Educational Aids for Teaching Hacking Principles to Strengthen Computational Thinking Skills to Elementary

Yujin Jung
Jeju National University, Jeju, South Korea. E-mail: yujinjung@jejunu.ac.kr

Eunsun Choi
Jeju National University, Jeju, South Korea. E-mail: choi910624@jejunu.ac.kr

Namje Park*
Jeju National University, Jeju, South Korea. E-mail: namjepark@jejunu.ac.kr

Received September 26, 2021; Accepted December 19, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V19I1/WEB19299

Abstract

Modern society is changing into an era of digital transformation with the development of advanced information and communication technology (ICT) and information systems. Various information is digitized and stored, and the value of information is increasing. As the value of information increases, hackers' techniques to take advantage of unfair profits using them are subdivided and advanced, causing unexpected big problems in society. In particular, it was noted that cases in which elementary school students, a digital native generation, are often reported to be involved in crimes. Therefore, based on the basic concepts and principles of computing for elementary school students, we developed a learning teaching tool that can provide hacking-related education in an interesting way using gamification based on computing thinking ability that can efficiently solve unexpected problems. The learning goal was set for the development of educational aids by analyzing the cyber-attack process, and the game material was selected by applying the information security hacking principle learning to Samuel Livingstone's simulation game model. Then, we set game figures, roles, resources, external factors, and goals of the educational game and designed game boards, mission papers, and worksheets. We also established the game rules using the game data designed. Lastly, we found complementary points with security experts and education experts to supplement the learning aid while running the game. This paper helped learners to understand the security equipment applied in the network environment. In the end, we developed a teaching aid that can strengthen learners' computational thinking and understand hacking principles. This game ensures infinite scalability of the challenge by having students perform three missions per challenge. The educational aids proposed in this paper are limited at the primary level that elementary school students can understand. However, it can be designed and extended to infer interleaving by combining transaction and lock functions.

Keywords

Hacking principles, educational aids, computational thinking skill, gamification, network environment, Cyber-attack, Elementary students.
Introduction

The recent increase in demand for non-face-to-face technology due to coronavirus-19 emerged in the early 2010s in an integrated form of artificial intelligence, Internet of Things, cloud computing, big data solutions, and mobile. In addition, in line with the development of advanced information and communication technology (ICT) platforms such as blockchain, it accelerates digital transformation. As a result, society has begun to build a new ecosystem through 'computerization' and 'digitalization.' Accordingly, information in the information society has become much more important value than the past (Agron et al., 2020; Namje et al., 2018). Whether it is the provider who provides the information or the user who uses it, the computer of the person using it stores much personal information.

As the value of information increases and the life using computers diversifies in society, hackers who try to hack information to make unfair profits are becoming denser, and hacking techniques are being subdivided and advanced. However, the age group using computers is rapidly expanding in their 20s to 40s, but it is difficult to escape the threat of hacking unless they are all computer experts. The Korea Internet & Security Agency (KISA) (2020) predicted that the number of reported infringement accidents in Korea would increase as hacking attack methods become intelligent and diversified. Graphs of the number of hacking accidents over the past ten years are published, raising awareness (KISA, 2020). The cause of the increase in cyberattacks is a rapidly developing information society. The development of an information society has a problem that must be solved based on understanding the power and constraints generated by computing based on flexible thinking skills. Computing thinking skills are needed to solve this problem. Improving computing thinking skills can develop students' problem-solving skills and further understand how to apply various means to solve problems (Choungbae, 2020; Yujin et al., 2020; Hitoshi et al., 2010). We live in an environment where the individual distribution of information devices has been expanded due to non-face-to-face classes (Namje et al., 2018). In an environment where the individual distribution of information devices is expanding due to non-face-to-face classes, the concept of information security is lacking (Namje et al., 2018; Yujin et al., 2019)

In this paper, we intend to provide education on hacking principles in information security for students and the general public in elementary and secondary courses who relatively lack the concept of information security. Simulation unplugged learning teaching tools have been developed to make it easier for learners to access technical parts to cultivate their ability to protect information. Assuming a situation where you can be attacked on the network, learn how to defend yourself, such as being a hacker and trying to attack, and
installing a device so that hacking fails. It strengthens the learner's ability to solve problems. Therefore, it prevents committing a crime by not being aware of security while accessing a computer (Eunkyung et al., 2021; Jinsu et al., 2020). In the developed education aids, learners become hackers to understand the principles of hacking, learn the causal relationship, and actively strive to find the best defense by applying simulation game elements. In the hacking principle game proposed in this paper, it is possible to teach principles for senior elementary school students, and in the case of lower grades, it is desirable to teach and learn HACK and DEFENCE stages after explaining basic knowledge related to hacking.

**Methods**

Although information security education uses high connectivity with actual life and higher thinking ability in the learning process, it is not easy to use it due to high barriers in the specialized field. Examples of learning and teaching aids combined with board games developed for vocational career education for some information security experts can be examined as follows. First of all, in a domestic case, Ko et al (2014) mentioned the effect of developing practical information security learning and teaching tools through hexagonal cell-based mock hacking activities to quickly learn the functional principles of hackers through Nol's techniques and recognize the importance of information security(Yeonghae et al.,2014). Lee et al (2016) developed elementary network information security learning textbooks and teaching aids using gamification mechanisms to image message flows between clients and servers so that they can visually grasp the movement path between cells and firewalls(Donghyeok et al., 2016).

