Check for updates

Journal of KIIT. Vol. 22, No. 2, pp. 177-193, Feb. 28, 2024. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2024.22.2.177

제주 설화를 접목한 네트워크 보안 교육 콘텐츠 개발

최은선*, 박남제**

Development of Network Information Security Educational Contents Infused with Folktales in Jeju

Eunsun Choi*, Namje Park**

이 논문은 2023년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2023S1A5B5A16081463).

요 약

네트워크 보안은 단순한 디지털 자산의 보호를 넘어서 네트워크 속 참여자의 흥망성쇠를 좌우하는 핵심 요소라 할 수 있다. 본 논문은 네트워크 보안 인식의 제고를 통해 정보보안 융합 인재 양성에 기여하는 것을 목적으로 한다. 본 논문에서는 제주 설화 오백 장군 전설, 고종달 설화, 영등할망 전설의 등장인물과 요소들을 활용하여 인문학적 요소를 접목한 네트워크 보안 융합 교육 콘텐츠를 제안하였다. 교육 내용으로는 DDoS 공격, 스푸핑 공격, 세션 하이재킹 공격을 선정하였다. 더불어, 초등학생 대상 수업에서 본 교육 콘텐츠를 접목하여 수업할 수 있도록 콘텐츠별 학습 게임을 개발하고 확장된 정보보호 통합학습 모형을 기반한 수업 방안을 설계하였다. 이 수업 방안을 통해 초등학생에게 네트워크 보안 교육을 실시할 수 있으며, 학습자들은 네트워크 보안 지식, 태도, 실천 역량을 함양할 수 있다.

Abstract

Network security can be considered a critical factor that goes beyond the simple protection of digital assets, influencing the prosperity and success of participants within the network. The aim of this paper is to contribute to the development of information security convergence talents by enhancing awareness of network security. In this paper, we proposed network security integrated education contents infused with humanistic elements by utilizing characters and elements from Jeju folklore of General five hundred, the Gojongdal, and the Yeongdeung Halmang. We also selected DDoS attacks, spoofing attacks, and session hijacking attacks as educational contents. In addition, we developed a learning game for each content and designed a teaching plan based on the KASP(Knowledge, Attitude, Skill and Practice) model so that this educational content can be applied to classes for elementary school students. Through this teaching plan, it is possible to provide elementary school students with education on network security, enabling learners to cultivate knowledge, attitudes, and practical skills related to network security.

Keywords

information security education, Jeju folktale, network security, educational game, information protection learning model

* 제주대학교 창의교육거점센터 학술연구교수
- ORCID: https://orcid.org/0000-0001-6384-5324
** 제주대학교 교육대학 초등컴퓨터교육전공 교수(교신저자)
- ORCID: https://orcid.org/0000-0003-4434-8933

· Received: Dec. 01, 2023, Revised: Feb. 02, 2024, Accepted: Feb. 04, 2024

· 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

대한민국은 지금 총성 없는 사이버 전쟁 중이다. 기업이나 개인을 대상으로 하는 사이버 위협은 꾸준히 증가하고 있는 실정이다. 과학기술정보통신부와 한국인터넷진흥원의 사이버 위협 동향 분석에 따르면, 국내 민간분야 2021년 침해사고 신고 건수가 640건에서 2022년 1,142건으로 증가했고 2023년 상반기만 664건에 이르는 것으로 나타났다[1]. 특히 인터넷 트래픽을 높여 네트워크 리소스 운영을 어렵게 하는 분산 서비스 거부 공격((DDoS, Distributed Denial of Service) Attack)은 2022년 상반기 48건 (10.1%)에서 2022년 하반기 74건 (11.1%), 2023년 상반기 124건 (18.7%)으로 급격하게 늘어난 것으로 보고되었다[1].

늘어가는 사이버 공격과 침해사고로 정보보안 교육의 중요성이 더욱 높아지고 있다. 더불어, 네트워크를 통해 중요한 데이터를 저장 및 전송하고 업무를 수행하는 환경에서 공격자로부터 네트워크를 보호하는 보안정책과 기술이 요구된다.

본 논문은 네트워크 보안 인식 제고를 목적으로 인문학을 연계한 네트워크 보안 교육 콘텐츠를 제안하였다. 인문학 접목 정보 융합 교육의 중요성을 바탕으로 네트워크 보안 기술 중 제주 설화와 연계할 수 있는 기술을 선정하여 네트워크 보안 교육 콘텐츠를 개발하였다. 더불어, 초등 정보보안 교육 모형 및 교육 프로그램의 효과성과 사례를 분석하여 초등학생 대상 교육이 가능하도록 수업 방안을 제안하였다. 이 연구는 제주의 설화를 활용하여 지역적 특색을 네트워크 보안 교육에 반영한 창의적인 접근 방식을 택했으며, 교육적으로 학습자에게 기술과 인문학이 융합하는 경험을 제공할 수 있다.

Ⅱ. 이론적 배경

2.1 인문학 연계 정보 융합 교육

이질적인 요소가 만나 지식이나 경험, 방법론 등이 결합하는 개념을 일컫는 융합은 IT(Information Technology) 산업의 발전 방법으로 부각되고 있다. 특히, 다양한 기술과 학문의 융합 중에서도 IT와 인문학의 만남은 디지털 기술이 발달함에 따라 함께 주목받고 있다. 디지털 기술 자체가 인간 지능의 확장인 IT와 커뮤니케이션기술이 융합한 것이며 이는 인간의 삶과 문명의 변화를 이끌고 있다[2].

기술의 발달에 따른 인간성의 소외에 많은 전문가가 우려하고 있다. 이에, 인간을 위한 기술이 개발되기 위해서는 IT의 개발에 인문학의 융합이 필수적으로 요구된다[3]. 이러한 흐름에 따라 정보 교육에도 인문학을 연계하고자 하는 연구가 증가하고 있다.

J.-Y. Kim and K. Kim(2022)은 예비 교사를 대상으로 노벨 엔지니어링을 기반으로 인공지능 융합 교과목을 운영했다[4]. 노벨 엔지니어링은 문학작품의 내용과 작품 속 등장인물, 학습자가 상호작용하는 맥락 안에서 공학적인 해결 방법을 모색하는 융합적 학습 활동이다[5]. 이 교과목에 참여한 학생들의 창의융합역량은 사전보다 사후에 통계적으로 유의하게 향상된 것으로 분석되었다.

E. Choi and N. Park(2023)는 정보기술과 인문학을 융복합한 교육을 수행할 때 프레임워크로 활용할 수 있는 교육 모델을 개발하였다[6]. 이 모델은 IT인문학 교재 연구, IT인문학 가치 확산, 메이커스페이스 조성, 글로컬 협의체 기반 리빙랩 거버넌스 구축 등 통합적으로 IT인문학 융복합 역량을 지닌 인재 양성을 목적으로 한다. 더불어, IT인문학 교육 모델을 바탕으로 예비 교원을 대상으로 창의적 융복합 미래융합IT인문학 교과목을 개발하였으며, 참여 학생의 창의성, 의사소통, 내용융합, 배려를 하위요인으로 가지는 융합적 사고력이 유의하게 증가한 것으로 나타났다[7].

2.2 네트워크 공격 기술

오늘날 기업과 개인의 인터넷에 대한 의존도가 늘어나면서 온라인상의 사이버 위협이 늘어나고 있다[8]. 따라서, 각종 중요 데이터의 전송이 이루어지는 네트워크를 보호하기 위해 해커의 다양한 공격 기술이 연구되고 있다. 네트워크 공격 기술에 관한 연구는 보안 기술을 개발하기 위해 선행되어야 하는 연구라 할 수 있다.

네트워크 공격 기술은 여러 연구자에 의해 그 유형이 분류되고 있다. B. Kim et al.(2003)의 연구에서는 네트워크 공격 기법으로 서비스 거부(DoS, Denial of Service) 공격과 스캐닝 기법에 주목했다[9]. DoS 공격은 대역폭 공격, 자원 고갈 공격, 프로그램 오류 공격, 라우터와 도메인 네임 시스템(DNS, Domain Name System) 공격, 혼합 공격으로 구분했으며, 네트워크 스캐닝은 호스트 스캐닝과 포트 스캐닝으로 분류했다.

D. Yang(2018)은 네트워크 공격 기술을 DoS와 DDoS(Distributed Denial of Service) 공격, 스니핑(Sniffing) 공격, 스푸핑(Spoofing) 공격, 세션 하이재킹(Session hijacking) 공격, 무선 네트워크 공격으로 구별하여 설명했다[10]. 이는 다양한 정보보안 기술을 다루는 기초 개론서에서 추출한 것이다.

