韓國IT서비스學會誌
第10卷 第2號
2011年 6月

온라인게임 서비스 분야에 정보보호 사전진단 적용시 효과성에 관한 연구

유동영* · 서동남** · 김휘강*** · 최진영****

A Study for Effectiveness of Preliminary Security Assessment on Online Game Service Domain

Dong-Young Yoo* · Dong-Nam Seo** · Huy Kang Kim*** · Jin Young Choi****

■ Abstract ■

The preliminary security assessment is an information security process to analyze security weaknesses before beginning of services. Discovering security weakness through preliminary security assessment is highly required because it costs much when security incident occur in the middle of service operation. However, this assessment is not widely spread in the online game service domain yet. In this paper, we summarize the security risk existed in the online game service, and we classify the security requirements related to the each risk. Also, through the case study, we evaluated the effectiveness of preliminary security assessment in this domain. In addition, we suggest checklists that should be reviewed once in game-client side, network-side and game-server side for the purpose of security enhancement.

Keyword : Online-Game Security, Game BOT, Preliminary Security Assessment

논문투고일 : 2011년 01월 21일 논문수정완료일 : 2011년 03월 16일 논문게재확정일 : 2011년 04월 18일

* 한국인터넷진흥원(KISA) 책임연구원, 주저자
** 고려대학교 정보보호대학원 석사과정
*** 고려대학교 정보보호대학원 조교수, 교신저자
**** 고려대학교 컴퓨터 · 전파통신공학과 교수

1. 서 론

정보보호 사전진단은 신규 IT서비스 개시 이전에 위협 및 취약점 분석 등 정보보호 진단을 수행하여 보호대책을 적용하는 정보보호 활동이다[2].

정보보호 사전진단이 필요한 이유는 취약점 발견 및 수정에 소요되는 비용이 서비스 설계단계에서 수행하는 것보다 서비스 운영단계에서 수행하는 것이 더 많이 소요되는 것을 근거로 들 수 있다.

설계단계에서 위협요소와 취약점을 서비스 운영 이전에 식별하여 해결 및 대책을 세워 두었다면 서비스 운영 이후 서비스 사용자들의 기밀성, 무결성, 가용성을 침해하지 않을 수 있다는 점에서 정보보호 사전진단 활동의 중요성이 증가하고 있다.

하지만, 그간 한국인터넷진흥원(KISA)의 다양한 연구에서 제시되고 발전되어온 정보보호 사전진단 활동은 아직 다양한 IT서비스에 대해 적용이 확산되지 않아, 그 중요성과 효용성에도 불구하고 많은 효과를 거두고 있지는 못한 상태이다.

정보보호 사전진단관련 연구는 그간 사업 분야별로 점진적으로 적용하면서 그 비용효과성을 검증하는 형태로 연구가 진행되어 왔는데, "정보보호 사전진단 방법론을 활용한 u-City 보안 모델 연구"[1]를 통해 서비스 개시 전에 적용한 정보보호 조치가 비용 효과적이라는 것을 검증한 연구사례가 있으며, RFID[4], VoIP와 IPTV[19], Zigbee를 통한 u-Service[17], 서비스 개발단계[3]에 대해서도 연구된 바 있다.

그럼에도, 아직은 정보보호 사전진단의 개념이 전체 IT서비스 영역을 고려해 볼 때, 아직은 도입단계이며, 비교적 최근에 등장한 특정 서비스에 시범적으로 적용을 시도했기 때문에 보다 범용적으로 이용 중인 서비스에 적용하여 검증해볼 필요가 있으며, 각 세부 서비스에 특화된 점검방법론을 지속적으로 개발을 해나가야 하는 상태라 할 수 있다.

예를 들어, 온라인게임 서비스의 경우에는, 많은 수출을 발생시키는 국가의 중요한 IT서비스임에도 불구하고 사전진단 방법론에 의거하여 최적화된 점검리스트가 도출되지 않았으며, 사전진단 방법론을 적용시 어떠한 기대효과를 거둘 수 있는지에 대한 연구는 아직 이루어지지 않은 단계이다.

본 논문에서는 온라인게임 서비스 분야에서 정보보호 사전진단의 활성화를 위해, 2010년 하반기에 새로이 서비스를 시작한 온라인게임에 사전진단 컨설팅을 수행하여 해당 서비스 영역에 특화된 점검리스트를 도출하였다. 더불어 국내 대표적인 온라인게임 서비스 회사의 사례를 토대로 실제 비용대비 효과를 분석하였다.

온라인게임 산업은 2009년 기준 국내 시장 3조 7,087억 원을 차지했으며, 온라인게임의 소비시장인 PC방 매출을 포함하면 5조 6429억 원으로, 전체 게임관련 시장 점유율의 81.1%를 차지한다. 2009년 온라인 게임의 세계시장 규모는 126억 달러를 기록하였다. 온라인게임 산업은 향후 2012년에는 국내 7조 1206억 원(PC방포함 9조 5339억 원), 세계 212억 달러의 시장으로 성장할 것으로 예측되는 각광받는 소프트웨어 산업이다[1].

국내 온라인게임에는 온라인 포털 서비스나 일반적인 전자상거래 서비스에 비해 심각한 침해사고 위협에 놓여있고, 지속적으로 피해사례가 발생하고 있다. 특히 국내에서 소위 2004년 이후 중국발 해킹이라 일컬어지는 공격들은 대부분 국내 온라인게임을 대상으로 할 정도로 공격의 발생 빈도 및 공격의 심각도가 높은 서비스 분야이다.

이는 온라인게임 내에서 게임플레이를 통해 생성되는 사이버 재화인 게임 내 아이템과 게임머니가 현금성 가치를 가지고 있기 때문이다.

[그림 1]에서 볼 수 있듯이, 온라인게임을 대상으로 한 중국발 해킹이 정점에 달했던 2010년 3월까지의 안철수연구소의 통계에 따르면 Win-Trojan/Onlinegamehack.159744.O가 10.6%, Dropper/Onlinegamehack. 184832가 7.8% 로 신종 악성코드 감염 1, 2위를 차지하였다. 이는 온라인게임을 대상으로 한 위협이 상당한 수준임을 보여주는 예라 할 수 있다[6].

