

The players will use a dice for movement on the map path. The movement of the player is dependent on the value that appears on the dice. In case after rolling the dice, if the number for reaching a particular room is greater as on than the dice needed, then the player has to wait for that particular value to appear. If a smaller or an exact value appears on the dice, the player can move that number on the path. The players have to save themselves from the police present on the way.

In any real life scenario, the attackers need to guess passwords and patterns and further take chances. Additionally, the attacker has to compromise the security system to access the restricted area. The same is mimicked by using puzzle cards, where they have to guess and solve the puzzle to get access to some area on the map.

We have used some of the important game elements (e.g. badge, time constraint, limited resources etc.) in our game which are extracted from the study [16]. Explained below are some of the important game elements used in CSRAG:

- Badge [1, 16]: Attacker role card and Attacker position cards are used in the game which is part of the badge game element.
- Limited Resource[1, 16]: Participants of CSRAG have limited life chances in game environment and limited attacks to select while writing hypothetical scenarios.
- Clear Goal[1, 16]: Working as an undercover government spy, players have to follow the initial clue to uncover the ransomware plan. The participants have a clear goal of discovering (insider) human asset involved and save the hospital from being a victim of cyber-attack or ransomware.
- Challenge [1]: Few of the challenges in CSRAG are that i) participants have to solve the puzzle to get access to the target room; ii) participants have to accurately fill the goal sheet.
- Fantasy [1]: The storyline, environment (context) of the game, and hypothetical attack scenarios at the end of the game contribute to this game element.

4.5 *Changeability of game: Problem context*

Within our game, minor modifications of the situation may result in updating the attack scenarios by the participants, but the outcome in the form of context, concepts and the reasoning process remains the same.

For advanced users, they need not to use the already designed map. They can generate any hypothetical map of their own by using the assets cards. Once the players are done with the initial few games using the designed map, players can use the asset cards to set the map of their own.

4.6 *Game Process : thinking like an attacker*

For the beginners, a map is already designed, which can be seen in Figure 2. The map shown depicts the environment of the hospital which has all the valuable assets (Human, IT, Office, etc.). Besides this, security personnel and the other relevant information can be seen in detail in Figure 2. The enlarged and complete version of the map can be seen by clicking the **link**[*].

Game Process is explained below for better understanding:

[*] *http://tinyurl.com/y7gpt6ko*

IET Software, pp. 1–12

• **Step 1: Select Room from Map** Firstly, the player has to plan the attack by selecting the target room on the map (given as the initial queue), and the path that will be taken for reaching the target.
• **Step 2: Select Insider or Outsider Attacker** The player has to see if he/she is an inside attacker or an outside attacker. If the team player is an outside attacker, then he/she has to additionally compromise the person standing at the entrance. By compromising, we mean suggesting the accurate attack with respect to the vulnerability and asset description.
• **Step 3: Roll the Dice** In order to move on the path, players have to roll the dice to move on the map of the organization. The resulting number tells how many steps a player has to move on the path. The player has to save himself from the cell which is labeled as the police. In case he/she gets onto that piece, the player will lose one life.
• **Step 4: Solve one puzzle to access that Room** Participant has to solve a puzzle from a puzzle deck in order to get access of the room.
• **Step 5: Selection of spy** After getting the access, the player has to select one of the assets randomly which he/she thinks of a possible spy. If this random selection is correct, the card on the back gives the player a direction towards the infected device; else, in case of an unsuccessful selection, the player loses one life. This can be seen by viewing the back of the asset card.
• **Step 6: See vulnerability and Description of the Asset** In the next step, the player has to move to the infected device room and suggest ways to compromise that infected device. The team players have to see the target asset description, position in the organization and weakness / vulnerability. After getting all the desired information, the attacker has to suggest a viable and most feasible attack from the attack cards given to them.
• **Step 7: Propose Hypothetical Scenarios** After successfully devising the attack, the player of the team has to write a hypothetical scenario for the attack.
• **Step 8: Discussion / Review between teams** After the process of scenario making, discussion session between the teams will start to improve further scenarios and give points to them.

5 Design Rationales of CSRAG

Section 5 defines important concepts and their utilization in designing CSRAG. Section 5.1 explains the security concepts (ontology) as discussed by Firesmith and the embedding of ontology in CSRAG; Section 5.2, discusses social engineering attack framework and its usage in CSRAG. Section 5.3 explains software system security principle in our game. Section 5.4 & 5.5 mention Fun elements and learning techniques used in designing CSRAG game respectively. Lastly, Section 5.6 discusses about factors embedded in our game to motivate behavior change.

5.1 Basic Security Concepts

Security Requirements Engineering addresses the security requirement at the early design phase. Security Requirements are taken as a non-functional requirement while designing any system; which is one of the primary constraints. Software systems are usually attacked by attackers using their vulnerabilities which motivates outlining a process by which security engineers can better elicit the security requirements. For the last two decades, researchers have proposed frameworks, models and processes to address this challenge [17–19].

