Information and Software Technology xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Information and Software Technology

journal homepage: www.elsevier.com/locate/infsof

Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG)

Affan Yasin[a], Lin Liu[*,a], Tong Li[b], Jianmin Wang[a], Didar Zowghi[c]

[a] School of Software, Tsinghua University, Beijing, China
[b] Faculty of Information Technology, Beijing University of Technology, Beijing, China
[c] Faculty of Engineering and IT, University of Technology Sydney, Australia

ARTICLE INFO

Keywords:
Organizational security
Security requirements inception
Requirements engineering
Security awareness
Security education
Serious game
Social engineering
Cyber security
Empirical study

ABSTRACT

Context: Security, in digitally connected organizational environments of today, involves many different perspectives, including social, physical, and technical factors. In order to understand the interactions among these correlated aspects and elicit potential threats geared towards a given organization, different security requirements analysis approaches are proposed in the literature. However, the body of knowledge is yet to unleash its full potential due to the complex nature of security problems, and inadequate ways to improve security awareness of key players in the organization. **Objective:** Objective(s) of the research study is to improve the security awareness of players utilizing serious games via: (i) Know-how of security concepts and security protection; (ii) guided process of identifying valuable assets and vulnerabilities in a given organizational setting; (iii) guided process of defining successful security attacks to the organization. **Method:** Important methods used to address the above objectives include: (i) a comprehensive review of the literature to better understand security and game design elements; (ii) designing a serious game using cyber security knowledge and game-based techniques combined with security requirements engineering concepts; (iii) using empirical evaluation (observation and survey) to verify the effectiveness of the proposed game design. **Result:** The solution proposed is a serious game for security requirements education, which: **(i)** can be an effective and fun way of learning security related concepts; **(ii)** mimics a real life problem setting in a presentable and understandable way; **(iii)** motivates players to learn more about security related concepts in future. **Conclusion:** From this study, we conclude that the proposed Security Requirement Education Game (SREG) has positive results and is helpful for players of the game to get an understanding of security attacks and vulnerabilities.

1. Introduction

Modern organizations are relying more on online information services, both as service providers and as service consumers. Given highly secured technical infrastructure, valuable information assets can still be at risk if humans in the loop have insufficient security knowledge and proper training. According to a 2016 survey **report**[1] by a consulting firm dedicated to security related market research, there is a 63% increase in cyber attacks targeting hospitals in the past year. Furthermore, 88% of the malware is targeting the healthcare industry. A recent ransomeware attack at National Health Service Trust in England has caused severe consequences to thousands of victims and has made privacy and security a key concern in organizations with sensitive data [1,2], e.g. hospitals, e-commerce service providers, government agencies, etc. While the concerns of an organization and data owner entail security and privacy, the responsibility of protecting it has to be shared by all people with access to the valuable assets in the organization. Thus, key questions to be answered by everyone within the organization include: Who has access to the data? How the data is being used? What data is allowed to be shared with whom? What is the level of the data sensitivity or security protection? [3,4].

Understanding the security requirements of an organization is an important prequisite for successful system development. Many researchers bear the dream of making security requirements activities more engaging, enjoyable, and rewarding to improve security requirements training/awareness and increase its impact in reality [5–7]. Stakeholders play an important role in requirements elicitation process; their presence and contribution improve the quality of requirements

* Corresponding Author.
E-mail addresses: yayf15@mails.tsinghua.edu.cn (A. Yasin), linliu@tsinghua.edu.cn (L. Liu), litong@bjut.edu.cn (T. Li), jimwang@tsinghua.edu.cn (J. Wang), Didar.Zowghi@uts.edu.au (D. Zowghi).

[1] https://trapx.com/trapx-reveals-2016-healthcare-breaches-increased-63-percent-year-over-year-medical-device-hijacks-and-ransomware-on-the-rise/.

https://doi.org/10.1016/j.infsof.2017.12.002
Received 14 April 2017; Received in revised form 2 December 2017; Accepted 2 December 2017

and ultimately, have a positive impact on the system to be developed. Unfortunately, in reality, the participation of stakeholders is, in most of the cases, insufficient and ineffective. Researchers are trying to apply the concept of game design to enhance the stakeholder engagement and hence, the quality of requirements gathered [8]. Recently researchers have taken inspirations from the processes and representations in movies, games, stories, improvisation theaters, industrial designs, and media production to develop innovative uses of games in requirements engineering practice and training [5,9,10].

Requirements, which are “soft” and “representational” in nature, require new and innovative tools that add value to a given organization. A possible approach is to encourage a more playful and enjoyable creative process for both requirements engineering trainings and practices, thus increasing the intrinsic motivation for being more effective. The current challenge is to train and educate the stakeholders regarding security requirements and possible security attacks without harming the organizational, physical, and IT assets. In this scenario, developing a game for training is one of the possible solutions. Our motivation is along the same line of the “Ctrl-Alt-Hack” game [9], and the social engineering card game [5] for Security Awareness. Furthermore, people can learn and develop new skills by practicing various tasks of a game [11]. The most important part of game-based learning is that players need not be fearful of results, in case of failures. In real life scenarios, higher management discourage failures because failures tentamounts to loss for the enterprise. However, in the game based learning, players can learn both from failures and mechanisms designed in the game [12].

Research studies from different fields explored the effect of game design while training the employees. Recently, Landers and Callan [13]. carried out an experiment on military personnel to train them regarding various guns, devices, etc. One way was to just educate the personnel on presentations or to just make a visit to the weapon room. The researcher designed an experiment using game elements and observed that the training session became more engaging. They concluded that game based design has positive learning experience which further shows a positive relation between game-based design and training of employees. Furthermore, Helser [14] performed a study aimed at training the students regarding identity theft. They used two approaches for education i.e. text-based model approach and game-based approach.

While there are both success and failure stories of game-based design in the literature this paper introduces an approach towards teaching, training, and practising security related awareness using gameplay. This paper makes the following contributions:

1. We present the design and implementation of an educational game that embeds: security concepts to evaluate the impact of game-based training on player’s cyber security awareness.
2. We evaluate the effectiveness of the game through an empirical evaluation using quantitative and qualitative analysis. Based on the outcome of the evaluation we suggest various observations and possible future work.

The rest of the paper is organized as follows. Section 2 discusses about the literature review, Sections 3 and 4 outlines security requirements educational game elements and game process respectively. Section 5 describes security requirements engineering design rationale by elaborating concepts from literature in SREG. Afterwards, Section 6 presents the empirical evaluation and the analysis of the results. It then, finally, concludes the paper with possible future directions.

2. Related work

Game based design, despite its widespread use, is still in its initial phases of development [15]. The advantage of game based design has so far been explored in the field of health, information science, education, and human computer interaction. Many researchers have tested this concept in training and by experiments performed on the students, resulting in an increase in engagement and learning [16,17].

Nowadays, researchers all over the world are studying the impact of games in training and education [18,19]. Hamari et al. [20] performed an experiment to investigate the impact of flow, engagement and learning in the game-based environment. The data collected by performing a survey on 173 players showed that there is a positive influence of game-based learning on the players [20]. An experiment, which used Badges, a game element, was performed on 8th-year chemistry students, to check the learning and performance of the students. This experiment was performed on 61 students, and the result showed that the students who received multiple badges showed better average learning performance in the experiment [21]. It was found that people like social influence, positive recognition, and good will [22], these makes important game elements to motivate people in adopting positive habits and learning activities.

Research studies suggest that game based design can change the training environment by changing the emotional experience of players: their sense of identity and their social position. Game based project gives the opportunity to experiment with the rules, feelings and social roles in a playful manner [8,23]. Game based learning is not only about learning but also about accelerating the learning experience and engagement of the students as well as the stakeholders by motivating them through the game elements [24]. The effect of game based learning is evaluated in training activities [25] on both players attitudes and performances. The study concluded that game elements plays an active role and further suggests that there is a particular need to integrate game elements with existing tools of the organization [26]. Educational games and gamification can draw increasing attention [27], as an experiment on 379 students has shown that social gamification plays a vital role in learning activities. The impact of game elements is also explored on higher education. The results indicate that by gamifying the e-learning softwares, high satisfaction, motivation, and engagement can be achieved [28]. The incentive mechanism has become an important topic of empirical research. An online test, which the participants were asked to complete via points, leader-boards, and levels, has shown that the game elements positively enhanced the internal motivation of the participants [29]. Game based learning strives to boost the internal motivation of the players, as a survey has identified a strong relationship between the attitude of the players and their likeability of future use [30].

As discussed in [5], even the most important technical security system is vulnerable to attacks by social engineers. Traditional security requirements elicitation approaches often focus on vulnerabilities in network software systems. The prevailing social-technical integrated attacks motivates us to design a game against the arising problem of security which educates people regarding the security of an organization as a whole (integrating the technical and social-technical aspects).

3. SREG : Security Requirements Educational Game

SREG is a multiplayer card game. The purpose of having multiple players is to facilitate a collaborative environment during security requirements education where stakeholders team up to fight competing teams. It focuses more on co-operation within the team while competing with other teams. The Security Requirements Education Game is designed in two languages so more players can access this game with ease and further learn the security related scenarios and concepts. Chinese and English languages are selected as the first released version of the game. From our experience, learning rules and processes of the game take significant time at the beginning. That is why, the first game may take up to 50 min or so. However, this time reduces after players play the game more frequently. Fig. 1 shows the detailed research protocol of our work. While in the above two sections, we introduced the research background and related work in security requirements,

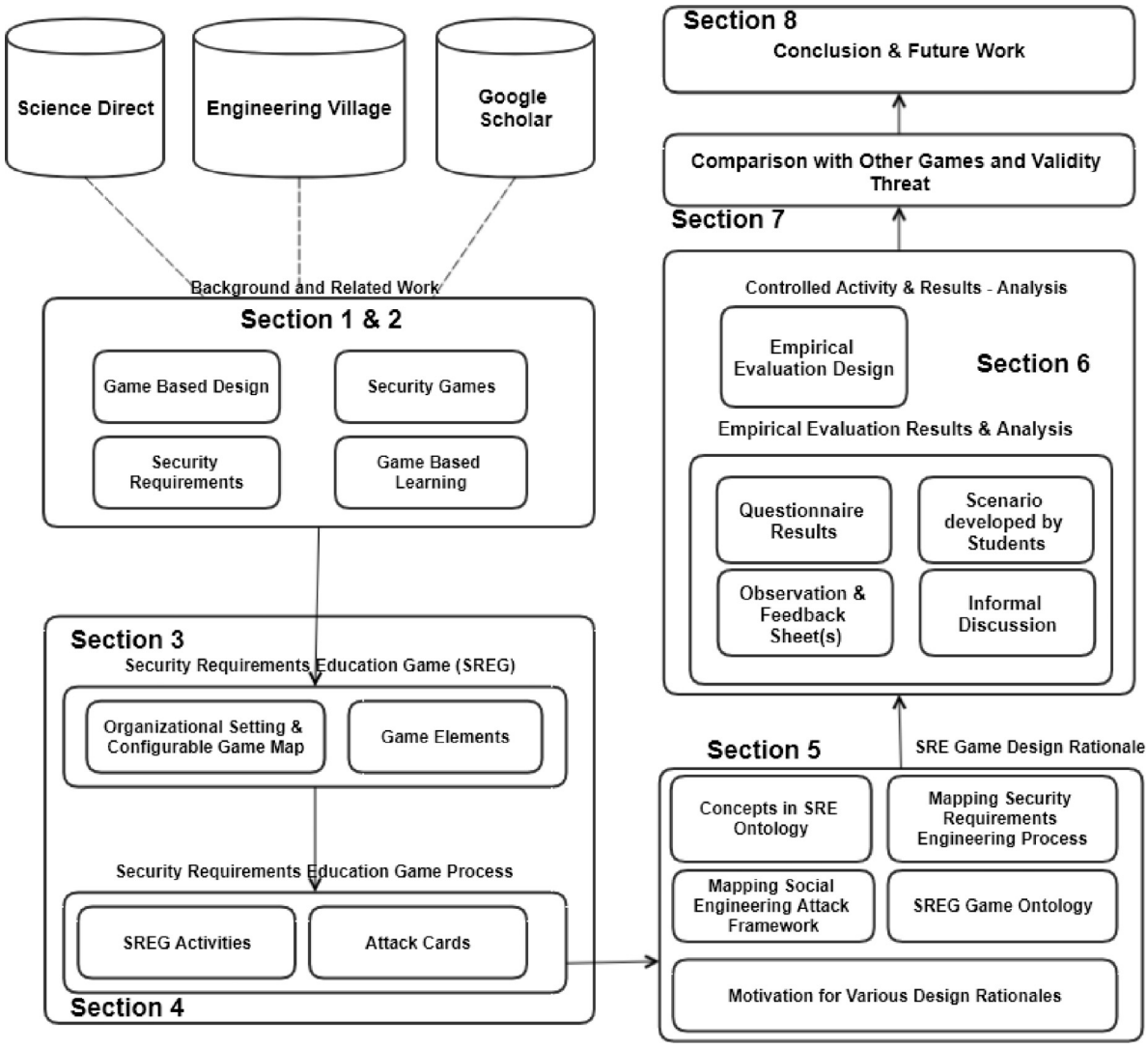


Fig. 1. Research protocol

game-based design & learning, and security related games. Furthermore, Section 3 introduces the game elements, the organizational context and settings to be captured by the game, as well as the extensible known attacks, Section 4 enlightens the game process, Section 5 describes the design rationales of the game by aligning game concepts with the ontology, attack framework and team building activities, Section 6 explains the empirical evaluation and results of the study, Section 7 explains the comparison with other games and analysis to threats, and finally Section 8 concludes the paper.