〈표 1〉 2010년3월 신종악성코드 감염 top20

순위	악성코드명	건 수	비 율
1	Win-Trojan/Onlinegamehack.159744.O	32,336	10.6%
2	Dropper/Onlinegamehack.184832	23,928	7.8%
3	Win-Adware/ColorSoft.106496.D	22,964	7.5%
4	Win-Trojan/Agent.53248.ACQ	18,310	6%
5	Win-Trojan/Onlinegamehack.81920.L	18,110	5.9%
6	Win-Trojan/Daonol.24064.T	15,865	5.2%
7	Win-Trojan/Bho.874496	15,539	5.1%
8	Win-Trojan/Onlinegamehack.75264.B	15,199	5%
9	BAT/Delfile	14,599	4.8%
10	Win-Trojan/Agent.250368.O	12,819	4.2%
11	Win-Trojan/Onlinegamehack.159744.Q	12,281	4%
12	Win-Trojan/Eyon.270336	12,271	4%
13	Win-Trojan/Onlinegamehack.78848.G	12,080	4%
14	Win-Trojan/Downloader.268288.F	11,918	3.9%
15	Win-Dropper/ColorSoft.168523	11,873	3.9%
16	Dropper/Onlinegamehack.148992	11,572	3.8%
17	Win-Trojan/Buzus.988160.B	11,368	3.7%
18	Win-Trojan/Agent.615424.G	11,031	3.6%
19	Win-Trojan/Onlinegamehack.187904	10,641	3.5%
20	Win32/Palevo.worm.108032.E	10,263	3.4%
		304,967	100%

현재까지 온라인게임을 대상으로 발생되어왔던 공격의 유형을 정리하여 보면 다음과 같다.

첫 번째로, 해커가 온라인게임 서비스 회사의 시스템을 직접 해킹하여 DB 조작을 통해 사이버 재화를 생성한 뒤 현금화 하는 유형이다.

두 번째로, 해커가 온라인게임 서비스 회사의 해킹에 성공한 뒤, 게임서버의 프로그램 등 소스코드와 실행파일을 탈취하여 사설 서버를 운영하여 금전적인 이득을 얻는 유형이다[22].

세 번째로, 첫 번째와 두 번째에서 언급한 시스템적인 해킹 자체가 쉽지 않을 때에는 자동으로 게임플레이를 수행해주는 "게임 봇 프로그램"[8, 9]을 이용하여 사람의 개입 없이 자동으로 게임 내 재화를 생산하도록 하여, 생산된 사이버 재화를 현금화 하는 방법을 쓴다.

특히 세 번째의 경우가 사회적으로도 많은 물의를 일으키게 되는데, 온라인 게임 내에서 취득한 사이버 재화를 현금거래를 하여 부당한 이익을 취하거나, 이 과정에서 취득한 현금을 외환밀반출 하려다 적발된 사례 등이 그 예라 할 수 있다[5].

이러한 부작용을 막기 위해 온라인게임 서비스 회사에서는 지속적으로 게임 봇 프로그램을 탐지하여 부정행위를 저지르는데 이용된 계정을 제재하게 된다. 악용되었던 계정이 제재가 될 경우 해커의 입장에서는 지속적으로 금전적인 이익을 얻기 위해서, 적발되어 제재당한 계정을 대신하여 계속 게임을 플레이 할 수 있도록 새로운 계정을 생성할 필요가 생기게 되는데, 이 과정에서 주민등록번호 등 회원가입에 요구되는 개인정보가 필요해지게 된다. 그러므로 개인정보를 탈취하기 위한 악성코드 또는 계정의 ID/Password를 도용하기 위한 악성코드를 제작하여 배포하는 것으로 공격이 확대되는 것이 일반적이다. 국내의 경우 리니지 온라인게임에서 실제로 대규모의 명의도용이 발생했던 사례가 있다[7].

서두에 언급한 바와 같이, 정보보호 사전진단이 아직은 u-city 등 몇몇 특화된 서비스에 대해서 시범적으로 적용된 상태여서, 아직은 온라인게임에 존재하는 이런 위협들에 대하여 대비할 수 있는 점검항목들이 갖추어 져 있지는 않다.

본 논문에서는 온라인게임 서비스, 특히 MMO RPG(대규모 다중 사용자 온라인 역할 수행 게임; Massively Multiplayer Online Role-Playing Game)에 초점을 맞추어 게임 봇 대응 및 예방부문, 대고객 보안부문, 사설서버 대응 및 예방부문의 세 가지 부문에 대하여 각각 게임 클라이언트 측면, 네트워크 측면, 게임 서버 측면의 관점으로 나누어 각 부문에서 필요한 보안 점검 사항을 제안하고, 이를 사전진단을 위한 체크리스트 형태로 제시하였다. 각 온라인게임 개발 및 서비스 회사는 이 체크리스트를 적용함으로써 고객의 중요정보를 지키고, 게임 봇 프로그램 및 사설서버와 같은 불법행위로부터 자신들의 중요한 자산을 지킬 수 있을 것이다.

2. 문헌 연구

온라인게임 보안은 그 영역과 대상에 따라 3가지로 분류할 수 있다. 첫째, 온라인 게임 회사뿐 아니라 인터넷 서비스나 온라인 서비스 등을 하고 있는 회사라면 모두 해당되는 시스템 및 네트워크 분야의 전통적인 보안이다. 서버, 네트워크, 데이터베이스, 어플리케이션 및 데이터 보안의 전통적인 보안기술들이 해당된다. 둘째, 온라인 게임의 특성상 대규모의 PC사용자들이 인터넷을 통하여 접속되는 형태의 서비스이므로, 사용자의 컴퓨터에 키보드 보안 솔루션을 설치해주거나, OTP(One Time Password)를 제공해주어, 고객의 계정과 고객정보를 보호하기 위한 보안이다. 은행에서 인터넷 뱅킹 서비스 이용자를 위해 다양한 보안수단을 제공해주는 것 또는 포털사이트들에서 계정도용을 예방하기 위해 다양한 보안수단을 제공해주는 것 역시 같은 범주라 할 수 있다. 다만, 온라인게임의 경우에는 제 1장에서 설명한 것처럼 해킹을 통해 얻을 수 있는 금전적인 이익이 크며, 공격 대상자가 다른 서비스들에 비해 월등히 많다는 차원에서 더욱 중요도가 높으며, 금융권에서는 아직 서비스되고 있지 않은 다양한 보안수단(예 : 휴대폰을 이용한 OTP)이 선도적으로 이용되기도 한다. 마지막으로 게임보안만의 특징으로, 게임 서버와 게임 클라이언트에 게임 봇 제작자에 의한 해킹을 방지하기 위한 다양한 보안조치로 대표되는 보안활동을 들 수 있다[18, 21].