J. Bang et al.(2019)는 네트워크 공격 패킷 기술을 TCP/IP 공격, 네트워크 포트 스캔, DDoS 공격, 대용량 패킷 공격, 웹 해킹, SMB(Server Message Block) 해킹, RAT(Remote Access Trojans) 감염 공격, 메일 서버 해킹, 무선 네트워크 해킹으로 나누었다[11]. 해당 연구는 네트워크 공격을 일선에서 대응하는 보안 실무자를 대상으로 한 것이다.

표 1. 네트워크 공격 기술 유형
Table 1. Network attack techniques

Researcher	Type of network attack
Kim et al. (2023)	• DoS attacks: bandwidth attack, resource depletion attack, program error attack, router and DNS attack, hybrid attack • Scanning: host scanning, port scanning
Yang (2018)	• DoS, DDoS attack • Sniffing attack • Spoofing attack • Session hijacking attack • Wireless network hacking
Bang et al. (2019)	• TCP/IP attack • Network port scan • DDoS attack • Large-scale packet attack • Web hacking • SMB hacking • RAT infection attack • E-mail server hacking • Wireless network hacking
Choi (2022)	• DoS attack • Sniffing attack • Spoofing attack • Poisoning attack • Session hijacking attack

J.-H. Choi(2022)의 연구에서는 네트워크 기반 보안 사고를 유발하는 공격 기법으로 DoS 공격, 스니핑 공격, 스푸핑 공격, 포이즈닝(Poisoning) 공격, 세션 하이재킹 공격을 대표적인 공격의 유형으로 언급했다[12]. 표 1은 다양한 연구자에 의해 분류된 네트워크 공격 기술의 유형을 정리한 것이다.

2.3 초등 정보보안 교육

정보보안이 국가와 기업의 흥망을 좌우하는 중요 요소로 떠오름에 따라 정보보안 교육은 정보보안 전문인력뿐만 아니라 초·중등학생, 대학생, 일반인 등을 대상으로 활발히 수행되고 있다. 사이버 범죄가 급속도로 증가하는 상황에서 학생들을 보호하고 범죄의 피해를 예방하기 위해서는 정보보안 교육이 필수적이다. 각종 보안 사고를 줄이고 더욱 교묘해지는 공격에 대응하기 위해 정보보안 교육 연구가 더욱 중요해지고 있다. 특히 인공지능을 포함하는 지능정보기술의 발전 속도가 매우 빠르고 양상이 다변화되어 초등학생도 사이버 위협으로부터 자유롭지 못한 것이 현실이다. 따라서, 사이버 범죄가 급속도로 증가하는 상황에서 학생들을 보호하고 범죄의 피해를 예방하기 위해서는 정보보안 교육이 필수적이다[13].

D. Lee and N. Park(2016) 연구에서도 게이미피케이션 메커니즘을 활용하여 초등 네트워크 정보보안 학습교재와 교구를 개발하였다[13]. 이들은 개발한 교재와 교구를 활용한 교육을 J시 초등학교에서 대면 형태로 수행하였고, 초등학생 학습자의 정보보호 지식, 태도, 기능, 실천능력에 효과적으로 작용했다고 분석하였다.

J. Kim et al.(2021)는 초등학생으로 하여금 자발적으로 학습에 참여하도록 유도하기 위해 게이미피케이션(Gamification) 기법을 적용하였다. 그들은 대면 수업에서 비식별화 기법 중 암호화 원리를 흥미롭게 학습할 수 있도록 파이프 게임을 설계하였고, 이를 위해 활동지와 파이프 카드를 개발했다[14].

C. Kim(2020)는 초등 실과 교육과정에 개인정보보호 교육 내용과 함께 정보보안 관련 교육 콘텐츠 수록이 필요하다 하였으며, 다양한 데이터 위협의 종류와 최신 공격 위협을 다루고 이에 대한 대응방안에 관한 내용도 포함해야 한다고 제안했다[15].

한편, S.-S. Park and S.-K. Han(2010)은 초등 정보보호 교육을 위해 정보보호에 대한 지식(Knowledge), 태도(Attitude), 기능(Skill)을 통해 실천력(Practice)을 향상시키는 확장된 정보보호 통합학습 모형(KASP model)을 설계했다[16]. 이들은 KASP Model을 기반으로 정보보호 통합 학습 영역을 지식 사회와 정보보호, 해킹과 바이러스, 네트워크 보안, 시스템 보안, 암호, 접근 통제, 데이터베이스 보안, 전자상거래 보안, 정보보호와 관리를 제안했다. 그리고 이러한 내용을 교수할 수 있는 수업의 방법으로 도입 단계에서는 토론학습과 협동학습을, 전개 단계에서는 직접 교수, 선행조직자, 프로젝트 학습, 문제해결학습을 제시했다. 이 모델을 적용하여 수업한 결과, 실험반의 정보보호 수준은 비교반보다 사전보다 사후에 유의하게 높은 수준으로 향상되었다.

III. 네트워크 보안 융합 교육 콘텐츠

본 논문에서는 선행 연구자들의 네트워크 공격 기술 구분을 참고하여 네트워크 보안 교육 콘텐츠 개발을 위해 네트워크 공격 기술의 대표적인 유형을 DDoS 공격, 스푸핑 공격, 세션 하이재킹 공격으로 선정했다. 또한, 인문학 요소 접목을 위해 선정한 네트워크 공격 기술과 연관이 있는 제주의 전설, 설화, 민담, 신화 등 다양한 제주 이야기를 탐구하였고 오백 장군 전설, 고종달 설화, 영등할망 전설을 발굴했다.

3.1 DDoS 공격-오백 장군 전설

3.1.1 DDoS 공격

DDoS 공격은 원격으로 다른 사람의 PC를 조종할 수 있는 악성코드로 일반 PC를 감염시켜 명령을 내리는 방식으로 여러 대의 디바이스를 한 번에 동작시켜 특정 사이트나 시스템을 공격하는 방식을 말한다[17]. DDoS 공격을 교수하기 위해 DDoS 공격을 가능케 하는 봇넷(Botnet)을 우선 설명하고 이후 DDoS 공격을 소개한다. 교육 콘텐츠에서는 봇넷의 정의, 봇넷 이름의 유래, 봇넷 공격의 실제 사례, 봇넷의 구성요소, 봇넷 제어 모델의 유형(중앙 집중식(C&C, Command & Control) 모델, 탈중앙화 형식(P2P, Peer to Peer) 모델, 봇넷의 작동 원리를 다룬다.

봇넷의 대표적 공격 유형 중 하나인 DDoS 공격 교육 콘텐츠로는 DDoS 공격의 정의, DDoS 공격의 실제 사례, DD0S 공격의 단계, 최근 DDoS 공격에 사용되는 봇넷 종류를 포함한다. 이에 더하여, DoS 공격, 한 공격 내에서 여러 공격 벡터를 사용하는 APDoS(Advanced Persistent Denial of Service) 공격, 분산 반사 서비스 거부(DRDoS, Distributed Reflection Denial of Service) 공격을 추가적으로 소개한다. 특히, DoS 공격의 종류인 Ping of Death, Teardrop, Land 공격의 원리와 공격자들이 DDoS보다 DRDoS를 택하는 이유를 설명한다. 그림 1은 봇넷과 DDoS 공격 교육 콘텐츠의 일부이다[18].

그림 1. 봇넷과 DDoS 공격 교육 콘텐츠[18]
Fig. 1. Educational contents for botnet and DDoS attack[18]

3.1.2 오백 장군 전설

제주 사람들의 구전으로 오백 장군은 제주 창조 여신 설문대할망의 아들들로 기록되고 있다. 일부 기록에서는 오백 장군은 영실기암과 연관된 설문대할망과는 독립된 설화였을 것으로 주장하지만 근래 설문대할망과 연관 지어 유포되는 특징이 있다. 본 교육 콘텐츠에서는 설문대할망 설화도 함께 교육하기 위해 오백 장군이 설문대할망의 자손이라는 이야기로 소개한다.

오백 장군 전설을 요약하자면 다음과 같다[19].

설문대할망이 하르방과 결합하여 낳은 자식인 오백 장군들은 그 수가 너무 많아 설문대할망이 배불리 먹여 키우기 어려움이 있었다. 어느 날 설문대할망은 큰 솥에 자식들을 먹일 죽을 끓였다. 거인 설문대할망에게도 솥은 너무나 컸고, 솥의 가장자리를 밟아가며 위태위태하게 죽을 저었다. 그러다 결국 설문대할망은 솥에 빠져 죽게 되었다. 이 사실을 알리 없는 오백 장군들은 집에 돌아와 죽을 발견했다. 배가 고픈 오백 명의 아들 중 한 아들이 죽을 맛있게 먹기 시작하자 다른 아들들도 허겁지겁 죽을 먹어치웠다. 그런데 가장 마지막에 온 막내 아들이 거의 다 먹어가던 죽을 뜨다 그만 솥에서 어머니의 뼈를 발견하게 되었다. 충격을 받은 막내 아들은 집을 뛰쳐나가 울다 차귀도에서 바위가 되었고 나머지 아들들도 영실에서 통곡하다 바위가 되었다.

