Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.787

게이미피케이션 메커니즘을 이용한 초등 네트워크 정보보안 학습교재 및 교구 개발*

이 동 혁,[1†] 박 남 제[1,2‡]
[1]제주대학교 일반대학원 컴퓨터교육전공, [2]제주대학교 교육대학 초등컴퓨터교육전공

Teaching Book and Tools of Elementary Network Security Learning using Gamification Mechanism*

Donghyeok Lee,[1†] Namje Park[1,2‡]
[1]Dept. of Computer Education, Graduate School, Jeju National University
[2]Dept. of Computer Education, Teachers College, Jeju National University

요 약

사이버 범죄가 급증함에 따라 초등학생에게도 정보보호 교육의 필요성이 증대되고 있다. 사이버 범죄로부터 학생들을 보호하고 예방하기 위해서는 정보보호에 대한 교육이 절대적으로 필요하다. 정보보호교육을 위한 소양 지식적 접근을 통해 태도와 소양기술이 통합된 실천중심의 정보보호교육이 이루어질 수 있다. 본 논문에서 개발된 게이미피케이션(gamification) 메커니즘을 이용한 초등학교 현장에서의 네트워크 정보보안 학습 교구가 초등학생들의 정보보호 지식 및 태도, 기능뿐만 아니라 실천능력에도 효과적임을 보였다.

ABSTRACT

This paper is directed for the information security education of the elementary students. The dependence on human involvement and human behavior to protect information assets necessitates an information security education to make the awareness of their roles and responsibilities towards information security. The information security education is needed even to elementary school students. The information security learning model integrating knowledge, attitudes, and ways to practice was developed, and the teaching plan and learning material hand-out were accordingly made out. As the test result analysis, it was verified that the developed teaching tools of elementary network security learning using gamification mechanism was effective to help the students learn the knowledge, attitudes, skills and ways to practice.

Keywords: Elementary Education, Elementary Network Security, Gamification, Teaching Tool, Security Learning

I. 서 론

최근 정보보호에 대한 관심이 점차 늘어나고 있는 추세이며, 이에 따라 대학에서도 정보보호 관련 학과가 대폭 늘어나는 추세이다. 현재 상황과 수요를 고려해 볼 때, 정보보호에 대한 진로는 매우 전망이 밝다고 볼 수 있으며, 향후에도 지속적으로 정보보호 인력이 필요하게 될 것이다[2].

초등학생은 향후의 진로를 자의 또는 타의에 의해서 여러번 고민하게 된다. 다양한 진로체험 방법이

Received(02. 19. 2016), Modified(04. 18. 2016), Accepted(04. 19. 2016)
* 이 논문은 2016년도 정부(교육부)의 재원으로 한국과학창의재단(2016년도 학부생 연구프로그램)의 지원을 받아 수행된 연구임. 그리고, 이 논문은 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2015S1A5A8018037).
† 주저자, bonfard@jejunu.ac.kr
‡ 교신저자, namjepark@jejunu.ac.kr(Corresponding author)

존재하면 이러한 진로 결정에 많은 도움이 될 것이나, 직종에 따라 그러한 여건이 어려운 경우도 있다. 특히, 정보보호 분야는 기술적인 부분이 매우 중요하고, 폭넓은 배경 지식을 필요로 한다. 이러한 특성에 따라 정보보호분야가 구체적으로 어떤 역할을 하는지 초등학생에게 쉽게 설명하기 어렵다는 문제가 있다.

본 논문에서 개발된 게이미피케이션 메커니즘을 이용한 초등 네트워크 정보보안 학습 교구는 이에 대한 한가지 해결책이 될 수 있으며, 초등학생의 흥미 유발과 함께 자연스러운 간접 직종 체험이 가능하다. 그러나, 정보보호 학습교구 및 학습게임 시장은 국내에서 매우 좁은 상황이다. 정보보호 시장의 급성장에 따라, 정보보호 에듀게임의 보급도 필요한 상황으로 보인다. 본 논문에서는 초등학생을 대상으로 정보보호 인식 제고 및 직종의 간접체험을 위한 네트워크 정보보안 학습 교재 및 학습 교구를 설계하고 개발하고자 한다. 대상이 낮은 연령대임을 감안하여, 복잡한 룰을 구성하지 않고 누구나 쉽게 배울 수 있으면서 손쉽게 플레잉이 가능한 게이미피케이션 메커니즘 기반의 학습게임을 설계 및 구현하였다. 본 논문에서 설계한 학습게임에서는 특정 기업에서 보안 담당자와 해커가 대치하는 상황을 가정하여, 기업 내의 비밀정보, 개인정보, 시스템 정보를 보호하기 위하여 보안 담당자는 방화벽 구성 정책을 세우고, 침입탐지 시에 어떻게 조치할 것인지를 플레이어가 스스로 결정할 수 있게 하였다. 또한, 공격자의 입장이 되어보기도 하여, 어떻게 해야 더욱 용이하게 방화벽을 파괴하고 비밀정보로 접근할 수 있을지에 대한 고민을 할 수 있도록 게임을 구성하였다.

본 논문에서 제안하는 정보보안 모의해킹 놀이식 학습교구는 미래 유망 직업군인 정보보안전문가와 관련된 프로젝트를 수행해 정보보안전문가에 대한 초등학생들의 관심과 흥미를 높이고 창의적 진로설계를 할 수 있도록 도움을 주는 것을 목적으로 한다. 또한 프로그램을 활용하는 교사와 학생이 정보보안전문가 관련 프로젝트 지도 및 수행과정을 통해 정보보안전문가가 하는 일과 필요한 역량이 무엇인가를 자연스럽게 이해하도록 프로그램을 설계하였다. 본 논문에서 제안한 정보보안 학습교구는 컴퓨터 보안 전문가의 기본 소양을 제안된 학습 교구를 응용하여 간접적으로 체험해보는 활동으로 설계하였다. 사이버 보안에 관련된 내용이 어렵고 낯설기 때문에 기술적인 부분보다는 해당 직업의 핵심 원리에 접근할 수 있도록 내용을 구성하였다. 이 프로그램을 통해 학생들은 문제를 해결하는 과정에서 서로 소통하고 컴퓨터 보안 전문가에 관심을 가지고 창의적으로 진로를 설계할 수 있을 것이다.

