국내 온라인게임 보안 서비스 현황

Status quo of online game security services in South Korea

김은아(삼성전자), 김휘강(고려대학교)

차 례

■ Keyword : Online Game Security | Security services | Status quo

1. 서론

온라인 게임은 월드 와이드 웹(World Wide Web)과 더불어 가장 성공한 인터넷 서비스 중에 하나이다. 글로벌 게임 업체 Spil Games의 보고서에 의하면, 2013년 기준 세계적으로 12억 명 이상의 게임 이용자 중에서 약 7억 명이 온라인 게임을 하는 것으로 나타났다. 이는 당시 전 세계 온라인 인구의 44%에 해당한다[1]. 글로벌 통계 업체 Statista는 2018년 전 세계 온라인 게임 트래픽이 월 2,857 페타바이트(petabyte)에 달할 것으로 예측하였다[2]. 산업 측면에서 게임은 고수익 고부가가치 산업으로, 2017년 전 세계 게임 시장은 약 786억 1천만 달러로 평가되었다. 2016년 기준 한국은 중국, 미국, 일본, 독일, 영국에 이어 세계 6위의 게임 수익 국가로 약 41억 9천만 달러의 매출 규모를 기록하였다[3].

온라인 게임 이용자가 증가하고 시장 규모가 커짐에 따라, 온라인 게임을 대상으로 하는 보안 위협이 증가하고 있다. 특히 온라인 게임 이용자의 개인정보 유출과 게임 서비스에 대한 부정행위는 게임 이용자와 게임사 모두에게 금전적 피해를 입힐 수 있는 심각한 문제이다. 국내 게임 이용자의 계정 정보 유출을 목적으로 하는 중국발 해킹이 2005년부터 발견되었고, 현재까지 끊임없이 개인정보 유출 사고가 발생하고 있다. 계정 정보 유출로 인한 개인정보 유출은 불법적으로 온라인 게임이나 인터넷 서비스를 이용하기 위한 명의도용으로 이어질 수 있으므로 위험성이 크다. 또한, 게임봇이나 게임핵을 이용한 게임 상의 부정행위, 작업장이나 사설서버 운영, 게임 서버나 네트워크 해킹 등도 최종적으로 금전적 이득이 목적인 경우가 대부분이므로, 게임사들은 이에 대한 다양한 대응책들을 시행중이다.

본고에서는 2017년 기준 국내 온라인게임사에서 게임 이용자에게 제공하는 보안 서비스들을 조사하고, 목적과 기능에 따라 분류하여 현황을 파악할 수 있도록 한다. 이를 통하여 온라인게임 보안 서비스를 구축하거나 보완하는데 도움을 줄 것으로 기대한다.

본고의 구성은 다음과 같다. 1장에서 온라인게임의 이용 현황과 산업 규모, 보안 위협 등에 대하여 살펴보았다. 2장에서 온라인게임 보안과 보안서비스 관련 기존 연구를 소개한다. 3장에서는 본 현황 조사의 목적과 조사 범위 및 방법을 밝힌다. 이어 4장에서 국내 온라인게임 보안 서비스들을 목적과 기능에 따라 분류하고, 각 서비스를 소개한다. 5장에서 국내 온라인게임사 별 보안 서비스 제공 현황을 보이고, 6장에서 결론을 맺는다.

2. 관련 연구

온라인게임 보안은 게임 배포사와 개발사의 시스템 및 네트워크 등의 정보자산을 외부의 침입으로부터 보호하는 것이다. 이와 관련하여 온라인게임사는 게임 이용자의 계정과 개인정보, 게임정보 등을 보호하는 다양한 서비스를 제공한다. 본고에서 소개하는 보안 서비스들의

대부분이 이에 속한다. 또한, 온라인게임사는 게임 이용자들이 신뢰할 수 있는 환경에서 게임할 수 있도록 서버 및 시스템, 네트워크, 클라이언트 단에서 보안 기술을 적용하고, 정책과 제도를 마련하기도 한다. 이는 게임봇, 사설서버, 작업장, 서버 우회 접속, 해킹 등의 부정행위를 예방하거나 탐지하고, 차단하거나 제재하는 등의 활동도 포함한다.