3.1.3 오백 장군 전설 속 DDoS 공격

오백 아들 중 한 명이 죽을 뜨는 모습을 본 다른 아들들은 홀린 듯이 그를 따라 죽을 마음 놓고 먹기 시작했다. 마치 바이러스에 감염되어 좀비가 된 아들로 인해 다른 아들들 또한 좀비 군대가 된 것으로 보인다. 물론 아들들은 봇넷처럼 의도적으로 다른 사람들에게 피해를 주지는 않았지만, 어머니인 설문대할망에게는 엄청난 불효를 저지르게 되었다.

DDoS 공격과 오백 장군 전설의 구성요소를 서로 연결해보자면 표 2와 같다. DDoS 공격을 수행하는 공격자가 설문대할망의 아들들인 오백장군이라면 이들의 표적은 의도치 않았지만 설문대할망이라 할 수 있다. 더불어, 가장 먼저 죽을 먹은 아들을 봇넷의 공격을 시작하게 만든 봇 마스터로 본다면, 그를 보고 죽을 먹은 나머지 아들들을 봇넷이라 볼 수 있다. 마지막으로 악성 프로그램의 역할을 수행하는 데몬은 공격의 매개체인 죽으로 비유해볼 수 있다.

표 2. DDoS 공격과 오백 장군 전설의 구성요소 연결
Table 2. Components of DDoS attack and the legend of general five hundred

DDoS attack	Legend of general five hundred
Attacker	General five hundred (Sons of Seolmundae halmang)
Bot master	The first son who took a sip of soup
Botnet	The remaining sons who ate the soup together
Demon	Soup
Target	Seolmundae halmang

3.2 스푸핑 공격-고종달 설화

3.2.1 스푸핑 공격

스푸핑은 승인받은 사용자인 것처럼 위장하여 시스템에 접근하거나 네트워크에서 허가된 주소로 가장하여 접근 제어를 우회하는 공격 행위로 정의된다[19]. 스푸핑 공격 교육을 위해 스푸핑의 어원, 스푸핑 공격의 실제 사례, 스푸핑의 유형(ARP(Address Resolution Protocol) 스푸핑, IP(Internet Protocol) 스푸핑, DNS 스푸핑)과 그 각 유형의 공격 원리를 교육용 콘텐츠로 선정했다. 그림 2는 스푸핑 공격 교육 콘텐츠의 일부이다[20].

3.2.2 고종달 설화

고종달 설화는 제주에 구전되어 오는 설화 중 하나로 이방 나라의 황제가 제주의 지기(地氣)를 꺾기 위해 제주로 보냈다는 고종달에 관한 이야기이다. 용천수가 나지 않는 마을이 외부인에 의해 혈이 단절된 것으로 해석한 것이 고종달 설화이다. 일부 문헌에서는 고종달을 고종달이라고 부르기도 한다.

고종달 설화를 요약하자면 다음과 같다[21].

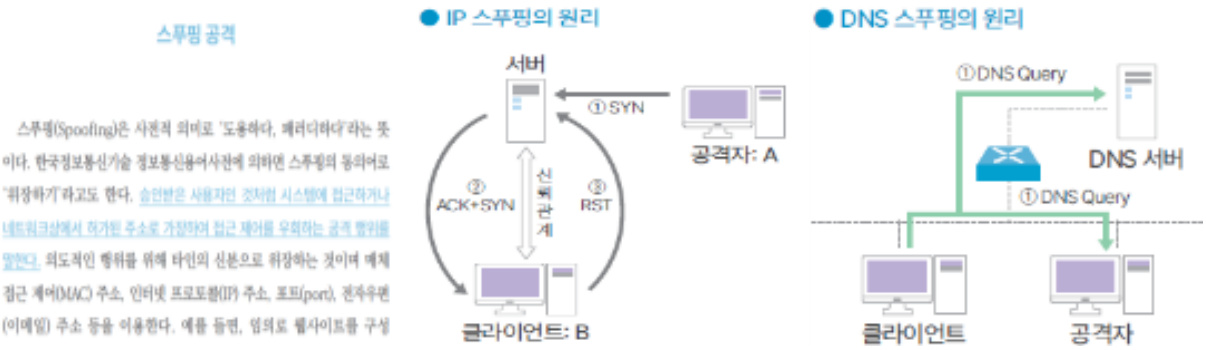

그림 2. 스푸핑 공격 교육 콘텐츠[20]
Fig. 2. Educational contents for spoofing attack[20]

어느 날 한 나라의 황제가 지리서를 보다 제주라는 곳의 지기가 범상치 않음을 느꼈다. 이에 황제는 소문난 풍수사 고종달을 불러 지금의 제주인 탐라국으로 그를 보내 제주의 혈맥을 끊도록 명했다. 고종달은 그 길로 탐라국의 종달리 마을을 방문했다. 고종달은 혈맥을 끊기 위해 어느 마을을 찾았다. 그곳에서는 한 농부가 밭을 갈고 있었는데, 지나가던 백발노인이 급한 얼굴로 농부에게 다가와 누군가가 행기(그릇)에 샘물을 담아 주며 누가 이 물을 찾으면 모른다고 하라며 부탁했다. 고종달은 지도를 보고 꼬부랑나무 아래 행기물이라는 샘물을 찾으며 농부에게 물었지만 농부는 모른다고 답했다. 고종달은 행기물이 샘물의 이름인 줄 알았지만 이 행기물은 아까 백발노인이 숨겨달라 부탁한 그릇의 물이었고 결국 행기물을 찾지 못한 고종달은 그대로 돌아갔다. 고종달은 배를 타고 돌아가다 한라산신이 일으킨 바람에 의해 배가 침몰해 죽고 말았다.

3.2.3 고종달 설화 속 스푸핑 공격

고종달이 물혈을 찾아 끊지 못하게 백발노인은 기지를 발휘해 샘물을 행기에 담아 농부에게 숨겨줄 것을 부탁했다. 농부와 백발노인의 협력으로 제주의 물길은 다 끊어지지 않게 되었다. 이는 신분을 위장하여 네트워크에 침입해 정보를 빼가거나 가짜 웹사이트로 유도하는 스푸핑 공격의 원리와 연결지을 수 있다. 고종달의 입장에서는 제주 사람들이 샘물의 형태를 위장시켜 자기 일을 훼방 놓은 공격자로 느껴졌을 것이다. 이들의 행기물 작전을 스푸핑 공격으로 비유할 수 있다.

스푸핑 공격과 고종달 설화의 구성요소의 연결점은 표 3에서 확인할 수 있다. 웹사이트를 활용한 스푸핑 공격으로 비교해보자면 공격자는 농부에게 접근한 백발노인, 표적은 고종달이다. 백발노인은 진짜 웹사이트인 마을의 물을 지키기 위하여 가짜 웹사이트인 행기물을 꾸며낸다. 또한, 네트워크 권한을 획득하여 공격에 성공하는 것은 고종달이 물혈을 찾는 일을 방해한 것으로 비유할 수 있다.

표 3. 스푸핑 공격과 고종달 설화의 구성요소 연결
Table 3. Components of spoofing attack and the tale of Gojongdal

Spoofing attack	Tale of Gojongdal
Attacker	Old man with grey hair
Fake website	Water in the vessel
Real website	Water of Village
Acquiring network permissions	Interference with water flow tracking
Target	Gojongdal

3.3 세션 하이재킹 공격-영등할망 전설

3.3.1 세션 하이재킹 공격

세션 하이재킹 공격은 정상적 접속 과정에서 일어나는 TCP(Transmission Control Protocol) 3-Way Handshaking 과정에서 발생하는 세션을 가로채는 공격 방식을 말한다[22]. 사용자가 로그인된 상태를 가로채 상대방의 접속 ID나 비밀번호를 알지 못해도 인증 작업 없이 사용자의 PC에 접근할 수 있는 권한을 얻게 된다.