본 논문의 2장에서 정보보호 및 학습교구 게임에 대한 이론적 배경을 먼저 살펴보고, 3장에서는 초등학교 현장에서의 정보보호 교육을 위한 학습교재 개발에 대해 기술한다. 4장에서는 정보보호 에듀게임에 대한 구체적인 설계 및 구현 결과를 살펴보고, 5장에서 학습효과성에 대한 분석을 진행한다. 마지막으로 6장에서 결론을 맺는다.

II. 이론적 배경

2.1 정보보호에 대한 기본적 개념

본 절에서는 정보보호의 개념을 살펴보고, 본 논문상의 정보보호 학습교구 게임에서 보호하고자 하는 정보보호의 주요 대상에 대하여 살펴보도록 한다.

2.1.1 개요

정보는 최근에 들어 가장 중요한 자원이 되었다. 정보 그 자체만으로도 훌륭한 가치를 가지게 되었고, 각종 아이디어들은 새로운 기업들이 탄생하고 성공을 하는 기반이 되었다. 이렇게 정보가 중요해진 상황에서 필요한 정보를 부당하게 얻으려는 움직임도 많아지고 있다. 그렇기 때문에 최근에는 정보를 보호하는 보안에 많은 관심이 모이고 있는 상황이다[2]. 정보보호에 대한 관점은 시대에 따라서 다른 모습을 보인다. 1970년대에는 정보보호를 데이터보안(Data security)라는 관점에서 보았고, 1980년대에는 컴퓨터 보안(Computer security), 1990년대 이후에는 보다 일반적인 정보통신 기술의 의미를 포함하여 정보보호(Information security)라는 개념을 사용하고 있다[1,3,5,8].

2.1.2 정보보호의 주요 대상

정보보호가 필요한 데이터는 매우 폭넓은 관점에서 접근할 수 있으나, 본 논문에서는 일반적인 기업과 같은 조직에서의 정보보호 환경을 가정하였으며, 이러한 환경에서는 주요하게 보호해야 할 데이터는 크게 세가지로 분류가 가능하다. 첫번째, 기업내 중요 기밀데이터로써, 회사 내의 주요 전략이나 여러

가지 외부에 알려져서는 안될 여러 중요한 비밀정보가 있을 수 있다. 이러한 기업비밀정보는 기업 입장에서는 당연히 매우 중요하게 관리되고 보호되어야 할 데이터로써, 취급상 각별한 주의가 요구된다[8].

두 번째로, 개인정보에 대한 보호가 필요하다. 개인정보보호의 중요성은 어느 누구도 부정하지 않을 만큼 폭넓은 공감대를 얻고 있으며, 기업은 고객의 개인정보를 외부에 노출하지 않아야 할 의무가 있다. 이러한 개인정보는 기업비밀정보와 함께 매우 중요한 정보이며, 개인정보가 유출될 경우 기업 자체의 신뢰도를 떨어뜨려 막대한 타격을 초래할 수 있다[5,7].

세 번째로, 시스템 그 자체에 대한 정보이다. 이는 시스템 파일, 혹은 시스템 계정정보 등 시스템에 대한 접근 권한을 외부에 넘길 우려가 있는 모든 정보로써, 시스템에 대한 정보가 노출되면 결국 다른 모든 정보가 노출되는 것과 마찬가지라 할 수 있다.

이러한 정보들은 기업 환경에서 반드시 안전하게 지켜야 할 정보들이다. 따라서 본 논문에서는 방화벽 설치, 백신 설치 등의 활동을 통하여 비밀 정보를 안전하게 지키는 활동을 게임화하여 구현하고자 한다.

2.2 게이미피케이션

게이미피케이션은 2010년 1월 미국에서 공식적으로 사용되기 시작하였다. 이는 게임이 아닌 것에 게임적 사고와 게임 기법을 활용해 문제를 해결하고 사용자를 몰입시키는 과정을 뜻한다[1,6,10].

게이미피케이션(Gamification;게임화)이란 용어는 2004년 3월 Nick Pelling에 의하여 컨설턴트 회사를 시작하면서 처음으로 만들어졌다. 그 후 관련 비즈니스에 게임이론에 기반한 게임 설계를 도입하여 관련 기업들의 생산성에 많은 영향을 미치게 되었다.

2.3 놀이 중심의 학습기반 게임

본 절에서는 놀이와 게임에 대한 관계, 에듀게임의 개요, 효과 및 정보보호 에듀게임의 필요성에 대하여 살펴보도록 한다[6,13,11].

2.3.1 놀이와 게임

게임은 일종의 놀이라고 볼 수 있으며, 아이들은 이러한 놀이를 비교적 쉽게 받아들이며 놀이 활동을 통하여 여가시간을 보내는 것을 즐기는 경향이 있다. 놀이에 대한 고찰을 최초로 한 학자는 후이징가(J.Huizinga)이다. 그는 '문화는 놀이 속에서 놀이의 대상으로서 발달한다'라는 명제를 주장하고 놀이하는 사람이라는 호모루덴스라는 개념을 만들었다. 이러한 놀이의 개념을 계승한 카이요와(R.Caillois)는 놀이를 그 본질적인 특징에서 네 가지로 분류했다. 첫 번째는 경쟁, 두 번째는 우연, 세 번째는 모의, 네 번째는 현기증이다. 세부적으로 살펴보자면 경쟁은 여러 퀴즈나 바둑, 운동 경기 등 체력이나 지력을 겨루는 방식이다. 우연은 주사위, 제비뽑기 등 운을 겨루는 방식이다. 모의는 상상을 통해 자기 자신이 아닌 다른 것이 되어보는 것을 뜻하며 마지막으로 현기증은 그네나 놀이기구처럼 현기증 등을 동원하여 현실에서 이탈하는 것을 뜻한다. 게임은 이러한 카이요와가 정의한 네 가지 놀이가 응축된 형태라고 할 수 있다. 아이들이 게임에 열중하게 되는 것은 게임에 여러 가지 경쟁과 현실에서 벗어날 수 있는 상황들을 제시하기 때문이다[13,14].

