sD&D: Design and Implementation of Cybersecurity Educational Game with Highly Extensible Functionality

Yoshiyuki Kido[1,2], Nelson Pinto Tou[2], Naoto Yanai[2], and Shinji Shimojo[1,2]

[1] Cybermedia Center, Osaka University,
5-1, Mihogaoka, Ibaraki-shi, Osaka 5670047, Japan,
{kido,shimojo}@cmc.osaka-u.ac.jp
[2] Graduate School of Information Science and Technology, Osaka University,
1-5, Yamadaoka, Suita-shi, Osaka 5650871, Japan
{nelson,yanai}@ist.osaka-u.ac.jp

Abstract. Cybersecurity issues have gained more attention due to the rapid development of new technology. In many cases, cyber theft happened due to a lack of understanding of how to secure a single piece of private information. In the present paper, we attempt to provide an inexpensive and easy tool for learning cybersecurity through a board game simulation called Security Defense and Dungeons (sD&D). The basic concept is not only to introduce the latest cybersecurity equipment and solutions, but also to provide cybersecurity education for players to raise awareness regarding cybersecurity threats. In addition, we attempt to train users in good practices concerning team communication and human resources. The simple game interface includes cybersecurity task scenarios, featured intuitive game design for users, and easy exploration of the provided scenario. In addition, the proposed game, in which players can share game resources and bits of knowledge, communicate via a chat room. In the present study, in order to evaluate the proposed method and prototype implementation, we performed a user study with student users. The questionnaire results were mostly positive comments and opinions.

Keywords: Gaming Education, Cybersecurity Education, Security Awareness.

1 Introduction

With the development of information and communications technology in recent years, it is now possible to manage and share information across the globe. However, information systems and the Internet not only bring convenience to our lives but also introduce various cybersecurity issues, such as attacks by malicious users, as well as leakage of personal information and cyberbullying, which can have serious repercussions. Therefore, information literacy in users is a key component for individuals or companies and organizations to improve protection

against attacks on cybersecurity measures. However, there are few educational game tools aimed at nurturing cybersecurity and improving the information literacy of individuals. Studies have suggested that students effectively learn what they have practiced [11]. Fundamentally game-based learning allows a learner to better engage the real world. Such games involve an artificial mockup or simulation of the environment of the real world. In the present study, we proposed the design of network multiplayer games and solve a scenario related to security issues. In comparison with analog and other digital game scalability and flexibility, achieving this remains challenging. For example, space for the player to play in analog games is a scalability issue that prevents the addition of a new player or setting up a new game environment. Furthermore, the flexibility to accommodate new security issues without significant modification of the game has not yet been adequately explored. Therefore, we attempt to build a cybersecurity game with scalability and flexibility, which will provide context-changeable security games for education.

There are many cybersecurity analog games that attempt to train users to improve their cybersecurity literacy. These games allow people to learn about general knowledge of cybersecurity while having fun. Although most of these games provide useful information on cybersecurity the games do not really give the user a sense of fully comprehending the tools or how to identify a security breach as early as possible. For example, methods by which to use these tools to perform a cybersecurity attack or to protect network resources are not shown in cybersecurity analog games. On the other hand, there are several programming contests and competition for cybersecurity learning called "Capture the Flag Unplugged" [6], which involves a very difficult competition regarding how to find security holes in an information system environment prepared by the competition organizer. This competition attempts to train cybersecurity engineers, rather than young people, with more professional skills. This is one motivation for our team to design a cybersecurity board game.

Another motivation for building this game application is the occurrence of cyberbullying targeting young people in social media communication [8]. In addition, according to a study on the definition and concept of cyberbullying, raising the awareness of how users share their information on the internet is one solution for cyberbullying prevention. Recently, a serious game of enhancing privacy awareness in social network tools has been developed [2]. In this game, users can learn how to behave correctly as well as cyber safety in social networks. However, their approach does not treat several technical issues in cybersecurity. Young people and technology beginners need knowledge of information and network technology. In order to understand the behavior of cybercrime more deeply, users should understand the mechanism of information technologies, such as authentication, access controls, and other cybersecurity mechanisms. The reason for this is that, if social network users do not know the behavior of the information and network system, each user cannot determine who obtained information regarding his/her personal identify.

Therefore, we herein consider the design of Security Defense and Dungeons (sD&D), which is a cybersecurity board game. The main contribution of the present paper is to raise the awareness of cybersecurity education and to consider game scalability and flexibility in context-changeable cybersecurity game education. As such, we have evaluated the game effectiveness regarding our intended goals through a user study.

In the present paper, we briefly introduce cybersecurity issues and describe the basic idea and games approach to expose people to thinking about security in Section 2. Section 3 and 4 show in detail the goals of the proposed games, architecture, and prototype design. In Section 5, we describe the evaluation of user impressions. Finally, we discuss task for future research and conclude the paper in Section 6.

2 Related Research

Cybersecurity educational games have shown significant efforts to provide end users with education. Their concepts include comprehending cybersecurity, which impacts privacy against malicious attacks, in particular to increase cybersecurity awareness for a user that is not an IT expert. Although we experienced raised cybersecurity awareness while playing the games, the games did have some weak points. For example, playing the game takes a long time, the game is complicated, and there is difficulty applying the game tools in real cybersecurity scenarios.