온라인게임에서의 보안 위협과 대응 기술에 대한 연구 및 현황 조사는 다양하게 이루어지고 있다. Jiyoung Woo 등은 온라인게임, 특히 MMORPG (Massive Multi-user Online Role Playing Game)와 같이 최근 인기 있는 게임 장르에서 빈번하게 발생하는 부정행위들을 정리하였다. 또한 학계와 게임 산업계에서 연구하고 적용한 대응책들을 조사하였다. 저자는 온라인게임 상의 부정행위를 탐지하고 대응하기 위한 실질적인 방안으로 서버, 네트워크, 클라이언트 단계에서 적용 가능한 기술들을 분류하고, 이에 따라 적용할 것을 제안하였다[4]. 온라인 게임에서의 부정행위와 탐지 및 예방 관련 기존의 연구들을 탐지 단계, 기법, 알고리즘, 탐지에 적용된 데이터, 게임 장르, 탐지 대상 등의 기준에 따라 분류한 연구도 있다. 이 연구에서는 특히, 온라인게임 별 특징이 다름을 지적하고 각 특징에 따른 부정행위 예방 및 탐지 방법을 분류하였다[5].

한국정보보호진흥원(KISA)이 2006년 발간한 온라인게임 해킹 대응 가이드에서 온라인게임 업체의 보안 현황과 공격 피해 현황, 온라인게임 해킹 관련 적용 법률 등을 소개하고 있다. 현황 파악을 위하여 국내에서 온라인게임 서비스를 하는 11개 업체를 대상으로 보안 장비, 보안 인력, 공격 피해 및 해킹 관련 고객 신고 현황 등을 설문조사 하였다. 또한, 온라인게임 서버 운영자 및 보안 담당자가 해킹 및 개인정보 유출을 예방할 수 있도록 네트워크, 서버, 애플리케이션 등의 각 요소에서 안전한 온라인게임 서비스를 제공할 수 있는 방법을 제시하기도 하였다[6]. Mee Lan Han 등은 2014년 기준 국내 온라인게임사가 제공하는 보안 서비스들을 안전한 트랜잭션과 계정 보호, 부가 서비스 등으로 분류하고, 각 서비스를 설명하였다[7].

온라인게임과 함께 보안 서비스가 필수적인 온라인 산업으로 금융을 들 수 있다. 금융 서비스가 온라인과 모바일로 확산됨에 따라 고객과 금융사의 자산을 보호하기 위하여, 금융계는 최신의 보안 기술을 빠르게 적용한다. 금융계에서 적용하는 온라인 보안 서비스들은 온라인게임에서도 적용되는 것이 적지 않다. 이와 관련하여 Gi Seong Lee 등은 2014년 기준 국내 6개 은행에서 제공하는 인터넷뱅킹 보안 서비스들을 조사하고, 인증과 클라이언트 보안 분야로 분류하여 각 서비스를 설명하였다[8].

한편, 국내 온라인게임이나 인터넷뱅킹에서 이용되는 사용자인증 기법 중 대표적인 OTP(One Time Password) 서비스 현황을 소개한 연구도 있다. 저자는 OTP 서비스 소개와 함께 MITM (Man-in-the-Middle) 공격과 역공학을 이용하여 OTP 적용환경의 취약점을 대상으로 하는 공격이 온라인게임과 인터넷뱅킹에서 가능함을 보였다[9]. Changsok Yoo 등의 연구에서는 OTP 시스템에 대한 알려진 공격 방법을 분석하여 새로운 OTP 공격이 가능함을 이론적으로 증명하였다. 또한, 발견한 공격 방법을 국내 인터넷뱅킹 서비스를 대상으로 테스트하여 국내 OTP 보안 시스템을 효과적으로 우회할 수 있음을 증명하고, 해결 방안을 제시하였다[10].