이처럼 온라인게임 보안은 타 분야의 보안과 공통되는 영역과, 게임의 특유의 보안영역이 융합되어 있는 특이성을 지닌 보안 분야이기 때문에 기존의 다른 IT서비스 영역에 적용하였던 사전진단 방법론을 적용할 수 없으며, 온라인게임 보안을 위한 사전진단 방법론을 개발하는 것이 필요하다.

3. 온라인게임 내의 위험요소

온라인게임 내에서 가장 문제가 되는 위험요소로는 게임 봇 프로그램에 의한 게임서비스 품질 저하, 계정도용으로 인한 피해, 그리고 사설서버로 인한 수익률 감소가 있다.

게임 봇 프로그램은 온라인게임을 사람의 개입 없이 자동으로 플레이 해주는 프로그램이다[20]. 계정도용은 타인의 정보 및 주민등록번호를 부정하게 사용하여 게임 계정을 만들거나, 타인의 계정으로 무단 접속을 하는 행위를 말한다. 사설서버는 게임 서버를 제작 및 운영하며 게임에 대한 저작권 및 서비스 권리 없이 영리나 비영리 목적으로 다른 단체 또는 개인이 게임 서비스 회사의 동의 없이 온라인 게임을 즐길 수 있도록 서비스하는 행위 또는 서버 자체를 지칭하는 말이다[13].

3.1 게임 봇 프로그램

게임 봇을 물리적인 형태로 구분하자면, 소프트웨어 형태, USB 형태, 마우스 형태로 나눌 수 있다. 소프트웨어 형태는 별도의 장비가 필요 없이 봇 프로그램만으로 작동하는 게임 봇이며, USB, 마우스 형태의 봇은 USB나 마우스에 펌웨어 형태로 게임 봇 모듈이 내장되어 있으며 별도의 게임 봇 프로그램과 내장되어 있는 모듈간의 통신에 의해 전기적인 신호를 보내어 작동하도록 제작된 게임 봇이다. 동작 방식에 의한 구분으로는 IG 봇과 OOG 봇으로 구분할 수 있다. IG 봇은 In Game BOT의 약어로 게임 클라이언트가 필요하고, 게임 클라이언트에 명령을 내리는 형태로 동작을 하며, OOG 봇은 Out of Game BOT의 약어로 게임 클라이언트 없이 직접 서버와 통신을 하는 형태로 non-client BOT 또는 non-game client BOT이라고도 한다.

게임 봇은 게임을 정상적으로 플레이하는 사용자들과 게임 서비스 회사 모두에게 해악을 끼친다. 대부분의 정상적인 게임 이용자들은 게임 봇을 사용하지 않으나, 사람의 경우에는 게임플레이를 지속할 수 있는 시간이 제한되는 것에 반해, 게임 봇 프로그램은 기계적으로 동작하므로 24시간 상시 게임플레이를 할 수 있어 게임 봇을 사용할 경우 다른 정상적인 게임 이용자에 비해 월등히 빠른

레벨상승을 할 수 있으며, 많은 게임 내 사이버재화를 취득하는 것이 가능하다. 즉, 게임 봇은 게임 내 공정한 플레이를 해치며 결과적으로는 게임 내의 경제, 레벨 등 기획과 운영상의 밸런스를 무너뜨린다는 점에서 문제가 크고, 특히 정상적으로 게임을 플레이하는 이용자들의 만족도를 떨어뜨리며 상대적인 박탈감을 유발하므로, 게임 봇으로 인해 많은 게임 이용자들이 해당 게임 서비스를 이탈하게 된다.

특히 게임 봇은 게임 서비스 회사의 입장에서 볼 때, 게임 제작과 서비스 운영에서 많은 비용을 발생시키게 되는데 첫째로, 게임 개발비가 상승하게 된다. 게임 봇으로 인한 빠른 컨텐츠 소모로 인해 잦은 컨텐츠 업데이트를 할 수 밖에 없으며, 이로 인하여 게임 개발비가 상승하게 된다. 둘째, 게임 내에서 부정행위를 감시하고 적발하기 위한 인원들의 인건비를 상승시킨다. 온라인게임 내에는 일반적으로 GM(Game Master)이라고 불리는 게임 내에서 상담을 통하여 고충을 듣고, 사용자들이 불편해 하는 사항을 접수하여 질 좋은 서비스를 제공하기 위한 게임 운영자들이 있는데, 게임 봇에 의한 게임 내 부정행위를 적발하기 위해 다수의 운영자들을 추가적으로 투입하여야 하고, 정상적인 게임이용자들에 투입되어야 할 운영자들의 노력이 게임 봇을 찾아내기 위한 업무에 과다 투입됨에 따라 인력 운영비용 증가는 물론, 게임 서비스 만족도 저하로 이어지고 있다.

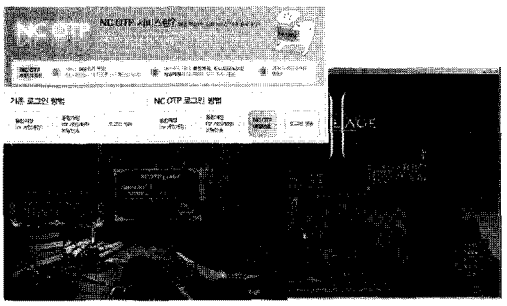
현재까지 이러한 게임 봇을 탐지하기 위한 해결책으로 튜링테스트, CAPTCHA[13], 데이터마이닝[16], 행동 패턴 분석[14], 네트워크 트래픽 및 패킷 분석[15] 등 여러 가지 방법들이 연구되어 왔지만, 100% 게임 봇을 탐지하는 해결책은 없으며, 오탐율로 인해 실제로 적용하기에는 한계가 존재한다. 국내에서 서비스 중인 MMORPG 와 같은 경우 대부분 회원가입자가 40~50만 명 정도 되기 때문에 정상이용자를 게임 봇으로 오진하는 오탐율이 1%만 되어도 4000~5000명의 정상적인 사용자가 피해를 보게 되므로 아직까지는 육안확인과 수작업에 의한 제재에 의존하는 경우가 대부분이다[10].

3.2 계정도용

우리나라의 경우에는 회원 가입 시 기존에 가입된 회원인지, 제재된 회원인지를 주민등록번호를 이용하여 확인을 하게 된다. 제 1장에서 설명하였듯이 온라인게임 서비스 회사에서는 게임 봇 프로그램을 탐지하여 해당 계정을 제재하게 될 경우 해당 주민등록번호 및 그에 속한 계정은 더 이상 이용할 수 없게 되는데, 해커는 적발되어 제재당한 계정을 대신하여 게임을 플레이 할 수 있도록 다른 계정을 생성하는 과정에서 타인의 개인정보를 필요로 하게 된다. 따라서 해커는 계정생성에 필요한 주민등록번호를 다양한 해킹방식(키로거, 악성코드, 백도어)을 통해 취득하게 된다.