2.3.2 에듀게임의 교육적 효과

에듀게임은 본 논문에서 주요 대상으로 하고 있는 초등학교 학생 계층에게 흥미를 유발하기에 좋은 학습도구이다. 백영균은 학습용 게임은 다음과 같은 다섯가지에 대하여 긍정적인 효과를 보인다. 첫째, 학습 동기와 관심을 고조시키는 효과가 있으며, 둘째, 게임이 인지적인 학습을 촉진시킨다. 셋째, 게임을 경험 한 후 특성을 변화시킬 수 있다. 넷째, 게임은 주체에 대한 감정이입이나 타인의 가치관에 대한 이해 등의 정서적 학습을 촉진시킨다. 다섯째, 게임은 자아 개념 형성에 긍정적으로 기여한다고 밝히고 있다[6]. 오경진은 창의성 계발을 위한 게임 중심 웹 기반 학습 시스템의 활용이 아동의 창의성을 신장시키며, 이러한 부분은 아동의 인지 발달에 영향을 미친다고 밝히고 있다[10]. 신상우는 컴퓨터 게임은 아동들의 집중력 향상과 기분전환 및 스트레스 해소에 긍정적인 영향을 미친다고 밝히고 있다[14].

2.3.3 에듀게임의 개발 전략

에듀게임을 개발하기에 앞서, 개발 전략이 필요하다. 백영균은 학습용 에듀게임의 설계 단계를 그림 1과 같이 제시하고 있다[11]. 게임 개발에 앞서, 우선 사전 기획이 필요하고, 이러한 기획안에 따라 세

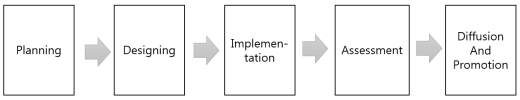

Fig. 1. Edugame Development Strategy

부 제품에 대한 설계가 필요하다. 설계가 완료되면 해당 프로그램을 구현하는 절차가 필요하고, 이후 구현한 프로그램에 대하여 평가 과정을 거친 후 보급 및 홍보 단계에 들어가는 것이 일반적인 에듀 게임의 설계 단계이다.

2.4 정보보호 에듀게임의 필요성

정보보호 분야의 특성상, 초등학생 아이들은 정보보호에 대한 전문지식을 쉽게 깨우치기 어려우며, 이러한 특성에 따라 해당 직무가 어떤 역할을 하는지, 자신의 진로에 적절한지를 구체적으로 판단하기 매우 어렵다고 볼 수 있다. 정보보호 에듀게임은 이러한 부분에 대한 보완책이 될 수 있다. 초등학교 학생들이 게임을 통하여 정보보호 관리자 혹은 전문가가 어떤 역할을 하는지를 기술적으로 깨닫는 것이 아니라 놀이를 통하여 자연스레 체득할수 있다는 점에서 기대효과는 매우 크다. 특히, 이러한 정보보호 에듀게임을 통하여 초등학생들이 정보보호에 대한 과정을 간접 체험함으로써, 향후 자신의 진로 결정에 도움을 받을 수 있을 것이다.

III. 제안된 초등 정보보호 교재 및 교구 개발

3.1 제안된 학습교구와 타 교구와의 차이점

본 논문에서 제안하는 학습교구와 동일한 규칙을 사용하지는 않지만 각각의 활동지를 보여주지 않는 상태에서 게임을 하는 유사한 보드게임으로서 빙고게임과 배틀쉽 게임이 있다. 상기 빙고게임은 잘 알다시피 임의로 부른 숫자를 활동지에 기재하여 연속적으로 1줄이 이루어지면 승리하는 게임이고, 배틀쉽 게임은 수비측 활동판의 다양한 교차점에 걸쳐 항공모함과 군함 및 비행기 등을 배치하고 상대방이 공격측 활동판의 교차점에 폭탄을 배치함으로써, 폭탄에 해당하는 공격측 활동판의 교차점과 상기 항공모함 등이 배치된 여러 개의 수비측 활동판의 교차점이 일치하면 항공모함 등이 격침되도록 하는 게임이다[4,6,11]. 빙고게임의 경우 수비(번호의 배치)가 무작위적인 성격이 강하여 수비자의 의도가 게임 중에 반영되기 어렵고, 게임종료 후 공격자의 공격순서나 공격패턴을 파악하기 힘들며, 수비측이 번호를 배치하고 나면 공격측의 공격에 대해 대처방법이 없는 수동적인 게임이고, 더욱이 빙고게임의 경우는 공격측의 공격에 연결성이 없이 이루어진다는 차이가 있다. 또한, 배틀쉽 게임은 단순히 폭탄을 수비측 활동판의 교차점에 배치하여 항공모함 등이 배치된 상대방 공격측 활동판의 교차점과 일치하도록 하기만 하는 것을 목표로 하는 게임이므로 차이가 있다.

이러한 빙고게임과 배틀쉽 게임을 비롯하여 종래에는 일반적인 학습용 게임교구에 대한 일부 선행문헌들이 존재하나, 정보통신의 기술이 계속해서 비약적으로 발달하고 있는 오늘날 정보보안 및 해커와 관련되어 누구라도 쉽게 정보보안과 해커에 이해를 쉽게 할 수 있도록 한 학습교구는 그 사례를 찾아보기 힘들다.

3.2 제안된 학습교구의 특징

본 논문에서 제안하는 정보보안 학습교구는 위의 타 유사한 학습교구 및 게임의 여러 문제점을 개선하기 위해 제안되었다. 이는 초등학교 저학년을 대상으로 정보보안 전문가의 직업진로를 간접체험 할 수 있는 학습교구이며, 구체적으로는 보호수단과 방어수단을 표시할 수 있는 수비용 모의해킹 활동지, 그리고 공격수단과 해킹수단을 표시할 수 있는 공격용 모의해킹 활동수단을 이용하여, 해킹과 방어의 개념을 각 활동지를 통한 공격과 수비에 의해 습득할 수 있다.

즉, 제안하는 정보보안 학습교구는 여러 기능적인 규칙을 통하여 정보보안의 개념 이해 및 해커의 활동을 이해할 수 있도록 하는데 목적이 있다.