Several studies have been carried out to incorporate an analog board game as part of cybersecurity education to increase user understanding of cybersecurity attacks. This includes the Control-Alt-Hack [4] tabletop board game, which was designed to address a variety of current technologies and actual threats regarding cybersecurity issues. An interesting part of this game is the role of characters in the cybersecurity field (social engineering) and addressing the core of cybersecurity issues. The design of the cards enforces exposure risks of various cybersecurity threats as well as mitigation or avoidance methods. For example, a cookie-blocked card describes the topic of writing a web browser extension to circumvent tracking cookies. However, the game may last longer if a player does not fully comprehend the game's rules or fails to complete a mission, which leads to loss of credibility. in addition, the game mechanism of rolling dice to determine whether a task was successfully carried out by the player, seems not to be a very intuitive approach.

Android: Netrunner [1] is a one-on-one commercial science fiction security card game. The game provides the concept of a megacorporation and secures their premises, while a runner or hacker tries to break into the premises. Unlike Android: Netrunner, the proposed game design focuses on simulating current security issues and presents simple rules to users. For example, each task in the proposed game attempts to engage a player to understand and use the property described in the task to attack or defend specific security faults.

D0x3d! [7] introduce network cybersecurity terminology, attack and defense mechanic and basic computer concepts. The game is a collaborative game with

up to four players. Throughout the game, the user gains cybersecurity knowledge from the pictogram shown on a card. For example, a pictogram featuring a broken border provides the notion of a reinforcement rule that a hacker can use to enter or exit a node.

Previous studies on digital games explain the cybersecurity theme to teach computer cybersecurity principles. For example, computer game simulation was used to enumerate computer cybersecurity lessons, as described in studies of "teaching objectives of a simulation game for the computer system" [10][3]. Such research suggested that digital game design can be used for positive training to identify cybersecurity threats easily [11]. Furthermore, as discussed in "Design and preliminary evaluation of a cybersecurity Requirements Education Game (SREG)" [12] revealed the need to integrate organizational tools into the game. Game-based learning not only accelerates the learning process, but also emulates a user's engagement to more actively identify a vulnerability attack, through social engineering, for example.

3 Research Goal and Concepts

3.1 Goal of the Present Research

The principal goals of the cybersecurity game are to raise awareness in security education. As described in the Introduction, there is a need to raise user awareness regarding security education in the era of information and technology, as this is essential to protect the user from cyber-thief and cyberbullying attacks. The awareness goals we hope to achieve are as follows.

First of all, we believe the game will be fun if it is easy to play and requires a low skill level related to the game theme. Our goal is to design a game that is easy to play and omit complex rules to provide a wide range of audiences of different skills and ages the opportunity to play the developed game. Furthermore, in order to increase the players' understanding of security tools, the design incorporates an easy scenario with adequate information displayed in the card window.

Next, the security game development quest of bringing the security scenario up to date was attempted including setting of the game configuration and behavior to provide security. We proposed simple rooms and cards, where each component can be added by the file configuration. In the future, we intend to provide a flexibility feature for adding a security scenario.

Finally, in many developing nations, for example, Timor-Lest the information and technology infrastructure are still not advanced compared to in developed countries. Impact tools, such as servers and network components, which provide an experimental environment for the students, are not affordable for some educational institutes. With this network game simulation, we hope students in such difficult situations can experience a simulation environment to better prepare for security considerations.

3.2 Why a Game?

Similar to Control-Alt-Hack [4], we assume that a game can provide excellent tools for the user to learn security education in a fun environment, rather than under pressure, and to engage in communication in a multiplayer game. With the digital game, network tools and security simulation are achievable. In particular, in delivering the freedom to experience threats without repercussions, we enable identification of cybersecurity threats, understanding, and interpretation of cybersecurity issues in terms of risk ramifications, and how to take proper avoidance actions.

In addition, game-based education is proving to be effective in altering user behavior [9]. Furthermore, Eagle [5] designed "Wu's Castle", a role-playing game in which students can use the C++ code to solve in-game problems. This game allows a student, to independently solve logic-related programming issues.

4 Design and Implementation

The basic idea of this game reutilizes an idea from conceptual card board games, which consist of a card deck that contains security information as a logical element for a player to explore. We combine the properties of a card game with current security attack threats in order to create scenarios for a player to play in our game. Our design implements room and card conceptually. A room is space for players to perform their tasks and include resource, trap and task rooms. The card components include hacker tools or network properties for a player to accomplish their mission.

4.1 Game Design

Figure 1 shows the proposed user interface of sD&D. The interface is composed of a player information window as well as a window showing the positions of the other players, rooms, cards and a chat room for interaction between players. Initially, the author explored a number of games to perceive the rules and mechanic for the sD&D design objectives. In making sD&D, the focus was on designing simple cybersecurity game rules as well as a game mechanism to enforce learning processes throughout the scenario provided in the game. Therefore, the sD&D design approach uses an $N \times N$ room to compose different game scenarios and properties for multiple players to explore the cybersecurity game as a team.