비단 계정도용이 아닌, 시스템 해킹에 의한 정보유출을 가정해 볼 때에도, 국내에서 서비스 중인 MMORPG 와 같은 경우 회원가입자가 보통 40~50만 명에 달하는 것을 감안해 보면, 온라인 게임 서비스 회사에 침해사고가 발생하여 고객 개인정보가 유출될 경우 그 파급도가 매우 크다고 할 수 있다.

이러한 계정도용은 온라인게임에서 가장 심각한 보안 문제 중 하나라고 여겨지고 있다. 하지만, 실시간으로 계정도용 유무를 탐지하기는 매우 어려워서 게임 서비스 회사에서는 계정도용을 당한 피해자가 신고를 하지 않는다면, 그 사실을 알 수 없는 경우가 많아 문제가 크다고 할 수 있다[11].



[그림 1] 엔씨소프트의 NC-OTP 구현 예

[그림 1]는 온라인 게임회사에서 이러한 계정도용 피해를 예방하기 위하여 모바일 OTP를 이용한 부가인증서비스를 게임 내에 구현해둔 예이다.

3.3 사설서버

사설서버들은 첫째, 게임 개발사가 개발한 컨텐츠를 무료로 즐길 수 있게 해줌으로써 개발사의 이익을 감소시키며, 둘째, 계정정보의 유출문제를 야기한다. 악의적인 운영자가 게임서버의 접속기내에 심어둔 악성코드로 인한 여러 가지 정보유출 또는 사설서버의 ID/Password와 실제 게임 및 다른 사이트의 ID/Password를 동일하게 설정하였을 경우 악의적인 운영자는 해당 ID/Password로 실제 게임 및 다른 사이트에 접속을 시도하기 때문이다. 특히 중국에서 만든 사설서버에 이런 ID/Password를 노린 코드가 숨겨져 있는 경우가 빈번하다.

사설 서버는 프로그램 복제권 혹은 2차적 저작물 작성권을 침해한 행위로, 저작권법에 따라 3년 이하의 징역 또는 3000만 원 이하의 벌금에 처해진다. 그러나 서버가 해외에서 운영되는 경우가 많아 단속이 쉽지 않으며, 저작권법이나 프로그램 보호법, 정보보호에 관한 법률이 확립되지 않은 해외 국가에서 운영될 경우 마땅한 법적인 조치를 할 수가 없으므로, 사전에 사설 서버 예방을 위한 기술적인 보호조치를 하는 것이 중요하다. 사설서버 존재가 알려지면서 이를 악용한 사기도 벌어지고 있다. 저렴한 비용에 게임을 이용할 수 있다는 식으로 광고를 하며 금품을 요구하는 내용이 유포되고 있으며, 성인용 등급 판정을 받은 게임이라도 사설서버에는 나이제한이 없어 미성년자들도 이용 가능하도록 사설서버 운영자가 연령 제한을 두지 않는다는 점에서 심각도가 높다고 할 수 있다.

사설서버는 게임 서비스 회사와 무관한 네트워크상에서 생성되고 접속하기 때문에, 게임 서비스 회사에서 사설서버 탐지는 매우 어려운 문제이다. 계정도용과 마찬가지로 사설서버 생성을 방지하기 위한 해결책은 현재까지 나와 있지 않다.

4. 점검 프레임워크

본 논문에서는 온라인게임의 점검 프레임워크를 게임 클라이언트 측면, 네트워크 측면, 게임 서버 측면의 점검으로 나누어 보았다.

이를 도식화 하면 [그림 3]와 같다.

4.1 게임 클라이언트 측면

게임 클라이언트 단의 주요 점검 보안사항으로는 '안티-디버깅, 안티-리버스엔지니어링 기법을 이용하여 게임 클라이언트 프로그램을 보호하였는지', '메모리 및 프로세스 보호를 통해 게임 클라이언트 프로세스가 우회되고 메모리가 제 3의 프로세스에 의해 참조되거나 변조됨을 막고 있는지'를 들 수 있다. 또한, 이와 같은 보호조치 외에도 PC 내에 악성코드, 게임 봇 프로그램의 구동 유무를 게임 클라이언트 단에서 점검해 주어야 한다.

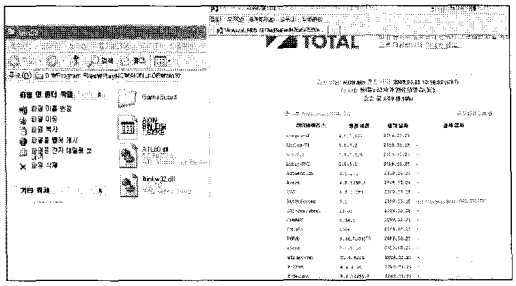
게임 클라이언트에서 점검을 수행하는 것은 다음과 같은 장점이 있다.

첫째, 게임 클라이언트에서 직접 점검을 수행할 수 있으므로 플레이어 PC 내부 악성프로세스와 같은 정보를 직접 취득하여 점검하는 것이 가능하다. 둘째, 클라이언트 용량이 크므로 탐지루틴을 내부적으로 구현할 때 코드 난독화와 패킹을 통해 보호만 적절히 하면, 악성코드 제작자 또는 게임 봇 제작자들이 보호조치를 역으로 분석하는데 걸리는 시간을 오래 걸리도록 할 수 있다.

이에 반해, 게임 클라이언트에서 점검을 수행하는 것의 단점은 첫째, 100% 완전한 프로세스 보호 방법은 사실상 존재하지 않으며, 보안의 적용등급을 높일 경우 사용자의 편의를 해칠 수 있는 문제가 존재한다. 그렇기 때문에 클라이언트에서 보호조치를 적용한다 하더라도 프로세스 인젝션, 프로세스 우회와 같은 기법으로부터 100% 안전할 수 없다.

둘째, 클라이언트의 프로세스나 메모리를 보호하려고 커널의 Ring 0 영역을 감시하여 타 프로세스의 프로세스 후킹 시도를 감시할 경우, 이와 같은 원리로 동작하는 다양한 다른 보안제품군들-

안티바이러스, DRM(Digital Right Management), DLP(Data Leakage Protection)-과의 충돌을 발생시키거나, 윈도우즈 OS 커널과의 충돌, 특정 하드웨어와의 충돌을 일으키는 문제가 발생하게 되어 사용자 편의성을 심각하게 떨어뜨리게 된다. [그림 2]은 정상적인 온라인게임의 실행파일을 악성코드로 오진한 예를 보여주고 있다.