3.3 제안된 학습교구의 주요 기능 및 방법

제안된 학습교구의 특징적인 기능을 살펴보면 다음과 같다. 본 논문의 셀 기반 해커추적 기능을 이용한 정보보안 학습교구의 구성은 한쪽에서 다른 쪽을 향해 일련의 숫자가 차례로 기재된 문자 셀이 구획되어 격자형상을 이루며, 보호수단 또는 방어수단을 상기 문자 셀에 표시한다. 또한, 방어수단은 보호수단에 인접한 문자 셀에 표시하는 수비용 모의해킹 활동지, 상기 수비용 모의해킹 활동지와 반대로 다른 쪽에서 한쪽을 향해 일련의 숫자가 차례로 기재된 문자

셀이 구획되어 격자형상을 이룬다. 본 논문의 학습교구 사용방법은 공격수단 또는 해킹수단을 문자 셀 중의 정해진 문자 셀 범위 내의 어느 하나의 문자 셀에서부터 표시를 시작하여 공격하는 공격용 모의해킹 활동지를 포함하여, 수비측과 공격측이 서로 각 활동지를 못 본 상태에서, 공격에 의해 계속해서 표시하는 문자 셀에 보호수단이 표시된 문자 셀과 일치하면 수비용 모의해킹 활동지를 공격측에 보여주고, 수비측은 활동지를 보여주기 전에 공격수단이 표시되는 문자 셀과 일치하는 방어수단의 문자 셀 표시에 의해 수비를 하거나, 공격측은 방어수단이 표시되는 문자 셀과 일치하는 해킹수단의 문자 셀 표시에 의해 수비를 무력화시키는 것이다.

위의 공격용 모의해킹 활동지에 의한 공격측의 공격은 마지막 문자 셀의 표시에서 근접한 문자 셀의 표시에 의해서만 이루어진다. 또 위의 그림에서 보호수단, 방어수단, 해킹수단은 수비용 모의해킹 활동지의 각 문자 셀에 붙여 표시하는 스티커이고, 공격수단은 공격용 모의해킹 활동지의 각 문자 셀에 표시하는 기호이고, 보호수단은 시스템 파일, 개인정보, 기업비밀 스티커이고, 상기 스티커는 수비용 모의해킹 활동지의 서로 인접하는 숫자 셀에 붙여 표시하지 않도록 한다. 방어수단은 방화벽 또는 백신 스티커로 방화벽 스티커를 수비용 모의해킹 활동지에 미리 붙여 표시해 놓고, 백신 스티커를 공격 측의 공격상황에 따라 붙여 표시하고, 해킹수단은 공격용 모의해킹 활동지에 붙여 표시하는 해킹 툴 스티커이고, 공격수단이 표시되는 공격용 모의해킹 활동지의 문자 셀에 일치하는 수비용 모의해킹 활동지에 방화벽 스티커가 붙어 있으면, 이를 공격측에 알려주어 해킹 툴 스티커를 붙여 표시하는 것을 선택할 수 있도록 한다. 또 해킹 툴 스티커가 붙어 표시된 문자 셀과 일치하는 수비용 모의해킹 활동지에 백신 스티커를 붙여 표시함으로써 수비를 하되, 백신 스티커가 붙여 표시되는 문자 셀에는 더 이상 공격수단을 표시할 수 없도록 한다.

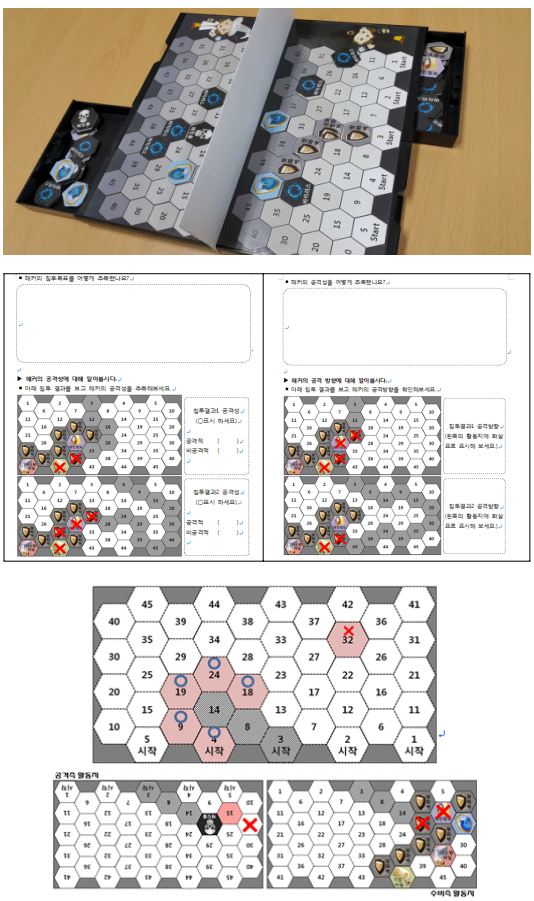

Fig. 2. Teaching tool and education sheet

IV. 초등 정보보호 학습게임의 설계 및 구현

본 장에서는 정보보호 에듀게임을 설계한다. 이에 앞서, 게임 대상, 절차 등을 먼저 살펴보도록 한다.

4.1 게임 대상

본 게임은 초등학생을 기준으로 고려하고 설계되었으며, 그 중에서 특히 초등학교 3~6학년 학생들을 대상으로 한다. 초등학교 교과 학습 과정을 고려했을 때 해당 연령대가 가장 효과적으로 본 게임을 이해하고 받아들이기에 적합할 것으로 보인다.

4.2 게임 진행 절차

4.2.1 플레이어 역할

게임의 시작에 앞서, 플레이어는 공격자 또는 수비자 둘 중 하나의 역할로 정해서 시작하게 된다. 간단히 말하자면, 공격자는 해킹을 시도하려는 측이며, 수비자는 보안 담당자 역할로서 회사의 기밀정보, 시스템 주요 정보, 개인정보를 공격자로부터 방어하는 임무를 가지고 있다. 본 게임은 두명이 진행하는 것이며, 쌍방 사전 합의하에 둘 중 한명은 공격자, 나머지 한명은 수비자가 되어 진행하도록 한다.