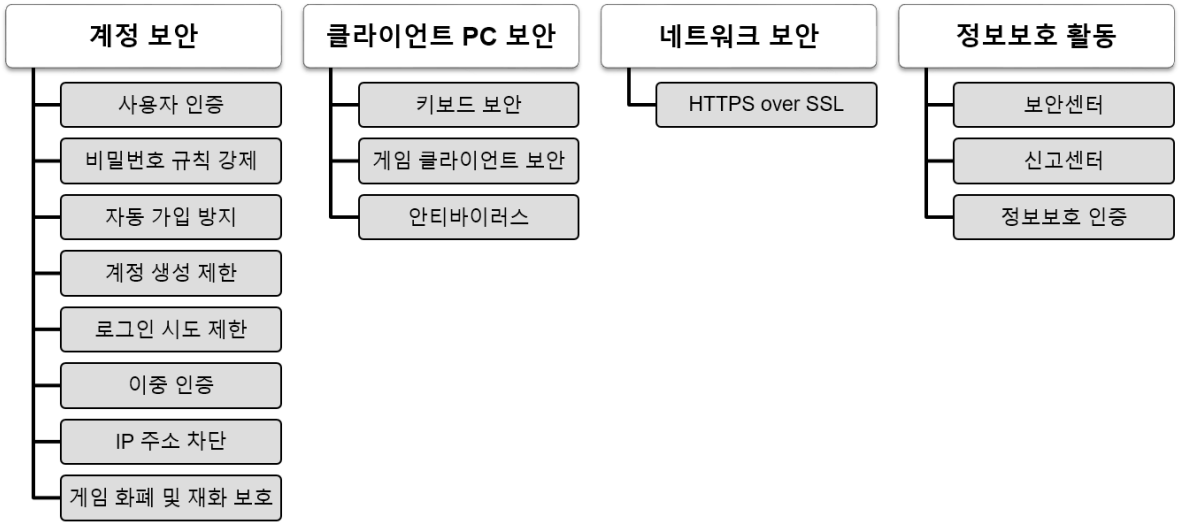
3. 현황 조사 개요

3.1 조사 목적

국내 온라인게임사의 보안 서비스들을 조사하고, 목적과 기능에 따라 분류하여 각 분야 별 제공 현황을 파악할 수 있도록 한다. 또한, 대표적인 국내 온라인게임사 별 보안서비스를 비교한다. 이는 향후 보안서비스 구축이나 보완에 참고가 될 수 있다.

게임 기업	참여지수	미디어지수	소통지수	커뮤니티지수	사회공헌지수	브랜드평판지수
넥슨	719,174	629,395	811,832	879,545	65,677	3,105,622
엔씨소프트	555,456	646,737	275,086	336,624	396,406	2,210,310
넷마블게임즈	615,657	663,182	174,734	200,498	140,736	1,794,807
골프존	195,672	262,522	193,844	131,008	290,854	1,073,900
컴투스	110,855	308,269	198,156	153,612	194,685	965,577
플레이위드	9,342	14,651	71,736	103,511	588,746	787,985
넵튠	40,081	24,219	166,992	502,151	7,037	740,480
웹젠	105,332	181,792	91,238	90,917	129,008	598,287
게임빌	95,469	196,443	95,256	57,758	91,478	536,404
NHN엔터테인먼트	105,726	151,892	81,340	42,084	16,419	397,461
위메이드	83,792	128,869	62,622	46,297		
네오위즈	32,830	125,879	115,836			
	86,632					

▶▶ 그림 1. 국내 게임회사 평판순위 (2017년 6월 1일 기준)[11]



▶▶ 그림 2. 국내 온라인게임 보안 서비스 분류

3.2 조사 범위 및 방법

2017년 6월에 발표된 한국기업평판연구소 국내 게임회사 브랜드평판 기준 상위 5개 온라인게임사를 대상으로 보안 서비스 현황을 조사하되, 모바일 전용 게임사는 제외하였다. 그림 1은 조사 대상 선정의 기준이 되는 국내 게임회사 평판순위를 나타낸다. 최종적으로 넥슨[12], 엔씨소프트[13], 넷마블게임즈[14], 웹젠[15], NHN엔터테인먼트의 한게임[16]이 조사 대상으로 선정되었다.

현황 파악을 위하여 각 게임사의 홈페이지를 통해 공개된 자료를 수집하여 분석하는 방법과 게임사의 홈페이지에서 제공하는 서비스를 직접 테스트 하는 방법을 선택하였다.

4. 국내 온라인게임 보안 서비스

앞서 선정한 온라인게임사들이 자사 게임에 적용하고 있는 보안 서비스들을 보호 대상이나 목적에 따라 크게 네 가지로 분류할 수 있었다. 그림 2와 같이 네 가지 분류는 계정 보안, 클라이언트 PC 보안, 네트워크 보안, 정보보호 활동이다. 분류 결과, 사용자 계정 보안 서비스가 가장 많았고, 계정을 생성하거나 로그인 시점에 주로 적용되었다. 게임 이용자에게 직접적으로 제공하는 보안 서비스는 아니지만, 게임사가 정보보호 관리체계를 수립하고 이행하는지에 대한 공인기관의 인증 또한 간접적으로 게임 이용자에게 보안 서비스를 제공하는 것이므로 정보보호 활동에 포함시켰다.

4.1 계정 보안 (Account Security)

4.1.1 사용자 인증

사용자 인증은 게임 이용자 본인을 확인하여 명의 도용을 방지하는 것이 목적이다. 게임 계정을 생성하거나 개인 정보를 사용하는 서비스를 이용할 때 필수로 인증 과정을 수행하도록 하고, 게임사 마다 평균 두 가지 이상의 인증 수단을 제공하고 있다. 대표적인 사용자 인증 수단으로 전화(유무선, 통신업체), 이메일, 아이핀[17], 소셜네트워크서비스 등이 있다.