본 논문에서 제안하는 세션 하이재킹 공격에 관한 교육 콘텐츠로는 세션 하이재킹의 정의, 하이재킹의 어원, TCP 3-Way Handshaking의 과정, TCP 세션 하이재킹 공격 단계, IP 스푸핑과의 차이점, 동기화 상태와 TCP 세션 하이재킹 후 비동기화 상태 비교가 있다. 또한 서버와 클라이언트의 연결을 해제하고 세션을 종료하는데 수행되는 과정인 TCP 4-Way Handshaking도 추가 설명할 것을 제안한다. 그림 3은 세션 하이재킹 공격 교육 콘텐츠의 일부를 보여준다[23].

3.3.2 영등할망 전설

제주의 바다를 지켜주는 영등신에 관해 전해 내려오는 이야기를 영등할망 전설이라 한다. 제주에서는 음력 2월 초하루부터 보름까지 영등할망이 제주에 머문다고 여긴다. 하여 해당 기간에 영등할망을 기리기 위해 영등굿을 행하고 있다.

영등할망 전설을 요약하면 다음과 같다[24].

어머니는 바다요, 아버지는 바람인 영등은 마음씨가 고와 바다생물들과 나는 새들도 그녀를 사랑했다. 그러던 어느 날 파도가 높게 들썩이고 태풍이 몰아치더니 제주에서부터 작은 고기잡이배가 위태롭게 파도에 휩쓸려왔다. 외눈박이 거인 식인종들이 사는 섬으로 밀려나는 고기잡이배를 목격한 영등은 자신의 미역 치마로 배와 사람들을 가려주었다. 그러나 반대편 섬의 거인들도 고기잡이배를 보고 입맛을 다시고 있었다. 갑자기 사라진 고기잡이배를 찾는 거인들에게 영등은 거짓말을 해 사람들을 살려주었다. 그러나 이 고기잡이배는 또 한 번 파도에 휩쓸려 이번에도 거인 식인종이 사는 섬으로 밀려나고 있었다. 마음이 어진 영등은 이번에도 그들을 딱히 여겨 거인들에게 거짓말을 하면서 고기잡이배를 숨겨주었다. 하지만 영등이 거짓말을 한 것을 알게 된 식인종들은 매우 화가 나 영등을 죽이고 말았다. 고기잡이배 사람들은 바다에서 고기를 잡다가 바다에 떠돌아다니던 영등의 토막 난 시신을 발견했다. 이들은 자신들 때문에 영등이 죽게 된 사실을 알게 되었고 통곡하며 울었다. 다행히 바다와 바람이 정성으로 영등을 돌보았더니 영등은 다시 살아났다. 이후로 영등은 매년 제주의 바다와 사람들을 지켜주었다.

3.3.3 영등할망 전설 속 세션 하이재킹 공격

외눈박이 거인들의 입장이 되어보면 정상적으로 자신들에게 향하고 있던 고기잡이배가 중간 침입자인 영등할망이 가로챈 덕분에 사라지게 된 것이다. 따라서 거인들은 자신들이 먹이를 먹지 못하게 만든 영등할망을 공격자로 여기고 그녀를 제거한 것이다. 이는 정상 데이터 통신 중 허가받지 않은 외부인이 침입하여 세션을 몰래 낚아채는 과정으로 비유할 수 있다.

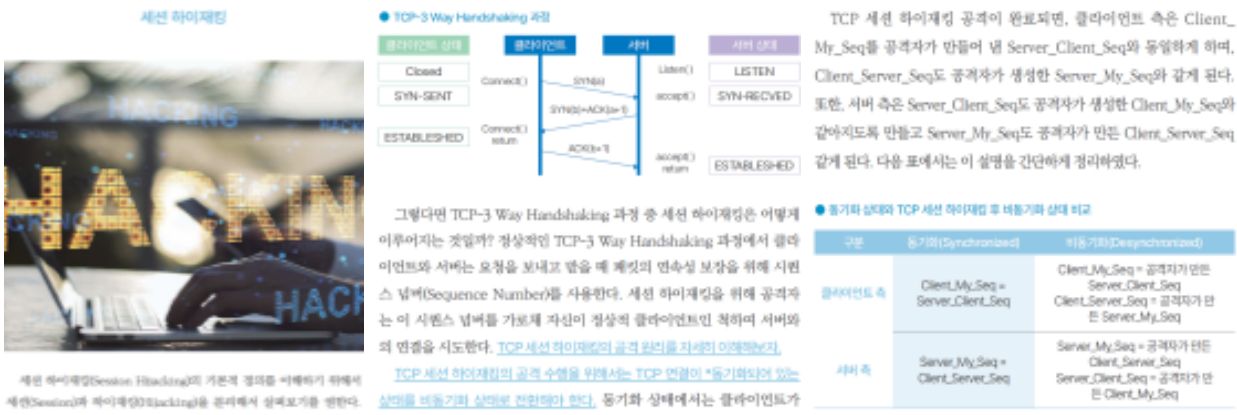

그림 3. 세션 하이재킹 공격 교육 콘텐츠[23]

Fig. 3. Educational contents for session hijacking attack[23]

세션 하이재킹 공격과 영등할망 전설의 구성요소를 연결한 결과는 표 4와 같다. 세션 하이재킹 공격은 클라이언트와 서버의 연결 사이에서 일어난다.

표 4. 세션 하이재킹 공격과 영등할망 전설의 구성요소 연결
Table 4. Components of session hijacking attack and the legend of Yeongdeung Halmang

Session hijacking attack	Legend of Yeongdeung Halmaing
Client	Cyclops
Intruder(Attacker)	Yeongdeung halmaing
Server	Wave
Sequence number	Fishing boat

이에 클라이언트는 외눈박이 거인 식인종으로, 서버는 파도라 할 수 있다. 이들의 통신을 방해한 것은 영등할망이다. 세션 하이재킹 공격에서는 공격자가 시퀀스 넘버를 가로채는데, 영등할망이 시퀀스 넘버인 고기잡이배를 중간에서 가로채 숨겨주었다고 표현할 수 있다.

Ⅳ. 네트워크 보안 융합 수업 방안

초등학생 학습자를 대상으로 흥미롭게 네트워크 보안을 교수할 수 있도록 학습 게임을 개발하였으며, 개발된 학습 게임을 포함하여 네트워크 보안 수업을 수행하는 수업 방안을 S.-S. Park and S.-K. Han(2010)이 제안한 KASP model[16]을 기반하여 전개하였다.

4.1 학습 게임 개발

4.1.1 놀이로 학습하는 DDoS 공격

봇넷 제어 모델의 C&C 모델과 P2P 모델을 통해 공격을 수행하는 원리를 놀이로 학습할 수 있도록 학습 게임을 개발했다. C&C 모델은 서버가 하나이므로 해커팀에서 C&C 서버 역할을 하는 학생 한 명을 선발해야 하며, 심판 역할을 할 교사나 부모가 필요하다. C&C 모델 이해 학습 게임의 절차는 표 5와 같고, 게임의 흐름도는 그림 4와 같다.

표 5. C&C 모델 이해 학습 게임 절차
Table 5. Procedure for educational game understanding C&C model

Stage	Instruction
1	Divide the teams into hacker team and tracker team.
2	Select one teacher or judge.
3	From the hacker team, select one friend to serve as the C&C server and one as the bot master.
4	People other than the C&C server and bot master in the hacker team become zombie PCs.
5	The bot master secretly passes information to the C&C server from the Hacker Team, and the C&C server secretly passes the information received from the bot master to other zombie PCs. It is important to note that this information must be passed without the Tracker Team knowing.
6	Once the secret information from the bot master has been passed to both the C&C server and zombie PCs in the hacker team, the tracker team interviews the hacker Team for a certain period.
7	After the interview time is up, the tracker team informs the judge of the identity of the bot master and C&C server in the hacker team and what the secret information was, based on the interview.
8	The hacker team also shares their roles and the content of the secret information with the judge.
9	If the tracker team has correctly deduced the roles and information of the hacker team, the judge declares the tracker team is the winner. However, if the secret information is correct but the information about the bot master or C&C server is wrong, the tracker team loses. If the hacker team manages to keep their roles secret and all zombie PCs have the same secret information, the judge declares the hacker team the winner.

P2P 모델 이해 게임은 C&C 모델 이해 게임과 기본적인 게임 절차가 비슷하나 P2P 모델은 C&C 서버 자체가 좀비 PC이므로 C&C 서버 역할을 할 사람을 따로 선발할 필요가 없다. P2P 모델 이해 학습 게임의 절차는 표 6과 같고, 게임의 흐름도는 그림 5와 같다.