4.2.2 도구 설명

게임은 도구를 사용함으로써 진행되며, 공격자, 수비자별로 각각 다른 도구를 사용하게 된다. 즉, 플레이어는 자신이 역할에 따라 할당된 도구에 한해서 사용이 가능하다. 공격자는 해킹툴을 사용할 수 있다. 해킹툴은 일반적으로 통용되는 해킹프로그램을 의미하며, 게임 진행 도중에 방화벽을 만나면 해킹툴로서 공격이 가능하다. 수비자는 방화벽, 백신을 각각 사용할 수 있다. 방화벽은 최대 7개까지 설치가 가능하며, 해킹을 막기 위한 도구로써 설치하게 되나, 해킹툴의 공격이 1회 들어오면 파괴되어 없어지게 된다. 또한, 해킹툴의 공격이 들어올 경우 백신을 사용하여 막을 수 있으며, 백신으로 한번 막은 셀은 공격자가 다시 공격할 수 없다.

4.2.3 게임 시나리오

게임 절차는 다음과 같다. 먼저, 수비측에서 주요 비밀정보 파일 3개를 각각 배치한다. 여기에서, 3개의 비밀정보는 각각 시스템 파일, 개인정보, 기업비밀로 한다. 배치에 앞선 전제조건으로, 이 3개의 비밀정보는 인접한 셀에 배치될 수 없다. 비밀정보의 배치가 완료된 이후, 수비측은 7개의 방화벽을 설치한다. 이러한 방화벽은 수비측에서 자유롭게 배치 가능하다. 이러한 과정이 끝나면 수비자측에서 행하는 초기 단계는 완료된 것이며, 이후 공격자의 해킹 활동이 시작된다. 공격자는 시작점으로부터 인접한 셀만을 이동해 다닐 수 있다. 이동시 공격자는 시스템 파일, 개인정보, 기업비밀, 방화벽 등 수비자가 배치한 위치를 알지 못한다. 따라서, 공격자는 해당 타켓을 찾을 때까지 계속하여 이동하게 된다. 셀의 이동시 마다 해당 부분이 방화벽이 존재하는 위치인지를 확인하면서 이동하게 된다. 만약, 방화벽을 발견하게 될 경우 해킹툴을 사용하여 파괴할 수 있다. 하지만 해킹툴은 분량의 제한이 있어, 무한히 사용할 수는 없다.

그림 3에서는 3개의 기밀정보와 7개의 방화벽을 설치한 모습을 나타낸다. 각 셀은 육면체로 되어 있으며, 이러한 벌집 모양의 구성은 공간의 낭비를 최소화 시키는 특징이 있다. 또한, 타 셀과 인접한 면이 여섯 개가 되므로, 정사면체로 구성했을 때 보다 더욱 다양한 방식으로 이동이 가능하여 플레이어에게 더욱 많은 자유도를 부여한다.

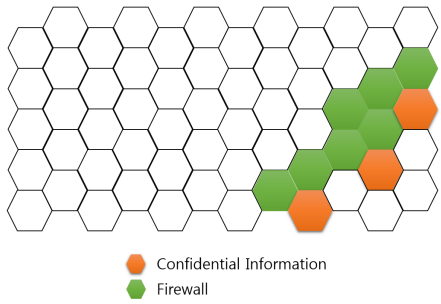

Fig. 3. Placement of Confidential Information and Firewall

4.3 게임 설계

4.3.1 알고리즘 설계

알고리즘은 공격자와 수비자의 관점에서 각각 구분하여 생각하여야 한다. 게임의 시작은 수비자가 우선이며, 수비자가 기밀정보와 방화벽 배치를 마친 이후에 공격자의 공격이 시작된다. 그림 4는 수비자측의 알고리즘을 나타낸다.

프로그램이 시작되면, 수비자는 기밀 데이터를 배치한다. 기밀데이터는 시스템 파일, 개인정보, 기업비밀정보로써 세가지가 존재하며, 수비자가 원하는 적재적소에 배치한다. 기밀데이터의 배치가 끝난 이후 7개의 방화벽을 적절한 곳에 배치한다. 이러한 과정이 끝나면, 수비자는 대기 모드 상태에서 공격자의 공격이 들어오기를 기다린다. 기밀정보 및 방화벽에 해당되지 않는 셀에 공격자가 위치할 경우는 별도로 처리할 필요가 없이 대기상태이며, 만약 방화벽에 공격자가 들어온 것이 감지되었을 경우는 백신을 설치할지에 대한 의사결정을 한다. 만약, 백신을 설치

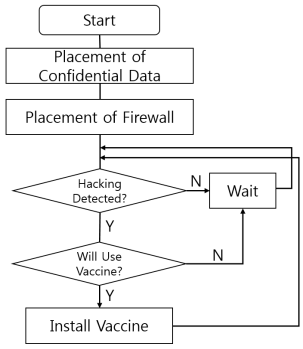

Fig. 4. Defender Side Algorithm

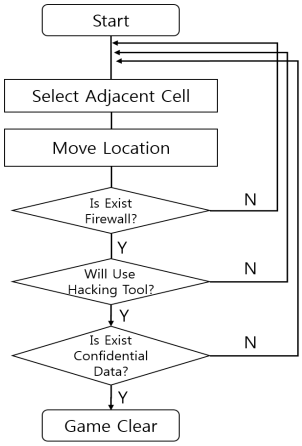

Fig. 5. Attacker Side Algorithm

할 경우 공격은 방어되며, 해당 셀에 대해서는 다시는 공격자는 공격할 수 없다. 그러나 백신은 총2회 사용이 가능하므로, 백신을 반드시 사용할지는 수비자가 선택하여 결정하여야 한다.

그림 5는 공격자 측의 알고리즘을 나타낸다. 공격자 측의 시작은 수비자 측에서 비밀정보와 방화벽에 대한 배치가 완료된 시점 이후라는 것을 가정하며, 그 이전에는 공격할 수 없다. 공격이 시작되면 공격자는 현재 위치하고 있는 셀에서 바로 인접한 셀에 대하여 이동이 가능하며, 공격자는 어느 셀로 이동할지를 결정한다. 결정이 끝나면 해당 셀로 이동하고, 방화벽의 존재 여부를 확인한다. 방화벽이 존재할 경우는 해킹툴을 사용하여 방화벽을 파괴할 것인지를 결정한다. 해킹툴을 사용하면 방화벽에 대한 파괴가 가능하며, 만약 방화벽 인접한 곳에 비밀정보가 존재한다면 이러한 비밀정보를 획득할 수 있을 것이다. 선택된 셀에 방화벽이 없을 경우는 다시 다른 셀로 이동하여 같은 과정을 반복한다.

