Lord of Secure: the Virtual Reality Game for Educating Network Security

Vasaka Visoottiviseth[1], Atit Phungphat[1], Nuntapob Puttawong[1], Pamanut Chantaraumporn[1], Jason Haga[2]
[1]Faculty of Information and Communication Technology, Mahidol University, Nakhon Pathom, Thailand
[2]Information Technology Research Institute, National Institute of Advanced Industrial Science and Technology, Tsukuba, Japan
vasaka.vis@mahidol.edu, {atit.phu, nuntapob.put, pamanut.cha}@student.mahidol.ac.th, jh.haga@aist.go.jp

***Abstract*—At the present, the security on the Internet is very sensitive and important. Most of the computer science curricula in universities and institutes of higher education provides this knowledge in term of computer and network security. Therefore, students studying in the information technology area need to have some basic knowledge about the security in order to prevent the potential attacks and protect themselves from hackers or intruders. Unfortunately, the network security concept is moderately abstract when students learn in the traditional lecture-based class. In this paper, to motivate and help students to perceive better than in the traditional classroom, we propose a security game called "Lord of Secure", which is a virtual reality (VR) game on Android for education. It is an alternative learning materials for learners to gain the knowledge about the network security effectively. The game composes of main topics of the network security such as Firewall, IDS, IPS, and Honey pot. Moreover, the game will give the players knowledge about network security through the virtual world. The game also contains several quizzes including pretest and posttest, so players will know how much they gain more knowledge about network security by comparing scores before and after playing the game.**

Keywords— network security, virtual reality, edutainment, education game

I. INTRODUCTION

Computer and network security is an important topic in the computer science education. It helps students to realize the importance of security, how to protect the systems from hackers and intruders, and how to prevent the potential attacks. Network security system is usually deployed at the first line on the organization's security in order to protect the secret or authorize information transferred on the Internet. Most of the computer science curricula in universities and institutes of higher education provide this knowledge in a course focused on network security.

Although universities provide the security class, they use the the traditional way of teaching in the class room and using some technologies such as Microsoft PowerPoint and website to teach the student. This teaching style is passive and not interactive. Some students may not be interested enough in the subject and may not understand it well enough because they cannot imagine the real situation or how it related to their real life. Further, the abstract nature of network security concepts require perception and imagination, but not all students can learn in the same way. Therefore, the traditional lecture-based teaching techniques have often been considered insufficient to accomplish these learning objectives [1]. In this digital era where people are familiar with digital media, an additional mechanism to stimulate student interest and engagement in such a course is required.

This reason brings us to focus on the concept of educational entertainment or edutainment. It is a method that combines the entertainment with the education in order to make learning more enjoyable and engaging [2]. The entertainment can be any kind of audios, videos, films, games, and toys. The recent interest in virtual reality (VR), which is a technology that immerses a user's physical presence in a virtual environment through a head-mounted display, is making VR a viable platform for the creation of entertainment games named "Lord of Secure".

Our target users are university students or learners who have their backgrounds in computer and are interested in the network security concept. Developing application on VR platform on Windows and Android operating systems that are supported by Unity. Topics in the network security that are included in this application are the basic concept of network security, firewall, DMZ (Demilitarized Zone), Honey Pot, Intrusion Prevention System (IPS) and Intrusion Detection System (IDS).

For the contribution of this paper, we developed a virtual reality game for educating the network security concepts to IT students to understand the lessons easily and efficiently. Further, students will be motivated to learn by themselves through our edutainment VR game, which supports both on Android phones and on normal desktop computers. Here, we would like to emphasize that our game is designed as an additional learning method, not as a substitute to the traditional style of class-based learning.

II. RELATED WORKS

There are some related works that developed a game for educating users about the security concepts.

CyberCIEGE [3] enhances computer security education by providing a construction and management resource simulation similar to the Tycoon series of video games. There are interfaces that inform the user of the scenario status and the objective to be followed. The game includes various scenarios that force students to make a series of choices that potentially affect the security of enterprise assets. It assesses students' progress from the log generated during playing the game.