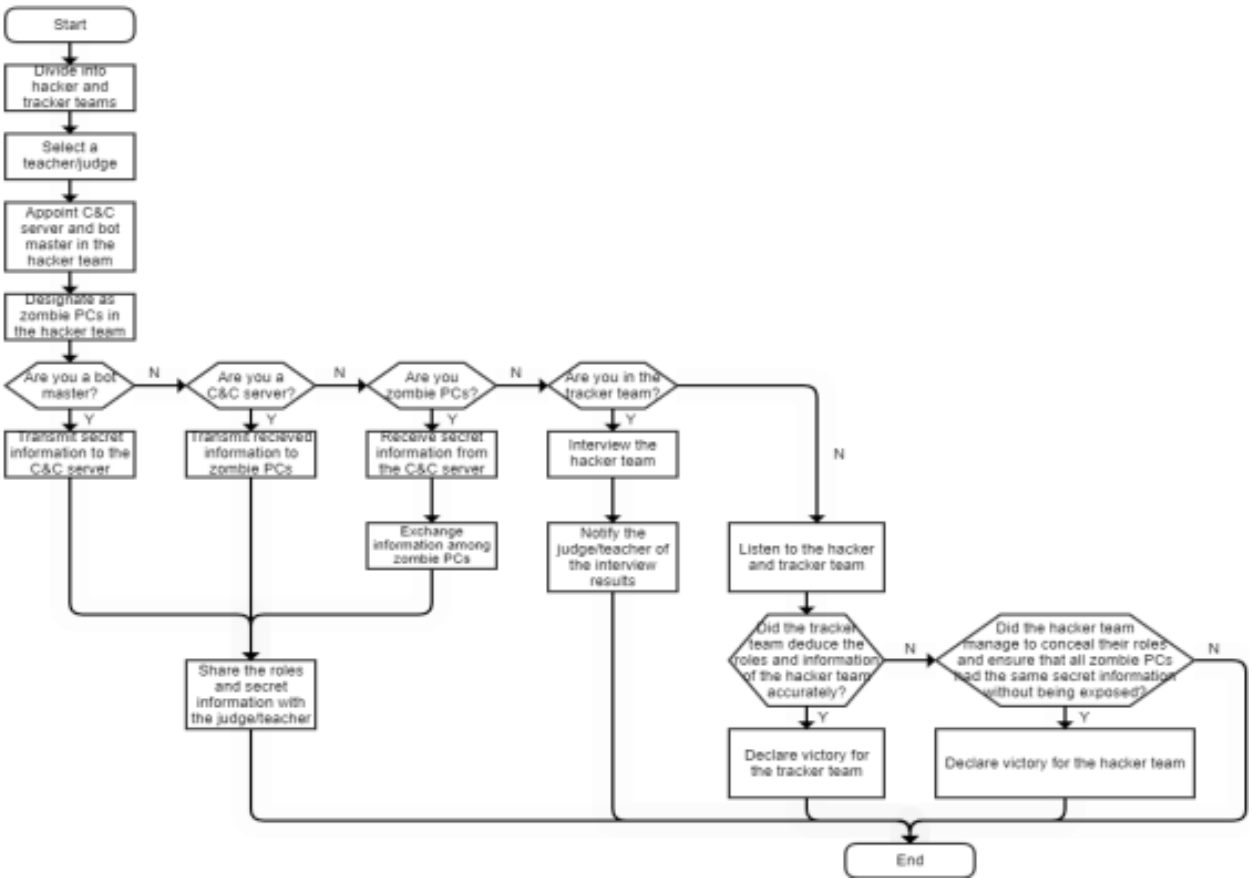

그림 4. C&C 모델 이해 학습 게임 흐름도
Fig. 4. Flow chart for educational game understanding C&C model

놀이에 역할이 다양하므로 최소 8명 이상이 되어야 놀이가 진행된다. C&C 모델과 P2P 모델 게임 모두 해커팀에서 봇 마스터, C&C 서버, 좀비 PC의 역할을 선발할 때 추적자 팀이 모르게 해야 한다. 해커 팀은 추적자 팀 몰래 비밀 정보를 전달하기 위해 노력해야 한다. 또한, 심판은 추적자 팀이 해커 팀을 인터뷰하는 시간을 적절하게 정해주어야 한다. C&C 모델 게임에서는 좀비 PC끼리는 비밀 정보를 공유하지 않고 무조건 C&C 서버만을 통해 비밀 정보를 전달받아야 하지만 P2P 게임에서는 좀비 PC끼리 서로 정보를 전달해도 된다.

표 6. P2P 모델 이해 학습 게임 절차
Table 6. Procedure for educational game understanding P2P model

Stage	Instruction
1	Divide the teams into hacker team and tracker team.
2	Select one teacher or judge.
3	In the hacker team, only the bot master needs to be determined. All other members of the hacker team become zombie PCs.
4	Similar to the C&C model game, the bot master communicates the secret information to all zombie PCs. Zombie PCs can also share secret information with each other
5	After the secret information sharing, the tracker team conducts interviews to uncover the bot master and the content of the secret information within a certain time frame
6	Both the tracker team and the hacker team convey their information to the judge
7	If the tracker team accurately identifies the bot master and the secret information of the hacker team, the rracker ream wins. Since there is no C&C server this time, identifying only the bot master and one secret information is sufficient for the tracker team to win. The hacker team is considered to win if the secret information shared among the zombie PCs is the same, and the tracker team successfully conveys this information to the judge without them knowing

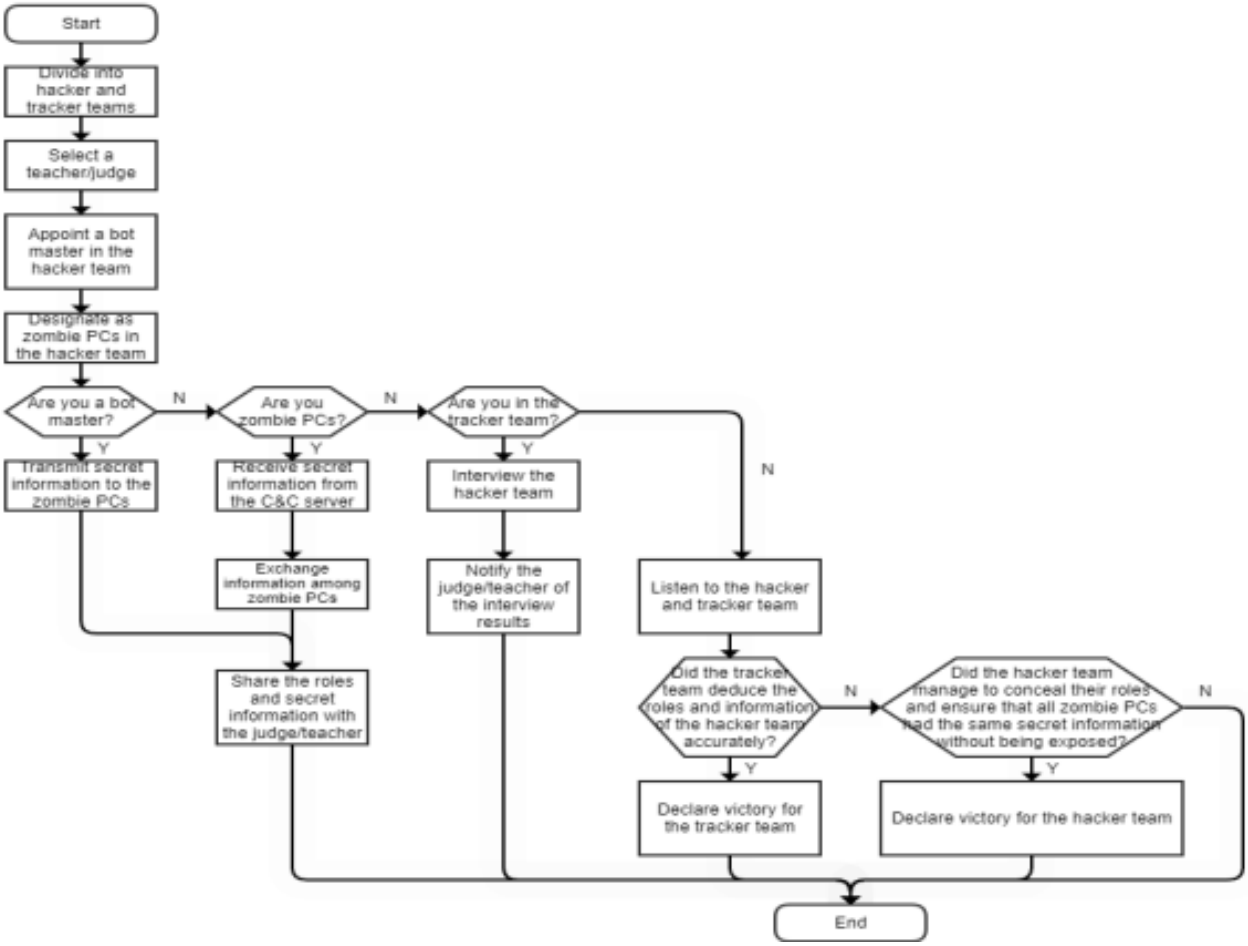

그림 5. P2P 모델 이해 학습 게임 흐름도
Fig. 5. Flow chart for educational game understanding P2P model

4.1.2 놀이로 학습하는 스푸핑 공격

스푸핑 공격 중 IP 스푸핑 공격을 놀이를 통해 이해할 수 있도록 학습 게임을 설계했다. 기본적으로 교사가 문제를 내고 학생들이 협력하여 맞히는 방식으로 진행된다. IP 스푸핑 공격 이해 학습 게임의 절차는 표 7과 같고, 게임의 흐름도는 그림 6과 같다.