4.3.2 전체 시스템 구성

시스템 구성은 클라이언트-서버 구조로 구성된다. 공격자와 수비자는 각각 다른 클라이언트를 사용하며, 이들 사이의 데이터 처리는 서버에서 중재한다. 클라이언트와 서버간의 통신은 XML 메시지로 교환된다.

4.3.3 프로그램 모듈 구성

프로그램 모듈은 그림 7과 같이 구성되어 있다.

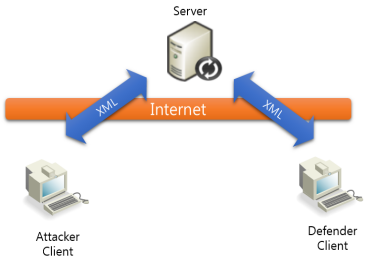

Fig. 6. System Component

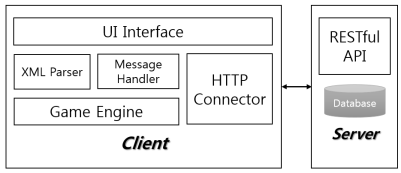

Fig. 7. Module Diagram

우선, 클라이언트에는 사용자에게 화면이 보여질 수 있도록 UI 인터페이스가 존재하며, 클라이언트와 서버간의 통신을 담당하는 HTTP Connector가 있다. 한편, XML 및 가공된 데이터의 처리는 Message Handler에서 담당하며, 게임 자체의 로직은 Game Engine상에 구현되어 있다. 서버측에서는 클라이언트와의 통신을 위한 RESTful API가 구성되어 있으며, 클라이언트와 서버는 HTTP상에서 게임 데이터를 주고받게 된다. 클라이언트로부터 서버가 수신한 게임 데이터는 서버상의 데이터베이스에 저장되어 관리되며, 공격자/수비자 양측 클라이언트간 화면에 나타나는 데이터는 서버상의 데이터베이스의 데이터를 기준으로 처리된다.

4.3.4 메시지 흐름

클라이언트와 서버간의 메시지 흐름은 그림 8과 같다. 우선, 수비자 측의 클라이언트 및 공격자 측의 클라이언트가 로그인을 하면 서버는 세션 아이디 ID_S를 생성하여 전달한다. 해당 세션 아이디는 한번의 게임당 일회성으로 사용되는 아이디이며, 게임이 종료되면 세션아이디는 삭제된다. 이후 수비자 측에서 비밀정보와 방화벽에 대한 배치를 완료하면 해당 데이터는 XML 데이터로 변환되어 서버측에 송신되며, 서버는 해당 데이터를 데이터베이스에 저장한다. 이후, 공격자는 특정 셀에 대하여 공격을 시도할수 있게 된다. 셀이 위치하는 특정 좌표를 기준으로 서

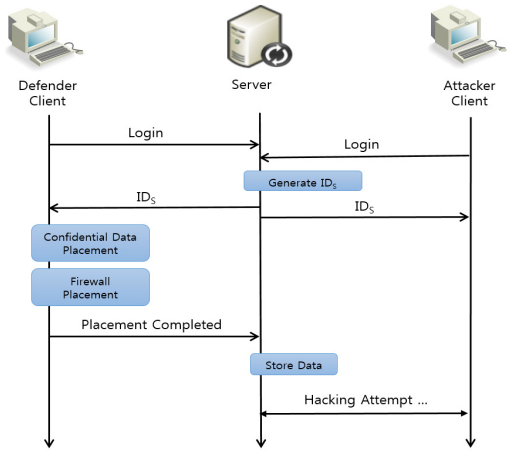

Fig. 8. Sequence Diagram

버에게 확인 요청을 하면, 서버측에서는 해당 셀에 방화벽이 있는지 여부를 공격자에게 개별적으로 응답하게 된다. 셀 상에 방화벽이나 비밀정보가 존재하지 않는 경우 공격자는 다시 반복적으로 다른 셀로 위치를 변경하여 방화벽/비밀정보 존재 유무를 확인한다.

그림 9는 공격자 클라이언트측에서 서버측에 송신한 XML 요청 문서를 나타낸다. 특정 좌표에 대한 위치변경 요청을 하면, 서버에서는 해당 위치에 방화벽의 존재 여부를 리턴한다.

```
▼<Request>
    <userID>testAttacker</userID>
    <sessionID>0b9b2712160f17bb755f44910e5691892f4df74e</sessionID>
    <role>Attacker</role>
    <act>Change_Location</act>
  ▼<coordinate>
      <x>7</x>
      <y>12</y>
    </coordinate>
</Request>
```

Fig. 9. XML Request Document

4.4 개발 구현환경

표 1에서 보는 것과 같이 본 게임의 개발은 특별한 고성능의 PC가 아닌 일반적인 보급형 PC에서 진행되었다. 사실상 본 논문에서 설명한 게임의 구현에 있어서 비교적 복잡하지 않은 알고리즘으로 구성되었고, 필요로 하는 데이터의 양도 크지 않기 때문에 특별한 고사양의 PC가 필요하지는 않다고 볼 수 있다.

Table. 1. Development Environment

H/W	CPU	Intel i5-3470 @3.2GHZ
	RAM	4GB
	VGA	Intel HD Graphics
S/W	O/S	Windows 7
	Language	C#

4.5 구현 내용

그림 10은 구현된 학습교구 프로그램을 나타낸다. 사용자가 마우스 등을 통하여 육각형 셀 상의 인접 위치로 움직일 수 있고, 그에 따라 해당 셀에 방화벽이 존재하는지 여부가 출력된다. 사용자가 이동한 내역은 우측에 기록되어 게임 진행 과정에서 어떻게 이동하였는지를 편리하게 확인이 가능하다.

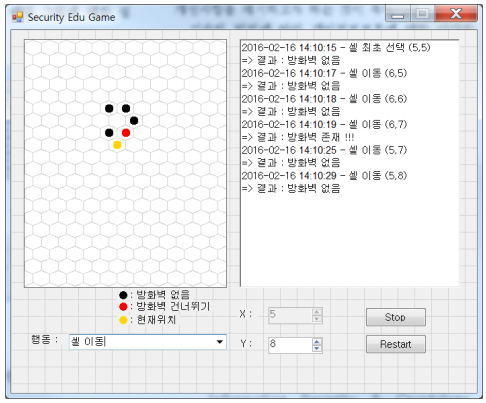

Fig. 10. Main Screen of Edugame

V. 현장 시범적용 결과 및 효과성분석

5.1 현장 시범학교 적용 결과

본 교구를 현장 적용한 학생들의 주요 활동내용은 그림 11과 같다.

