Journal of KIIT. Vol. 19, No. 5, pp. 111-119, May 31, 2021. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2021.19.5.111

사이버 공격 및 방어 해킹 원리 언플러그드 학습교구 디자인

정유진*, 박남제**

Design of Unplugged Learning Tools for Cyber Attack and Defence Hacking Principle

Yujin Jung* and Namje Park**

This work was supported by the Korea Foundation for the Advancement of Science and Creativity(KOFAC) grant funded by the Korea government(MOE). And, This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A5C2A04083374).

요 약

정보 시스템의 발전은 첨단 정보통신기술(ICT) 플렛폼과 맞물려 현대 사회를 디지털 전환의 시대로 이끌어 나가고 있다. 이는 점차 현대사회가 고도화된 내용의 정보화 사회로 변환하고 있음을 의미한다. 정보의 가치가 높아지면서 이를 이용한 부당한 이익을 챙기려는 해커의 기법은 세분화되고 고도화되고 있지만 정보사회의 구성원으로서 정보윤리와 정보보호의 필요성이 요구되는 만큼의 교육은 이루어지지 않고 있다. 본 논문에서는 학습자 스스로가 정보를 보호할 수 있는 능력 함양을 할 수 있도록 기술적인 부분을 보다 쉽게 접할 수 있는 시뮬레이션 언플러그드 학습교구를 개발 하였다. 본 논문에서 설계한 학습교구는 네트워크 환경에서 적용되는 보안장비의 역할을 수행하는 패널들을 구성하여 공격을 수행하도록 함으로써 학습자에게 네트워크에서 적용될 수 있는 보안장비의 역할을 이해하도록 도움을 주어 학습자의 컴퓨팅 사고력을 강화하는 것을 목적으로 한다.

Abstract

The development of information systems leads modern society into the digital era along with the advanced information and communication technology (ICT) platform. It means that modern society is gradually transforming into an information society with advanced content. As the value of information increases, hackers' techniques to take advantage of unfair profits using it are becoming more subdivided and advanced. However, as a member of the information society, education is not provided as much as information ethics and information protection are required. In this paper, we developed a simulation unplugged learning tool that allows learners to access technical concepts more easily to develop their ability to protect information. The learning tool designed in this paper composes panels that play the role of security equipment applied in a network environment to perform an attack. It aims to strengthen learners' computational thinking ability by helping learners to understand the role of security equipment that can be applied in the network.

Keywords

information security education, unplugged computing, board game, cyber attack, hacking simulation

* 제주대학교 융합정보보안학협동과정 박사과정, 과학기술사회연구센터 책임연구원
- ORCID: https://orcid.org/0000-0001-9275-1511
** 제주대학교 초등컴퓨터교육전공 교수(교신저자)
- ORCID https://orcid.org/0000-0003-4434-8933

· Received: Mar. 08, 2021, Revised: May 25, 2021, Accepted: May 28, 2021
· Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

최근 코로나바이러스-19(Coronavirus: Covid-19)로 인한 언택트(Untact) 기술의 수요 증가는 2010년대 초반 AICBM으로 통칭되는 인공지능(Artifical intelligence), 사물인터넷(Internet of things), 클라우드(Clould) 컴퓨팅, 빅데이터(Big data) 솔루션과 모바일(Mobile)의 통합된 형태로 나타난 블록체인 등 첨단 정보통신기술(ICT) 플랫폼의 발전과 맞물려 디지털 트렌스포메이션(Digital transformation)으로의 변화를 앞당기고 있다.

사회는 '전산화(Computerization)'와 '디지털화(Digitization)' 과정을 통해 새로운 생태계를 구축하기 시작하였고, 이에 따라 정보화 사회에서의 정보는 이전보다 훨씬 더 중요한 가치를 지니게 되었다[1].

정보를 제공하는 공급자의 측면이든 정보를 사용하는 사용자의 측면이든 컴퓨터를 사용하는 사람의 컴퓨터는 많은 개인정보를 저장하고 있고. 정보의 가치가 높아질수록, 사회에서 컴퓨터를 활용한 생활이 다양화될수록 정보를 해킹하여 부당한 이익을 챙기려는 해커들은 치밀해지고 해킹 기법은 세분화·고도화되고 있다. 그러나 컴퓨터를 사용하는 연령대는 20대~40대에서 급속히 확장하고 있지만 모두 컴퓨터 전문가가 아닌 이상 해킹의 위협에서 벗어나긴 어렵다. 한국인터넷진흥원(KISA)에서는 해킹 공격 방법이 지능화·다양화됨에 따라 국내 침해사고 신고 접수 건수도 증가할 것으로 전망하였으며 최근 10년간의 해킹사고 건수의 그래프를 그림 1과 같이 발표하고 경각심을 일깨우고 있다[2].