Element: Room The concept of room design is as space for the player to perform their mission, to move around, and to pick up available cards. There are three different types of rooms scattered according to the number of rooms defined in the game. Each room provides a distinct learning goal for the player while the player is accomplishing his/her task or learning a new security concept. A trap room is a room with no access door. The design of the trap room is such that once a player enters the room, a correct answer must be provided in order to

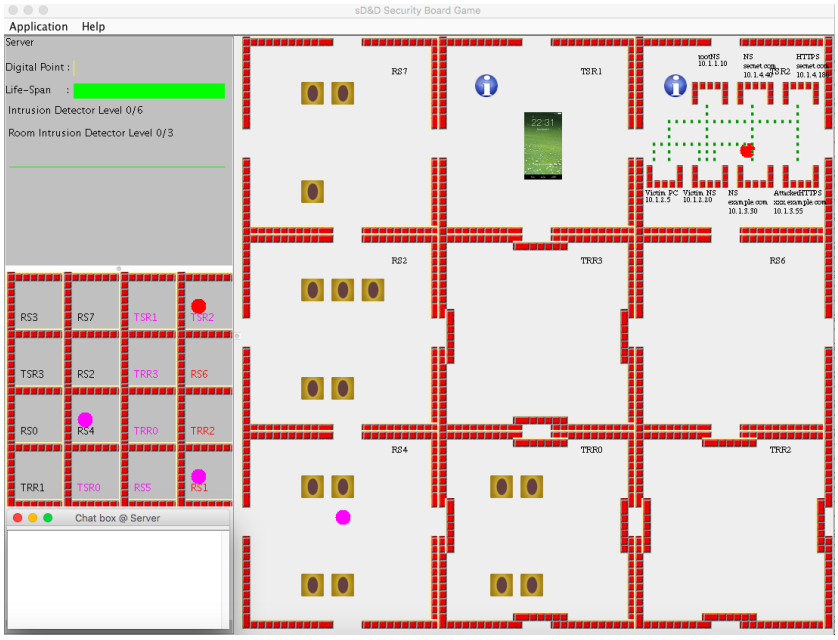


Fig. 1. Main Window of sD&D

unlock the door. The trap room may be an empty room or may contain essential cards required by a player to solve a cybersecurity task. As a prerequisite to unlocking a door, the player must drop a card. Therefore, when entering this room, the player has to have cards as resources and knowledge as the key to further proceed in the game, otherwise the game is ended.

A cybersecurity-related quiz is loaded dynamically via file configuration. As shown in Fig. 2(a), "What is the main purpose of a DNS server?" is an example of a cybersecurity question in the quiz. The game's administrator can quickly add new quiz entries by modifying the file configuration.

The second type of room is a resource room. A resource room can be assumed to be a deck of cards in card games. In sD&D design, the cards are scattered in the room face down rather than being placed in a pile. This method allows for multiple players to pick up cards simultaneous without waiting for the turn to advance. Figure 2(b) shows the resource room design used in this game.

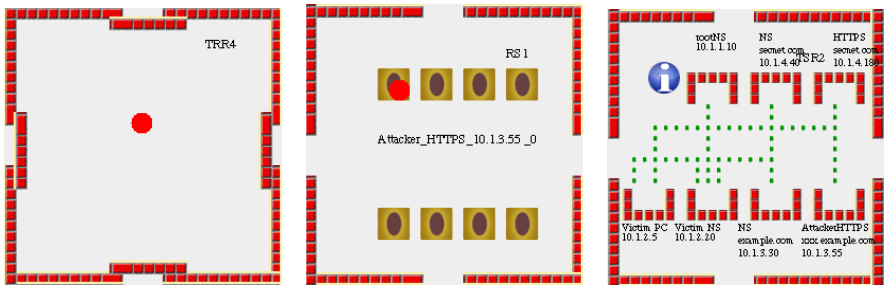
The third type of room is a task room, as shown in Fig. 2(c). A task room is an attempt to map the cybersecurity simulation as close as possible to a real cybersecurity attack. The cybersecurity scenario composed in the task room is designed to raise the awareness of cybersecurity issues and broaden the understanding of software faults, which can potentially lead to a cybersecurity breach. Furthermore, a simulation with a specific example of a cybersecurity topic triggers the user to think deeply about the issues and inspires the user to come up with a solution to the problem. Figure 3 shows the simulation window im-

age of the cybersecurity scenario in DNS cache poisoning. In this window, a user can perform DNS spoofing on target DNS servers along the scenario script (DNS cache poisoning scenario is as shown below). Throughout the scenario, a player is expected to grasp basic network design and to comprehend the DNS information flow and ultimately understand the danger of DNS cache poisoning combined with other cybersecurity attacks, such as phishing.