CyberAware [4] is a mobile game-based application for cybersecurity education and awareness running on Android platform. It aims to deliver the knowledge with a digital game-based activity that targets K-6 children. Moreover, the game includes the systematic design process for promoting and driving motivation during the learning process.

Anti-Phishing Phil [5] is an online web-based game developed by Carnegie Mellon University. It teaches players good habits to notice uncommon URLs to avoid phishing attacks. It is implemented in 2D using Flash 8. The game

978-1-5386-7805-3/18/$31.00 ©2018 IEEE

contents are loaded from a data file at the game start, including URLs and training messages.

Cloud Defense [6], is a tower defense style game that teaches Amazon Web Services (AWS) security protocols. Players defend their application against a hacker attacks with increasing levels of difficulty. Each level introduces a new challenge and "tower", which allows the players to practice the protocols by allowing good traffic to pass through the web infrastructure while protecting their database from malicious attacks.

Cyber Security Defender [7] is a game teaching about attacks from hacker and viruses. This game won the Gold medal in structure program award in 2015 Wecode Competition. In this game, the player will be a ball defender that protects the core center from the hacker or any other viruses. It also has some firewalls that are generated to block the viruses in the period of time for helping the player. The longer player survives, the harder level will be increased.

Cyber Wellness and Cyber Security Awareness [8] is a game that teaches nine types of security awareness to the user. It was designed on a multi-touch table for public users which was created by Playware Studio (Singapore) for the celebration of cyber security awareness day 2013. This game has many features to play because it teaches in different situations such as protecting a computer from viruses, creating a strong password, teaching how to use smartphone, building smartphone, how to use Wi-Fi to send data, how to protect Wi-Fi from other access, avoiding dangerous Wi-Fi, checking which website is fraud, and how to interact or respond to each situation.

TABLE I. COMPARISON OF RELATED WORKS

Features	CyberCIEGE	CyberA-ware	Anti-Phishing Phil	Intuit Cyber security game	Cyber Security Defender	Cyber Wellness and Cyber Security Awareness
3D Environment	YES	NO	NO	YES	NO	NO
VR technology	NO	NO	NO	NO	NO	NO
Instruction	YES	YES	YES	YES	YES	YES
Picture tutorial	YES	YES	YES	YES	NO	YES
Text tutorial	YES	YES	YES	YES	NO	YES
Pretest and posttest	NO	NO	NO	NO	NO	NO
Quiz	YES	NO	NO	NO	NO	NO
Game Chapter	YES	YES	YES	YES	YES	YES
Timing	NO	NO	YES	NO	NO	YES
Score	NO	YES	YES	YES	YES	YES
Result/Feedback	NO	NO	YES	NO	NO	NO
Hint/Navigation	YES	YES	YES	NO	NO	YES

Table I compares six related works based on the features that we consider for Lord of Secure. The description of each feature is as follows.

- *3D Environment*: A game is created in the 3D environment, which is computed in three directional dimensions. The player is able to interact with environment freely.
- *VR technology*: A system supported VR technology that immerses a user's physical presence in a virtual environment through a head-mounted display.
- *Instructions*: To demonstrate the player how to play, control, and win a game.
- *Picture tutorial*: Providing some knowledge about network security through pictures.
- *Text tutorial*: Providing some knowledge about network security through texts.
- *Pretest and posttest*: A function that tests player's basic knowledge about network security before playing and after playing.
- *Quiz*: Some challenges for player to measure understanding for each module in game.
- *Game Chapters*: Including games; and the higher chapter is more difficult and challenging.
- *Timing*: A timing system to count the time that a player need to pass each chapter in the game.
- *Score*: Scores will be accumulated when the player achieves the mission, objective or pass a chapter.
- *Result/Feedback*: When the player passes or fails a mission in each chapter, the system will show the results and feedback.
- *Hint/Navigation*: Hint system will help the player to find a way to pass the chapter.