- ARS(Automatic Response Service): 사용자 소유의 유선 전화나 휴대폰으로 인증을 위한 전화 통화를 시도하여, 게임 서비스 이용자가 본인임을 확인한다.
- SMS(Short Message Service): 사용자 소유의 휴대폰에 인증 번호 등의 정보를 문자 메시지로 전송하고 이를 확인한다.
- ISP(Internet Service Provider): 휴대폰 가입자 정보를 가지고 있는 ISP에서 사용자 인증 서비스를 제공하여, 게임사가 직접 사용자 인증을 하지 않아도 된다.
- 이메일(E-mail): 사용자 소유의 이메일 계정으로 인증 번호, 인증 링크 등의 정보를 전송하고 수신 여부를 확인한다.
- 아이핀(i-PIN): 국내 본인확인기관(서울신용평가정보 등)에서 발급받은 아이핀 계정과 비밀번호를

이용하여, 인터넷 상에서 주민등록번호를 사용하지 않고 본인 인증을 할 수 있다.

- SNS(Social Network Services): 게임 이용자가 가입되어 있는 인터넷 소셜네트워크 서비스와 연동하여 계정 정보를 게임사로 안전하게 전달한다. 주로 게임 계정을 생성할 때 이용하고, 추가적인 정보 입력을 필요로 한다.

4.1.2 비밀번호 규칙 강제

비밀번호는 게임 이용자의 정보를 수집하여 추측하거나 사전공격으로 알아맞히기 어렵도록 구성되어야 한다. 온라인게임 뿐만 아니라 다양한 인터넷 서비스에서 계정 생성 시 비밀번호를 복잡하게 구성하는 것을 강제하고 있다. 비밀번호 규칙으로 영문, 숫자, 특수문자를 조합하는 것과 일정 길이 이상일 것 등이 있다.

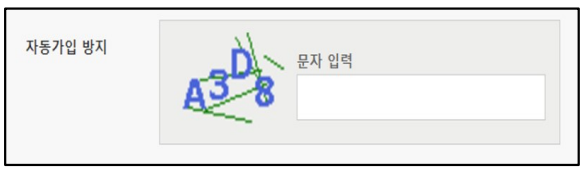
4.1.3 계정 등록 보안

1) 자동 가입 방지

자동화 도구를 이용하여 계정을 생성하는 것을 방지하기 위하여 온라인게임 뿐만 아니라 다양한 인터넷 서비스에서 계정 생성 시 CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)[18]를 사용한다. 그러나, 조사 대상 게임사 중 한 곳만 CAPTCHA를 사용하였다. 그림 3은 넷마블게임즈 계정 생성 단계의 자동가입방지 CAPTCHA이다.

2) 계정 생성 제한

동일한 본인 식별 정보 (이름, 주민등록번호, 전화번호, 주소 등)를 사용하는 계정의 수를 제한하여, 도용된 명의로 다수의 게임 계정을 생성하는 것을 방지한다. 또한, 게임 이용자가 본인의 계정을 생성한 후에 추가 계정을 생성하지 못하도록 설정하는 기능을 제공하는 게임사도 있다. 이러한 설정은 개인 정보를 이용하는 민감한 서비스로, 설정 변경 시 사용자 인증을 수행해야 한다.



▶▶ 그림 3. 자동가입방지 CAPTCHA, 넷마블게임즈

4.1.4 로그인 보안

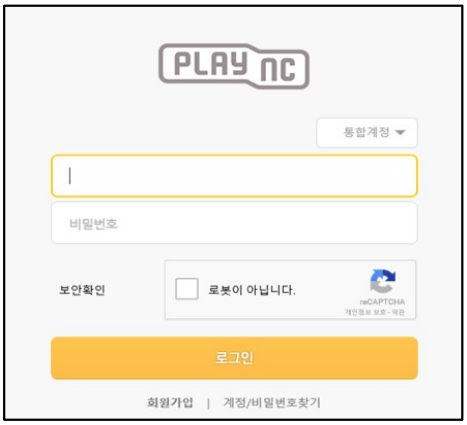
1) 로그인 시도 제한

잘못된 계정 정보로 로그인을 시도하는 경우, 일정 시도 횟수 이후 로그인을 차단하거나 일정 시간 동안 로그인을 제한하여 무차별대입공격(Brute-force attack)을 방지한다. 또한, 자동화 도구를 이용한 로그인 시도를 방지하기 위하여 CAPTCHA 인증을 추가로 수행하기도 한다. 그림 4는 엔씨소프트의 로그인 시도 제한 수단인 reCAPTCHA를 나타낸다. 5회 이상 로그인 실패 시 수행한다.