Overseas examples include cybersecurity logic games developed by Engelberg(2018). This game has become an agent to stop cybercriminals and is a board game that performs step-by-step missions to experience programming(Mark et al., 2018). Gasiba et al (2020) analyzed cybersecurity games for security programming and analyzed that training awareness structure to solve cybersecurity problems as security coding technology games affect improving security awareness (Tiago et al., 2020). This paper intend to provide technical education that requires professional knowledge such as cyberattacks to cultivate talent in a more diverse professional technology field and advanced future information society, including the advantages of the unplugged game method. This worksheet and tools were designed under the theme of hacking to reach the destination from the attacker's point of view. For the design of learning, the process of an attacker reaching the target on the network can be seen as finding
the target's network path and reaching the target through the target's security equipment. Figure 1 briefly explains the process of cyberattacks.

![Figure 1. Process of Cyber Attack](image)

**Results**

In order to prevent learning on the principles of information security technology from being shunned by learners, not experts, learners can be set as hackers, and the process of stealing files and fleeing safely can be programmed only with a simple direction key. In the next step, the program code in the previous step was analyzed to find security vulnerabilities, find ways for learners to change the program and infect the virus, and finally, the program can be protected using knowledge of the system's weaknesses found in the previous two steps. To protect the program, the program is modified to prevent cyberattacks with alarms and transactions, which are intrusion detection systems. Figure 2 shows the design of this hacking principle learning and teaching game flow chart. As the stage continues, learners can modify their algorithms by performing new missions in a more complex environment through coding, defense, and fix stages.

![Figure 2. Game flow chart for teaching hacking principles](image)
The development procedure of the hacking principles learning tools was set up as shown in Table 1, referring to the modeling procedure of the simulation game proposed by Samuel Livingstone (1973), and fused to the development procedure (Samue, 1973). The simulation game model procedure proposed by Samuel Livingstone is often cited in domestic published papers related to game development such as board games. Livingstone’s simulation game was described as setting learning goals, selecting materials, designing structures and materials, and implementing and modifying rules after writing them.

<table>
<thead>
<tr>
<th>Setting Learning Objectives</th>
<th>Choosing Game Materials</th>
<th>Game Structure Design</th>
<th>Game Materials Design</th>
<th>Game Rule Development</th>
<th>Evaluation &amp; Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Education</td>
<td>Applying information security hacking principle learning to game model</td>
<td>Setting the role of the game figures, resources, external factor goals, etc.</td>
<td>Game board, mission paper, and worksheets design</td>
<td>Developing the game’s objectives, procedure, players’ roles and rules as steps</td>
<td>Running and modifying the game</td>
</tr>
</tbody>
</table>

Looking at the contents of the step-by-step development, students can learn the importance of information security through hacking games and devise a hacking principle algorithm in determining the first-step learning goal. In the second step of hacker game material selection, learners can learn to become hackers and steal files safely from security devices. In the third step of designing the game's structure, the game board consists of 16 tile grids of 4x4, with five rotating platforms on the board, two clockwise and three counterclockwise. The learner sees the five rotating platforms and tiles that control each movement on the mission paper and places them as initial settings for each stage on the board. On the game board, there is one hacker, three arrow keys, one rotating panel, a file panel that is the hacker's goal, and a honeypot that attracts hackers to induce hacking to fail. In addition, it was designed as an exit to indicate the success of the final mission and alarm that can prevent hacking attempts by safely terminating the program when the hacker touches it. Table 2 shows the components of the game, the primary role contents, and the name of the system confronted for learning the role in this learning lesson.

<table>
<thead>
<tr>
<th>Game Components</th>
<th>Main roles</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker</td>
<td>Players of the game</td>
<td>-</td>
</tr>
<tr>
<td>Arrow key</td>
<td>Choosing hacker’s direction</td>
<td>Router</td>
</tr>
<tr>
<td>Rotation panel</td>
<td>Clockwise and counterclockwise moving</td>
<td>Traffic</td>
</tr>
<tr>
<td>Data file</td>
<td>Data hackers want to steal</td>
<td>Client</td>
</tr>
<tr>
<td>Alarm</td>
<td>Notification for hackers’ intrusion</td>
<td>IDS/IPS</td>
</tr>
<tr>
<td>Honey pot</td>
<td>Inducing hacking failure</td>
<td>Honey pot</td>
</tr>
<tr>
<td>Exit</td>
<td>Hacking success</td>
<td>-</td>
</tr>
</tbody>
</table>
In order to proceed with hacker games in the four-step game materials design, game manuals, mission papers, and worksheets for algorithm design at each stage, panels and game figures that can directly implement each role on a board are needed. The game is basically played by arranging game icons such as game pieces, data, panels, and honeypots on the board. The left of Figure 3 is an example of arranging panels and game pieces on the board, and the right is a worksheet that can simulate the path to the exit by setting the direction of the hacker X. On the board, each icon represents a hacker (👨‍💻), a data file (📄), an exit (🚪), a honey pot (🍯), and a rotating panel (🔄). The hacker picks up the data file and performs a mission to go out without touching the honey pot.