3.1. Elements of SREG

In this section, we explain game elements used in SREG. Game elements improve fun, interaction and engagement of the player. We are using several game elements in SREG as follows:

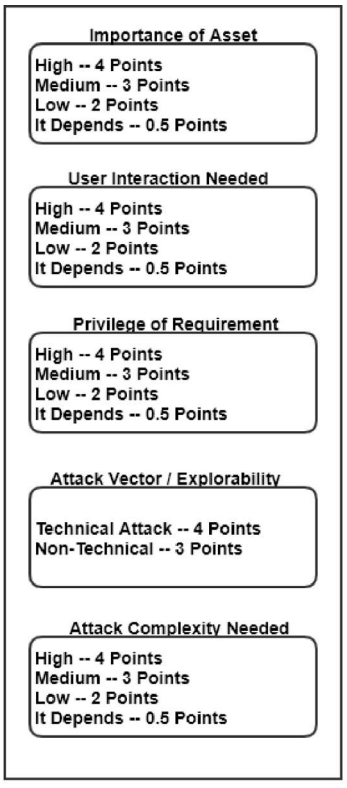
3.1.1. Aggregated attack calculation

Every player is required to calculate for the attack selected by the player. The process of calculation is simple; players are given options; including but not limited to Attack complexity. They, then, have to select from one of the options (high, medium, low) depending upon their subjective opinion of knowledge. The greater the number of points are, the more difficult and unfeasible to launch the attack. The motivation of doing this is to give players an idea of aggregate attack and a possible way of quantification. Besides this, aggregate attack can be used in future selection of highly important targets. The aggregate value for a suggested attack can have a maximum value of 20 points and minimum value of 5.

Since the player can be a beginner or a novice in security related domains, having too many explanations and options may confuse him or her. To first check the response from the empirical evaluation, we use this simple checklist shown in Fig. 2(a). By including this calculation, the player becomes cognizant of the basic idea of calculation by using a checklist method. Moreover, they can see the important aspect that contribute towards the calculation. In the game, just to give a basic idea of point system, we have given points that depend upon the basic thinking and understanding.

The players of the game can be from a different background (with or without good knowledge of security concepts). To make the player fully engaged in the game and to make him/her not feel stuck at any point, we also give the option of “It Depends”. This option can be used by the player when he/she is not sure about the correct option or even when he or she doesn’t know much of the attribute. If the player selects this option, it will be discussed in the last session of discussion and will be a way of learning for the player.

We have adapted the concept of weighing from the study [31] in which Software Security Evaluation was calculated by using AVT model. Fig. 2(a) shows the card. Further explanation of the aggregated



(a) Aggregated Attack Card

(b) Different type of Attack Cards

Fig. 2. Game elements : aggregated attack card and attack type.

attack card can be seen below:

- **Attack vector / attack exploitability:** Attack of different types is given different weights, depending on the inherent difficulty. For example, network attacks are easier to exploit than internal SE attacks. This basically means that an attacker has to be an employee of the victim company to execute the attack.
- **Attack complexity** is evaluated by individual player based on its difficulty and complexity. Attack complexity refers to the complexity for the attacker to perform the attack.
- **Privilege requirements** is further evaluated according to level of permission required against the systems under attack.
- **Importance of assets** is evaluated depending upon the importance of the asset. Higher importance asset will be marked as maximum points.
- **User interaction** is evaluated depending upon the level of user interaction needed for the attack.

3.1.2. Puzzle cards

To mimic the real life security system in our SREG, we are using the puzzle deck. Players have to correctly complete the word given on the puzzle card to get access to a particular floor or room etc. The motivation of making use of puzzle word is to make use of most common security-related terms and concepts in the puzzle. Not only this, the team members, when working together to solve this puzzle, benefit from collaborative learning and reasonable discussions on other related terms and concepts of security. Fig. 3(a) shows possible option for puzzle card.

3.1.3. Attack types / attack cards

The attack cards are designed in a self-explained way. The card not only explains the attack name but also explains how this attack is carried out with an explanation of few lines. We believe that by reading a detail of the attack, the player gets an elaborative lucid picture of the dynamics of the attack which in turn leads to a deeper understanding of how an attack is made in a real scenario. From the attack cards, our motivation is to make players learn about various types of attack and possible explanation of that attack. This also enhances the odds of the player protecting him/her self in some situations. Fig. 2(b) shows possible option for attack type cards.

3.1.4. Vulnerabilities/weakness of assets

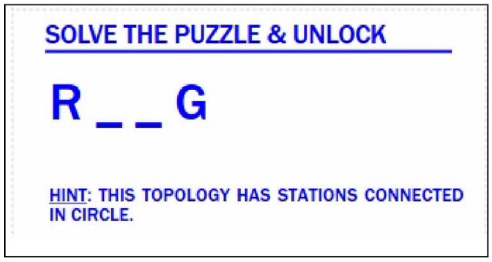
For every asset, either physical, human, or informational, there is some vulnerability attached to it. The motivation is to give a clear idea to the players that every asset has some vulnerability/weakness. By playing the game, the players will get a deeper understanding about how the attacker can take advantage of vulnerable situations. Fig. 4 shows example cards of human weakness and technical vulnerability.

3.1.5. Insider/outsider attacker(s)

Whenever we conceptualize an attack on an organization, we usually imagine someone attacking the network from outside and stealing the information. To give another aspect to the game and to the players, we have suggested two positions of the players: insider position and outsider position. The attacker can be an insider (i.e. works for the organization) or an outsider (i.e. doesn't belong to the organization). The team players may have any combination of attacker position. If an attacker is an outsider, the player needs to start from outside the organization to solve a puzzle. The reverse is true for the insides position. Fig. 5 shows possible cards for attacker.

3.1.6. Virtual identity in game

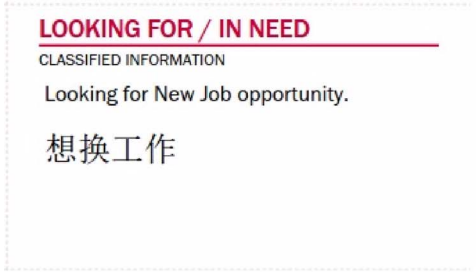
Introducing a virtual identity in the game (for the players) has a positive learning experience for the players [32,33]. In SREG every player in the game is given a virtual identity with special power settings to play in the game. From this perspective, players can play, enjoy, and



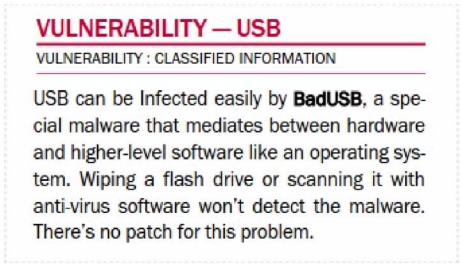
(a) Puzzle Card

(b) Attacker's Various Roles / Virtual Identity

Fig. 3. Game elements : puzzle and attacker role card.



(a) Human Weakness



(b) Technical Vulnerability

Fig. 4. Game elements : weakness and vulnerability card.

learn the various aspects of the game. Fig. 3(b) shows a card with sample identities / roles.

3.2. Capturing the organizational setting with a configurable game map

Organizational assets are humans playing different roles in the organization, while physical and IT assets include physical properties, hardware, software systems, as well as information assets. To secure organizations from attacker(s) (insider or outsider), we need to identify different kinds of valuable assets to be protected. In reality, if we have to secure an information system we have to secure both the human assets and the IT assets from various vulnerabilities and weaknesses; For examples we need to know, the potential motives and alternatives one might have while attacking valuable assets of the organization. Information systems can be accessed by IT products and finally used by human assets. The relationship between IT products and information systems is shown in the Fig. 6. We have tried to map the real world organizational setting in a game map. The map in Fig. 6 shows the floor plan of a hospital. It includes doctors offices, clinic rooms, operation rooms, laboratories, radiology rooms, and server rooms.

In our design, every room contains certain types of assets(Human & IT). For Example, reception room, includes four Human and three IT assets. The detail of the assets can be seen in the map shown in Fig. 6. An enlarged figure can be seen by clicking on **link**[2].

The map is supposed to approximate an organization under consideration. The floor plan can be obtained from various sources, which provides us with the idea that we can just take the floor plan of any company and try to map valuable assets on top of it. The position of the assets is not static. The assets cards can be moved to any room. They can even be removed. We can place the cards on any plane and make our hypothetical floor plan. The motivation for this is to give changeability to the game. Players can have their new map on the plane to play. This context map can be easily extended to include virtual properties, such as the technical architecture of an organization's information systems setting. In this particular example, the map shows a coloured circle on every door of the floor plan, which represents the security system of the room or floor entrance. To cross that passage or to enter into the room, players have to solve one puzzle. By this, we have implemented the security of the rooms or floor. If players successfully solve the puzzle, they can proceed further. The motivation for this step is to give players some real life hurdles, which typically attackers have to face. By understanding the importance of this security checkpoints the players can realize the importance of the security systems installed at various places. We achieved three goals from designing these puzzle card: (i) learning by guessing the security terms on puzzle card; (ii) mimicking the real life scenario of the security system and (iii) introducing fun and collaborative part in the game design. (The team members collaborate to solve the puzzle card)

Let us assume Team-x consists of four players. Every player of the team is given three pieces to move in the beginning: a character card,

Fig. 5. Game element: attacker position.

[2] https://www.dropbox.com/s/e8mjihwwcwgwjat/map.jpg?dl=0.

Fig. 6. A map capturing the organizational context of a hospital.

an attack card and a goal sheet. Every player will follow the process of the game from selection of asset to attack, puzzle solving, etc (explained in Section 4). The collaborative tasks for the team members include: getting help in suggesting the type of attack, writing scenario(s), selecting attack points and, in the end, reviewing other teams goal sheet. In the game context, a player refers to any player playing the game and players refer to the team.

In our game, vulnerability for assets are dynamic. The motivation to do this was to make the weakness and vulnerabilities for assets dynamic. In future, if the players want to change the weakness of human assets, it can be switched easily between human assets or IT assets. Moreover, for IT assets, more than one vulnerability can be associated, and the player can pick one randomly to play. This gives the game a dynamic aspect. The detail of the hospital map can be seen in the Fig. 6.

3.2.1. Example story line of the game

In the example, we assume that the players belong to the team of a Health IT Security Agency. The Agency has received Intelligence news from various sources that one particular hospital is the potential target of attack. The players are instructed to go and evaluate that particular hospital's organizational and informational setting, obtain vulnerability/weakness and, finally, compromise it by suggesting the concrete attack scenarios. The players are working as a team with a common goal to achieve. However, there is competition with other teams. Successful attack scenarios by analyzing vulnerability and situation for assets are the winning criteria.

3.2.2. Example floor plan

The motivation of using floor plan is that by seeing the floor plan of the organization, one can get an idea of the organizational rooms, IT rooms, stairs etc. To mimic a hospital, we believe that using floor plan gives a clear view of the map to the players. Besides this, in our game, we put different types of assets in one room representing real life situation, where in one room doctor is a human asset, mobile phone is a physical asset, laptop and wireless router is a network asset. The detail of the game map can be seen in Fig. 6.

3.2.3. Assets cards (software, hardware, facility, and people)

Using various asset cards ranging from human, software, hardware in the game gives further knowledge to the players regarding how valuable these assets are to the organization. After playing the game a player can eventually identify other organizational assets and have a clear understanding of assets and its importance. Fig. 7 shows sample assets cards.

3.2.4. Leader/captain in game

In SREG we have used a leadership card for the team leader (captain) reflecting the vertical leadership, which means that one player will be the leader of the team [34]. When the game starts, team players will decide and select the leader by mutual understanding and discussion. After that, the team players under the leadership of their captain will work together in achieving the common goal.

Games are enjoyable and fun due to the presence and contributions of certain game elements [15]. In Table 1, we have not only listed the game elements but also provided the logic whereby we have implemented and adopted the game elements in our design.

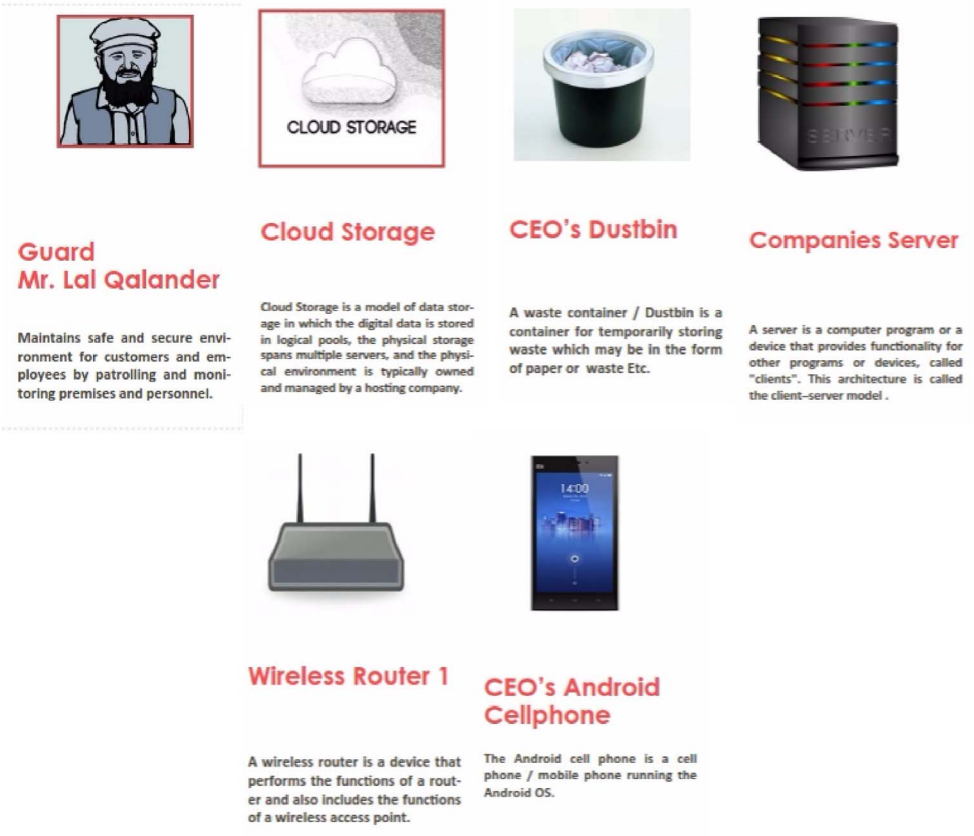


Fig. 7. Game element: assets card of SREG.

Table 1
Game elements used in Security Requirements Educational Game (SREG).