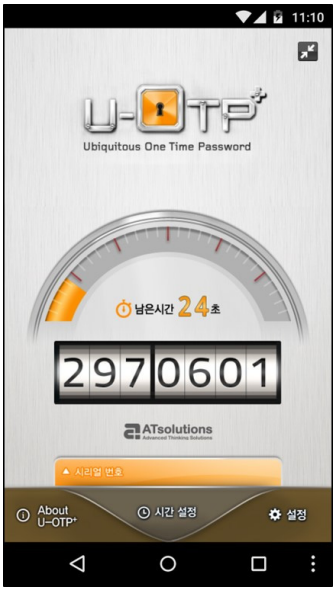
2) 이중 인증 (2-factor Authentication)

이중 인증은 다중 요소 인증의 한 유형으로 서로 다른 두 개의 인증 요소를 조합하여 사용자의 신원을 확인하는 방법이다. 단일 인증의 보안 취약성을 보완하기 위하여, 계정 아이디와 비밀번호 입력 외에 추가적인 인증 수단을 이용한다[19]. 국내 온라인게임사에서 적용하고 있는 이중 인증 수단은 다음과 같다.

- OTP (One Time Password): 휴대폰에 설치된 모바일 애플리케이션 형태의 OTP 또는 OTP 생성기 등으로부터 일회용 비밀번호 발급받아 로그인 시 입력한다. 이는 등록된 모바일 기기의 애플리케이션이나 OTP 생성기 소유자를 확인하여, 명의 도용을 방지하는 효과가 있다. 모바일 애플리케이션 OTP의 경우, 자체 솔루션을 구축하지 않고, 외부 솔루션을 적용한다. 대표적인 모바일 OTP 솔루션으로 U-OTP+[20], MOTP[21] 등이 있다. 그림 5는 넥슨과 웹젠에서 채택한 AT 솔루션의 U-OTP+ 모바일 화면을 나타낸다.



▶▶ 그림 4. 로그인 추가 인증 reCAPTCHA, 엔씨소프트



▶▶ 그림 5. U-OTP+, AT 솔루션

- 보조 비밀번호 (Secondary Password): 계정 비밀번호 외에 게임 실행을 위한 추가적인 비밀번호를 사용하여 보안성을 높일 수 있다.
- ARS: 사용자 인증 과정과 동일하다.
- 지정 PC (Designated PC): 게임 이용자 소유 또는 주로 사용하는 PC를 게임사에 등록하고, 로그인 시 PC를 확인하여 사용자를 인증한다. 지정 PC를 사용하는 경우 이중 인증을 생략하여 편의성을 높일 수 있다.

3) IP 주소 차단 (IP Address Blocking)

로그인 IP 주소를 모니터링 하여, 게임 이용자 본인이 아닌 비정상 접속을 탐지하고 차단한다. 주로 해외 IP 로그인을 탐지하거나, 로그인 이후 접속 IP의 변동 여부 등을 탐지한다. 비정상이 탐지되면 접속을 차단하고 사용자 인증 후 접속을 허용하는 등의 대응을 한다. 그림 6은 NHN 한게임의 IP 보안 선택 화면을 나타낸다.

▶▶ 그림 6. 로그인 시 IP 보안 선택, 한게임

4.1.5 게임 화폐 및 재화 보호

게임사의 통합 화폐를 부정 사용하는 것을 방지하기 위하여, 게임 화폐를 사용할 게임을 게임 이용자가 미리 지정하는 보안 서비스가 있다.

4.2 클라이언트 PC 보안 (Client PC Security)

클라이언트 PC 보안은 게임 이용자의 PC와 주변 기기, 게임 클라이언트 프로그램에 대한 해킹 공격에 대응하기 위한 보안 서비스로, 주로 게임 이용자의 PC에 설치하는 소프트웨어 솔루션을 이용한다.

4.2.1 키보드 보안 (Keyboard Security)

키보드 입력 정보를 실시간으로 암호화 하여 웹사이트 로그인과 같이 개인 정보를 입력할 때 정보 유출을 방지하는 프로그램이다. 개인 정보 유출을 시도하는 키로그 프로그램, 백도어, 해킹툴, 키보드 후킹 프로그램, 스파이웨어 등의 설치 및 실행 여부를 감시하고, 이러한 프로그램이 동작할 경우 사용자에게 경고 알람을 제공하기도 한다. 게임사는 AhnLab, nProtect, 라온시큐어 등의 보안 업체의 키보드 솔루션을 적용하고, 키보드 보안 서비스 이용 여부는 사용자의 선택 사항이다.