III. SYSTEM DESIGN

A. System Architecture Overview

Lord of Secure contains five main modules which are game interaction, teaching, game play, pretest and posttest, and the menu. The teaching system will get the signal that the player interacts with the system to perform the task in the game, and pretest and posttest will be in the form of quiz. Menu is the shortcut for a player, when he is in the game so that a player can go back to main menu, select a new chapter, restart, or quit the game.

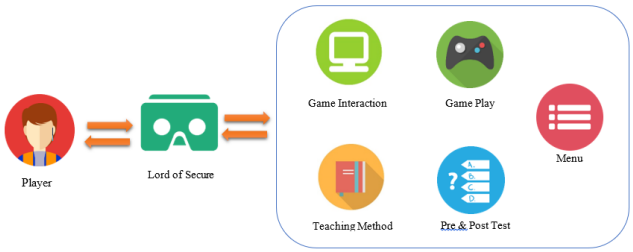

Fig. 1. System Architecture of Lord of Secure Game

B. Game Story and Chapter Design

In our game, a player is assumed to be the main character named "Hackita" who is one of the soldier in the Luna Kingdom. One day the princess named "Arwy" is kidnaped, and the king "Sautron" order Hackita to take her back from Kondora Kingdom.

Fig. 2 shows the chapter design of this game. This Lord of Secure game is separated into three chapters which are forest (network security), desert (firewall), and Kondora kingdom (IDS/IPS & honeypot).

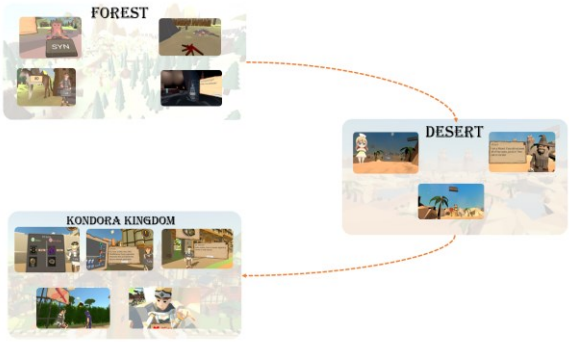

Fig. 2. Chapter Design

a) Chapter 1: Network Security Concepts

The theme of Chapter 1 is the forest where the player will be educated about the basic concepts of network security. Network security contents in this chapter contain TCP three-way handshake, TCP covert channel, IP address spoofing, flooding, and malicious software.

In this chapter, the player has to walk through Malware forest. The player will get the knowledge of various types of attack in network security concept, and it has a system to test the player's knowledge about IP address spoofing, TCP Covert Channel, and flooding. Firstly, player will find a villager in front of the forest. The player and villager will greet each other like doing the three-way handshake in TCP. Next, the player will find a village, and he has to do every quests completely to pass this chapter.

There are several quests in the forest. To educate the player about TCP Covert Channel, the game will require the player to swipe a letter to get an ax handle. Next, the player needs to swipe the card from Kondora soldier (IP Address spoofing) to get an ax blade. After getting both partitions, player can use an ax to cut trees that against the unknown entrance. The player needs to enter the witch kingdom to help the villager's daughter and stop the witch by overflowing the holy river. This one will deliver the knowledge about the flooding attack. Moreover, a player will get some knowledge about malicious virus in the witch kingdom.

b) Chapter 2: Firewalls

After the player exits from the forest, he will enter the desert where the player will be educated about four kinds of firewall, which are stateful, stateless, circuit firewall, and proxy application gateway. Furthermore, a player can do some exercises with a wizard before doing the posttest.

c) Chapter 3: DMZ IDS/IPS

Chapter 3 is the last chapter which educates the player about DMZ, IPS/IDS, and honeypot. The player needs to destroy the crystal or seal at every firewall such as circuit firewall, stateful firewall, stateless firewall, and proxy gateway firewall to pass this chapter. Moreover, player can meet the wizard to practice before do the quiz to pass the wall.