학습자들이 공격자로 분한 교사가 전송한 변조된 IP 주소를 찾아내 IP 스푸핑 공격을 막는 원리를 간단하게 이해할 수 있도록 개발했다. 한 학급의 인원이 적다면 팀을 나누지 않고 한 학급 전체가 교사를 상대로 게임을 진행할 수도 있다.

표 7. IP 스푸핑 공격 이해 학습 게임 절차
Table 7. Procedure for educational game understanding IP spoofing attack

Stage	Instruction
1	Students are divided into multiple teams within a class, with each team consisting of at least two members.
2	The teacher creates nine IP addresses following a specific rule, with one IP address being randomly generated without any rule.
3	Students, in their respective teams, discuss and try to identify the fake IP address.
4	Students reveal the fake IP address they have identified and present their reasoning.
5	After all teams have presented, the teacher reveals the rule behind the fake IP address and real IP addresses.
6	The team that accurately identifies the fake IP address and the rule wins.

그림 6. IP 스푸핑 공격 이해 학습 게임 흐름도
Fig. 6. Flow chart for educational game understanding IP spoofing attack

4.1.3 놀이로 학습하는 세션 하이재킹 공격

서버와 클라이언트의 통신을 방해하는 해킹 기법인 세션 하이재킹을 비밀 메시지를 전달하는 놀이로 이해할 수 있도록 학습 게임을 설계했다. 네 명을 모아 해커, 서버, 클라이언트, 해커조력자로 역할을 나누어 해커를 피해 서버와 클라이언트가 통신에 성공하도록 만드는 게임이다. 세션 하이재킹 공격 이해 학습 게임의 절차는 표 8과 같고, 게임의 흐름도는 그림 7과 같다.

표 8. 세션 하이재킹 공격 이해 학습 게임 절차
Table 8. Procedure for educational game understanding session hijacking attack

Stage	Instruction
1	Hackers, servers, clients, and hacker accomplices are divided by drawing lots.
2	Conduct the day's work or class as usual.
3	While doing other tasks, hackers must secretly find their hacker accomplice, and hacker accomplices find the hacker. The hacker and hacker accomplice form a team to manipulate and disrupt the sequence numbers transmitted by the server and client, pretending to be the server or client by manipulating and transmitting the sequence numbers.
4	The server writes down the sequence numbers to be given to the client on their smartphone.
5	Similarly, while doing other tasks, servers must secretly find clients, and clients find the server. When the server finds the client, they show the sequence numbers written on the smartphone to the client.
6	At the end of the game, everyone reveals the slips of paper they had drawn. The client reveals the sequence numbers to everyone. All compare the sequence numbers revealed by the client with those written on the server's smartphone to confirm if they match. If the sequence number received by the client matches the one sent by the real server, the server and client win.
7	Hackers and hacker accomplices also reveal all the manipulated sequence numbers to everyone. If the manipulated sequence numbers sent by the hackers and hacker accomplices match those received by the server and client, the hackers and hacker accomplices win.

4.2 융합 수업 방안

학습 순서 도입은 이해 단계로 네트워크 보안의 개념과 중요성을 이해하고 네트워크 공격 기법을 알아보도록 한다. 팀별로 나누어 조사하고 발표하는 협동학습 방법을 사용한다.

학습 순서 전개는 소양과 활용 단계로 DDoS 공격, 스푸핑 공격, 세션 하이재킹 공격 기술을 구체적으로 이해하는 시간을 가진다.

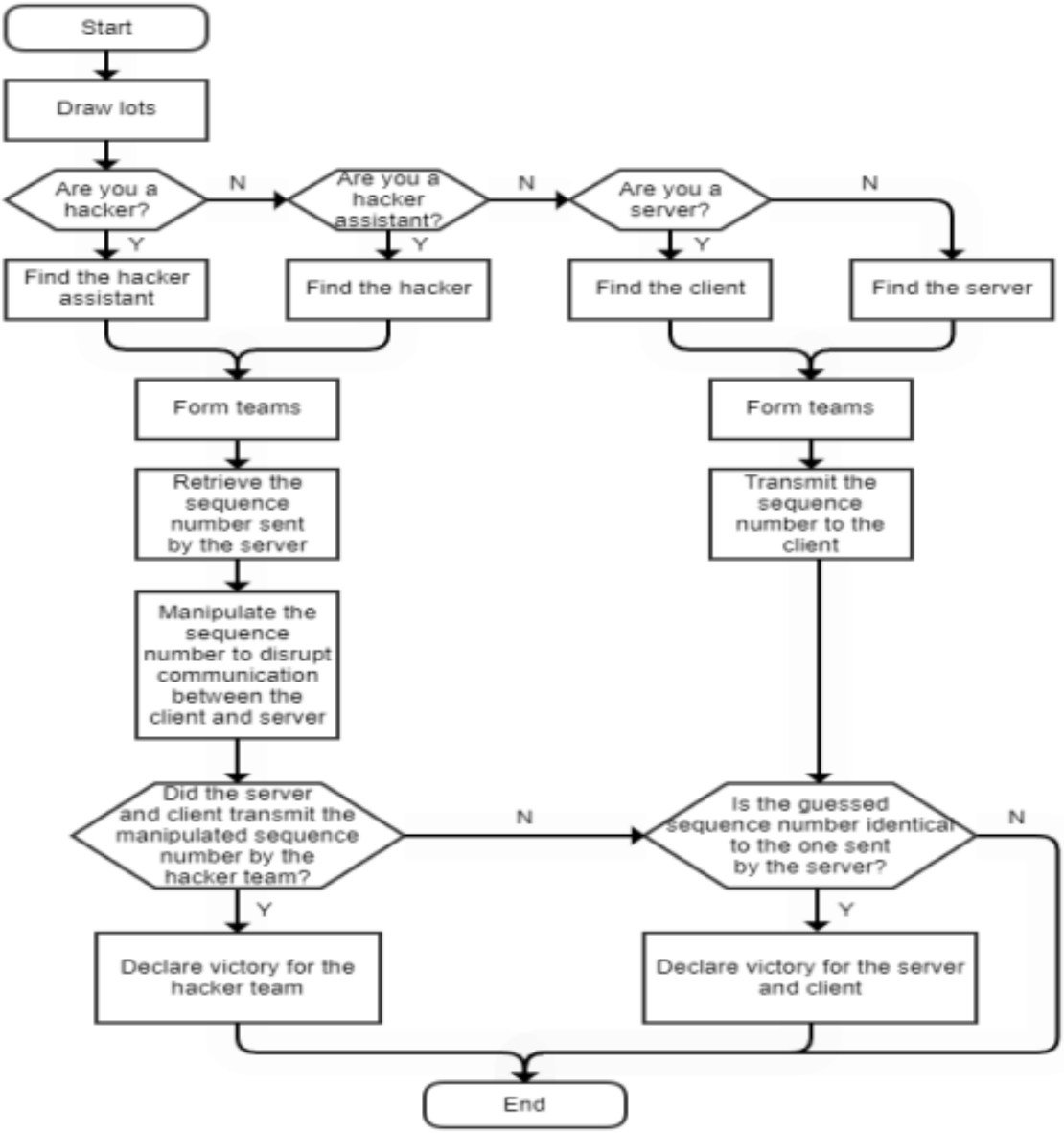

그림 7. 세션 하이재킹 공격 이해 학습 게임 흐름도
Fig. 7. Flow chart for educational game understanding session hijacking attack

이 단계에서는 교사의 직접교수법으로 학생들에게 직접 기술을 설명하는 것으로 시작해 각 기술과 연계된 제주 설화를 제공하여 학습자들로 하여금 직접 읽고 각 기술을 비유적으로 표현한 내용이 무엇인지 찾아보도록 한다. 그리고 개발된 학습 게임을 수행하여 학습자들에게 어렵고 낯선 개념을 흥미롭게 교수한다. 마지막 학습 순서 정리는 평가단계로 실생활에서 실천할 수 있는 네트워크 보안 방법을 모색하고 동료 평가를 통해 서로의 학습 태도를 평가하며 마무리한다.