4.2.2 게임 클라이언트 보호 (Game Guard)

게임 패킷 암호화와 위변조 검사를 통해 게임 데이터를 보호하고, 개인정보 유출을 방지하는 프로그램이다. 게임핵, 스피드핵, 원격제어, 오토마우스와 같은 게임 해킹 도구를 진단하고 차단하는 기능과 시스템 바이러스 진단 및 차단 기능을 포함하기도 한다. 게임 클라이언트 실행 중에 게임 클라이언트 보호 프로그램이 정상적으로 실행되어야 하므로, 지속적으로 게임 서버와 통신을 하고 인증을 한다. 또한, 게임 접속 IP가 인가된 IP 인지 확인하고, 프록시 서버 등을 통한 비정상 접속인 경우 해킹 시도로 간주하여 차단시킨다.

게임 클라이언트 보호 프로그램은 필수 프로그램으로, 게임 클라이언트 실행 시 자동으로 실행된다. 그림 7은 nProtect 사의 게임 클라이언트 보호 프로그램인 GameGuard의 동작 과정을 나타낸다. GameGuard는 엔씨소프트의 게임 클라이언트에 적용되었다.

▶▶ 그림 7. GameGuard, nProtect [22]

4.2.3 안티바이러스 (Anti-Virus)

인터넷을 통한 개인정보 유출을 방지하기 위한 프로그램으로, 실시간 프로세스 감시를 통한 바이러스 감염이나 악성코드 설치 등을 진단하고 실행을 차단한다. 또한 웜 패킷의 패턴을 이용하여 네트워크 단에서 차단하는 기능을 포함하기도 한다. 추가적으로 악성코드 탐지 로그를 기록하여 사후 분석을 가능하도록 한다. 안티바이러스 프로그램의 예로 nProtect 사의 Netizen 프로그램[22]을 엔씨소프트에서 제공하고 있으나, 설치 및 실행은 사용자의 선택 사항이다.

4.3 네트워크 보안 (Network Security)

온라인게임사 홈페이지에 접속하여 서비스를 이용할 때, 개인정보 등의 민감한 정보를 안전하게 전송하기 위하여 보안이 강화된 웹 통신 프로토콜인 HTTPS를 사용한다. HTTPS는 TCP/IP 소켓 통신 시, SSL(Secure Socket Layer) 또는 TLS(Transport Layer Security) 프로토콜을 사용하여 인증과 암호화를 수행하므로, 신뢰성 있는 통신을 제공한다. 웹페이지의 URI는 'https://'로 표현되고, 웹브라우저에서 통신하는 서버의 인증서를 확인할 수도 있다. 국내 온라인게임사의 홈페이지에서 로그인 페이지는 HTTPS 통신을 사용하고 있다. 그림 8은 엔씨소프트의 로그인 페이지에서 웹브라우저의 보안

▶▶ 그림 8. 웹브라우저 HTTPS 보안 연결 확인, 엔씨소프트

연결을 확인한 예이다. 연결 대상 서버의 인증서 또는 인증기관의 인증서를 확인할 수 있다.

4.4 정보보호 활동 (Security Operations)

4.4.1 보안센터 (Security Support)

사용자 계정 및 개인정보보호, 클라이언트 PC 및 게임 클라이언트 보호를 위한 서비스 안내와 설정을 위하여 게임사 웹사이트에 보안센터를 운영한다.

4.4.2 신고센터 (Illegality Report)

계정도용, 결제정보도용, 불량이용자 (사기, 불법프로그램, 유해정보 배포), 권리침해 등의 사례가 발생한 경우에 게임 이용자가 직접 신고할 수 있도록 한다. 실시간 게임 중에 게임 내에서 또는 온라인게임사의 홈페이지 내, 신고센터를 이용할 수 있다.

4.4.3 정보보호인증 (Security Certificates)

정보보호인증 제도는 공인기관으로부터 기업이 정보보호를 위하여 기술적, 제도적으로 적절한 노력을 기울이고 있는지에 대하여 평가 받고 인증 받는 제도이다. 국내 온라인게임사는 다음 네 가지의 인증제도 중 하나 이상의 인증을 보유하고 있는 것으로 조사되었다.

1) PIMS (Personal Information Management System)[23]

기관 및 기업이 개인정보보호 관리체계를 갖추고 체계적, 지속적으로 보호 업무를 수행하는지를 평가하는 인증제도로, 인증기관은 한국인터넷진흥원이다. 개인정보보호 관리체계 구축을 통해 기업이 보유하고 있는 개인정보를 안전하게 관리하고 인증 기업의 대외 신뢰도 향상이 목적이다.