Before entering into Kondora kingdom, he needs to pass IPS security guard to check player's belonging. Then, player can find the village in the kingdom that can be referred to DMZ zone in network, and honeypot that trick the player if player answers a wrong one. This area in Kondora kingdom compares as DMZ with an external firewall which have a trap for luring people who are not in the kingdom of Kondora to get in. The luring trap is a fake castle or Honeypot. Kondora kingdom has soldiers who walk in front of the castle for inspecting the suspect people (comparing as a IDS in the network security concept). Finally, Hackita reaches Arwy room and takes her back to Luna kingdom.

C. Structure Chart

Fig. 3 illustrates three main functions in Lord of Secure game, which are the teaching system, practice system and interface. Detail of each module is described as below.

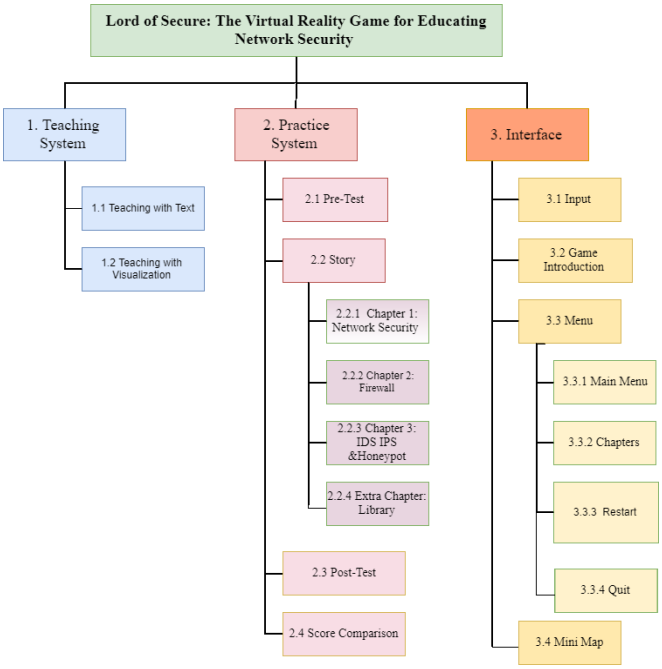

Fig. 3. Structure Chart of Lord of Secure Game

1. Teaching system

1.1. Teaching with text – Teaching with text the most basic communication with a player. For example, the detail about how firewall, IDS, IPS operate in the network which be shown in the game for easily understanding.

1.2 Teaching with visualization – Teaching with visualizations will help a player to understand how network security operates which is clearer than an alphabet. Each visualization such as video in the game will be used to as descriptive tools. It will be more entertain and interesting than traditional lecture base teaching in the class.

2. Practice system – Practice system is a module that operates the contents in the game. There are four main functions which are pretest, story, posttest, and score comparison. The details about each function will be described below.

2.1. Pretest – Before processing the story, a player needs to do the pretest for checking the basic knowledge of the player which is used to collect the score

before and after when the game is finished. Moreover, the lecture can adjust the test by just changing the configuration file of this game.

2.2. Game story– This module is for testing the knowledge of the player through the game. A player needs to pass the test of each chapter.

2.3 Posttest – After the player finished the whole game completely, a player has to perform the posttest in order to calculate the final scores. Moreover, the lecture can adjust the test by changing the configuration file.

2.4 Comparing between pretest and posttest scores – Scores that player gathers from performing the pretest and posttest will be compared and shown to the player at the end of the game.

3. Interacting system – Interacting system is the module that manages the interaction between a player and the system. There are three main functions which are Input, Recommendation, and Setting.

3.1. Input – Receiving any action from the player by moving the player's head to interact with the item. It also uses to solve the problem and learn any information inside the game.

3.2. Recommendation – This function uses to suggest any controlling or configuration before game start. A player can also open this function during the gameplay.

3.3. Menu – This function allows a player do several things when a player is in the game which are going back to main menu, selecting new chapter, restart, and quit the game.

3.4 Mini map –It is a map at the top left corner of the screen. It is like a navigation that helps a player to prevent losing in the game. We developed this function according to the user feedback from the preliminary evaluation.