그림 1. 연도별 해킹 사고 건수 [2]
Fig. 1. Number of hacking accidents by year [2]

사이버 공격 증가의 원인에는 급격히 발전하는 정보 사회가 있다. 정보 사회의 발전에는 유연한 사고력을 기반으로 현대 사회에서 컴퓨팅에 의해 발생하는 힘과 제약사항에 대한 이해를 기반 문제를 해결하는 컴퓨팅 사고력이 요구된다. 컴퓨팅 사고력의 향상은 학생의 문제해결능력을 발전시킬 수 있으며, 나아가 문제의 해결을 위해 다양한 수단을 적용하는 방안을 이해할 수 있다[3]-[5].

본 논문에서는 비대면 수업 등으로 인한 정보화 기기의 개별 보급으로 인하여[6] 상대적으로 정보보안에 대한 개념이 부족한 초·중등 과정의 학생 및 일반인을 대상으로 사이버 공격 과정에 대한 정보보안분야 해킹 교육을 실시하기 위해 학습자 스스로가 정보를 보호할 수 있는 능력 함양을 할 수 있도록 기술적인 부분을 더 쉽게 접할 수 있는 시뮬레이션 언플러그드 학습교구를 개발 하였다. 이를 통하여 학습자의 문제해결 능력을 강화하고 컴퓨터를 접하면서 보안의 개념을 제대로 인지하지 못하여 범죄를 저지르는 사례를 방지할 수 있도록 한다.

본 교구는 학습자 스스로가 해커가 되어 해킹의 원리를 파악하고, 해킹의 인과관계를 학습하여 최선의 방어책을 찾아볼 수 있는 적극적인 노력을 할 수 있도록 시뮬레이션 게임 요소를 적용하였다.

Ⅱ. 관련 연구

2.1 언플러그드 컴퓨팅(Unplugged Computing)

컴퓨팅의 원리와 개념을 이해하고, 이를 바탕으로 문제를 효율적으로 해결하는 능력을 의미하는 컴퓨팅 사고력은 현대 사회가 과학기술의 정보화로 인하여 제기되는 문제가 융합적 지식 사고를 요구하고 탐구학습을 위한 시뮬레이션 학습 능력 함양을 위한 정보 생성과 시뮬레이션 학습 환경을 다루기 위한 컴퓨팅 능력을 키울 수 있는 핵심역량 따라 점차 강조되고 있다[7]. 컴퓨팅 사고력의 중요성이 증가에 따라 교육 시설에서 컴퓨팅 교육을 위한 기반시설을 마련하기 위한 필요비용을 낮추면서도 컴퓨팅 사고력의 향상을 위한 교육 활동을 진행할 수 있는 언플러그드 학습 활동에 대한 연구가 활발

히 진행되고 있다. 언플러그드 교육은 컴퓨터를 사용하지 않고서 컴퓨팅 사고력을 발전시키기 위한 교육으로 초등 학습자를 대상으로 한 다양한 교육이 연구되고 있다.

허영(2019)은 코딩 교육이 단순한 문제 해결에 목적을 두던 과거와 달리 현재에는 문제해결 능력을 보다 중요시한다는 점을 언급하며 2018년 기준 약 85.5%의 학생이 코딩 교육을 받지 못하고 있음을 강조하였다. 교육의 어려움에는 기자재의 보급 문제가 존재하며, 이를 보완하기 위하여 기자재 없이 교육 가능한 미술활동을 접목한 언플러그드 코딩 교육 프로그램을 개발하여 효과적임을 검증하였다[8].

김진수, 박남제(2019)는 초등과정을 위한 인공지능 학습원리를 보드게임으로 교육하는 프로그램을 실증하여 IT 원리 교육에 대한 유의미한 성과를 얻었다[9]. 이명숙(2020)은 발전하는 사회상에서 컴퓨팅 사고력의 향상을 위한 언플러그드 교육의 효과성에 대한 연구를 진행하였으며, 교육모델을 설계하고 이를 비전공자를 포함하는 교수자 집단을 대상으로 교육하여 사전-사후 t-검증을 진행한 결과 4점 척도를 기준으로 교육을 받기 전에는 컴퓨팅 사고력에 대한 척도가 불과 2.67의 값을 보인반면, 교육 후 3.07로 증가하며 유의미한 결과를 보였다[10]. 이처럼 놀이를 기반으로 과학의 원리에 대한 이해를 돕기 위한 학습 활동으로 초·중등 과정의 학생뿐만 아니라 전공 과정이 아닌 일반 성인을 대상으로도 효과를 발휘할 수 있다.