표 1. 국내 온라인게임사 별 보안 서비스 제공 현황

			넥슨	엔씨소프트	넷마블게임즈	웹젠	NHN 한게임
계정 보안	사용자 인증		● 휴대폰, E-mail	● 휴대폰, E-mail, i-PIN, SNS	● 휴대폰, I-PIN	● 휴대폰, E-mail, SNS	● 휴대폰, I-PIN
	비밀번호 규칙 강제		● 10~16	● 8~	● 8~15	● 8~20	● 6~15
	계정 등록 보안	자동 가입 방지	-	-	● CAPTCHA	-	-
		계정 생성 제한	● 3 IDs	● 10 IDs	-	-	● 5 IDs
	로그인 보안	로그인 시도 제한	● 5, CAPTCHA	● 5, reCAPTCHA	● 5, 사용자정보	● 5, CAPTCHA	● 3, CAPTCHA
		OTP	○ U-OTP, Playpass	○ Google OTP	○ MOTP	○ U-OTP	○ U-OTP
		보조 비밀번호	-	-	○ 게임 실행	-	-
		ARS 전화 인증	-	○ 유료	○ 유료	○	-
		지정 PC	○	○		-	○
		IP 주소 차단	● 해외 IP	-	-	-	○ 해외 IP, IP변동여부
	게임 화폐 및 재화 보호		○ 게임 지정	-	-	-	-
클라이언트 PC 보안	키보드 보안		○ AhnLab	○ nProtect	○ AhnLab	○ 라온시큐어	
	게임 클라이언트 보호		-	● nProtect	-	-	-
	안티바이러스		-	○ nProtect	-	-	-
네트워크 보안	HTTP over SSL		●	●	●	●	●
정보보호 활동	보안센터		●	●	●	●	●
	신고센터		●	●	●	●	●
	정보보호인증		PIMS, ISMS, e-Privacy	PIMS, ISMS, BS10012	PIMS, ISMS	ISMS	PIMS, ISMS,

2) ISMS (Information Security Management System)[24]

기업이 주요 정보자산을 보호하기 위해 수립, 관리, 운영하는 정보보호 관리체계를 평가하는 인증제도로 인증기관은 한국인터넷진흥원이다. 정보보호 위험관리를 통한 비즈니스 안정성을 제고하고, 윤리 경영을 위한 법적 준거성을 확보하여 침해사고, 집단소송 등에 따른 사회·경제적 피해를 최소화 하는 것이 목적이다.

3) e-Privacy[25]

인터넷사이트를 안전하게 이용하기 위하여 개인정보보호 수준을 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'과 '개인정보보호법'에 근거하여 평가하는 인증제도로 인증기관은 개인정보보호협회이다.

4) BS10012

기업의 개인정보보호를 위한 관리체계의 수립 및 이행에 대하여 평가하는 유일한 국제표준으로 인증기관은 영국표준협회 (BSI)이다. EU 개인정보보호 지침, OECD 개인정보보호 8원칙, Data Protection Act of UK, Global Best Practice 등을 기반으로 제정된 개인정보 경영시스템(PIMS)의 일종이다.

5. 국내 온라인게임사 별 보안 서비스

본 장에서는 조사 대상 온라인게임사 별 보안 서비스들을 정리하였다. 보안 서비스는 앞서 설명한 것과 같이 목적과 기능에 따라 분류하였고, 각 서비스 별 세부 사항을 기록하여 현황을 한 눈에 파악할 수 있도록 하였다.

표 1의 국내 온라인게임사 별 보안 서비스 현황에서 사용자 인증, 비밀번호 규칙 강제, 로그인 시도 제한 등과 같이 필수 서비스로 제공되는 것은 검정색으로 표시하였고, 사용자 선택 보안 서비스들은 흰색으로 표시하였다. 각 사의 비밀번호 상세 규칙은 표 2를 참고하도록 한다.

표 2. 국내 온라인게임사 계정 비밀번호 규칙 사례

넥슨	10~16자 영문/숫자/특수문자 2가지 이상 조합 같은 문자 3회 이상 금지
엔씨소프트	8자 이상 영문/숫자/특수문자 조합
넷마블게임즈	8~15자 영문/숫자 조합
웹젠	8~20자 영문/숫자/특수문자 2가시 이상 조합
NHN 한게임	6~15자 영문/숫자/특수문자 조합

6. 결론

본고에서는 2017년 기준 국내 온라인게임사에서 게임 이용자에게 제공하는 보안 서비스들을 조사하여 목적과 기능에 따라 분류하였다. 또한, 각 온라인게임사 간의 보안 서비스 제공 현황을 비교하였다.