IV. Implementation

A. Hardware and Software Specifications

TABLE II. Hardware and Software Specifications

Component	Specifications
Laptop	OS: Windows 8.1 64-bit CPU: Intel Core i7-4720HQ (2.60 - 3.60 GHz) RAM: 8 GB Graphic Card: NVIDIA GeForce GTX 965M
Smartphone	OS: Android 5.0 Brand: Samsung Model: Galaxy Note 3 LTE SM-N900 CPU: (A15 1.9 GHz + A7 1.3 GHz) Octa Core RAM: 3 GB Display: 1920x1080 @ 386 PPI
Editors	Unity 3D – Game Engine Microsoft Visual Studio – C# Scripting Blender – 3D objects and environments Android Studio – Establishing building-connection of Android smartphone
Database Management System (DBMS)	DynamoDB with Playfab API
Programming and Scripting Tools	C#

Table II shows the hardware and software specifications of our Lord of Secure game. We develop two versions: Android version and PC version. Unity is the main programming language to develop this virtual reality game.

B. Screen Outputs

Fig. 4. First Menu Screen

When a player starts the game, the first menu screen will be shown. It consists of five functions which are start game, continue, how to play, result, and quit as shown in Fig. 4.

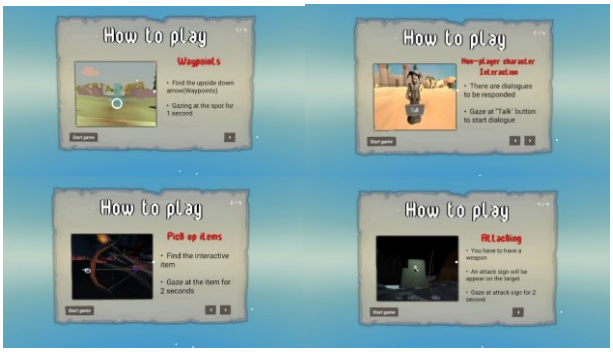

Fig. 5. Introduction about how to play this game

In how to play function, player will be introduced about how to play or interact with objects in this game. For example, when a player need to walk, he/she needs to put a pointer on the arrow for 1-2 second. To interact with NPC, pick up the item, and attacking, a player needs to move a pointer on a button or item, and click (PC version) or hold on for (VR version) as shown in Fig. 5.

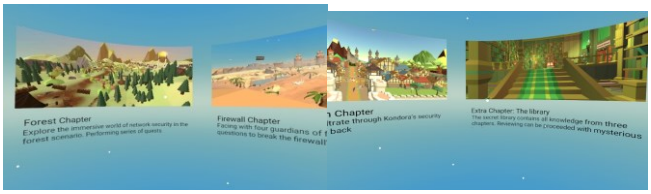

Fig. 6. Chapter Selection

After player clicks "start game" button, player can select chapters in the game that they need to play. Initially, player need to pass chapter 1 first before a player can select others chapters. There are 3 chapters in the game which are Forest (network security), Desert (firewall), and Kondora Kingdom (IDS/IPS & honeypot). Moreover, there is a library where a player can come and review the content that he/she has learnt in the extra chapter "the Library" as shown in Fig. 6.

The first chapter is forest that is the path to go to Kondora Kingdom. This chapter educated a player about network security such as TCP covert channel, IP address sproofing, flooding, and some malware as shown in Fig. 7.

Fig. 8 illustrates Witch Kingdom. A player needs to help kidnapped girl and take down the witch. This scene educates player about flooding and malware. Fig. 9 is the second chapter of this game that will educate a player about each type of firewall.