개발된 교재와 수업의 효과성을 검증하기 위하여 제주동초등학교 학생을 대상으로 각각의 수업을 진행하였다. 사전설문조사를 통해서 정보보호관련 직업 호감도에 대한 학생들의 인식을 조사하였고, 교육 후에 사후설문조사를 통해서 어떠한 변화가 있는지 확인하였다.

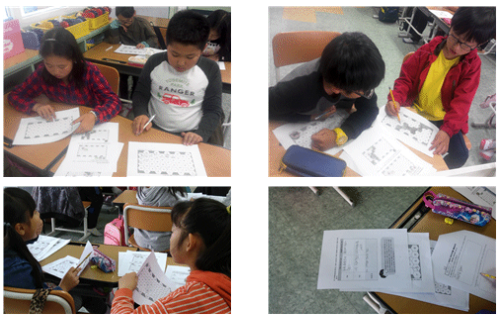

Fig. 11. Photo and Result of Real Tesetbed

5.2 수업에 참여한 학생들 대상 설문조사 분석

설문지는 5점 만점의 리커트(Likert) 척도로 구성한 문항 5개와 서술형 문항 5개로 이루어져 있으며, 적용 결과는 표 2 및 그림 12와 같다.

수업과 교재 관련 난이도는 평균 4.21으로 적절하다는 응답을 보였고, 제시된 단어와 문장의 수준도 4.21으로 적절하다는 응답을 보였다. 교재 및 수업에 대한 흥미도는 평균 4.71으로 교재 및 수업에 대한 흥미와 만족도가 매우 높게 나타났다. 향후 학습에 대한 태도는 4.61으로 향후 융합 교육과정에 대한 학습의지가 높은 것으로 확인되었고, 타 교과학습 연계효과 정도도 4.41으로 효과가 높다는 응답을 보였다.

그림 13의 그래프는 본 학습교구를 이용한 시범수업을 받은 학생들(초등학교 3-4학년과 5-6학년 학생)을 대상으로 한 교육프로그램에 따른 진로 및 관련 학문 인식의 변화를 살펴보기 위하여 구성하였다. 관련 직업에 관한 호감도는 3-4학년의 경우 교육프로그램 적용 전과 적용 후에 큰 차이가 있었다. 즉 교육프로그램을 통해 관련 직업에 대한 학생의 관심과 흥미가 증가하였다는 것을 알 수 있다. 5-6학년은 소폭의 증가가 있었으나 유의미한 차이는 발견할 수 없었다.

Table 2. Application Result of Education Program

Subject	Frequency (Person)	Average	Standard Deviation
Level of difficulty of the class and learning materials	100	4.21	.76
Level of words and sentences used	100	4.21	.76
Interest in and satisfaction with learning materials and the class	100	4.71	.49
Preference to learning through the program in the future	100	4.61	.67
Degree of program's effect in connection with other school subjects	100	4.41	.67

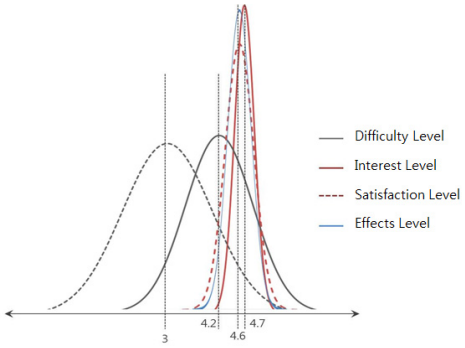

Fig. 12. Result of applied Education Program

서술형 문항에서도 실생활과 IT 신기술, 융합형 교육이 통합적으로 적용된 교육프로그램에 대해서 긍정적인 응답이 많았고, 차시 중에서는 전개 부분의 로봇 조립 및 활용내용이 가장 만족도가 높았다. 서술형 문항의 결과는 다음과 같다.

- 모든 활동이 좋았다. 완전 재미있다.
- 다음에 기회가 있으면 꼭 하겠다.
- 재미있고 다음에 또 하고 싶다.
- 아주 좋았다. 정보보호에 대해서 더 알고 싶다.
- 재미있는 만들기가 더 추가되면 좋겠다.

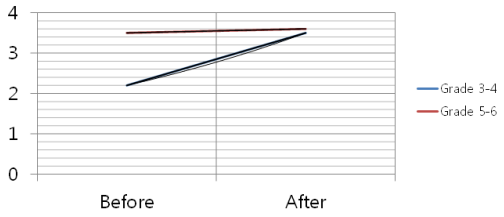

Fig. 13. Desirability Change

5.3 시범학교 적용 결과 수업에 참여한 교사들 대상 설문조사 분석

본 연구에서는 개발한 교재와 교육프로그램을 현직 초등학교 교사에게 분석을 의뢰하고 설문조사지를 통해 교재와 교육과정의 적절성에 대해 분석하였다. 교재와 교육프로그램에 대한 교사의 설문조사 결과는

다음과 같다.

- 정보보호 개념으로 쉽게 이해할 수 있게 초등학생용 교재가 구성되었고 학습활동이 이루어졌다.
- 시간이 더 주어진다면 정보보호의 다양한 기능적 교육과 원리의 형태를 추가해도 좋을 것 같다.
- 새로운 ICT 주제의 초등학생 전문교육의 흐름을 알 수 있는 기회를 마련해준다.
- 초등학생들이 쉬운 학습을 활용해 보안의 핵심 원리를 스스로 학습함으로써 정보보호교육을 실천하는 자세를 더욱 형성시켜줄 수 있다.
- 네트워크 보안의 원리를 스스로 공부하는 직접 학습하는 활동을 통하여 학생들이 즐겁고, 창의적인 활동을 할 수 있다.