2.2 사이버 공격 프로세스 학습 교재 및 교구

정보보안 교육은 실생활과의 높은 연계성과 학습 과정에서의 고등사고력을 활용하고 있음에도 불구하고 전문분야의 높은 장벽으로 인하여 교육콘텐츠로서의 활용이 용이하지 않은 실정이다. 일부 정보보안 전문가 직업 진로교육의 취지로 개발된 보드게임 등과 접목한 학습교구의 개발 사례를 다음과 같이 살펴볼 수 있다. 우선 국내 사례에서 고영해(2014)는 육각형 셀 기반 모의해킹 활동을 통한 효과적인 정보보안 학습교구를 개발 하여 놀의 기법을 통한 해커의 기능 원리를 쉽게 학습시키며 정보보안의 중요성을 인식시킬 수 있는 효과에 대해 언급하였고[11], 이동혁, 박남제(2016)는 게이미피케이션 메커니즘을 이용한 초등 네트워크 정보보안 학습교재 및 교구를 개발하여 클라이언트와 서버 간의 메시지 흐름을 이미지화하여 셀과 방화벽 간의 이동 경로를 육안으로 파악할 수 있도록 하였다[12]. 국외의 사례로는 Mark Engelberg et el.(2018)가 개발한 사이버보안 로직 게임이 사이버 범죄자를 저지하기 위해 에이전트가 되어 각 단계별 미션을 수행하는 보드게임을 개발하여 프로그래밍을 체험할 수 있도록 하였고[13], Tiago Gasiba et el.(2020)은 보안 프로그래밍을 위한 사이버 보안 게임을 분석하여 사이버 보안 문제를 해결하기 위한 인식 구조화를 보안 코딩기술 게임으로 교육하는 것이 보안에 대한 인식향상 측면에 영향을 미치는 것으로 나타났다고 분석하였다[14].

본 논문에서는 이상의 사례들이 가지고 있는 언플러그 게임 방식의 장점을 취하고, 보다 전문 기술분야의 다양성과 미래 고도화된 정보화 사회에 인재 양성을 위해 사이버 공격과 같이 전문적 지식을 필요로 하는 기술분야 교육을 비전문가 및 초·중등생에게 교육하는 목적으로 설계하여, 컴퓨팅 사고력 증진을 위한 언플러그드 학습 교구로 활용할 수 있도록 개발하였다. 공격자의 입장에서 목적지에 도달하는 것을 목적으로 하는 해킹을 주제로 언플러그드 교육을 설계하였다. 교육의 설계를 위해 네트워크상에서 공격자가 대상자에게 도달하는 과정은 크게 대상자의 네트워크 경로를 찾는 과정, 대상자의 보안장비를 거쳐 대상자에 도달하는 과정으로 볼 수 있다. 그림 2는 사이버 공격에 대한 과정을 간략하게 설명하는 것이다.

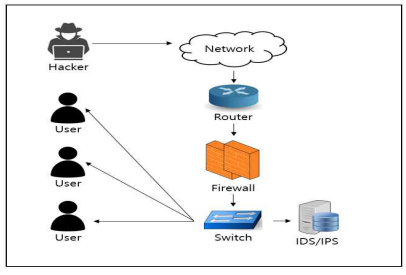

그림 2. 사이버 공격 프로세스
Fig. 2. Cyber attack process

III. 제안된 해킹원리 언플러그드 학습교구설계

정보보안 기술의 원리 교육이 자칫 기술적인 내용으로만 구상되어 전문가가 아닌 학습자에게 외면되지 않도록 하기 위하여 학습자를 해커로 설정하고, 파일을 훔쳐서 안전하게 도피하는 프로세스를 간단한 방향키로만 프로그래밍할 수 있도록 하였다.

다음 단계에서는 전 단계에서 코딩한 프로그램을 분석하여 보안 취약점을 찾아서 학습자가 프로그램을 변경하고 바이러스로 감염시킬 수 있는 방법을 찾아보며 마지막으로 이전 두 단계에서 찾은 시스템의 약점에 대한 지식을 사용하여 프로그램을 보호할 수 있도록 하였다. 프로그램을 보호하기 위해서는 침입탐지 시스템인 알람 및 트랜잭션(Transaction)으로 사이버 공격을 방지하도록 프로그램을 수정한다. 그림 3은 본 학습교구 설계를 그림으로 나타낸 것이다. 스테이지를 거듭할수록 학습자는 코딩, 디펜스, 픽스의 단계를 거치며 좀 더 복잡한 환경 속에서 새로운 미션을 수행해 나아가며 알고리즘을 수정할 수 있다.

3.1 해킹 원리 언플러그드 학습교구 개발 절차

해킹 원리 언플러그드 학습교구의 개발 절차는 리빙스톤과 스톨(Livingston and Stoll, 1973)이 제안한 시뮬레이션 게임의 모델 제작 절차를 참고하여 표 1과 같은 단계를 설정하고 이를 본 해킹 원리 학습 교구 개발 절차에 융합하였다[15,16]. 리빙스톤과 스톨이 제안한 시뮬레이션 게임 모델 제작 절차는 시뮬레이션 게임의 개발 과정을 학습목표 설정, 소재 선정, 구조와 자료설계, 규칙작성 후 실행 및 수정으로 기술하여 보드게임 등과 같은 게임 개발과 관련된 국내 발표 논문에서 다수 인용되고 있다.