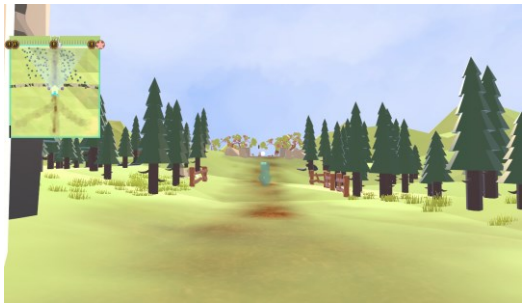

Fig. 7. The First Chapter "Forest"

Fig. 8. Witch Kindom

Fig. 9. Chapter 2 "Desert"

Fig. 10. Chapter 3 "Kondora Kindom"

Fig. 11. IDS Guard and Bad Behavior Man

Fig. 10 shows the entrance of Kondora Kingdom that is the last chapter of this game, and a player will meet with princess Arwy. This chapter educates a player about DMZ, IPS/IDS including honeypot in the network.

Fig. 11 shows that IDS guard can detect the bad behavior and direct him to the honeypot. Fig. 12 shows the ending scene and the score board that shows pretest and posttest that a player performed. Fig. 13 shows the extra chapter that consists of book that a player has learnt in the previous chapters, so that he/she can review his/her knowledge. Fig. 14 shows the example of pretest, posttest and quiz in the game that a player need to perform in each chapter.

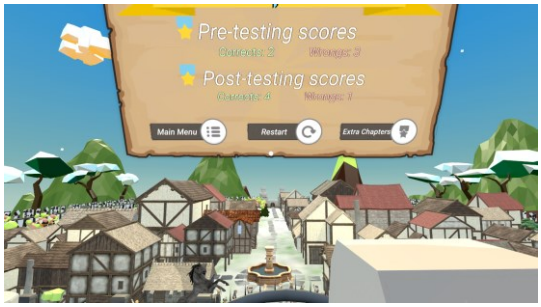

Fig. 12. Ending and the Score Board

Fig. 13. Library and Knowledge

Fig. 14. Pretest, Posttest and Quiz

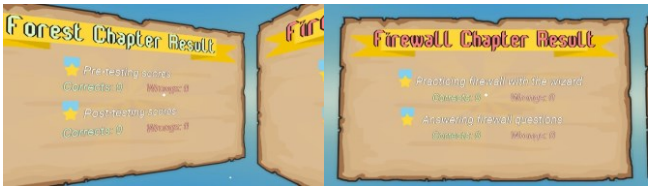

Fig. 15. Results of each chapter

Fig. 15 shows the result of all chapters that a player finish playing this game. The purpose of this function is that a player can know his/her improvement after playing each chapter. To see this score, a play need to select 'result' button in the first screen of this game.

V. Evaluation Results

The target users of Lord of secure are students who study in IT area and other students who are interested in network security. There are 33 students in total that joined our testing and evaluating the system. We separated the evaluation process into two main topics, which are the evaluation of playing with VR headset equipped with the Android phone and the evaluation of playing with PC version.

In the first evaluation, we evaluated the graphical user interface using VR headset with five male IT students. 80% of them have a little knowledge about the network security. Most of them told us that some of interactive objects are hard to interact by the VR headset, and some walking path in our VR game is not clear. Moreover, they are not giddy when they are playing with VR headset, whereas, some of them feels a little bit giddy. In addition, 60% of them like our graphics through VR headset, but 80% of them told us that the Ray-casting system responded slowly.

In the second evaluation, we evaluated 28 students; and more than 80% of them have basic knowledge about network security. In UI testing, some participants confused some walking paths in Chapter 1. As in Fig. 16 and 17, there are more than 90 % of participants understand well with the teaching method, and 82% of them think they can understand the contents more than in the class room. Some participants think that some buttons are hard to interact, and most of participants like the game story.