[그림 2] 정상적인 온라인게임 실행파일을 악성코드로 오진하는 사례

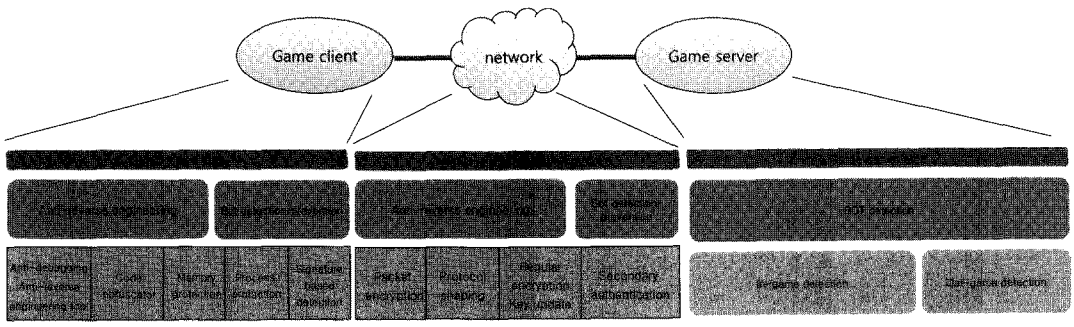
셋째, 보안모듈을 지속적으로 보호하고 분석을 어렵게 하기 위하여 클라이언트 내의 보안모듈 업데이트를 자주 수행할 경우 이를 네트워크 상으로 업데이트하기 위한 다운로드 트래픽 증가로 인해 네트워크 관리비용의 증가가 발생하게 된다.

4.2 네트워크 측면

네트워크 단에서의 주요 점검할 보안사항으로는 '게임 클라이언트와 게임 서버 간 통신 프로토콜이 적절한 강도의 암호화를 통해 통신 트래픽이 안전하게 보호하였는지', 또 '통신 프로토콜을 정기적으로 변경을 하고, 통신 패킷을 랜덤하게 스크램블 시켜 게임 봇 프로그램의 접속을 탐지 및 차단시키는 보호조치가 구현 되어있는가' 이다.

네트워크에서 점검의 장점은 첫째, 클라이언트 단에서 직접 대응하는 것이 아니므로, 사용자가 게임 플레이를 할 때 편의성을 떨어뜨리지 않고 대응할 수 있다는 점에 있다. 둘째, 게임 클라이언트가 존재하여 게임 서버와 지정된 프로토콜로 통신을 하고 있는지를 네트워크상에서 수행할 수 있으므로, 지정된 게임 클라이언트 프로그램 없이 동작하는 게임 봇 프로그램을 탐지하는 능력이 높다. 주로 게임 클라이언트가 존재할 때만 줄 수 있는 응답 프로토콜을 정기적으로 업데이트하여, 현재 버전의 프로토콜 명령어에 정상적으로 응답하는지 유무를 이용하여 탐지 및 차단할 수 있다.

네트워크에서 점검의 단점은 첫째 네트워크 트래픽에 강력한 암호화를 적용할 경우 봇 제작자에 의한 트래픽 분석을 막을 수는 있으나, 암호화 연산을 수행해야 하는 서버의 부하를 유발시켜 게임 내 지연(lag)을 발생시키게 된다는 점에 있다. 둘째, 게임 클라이언트와 게임 서버 간의 통신 프로토콜을 업데이트 한 후 구버전 프로토콜로 반복 접속을 시도하는 게임 봇 프로그램이 있을 경우, 이 게임 봇 프로그램이 지속적으로 생성하는 패킷에 의해 네트워크의 가용성이 심각하게 손상 받을 수 있다.



[그림 3] 온라인 게임 점검 프레임 워크

4.3 게임 서버 측면

게임 서버 단에서의 주요 점검할 보안사항으로는 '게임 내 로그를 남기고, 게임 패킷들을 서버에서 직접 검사하여 게임 봇 및 게임 내 불량행위를 탐지하고 있는지'로 요약할 수 있다.

게임 서버에서 점검의 장점은 첫째, 서버 단에서 점검하므로 탐지 루틴이 노출될 확률이 가장 낮다는 점에 있다. 둘째, 서버에서 직접 패킷을 기반으로 점검하므로 위변조 탐지능력이 우수하다고 할 수 있다. 셋째, 게임 서버에서 탐지와 동시에 실시간으로 부정 접속에 대해 차단대응을 할 수 있다.

게임 서버에서 점검의 단점은 온라인 게임의 경우 서버 당 동시 접속 세션을 4,000~5,000개 이상을 처리하여야 하는데, 게임 서버 내에서 이러한 게임 연산 처리 외에 게임 봇, 게임 내 해킹시도 및 불량행위 탐지를 위한 연산까지 수행해야 하므로 게임 서버 내에서 성능저하가 발생할 수 있다. 탐지를 위한 감사 로그를 다수 생성할 경우 서버에 많은 I/O를 발생시키게 되어 디스크의 성능저하 및 대량의 로그저장을 위한 시설투자비용을 유발하게 된다.

5. 사전점검 체크리스트

온라인게임 서비스의 보안점검 체크리스트의 대분류로 "게임 봇 대응 및 예방", "대고객 보안", "사설서버 대응 및 예방" 의 세 가지 부문으로 구분하였으며, 사전에 조치해야 할 보안사항들을 중분류로 "게임 클라이언트 측면", "네트워크 측면", "게임 서버 측면"으로 구분하였다.

본 논문에서 제시한 체크리스트는 국내 시장점유율 1~2위인 대표 온라인게임회사 2곳에서 현업부서와 논의를 거쳐 도출되었으며, 2010년 하반기에 출시한 신규 MMORPG 게임 서비스를 개시하기 전에 사전 점검을 수행하는데 사용되었다[12, 16].

5.1 게임 봇 대응 및 예방부문

게임 봇은 게임 클라이언트를 리버스엔지니어링 기법을 통해 게임 클라이언트 내에 구현된 모듈 및 알고리즘, 네트워크 통신 프로토콜 등을 분석하여 제작을 시작한다. 분석이 완전히 끝난 경우에는 게임 클라이언트 없이도 게임을 구동시킬 수 있는 "non-client BOT"까지 만들 수 있다. 일반적으로 게임 클라이언트는 많은 자원을 사용하기 때문에 컴퓨터 한 대에서 실행 시킬 수 있는 클라이언트 수가 제한되지만 "non-client BOT"은 많은 자원을 사용하지 않기 때문에 한 대의 컴퓨터에서 수십 대의 게임 봇을 실행할 수 있는 장점이 있다. 하지만 클라이언트가 있어야만 응답할 수 있는 질문에 대한 응답 유무로 쉽게 탐지가 되기 때문에 역설적으로 "non-client BOT"이 완벽한 분석 후에 제작되는 반면 그 탐지 방법은 일반적인 게임 봇 보다 쉽다고 할 수 있다.