– DNS cache poisoning scenario script

```
Your mission: Eavesdropping user information utilizing DNS
cache poisoning
Goal :

Inject cache poisoning to the cache server, by changing the
legitimate IP address to attacker IP address. First, your
task is to build network configuration according to the
following information:

1. Cache Server: 10.1.2.20 pointed to the root DNS

2. Root DNS Server with all legitimate NS record

3. DNS secnet.com: 10.1.4.40 with NS record secnet.com ->
10.1.4.180

4. DNS attacker: 10.1.3.30 with ns record secnet.com ->
10.1.3.55 and xxx.example.com -> 10.1.3.55. Your second task
 is injecting DNS cache poisoning to the cache server using
“ dnsspoof ” to change the legitimate IP address 10.1.4.180
to attacker web IP address 10.1.3.55. A successful mission
shown ping to secnet.com will get a reply from the IP
address of attacker IP address: 10.1.3.55

Necessary tools (cards):

1. PC for testing

2. Server for root DNS

3. Server for victim DNS

4. Server for attacker DNS

5. Server for DNS secnet.com

6. Server for HTTPS secnet.com

7. Server for attacker HTTPS

8. dnsspoof tools

Instruction:

Following are list of task player have to do:

1. Server setup

2. Run the dnsspoof tool
```

```
3. Ping the attacker legitimate web address xxx.example.com.
the attacker DNS will reply legitimate NS record for xxx.
example.com but also make a query request and reply for
secnet.com domain

4. after some time the DNS cache poisoning eventually
succeed

5. from PC victim ping secnet.com and verify reply is IP
address of attacker PC
```



(a) Trap Room of sD&D (b) Resource Room of sD&D (c) Task Room sD&D

Fig. 2. Overview of Room Design of sD&D

Communication is a tool for successful collaboration in any aspect of a collaboration task. It is essential to interact with other players in order to win the game as a team, especially in network multiplayer games. In order to facilitate collaboration, such as requesting an answer to a question or exchanging cards between players a chat room is available.

Element: Card The card design in sD&D is primarily inspired by dox3d![7] and the Control-Alt-Hack[4]. However, in the present study, the author designates three types of cards, resource cards, intrusion detection cards, and magic patch cards, with detailed descriptions of the information of security tools. Each card provides specific cybersecurity tools for attack and defense. For example, a resource card can consist of a hacking tool, such as AirPlay-NG which is used to attack a wireless access point. The details of the card are as shown in Fig. 4(d). Also, resource cards such as DNS Server in Fig. 4(c), are used to set up the environment for the security incident simulation. The intrusion detection card is a type of card for the system administrator to provide defense of an information system, and an example of this card is shown in Fig. 4(a). Finally, the magic patch card, the counter-attack for the administrator defense card, is shown in

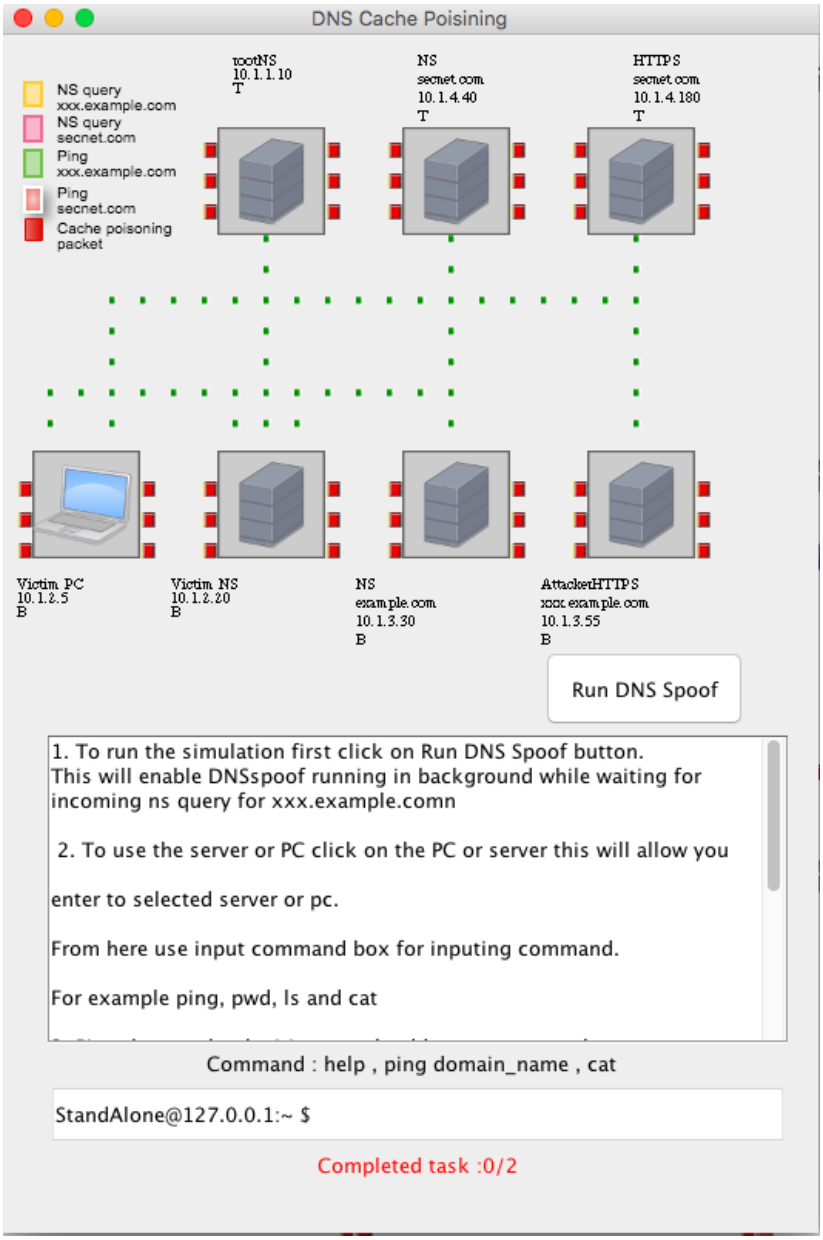
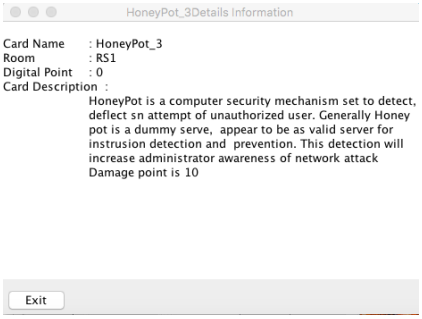
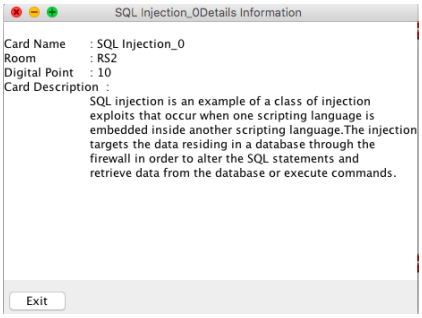