Game elements	Explanation	Usage in SREG	References
Badge	Players get a badge randomly at the beginning of the game.	Attacker type (Network, Physical Etc.) Attacker Position (Inside or Outside)	[15,35,36]
Time constraint	Each step of the Game has time limit.	1. Reaching the target asset within 20 min. 2. Suggesting an attack within 15 min 3. Writing hypothetical scenario and filling goal sheet in 15 min	[15]
Limited Resources	Player has limited Limited life, coin points, weapon, and ability in games.	Limited numbers of attacks to select depending on vulnerabilities of assets.	[15]
Turns	Multi-player take turn	Team members take turns to present their attack	[15]
Clear Goal	The Goal for each player is clear	Clear Goal for player. The player has to go and compromise the target organization's valuable asset.	[15,37]
Variety of Styles	The structure of the organization, the difficulty level is changeable.	Attacker type, Attacks pool, the map of the game, the combination of attacks vulnerability, assets and allowed all correspond to variety of styles.	[15,37]
Challenge	Obstacle in game Course	Challenge is to Solve the puzzles in the game to gain access to assets. Second challenge is to accurately filling the goal sheet.	[38,39]
Fellowship	Social Framework	Team members work together to achieve the common goal of compromising the particular assets; to identify the issues in opponents goal sheet in the review session	[36,39]
Fantasy and Narrative	Game as Drama	The storyline and hypothetical environment created for players.	[36–39]
Discovery	Uncharted Territory	Based on the floor map of the hospital, the players have to discover the target, path and cooperate with other team-members to achieve the goal and win the game.	[39]

4. SREG process

Players take the role of attackers. All the players (of a team) have to play via pieces, and they get to their turn in a clockwise fashion. The first player first takes turn and then the second player of the same team takes the next and so on. All the players have to select one target from the organization's assets. Attacker makes a choice by selecting the particular asset of the organization since every asset has a vulnerability associated with it. As this is a collaborative team task, all the team players, besides selecting and targeting different assets, can collaborate and discuss the selection of attack and the hypothetical scenario writing.

Once a player identifies the target asset, the victim, and his/her vulnerability, then the player has to calculate the aggregate value for the proposed attack. After writing the type of Attack, player has to rank the attack attributes on the basis of points such as attack complexity (high, medium, low, depends), privilege requirements (high, medium, low, depends), importance of Asset (high, medium, low, depends), and user interaction (Direct Interaction, indirect interaction, no interaction, it depends). These points are calculated depending on the knowledge and experience of the player. This step in game mimics the attack element in the Security Requirements Ontology as shown in Fig. 10. In the next step, players write the scenario: how they will use the attack type and their execution of the attack type, the vulnerability and asset (s) attacked to achieve the target. Finally, there is a review process where all the team members discuss the goal sheets of the opponent teams and suggest if they find any issue or want to make any changes. After completion of this step, discussion among the team(s) take place regarding the improvement in the goal sheet, security of the assets, type of attacks selected, and the scenarios. The above steps of the game map onto Security Requirements Analysis process. Moreover, the scenarios developed by players can vary with every player of the game as it depends on the selection of asset to be attacked by each player. Also, the selected asset has associated vulnerability (which can make a different situation for a player to suggest attack type and hypothetical scenario). So, for example, if four players are playing a game in a team A, all the players will play and attack the organization's assets. At the end of the attack, the team will get four goal sheets which actually is the number of players.

The simplified version of the game process is shown in Fig. 8 and detail of the process is summarized in Fig. 9 for better understanding.

Steps 1 and 2: goal and target identification: One of the primary goals of the game is to "Educate Players about Knowledge of Security Attacks". In the goal sheet given, the player identifies his/her target asset in the organization according to the attacker type. The player is given a card indicating whether he is an inside attacker or outside attacker. Depending on the card, he gets a different starting point. The internal attacker will start somewhere inside the organization, whereas the outside attacker will initiate the game from outside the organization.

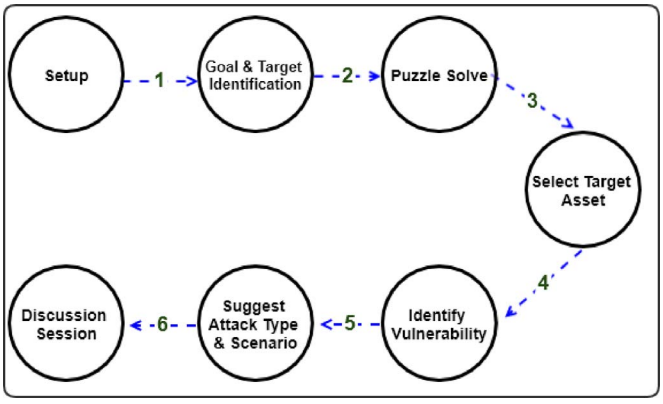


Fig. 8. Security requirements educational game process - simplified version.

Steps 3 and 4: solving puzzle and reaching room of the asset: The player moves towards the target asset on the map (according to his free will choice). The player needs to put the piece at the entrance of the selected room only. The player is required to "Solve a Puzzle Card". This shows that in order to proceed or to access some room, one has to solve one puzzle card, and mimic how real life security system work. The attacker, after reaching the room of the target asset, has to undermine the security system in order to get access of the room or floor.

Steps 5 and 6: vulnerability identification and selection of appropriate attack: In this step, the player has to see the vulnerability/weakness of the target asset by swapping the card. After getting the information of the asset persona, the vulnerability/weakness, the player has to suggest the most accurate attack from the attack cards available to the player in that particular situation. In game context, player refers to the member of a particular team-x and there is a turn per player (of the team).

The map already has printed assets in particular portions or area of the organization (shown in map figure). Besides this, we have designed assets cards which are placed in the same position as shown on the organizational map. These cards have the figure of the asset and the description on the front side and the particular vulnerability of the asset on the back side. By swapping the asset cards, the player will get a particular vulnerability of the asset.

Steps 7, 8 and 9: discussion, rating and writing up attack: After selecting the appropriate attack, the player has to discuss the selection with other team members and with the captain of the team. After discussion, the player has to write the attack on the goal sheet. After proposing the type of attack, the player has to aggregate the attack points. Depending upon the scenario suggested by the player, the aggregation of attack point is calculated. The aggregation of attack point is calculated by using the five elements given in Fig. 2(a). This calculation is based on the experience/knowledge of the player. Then, the player has to write a hypothetical scenario of the situation. The player has target asset, persona, vulnerability, and attack type as a starting point.

Steps 10, 11 and 12: exchanging and reviewing opponent teams work: Teams change the goal sheet between them. Players start discussing the goal sheet of the opponent team and try to identify issues and possible suggestions for the opponent team. In this step the team gives back the issue sheet to the opponent team for their point of view.

Steps 13 and 14: discussions: In this step, the two teams discuss the possible issues/suggestions and further improvements, if any. Both teams discuss the feasibility of the attacks and further come to a common conclusion. Players discuss possible security vulnerabilities of asset and possible security measures taken in response. The rectangular box in Fig. 9 has different colour which represents that this step is undecided and depends on situation and scenarios.

Besides the feedback and the discussion, these scenarios are further given points depending upon their viability, intensity, and completeness as suggested by the reviewer team. These points help to rank the teams. Furthermore, in future version of the game, we are planning to design level system for the game, where we use a formula involving attack points and these points to suggest the next target of the organization.

5. SRE game elements and design rationale

In this section, we present the detailed game design based on the established body of Security Requirements Engineering (SRE) knowledge [15]. In particular, we introduce the core concepts of existing security requirements ontologies and the SRE analysis process.

5.1. Concepts in security requirements ontology

Ontology represents a conceptualization of a particular domain. In

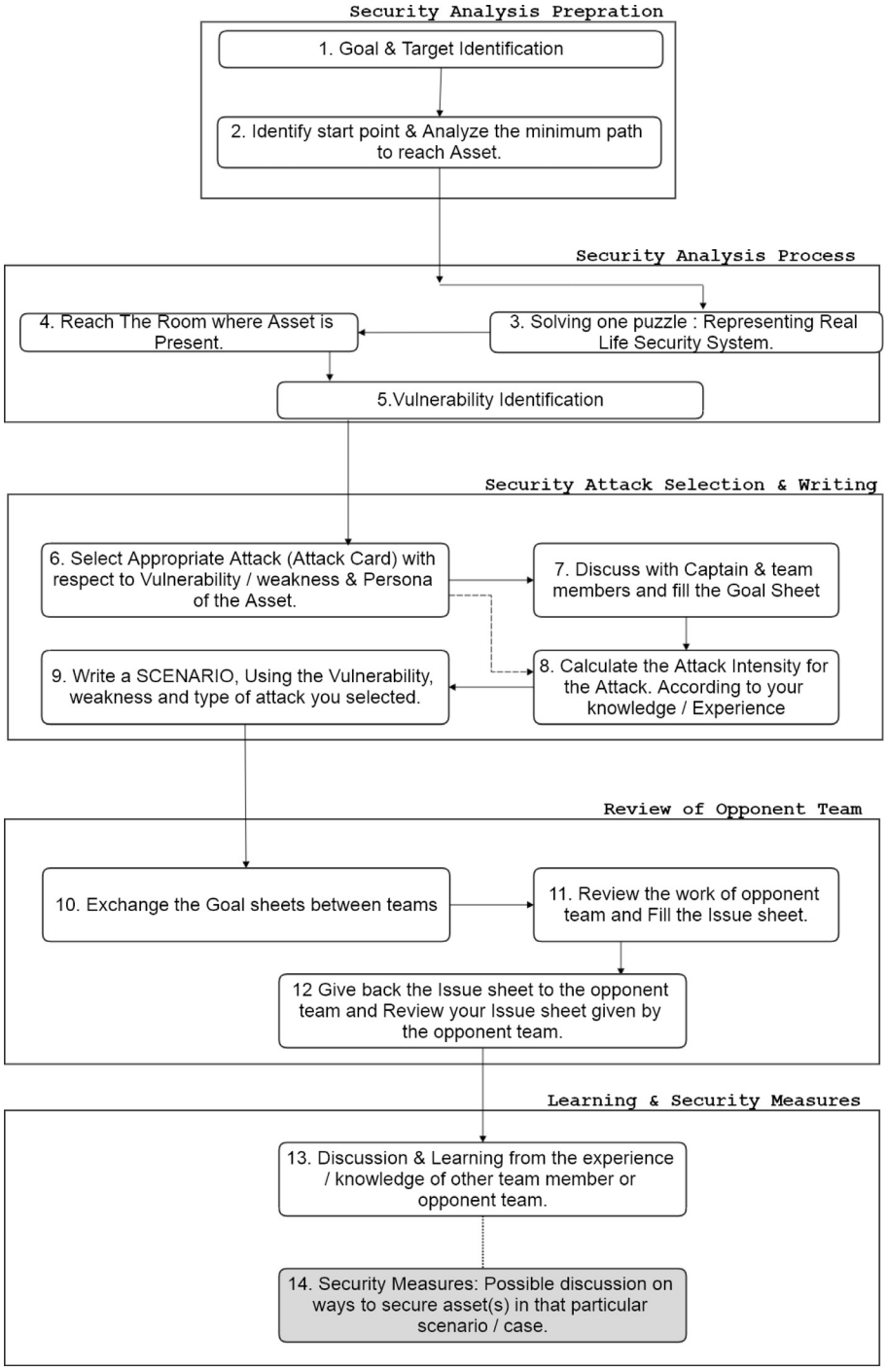


Fig. 9. Security requirements educational game process - detail version.

order to create a comprehensive security requirements educational game, game elements have to cover essential concepts of existing security requirements ontologies. Currently, more than 20 security requirements modeling languages have been proposed [40,41]. Despite the specific focuses of each proposal (e.g., risk-oriented, web-oriented), an essential common set of security requirements concepts has been recognized by the majority of existing ontologies. The set includes the following:

- **Asset:** A valuable thing which can be tangible or intangible, e.g, human or IT products.
- **Vulnerability:** The vulnerability is the shortcoming of an organizational asset to withstand the attack. Vulnerability of the asset which can be exploited by attacker(s). Vulnerability depends upon type of assets,e.g, Human or IT product.
- **Threat:** Threat is the danger or fear with respect to loss or damage to the assets. A threat may be accidental or intentional.
- **Attack:** An attempt in which one entity wants to harm **red**or to get control the assets of the organization.
- **Security objective:** What stakeholders/organizations want to achieve with respect to security.
- **Security requirements:** Requirements are the conditions that need to be filled in-order to attain the security goal or objective.
- **Attacker:** Attacker is the person who tries to get control of the valuable asset(s) of the organization or tries to damage or cause harm to assets. For a Denial-of-Service attack, we will define the availability of a given service as an asset to protect, and the vulnerability of that attack will not be a constraint on the flood of service

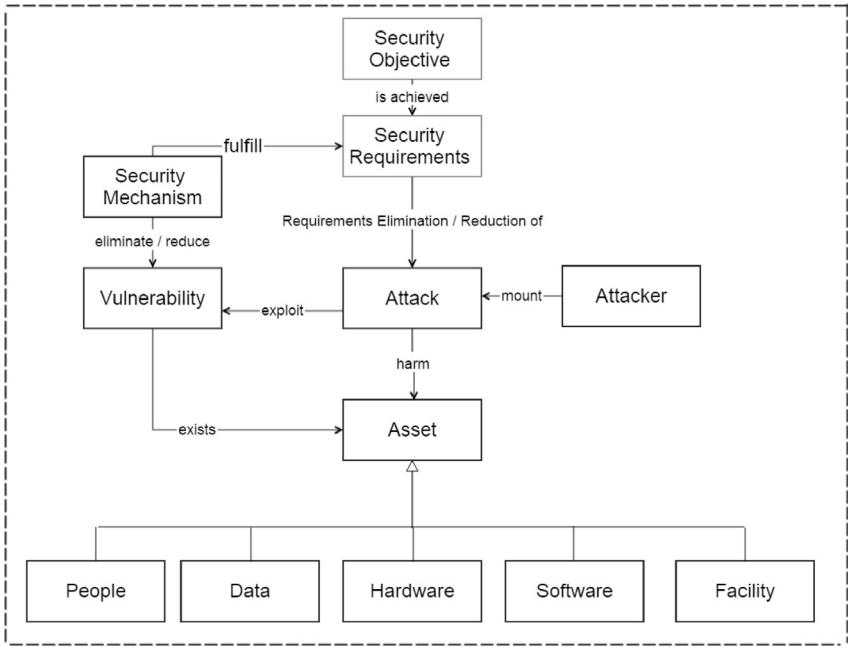


Fig. 10. Concepts in security requirements ontology by Firesmith [41].

requests. In other words, assets can be intangible as well.