**Figure 3. Game board and worksheet**

In step 5 of setting game rules, simulation of attacker and defender of hacking is coded over three steps of HACK, DEFENCE, and FIX. The instructor ensures that the learners (players) achieve the goal within a set number of times. The players can set the movement direction in four directions: left, right, up, and down.

In the HACK stage, the attacker in the learners aims to obtain data and escape through the exit. Hacker X envisions an algorithm to get to the exit point without falling into the honey pot. In the HACK stage, players have to write code using only three arrows keys. Hacker X picks up the data file and determines the direction of movement by examining the board to reach the corresponding endpoint (exit). The players could test according to the code they wrote. At this time, it rotates one space according to the arrow of the traffic. Hacker X wins if he or she picks up the file and arrives at the exit point following the last movement instructions. Winners leave the written code as it is and move on to the DEFENCE stage.
In the DEFENCE stage, the players analyze the program code in the HACK stage to find security vulnerabilities. The way to find security vulnerabilities is to find out how hackers can change programs and infect them with viruses. The purpose of the DEFENCE stage is to induce the learner who is the defender to the honeypot so that the attacker cannot escape. The learner must reach the destination by changing only the three movement directions set in the Hack stage and the order of the variables set by the instructor. It is considered a failure if students exceed the set number of times or reach a destination other than the destination. For the player to win, return the game board according to the original settings described in the mission paper and move the arrow keys and the rotation panel only left and right on the worksheet to get Hacker X to the honey pot. Winners leave the written code as it is and move on to the FIX stage. In the FIX stage, an alarm is installed after determining the game board's space, the honey pot location, and the end location. When Hacker X comes in contact with the alarm, the alarm is triggered, and the program devises an algorithm to end the program safely.

In the FIX stage, the alarm is installed in the attacker's movement path to understanding the attacker's intrusion attempt. The learner becomes a defender and can install an alarm variable in a space in the worksheet. The learner should configure the attacker to move to the honey pot immediately after reaching the alarm. A failure is considered if the attacker does not pass the alarm or does not reach the honey pot. However, when tracking a hacked program, an alarm must be triggered before Hacker X reaches the honey pot. If an alarm is placed on the game board and the program coded in the DEFENCE stage and the program coded in the HACK stage are not disturbed, the players win. After completing the HACK, DEFENCE, and FIX stage, players can move to the next stage.

In the final 6th step, the inspection and correction stage was designed so that the hacker game would reach the endpoint by selecting the data file. In addition, it was conceived as a setting to protect against cyberattacks by finding security vulnerabilities and supplementing system weaknesses. Finally, it is developed into a high-quality learning tool by supplementing and correcting problems found in the implementation process. Figure 4 schematically shows the flow of each procedure of HACK, DEFENCE, and FIX per each stages.
This game allows students to perform three steps of missions per one challenge to ensure the infinite expandability of the challenge. In this paper, only the basic level that elementary school students can understand is mentioned. For learners who have completed this task, it can be conceived to learn the lock function and transaction function to control concurrency by repeating the challenge. Furthermore, we design that hackers can design extensions to allow players to reason about interleaving through locking, using strategies similar to those used by real programmers.

**Conclusion**

As the value of information increases in the information society, related crimes are rapidly increasing, but the age of users is decreasing, and preparation for this is insufficient (Sameer et al., 2013; Namje et al. 2019). Moreover, the problems faced in the era of digitization of everything in which ICT and software technologies in various fields are grafted require convergence, creative thinking, and practical ability that crosses various fields of knowledge.

Therefore, we design the education aids for learners to cultivate computational thinking skills with these problem-solving capabilities. Computational thinking ability was found to be related to information education among various activities through the operating principle of computers, as shown in the unplugged computing. Therefore, the information education course designed a security logic learning tool as a hacking game, focusing on exploring and enhancing computational thinking skills through education that applies advanced thinking skills such as communication skills, problem-solving skills, and creativity to each activity.

In addition, the learner became a hacker, learning the algorithm on his own and completing each step.
The hacker game presented in this paper induces engaging learning by focusing on the meaning of attack and defense of each icon rather than the description and role of the system so that learners at the upper elementary level can learn. The goal is to develop computational thinking skills by devising a technology algorithm for information security rather than interest as the stages are repeated. In the future, we will operate and verify elementary and middle school students and the general public, education experts, and related technical experts by pilot classes. Moreover, we will execute pre/post and satisfaction tests. We will conduct continuous research to complete more advanced educational tools for teaching information security through systematic effectiveness and satisfaction analysis.

**Acknowledge**

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A5C2A0408374). And, this work was supported by the Korea Foundation for the Advancement of Science and Creativity(KOFAC) grant funded by the Korea government(MOE).

**References**