게임 봇 대응 및 예방부문의 사전보안점검항목의 예는 <표 2>과 같다.

〈표 2〉 게임 봇 대응 및 예방부문 사전점검항목 예

적용 단	체크리스트 항목	비고
게임 클라이언트 측면	◦ 게임보안 전용 프로그램을 사용하고 있는가?	
	◦ 게임보안 전용 프로그램을 사용하지 않을 경우, 자체적으로 만든 보호모듈을 이용하여 게임 클라이언트 구동 시 함께 구동되어, 메모리 보호, 프로세스 보호를 하고, 알려진 게임 봇 들이나 악성코드, 일반적인 디버거의 접근 시도를 차단하고 있는가?	
	◦ 별도의 인증 모듈을 이용하여 non-client BOT을 탐지/차단할 수 있는가?	

게임 클라이언트 측면	◦ 게임 클라이언트가 자체적인 검진 기능을 보유하고 있는가? ◦ (예 : 일정한 주기를 두고 게임 클라이언트 프로세스의 PPID, 게임 클라이언트의 실행파일이 적재하고 있는 DLL 파일, 게임설정이 저장된 ini 파일들의 checksum 값의 변경 유무를 확인)	
	◦ 게임 클라이언트의 주요 exe file과 dll file에 난독화를 위한 패커(packer) (예 : winlicense, yoda's protector, ASPack)를 적용하였는가?	
	◦ 패커 프로그램을 적용할 경우, 안티바이러스 및 DRM/DLP 등 보안프로그램들과 충돌이 발생하는지를 사전에 점검하는 업무 프로세스를 운영하고 있는가?	
	◦ 패커 프로그램을 적용할 경우, 아직까지 언패킹된 적이 없는 최신버전을 사용하고 있는가?	
	◦ 안티바이러스 및 DRM/DLP 등 보안프로그램들과 충돌 또는 오진이 발생할 경우에 대비하여 보안 회사들과 비상연락망을 유지하고 있는가?	
	◦ 게임 클라이언트의 주요 exe file과 dll file에 패커프로그램을 적용하기 어려운 경우, 이에 준하는 자체적인 리버스엔지니어링 방지 방안을 구현하여 두었는가?	
	◦ 게임 클라이언트 프로그램 또는 같이 구동되는 보안프로그램을 통해서 잘 알려진 디버거 프로세스, 매크로 프로그램 툴이 구동 중인지 정기적으로 체크하는가?	
	◦ 게임 클라이언트와 서버간의 통신을 보호하기 위해 암호화 통신이 구현되어 있는가? ◦ 이때 초기 키 값이 게임 클라이언트 내에 하드 코딩 되어 있지 않는가?	
	◦ 게임 클라이언트 내에 구현된 보안모듈(예 : 암호키 교환 모듈)에는 코드 가상화와 같은 VM 기술을 적용하여 코드를 추가적으로 보호하고 있는가?	
	◦ 게임 클라이언트를 업데이트하는 런처/업데이터에 패커나 디버깅 방지 툴을 적용하였는가?(단, 오진 발생 시 업데이트를 할 방법이 상당히 제약될 수 있음)	
	◦ 디버그 관련 정보가 함께 배포되지 않았는가? - 게임개발 중 사용한 디버그 로그, PDB 파일의 배포 - 디버깅 모드로 컴파일 된 게임 클라이언트 프로그램의 배포	
	◦ 게임 클라이언트의 입력처리 과정에서 SQL Injection 및 XSS 가 발생하지 않도록 입력 값을 적절히 필터링 하였는가? ◦ SQL injection, XSS가 유발될 수 있는 입력 값들에 대한 처리를 구현하여야 한다. 특히 게임 내 쪽지, 게임 내 메일, 게임 내 게시판, 게임 내 상점 등에서 SQL injection, XSS를 유발할 수 있는 특수문자나 태그의 입력을 막아야 한다.	
	◦ 게임 클라이언트에 함께 배포되는 아트리소스, 음원 등의 리소스, 텍스트 파일에 대한 보호조치를 하고 있는가? ◦ 주요 점검항목 - 음원, 매쉬 데이터 들이 그대로 추출되지 않는가? - 알려진 언패커에 의해 풀리지 않는가?	
	◦ 게임 클라이언트 시 아트리소스가 위변조 되지 않았는지 점검하는가? ◦ 랜덤하게 아트리소스 파일들의 checksum을 확인하여 로딩 되는 아트리소스 파일이 위변조 되지 않았는지 확인 - 아트리소스 위변조 예방(주 활용예 : 누드패치 등 악용되는 사례 방지용도) 및 라이센스가 보호되어야 할 아트리소스의 무단추출(예 : 음원)을 막기 위함	
	◦ 정기적으로 인터넷/P2P 상에 구버전 클라이언트 및 언패킹된 클라이언트 파일이 유출되지 않았는지 확인하는 프로세스를 운영 중에 있는가?	
	◦ 구버전 파일이 계속 구동/유통되지 않도록 보호조치를 취하고 있는가? - DVD/CD를 통한 구버전 클라이언트의 무료 배포 후 회수 조치가 마련되어 있는가? - 게임 클라이언트 내에 만료 기간을 지정, 특정 날짜가 지난 구버전 파일은 동작하지 않도록 조치가 되어 있는가? - 게임 구동 시 클라이언트의 주요 파일, 통신 프로토콜 버전을 체크하여 정상적인 버전이 아닐 경우 접속을 차단하거나, 강제 파일 업데이트를 하는 조치가 구현되어 있는가?	