SREG is based on concepts from the Security Requirement Engineering Ontology proposed by Firesmith [41] and Souag et al. [42].

5.2. SREG game ontology

To adequately reflect the security ontology concepts in the game, the existing security ontology is analyzed thoroughly. Some of the concepts inherently correspond to game elements, such as assets of the firm/organization, which may be human, software, or resources. Another example of one to one mapping is security mechanism. Real life physical security systems were mimicked by placing various puzzles in the way of attackers as obstacles for them to access the asset in the game. Some of the concepts cannot be directly mapped to the elements of the game, such as vulnerability of the IT asset and weakness of the human assets. To comply with the ontology elements, these elements in the game are associated with the assets as property. The front side of a card shows the picture and explanation of an asset and the backside explains the vulnerability/weakness of that asset. In SREG, some of the game elements are the extension or instantiation of the original security ontology as proposed by Firesmith [41] and Souag et al. [42]. Examples, include attacker type and attacker position. To give a real feeling to the game, players Attacker type was further decomposed into network attacker, physical attacker, and social engineering attacker. Similarly, attacker position was further extended by insider attacker or outside attacker. The detail of the extended version of the ontology are illustrated in Fig. 11. We also developed the knowledge model of the SREG in Protégé by using the ontology in Fig. 11. The aim of this knowledge model is to convey a clear understanding regarding the game relations and explanation of knowledge base. The files can be assessed as a supplementary material or they can be found online here.

5.3. Mapping security requirements engineering process

To develop the game process and to align it with the original process, we analyzed various security processes mentioned in literature, summary of which is shown in Table 2.

After analyzing existing security requirement engineering process, we came up with a process which inherits the merits of two security requirements processes. One is proposed by Haley et al. [43], and the other is proposed by Boström et al. [44]. The primary motivation to merge these two SRE processes was to get better coverage with respect to knowledge while designing the game. The detail of the mapping between these processes and our game is shown in Table 3. In Table 3, '✓' represents the presence of that phase in the game and 'X' represent absence of that phase in the game.

- **Definition of concepts:** Definition of critical assets and concepts etc. SREG does not have any formal definitions; however, the concepts are implicit in the description of the game rules and mechanisms. The definition of critical assets can be found in game rules and manual.
- **Business objective:** Objectives refer to high level (business) goals of the organization. In SREG, the objective of an individual player is to compromise the assets of the organization by exploiting their vulnerabilities. Furthermore, the objective of the game is to let the player understand the business objective of the organization and improve their awareness of security risks.
- **Misuse/threat modeling:** Violation of security criterion is the danger with respect to loss or damage to the assets. The threat may be accidental or intentional. SREG supports the modeling of misuse cases and potential threats. This can be seen in the vulnerability cards and user planning phase.
- **Assets identification:** Identification of the potential assets of the organization. In SREG, players got the potential knowledge of different type of assets (human, IT etc). Also, this asset identification can be seen in the Assets cards.
- **Coding standards:** This includes the possible languages to use in order to avoid any mishap or attack. In SREG, this phase is mapped in the group discussion section where team members discuss about possible attacks etc.
- **Categorize and prioritize:** Categorize and Prioritize the security requirements depends on the organizational experiences and stakeholders knowledge. In SREG, players, while selecting the target, have to first categorize the potential target according to the specialty of the role and, then, prioritize by choosing the one attack card to initiate attack.
- **Inspection and validation:** Inspect and Validate the agreed upon requirements with respect to major stakeholders. This phase in SREG can be seen during discussion between teams, where teams analyze and discuss. Where teams analyze and counter-part team

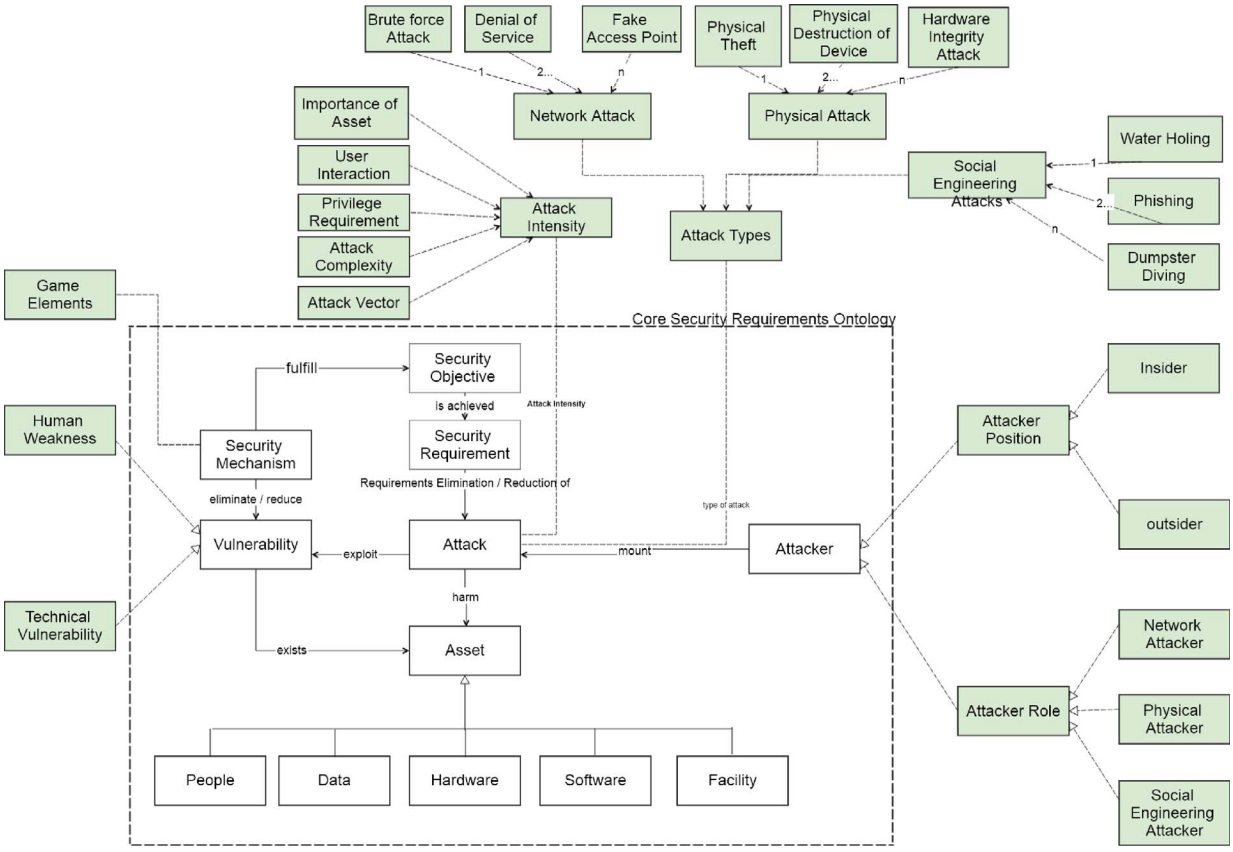


Fig. 11. Security requirements engineering ontology in SREG [41].

Table 2
Different approaches handling different phases of requirements engineering [45] - A summary.

Approach	Definitions	Objectives	Misuse Threats	Assets	Coding Standards	Categorize & Prioritize	Inspect & Validate	Process Planning
SQUARE	✓	✓	✓			✓	✓	
Charles Haley et. al		✓	✓	✓			✓	
Boström et. al			✓	✓	✓	✓		
CLASP		✓		✓			✓	
Microsoft		✓	✓	✓				✓
Axelle Apvrille and Makan		✓	✓			✓		
Eduardo Fernandez			✓					
Kenneth Van Wyk and Gary McGraw			✓					
Gunnar Peterson			✓					
Abuse Case [46]		✓	✓			✓	✓	
Security Misuse Case [47]		✓	✓			✓	✓	
Becker et al. [5]		✓	✓	✓		✓	✓	

validate and suggest the possible alternatives.

- **Process planning:** This phase includes, process planning for the security related activities. After playing SREG, the players might have better understanding and knowledge for planning the security requirements engineering process as this is the design rationale of the game.

5.4. SREG activities

Research in software project management and related fields have explored the process and strategies by which the efficiency and performance of the teams may be increased. Team building activities help in raising profits [48]. Researchers suggest proven strategies for team building activities [49] and discuss the team building processes [50].

We have realized the importance of team building activities and

Table 3
Game process alignment with Security Requirements Engineering (SRE) Process.

SRE process	Boström [44]	Haley[43]	Presence in SREG
Definition of Concepts	x	x	Game Rules and Manual
Business Objectives	x	✓	Game objective
Misuse/Threats Modeling	✓	✓	Vulnerability Cards
Assets Identification	✓	✓	Assets Cards
Coding Standards	✓	x	In group discussion
Categorize and Prioritize	✓	x	Victim selection & Aggregate attack Card
Inspection and Validation	x	✓	Inter teams discussion
Process Planning	x	x	Design Rationale of Protection

Table 4
Team building activities in Security Requirements Education Game.

Activities	Presence in SREG	Reference
Planning	In our game players are required to make the team plan and then start and achieve the common goal. This team building activity is carried out throughout the game process. Planning for target selection, planning to choose the gate to enter, which path to take, target selection Etc.	[48,51,52]
Communication	Communication between the team members is the vital part of our game. From the start of the game till the last session of discussion every phase requires an intense discussion and communication between team members.	
Problem Solving	The challenge is placed in the game so that team members can work together to solve the puzzles. Not only solving puzzle is the challenge but suggesting accurate attacks for the vulnerability is also a challenge which eventually results in winning or losing the game.	

tried to cover this concept in our game by assigning teams to achieve a common goal.

A traditional type of team building activities discussed in the literature and which our game followed is discussed in Table 4.

5.5. Other motivational rationale

5.5.1. Scenario Based Learning (SBL)

Scenario Based Learning is used extensively in industry and enjoys a reputation of one of the most productive ways of training and learning [53,54]. In our study, players of the game gather information from the game based environments. One of the learning goals of the SBL is to make players think like an attacker, so that, by playing the role of the attacker, they would learn attackers' perspectives.

5.5.2. Players intrinsic motivation

Motivation is a key pre-requisite for players to learn. Without motivation, it is hard for players to learn the concepts embedded in the game design. According Kuvass et al. [55], participants must address intrinsic as well as extrinsic motivations. To follow the suggestions of this study, we filtered the participants by using the email system. If the participants were motivated enough, they responded by an email to take part in the activity. Their prior motivation was then supplement by game design concepts which essentially acted as extrinsic motivation.

5.5.3. Motivation for using Blooms Taxonomy

In [56,57] Anderson et al. proposed a taxonomy based on Blooms Taxonomy. The taxonomy is shown in Fig. 12. The taxonomy shows different learning levels. If we compare this with scenario based learning process adopted in the game, the players first have to evaluate the situation in the game. Secondly, they need to analyze and apply their knowledge to generate attack scenarios. Once the players have written the scenarios, discussion between the participants takes place which helps players understand, explain, and possibly remember the situation and the learning outcomes. Thus, the design follows the learning level as proposed in [56,57].

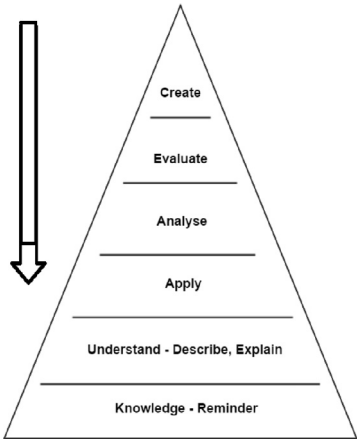


Fig. 12. Learning level based on Blooms Taxonomy.

5.5.4. Motivation for using collaborative game based learning

An experiment performed on students using game-based learning activities in the past has shown significant positive results in student performance [58,59]. The same motivation was taken for our game. One of the sub-goals is to provide a collaborative learning environment for the players so that the players can enjoy and learn security related concepts.

5.5.5. Motivation for using common goal to achieve / achievement

The experiment was performed to observe the relationship between goal commitment and team effectiveness criterias such as task interdependence, role mediation between players, etc. It was found that goal commitment is positively related to task interdependence and role mediation [50]. To improve the commitment between the players in our game, we followed the same results from [50]. We provided the team one goal to achieve. To achieve that particular goal the team members have to support other players in their tasks, eventually increasing the team effectiveness.

5.5.6. Knowledge model of persuasion

To make the SRE game persuasive for the players, we have followed a Knowledge model given by Conde-pumpido [60], shown in Fig. 13. This onion model is explained in three spiral layers; the inner most layer is about signs in the game which includes visual, haptic, linguistic, and sound; the middle layer talks about the system of the game which

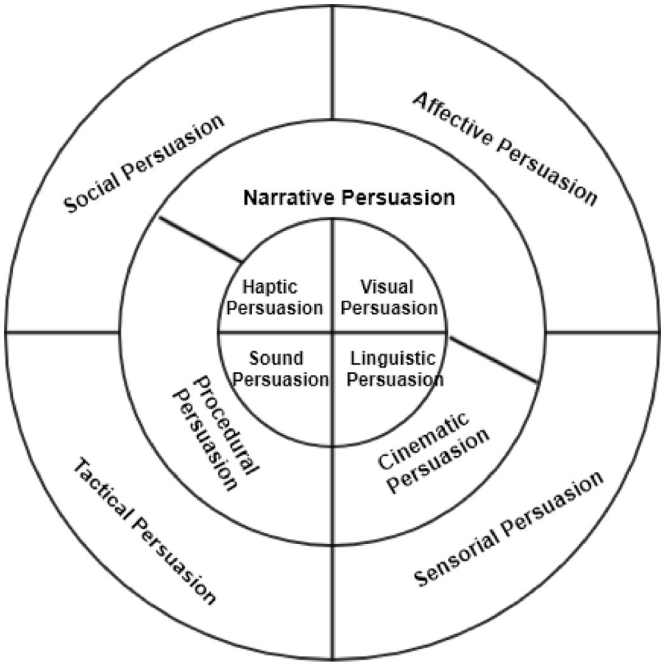


Fig. 13. Knowledge model for persuasive game - Teresa De La Hera model

includes scripts and scenes of the game; and the outer most layer speaks of the setting of the game. We have used visual persuasion to satisfy the first layer in SREG game. As this is a card game, any other type of signs such as sound and linguistic were not possible. From the second layer, we have used Narrative and Procedural persuasion for our card game, and from the third layer, we have used tactical and social persuasion.