Information Security Ontology definitions are necessary to minimize vaguely defined terminologies and definitions and accurate the complete knowledge base. To make our game design base in parallel to the ontology explained in the published literature we followed Firesmith ontology [20] to design our game. The explanations of items in the ontology can be seen below [21]:

• **Asset:** A valuable thing or resource of the organization e.g. data, information, human, computers, office etc.
• **Vulnerability:** Weakness of the asset which can be exploited by an attacker to get control of things to do.
• **Attack:** An offensive decision taken against a person or organization.
• **Attacker:** The person or organization who attacks is known as the attacker.
• **Security Mechanism:** Mechanism by which we can defend against the assault or minimize the effect of the attack.
• **Security requirements:** Requirements needed to be completed or acted upon to achieve security goal or minimize the chance of cyber-attack.
• **Security Objective:** A security objective is a way of representing a security goal. Moreover, Security Objective explains the ideal desired security state by any organization.

The ontology proposed by Firesmith was meticulously analyzed to fully embed the concepts of security requirements in the CSRAG game. One to one mapping was performed for the game assets or elements. Interestingly, some of the concepts mapped directly, such as security mechanism i.e. the process of solving a puzzle card to get access to the room (in the game environment) reflects this aspect of ontology. Regarding various concepts such as an attacker, we further extend the idea into Attacker Position and Attacker Role which are in turn, further divided into different positions (Insider or outsider) and different roles (Network, physical or social engineer) respectively. In our CSRAG game, concepts in the existing security requirements ontology are mapped to concrete game elements. For example, we designed assets cards of five types namely person, data, hardware, software, and physical assets. An asset card has an icon, a name as well as a description of the asset in the front and the associated vulnerability defined in the back. The mapping of the game elements using the security concepts can be seen in Figure 3. The boxes in dotted rectangle show Firesmith [20] fundamental ontology, and the boxes in green outside the dotted box represent the extension of the ontology in the game. Figure 3 also shows the template cards designed for this game. Against each item of ontology, a template card is shown.

5.2 Social Engineering Attack Framework (SEAF)

Social Engineering is the psychological manipulation of the people to perform the actions one desires them to do. Social Engineering Attack framework explains the way a particular attack takes place. Our CSRAG game follows social engineering attack framework as proposed by Mouton's [22]. The primary goal is to align the game processes with the published literature of security. Table 2 explains that our game process is aligned with Social Engineering Attack Framework mentioned in [22]. We also explored how our method covers different phases of security requirements engineering. Firstly, we collected few security requirement engineering techniques from literature and, further, mapped how they covered the different phases. The details on how our game covers such different phases as compared to other methods can be seen in the study [1].

Table 2 Game Alignment with Social Engineering Attack Framework (SEAF).

SEAF [22]	Presence in CSRAG
Attack formulation	Queue card, Floor map, Attack cards
Information Gathering	Asset description, Vulnerability, Shortest path to move
Preparation	In developed Attack Scenarios Intra-team discussion
Develop Relationship	In developed Attack Scenarios, Intra-team discussion
Exploit Relationship	In developed Attack Scenarios Intra-team discussion
Debrief	Optional : In developed Attack Scenarios Intra-team discussion Inter-team discussion

• **Attack formulation:** In this phase, secret spy team has to select the room as given in the queue card and formulate plan for an attack.