네트워크 측면	◦ 네트워크 통신 프로토콜을 리버스엔지니어링 하지 못하도록 암호화 하고 있는가?	
	◦ 이 때 사용되는 암호화 키를 정기적으로 변경하고 있는가?	
	◦ 게임 클라이언트와 서버 간 통신 프로토콜은 정기적으로 변경하고 있는가?	
	◦ 네트워크 패킷 분석 상으로 게임 봇 을 탐지할 수 있는 hidden protocol command를 구현하여 두었는가? - hidden protocol command : 평소에는 거의 사용되지 않는 명령으로 서버에서 클라이언트가 봇 프로그램인지를 확인하기 위해 던지는 질의/응답 명령을 의미. 이를 이용하여 극히 드문 주기로 임의 추출된 사용자에게 질의 패킷을 보내어 특정 회수 이상 응답이 없을 경우 봇으로 탐지하거나 이상사용자로 분류하도록 함	
	◦ 게임 클라이언트와 서버 간 통신 시 랜덤하게 더미 데이터(dummy data)를 페이로드에 첨부하여 분석을 어렵게 하고 있는가? - 예 : 이동 등 특정 액션마다 발생하는 패킷이 동일하면 암호화 되어 있다 하더라도 분석이 용이, 가비지 데이터를 랜덤하게 첨부시켜서 보내는 등 분석을 어렵게 하는 방법을 적용하고 있는가? ◦ 다음 사항을 주의하여 본 점검항목을 수행하도록 한다. - 이와 같은 방식을 이용하여 모든 사용자에 동시에 보낼 경우 BOT 제작자에 의해 분석되기 쉬운 단점이 있다. - 자주 사용할 경우 분석되기 쉬우므로, 질의 패킷과 답변이 동적으로 변경될 수 있도록 설계하여야 함	
	◦ 게임 클라이언트, 게임 서버와 무관하게 네트워크 접속 패턴만을 이용하여 게임 봇 탐지를 네트워크 측에서 할 수 있도록, 전용 정밀검사용 서버를 운영하고 있는가?	
게임 서버 측면	◦ 정기적으로 게임 내 로그(in-game log)를 분석하여 불량사용자 및 게임 봇 사용자를 탐지하고 있는가?	
	◦ 게임 내 로그 외에 게임 외 로그(out-game log; 인증, 결제 등) 등 타 로그와 교차분석을 수행하고 있는가?	
	◦ 로그 분석만을 위한 전용 분석서버를 두어 대응하고 있는가?	
	◦ 게임 서버에서 로그분석에 기반한 자체 봇/불량행위 탐지 규칙을 적용하며, 정기적으로 탐지 규칙을 업데이트 하고 있는가?	
	◦ 게임 서버에서 자체적인 패킷 점검을 통해 '실시간'으로 탐지와 차단이 가능하도록 설계해 두었는가?	
	◦ 게임 내 CAPTCHA와 같은 제 3의 서버 측의 불량사용자 탐지방안이 구현되어 있는가? - 적용 시 게임유저들의 몰입을 해치지 않기 위한 방안 고려가 되었는가? - 게임서버의 부하를 줄이기 위해 게임서버와 별도의 독립적인 게임 내 CAPTCHA 서버를 운용하고 있는가? - 예 : CAPTCHA 서버는 백그라운드로 CAPTCHA 이미지를 지속적으로 생성 후 정답과 CAPTCHA ID를 저장, 게임 서버로 이미지 전달과 정답 확인요청 질의에 결과를 전달 - CAPTCHA 서버는 게임 클라이언트에 노출되지 않으며 외부 공인 IP를 갖지 않음	
	◦ 로그분석 기반 또는 CAPTCHA와 같은 제 3의 서버 측 탐지를 할 경우 탐지/제재와 같은 운영규칙은 약관에 부합하는가?	
	◦ 고객과의 분쟁에 대비, 분석과 탐지 알고리즘은 항상 오류가 없음을 입증할 수 있는가?	
	◦ 정기적으로 VPN/PPTP 를 통해 우회 접속하는 IP 주소에 대해 차단을 하고 있는가?	
	◦ 단일 PC에서 동시에 여러 개의 접속을 허용하고 있는가?	

5.2 대고객 보안 부문

대고객 보안 부문은 주로 계정도용, 사용자가 게임을 원하는 시간에 플레이를 할 수 있는 가용성 및 개인 사용자에 대한 해킹에 중점을 둔 부문이다.

개인 사용자에 대한 해킹은 바이러스, 외부 게시판, 사설서버 등을 통하여 사용자의 ID/Password를 알아내어 접속하고 아이템 및 게임머니를 도용하는 경우가 많기 때문에, ID/Password 외에 OTP 서비스, 보안카드 서비스, 피씨등록 서비스, 전화인증 등의 2채널 인증 서비스를 제공하거나 IP 상으로 드러나는 특정국가나 위치를 차단하는 방법 등이 있으며, 사용자의 가용성을 위해 회선 이중화, ISP(Internet Service Provider), IDC(Internet Data Center) 및 관련 공공기관의 공조를 통한 DDoS(Distributed Denial of Service) 대응 체계 구축 등이 있다.

대고객 보안 부문의 사전보안점검항목의 예는 <표 3>와 같다.

5.3 사설서버 대응 및 예방 부문

제 4장에서 기술한 바와 같이, 사설서버 대응 및 예방 부문에서는 실제 온라인게임 서비스 회사와

〈표 3〉 대고객 보안 부문 사전점검항목 예

적용 단	체크리스트 항목	비고
게임 클라이언트 측면	◦ 계정도용 시도를 탐지/차단하기 위한 기능을 구현하여 두었는가?	
	◦ 클라이언트 프로그램에 연속적인 ID/Password 입력 실패 발생 시, CAPTCHA 이미지를 불러오도록 구현하여 두었는가?	
	◦ 웹 로그인의 경우 웹 로그인 홈페이지에 CAPTCHA 이미지 인증을 하도록 구현하여 두었는가?	
	◦ 이때 CAPTCHA는 OCR 자동판독을 당하지 않도록 충분한 강도를 유지하는가?	
	◦ 고객 PC 보안을 위해 다양한 보안솔루션을 제공하여, 계정도용을 예방하는 조치를 취하였는가? ◦ 예 : 국내 제공 중인 계정도용 예방 서비스/제품은 다음과 같다. - 피씨등록 서비스 - 모바일 OTP - OTP 기기 - 전화인증 서비스 - 무료 온라인 백신 - 무료 키보드보안 제품	
	◦ 전수(Brute force) 공격을 통해 로그인 실패율이 높은 블랙리스트 IP에서 계정생성, 게임접속이 불가능하도록 주기적으로 차단하고 있는가?	
	◦ 접속이 차단된 IP에서 접속한 게임 클라이언트, 웹 브라우저 쪽으로 에러 메시지는 차단 의도를 알 수 없게끔 단순하게 전달해 주고 있는가?	
	◦ 이 IP 주소 대역에서 접속한 선량한 피해자가 접속이 차단되었음을 콜센터로 통지할 경우에 대비하여, 대응 시나리오를 마련해 두었는가?	
네트워크 측면	◦ 서비스 거부 공격에 대비하여 적절한 보안솔루션 또는 대응방안을 갖추어 두었는가? - 회선이중화, ISP/IDC 와의 공조체제 구축, KISA 와의 공조, DDoS 방지 솔루션 구축 등 - 무차별로 로그인을 시도 등 서버 과부하 또는 서버 다운을 목적으로 하는 공격에 대비하여 서버 로드밸런싱을 구성하여 두도록 한다.	
게임 서버 측면	◦ SQL injection/XSS 취약점이 발생하지 않도록 서버에서 필터링을 수행하고 있는가?	
	◦ 서버 측에서 저장 프로시져 입력 값 점검, 게임 내 쪽지, 게임 내 메일, 게임 내 게시판 내 특수문자 입력 값들에 대해 엄격한 필터링을 적용하고 있는가?	