KASP 모델은 본래 대면 수업을 가정하여 개발된 것이지만, 본 논문에서 제안하는 융합 수업 방안은 대면 수업은 물론 비대면 수업에서도 적용할 수 있다. 특히 메타버스 공간을 활용한다면 학습자와 교수자 간 적극적 상호작용을 강화할 수 있고, 학습 게임 수행시 학습자의 수업 집중도를 높이며, 학습자가 주도적으로 수업에 참여할 수 있는 기회를 제공할 수 있다.

KASP 모델을 기반하여 설계한 초등학생 대상 인문학적 요소 접목 네트워크 융합 수업 방안은 표 9와 같다.

표 9. 네트워크 보안 융합 수업 방안
Table 9. Network security integration teaching plan

Stage		Learning element	Teaching and learning content and activities	Learning method
Introduction	Understanding	Knowledge and attitude	▶ Understanding the concept of network security Research the definitions of network and information security. ▶ Understanding the importance of network security Investigate and present cases of damages caused by network attacks by teams.	Cooperative learning
			▶ Exploring network attack techniques Research and present the techniques used to attack networks by teams.	
Development	Cultivation of competency Utilization	Practice	▶ Understanding DDoS attack techniques - Understand the definition of botnets, the origin of the term botnet, real cases of botnet attacks, components of botnet, and types of botnet control models through the teacher's explanation. - Understand the definition of DDoS attacks, real cases of DDoS attacks, stages of DDoS attacks, and types of botnets used in recent DDoS attacks through the teacher's explanation. - Understand DoS and DRDoS attacks through the teacher's explanation. ▶ Exploring DDoS attacks in the legend of General five hundred Read the legend of General General five hundred provided by the teacher and analyze the DDoS attack techniques hidden within the legend of General General five hundred. ▶ Learning through the DDoS attack games - Understand the method of attacks utilizing the C&C model through a learning game on understanding the C&C model. - Understand the method of attacks utilizing the P2P model through a learning game on understanding the P2P model.	Direct instruction Gamification
	Cultivation of competency Utilization		▶ Understanding spoofing attack techniques - Understand the origin of spoofing, real cases of spoofing attacks, and types of spoofing (ARP spoofing, IP spoofing, DNS spoofing) through the teacher's explanation. - Understand similar terms such as sniffing and snooping through the teacher's explanation. ▶ Exploring spoofing attack in the legend of Gojongdal Read the legend of Gojongdal provided by the teacher and analyze the spoofing attack techniques hidden within the legend of Gojongdal. ▶ Learning through the spoofing attack game Play a learning game on IP spoofing attack to understand the principle of detecting manipulated IP addresses and responding to attack.	Direct instruction Gamification
	Cultivation of competency Utilization		▶ Understanding session hijacking attack techniques - Gain understanding of session hijacking by learning the definition, origins, TCP 3-Way Handshaking process, stages of the TCP session hijacking attack, distinctions from IP spoofing, and differences between synchronized and desynchronized states following TCP session hijacking, as explained by the teacher. - Grasp the advanced concept of TCP 3-Way Handshaking through the teacher's explanation. ▶ Exploring session hijacking attacks in the legend of Yeongdeung Halmang Read the legend of Yeongdeung Halmang provided by the teacher and analyze the session hijacking attack techniques hidden within the legend of Yeongdeung Halmang. ▶ Learning through the session hijacking attack game Play a learning game on understanding session hijacking attacks to understand the hacking principles of disrupting communication between servers and clients.	Direct instruction Gamification

Conclusion	Review	Knowledge and attitude	▶ Researching network security methods I can implement in real life - In teams, search for network attack cases related to our daily lives. - Explore ways to practice network security in our daily lives.	Problem-solving learning
		Practice	▶ Evaluating each other's learning attitudes Evaluate classmates' learning performance, presentation attitudes, etc., through peer evaluations.	

Ⅴ. 결론 및 향후 과제

정보통신기술의 발전을 통해 현실 세계와 디지털을 기반한 가상세계가 융합되며 점차 인간은 두 세계에 동시에 거주하는 상태가 되었다[25][26]. 특히 태어나자마자 디지털 환경에 노출되어 디지털 기기 활용에 익숙한 디지털 네이티브 세대는 이미 온라인 공간과 오프라인 공간을 별개의 공간으로 인식하지 않는다[27]. 이제 인간은 현실에 존재하며 동시에 정보 환경과 유기적으로 연결되어 정보적으로 체현된 인포그(Inforg)가 되어가고 있다[28]. 이렇듯 IT와 인간은 매우 밀접한 관계를 맺고 있다.

2019년 12월 정부가 발표한 인공지능 국가 전략에서는 어릴 때부터 소프트웨어와 인공지능을 배울 수 있도록 지원할 것이며 전 연령과 직군에 걸쳐 모두가 인공지능 기초 역량을 습득할 수 있는 체계를 구축하겠다고 밝혔다[29][30]. 즉, 정보보안에 관한 인식도 이제 전문가뿐만 아니라 초등학생도 가져야 할 교양 지식이라 할 수 있겠다.

이에, 본 논문에서는 교육 참여자의 네트워크 보안에 관한 이해도를 높이고 이에 더하여 융복합적 사고 증진 또한 가능케 할 수 있도록 인문학을 융합하여 정보 교육을 설계하고자 하였다. 이러한 목적 달성을 위해 선행 연구를 분석하여 네트워크 보안 교육 콘텐츠를 선정하고자 하였는데, B. Kim et al.(2003)[9]의 연구에서는 DoS 공격과 스캐닝을 제안했으나 본 논문에서는 DoS 공격보다 복잡하고 최근 매우 빈번하게 이루어지는 DDoS 공격을 다루기로 했으며, 유사개념인 DoS, DRDoS, APDoS 공격은 해당 콘텐츠 내에서 포함하여 언급하였다. 더불어 D. Yang(2018)[10]의 연구는 비교적 최근에 이루어졌으며 기초 정보보안 교육을 위해 개발되었기 때문에 본 연구에서는 기본적으로 해당 연구자의 기술 분류를 기반하여 교육 콘텐츠를 선정하였다. 또한 J. Bang et al.(2019)[11]의 연구는 현장 실무자를 대상으로 이루어져 네트워크 공격 기술을 세밀하게 구분하였다. J.-H. Choi et al.(2022)[12]의 연구도 최신의 연구이며 D. Yang(2018)[10] 연구와 유사하게 네트워크 보안 기술을 분류했고, 이들의 연구에서 언급한 포이즈닝 공격 기술은 다른 연구에서는 분류되지 않았던 개념이라 교육 콘텐츠로 다루지 않았다.

이에 더하여, 본 논문에서는 D. Lee and N. Park(2016)[13], J. Kim et al.(2021)[14]의 연구를 반영하여 학습자의 흥미를 일으킬 수 있는 방향으로 교육을 수행할 수 있도록 학습 게임을 설계하였고, 이를 S.-S. Park and S.-K. Han(2010)[16]이 제안한 정보보호 교육을 위한 모델을 기반하여 본 연구에서 선정한 교육 콘텐츠를 초등학교 수업에 적용할 수 있도록 수업 방안을 구상하였다. 이 수업 방안을 활용하면 협동학습, 직접교수법, 게임화, 문제해결학습 등 다양한 학습방법을 통해 초등학생의 네트워크 보안 지식, 태도, 실천 역량을 함양할 수 있다.

본 논문은 DDoS 공격, 스푸핑 공격, 세션 하이재킹 공격과 같은 중요한 보안 주제를 다루었으며, 이를 교육의 콘텐츠로 하여 초등학생을 대상으로 적용할 수 있는 학습 게임을 개발하였다. 더불어, 확장된 정보보호 통합학습 모형을 기반으로 수업 방안을 제시하였는데, 이 수업 방안을 통해 구체적인 적용 가능성을 모색할 수 있다. 특히 선행 연구에서 찾아보기 어려운 보안교육에 인문학적 측면을 접목한 창의적인 교육 방식을 취해 학습자의 IT인문학 기반의 융·복합적 사고력 향상에 기여할 수 있다.