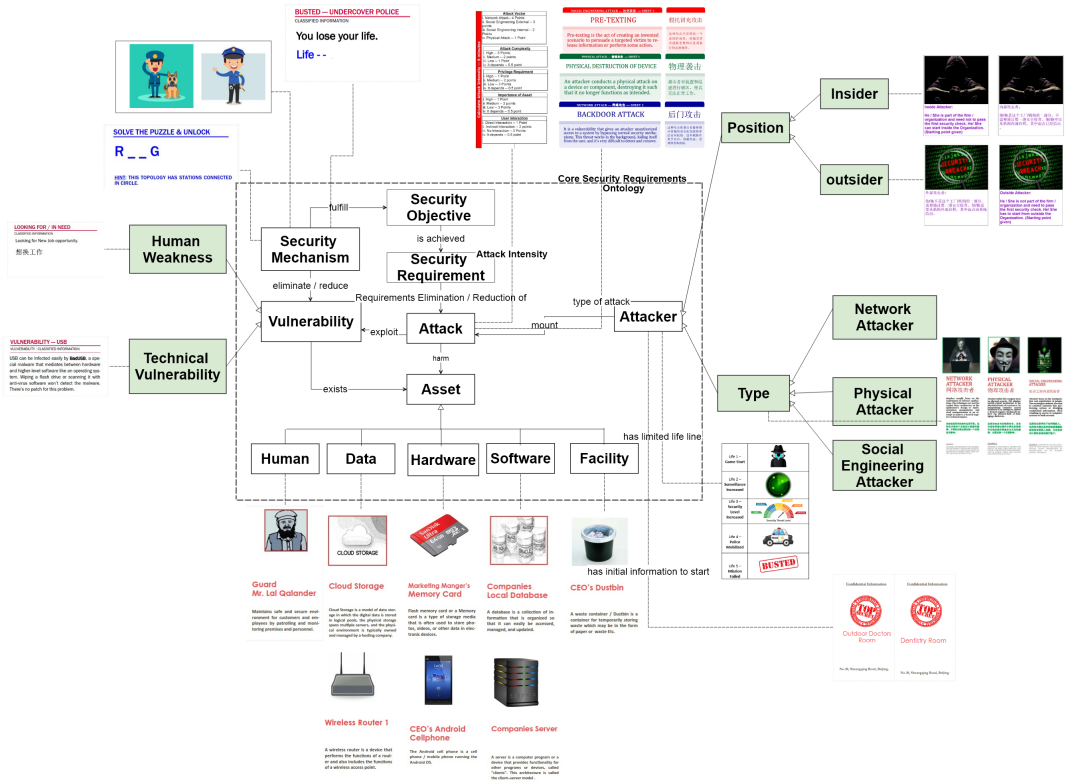

Fig. 3: Game Structure and the Corresponding Game Cards

- **Information Gathering:** In this step, the secret spy team has to first correctly select the spy from the room mentioned in the queue card and, further, get the information of the infected device in the hospital.
- **Preparation:** In this phase, spy attackers prepare them for the attack.
- **Develop Relationship:** In this step of developing relationships, the secret spy team develops scenarios in the game which fulfill this phase of the attack.
- **Exploit Relationship:** Here, attackers exploit the trust to get critical information from the human asset.
- **Debrief:** In this phase, the attackers try to normalize the victim.

5.3 Software System Security

One of the important security design principles is securing the human link in the security **chain***. Organizations are spending millions of dollars on enhancing the company security systems and ignoring the human aspect of the security chain. The human aspect is one of the vital factors in software system security. While designing any human system interactions, designers shall not only focus on the technical side of the system but also focus on users perspective [23]. According to study a [24], human is one of the most vulnerable point in the loop and causing about 95% of the cyber breaches. We attempted to focus this system security principle by making the end users informed regarding various attack strategies, techniques, and possible attack scenarios.

5.4 Fun Elements in Security Requirements Concepts

To utilize the full potential of game-based learning; Security Requirements Engineering concepts need to be taught in a concrete and fun to learn way. The same is done while designing the game. We have used fun elements as extracted from [16] to make the game enjoyable to play. Some of the essential fun elements used are: i) **Challenge:** Challenging part is to attack and compromise the target asset by using the most feasible attack scenario and further detail review of opponent teams scenario; ii) **Fellowship:** The players have to play in teams thus helping them to assist and share their experience and knowledge; iii) **Discovery:** Players have to discover the target asset, the most feasible path and possible ways to attack the asset; iv) **Fantasy:** The games story line brings the fantasy by making participants an under cover agents; additionally the colour combination and quality of game material used help the participants to feel that environment.

5.5 Learning Techniques

In CSRAG, we have tried to utilize the already mentioned learning techniques to make participants learn during the activity. Details of each can be seen below:

- **Inquiry-based Learning:** It is a way of active learning where scenarios, questions or problems are posed and discussed instead of

*https://www.amazon.com/Building-Secure-Software-Addison-Wesley-Professional/dp/0321774957

IET Software, pp. 1–12

Table 3 Behavioural Determinants for Changing User Behavior

Behavioral Determinants	Security Context for the Game Player	Incorporating in Game
Perceived Vulnerability	Assessment of an event occurring as the result of a breach	Incorporated in two phases. Step 6 & 7 of Game Process.
Perceived Security	The severity and consequences of a security breach	Incorporated in two phases. Step 3 & 7 of Game Process
Response Efficacy	Belief as to whether the recommended action will actually avoid the threat	Incorporated in Discussion Session. Step 8 of game process.
Self-efficacy	Belief that they have enough knowledge and skill	A special session in the start of the game activity is used to present the goal, game rules and process. Besides that for guidance or question answers, one of the researcher was in the class.
Attitude	Feelings towards security behavior	An initial session was conducted telling the importance of this activity and recent attacks and hack.
Locus of Control	Their thinking how much they control	The game design principles are done in a way that the player feel the actual environment and must not think of impossible situation.
Psychological Ownership	Ownership of what they are protecting	This is shown in the story line of the game.
Subjective Norm	Social pressure when other are doing any act.	The game is designed as team work. The team work together to achieve the common goal and compete with other teams. The game based learning may be helpful to understand social pressure and to overcome in important situations.

presenting facts [25, 26]. We have embedded this learning technique in our game process step 6, 7 and 8; where participants will think, discuss and further inquire in the game environment.

- **Team-based learning:** Team-based learning is a strategy where participants play in teams and further discuss and solve problems [27]. The same strategy is embedded in our CSRAG in game process step 6, 7 and 8. Participants will play in teams and will not only educate the members of their own team along the way but also help the opponent team play and build attack scenarios by providing them the feasibility of their scenario. This way we have an inter as well as intra team learning environment.
- **Learning through playing:** While playing, participants/players need not be worried about the consequences. Participants can explore and learn without any fear of loss [28, 29]. This is embedded in our game where participants can take decisions and play without any fear of failure. By using this strategy, we believe, participants can truly explore and learn. This strategy is the base of CSRAG design which focuses on providing the participants an active environment to learn. This can be seen from the start till the last step of the game process.

5.6 Behavior Change

Blythe suggested some of the behavior determinants be targeted for behavior change while designing serious game. This conceptual framework suggested was further adapted from protection motivation theory and theory of planned behavior. To have a positive behavior change in the players, we have followed this framework to design our game [30]. The detail how we have incorporated in our study is shown in the Table 3.