Fig. 3. DNS Cache Poisoning Simulation

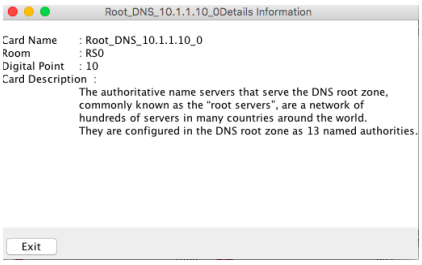
detail in Fig. 4(b). For example, during the game, if a player has collected an intrusion type of card, the player is detected by the system administrator, and, as consequence of the intrusion, the detection level is raised. Therefore, the player's lifespan is decreased, and the level of difficulty of the game also increases. However, the player can nullify the intrusion detected by using a magic patch card as a counter-attack.



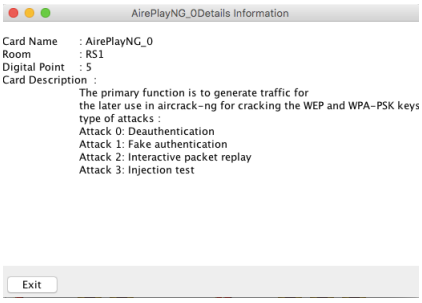
(a) Intrusion Card: HoneyPot



(b) Magic Patch Card: SQL Injection



(c) Resource Card: DNS Server



(d) Resource Card: AirPlay-NG

Fig. 4. Overview of sD&D Card Design

4.2 Scalability and Flexibility Concept

In this research, we define the scalability of the sD&D design as the suitable for the implementation of additional components (card, room, and task) in games via XML file configuration without significant modification of the core of the game framework. Therefore the structure of the XML file should provide ease of user in adding new rooms, cards, and scenarios at the same time, subject to the constraints and rules of sD&D.

One of the most challenging objectives of sD&D is to provide cybersecurity awareness regarding current cybersecurity contextual issues through game simulation. Since current cybersecurity issues evolve rapidly simulating a scenario

for a player to experience a cybersecurity threat, such as how an attack method can damage an information system as well as possible early detection to avoid further risk, is not an easy task. Of course, adding such new simulation often requires the additional of a feature to the game framework, which results in a significant modification of the game framework. In order to overcome significant changes in the game framework, the sD&D design provides flexibility to the user with administrator privilege to design, modify and implements new scenarios in the game's file configuration.

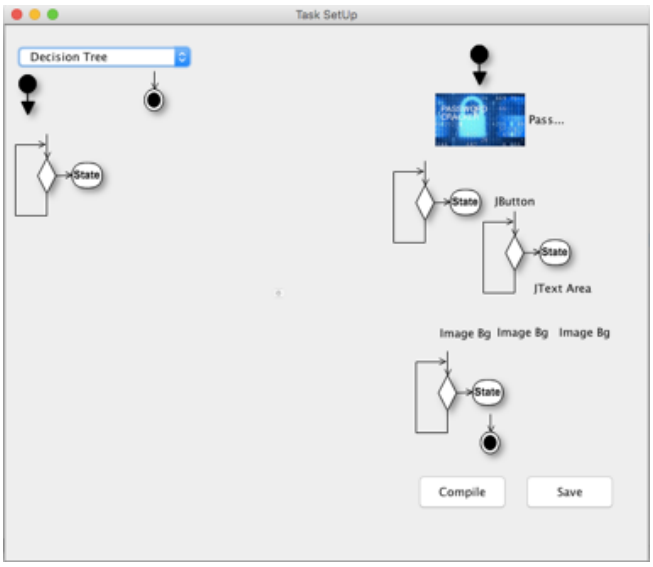


Fig. 5. Cybersecurity Scenario Design sD&D

Figure 5 shows the sD&D scenario design and configuration window. A user can define a cybersecurity scenario and simulation diagrams using this window before starting the game. In the present research, the author assumes the flexibility concept as a capability of sD&D in order to clarify the various inputs from the users, subject to modification and the use of simulation components in the sD&D platform, to generate new or modified cybersecurity simulation scenario.