5.5.7. Motivation for using random attack cards

In the start of the game, every player of the team has been given a random sheet of attack cards. The sheet contains four different types of attacks which may belong to Network Attacker, Physical attacker, or Social Engineering Attacker. By giving random cards to the players, players will have a diverse knowledge of different attacks and different situations to handle. Besides this, randomness in the game further increases the curiosity of the players.

The game is designed in a way that team players can achieve a common goal by collaborating. The last part of the discussion in the game can be more effective if every team has at least two players.

5.6. Adding various attack cards from literature

In SREG, we include three types of attacks, namely Social Engineering attack, Physical attack, and Technical attack. Social Engineering is the art of manipulating people to perform actions you desire them to do. Social Engineering Attack framework captures the way a particular attack usually takes place. SREG follows social engineering attack framework proposed by Mouton et al. [61]. The aim is to align the game processes with the published security related processes.

To select the type of **social engineering attacks** for the card game, we searched for the famous social engineering attacks in the published literature and further shortlisted them on the basis of complexity. In order to make the learning curve of the players smooth, we included the social engineering attacks mentioned in the Table 5.

For **physical attacks** selection, we go through one of the most comprehensive attack knowledge repository known as Common Attack Pattern Enumeration and Classification (CAPEC). As the next step, we further explored the published literature. Table 6 shows the types of attacks selected for the game and their reference from the literature for further authentication.

Similar process was repeated for the **technical attacks**; however, this time for the inclusion of the technical attacks, we discussed the attacks with one of the specialists of network security and finally selected the most relevant type of attacks. Details of the types of attacks and the references can be seen in the Table 7.

6. SREG empirical evaluation

Fig. 14 shows the research model for our game, as our statements (S) and their contribution towards the intended learning goals. In order to test our statements that “SREG game is fun to play”, we asked the players to fill out a questionnaire to have their feedbacks. Player after playing the first time, in test session, would like to try it in future, and by playing SREG game it increases their security knowledge as well. Furthermore, having a common goal between players and working as a team increases the collaboration and motivation of the players to achieve the goal.

6.1. Controlled activity design

The design questions of the SREG is the following:

Goal: Feedback of Game

S1: Security Requirements Educational Game is enjoyable to play. (For responses see Fig. 15)

S1.1: Players can follow the game procedures easily.

S1.2: Players find the game fun to play.

S2: Making an effort to win SREG encourages collaborations between players. (For responses see Fig. 18)

Table 5
Social engineering attacks included in game.

Social engineering attacks	References	Explanation
Phishing	[5,62]	In this type of attack, attacker attempts to obtain sensitive information (password,credit card etc.) of the victim usually in electronic communication.
Impersonation	[5,63]	In this type of attack, attacker pretends to be another person for the purpose of entertainment or fraud.
Shoulder Surfing	[5,64]	In this type of attack, attacker use direct observation techniques, such as looking over someone’s shoulder, to get information e.g. Password etc.
Dumpster Diving	[5,62]	In this type of attack, attacker search through commercial or residential waste to find items that have been discarded by their owners, but that may prove useful to the picker.
Pre-Texting	[5,62]	In this type of attack, attacker creates an invented scenario to persuade a targeted victim to release information or perform some action.
Water Holing	[5,62]	In this type of attack, attacker guesses or observes which websites the group or individual often visits and infects one or more of them with malware to get the control of the victims device.
Reverse Social Engineering	[5,64]	In this type of attack, an attacker convinces the target that he or she has a problem (or in future) and he is ready to solve the problem.
Tailgating	[5,65]	In this type of attack, an attacker used to get into the office or some premises by following the authorized person.
Need & Greed Attack	[5]	In this type of attack, an attacker explore for the needs and desires of the victim. Usually needs and desires make people vulnerable. Once an attacker has the information he/she can easily manipulate the victim.
Direct Approach	[5]	In this type of attack, an attacker used to approach the victim and get the desired information.
Distraction Approach	[5]	In this type of attack, an attacker engage in an activity to redirect victims mind/attention.

Table 6
Physical attacks included in game.

Physical attacks	References	Explanation
Physical Theft	[66]	In this type of attack, an attacker gains physical access to a system or device through theft of the item.
Physical Destruction of Device	[66]	In this type of attack, an attacker conducts a physical attack on a device or component, in such a way that it no longer functions as intended.
Hardware Integrity Attack	[66]	In this type of attack, an attacker changes a technology, product, component, or sub-component during its deployed use at the victim location for the purpose of carrying out an attack.
Malicious Logic Indertion	[66]	In this type of attack, an attacker installs or adds malicious logic into a seemingly small component of the system. This logic is often hidden from the victim system and works behind the scenes to achieve target.

Table 7
Technical attacks included in game.

Technical Attacks	References	Explanation
Backdoor Attack	[67]	In this type of attack, an attacker gets an unauthorized access to a system by bypassing normal security mechanisms. This threat works in the background, hiding itself from the user.
Denial of Service	[68]	In this type of attack, an attacker tries to make a machine or network resource unavailable to its intended users.
Fake Access Point	[69]	In this type of attack, an attacker provides a fake access point to attract victims and other wireless users in order to collect information about them.
Brute Force Attack	[70]	In this type of attack, an attacker tries many passwords or pass-phrases with the hope of eventually guessing correctly.
Privilege Escalation	[67]	In this type of attack, an attacker exploits a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.
SQL Injection	[69]	In this type of attack, an attacker inject unauthorized database statements into a vulnerable SQL data channel. These injected statements are specifically crafted to be executed on the database side for malicious purposes.
Trojan Horse Attack	[62]	In this type of attack, an attacker writes malicious computer program which is used to hack into a computer by misleading users of its true intent.

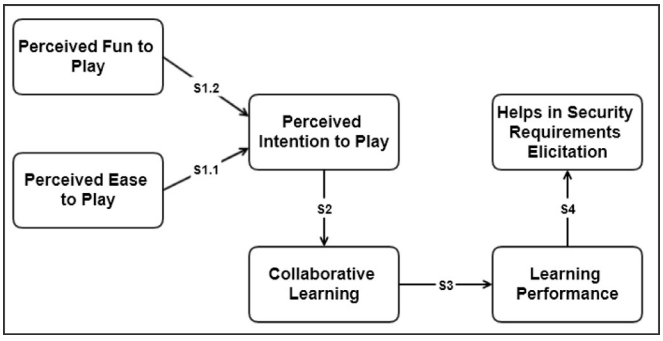


Fig. 14. The research model adapted from technology acceptance model [71].

Goal: Security Education/Training

S3: Playing security card game helps to identify potential security attack(s) in a given situation. (For responses see Figs. 16 and 17)

Goal: Security Requirements Elicitation

S4: Playing security card game helps to elicit security concepts / requirements. (For responses see scenarios made by students)

6.2. Descriptive observation - physical setting

The empirical evaluation was not only designed to know the students liking the game but also to gauge the game's success in educating students about security requirements. For the empirical evaluation, the students were invited by an advertisement which was published on the university notice board and by an email to those taking Requirements Engineering or Software Engineering courses. The total number of requests to participate was further shortlisted by a set criteria i.e. the person is either a student or professional) to make groups. After shortlisting, the team of researchers discussed the need for further inclusion or exclusion of students depending upon their experience and knowledge. In total, 35 requests were received out of which 20 students were shortlisted for the empirical evaluation. However, on the day of the activity only 16 were present. SREG was played by sixteen people in five groups. The class was given a session of about 30 min to explain the goal, motivation, and different type of cards used in SREG. Two mentors were available in the class throughout the session in case any group has a question(s) or confusion. Individual players filled the survey questionnaire after playing the game for about 2 h in the session. The gathered data from students was further analyzed and will be discussed in the Results and Discussion sections. Students answered a series of questions using their mobile or computer devices. The Questionnaire was divided into three sections. The first section asked for demographic and background knowledge of the players. The second part of the Questionnaire asked the players about the experience of playing the game. The third section tested the players knowledge by asking security related scenarios. Questionnaire can be assessed here on the **link**.[3]

6.3. Empirical evaluation results and analysis

6.3.1. Survey results after playing SREG

The scale used to collect the responses of the respondents contains 7-item Likert-type scale ranging from Strongly Disagree, Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree and Strongly Agree. The respondents were 62% male and 38% female. Regarding education level of the respondents, all the respondents had a minimum education of bachelor. 75% of the respondents were students of MS and 25% were student of Ph.D. stream. Furthermore, 69% of the respondents didn't have any prior knowledge of security analysis during system development but 31% had practical experience in security analysis. The players were further divided into five groups. The first group had all full-time students of Master of Science in Software

[3] http://www.surveygizmo.com/s3/3209899/A-Game-on-Eliciting-Security-Requirements-Class.

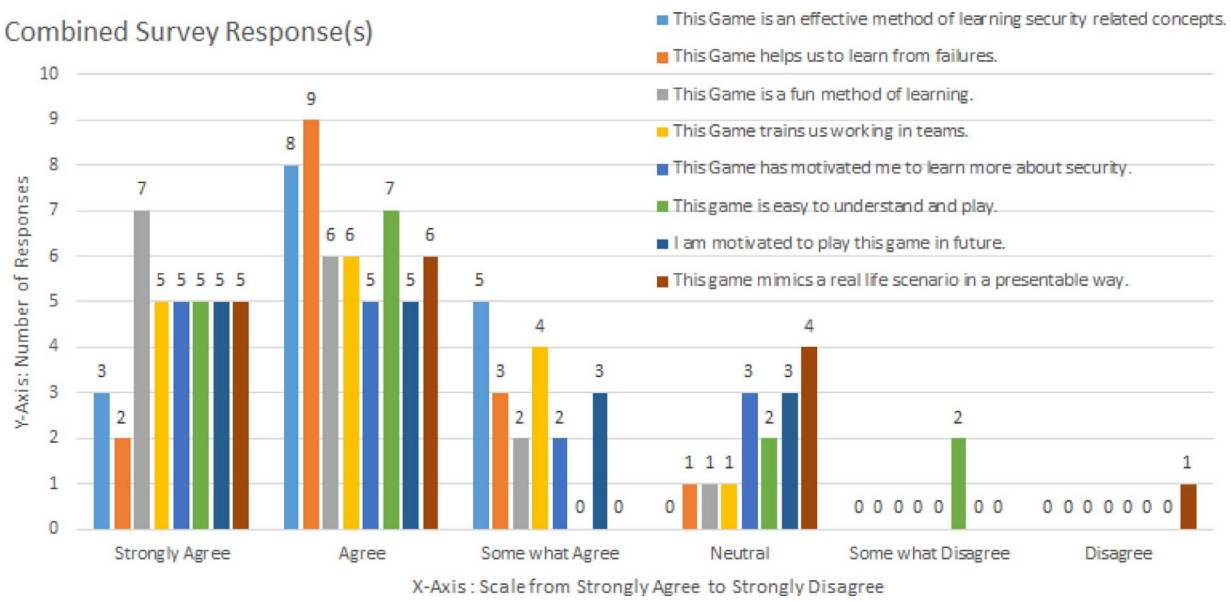


Fig. 15. Survey responses on Security Requirements Educational Game.

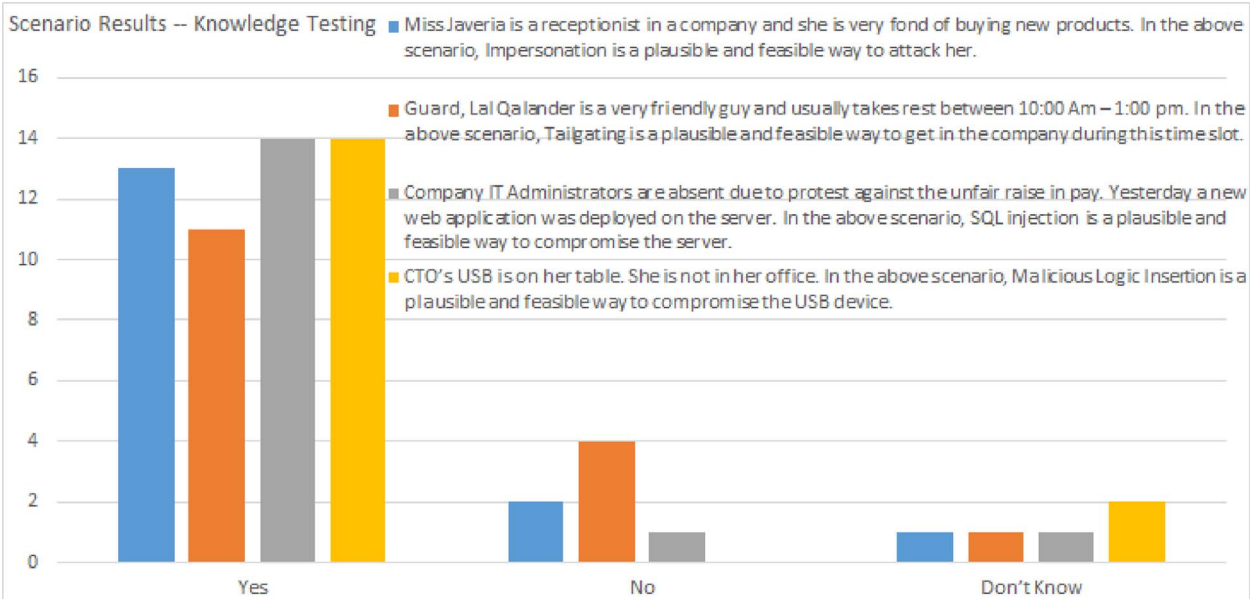


Fig. 16. Survey responses on security related scenarios.

Engineering; the Second Group had all the students belonging to the Ph.D. stream. The third group had players who were studying part-time. The fourth group had participants who were working in software industry. Finally, the fifth group consisted of International students. We believe that this combination of groups gave us balanced participants for empirical evaluation. The decision to divide the participants in five groups was in place to get valuable feedback from different groups.

S1: Security Requirements Educational Game is enjoyable to play. (For responses see Fig. 15)

S1.1: Players can follow the game procedures easily.

S1.2: Players find the game fun to play.