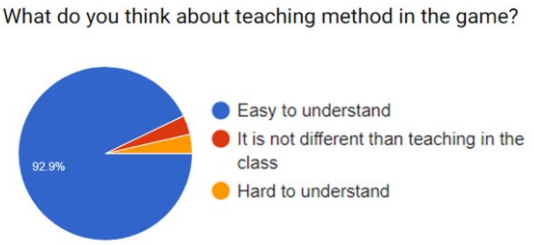

Fig. 16. Questionnaire results about the teaching method in the game

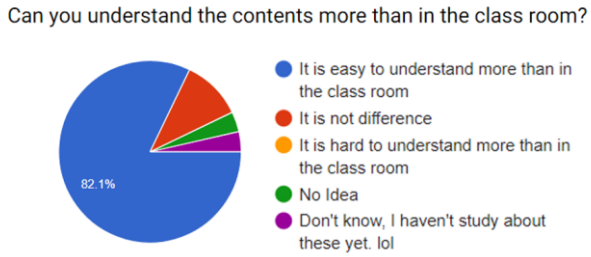

Fig. 17. Questionnaire results about the contents of the game

Moreover, in the evaluation of contents, most of participants cloud understand the content easier more that in the class room. As shown in Fig. 18, most students had the posttest scores higher than the pretest scores. Note that, in Chapter 2, which teaches about the firewall rules, we do not have the pretest, but the player has to pass the quizzes at the end of the chapter. In addition, the participant would like us to feed more content into the game and fix some buttons and interactive place to be interacted better.

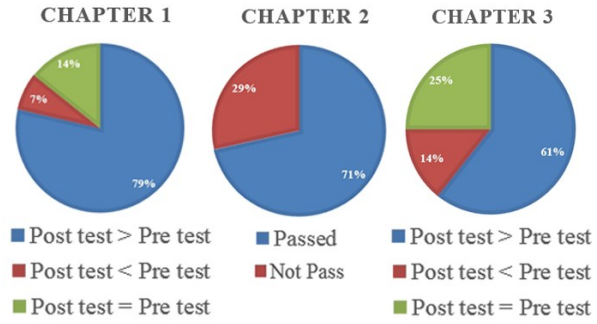

Fig. 18. Comparing pretest and posttest scores of each chapter

VI. Conclusion and Future Works

Our Lord of Secure game is developed to help IT students to learn and understand the network security lessons easily and to make the contents more exiting, interesting, and understandable by using VR technology. We aim to motivate students to learn by themselves through our edutainment game. From the evaluation results, most of participants are interested about adapting VR technology with the academic. They can understand the contents that are fed into the game easily. Therefore, the evaluation result shows that students enjoyed learning through VR game, and this game can be an alternative way to learn about the network security concept. For our future work, Lord of Secure should be developed to support more platforms such as iOS platform and also support multiple players. Further, we should provide a graphical interface for lecturers to add or change the contents in the game. Currently, we just allow them to modify the pretest and posttest questions from the text-based configuration files. Moreover, after a player finished playing this game, he should be able to share the results on the social media such as Facebook, or Twitter.

References

[1] En.wikipedia.org. (2017). Network security. [online] Available at: https://en.wikipedia.org/wiki/Network_security [Accessed 7 Oct. 2017]

[2] Wikipedia.org, “Educational Entertainment”. [Online]. Available: https://en.wikipedia.org/wiki/Educational_entertainment

[3] C.E. Irvine, M.F. Thompson, “CyberCIEGE: gaming for information assurance” IEEE Security & Privacy (Volume: 3, Issue: 3, May-June 2005)

[4] Filippos Giannakas, Georgios Kambourakis, Stefanos Gritzalis, “CyberAware: A mobile game-based app for cybersecurity education and awareness” in Interactive Mobile Communication Technologies and Learning (IMCL), 2015 International Conference on.

[5] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth Nunge, "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish," in Proceedings of Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA.

[6] Intuit Cyber security game. [online] Available at: https://www.youtube.com/watch?v=_3VLx0pXSYs [Accessed 7 Oct. 2017].

[7] 2015 WeCode National Competition : Cyber Security Game - Lim Yu Cheng From SJK(C) Puay Chai 2. [online] Available at: https://www.youtube.com/watch?v=Bb_gGq1QMUU [Accessed 7 Oct. 2017].

[8] Cyber Wellness and Cyber Security game for the IDA. [online] Available at: https://www.youtube.com/watch?v=g7Mz9vFceMU [Accessed 7 Oct. 2017].