6 Empirical Evaluation of Serious Game

We have designed an empirical evaluation to verify the proposition that CSRAG helps in security requirements engineering concepts learning. In order to perform pilot-activity, we prepared printed version of the card game, presentation slides for introductory lecture, and survey links for pre-questionnaire. After this, an email was sent to the students, alumni and colleagues for their voluntary participation which was further filtered according to the availability, prior knowledge, and level of interest of candidates. The other important criteria for recruiting players were by identifying candidates who require and are interested in security awareness training, and grouping players in a way to facilitate interactions. We received more than a hundred requests and after, filtering, we, finally, had 96 participants. This whole process of publicizing, filtering, and evaluating took nearly five months.

We have used a game to mimic a real-life problem setting in which the players were asked to think from an attacker's perspective. By putting on the hat of attackers, players elicit potential attack scenarios. The scenarios are then evaluated as evidence of elicited security requirements. The security behaviors of players will, thus, be improved by having potential attackers in mind, thinking of possible attacks and vulnerabilities in real life.

In order to calculate the winner, we came up with a point system. The team which suggests the most severe and feasible attacking scenarios wins. In the game, this is decided after the discussion session. This empirical evaluation can be taken as an activity to collect feedback from players and further enhance and update rules, cards, or process.

Section 6.1 explains the design and findings of the pre-survey, Section 6.2 discusses about the scenario based learning and presents game-based hypothetical scenarios developed by participants. Section 6.3 presents the responses of players when given some real life SE attack scenarios. Section 6.4 further check the learning by showing animated videos designed and developed using USA Health IT website. Section 6.5, presents the design rationales and participants' responses on post-questionnaire given to them.

6.1 Pre-Survey : Learner's Prior Knowledge Examination

We have used a pre-questionnaire so that before starting the game, we can have an idea of the pre-existing awareness/knowledge of the participants regarding security related scenarios.

The pre-questionnaire was adapted from the study [13, 31]. Figure 5 further shows the detail of response distribution on a five point five scale. In the pre-survey, we asked questions like: i) "There is no need to write security policy as all the thing in a company are insured," ii) "There is no need to remember passwords as its written on the table" etc. These are actions that employees usually perform without knowing how dangerous it could be for the company or how helpful it could be for any social engineer. If we observe the survey responses, we will come to know that majority of the participants make similar mistakes without knowing their effects. This may be due to company/lab culture where people don't focus on these types of little loop holes. As cyber attacks are increasing, companies need to focus on educating employees so that chances of SE attacks can be minimized.

Below mentioned are important findings from the pre-survey.

- 47 participants out of a total of 96 were involved in security analysis process before as either a part time or a full time employee. Rest of the 49 participants were students from different departments with no previous security related knowledge.
- By analyzing the answers, we can say that the responses are diverse and participants need a security awareness session to be adequately apprised to the concepts.

6.2 Example Hypothetical Scenarios Developed by Players

When we have to deal with perception and imagination we usually use an approach called scenario-based approach. In this method, people have to use imagination and perception. This approach has extensively utilized for more than fifteen years by organizations to

Table 4 Players Responses during Game progression - 1 | Human Asset - Patient Care Assistant

Scenario Structure	Game Instance for Team 1	Game Instance for Team 2
1. Vulnerability of Human Asset	Looking for new friends	Looking for Bonus / Extra Pay
2. Psychology to target	Trust	Need & Greed Attack
3. Type of Attack selected	Need and Greed Attack	Impersonation or Tailgating
4. Scenario developed by Teams	I will pretend I know an old friend who works for the company, we are going out this evening and need to drop something off. I would invite him to join us. With the opportunity to make more friend, he will compromise and allow me inside.	Pretend we have to use the rest room OR Give him some money.
5. Aggregated attack calculation	10 out of 16	11 out of 16
6. Suggestion given by Opponents	You must have done small talk and using opposite sex person might have better chance. Tell the person about you and earn trust.	Its not the public place so getting permission to go for rest room may not be feasible.
7. Reply by the Team members	As our team consist of only guys this cannot be possible.	As we have given two options of attack, the first one may be weak but giving a bribery can be another good option.
8. Suggestion given by Expert	Composed attacks are reasonable.	The vulnerability of the person hasn't been well exploit.
9. Reply by the Team members	Ok. :)	As we have given two options of attack, the first one may be weak but giving a bribery can be another good option.