In Fig. 15, the majority of the respondents chose the "Agree" option and no respondent selected "Strongly Disagree" option (Thats why that option is not shown in the Fig. 15). 90% of the respondents responses are within the agree section, which shows a promising result for our SREG game.

Fig. 15 shows that for few options, the trend of respondents shift from agreeing to "Neutral" and "Some-What disagree". By analyzing this carefully, we know that the first survey question which needs to be observed is "The Game is Easy to play and Understand." Few of the respondents selected "Neutral" and "Some-what disagree". This means that there is something complex regarding mechanism or rules or even explanation of the game in the first session that makes them feel this game is complex. From this, we have a clear indication that we need to work on improving the mechanism, rules and even the presentation of the game in a more natural and understandable way.

Secondly, for the survey question "This Game Mimics a real life scenario in a presentable way", four players selected "Neutral" and one player selected "Disagree" option. The possible reason for this is that players only played one round of the game which is the minimum number to play this game. We believe that there is a need to improve the map which describes the context from the literature and represents real life issues and environment.

Thirdly, for the survey question "This game has motivated me to learn more about security," three respondents selected the "Neutral" option. This can be explained by the same reason: players had only

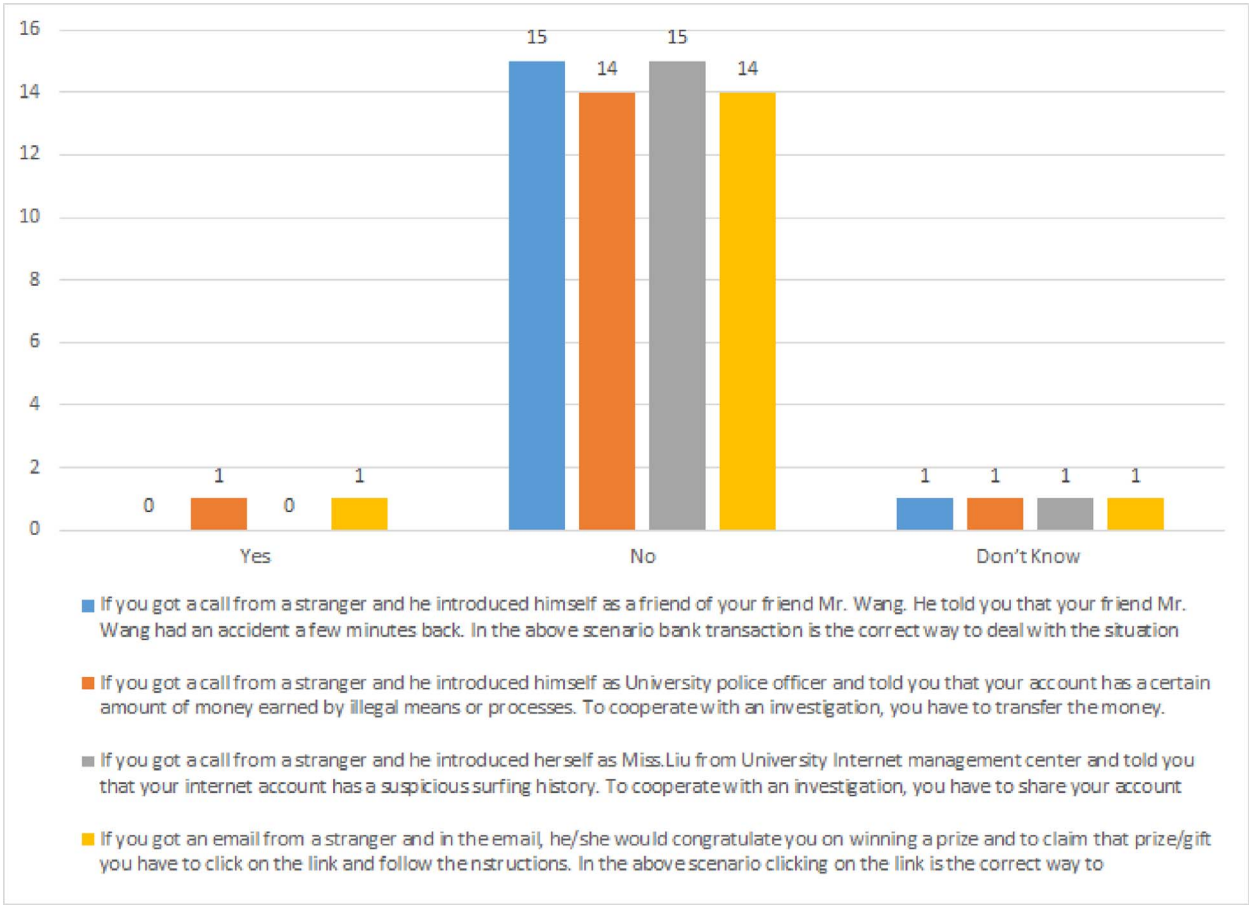


Fig. 17. Survey responses on phone/email scam.

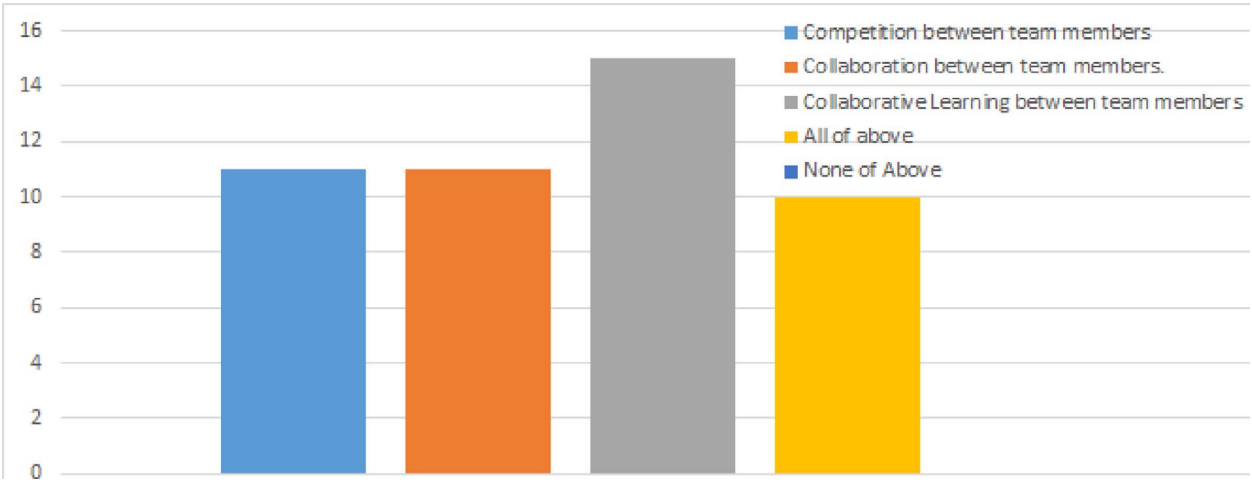


Fig. 18. Verifying competition between teams increase collaboration.

played one round of the game. However, we still need to check further on how can we make this game more enjoyable, so that players may feel motivated to read and learn more about security related stuff.

S2: The attempt to win SREG encourages collaboration between players. (For responses see Fig. 18)

In Fig. 18, our primary goal was to check if the game increases competition and collaboration, within team members. The motivation for asking this question is to check the effectiveness of the game elements embedded in the game design. Furthermore, the respondents can select one or two options or all of above as it is a multiple choice question. From the responses, the competition for winning the game has a positive impact on collaboration within the team members.

S3: Playing Security Card game helps to identify potential security attack(s) in a given situation. (For responses see Figs. 16 and 17)

In this section, students were given example scenarios. Each Scenario was used to check the attack-based knowledge of the respondents. The respondent was given a complete scenario and, in the end, asked whether in a particular situation this particular attack is feasible and plausible to use. The detail results and scenarios can be seen in the Fig. 16. For most of the options in this section, respondents have selected the correct options. Nevertheless, if we closely analyze the “Dont Know” side of the bar chart, there is one respondent who

selected Dont Know for every option. This may be the reason that the respondent has just filled the survey for fun, but we still mark this as the point of improvement for our game. For Fig. 16, correct answers for all the given scenarios are YES.

In this section, students were given four scenarios. Each scenario was based to check the knowledge of Email/Phone scam of respondents. After given a specific scenario, the respondents were asked if transferring bank account and clicking on the link was the better solution. The detail results and scenarios can be seen in the Fig. 17. Furthermore, if we closely observe the responses and especially the section of "Don't Know" part, we can see that trend of selecting the "Dont Know" option by one respondent is consistent. There may be many reasons of this behavior of that survey respondent. This may be for fun to select all these options or may be any other possibility regarding unusual behavior. For Fig. 17, correct answers for all the given scenarios are NO.

6.3.2. Scenarios developed by students

S4: Playing security card game helps to elicit security concepts and attackers intentions. In the empirical evaluation, students developed the scenarios which included social engineering attacks, network attacks, and physical attacks. Below mentioned are few scenarios developed by the students. To analyze the scenarios developed by the players, we deciphered the most important information from the produced scenarios.

Scenario 1: An insider attacker trying to challenge authority had identified an attacking strategy of using brute force to access classified information. Essentially, the attacker is a network administrator who managed to intercept sensitive information (passwords, credit card numbers, and classified emails) from the organization's LAN by planting a falsified Wi-Fi router. The attack can be mitigated by security protection of network devices and network traffics. Table 8 extracts the important information from the scenario 1 developed by players.

Scenario 2: Another insider attacker tried to disguise as a Trojan program which he/she had planted in the corporate information system by social engineering approaches. Essentially, he pretended to help an intern in the organization to fix his bugs by running a malicious script, so that the intern can attend a corporate job affair in the afternoon. Table 9 extracts the important information from the scenario 2 developed by the players.

Scenario 3: An outsider attacker intended to cause damage to a competitor's corporate information system using the foot-printing attack to break into the network of the organization. He/She conducted SQL injection to obtain user account information and to escalate his privilege to get valuable information. Table 10 extracts the important information from the scenario 3 developed by players.

Scenario 4 - Target asset - Employee info, confidential data, file of the company, etc: The attacker intrudes into the company's network by "Foot-printing" through the WIFI router in room 11-417, gets the users information by SQL Injection, and gets advanced authority through the abuse of access authority to get more valuable information. Table 11 extracts the important information from the scenario 4 developed by players.

Scenario 5 - Target asset - Data in the company's database: An attacker can occupy the IP of someone after he establishes a connection to the database. (Just like University network account). Table 12 extracts the important information from the scenario 5 developed by players.

Scenario 6 - Target asset - Important document of the project: The insider attacker can threaten the trainee that he has made a terrible mistake while coding which may lead to serious repercussions that the attacker hasn't conveyed to the manager. However, to save the stuck trainee the attacker can help to fix the problem. Then he finally gets the document and has a chance to change the source code of the project.

Table 8
Deciphering attack scenario developed by players - Scenario 1.

Deciphering attribute	Details
Attack Medium	Indirect communication.
Target Asset	Organization network.
Attacker	Inside attacker.
Goal	Getting critical information of organization.
Technique	False Wifi Network.
Psychology / Compliance Principle	N/A.

Table 9
Deciphering attack scenario developed by players - Scenario 2.

Deciphering attribute	Details
Attack Medium	Face to Face communication.
Target Asset	New Internee.
Attacker	Inside attacker.
Goal	Getting critical information of organization.
Technique	Reverse Social Engineering Attack.
Psychology / Compliance Principle	Trust, Social Compliance, Helpful.

Table 10
Deciphering attack scenario developed by players - Scenario 3.

Deciphering attribute	Details
Attack Medium	Indirect communication.
Target Asset	Getting Access of organization's Database.
Attacker	Outside attacker.
Goal	Getting critical information of organization.
Technique	SQL injection.
Psychology / Compliance Principle	N/A.

Table 11
Deciphering attack scenario developed by players - Scenario 4.

Deciphering attribute	Details
Attack Medium	Indirect communication.
Target Asset	Organization network.
Attacker	Outside attacker.
Goal	Getting critical information of organization.
Technique	SQL injection.
Psychology / Compliance Principle	Not applicable as network attack.

Table 12
Deciphering attack scenario developed by players - Scenario 5.

Deciphering attribute	Details
Attack Medium	Indirect communication.
Target Asset	Organization network.
Attacker	Outside attacker.
Goal	Getting access to organization database
Technique	Footprinting
Psychology / Compliance Principle	Not applicable as network attack

Table 13
Deciphering attack scenario developed by players - Scenario 6.

Deciphering attribute	Details
Attack Medium	Direct communication.
Target Asset	Project documents.
Attacker	Inside attacker.
Goal	Getting access to project. documents.
Technique	Pre-texting.
Psychology / Compliance Principle	Panic / Time pressure.

Table 14
Deciphering attack scenario developed by players - Scenario 7.

Deciphering attribute	Details
Attack Medium	Indirect communication.
Target Asset	Money.
Attacker	Outsider attacker.
Goal	Getting access to money.
Technique	Pre-texting, Impersonation.
Psychology / Compliance Principle	Trust, Need & Greed.

Table 15
Deciphering attack scenario developed by players - Scenario 8.

Deciphering attribute	Details
Attack Medium	Direct communication.
Target Asset	USB.
Attacker	Inside attacker.
Goal	Damage USB.
Technique	Physical destroying the USB.
Psychology / Compliance Principle	Not Applicable as its physical attack.

Table 13 extracts the important information from the scenario 6 developed by players.

Scenario 7 - Target asset - Financial gain: The outside attacker pretends to be a member of the staff of an international office of a prestigious college. He, then, asks the marketing manager to apply for a scholarship and ultimately, defrauds her. Table 14 extracts the important information from the scenario 7 developed by players.

Scenario 8 - Target asset - USB disk: An inside attacker assaults the USB directly to cause damage. Table 15 extracts the important information from the scenario 8 developed by players.

In Fig. 19, we have created a word cloud from the scenarios made by the students. From the word cloud, we can see the thinking process of the players as well as the areas that they considered during writing the scenarios. If we look closely, we can see that players have used a lot of attack names such as SQL, physical, pre-texting, insertion etc. Besides this, the players have used words like marketing, outsider, router, help, insertion strategy, malicious, theft, website, access, altered, attack, inject, documents etc, thus, giving us an indication that players have made diverse scenarios. The scenarios may not be accurate at this point but the SREG game, has given the participants a path to think, learn, and save themselves in future.