5 Evaluation

The author measured the performance of the proposed sD&D game by comparing the CPU and memory loads. Furthermore, the estimated time consumption of multicast packet interchange between nodes with respect to the number of players and rooms determine the scalability of the game. A user study was conducted with a number of students to evaluate the accessibility and the ability to achieve the design goals of the sD&D.

Table 1. Computing Node Specifications

	Spec
CPU	Intel Core i7, 2.2 GHz
Memory	8GB, 1600 MHz DDR3
Network	AirPort Extrem (0x14E, 0x117), 54Mbps
OS	macOS High Sierra version 10.13.3
Java	Version 1.8.0_77

In this evaluation, the author assumes that the game is scalable if it can support a minimum of 36 different rooms with reasonable computation and network resources. The 36 rooms are capable of supporting up to approximately 208 different cards, assuming that 26 of the rooms are resources and trap room with maximum eight cards in each room and 10 of the rooms are task rooms.

5.1 Scalability Evaluation

Table 1 shows the specification of each computing node on the performance evaluation test. In this evaluation, the game size limit of 6×6 rooms (36 rooms) is based on the author's assumed criteria for measuring the scalability of the proposed game. In the performance evaluation, the consumption of CPU and memory by each computing node is shown in Fig. 6. As the number of rooms increases, the CPU load increases to a maximum of 52% of CPU consumption upon initialization of the game. However, the proposed game is capable of minimizing the CPU load while the game is played.

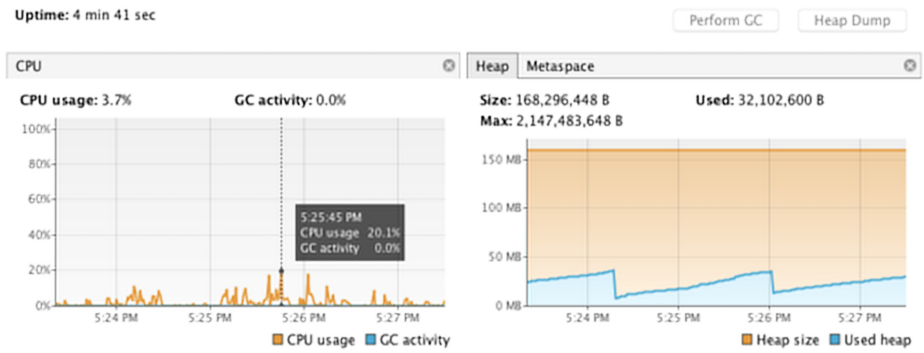
In order to reduce the usage of computational resources during the game, sD&D only draws a default matrix of 3×3 with the respective room properties to the screen. Each player screen is applied to map the whole room dimension in a different panel respectively to room name attribute and another player location.

Figure 7 illustrates the evaluation of the multicast packet round trip average with respect to the numbers of players. The highest round trip time (RTT) occurred when request authentication was performed. This is because, upon an authentication request, a number of procedures need to be accomplished to build the game environment.

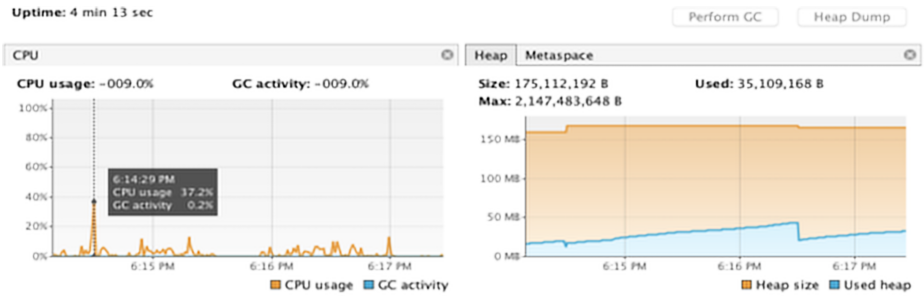
As the number of players increases, the RTT of the packet also increases. However, in this game, the packet size is constant, ranging from 32 to 107 bytes. A packet is sent throughout the network only if it is triggered by player action. As a result, an increase in the number of RTT packets with respect to the number of players is not expected to exceed 50% of the average RTT.