(a) Animated Video 1- Scene 1 (b) Animated Video 2- Scene 1

Fig. 4: Animated Videos Scenes

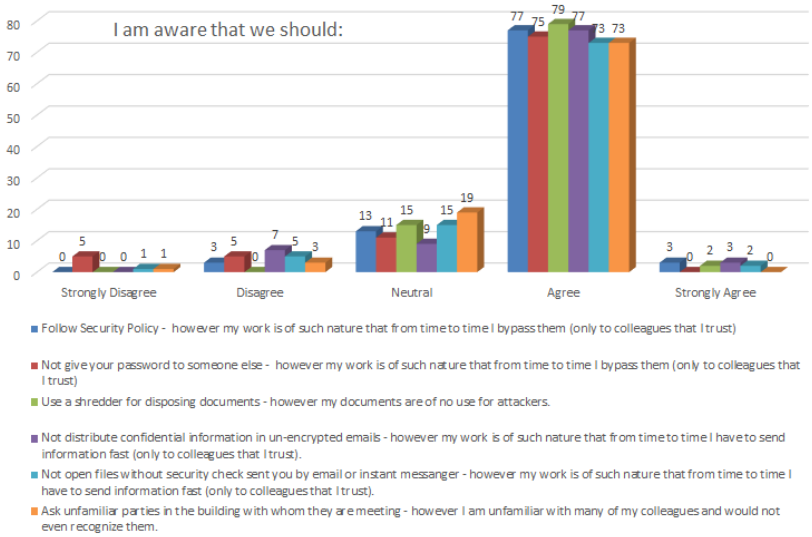

Fig. 5: Pre-Questionnaire Responses - some scenarios and responses shown

predict futures of the organizations [32, 33]. In order to further train and educate the players regarding the future challenges of security attacks and possible countermeasures, players were asked to

Table 5 Animation video of Real Life Social Engineering attack scenarios taken from different Police Public Awareness Data Sources

Real Life SE attack Scenarios	Response of Team 1	Response of Team 2
S1: Walmart: Spam Email for product delivery	She should confirm from the shopping history and must not give her personal detail.	Ignore the email, it's a spam.
S2: Scholarship : Spam Call Pretending from university.	1.She should confirm from the school by visiting the official school website and getting their contact. 2. She can call the administrative office or send an email to confirm. 3.Until she receives an official letter, No payment transfer.	She has to visit university and must not share password or account information.
S3: House Sold - Spam call pretended to be Tax officier	If there is no wrong doing in the sale of the house, the professor should visit the office of the authority to discuss and further report it for further investigation.	Call the police.
S4: Refund: Spam call pretended to be customer support	The website is supposed to have important details so there is no need to give out your information.	Ignore or she should not enter details on the web link.
S5: Kidnap - Spam call pretended to kidnap loved one	She must first confirm with the person who is kidnapped if she really is; she must contact police and tell the whole threat and follow instruction of police.	Let me talk the person first after getting confirmed he really got confirmed I will take some time and will contact police.

Table 6 Animation video of Scenarios taken from U.S.A Health IT website : Training Game

Training Scenarios	Response of Team 1	Response of Team 2
S1: Contingency Plan: Importance of taking backup, security and privacy.	Regular backup	1.Regular backup. 2.Disaster Recovery site. 3.Also must have backup on clouds
S2: Information Security: What to do when you have to transfer imp information on unsecured data.	Don't send unencrypted information that will be accessed in a public network.	Ask your I.T people for possible solution(s); one possible solution is to setup VPN for that kind of transfer.
S3: USB : Someone wants to use USB for taking print from the organization.	The USB might be infected with virus.	Scan first and then print if needed.
S4: Sales Rep: Needs to access server to show software update	Don't trust external access to your server.	Find out which data is required and discuss with data security team if it's possible to share.
S5: Lost : Company laptop stolen and related situation.	1.Don't take personal data outside. 2.Report the theft.	Report to police

develop scenarios according to the situations provided. In a particular case, the decisions taken by the teams are discussed as shown in Table 4 for information. Table 4 shows how the teams responded to the human asset on the entrance of the hospital with respect to his/her vulnerability and, after the completion of the game, what other reviewers suggested for possible improvements. The details of attack selection with respect to vulnerability, comments of reviewers, and team's response to the comments can be seen in Table 4.

There were two reviewers for accessing the hypothetical scenarios for the teams; one was the expert of the security requirements field and the other was the opposite team competing. Table 4 further explains the decisions taken by the teams during the flow of the game. Additionally, this, the evaluation by the expert reviewer is displayed. This phase of the game will be helpful for the players to better elicit the security threats within the game scenarios and learn by discussing and analyzing the game situation.

6.3 Animated clips of Real world Attack Scenarios & Responses from Teams

To further enhance the skill and security threat level awareness of the players, the students were shown some real-life social engineering attack scenarios in the form of animation movie clips and were asked their response and suggestions in those particular situations. The details of the some scenarios are given in Table 5 with the responses of the two teams mentioned afterwards. Also, few images of one scenario S3 also shown in Figure 4a. This phase of the game will be helpful in understanding the way real life attacks take place, so that participants can better understand by comparing the learning from the previous phases where they themselves developed attack scenarios.

6.4 Animated Clips for Scenarios Adapted from USA HealthIT Website

By going a step further, we adapted our training scenarios from the website of USA HealthIT* and further converted those into animation videos. The primary goal is to see how our players react to the scenario as suggested by the USA HealthIT. The details of the responses can be seen in Table 6 where one of the scenarios in the form of the animated images is shown in Figure 4b for information. Adding attack scenarios taken from USAHealthIT website will help us to use standardized learning scenarios in awareness program. By responding to and discussing those scenarios, participants will be exposed to diverse ways of social engineering attacks which will be finally will be helpful in counteracting if a similar situation appears in their lives.

6.5 Post Questionnaire

Technology Acceptance Model (TAM) was first introduced in 1986. It's primary goal is to elaborate influence on behavior due to adopting new technology. Previous research studies further confirmed the authenticity and effectiveness of using TAM for technology acceptance behavior. Further, a recent review study concluded that out of 42 studies, on technology acceptance, 36 studies used TAM as the base theory [34].