6.3.3. Observations

The observational method is a qualitative method derived from the field of anthropology and is used where we need to study human behavior in a particular environment. This method helps understand the in-depth feedback in the form of comments, facial emotions, discussion, feedback, etc. [72].

In our study, two researchers are playing the role of observer. One person sits in a group, and observe how team players interact and conduct the required game activities. One person is walking around, and observing the differences among groups in terms of group dynamics. The third person is responding to questions about game rules and controls the time and pace of the game.

The important primary observations which all the researchers agreed upon are given in Table 16. These are the major questions raised by the game players during the game process, which indicate issues to be resolved. The four questions belong to four different areas: card design shall avoid misleading images or icons; game processes shall be clearer and indicative, in term of next step and termination; Inter-group communication shall be facilitated better in multi-language settings and game design in general must be improved further.

Based on researchers observations we have identified following secondary observations:

- **Accessibility problem in Game Design (GD):** First observation from the empirical evaluation is that technical writing as the vulnerability of IT assets is difficult to understand. The sub-goal for the next version is to represent vulnerability of IT asset in a way which can be easily understood and remembered. For example, there may be various technical vulnerabilities of database. Besides this, other ways to improve awareness is by adding common mistakes, such as forget to change the default password to access the database etc. Everyone knows the default username and password for the access. A little change in the vulnerability will definitely make things simple, interesting and more enjoyable to play and learn.
- **Adding warm-up session in the Game Process (GP):** We observed that by presenting the rules, cards, characters makes the players

Fig. 19. Word Cloud developed from the Scenarios created by players.

Table 16
Primary observations.

Questions from Participants	Interpretation	Issue Category
"How can i write a psychology attack for IT product?"	This is due to the picture on asset card where the girl is using a computer which confuses the player as an IT product instead of a human asset.	Card Design (CD)
"How to move on the map"	As in the initial phase of the game, we have not devised any specific mechanism for movement. However, this indicates improvement for future.	Game Process (GP)
"What you want to say? I dont understand?"	In the international group, where participants are using English language as communication, instead of their mother language.	Communication and Language (C&L)
"Game Ends? Hahaha."	The participants need active learning instead of passive one. There must be some explanation in the end session where the usefulness of this activity can be explained.	Game Design (GD)

enthusiastic to play. However, they need to be guided on how to play by demonstration. One dummy game must be played in front of the players so that they may see the process in advance and can ask questions.

- **Defining clearer player movement rules in the Game process (GP):** Observation from the empirical evaluation is that the movement of players on the map must have some element of amusement associated to it. Right now, the movement in the game is static. The players just move and place the piece in front of the room, solve the puzzle and so on.
- **Use of mother language in Game Communication (C & L):** We observed that if the game is in mother language of the players, the quality of the discussion and the amount of learning gets enhanced. In our game we had five groups: one group of international students which consisted of two students from Pakistan, one from Korea and one from China, and less detailed vis-a-vis other groups who were using mother language (Chinese version) of the game. We believe that natural language/mother language helps players to play, explore, and discuss various options thoroughly, and eventually help players in learning.
- **Captain card is not effective (GD):** From the empirical evaluation we have observed that the captain card and leader concept is not well followed by the team players. In the activity, players just ignore the captain command and the aim to work together to achieve the common goal; thus, bring up the shared leadership concept [34]. In future, we may consider replacing the captain card with shared leadership, where all team members share the leadership responsibilities in the area of their expertise.

7. Discussion

From this study, we conclude that game based solution can be an alternative way for methodological education. The proposed Security Requirement Engineering Game in the initial phase had shown promising results. From this study, we conclude that the proposed Security Requirement Engineering Game (SREG) has, in general shown, positive results and is helpful for players of the game to get an understanding of security attacks and vulnerabilities. Table 17 shows the summary comparison between the games, which educate players regarding the security requirements concepts. These games were played in the lab by the researchers, and the result is compiled and analyzed. Table 17, summarizes all the four games. We can see from the table that Security Requirements Educational Game (SREG) provides a maximum of the factors. Overall, we believe that SREG is a multi-knowledge game which not only trains players with Network related concepts but also focuses on physical and social engineering aspects. Besides these advantages, it also helps players to work in a team and achieve a common goal. In Table 17, 'Some+' identifies that this phase is present to good extent in the game. '✓' represents the complete presence of that phase in the game and 'X' represent absence of that phase in the game.

Table 17
SREG comparison with other Games.

Characteristics	SREG	Ctrl-ALt-Hack [9]	Social Engineering [5]	Dox3d
(Attack) Characters in game	✓	✓	x	✓
Map Used in the game for reference	✓	x	✓	✓
Dynamic Nature of Map (Changeability)	some+	x	x	✓
Players play by moving on the Map	✓	x	x	✓
Different type of Attack Cards	✓	some+	✓	x
Dice for Randomness	x	✓	x	x
Game Address Social Engineering Issues	✓	some+	✓	some+
Game Educate Network Security Related Issues	✓	some+	x	✓
Game Educate Physical Security Related Issues	✓	some+	x	some+
Making Scenario	✓	x	✓	x
Attack Mechanics	✓	✓	✓	✓
Defence Mechanics	x	x	x	✓
Story line of the Game	✓	✓	x	✓
Mission for the Team and Player	✓	✓	x	✓
Discussion Session (Knowledge/Experience sharing)	✓	some+	✓	some+

7.1. Validity threats

This study faces some threats to validity. We, as a team, tried our best to identify and eliminate the threats but some of the restrictions and threats are beyond our control. They are discussed below.

7.1.1. Conclusion validity

Conclusion validity deals with the reliability of the research results [73,74]. Its aim is to make sure that there should not be any threat to the conclusion of the study. The survey data was taken on-line anonymously by the players, and the results were further generated by the online tool. The data received in the form of table and graphs were further discussed among the researchers for possible interpretation. Thus, minimizing the threat related to conclusion validity. Furthermore, the results and deductions were further cross-checked by other researchers for their comments. The goal is to minimize any bias/threat which is related to a conclusion. **Moreover, due to a small number of participants in the activity, there exists a threat to conclusion validity which, in future, will be minimized by involving more participants in the empirical evaluation.**

7.1.2. External validity

Reporting the context of a controlled activity in the study holds great significance as it helps to understand which cases can be compared. Furthermore, every single case study is a significant contribution in the area giving an in-depth understanding [74]. Although, our

empirical evaluation for this serious game is performed in a multi-cultural environment of a graduate class, further verification for external validity is yet to be performed in future.

7.1.3. Theoretical validity

Past experience affects behavior [74]. There may be a case that some students already faced a particular type of security attack in the past and thus can relate to the game. This leads to a greater learning curve in resulting survey. To minimize this possibilities, we tried to form five different groups and further compare the quality of scenarios created by the players. The detail of groups can be seen in the empirical evaluation section.

7.1.4. Internal validity

Internal validity includes researcher bias and interpretation of data [73–75]. To minimize the internal validity in controlled activity setting, survey design, conclusion, and deduction, researchers of the study discussed and shared their experiences regarding development and execution of the empirical evaluation to minimize the associated threats. After the detailed discussion, finalized steps were tested on a small group of students to check and update the process and, finally, discussed with other researchers for their feedback.

We dont purport the game to be comprehensive as of now. On the other hand, however the controlled empirical evaluation helps to get initial results, observations, feedback, and suggestions.

Concerning the selection of participants or subjects, we have not made a random selection but followed comprehensive steps which are discussed in the empirical evaluation section.

Following the Table 18, we have discussed various factors which are controlled during the empirical evaluation to minimize any bias in the results.

7.1.5. Construct validity

Construct validity can be misleading due to possible threats to hypothesis and Experiment design. Some of the threats related to our study are discussed below:-

1. Hypothesis Guessing: If the participants know or guess the desire result of the empirical evaluation, his/her behavior may change towards the desire results. To minimize this, we tried to remain neutral during the activity and provided phases of feedback and informal discussions where participants shared their suggestions, feedback and comments.
2. Bias in Empirical Evaluation design: To minimize the bias in empirical evaluation design, we reviewed and further adapted the survey design pattern and scenario based technique from published literature [5]. In future studies, we will try to improve by adopting the evaluation material and methods used by other published studies, which may be helpful in concluding and comparing our results.

The observation biases [72] for the observational part of the study is minimized by a discussion session among the researchers. One category is the “Strong”, in which all the researchers agree with the observation. “Medium / Low” category is where one or two researchers agreed. Only the findings labelled as strong are discussed in this study.

8. Conclusion and future work

In this paper, an organizational security educational game is designed to transform security requirements concepts into game elements and to implement security requirements analysis process in terms of game playing rules. By letting players immerse into a game-based setting that mimics the organizational and technical context of a given enterprise system, the security requirements analysis tasks will become easier and more enjoyable. In particular, our approach aims to support a systematic elicitation of potential attackers intentions, their capabilities of attacks while conducting end user security training and awareness improvement. Our proposal eventually educates players regarding security requirements based on identified attack scenarios, which are evaluated and discussed among players thoroughly. We evaluated our approach through an empirical evaluation which is carried out in a requirements engineering graduate class using a hospital information systems setting. In the empirical evaluation, students first created hypothetical scenarios according to the game environment. A further one by one discussion followed in class to analyze and contribute if required. This session helped players know unique ways of attacking. Besides this, it would eventually help them to be cautious if something similar happens in their future life. Moreover, we have conducted survey and collected feedback at the end of the game session. In the feedback, overall, students gave positive comments. However, one of the things worth mentioning is the complexity of the game as pointed out in written and informed discussions. Survey results further helped us evaluate the learning effectiveness of the game. Moreover, initial results of the empirical evaluation, including players performance and feedback confirm the effectiveness of the approach. From the controlled empirical evaluation results, we can get an idea that majority of the players agree with our stance that SREG is easy and enjoyable to play. Moreover, SREG has helped the players get a reasonable knowledge about security related concepts. Apart from this, in the data collected on feedback sheets, 14 out of the 16 players agree that collaboration and learning between team members increases the chances of winning the game.

The empirical evaluation performed for the game has indicated several areas for improvement, including the map of the game, can be further extended by providing more focused view of certain aspect of an organization to reduce complexity and waste game time; update the pool of known attacking measures according to the most recent applicable ones; if the game will run in a bilingual environment, ensuring the expression of the attacks and context are on the same page; more game elements to further increase the fun and enjoyable level of the game is necessary. In order to make the movement on the map more attractive and fun, we are planning to introduce an element of chance in the future version. In the current version of the game, the movement of the players is not associated with the dice. Adding the dice for the game will help the players move (with chance) on the map either some restriction(s) can be implemented or some kind of surprise in movement

Table 18
Control factors for internal validity.

Control Factor	Explanation
Class Instructor	The class instructor and the activity facilitator person was in the class to help out or guide the students, if needed.
Class Time	The class timings were divided into three sections. In first session lecture is given, in second session activity is performed and in the last session discussion took place.
Learning Context	The learning content of the game was in English & Chinese.
Class Setting	The class students were divided into five groups.
Initial selection of Participants	The selection of the participants was done by a process explained in the Section 6.2.
Teaching Method	Powerpoint slides were used to explain the game process and rules to the students.
Gender, Age, Academic Qualification	Students of Graduate Level, Age and gender were fixed from the start of the activity.

can be added. Specially designed dice can be used to move the players. We can restrict the player to move 1, 2 or 3 places in one turn. Besides this, in future, we are planning to develop a level system for the game in which, the attack feasibility will decide what will be the next target. The point system may be updated in future, depending on the discussion, feedback, and suggestions. Furthermore, in future we plan to make a hybrid version of the card game (some functionalities will shift to online or android app).

Acknowledgement

Financial support from the National Science and Technology Support Program Project no. 2015BAH14F02, and Natural Science Foundation of China Project no. 61432020. Tong Li acknowledges the support of Beijing University of Technology Startup Funding Project no. 007000514116022. We thank Awaid Yasin for reviewing the paper.

Appendix A. SREG data download link

The complete game data and how to setup the game can be downloaded from the **Mendeley link**[4] or by using DOI: 10.17632/38kb4rxtw4.1 or can request for the data by emailing at affan.yasin@qq.com.

Appendix B. Setup guidelines

1. Print the map of the game. (The original dimension of the map size is set to adjust on the table). [Map Hospital.jpg]
2. Print human asset cards [Assets Cards Hospital.pdf] and weakness cards for human assets [Weakness people.pdf].
3. Attach / pin the human asset cards with the weakness card on the back.
4. Print Vulnerability card [Vulnerability IT Devices new.pdf].
5. Attach / pin the IT asset cards with the respective vulnerability card on the back.
6. Print and cut the psychology card [Psychology compliance principle.pdf].
7. Print and cut the puzzle card [Riddle or puzzle.pdf].
8. Print the Network Attack techniques card [Network Attack Cards.pdf].
9. Print the Physical Attack techniques card [Physical Attacker cards.pdf]
10. Print the Social Engineering Attack techniques card [Social Engineer cards.pdf].
11. Print and cut the role card [Player role card.pdf].
12. Print the attackers positions cards [Attacker position.jpg].
13. Print Goal Sheets for social engineering attackers [gs2.png].
14. Print Goal sheets for physical and network attacker [gs1.png].
15. Take simple paper sheet for players to write hypothetical scenarios.
16. Print discussion sheet [score sheet discussion.pdf].
17. Others:
    - Take any paper sheet for getting feedback.
    - For discussion session or observation use any paper sheet to record.
    - Survey1.pdf, Survey2.pdf and Survey3.pdf can be used to get feedback regarding the game.
    - Learning scenarios can be taken from the paper.
    - To design game cards, e.g., human assets, attacker role, etc. we have used some images from an online source. The usage is only to complete the card design and further check the initial results of the game from an educational point of view.

[4] https://data.mendeley.com/datasets/38kb4rxtw4/1.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.infsof.2017.12.002.