5.2 User Study Case

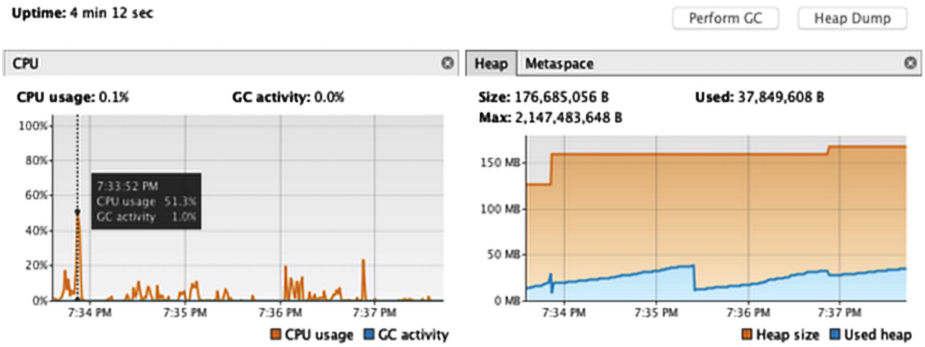
A survey was conducted for six students after playing the sD&D game. The participants were five male students and one female student. Of these, two were



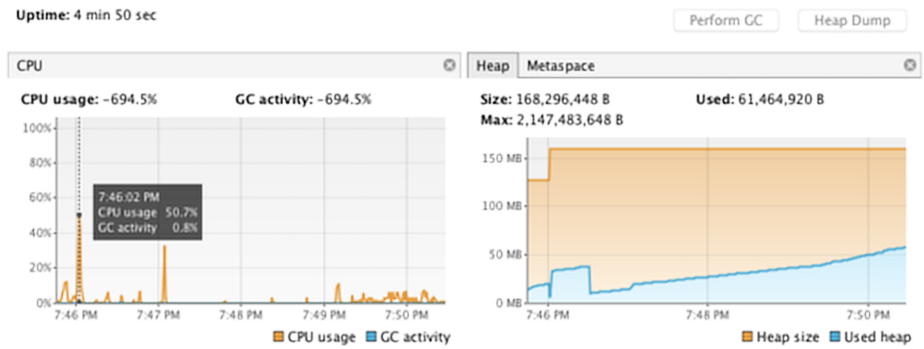
(a) Game Size: 3×3 rooms



(b) Game Size: 4×4 rooms



(c) Game Size: 5×5 rooms



(d) Game Size: 6×6 rooms

Fig. 6. CPU and Memory Consumption

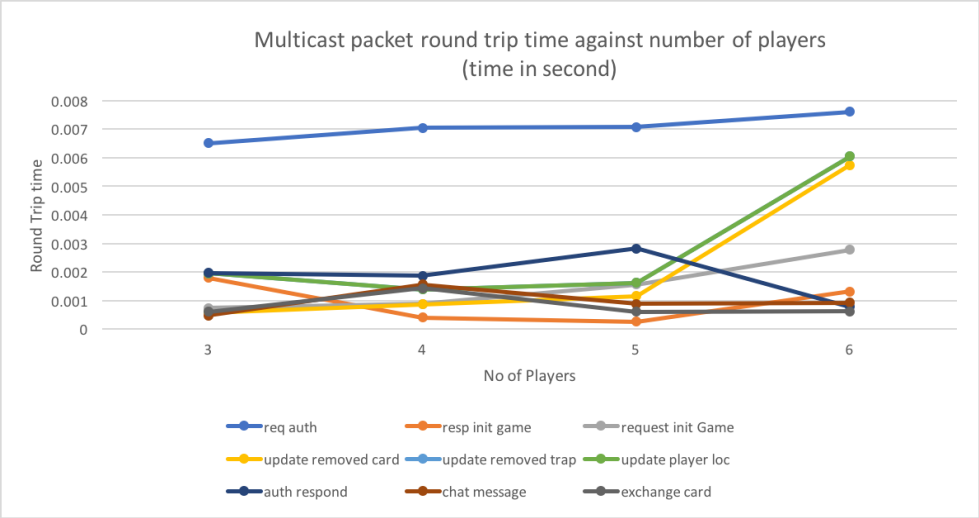


Fig. 7. Round Trip Time

Table 2. Survey Question and Result

Survey Question	Rating
Game design interface according to ease of task completion	4/6
Understanding the rule of the game	3/3
Ease of following the game instruction	5/6
Appropriateness of using the key input in the game	5/6
The card design provides sufficient information on a particular security topic	5/6
The ease of room design allows for exploration of the components in the room	6/6

international students and four were local students. Mean age was 25. Most of the participants were graduate students in computer science and information technology, and one was Ph.D. candidate student studying in applied physics.

Table 2 shows the level of satisfaction (participant rating) after playing the sD&D game. The scale ranges from 0 to 10 points, and a satisfactory rating is considered to be a participant score of over 5 points. Overall, most of the participants have a positive response after playing the game, as shown in Table 2. However, question 1 (Game design interface according to ease of task completion) and question 2 (Understanding the rules of the game) still need significant improvement.

Table 3 lists open questions and the participant reason for the rating. Open questions include: “How does the game increase the players’ awareness of security education?” and “Do you want to play the game again or recommend the game to a friend or critic of the game?”. Most of the participants agree that the proposed game raises their knowledge of cybersecurity education and is accessible to play.

However, one of the participants found it quite challenging to start the game due to lack of information on the rules and the startup procedure. This small problem occurred because the participant did not go through the help menu.