단계별 전개 내용을 살펴보면 1단계 학습 목표 결정에서는 해킹게임을 통하여 정보보안의 중요성을 알고 해킹 원리 알고리즘을 구상할 수 있다[17]-[24].

표 1. 단계별 해킹 게임 모델 개발 절차
Table 1. Hacking game model development procedure

Set Learning Objectives	Information security unplugged education through hacking principle learning
Game Material selection	Applying information security hacking principle learning to simulation game model
Game Structure design	Set the role of the game end, resources, and targets for external factors
Game Material design	Game board, mission sheet and worksheet design
Creating Game rules	The purpose of the game, the procedure, the roles and rules of the players in stages
Inspection and Modify	Running and modifying the game

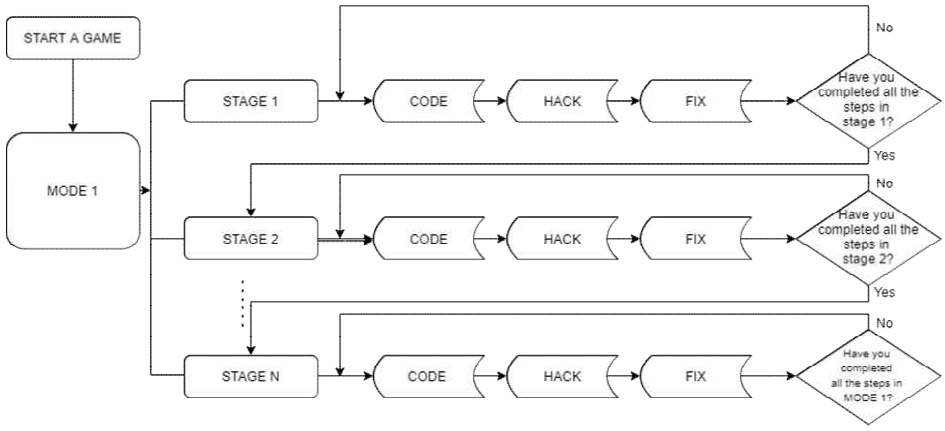

그림 3. 제안된 해킹 원리 언플러그드 학습 티칭 게임 플로우
Fig. 3. Proposed hacking principle unplugged learning teaching game flow chart

2단계 정보보안 해커 게임 소재 선정에서 해킹 원리교육 언플러그드 학습교구의 소재는 학습자가 해커가 되어 보안장치를 피해 파일을 안전하게 탈취하는 목적을 달성하는 과정을 보드게임으로 학습할 수 있도록 하였다.

게임의 구조를 설계한 3단계에서 게임 보드는 4x4의 16개 타일 그리드로 이루어져 있고 보드판에는 5개의 회전 플랫폼이 놓여있으며 2개는 시계방향으로 3개는 시계 반대 방향으로 회전한다. 학습자는 5개의 회전 플랫폼과 각각의 이동을 제어하는 타일을 미션지에 따라서 보드판에 스테이지 별 초기 설정으로 놓는다. 게임 보드판에는 한 명의 해커와 3개의 방향키, 한 개의 회전 패널, 해커의 목표인 파일 패널과 해커를 끌어들여 해킹을 실패 하도록 유인하는 허니팟 및 해커가 터치하면 프로그램이 안전하게 종료되어 해킹시도를 저지할 수 있는 알람과 최종 미션의 성공을 나타내는 출구로 설계하였고 표 2는 게임의 구성품과 주요 역할 내용 및 본 학습교구에서 역할의 학습을 위해 대치한 시스템 명이다.

표 2. 게임 내 주요 역할 내용 및 시스템
Table 2. Main role content and system in the game

Components (Icon)	Main role content	Replaced system
Hacker	Player of the game	-
Arrow keys	Set the direction of the hacker's front, back, left, and right	Router
Rotating panel	Move one space in clockwise and counterclockwise directions	Traffic
Data file	Information hackers want to steal	Client
Alarm	Hacker intrusion notification	IDS/IPS
Honeypot	Attracting hackers to induce hacking failure	Honeypot
Exit	Safe hacking success	-

4단계의 게임 자료 설계에서 해커 게임의 진행을 위해 게임의 진행 방법을 제공하는 설명서와 각 단계별 수행 해야하는 미션지와 알고리즘 설계 할 수 있는 워크시트, 각 역할을 직접 보드에 구현할 수 있는 패널과 게임 말이 필요하다. 그림 4는 보드판에 미션지에서 요구하는 대로 패널과 게임 말을 배치한 이미지 모습이다.