많은 현장 교사들이 교재의 적절성에 대해 긍정적인 답변을 하였다. 학생이 이해하기 쉽게 구성되었다는 응답이 많았으며, 스스로 학습이 가능하도록 구성된 부분에 대한 긍정적 답변도 많았다. 학습활동이 학생들이 좋아하는 활동으로 구성되어 학습이 효과적으로 이루어졌다는 참관교사도 있었다. 다만 공학적 알고리즘 내용이 많아서 흥미도를 떨어뜨릴 수 있다는 지적과 더욱 다양한 금융공학의 학습사례를 추가하면 더 좋을 것 같다는 지적도 있었다.

VI. 결 론

최근 들어 정보보호에 대한 중요성은 크게 부각되고 있다. 이러한 상황에 맞물려 정보보호에 대한 시장도 증가하고 있는 상황이다. 그러나, 국내에서는 아직 정보보호 에듀게임 시장은 넓지 않은 편이다. 초등학생의 정보보호 인식 제고를 위해서는 정보보호 에듀게임의 활성화가 필요하다. 따라서, 본 논문에서는 정보보호 에듀게임을 설계 및 구현하였다. 본 논문의 셀 기반 해커추적 기능을 이용한 정보보안 학습교구는, 해커의 활동과 관련된 정보보안의 개념을 쉽게 게임방식으로 이해할 수 있으므로 초중고의 학생들이 향후 직업을 선택하기 전에 정보보안 전문가의 직업진로를 체험할 수 있는 효과가 있다. 문자 셀 기반의 공격과 방어 기능을 이용하여 여러 상황에서의 결과들을 분석하고 학습할 수 있고, 게임 놀이방식을 통한 정보보안 및 해커의 기능 원리를 보다 쉽고 재미있게 학생들에게 학습시킴과 더불어 정보보안의 중요성을 인식시킬 수 있는 효과가 있다. 또한 여러 가지 정보보호 핵심 기능 및 학습 소양 능력을 분석하고 학습할 수 있고, 실험자가 계속 관찰하지 않아도 해당 결과값들을 축적하여 재활용할 수 있는 효과도 있다. 이러한 정보보호 에듀게임은 일반적인 여가의 목적 뿐 아니라 정보보호의 학습 도구로서도 활용될 수 있고, 초등학생의 정보보호 직종 분야의 간접체험에 도움이 될 것으로 보여진다. 향후 연구방향으로, 본 논문의 결과를 통하여 실제로 초등학생의 정보보호 인식 제고 및 만족도여부에 대한 실증적 분석이 필요하다.

References

[1] KERIS, "The Effectiveness Analysis of U-Learning," CR-2006-26, Korea Education and Research Information Service, 2006.

[2] Min-Jeong Kim, Haeni Lee, Shin-Jeong Song, Jinho Yoo, "A Study on the Curriculum of Department of Information Security in Domestic Universities and Graduate Schools and Comparison with the Needs of Industry Knowledge," Journal of The Korea Institute of Information Security & Cryptology, 24(1), pp.195-205, Feb. 2014.

[3] Seong-Yong Park, "Meaning of The Legislation on Building and Promoting The Use of Smart Grid," Journal of Electrical world Monthly magazine, 414, pp.52-54, Jun. 2011.

[4] Computing at School Working Group, "Computer Science: A Curriculum for Schools," Computing At School, 2012

[5] Namje Park, Marie Kim, "Implementation of Load Management Application System using Smart Grid Privacy Policy in Energy Management Service Environment," Cluster Computing, vol. 17, no. 3, pp. 653-664, Sep. 2014

[6] Inkee Jeong, "A Study on Curriculum for Problem Solving Field in the Computer Science of Elementary School," The Journal of Korean Association of

Computer Education, 10(2), pp. 17-26, Mar. 2007
〔7〕 Namje Park, "User Privacy Preserving Mobile RFID Personal Information Security Service System," Journal of Korean Institute of Information Technology, 8(10), pp.87-96, Oct. 2010
〔8〕 Jisup Kwak, Wanhong Kim, Soonhee Kang, Jaesung Kim, "Current Security Issues on Smart Grid and Cyber Security Strategy in Korea," Proceedings of The Korean Institute of Electrical Engineers, pp. 1209-1210, Jul. 2010.
〔9〕 Min-cheol Jeon, Sin-Kyu Kim, "A Research on the Possibility of Employing Existing Security Compliance Enforcement System for the Smart Grid," Journal of The Korea Information Science Socity, 32(9), pp. 55-59, Sep. 2014.
〔10〕 Yeonghae Ko, Jaeho Ahn, Namje Park, "Elementary school computer education with the focus on case study bases on fractal geometry theory using LOGO programming language," The Journal of Korea Institute of Information Technology, 9(8), pp. 151-163, Aug. 2011.
〔11〕 Young Kyun Baek, "A Study on Pre-conditions to Introduce GBL into the Classroom," Communications of the KIISE, 24(2), pp. 45-5, Feb. 2006.
〔12〕 Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, Howon Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment," Advanced Web and Network Technologies, and Applications, LNCS 3842, pp. 741-748, 2006.
〔13〕 Yeonghae Ko, Namje Park, "A Study of IT Centered Smart Grid's STEAM Curriculum and Class for 3rd and 4th Graders in Elementary School," Journal of Korea Association of Information Education, 17(2), pp.167-175, Jun. 2013.
〔14〕 Yilip Kim, Namje Park, "The Effect of STEAM Education on Elementary School Student's Creativity Improvement", Communications in Computer and Information Science, Vol.339, pp.115-121, Nov. 2012.

〈저자소개〉

이 동 혁 (Donghyeok Lee) 정회원
2007년 2월: 동국대학교 전자상거래기술전공 공학석사
2007년 6월~2008년 5월: 한국전자통신연구원 정보보호연구단 연구원
2008년 11월~2015년 6월: KT 플랫폼개발단 과장
2015년 9월~현재: 제주대학교 컴퓨터교육전공 박사과정
〈관심분야〉 클라우드 보안, 스마트그리드 보안, 데이터베이스 보안

박 남 제 (Namje Park) 종신회원
2008년 2월: 성균관대학교 컴퓨터공학과 박사
2003년 4월~2008년 12월: 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월~2009년 12월: 미국 UCLA대학교 공과대학 Post-Doc,WINMEC연구센터 Staff Researcher
2010년 1월~2010년 8월: 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년 9월~현재: 제주대학교 교육대학 초등컴퓨터교육전공 교수
〈관심분야〉 컴퓨터교육, 융합기술보안, 스마트그리드, IoT, 해사클라우드 등