국내 온라인게임사가 제공하는 보안 서비스들은 주로 사용자 계정과 개인정보보호에 치중하는 편이었고, 사용자의 선택에 맡기는 경향을 보였다. 게임 클라이언트가 실행되는 PC 및 게임 클라이언트 소프트웨어를 보호하기 위한 방법으로는 자체적인 솔루션 보다 외부 전문 업체의 솔루션을 적용하는 경향을 보였다. 네트워크 보안의 경우 공개된 웹 보안 기술을 적용하는 것 이외에 자체적인 네트워크 보안 서비스에 대한 정보는 공개되지 않았다.

본고를 통하여 국내 온라인게임에 적용된 보안 서비스들을 점검할 수 있는 계기가 되었고, 향후 보안 서비스를 구축하거나 보완할 시 도움이 될 수 있기를 기대한다.

참 고 문 헌

[1] https://venturebeat.com/2013/11/25/more-than-1-2-billion-people-are-playing-games/

[2] https://www.statista.com/statistics/267190/traffic-forecast-for-internet-gaming/

[3] https://www.statista.com/statistics/308454/gaming-revenue-countries/

[4] Jiyoung Woo, and Huy Kang Kim, "Survey and research direction on online game security", Proceedings of the Workshop at SIGGRAPH Asia(WASA '12) pp. 19-25, Nov, 2012. ACM.

[5] 곽병일, 김휘강, "온라인 게임에서의 이상 징후 탐지 기법 조사 및 분류", 한국정보보호학회논문지 VolL. 25, No .5, 2005. 10.

[6] 한국정보보호진흥원, "온라인게임 해킹 대응 가이드", 2006.06.

[7] Han Mee Lan, and Huy Kang Kim, "Security services in South Korean online games, the status Quo," http://www.hksecurity.net/home/pds/Online Game Security Service.pdf, Dec, 2014.

[8] Gi Seong Lee, Huy Kang Kim, "Internet Banking Security Services in South Korea, the status quo," http://www.hksecurity.net/home/pds/Internet banking security services.pdf, Feb, 2014.

[9] Byung-Tak Kang and Huy Kang Kim, "A study on the vulnerability of OTP implementation by using MITM attack and reverse engineering," Journal of the Korea Institute of Information Security & Cryptology, Vol. 21, No. 6, pp. 83~99, Dec, 2011.

[10] Changsok Yoo, Byung-Tak Kang, and Huy Kang Kim, "Case study of the vulnerability of OTP implemented in internet banking systems of South Korea," Multimedia Tools and Applications 74.10 (2015): 3289-3303.

[11] 한국기업평판연구소, http://www.rekorea.net

[12] NEXON, http://www.nexon.com

[13] NCSOFT, http://kr.plaync.com/

[14] Netmarble Games, http://www.netmarble.net/

[15] Webzen, http://www.webzen.co.kr/

[16] NHN Hangames, http://www.hangame.com

[17] 한국인터넷진흥원, 아이핀, https://i-pin.kisa.or.kr/

[18] https://en.wikipedia.org/wiki/CAPTCHA

[19] https://en.wikipedia.org/wiki/Multi-factor_authentication

[20] AT Solutions, U-OTP+, http://www.atsolutions.co.kr

[21] KG Mobilians, MOTP, http://www.mobilians.co.kr

[22] nProtect, http://www.nprotect.com

[23] 한국인터넷진흥원, PIMS, https://isms.kisa.or.kr/main/pims/intro/

[24] 한국인터넷진흥원, ISMS, https://isms.kisa.or.kr/main/isms/intro/

[25] 정보보호인증마크제도, e-Privacy, http://www.eprivacy.or.kr/

저 자 소 개

● 김 은 아(Eunah Kim)

- 2003년 8월: 이화여자대학교 컴퓨터학과 학사
- 2005년 8월: 이화여자대학교 과학기술대학원 컴퓨터학과 석사
- 2006년~현재 : ㈜ 삼성전자 책임연구원

<관심분야> : 네트워크 보안, 온라인게임 보안

● 김 휘 강(Huy Kang Kim)

- 1998년 2월: KAIST 산업경영학과 학사
- 2000년 2월: KAIST 산업공학과 석사
- 2009년 2월: KAIST 산업및시스템공학과 박사
- 2004년 5월~2010년 2월: 엔씨소프트 정보보안실장, Technical Director
- 2010년 3월~2015년 2월: 고려대학교 정보보호대학원 조교수
- 2015년 3월~현재: 고려대학교 정보보호대학원 부교수

<관심분야> : 온라인게임 보안, 네트워크 보안, 네트워크 포렌직