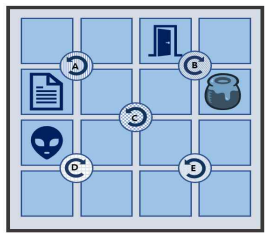

그림 4. 보드판에 구상한 미션지 내용
Fig. 4. Contents of the mission paper envisioned on the board

본 그림에서 각각의 아이콘은 해커( ), 데이터파일( ), 출구( ), 허니팟( )과 회전패널( )을 나타내며 해커가 데이터파일을 집어서 허니팟을 건드리지 않고 출구로 나가는 미션을 수행한다. 아래 그림 5는 워크시트로 해커X의 방향을 정하여 출구까지의 경로를 시뮬레이션할 수 있도록 제작한 워크시트이다.

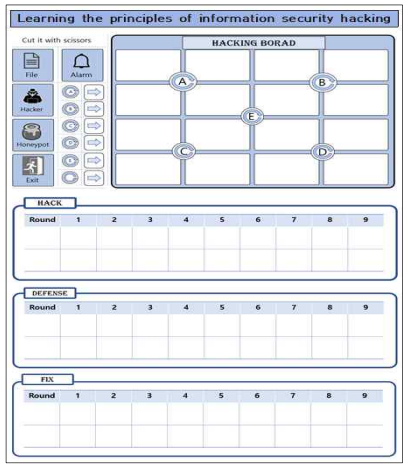

그림 5. 해킹 원리 교육 워크시트
Fig 5. Hacking principle worksheet

게임 규칙을 설정하는 5단계에서는 HACK, Defense, Fix의 3단계에 걸쳐 해킹의 공격자와 방어자의 시뮬레이션을 코딩한다. 먼저 특정한 포인트의 회전과 같은 조건을 사전에 설정하여 그림 6과 같이 게임의 미션지를 설계할 수 있다.

Round	1	2	3	4
Traffic				
Haker X				

그림 6. 해킹 게임 미션지
Fig. 6. Hacking game missions

교수자는 학습자가 정해진 횟수 이내에 목표를 달성할 수 있도록 한다. 본 연구에서는 학습자에게 3번의 이동 기회를 제공한다. 학습자는 좌, 우, 상, 하의 4방향으로 이동 방향을 설정할 수 있다. 학습자는 차례로 이동 방향을 설계하되, 교수자에 의해 해당 차례에 변수가 설정된 경우 다음 차례에 이어서 진행한다. HACK 단계에서는 공격자인 학습자가 자료를 획득하고 출구를 통하여 탈출하는 것을 목표로 하고, 정해진 횟수를 넘어서거나 목적지가 아닌 곳에 도달한 경우 실패로 간주한다. 위 그림 6과 같은 게임의 미션지를 보고 게임판위에 트래픽 아이콘을 놓는다. 해커 X가 허니팟에 빠지지 않고 출구지점에 도착하도록 알고리즘을 구상한다.

HACK에서는 화살표 3개만을 이용하여 코드를 짜야 한다. 해커 X가 데이터 파일을 집어들고 해당 종료 지점(출구)에 도달하도록 게임판을 조사하여 이동방향을 결정한다. 작성한 코드대로 테스트를 한다. 이때 트래픽의 화살표 대로 한칸 회전한다. 해커 X가 파일을 집어서 마지막 이동 지시대로 출구지점에 도착하면 이긴다. 작성한 코드는 그대로 남겨두고 DEFENCE로 넘어간다.

DEFENCE단계 에서는 HACK에서 코딩한 프로그램을 분석하여 보안 취약점을 찾는다. 해커가 프로그램을 변경하고 바이러스로 감염시킬 수 있는 방법을 알아본다. DEFENCE 단계에서는 방어자인 학습자가 공격자가 탈출할 수 없도록 허니팟으로 유도하는 것을 목적으로 한다.

학습자는 Hack 단계에서 설정한 이동 방향 3개와 교수자에 의해 설정된 변수의 순서만을 변경하여 목적지에 도달하여야 한다. 정해진 횟수를 넘어서거나 목적지가 아닌 곳에 도달한 경우 실패로 간주한다. 이때 미션지에 설명된 원래 설정에 따라 게임판을 복귀하고 워크시트 위에 방향키와 회전 패널을 좌, 우로만 움직여 해커X가 허니팟에 도착하면 이긴다. 작성한 코드는 그대로 남겨두고 FIX로 넘어간다.