Game data, post questionnaire research model and its questions can be seen in **supplementary material**†. The questionnaire is divided into six portions named as "Fun to play", "Ease to play", "Intention to play", "Game-based learning", "Cyber security knowledge" and "Avoidance behavior". The post survey adapted from study [34–37] can be seen in supplementary material. If we visualize the responses, we will come to know that out of 96 majority of the participants responses lie in the agree portion, which shows an overall positive indication from the participants.

*https://www.healthit.gov/

†https://data.mendeley.com/datasets/sxm5cvrcx8/1

7 Discussion

In this study, we have evaluated the outcomes by using various empirical techniques such as: i) **pre-survey:** is used to produce initial knowledge by posing some real-life office situations; ii) **scenario based learning:** helps the participants think and suggest possible solutions to particular situations; iii) **post-survey:** gives feedback regarding the game and its learning experience; iv) **Feedback sheets:** are used to get detailed feedback and suggestions from the participants; v) **Observation:** One of the game representatives observed the environment for valuable insights of the room and participants.

Below are some of the scenarios developed by the players during empirical evaluation of the game. These scenarios are further deciphered to extract important information. The details of this can be seen below:

- **Scenario 1 - Target Asset - USB disk of the Marketing Manager** The attacker launch a Trojan virus attack by cheating the student researcher and thus damage the USB which is intended to achieve.
  - Attack Medium: Direct communication
  - Target Asset: Marketing strategy
  - Attacker: Inside attacker
  - Goal: To get access to the marketing strategy
  - Technique: Reverse social engineering attack
  - Psychology / Compliance Principle: Trust
- **Scenario 2 - Target Asset - Damage the router**
  Inside attacker pretends to get a “personal well paid" project, calls the R&D manager out of his office, as the manager will be excited the attacker can damage the router as planned.
  - Attack Medium: Direct communication
  - Target Asset: Human asset
  - Attacker: Inside attacker
  - Goal: Damage the router of a particular room.
  - Technique: Distraction attack
  - Psychology / Compliance Principle: Curiosity
- **Scenario 3 - Target Asset - Access of the inner network of the company** An outside attacker gets into room 418, approach the router and get the access with the help of an internal attacker.
  - Attack Medium: Direct communication
  - Target Asset: Network of organization
  - Attacker: Inside & outside attacker
  - Goal: Getting access to the company network
  - Technique: Physical destruction of device
  - Psychology / Compliance Principle: Not Applicable as network attack

Some of the findings and observations regarding the study can be seen below:

- If we holistically analyze the participants attack techniques, a good number of the participants tried to attack women or senior (aged) persons in the first chance by using various types of social engineering attacks.
- Other important observation is that the guard on the entrance was compromised by using simple excuses of emergency or a bribe in most of the cases.
- Most of the students used reverse social engineering attack technique as the attack strategy to compromise the human victim.
- In most of the social engineering attack scenarios, participants pretended to be some official from income tax, police etc. to get the desired information.
- There were 96 participants, consisting of a total of 31 groups. Each of the group made two game based attack scenarios during the game session. After analyzing the attack scenarios developed by participants, we came to know that nearly 90% of the scenarios developed were feasible while the remaining 10% were further improved during the discussion session. Some of the scenarios developed by the participants are shown in Section 7.
- The activity was lengthy as it comprised of five sessions. It is sometimes difficult to keep participants engaged and motivated throughout the process. In our case, we tried to give 15 minutes break after each session, so that participants may feel revitalized and involved.
- Initially, we tried to apply all the animated evaluations techniques in the process but after a few initial sessions we soon realized that these evaluations were not only taking a lot of time but also diminishing the motivation of the participants for any future participation. So, we started using these animated evaluation techniques randomly in the following empirical activities. Then, some of the participant’s responded to the “Real world attack scenarios" while others gave their point of view on scenarios extracted from “USA Health IT Website".

During feedback session, participants were asked to give positive and negative of the game. Furthermore, we motivated them to be fair as their feedback will be helpful in improving the game. Below is the important area where participants want us to improve the game:

- **Taking a long time to learn and Play:** This is trade-off situation for us, as to follow the literature and embed the attack process and other vital findings in literature we have to design a game in such a way that participant may learn by playing. To make the game rules learn smoothly by the participants, we are planning to make an animation video in future which will explain different scenarios and possible responses or steps required by the participants. Besides this, we are planning to improve the session of the game where we explain the rules, process, and background to the participants. Once the participants fully understand the process, rules, and goal; we believe that the time to play will also improve.

To minimize the internal **validity threats**, we have controlled the factors which were adapted from [38, 39]. The control factors are: i) **Activity time:** The sessions were clearly defined in sessions in-order to control the factor of time; ii) **Learning context:** English is used as the Language of the game; iii) **Gender, age and qualification** remains constant throughout the session; iv) **Class setting:** The students were divided into groups of three/four participants and the participants were randomly assigned to group. Furthermore, external validity of the study is yet to be verified in future.