향후 전문가를 대상으로 본 논문에서 선정한 교육 콘텐츠의 타당도와 적합성을 분석할 필요가 있으며, 중요도-수행도 분석(IPA, Importance-Performance Analysis)이나 효과성 분석을 통해 고안한 네트워크 보안 융합 수업 방안의 개선 연구의 진행이 후속적으로 진행되어야 하겠다. 더하여, 본 논문을 통해 초등 정보교육 및 정보보안 인식 교육 연구에 여러 시사점을 제공하기를 희망한다.

References

[1] Korea Internet & Security Agency, https://www.kisa.or.kr/20205/form?postSeq=1024&lang_type=KO. [accessed: Oct. 13, 2023]

[2] H.-Y. Kim, "One big data and humanities", Citizen and Humanities, Vol. 30, pp. 70-95, Feb. 2016.

[3] E. Choi, D. Hyun, H. Lee, and N. Park, "A proposal for development plan of mid-to long-term advanced policy for IT humanities convergence education", Proc. of KIIT Conference, Jeju, Korea, pp. 27-27, Jun. 2022.

[4] J.-Y. Kim and K. Kim, "The educational effect of novel engineering on artificial intelligence convergence liberal arts course for pre-service teacher", Journal of The Korean Association of Information Education, Vol. 26, No. 6, pp. 507-515, Dec. 2022. http://dx.doi.org/10.14352/jkaie.2022.26.6.507.

[5] S. Kim, "Exploring the design of artificial intelligence convergence liberal arts curriculumbased on flipped learning and maker education: focusing on learner needs assessment", Journal of Practical Engineering Education, Vol. 13, No. 2, pp. 221-232, Aug. 2021. https://doi.org/10.14702/JPEE.2021.221.

[6] E. Choi and N. Park, "A design and demonstration of future technology it humanities convergence education model", The Journal of the Convergence on Culutre Technology (JCCT), Vol. 9, No. 3, pp. 159-166, May 2023. https://doi.org/10.17703/JCCT.2023.9.3.159.

[7] E. Choi, J. Ko, K. Choi, H. Kim, H. Lee, and N. Park, "Creative convergence course 『Future confluence IT humanities』 development and operational effectivenvess verification", Journal of Korea Multimedia Society, Vol. 24, No. 4, pp. 569-582, Apr. 2021. https://doi.org/10.9717/kmms.2020.24.4.569.

[8] S.-H. Oh and T. Nam, "Trend analysis for network security technologies", Proc. of 2003 Korean Institute of Information Scientists and Engineers, Vol. 30, No. 2, pp. 688-690, Oct. 2003.

[9] B. Kim, H. Son, and S. Park, "Countermeasures against denial of service attacks and scanning techniques", Korea Information Processing Society Review, Vol. 10, No. 2, Mar. 2003.

[10] D. Yang, "Information security", Hanbit Academy, Inc, pp. 117-182, Jan. 2018.

[11] J. Bang, J. Lee, and J. Lee, "Network attack packet analysis for security practitioners", Freelec, pp. 4-13, Nov. 2019.

[12] J.-H. Choi, S. Lee, and Y. G. Seo, "Spoofing attack detection and blocking model based on ARP attack signature information", Journal of Digital Contents Society, Vol. 23, No. 8, pp. 1485-1495, Aug. 2022. http://dx.doi.org/10.9728/dcs.2022.23.8.1485.

[13] D. Lee and N. Park, "Teaching book and tools of elementary network security learning using gamification mechanism", Journal of the Korea Institute of Information Security and Cryptology, Vol. 26, No. 3, pp. 787-797, Jun. 2016. http://dx.doi.org/10.13089/JKIISC.2016.26.3.787.

[14] J. Kim, S. Kim, and N. Park, "Suggestion of elementary school information security education elements based on pipe game to understand the principle of data de-identification", Journal of the Korea Institute of Information Security and Cryptology, Vol. 31, No. 5, pp. 1063-1069, Oct. 2021. https://doi.org/10.13089/JKIISC.2021.31.5.1063

[15] C. 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. https://doi.org/10.9708/jksci.2020.25.10.069.

[16] S.-S. Park and S.-K. Han, "KASP-Integrated

learning model for the information security education in elementary education", Journal of the Korean Association of Information Education, Vol. 14, No. 2, pp. 157-164, Mar. 2010.

[17] S. Hong, "DDoS Attack traffic through the analysis of responses to research", Journal of Convergence Society for SMB, Vol. 4, No. 3, pp. 1-6, Sep. 2014.

[18] E. Choi and N. Park, "Encountering Information Security Humanities through Jeju Stories", Jeju University Press, pp. 214-220, Dec. 2022.

[19] J. -H. Lee, "A study on cultural planning based on the characteristics of domestic cultural archetypes: focusing on the Jeju folktale ‘Seolmundae halmang and obaek general’", Journal of the Korea Entertainment Industry Association, Vol. 15, No. 7, pp. 259-269, Oct. 2021. https://doi.org/10.21184/jkeia.2021.10.15.7.259

[20] E. Choi and N. Park, "Encountering Information Security Humanities through Jeju Stories", Jeju University Press, pp. 67-71, Dec. 2022.

[21] The Academy of Korean Studies. http://www.grandculture.net/seogwipo/toc/GC04601886 [accessed: Oct. 16, 2023]

[22] J.-Y. Choi, J.-H. Park, Y. G. Seo, S.-W. Hong, and S.-B. Kim, "A reliable service provided model for session hijacking attacks in big data service environments", Journal of Knowledge Information Technology and Systems, Vol. 11, No. 6, pp. 597-606, Dec. 2016.

[23] E. Choi and N. Park, "Encountering Information Security Humanities through Jeju Stories", Jeju University Press, pp. 292-298, Dec. 2022.

[24] H.-S. Song, "Ocean belief in east Asia and Youngdung halmang and seonmundae halmang in Jeju Island", Tamla Culture, No. 37, pp. 183-222, Aug. 2010. https://doi.org/10.35221/tamla.2010..37.006.

[25] M. Johnson-Roberson, C. Barto, R. Mehta, S. N. Sridhar, K. Rosaen, and R. Vasudevan, "Driving in the matrix: Can virtual worlds replace human-generated annotations for Real World Tasks?", Proc. of International Conference on Robotics and Automation, arXiv:1610.01983, Feb. 2017. https://doi.org/10.48550/arXiv.1610.01983.

[26] M. Kim and M. Lee, "A study on the factors influencing the intention to use the metaverse: Focusing on innovation resistance model", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 23, No. 1, pp. 51-58, Feb. 2023. https://doi.org/10.7236/JIIBC.2023.23.1.51.

[27] A. J. Autry Jr and Z. Berge, "Digital natives and digital immigrants: getting to know each other", Industrial and Commercial Training, Vol. 43, No. 7, pp. 460-466, Oct. 2011. https://doi.org/10.1108/00197851111171890.

[28] E. Song, "The humanities education in the era of the 4th industrial revolution : centered on the philosophy and ethics of information", The Journal of Cultural Exchange, Vol. 8, No. 2, May 2019, https://doi.org/10.30974/kaice.2019.8.2.69.

[29] Y. Jeong, "A critical analysis of the draft proposal of 2022 revised practical arts (technology·home economics) curriculum", Journal of The Korean Association of Information Education, Vol. 26, No. 5, pp. 457-465, Oct. 2022. http://dx.doi.org/10.14352/jkaie.2022.26.5.457.

[30] Y.-H. Jeong, H. Kim, K. R. Park, and S. M. Yoo, "A study of AI education program based on big data: Case study of the general education high school", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 23, No. 1, pp. 83-92, Feb. 2023. https://doi.org/10.7236/JIIBC.2023.23.1.83.

저자소개

최 은 선 (Eunsun Choi)

2016년 7월 : 북경어언대학교 국제중국어교육(교육학석사)
2022년 8월 : 제주대학교 일반대학원 컴퓨터교육전공 (교육학박사)
2020년 3월 ~ 2023년 5월 : 제주대학교 사이버보안인재교육원 선임연구원
2023년 6월 ~ 현재 : 제주대학교 창의교육거점센터 학술연구교수
관심분야 : 컴퓨터교육, 정보교육, IT인문학, 융복합교육, 인공지능 교육, 창의교육, STEAM

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
2003년 4월 ~ 2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월 ~ 2009년 12월 : 미국 UCLA대학교 공과대학 Post-Doc, WINMEC 연구센터 Staff Researcher
2010년 1월 ~ 2010년 8월 : 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년 9월 ~ 현재 : 제주대학교 초등컴퓨터교육전공, 대학원 융합정보보안학과 교수
2011년 9월 ~ 현재 : 창의교육거점센터장, 과학기술사회(STS)연구센터 부센터장, 정보영재 주임교수, 사이버보안인재교육원장
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드