FIX단계에서는 게임판의 빈공간과 허니팟의 위치, 종료 위치를 파악한 후 알람을 설치한다. 해커X가 알람과 접촉하면 경보가 트리거(Trigger)되면서 프로그램은 안전하게 종료하도록 알고리즘을 구상한다. FIX 단계에서는 공격자의 이동경로에 알람을 설치하여 공격자의 침입 시도를 파악하는 것을 목적으로 한다. 학습자는 방어자가 되어 알람 변수를 학습지 내의 비어있는 공간에 설치할 수 있다. 학습자는 공격자가 알람에 도달한 직후에 허니팟으로 이동하도록 구성하여야 한다.

공격자가 알람을 지나치지 않거나, 지나친 경우에도 허니팟에 도달하지 못하는 경우 실패로 간주한다. 단, 해킹된 프로그램을 추적할 때 해커X가 허니팟에 도달하기 전에 알람이 작동해야 한다. 게임판에서 알람을 놓고 DEFENCE에서 코딩한 프로그램과 HACK에서 코딩한 프로그램을 방해하지 않으면 학습자가 이긴다. 그림 7은 해킹 게임 미션 완료 시 학습지의 답안 예시로 학습자의 미션 성공 여부를 알 수 있다.

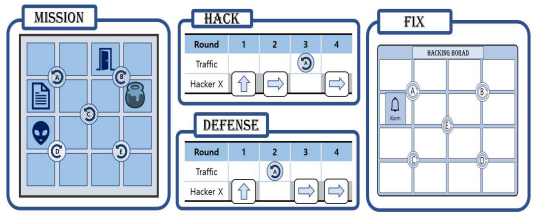

그림 7. 해킹 게임 미션 완료 답안 예시
Fig. 7. Example of completing a hacking game mission

HACK, DEFENCE, FIX를 모두 수행하면 다음 스테이지로 이동한다. 마지막 6단계에서는 검사 및 수정단계로 해커 게임이 해커가 데이터 파일을 선택하여 종료지점에 도달하도록 프로그램을 구상하고, 보안 취약점을 찾아 시스템 약점을 보완하여 사이버 공격을 방어하는 설정으로 구상하였다. 실행하는 과정에서 발견되는 문제점을 보완하고 수정하여 완성도 높은 학습교구로 발전시킨다. 그림 8은 한 스테이지 당 HACK, DEFENCE, FIX의 절차별 흐름을 도식화 한 것이다.

3.2. 해킹 원리 학습교구의 확장 설계

본 게임은 하나의 도전과제당 3단계의 미션을 수행하게 하여 도전과제의 무한한 확장성을 보장할 수 있도록 하였다. 본 논문에서는 초등학생이 이해할 수 있는 정도의 기초 단계만 언급하였다. 본 과

제를 모두 수행한 학습자에게는 도전과제를 거듭하여 동시성을 제어하는 잠금(Lock)기능과 논리적인 작업을 모두 완벽하게 처리하거나 또는 처리하지 못할 경우에 원상태로 복구하여 작업의 일부만 적용되는 현상이 발생하지 않게 하여 작업을 완전성을 보장해주는 트랜잭션(Transaction) 기능을 학습하도록 구상해 볼 수 있다.