8 Conclusion

In sum, this paper explicates a serious game aimed at improving software security awareness of system stakeholders. The design rationales of the game are discussed in detail to highlight the assumptions and prerequisites of a game that is to deliver security related concepts and principles to players who have zero to minimum background knowledge in security. This includes the selection and execution of viable game elements into the game processes. We evaluated the designed game and game design approach by running it in a classroom setting, and then collecting the game outcomes and feedbacks from 96 players. The results were encouraging since all participants acknowledged that they understood the security concepts and principles that the game tried to convey. By developing attack scenarios by oneself and then exchanging them with teammates, players understand the attacker’s intention in a more realistic way and know of possible countermeasures to mitigate these situations. Thus, CSRAG is interdisciplinary outcome which not only addresses one of the most dire needs of the world of software but also does so in a practical, feasible, user-friendly and an intellectually engaging way.

9 Acknowledgments

Natural Science Foundation of China Project no. 61432020 are gratefully acknowledged. Tong Li acknowledges the support of BJUT Startup Funding No.007000514116022. We acknowledge

Awaid Yasin (Lahore University of Management Sciences (LUMS), Lahore, Pakistan) for reviewing the paper.

10 References

1 A. Yasin, L. Liu, T. Li, J. Wang, D. Zowghi. "Design and preliminary evaluation of a cyber security requirements education game (sreg)", *Information and Software Technology*, **95**, pp. 179 – 200, (2018), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0950584917301921.

2 S. Olgun, M. Yilmaz, P. M. Clarke, R. V. O'Connor. "A systematic investigation into the use of game elements in the context of software business landscapes: A systematic literature review", A. Mas, A. Mesquida, R. V. O'Connor, T. Rout, A. Dorling (Eds.), *Software Process Improvement and Capability Determination*, pp. 384–398, (Springer International Publishing, Cham, 2017).

3 E. Herranz, R. C. Palacios, A. de Amescua Seco, M. Sánchez-Gordón. "Towards a gamification framework for software process improvement initiatives: Construction and validation", *J. UCS*, **22(12)**, pp. 1509–1532, (2016), [Online]. Available: https://doi.org/10.3217/jucs-022-12-1509.

4 A. Calderón, M. Ruiz, R. V. O'Connor. "A multivocal literature review on serious games for software process standards education", *Computer Standards & Interfaces*, **57**, pp. 36–48, (2018), [Online]. Available: https://doi.org/10.1016/j.csi.2017.11.003.

5 B. Taspinar, W. Schmidt, H. Schuhbauer. "Gamification in education: A board game approach to knowledge acquisition", *Procedia Computer Science*, **99**, pp. 101 – 116, (2016), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916322499, international Conference on Knowledge Management, ICKM 2016, 10-11 October 2016, Vienna, Austria.

6 M. Sanmugam, Z. Abdullah, H. Mohamed, B. Aris, N. M. Zaid, S. M. Suhadi. "The affiliation between student achievement and elements of gamification in learning science", *2016 4th International Conference on Information and Communication Technology (ICoICT)*, pp. 1–4, (2016).

7 C.-H. Chen, V. Law. "Scaffolding individual and collaborative game-based learning in learning performance and intrinsic motivation", *Computers in Human Behavior*, **55**, pp. 1201–1212, (2016).

8 B. T. Eng. "Game-based learning to teach assertive communication clicktalk for enhancing team play", *International Conference on Information Science and Applications*, pp. 660–667, (Springer, 2017).

9 S.-Y. Tao, Y.-H. Huang, M.-J. Tsai. "Applying the flipped classroom with game-based learning in elementary school students' english learning", *Educational Innovation through Technology (EITT), 2016 International Conference on*, pp. 59–63, (IEEE, 2016).

10 J. Abawajy. "User preference of cyber security awareness delivery methods", *Behaviour & Information Technology*, **33(3)**, pp. 237–248, (2014).

11 R. Senderek, B. Brenken, V. Stich. "The implementation of game based learning as part of the corporate competence development", *Interactive Collaborative and Blended Learning (ICBL), 2015 International Conference on*, pp. 44–51, (IEEE, 2015).

12 T. Denning, A. Lerner, A. Shostack, T. Kohno. "Control-alt-hack: the design and evaluation of a card game for computer security awareness and education", *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 915–928, (ACM, 2013).

13 K. Beckers, S. Pape. "A serious game for eliciting social engineering security requirements", *Requirements Engineering Conference (RE), 2016 IEEE 24th International*, pp. 16–25, (IEEE, 2016).

14 V. Gomes, S. Marczak. "Problems? we all know we have them. do we have solutions too? a literature review on problems and their solutions in global software development", *2012 IEEE Seventh International Conference on Global Software Engineering*, pp. 154–158, (2012).

15 R. Hoda, M. A. Babar, Y. Shastri, H. Yaqoob. "Sociocultural challenges in global software engineering education", *IEEE Transactions on Education*, **PP(99)**, pp. 1–10, (2017).

16 S. Deterding, D. Dixon, R. Khaled, L. Nacke. "From game design elements to gamefulness: defining "gamification"", A. Lugmayr, H. Franssila, C. Safran, I. Hammouda (Eds.), *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, MindTrek 2011, Tampere, Finland, September 28-30, 2011*, pp. 9–15, (ACM, 2011), [Online]. Available: http://doi.acm.org/10.1145/2181037.2181040.

17 P. Salini, S. Kanmani. "A novel method: Ontology-based security requirements engineering framework", *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, pp. 1–5, (2016).