6 Conclusion

In the present study, we proposed a cybersecurity game prototype that will be made available on our web site[1]. The game attempts to raise education awareness of cybersecurity issues, and primarily strengthens user knowledge of essential cybersecurity tools and software flaws that can be used in a cybercrime. By understanding the method of cybersecurity breaches, the prevention of information theft while using internet services can be avoided. Moreover, students who have studied networks and cybersecurity can fully comprehended the issues. As a result, a new approach to solving cybersecurity breaches can emerge.

The proposed mechanism characterized the simulation of a current cybersecurity network, implemented using the multicast socket developed in the Java programing language, combined with the tabletop card game concept. The simple game interface consists of rooms, cards, and a multiplayer display of a matrix of three by three rooms to be explored by the player during the game. Furthermore, evaluation experiments indicated that the scalability and performance of the game are quite reasonable.

Acknowledgements. A part of this research work was supported by the JSPS KAKENHI Grant Number JP18K11355.

References

1. Andriod: Netrunner. https://www.fantasyflightgames.com/en/products/android-netrunner-the-card-game/
2. Cetto, A., Netter, M., Pernul, G., Richthammer, C., Riesner, M., Roth, C., Sänger, J.: Friend inspector: A serious game to enhance privacy awareness in social networks. CoRR abs/1402.5878 (2014), http://arxiv.org/abs/1402.5878
3. Cone, B., Thompson, M., Irvine, C., Nguyen, T.: Cyber security training and awareness through game play. In: Security and Privacy in Dynamic Environments (SEC 2006), IFIP International Federation for Information Processing. vol. 201, pp. 431–436 (2006)
4. Denning, T., Lerner, A., Shostack, A., Kohno, T.: Control-alt-hack: The design and evaluation of a card game for computer security awareness and education. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. pp. 915–928 (2013)
5. Eagle, M.: Level up: a frame work for the design and evaluation of educational games. In: Proceedings of the 4th International Conference on Foundations of Digital Games. pp. 339–341 (2009)

[1] https://viscloud.ais.cmc.osaka-u.ac.jp/sdandd/

6. Ford, V., Siraj, A., Haynes, A., Brown, E.: Capture the flag unplugged: An offline cyber competition. In: Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education. pp. 225–230 (2017)
7. Gondree, M., Peterson, Z.N.: Valuing security by getting [d0x3d!]: Experiences with a network security board game. In: Presented as part of the 6th Workshop on Cyber Security Experimentation and Test (2013), https://www.usenix.org/conference/cset13/workshop-program/presentation/Gondree
8. Grigg, D.W.: Cyber-aggression: Definition and concept of cyberbullying. Australian Journal of Guidance and Counselling 20(2), 143–156 (2010)
9. Gustafsson, A., Katzeff, C., Bang, M.: Evaluation of a pervasive game for domestic energy engagement among teenagers. Computers in Entertainment (CIE) 7(4) (2009)
10. Irvine, C.E., Thompson, M.: Teaching objectives of a simulation game for computer security. In: Proceedings of the Informing Science and Information Technology Joint Conference (2003)
11. Jin, G., Tu, M., Kim, T.H., Heffron, J., White, J.: Game based cybersecurity training for high school students. In: Proceedings of the 49th ACM Technical Symposium on Computer Science Education. pp. 68–73 (2018)
12. Yasin, A., Liu, L., Li, T., Wang, J., Zowghi, D.: Design and preliminary evaluation of a cyber security requirements education game (sreg). Information and Software Technology 95, 179–200 (2018)

Table 3. Survey Open Question and Result

Open Question	Answer		
	P4	P5	P6
Briefly explain the reason for your ranking evaluation	Because of the lack of an initial explanation as to how to win this game and use resource cards in missions, players have difficulty in understanding what to do first.	I think it is a fun game that also has valuable cybersecurity knowledge elements in it.	I like this game, it easy to understand and fun to play. Also, the game requires you to use your mind to solve the problems.
What topic (security scenario) are most influenced you in understanding security issues?	Social media attacking	Hacking other people's account	
How did the tools (room and card) in the game help you to understand the security domain?	They were helpful in understanding that there are many tools for attacking IT devices. However, I could not understand the meanings of the commands and option parameters.	I was able to spend some more time playing in order to gain a deeper understanding of security as a whole.	The game is really good. The security domain is explained in game fashion, and you have to complete tasks to understand the domain.
How would you describe your knowledge of the security domain after playing this game?	I came to understand two things by playing this game. First, WPA2 keys are not always safe (WPA2 keys might be weak to dictionary attack). Second, leaving a personal electronic device (e.g., iPhone) somewhere people freely come and go (e.g., cafe or office) can increase the risk of a social media attack.	Moderate	My knowledge about the security domain has increased. Before playing game, I wasn't much aware of the security protocol, but now I know what can happen if I don't follow some instructions.
Do you want play the game again?	Yes	Yes	Yes
Will you recommend this game to a friend?	Maybe	Yes	yes
Critics of the game	I think this game can be helpful in learning about cybersecurity. In order for it to be more friendly to users, an initial explanation about this game is necessary.	The game is a great game to play but simplified instructions are needed for non-tech-savvy users.	The game was good.