References

[1] P. Kierkegaard, Electronic health record: wiring Europes healthcare, Comput. Law Secur. Rev. 27 (5) (2011) 503–515.
[2] E.K. Wang, Y. Ye, X. Xu, S.-M. Yiu, L.C.K. Hui, K.-P. Chow, Security issues and challenges for cyber physical system, Proceedings of the 2010 IEEE/ACM International Conference on Green Computing and Communications & International Conference on Cyber, Physical and Social Computing, IEEE Computer Society, 2010, pp. 733–738.
[3] F.A. Rahim, Z. Ismail, G.N. Samy, Information privacy concerns in electronic healthcare records: a systematic literature review, Research and Innovation in Information Systems (ICRIIS), 2013 International Conference on, IEEE, 2013, pp. 504–509.
[4] D. McGraw, R. Belfort, H. Pfister, S. Ingargiola, Engaging patients while addressing their privacy concerns: the experience of project healthdesign, Pers. Ubiquitous Comput. 19 (1) (2015) 85–89.
[5] K. Beckers, S. Pape, A serious game for eliciting social engineering security requirements, Requirements Engineering Conference (RE), 2016 IEEE 24th International, IEEE, 2016, pp. 16–25.
[6] D. Callele, E. Neufeld, K. Schneider, Requirements engineering and the creative process in the video game industry, Requirements Engineering, 2005. Proceedings. 13th IEEE International Conference on, IEEE, 2005, pp. 240–250.
[7] R. Smith, O. Gotel, Gameplay to introduce and reinforce requirements engineering practices, International Requirements Engineering, 2008. RE'08. 16th IEEE, IEEE, 2008, pp. 95–104.
[8] P. Lombriser, F. Dalpiaz, G. Lucassen, S. Brinkkemper, Gamified requirements engineering: model and experimentation, International Working Conference on Requirements Engineering: Foundation for Software Quality, Springer, 2016, pp. 171–187.
[9] 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, ACM, 2013, pp. 915–928.
[10] A. Hannemann, C. Hocken, R. Klamma, Community driven elicitation of requirements with entertaining social software, Software Engineering (Workshops), (2009), pp. 317–328.
[11] C. Mainemelis, When the muse takes it all: a model for the experience of timelessness in organizations, Acad. Manag. Rev. 26 (4) (2001) 548–565.
[12] C. Klimmt, Serious games and social change: why they (should) work, Serious Games: Mechanisms and Effects, (2009), pp. 248–270.
[13] R.N. Landers, R.C. Callan, Casual Social Games as Serious Games: The Psychology of Gamification in Undergraduate Education and Employee Training, Serious Games and Edutainment Applications, Springer, 2011, pp. 399–423.
[14] S. Helser, Fit: identity theft education: Study of text-based versus game-based learning, Technology and Society (ISTAS), 2015 IEEE International Symposium on, IEEE, 2015, pp. 1–4.
[15] S. Deterding, D. Dixon, R. Khaled, L. Nacke, From game design elements to gamefulness: defining gamification, Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, ACM, 2011, pp. 9–15.
[16] C.G. von Wangenheim, R. Savi, A.F. Borgatto, Deliver an educational game for teaching earned value management in computing courses, Inf. Softw. Technol. 54 (3) (2012) 286–298, http://dx.doi.org/10.1016/j.infsof.2011.10.005.
[17] K. Seaborn, D.I. Fels, Gamification in theory and action: a survey, Int. J. Hum. Comput. Stud. 74 (2015) 14–31.
[18] M. Souza, L. Veado, R.T. Moreira, E. Figueiredo, H. Costa, A systematic mapping study on game-related methods for software engineering education, Inf. Softw. Technol. (2017), http://dx.doi.org/10.1016/j.infsof.2017.09.014.
[19] A. Ampatzoglou, I. Stamelos, Software engineering research for computer games: a systematic review, Inf. Softw. Technol. 52 (9) (2010) 888–901, http://dx.doi.org/10.1016/j.infsof.2010.05.004.
[20] J. Hamari, D.J. Shernoff, E. Rowe, B. Coller, J. Asbell-Clarke, T. Edwards, Challenging games help students learn: an empirical study on engagement, flow and immersion in game-based learning, Comput. Hum. Behav. 54 (2016) 170–179.
[21] L. da Rocha Seixas, A.S. Gomes, I.J. de Melo Filho, Effectiveness of gamification in the engagement of students, Comput. Hum. Behav. 58 (2016) 48–63.
[22] J. Hamari, J. Koivisto, Working out for likes: an empirical study on social influence in exercise gamification, Comput. Hum. Behav. 50 (2015) 333–347.
[23] J.J. Lee, J. Hammer, Gamification in education: what, how, why bother? Acad. Exch. Q. 15 (2) (2011) 146.
[24] K.M. Kapp, The Gamification of Learning and Instruction: Game-Based Methods and Strategies for Training and Education, John Wiley & Sons, 2012.
[25] R.N. Landers, M.B. Armstrong, Enhancing instructional outcomes with gamification: an empirical test of the technology-enhanced training effectiveness model, Comput. Hum. Behav. (2015).
[26] O. Pedreira, F. García, N. Brisaboa, M. Piattini, Gamification in software engineering–a systematic mapping, Inf. Softw. Technol. 57 (2015) 157–168.
[27] L. de Marcos, E. Garcia-Lopez, A. Garcia-Cabot, On the effectiveness of game-like and social approaches in learning: comparing educational gaming, gamification &

social networking, Comput. Educ. 95 (2016) 99–113.
[28] M. Urh, G. Vukovic, E. Jereb, et al., The model for introduction of gamification into e-learning in higher education, Procedia-Social and Behavioral Sciences, 197 (2015), pp. 388–397.
[29] E.D. Mekler, F. Brühlmann, A.N. Tuch, K. Opwis, Towards understanding the effects of individual gamification elements on intrinsic motivation and performance, Comput. Hum. Behav. (2015).
[30] J. Hamari, J. Koivisto, Why do people use gamification services? Int. J. Inf. Manag. 35 (4) (2015) 419–431.
[31] T. Long, L. Liu, Y. Yu, Z. Jin, Avt vector: a quantitative security requirements evaluation approach based on assets, vulnerabilities and trustworthiness of environment, 2009 17th IEEE International Requirements Engineering Conference, (2009), pp. 377–378, http://dx.doi.org/10.1109/RE.2009.53.
[32] N. Crowe, S. Bradford, Identity and structure in online gaming: young peoples symbolic and virtual extensions of self, Youth cultures: Scenes, Subcultures and Tribes, Routledge, New York, 2007, pp. 217–231.
[33] M. Ståhl, Gender and identity in video games as a virtual learning environment, The International Scientific Conference eLearning and Software for Education, 1 “Carol I” National Defence University, 2016, p. 541.
[34] C.L. Pearce, H.P. Sims Jr, Vertical versus shared leadership as predictors of the effectiveness of change management teams: an examination of aversive, directive, transactional, transformational, and empowering leader behaviors. Group Dyn. 6 (2) (2002) 172.
[35] E.C. Metzger, L. Lubin, R.T. Patten, J. Whyte, Applied gamification: creating reward systems for organizational professional development, Foundation of Digital Badges and Micro-Credentials, Springer, 2016, pp. 457–466.
[36] I. Kotini, S. Tzelepi, A gamification-based framework for developing learning activities of computational thinking, Gamification in Education and Business, Springer, 2015, pp. 219–252.
[37] A. Amory, K. Naicker, J. Vincent, C. Adams, The use of computer games as an educational tool: identification of appropriate game types and game elements, Br. J. Edu. Technol. 30 (4) (1999) 311–321.
[38] M. Habgood, S. Ainsworth, S. Benford, Intrinsic fantasy: motivation and affect in educational games made by children (2005).
[39] R. Hunicke, M. LeBlanc, R. Zubek, Mda: A formal approach to game design and game research, Proceedings of the AAAI Workshop on Challenges in Game AI, 4 (2004).
[40] A. Souag, C. Salinesi, I. Comyn-Wattiau, Ontologies for security requirements: a literature survey and classification, International Conference on Advanced Information Systems Engineering, Springer, 2012, pp. 61–69.
[41] D. Firesmith, Specifying reusable security requirements, J. Object Technol. (2004) 61–75.
[42] A. Souag, C. Salinesi, R. Mazo, I. Comyn-Wattiau, A Security Ontology for Security Requirements Elicitation, Springer International Publishing, Cham, pp. 157–177.
[43] C. Haley, R. Laney, J. Moffett, B. Nuseibeh, Security requirements engineering: a framework for representation and analysis, IEEE Trans. Softw. Eng. 34 (1) (2008) 133–153.
[44] G. Boström, J. Wäyrynen, M. Bodén, K. Beznosov, P. Kruchten, Extending XP practices to support security requirements engineering, Proceedings of the 2006 International Workshop on Software Engineering for Secure Systems, ACM, 2006, pp. 11–18.
[45] I.A. Tondel, M.G. Jaatun, P.H. Meland, Security requirements for the rest of us: a survey, IEEE Softw. 25 (1) (2008) 20–27, http://dx.doi.org/10.1109/MS.2008.19.
[46] I. Williams, X. Yuan, J.T. McDonald, M. Anwar, A method for developing abuse cases and its evaluation, JSW 11 (5) (2016) 520–527, http://dx.doi.org/10.17706/jsw.11.5.520-527.
[47] G. Sindre, A.L. Opdahl, Eliciting security requirements with misuse cases, Requir. Eng. 10 (1) (2005) 34–44.
[48] A. Keavney, et al., Team building strategies, Train. Dev. 43 (2) (2016) 26.
[49] S.I. Tannenbaum, R.L. Beard, E. Salas, Team building and its influence on team effectiveness: an examination of conceptual and empirical developments, Adv. Psychol. 82 (1992) 117–153.
[50] Z. Carlson, T. Sweet, J. Rhizor, J. Poston, H. Lucas, D. Feil-Seifer, Team-building activities for heterogeneous groups of humans and robots, International Conference on Social Robotics, Springer, 2015, pp. 113–123.
[51] K. Rogers, Team building activities for young students, Strategies 17 (4) (2004) 17–19.
[52] S. Hagood, S. Lynn, O. Riverso, Instructing and assessing cooperative team-–building, Strategies 19 (2) (2005) 21–26.
[53] L. Van der Merwe, Scenario-based strategy in practice: a framework, Adv. Dev. Hum. Resour. 10 (2) (2008) 216–239.
[54] A. Dix, J.E. Finlay, G.D. Abowd, R. Beale, Human-Computer Interaction, 3 edition, Pearson, 2004.
[55] B. Kuvaas, R. Buch, A. Weibel, A. Dysvik, C.G. Nerstad, Do intrinsic and extrinsic motivation relate differently to employee outcomes? J. Econ. Psychol. 61 (2017) 244–258, http://dx.doi.org/10.1016/j.joep.2017.05.004.
[56] L.W. Anderson, A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom’s Taxonomy of Educational Objectives, Abridged Edition, Pearson new international edition, Pearson Education Limited, 2013.
[57] L.W. Anderson, A Taxonomy for Learning, Teaching, and Assessing : A Revision of Bloom’s Taxonomy of Educational Objectives, Longman, 2001.
[58] H.-Y. Sung, G.-J. Hwang, A collaborative game-based learning approach to improving students’ learning performance in science courses, Comput. Edu. 63 (2013) 43–51.
[59] H.-J. So, T.A. Brush, Student perceptions of collaborative learning, social presence and satisfaction in a blended learning environment: relationships and critical factors, Comput. Edu. 51 (1) (2008) 318–336.
[60] T. de la Hera Conde-Pumpido, A conceptual model for the study of persuasive games, Proceedings of DiGRA, (2013).
[61] F. Mouton, M.M. Malan, L. Leenen, H.S. Venter, Social engineering attack framework, Information Security for South Africa (ISSA), 2014, IEEE, 2014, pp. 1–9.
[62] E. Osuagwu, G. Chukwudebe, T. Salihu, V. Chukwudebe, Mitigating social engineering for improved cybersecurity, Cyberspace (CYBER-Abuja), 2015 International Conference on, IEEE, 2015, pp. 91–100.
[63] S.D. Applegate, Social engineering: hacking the wetware!, Inf. Secur. J. 18 (1) (2009) 40–46.
[64] K. Krombholz, H. Hobel, M. Huber, E. Weippl, Advanced social engineering attacks, J. Inf. Secur. Appl. 22 (2015) 113–122.
[65] N.Y. Conteh, P.J. Schmick, Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks, Int. J. Adv. Comput. Res. 6 (23) (2016) 31.
[66] T. Li, E. Paja, J. Mylopoulos, J. Horkoff, K. Beckers, Security attack analysis using attack patterns, Research Challenges in Information Science (RCIS), 2016 IEEE Tenth International Conference on, IEEE, 2016, pp. 1–13.
[67] L. Davi, A. Dmitrienko, A.-R. Sadeghi, M. Winandy, Privilege escalation attacks on android, International Conference on Information Security, Springer, 2010, pp. 346–360.
[68] A. Hussain, J. Heidemann, C. Papadopoulos, A framework for classifying denial of service attacks, Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, ACM, 2003, pp. 99–110.
[69] A. Kieyzun, P.J. Guo, K. Jayaraman, M.D. Ernst, Automatic creation of SQL injection and cross-site scripting attacks, Software Engineering, 2009. ICSE 2009. IEEE 31st International Conference on, IEEE, 2009, pp. 199–209.
[70] A.W. Kong, D. Zhang, M. Kamel, Analysis of brute-force break-ins of a palmprint authentication system, IEEE Trans. Syst., Man, Cybern., Part B (Cybern.) 36 (5) (2006) 1201–1205.
[71] A.U. Jan, V. Contreras, Technology acceptance model for the use of information technology in universities, Comput. Hum. Behav. 27 (2) (2011) 845–851. Web 2.0 in Travel and Tourism: Empowering and Changing the Role of Travelers. doi: 10.1016/j.chb.2010.11.009
[72] M.N.K. Saunders, Research Methods for Business Students, Pearson Education Limited, Harlow, Essex, England, 2016.
[73] C. Wohlin, P. Runeson, M. Höst, M.C. Ohlsson, B. Regnell, A. Wesslén, Experimentation in Software Engineering, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 123–151.
[74] K. Petersen, C. Gencel, Worldviews, research methods, and their relationship to validity in empirical software engineering research, 2013 Joint Conference of the 23rd International Workshop on Software Measurement and the 8th International Conference on Software Process and Product Measurement, (2013), pp. 81–89.
[75] C. Wohlin, P. Runeson, M. Höst, M.C. Ohlsson, B. Regnell, A. Wesslén, Experimentation in Software Engineering, Springer Science & Business Media, 2012.