18 A. Souag, R. Mazo, C. Salinesi, I. Comyn-Wattiau. "Reusable knowledge in security requirements engineering: a systematic mapping study", *Requirements Engineering*, **21(2)**, pp. 251–283, (2016), [Online]. Available: http://dx.doi.org/10.1007/s00766-015-0220-8.

19 L. Liu, E. Yu, G. Jabeen. "Social threats modelling with *i**", L. López, Y. Yu (Eds.), *Proceedings of the Ninth International i* Workshop co-located with 24th International Conference on Requirements Engineering (RE 2016), Beijing, China, September 12-13, 2016.*, volume 1674 of *CEUR Workshop Proceedings*, pp. 97–102, (CEUR-WS.org, 2016), [Online]. Available: http://ceur-ws.org/Vol-1674/iStar16_pp97-102.pdf.

20 D. Firesmith. "Specifying reusable security requirements. 2004", *Journal of Object Technology*, pp. 61–75.

21 A. Souag, C. Salinesi, R. Mazo, I. Comyn-Wattiau, *A Security Ontology for Security Requirements Elicitation*, pp. 157–177, (Springer International Publishing, Cham, 2015).

22 F. Mouton, M. M. Malan, L. Leenen, H. S. Venter. "Social engineering attack framework", *Information*

Security for South Africa (ISSA), 2014, pp. 1–9, (IEEE, 2014).

23 M. D. Harrison, J. C. Campos. "Analysing human aspects of safety-critical software", *ERCIM News*, **2008(75)**, (2008).

24 S.-J. Kim, S.-W. Lee. "Social engineering based security requirements elicitation model for advanced persistent threats", M. Kamalrudin, S. Ahmad, N. Ikram (Eds.), *Requirements Engineering for Internet of Things*, pp. 29–40, (Springer Singapore, Singapore, 2018).

25 S. K. Chu, R. B. Reynolds, N. J. Tavares, M. Notari, C. W. Y. Lee. *21st Century Skills Development Through Inquiry-Based Learning - From Theory to Practice*, (Springer, 2017), [Online]. Available: https://doi.org/10.1007/978-981-10-2481-8.

26 Ángel Suárez, M. Specht, F. Prinsen, M. Kalz, S. Ternier. "A review of the types of mobile activities in mobile inquiry-based learning", *Computers & Education*, **118**, pp. 38 – 55, (2018), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0360131517302397.

27 I. Cabrera, J. Villalon, J. Chavez. "Blending communities and team-based learning in a programming course", *IEEE Transactions on Education*, **60(4)**, pp. 288–295, (Nov 2017).

28 M.-T. Cheng, Y.-W. Lin, H.-C. She. "Learning through playing virtual age: Exploring the interactions among student concept learning, gaming performance, in-game behaviors, and the use of in-game characters", *Computers & Education*, **86**, pp. 18 – 29, (2015), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0360131515000767.

29 J. X. Chen. "Learning abstract concepts through interactive playing", *Computers & Graphics*, **30(1)**, pp. 10 – 19, (2006), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0097849305002037.

30 J. Blythe, L. Coventry. "Cyber security games: a new line of risk", *Entertainment Computing-ICEC 2012*, pp. 600–603, (2012).

31 H. Kruger, W. Kearney. "A prototype for assessing information security awareness", *Computers & Security*, **25(4)**, pp. 289 – 296, (2006), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404806000563.

32 A. Dix, J. E. Finlay, G. D. Abowd, R. Beale. *Human-Computer Interaction*, 3 edition edition, (Pearson,).

33 L. Van der Merwe. "Scenario-based strategy in practice: a framework", *Advances in Developing Human Resources*, **10(2)**, pp. 216–239, (2008).

34 F. Abdullah, R. Ward, E. Ahmed. "Investigating the influence of the most commonly used external variables of {TAM} on students' perceived ease of use (peou) and perceived usefulness (pu) of e-portfolios", *Computers in Human Behavior*, **63**, pp. 75 – 90, (2016), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747563216303387.

35 N. A. G. Arachchilage, S. Love. "A game design framework for avoiding phishing attacks", *Computers in Human Behavior*, **29(3)**, pp. 706 – 714, (2013), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747563212003585.

36 H. yi Sandy Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, S. R. Cotten. "Understanding online safety behaviors: A protection motivation theory perspective", *Computers & Security*, **59**, pp. 138 – 150, (2016), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404816300190.

37 N. A. G. Arachchilage, S. Love. "Security awareness of computer users: A phishing threat avoidance perspective", *Computers in Human Behavior*, **38(Supplement C)**, pp. 304 – 312, (2014), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747563214003331.

38 P.-N. Chou, C.-C. Chang, C.-H. Lin. "{BYOD} or not: A comparison of two assessment strategies for student learning", *Computers in Human Behavior*, **74**, pp. 63 – 71, (2017), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747563217302662.

39 G. W.-H. Tan, K.-B. Ooi, L.-Y. Leong, B. Lin. "Predicting the drivers of behavioral intention to use mobile learning: A hybrid sem-neural networks approach", *Computers in Human Behavior*, **36**, pp. 198 – 213, (2014), [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747563214001745.

11 Appendix : Game Data

The complete game data can be downloaded from the link http://dx.doi.org/10.17632/sxm5cvrcx8.1