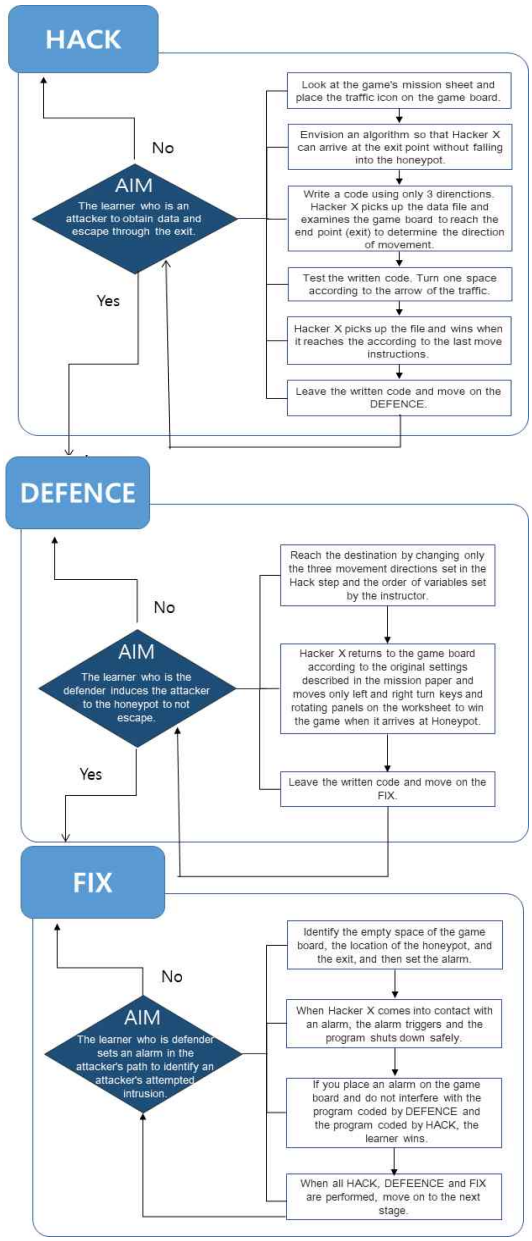

그림 8. 해킹 게임 플로우
Fig. 8. Hacking game flow

해커는 플레이어가 실제 프로그래머가 사용하는 것과 유사한 전략을 사용하여 잠금 기능을 통해 두 스레드(Thread)가 동시에 코드의 동일한 중요 섹션을 차지하게 하는 인터리빙(Interleaving: IP 네트워크 즉 유선 통신 네트워크 또는 무선 통신 구간을 통하여 트래픽을 전송할 때, 발생할 수 있는, 군집 에러를 랜덤 에러로 변환하여, 에러 정정을 용이하게 하기 위하여 사용되는 기법)에 대하여 추론할 수 있도록 확장하여 설계할 수 있다.

Ⅳ. 결론 및 향후 연구

정보화 사회에서 정보에 대한 가치가 높아짐에 따라 관련 범죄가 급증하고 있지만, 사용자의 연령대는 낮아지고 이에 대한 대비는 미흡하다. 다양한 분야에서의 ICT와 소프트웨어 기술이 접목된 모든 것의 디지털 화(化)인 시대에 직면한 문제들은 다양한 지식의 영역을 넘나드는 융합적이고 창의적인 사고력과 실천력을 필요로 하고, 이러한 문제해결 역량을 컴퓨팅 사고력의 함양에서 모색하였다. 컴퓨팅 사고력은 앞서 언급한 언플러그드 컴퓨팅에서도 보여주는 대로 컴퓨터의 작동 원리를 통한 여러 활동 중에서 정보교육과의 연관성을 찾았다.

정보교육 과정은 학습자의 의사소통 능력, 문제해결 능력, 창의력 등 고급 사고력을 각 활동에 적용하는 교육을 통하여 컴퓨팅 사고력을 탐구하고 신장시킬 수 있다는 점에 착안하여 해킹 게임으로 보안 로직 학습교구를 구상하였고 학습자가 해커가 되어 스스로 알고리즘을 학습하고 각 단계를 완수하도록 하였다.

논문에서 제시한 해커게임은 초등학교 고학년 수준의 학습자가 학습할 수 있도록 시스템의 설명 및 역할보다는 각 아이콘이 의미하는 공격과 방어의 의미에 중점을 두어 흥미로운 학습을 유도하였다. 단계를 거듭할수록 흥미보다는 정보보안의 기술 알고리즘을 구상하여 컴퓨팅 사고력 신장의 그 목적을 두고 있다. 향후, 초·중등생 뿐만 아니라 일반인 그리고 교육 전문가 및 관련 기술 전문가에게 시범 수업을 운영하여 검증하고 사전·후 검사 및 만족도 검사를 계획하고 실행하여 체계적인 효과성 및 만족도 분석을 통하여 완성도 있는 정보보안 해커 학

습 교구로서의 역할을 다할 수 있도록 지속적인 연구를 진행할 것이다.

References

[1] D. J. Choi, "Next-generation IoT security in the 5G era." https://www.itfind.or.kr/publication/regular/weeklytrend/weekly/list.do?pageIndex=0&pageSize=10, pp. 2-16, Sep. 2019.

[2] Korea Internet and Security Agency, "Number of hacking accidents", https://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1363, Apr. 2020.

[3] C. B. Kim, "An Analysis of Information Security Curriculum in Elementary School practical arts, Secondary School Informatics Teaching and Suggestions for Improvement" Journal of the Korea Society of Computer and Information, Vol. 25, No. 10, pp. 69-75. Oct. 2020.

[4] J. M. Kim and W. G. Lee, "Controversial Issues in Knowledge and Problem Solving Skills of Information Subjects Observed after Amending the Curriculum in the U.K. The Journal of Korean Association of Computer Education", Vol. 17, No. 3, pp. 53-63, May 2014.

[5] Y. J. Jung, J. S. Kim, and N. J. Park, "Development and Effects of Intelligent CCTV Algorithm Creative Education Program Using Rich Picture Technique", Journal of the Korea Convergence Society, Vol. 11, No. 4, pp. 125-131, Apr. 2020.

[6] D. H. Lee and N. Je. Park. "A Blockchain-based Untact Education System for the Post-COVID-19 Era", Korean Institute of Information Technology, Vol. 18, No. 11, pp. 109-121, Nov. 2021.

[7] Y. J. Jang, D. H. Kim, H. S. Kim, W. G. Lee, and H. C. Kim, "Development of Unplugged Activity and its Evaluation of Usability for Information Security Education", The Journal of Korean Association of Computer Education, Vol. 14, No. 1, pp. 55-67, Jan. 2011.

[8] Y. Hur, "Development of Unplugged Coding Education Program for the Elementary School", Journal of Basic Design & Art, Vol. 20, No. 1, pp. 585-596. Jan. 2019.

[9] J. S. Kim and N. J. Park. "Development of a Board Game-based Gamification Learning Model for Training on the Principles of Artificial Intelligence Learning in Elementary Courses", Journal of The Korean Association of Information Education, Vol. 23, No. 3, pp. 229-235. Jun. 2019.

[10] M. S. Lee, "Effectiveness Analysis of Computing Thinking with Unplugged in Digital Transformation", Journal of Digital Convergence, Vol. 18, No. 3, pp. 35-42, Mar. 2020.

[11] Y. H. Ko and N. J. Park, "Teaching Tools of Effective Information Security through Simulation Hacking Play Activities based on Hexagon Cell", Proceedings of The Korean Institute of Information Scientists and Engineers, pp. 654-656, Dec. 2014.

[12] D. H. Lee and N. J. Park, "Teaching Book and Tools of Elementary Network Security Learning using Gamification Mechanism", Journal of the Korea Institute of Information Security & Cryptology, Vol. 26, No. 3, pp. 787-797, Jun. 2016.

[13] M. Engelberg, et al, "Thinkfun-cybersecurity logic game", In Thinkfun, Virginia, 2018.

[14] T. Gasiba, U. Lechner, F. Rezabek, and M. Pinto-Albuquerque, "Cybersecurity Games for Secure Programming Education in the Industry: Gameplay Analysis", International Computer Programming Education Conference, Vol. 81, No. 10, pp. 1-11. Oct. 2020.

[15] S. A. Livingston and C. S. Stoll. "Simulation games, an introduction for the social studies teacher", Free Press, New York, pp. 39-40, 1973.

[16] J. Kim and N. Park, "A Face Image Virtualization Mechanism for Privacy Intrusion Prevention in Healthcare Video Surveillance Systems", Symmetry, Vol. 12, No. 6, pp.1-15,

Jun. 2020.

[17] Jinsu Kim and Namje Park, Geonwoo Kim and Seunghun Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving -Transformation in the Emerging Multimedia", Electronics, Vol. 8, No. 4, pp. 1-15, Apr. 2019.

[18] N. Park, Y. Sung, Y. Jeong, S. B. Shin, and C. Kim, "The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary School in Korea", International Conference on Computer and Information Science, USA, pp.1-15, Sep. 2018.

[19] Namje Park, Byung-Gyu Kim, and Jinsu Kim, "A Mechanism of Masking Identification Information regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission", ELECTRONICS. Vol. 8, No. 7, pp. 735, Jun. 2019.

[20] Jinsu Kim and Namje Park, "Blockchain-Based Data-Preserving AI Learning Environment Model for AI Cybersecurity Systems in IoT Service Environments", Applied Sciences. Vol. 10, No. 14, Jul. 2020.

[21] Jinsu Kim and Namje Park, "Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing", Personal and Ubiquitous Computing, pp. 1-9, Aug. 2019.

[22] Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, and Howon Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", Conferences of Asia-Pacific Web Conference, Harbin, China, 741-748, Jan. 2006.

[23] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree", Multimedia Tools and Applications, Mar. 2020.

[24] S. Ryu, J. Kim, N. Park, and Y. Seo, "Preemptive Prediction-Based Automated Cyberattack Framework Modeling", Symmetry, Vol. 13, No. 5, pp.1-20, May 2021.

[25] J. Kim and N. Park, "Role-based Access Control Video Surveillance Mechanism Modeling in Smart Contract Environment", Transactions on Emerging Telecommunications Technologies, e4227, Feb. 2021. https://doi.org/10.1002/ett.4227.

저자소개

정 유 진 (Yujin Jung)

2007년 2월 : 국민대학교 국어국문학과 문학사
2019년 2월 : 한국외국어대학교 외국어계열 한국어학과 문학사
2020년 2월 : 제주대학교 일반대학원 융합정보보안학협동과정 공학석사
2020년 3월 ~ 현재 : 제주대학교 대학원 융합정보보안학협동과정 박사과정
2017년 3월 ~ 현재 : 제주대학교 창의교육거점센터, 사이버보안인재교육원, 과학기술사회연구센터 책임연구원
관심분야 : 초등 정보교육, IT융합보안기술, 창의교육, 지능정보기술 등

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과 박사
2003년 4월 ~ 2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월 ~ 2009년 12월 : 미국 UCLA대학교, ASU대학교 Post-Doc.
2010년 9월 ~ 현재 : 제주대학교 초등컴퓨터교육전공, 대학원 융합정보보안학과 교수
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등