통신을 하는 것이 없기 때문에 네트워크 측면에서는 탐지할 수 있는 적절한 방법이 없는 상태이다.

하지만 사설서버 역시 게임 클라이언트를 분석하여 서버와의 통신을 분석하고 해당 서버를 구현하는 방식이 주를 이루기 때문에, 사전에 클라이언트 분석을 막기 위한 디버깅 방지, 리버스엔지니어링 방지기법을 충분히 구현하여 예방할 수 있으며, 게임 개발 및 테스트 단계에서 해킹을 통해 게임 서버의 실행 파일이 유출되어 사설서버가 구현되는 것을 방지하기 위해 개발 및 테스트 단계에서부터 서버 단에 보안 시스템을 구축함으로써 대응을 하는 것이 가능하다.

완벽한 예방은 할 수 없지만, 최대한 탐지능력을 극대화 할 수 있도록, 클라이언트에서 공식 서버를 제외한 다른 IP address로 접속하려는 시도가 발생 시 클라이언트 자체적으로 게임서비스 사에 정보를 송출하는 기능을 구현해 두어 증거로 삼아 추후 법적인 대응을 할 수 있도록 대응 시스템을 구축하는 방법이 주를 이룬다. 사설서버 대응 및 예방 부문의 사전보안점검 항목의 예는 <표 4>과 같다.

6. 정보보호 사전진단 효용분석 결과

본 절에서는 온라인게임 서비스의 개발단계에서 정보보호 사전진단을 통해 설계 단계의 보안 취약점을 제거하여 상용화를 할 경우, 어느 정도의 정보보호 비용이 절감되는지를 살펴보고, 이를 통해 정보보호 사전진단의 효용성을 살펴보고자 한다.

현재 상용화된 온라인 게임 서비스의 경우 일반적으로 게임서버, 웹 및 인증 서버, 결제 서버, 이 서버군들의 네트워크 구축을 위해 사용되는 관련

〈표 4〉 사설서버 대응 및 예방부문 점검항목 예

적용 단	체크리스트 항목	비고
게임 클라이언트 측면	◦ 사설서버 예방을 위해, 게임 클라이언트에서 사용하는 별도의 설정파일(예 : *.ini, *.conf) 에 접속정보가 기록되어 있는 경우 이를 강력한 알고리즘으로 암호화 하여 보호하고 있는가?	
게임 클라이언트 측면	◦ Ini 파일 등의 별도로 분리된 설정 파일을 이용하지 않고, 게임 클라이언트 내에 접속에 관련된 설정 정보가 하드 코딩되어 있을 경우 이 정보가 추출되거나 변조되지 않도록 코드 가상화나 강력한 패커를 사용하여야 한다. ◦ 리소스 파일을 포함하여 보호할 수 있도록 별도의 보안프로그램을 이용하여 보호하고 있는가?	
	◦ 정기적으로 암호화 알고리즘 또는 키를 변경하고 있는가?	
	◦ 게임 클라이언트가 비정상 종료 시 게임 서비스사로 경고 메일 발송하게 하고 있는가?	
	◦ 이 정보는 사설서버 접속 시도 탐지에 활용할 수 있도록 DB에 저장하여 관리하고 있는가?	
	◦ 게임 클라이언트가 공식 IP 주소가 아닌 곳으로 접속할 경우에 이를 보고하는 기능을 구현하여 두었는가? 또는 서드파티(3rd party) 게임보안솔루션을 이용하여 이러한 기능을 이용하고 있는가?	
	◦ 이 루틴은 코드 가상화 및 난독화툴(obfuscator) 및 리버스엔지니어링 방지 툴에 의해 보호되고 있는가?	
게임 서버 측면	◦ 호스트 레벨에서 게임 서버의 실행파일의 유출에 대비하여, 유출이 되어도 동작하지 않도록 기술적인 보호조치를 취하였는가? - 서버의 MAC 주소, CPU 일련 번호, 디스크 이름 정보 등 회사 내 서비스하는 장비의 하드웨어에 종속한 정보를 이용하여 해쉬 값을 생성하고, 이 해쉬 값이 일치할 때에만 게임 서버가 구동되도록 구현하여야 함 - 서버는 초기 구동 시 입력된 시리얼 정보가 맞지 않을 경우 자동 종료되도록 함	

게임 서버 측면	◦ 네트워크 레벨에서 게임 서버의 실행파일이 유출이 되어도 동작하지 않도록 조치를 취하여 두었는가? - 내부 IDC 의 IP 주소 대역 에서만 동작하도록 함 - 예 : Windows 도메인 정보, 사설 IP 주소 범위가 일치하는 경우에만 동작하도록 하거나 서버 초기 구동 시 내부의 도메인 조절기나 인증 서버에 접속이 가능한 경우에만 구동되도록 함 - 이 경우 인증 서버는 사설 IP만을 가지며 외부 인터넷에서는 접근이 불가능 하도록 ACL(access control list)을 구성하여 보호함 - 첫 구동 시점 외 구동 중에도 인증 서버에 접속을 시도하여 접속이 안 될 경우 종료되도록 함 - 시작 시점에 우회되었을 수 있으므로 랜덤한 간격으로 허가하여 인증 서버에서 인증 받을 수 없는 경우 종료하도록 함. 단, 인증 서버의 안정성이나 내부 IDC 네트워크의 안정성이 보장될 수 있는 환경이어야 적용이 가능함	
	◦ 게임 서버의 실행파일이 유출이 된 것을 추적할 수 있도록 구현하여 두었는가? - 게임 서버가 구동(up), 정지(down), 오류로 인한 종료(crash) 될 때 서버 crash 정보 및 up/down 정보를 SMTP 또는 HTTP 를 이용하여 정보를 온라인게임 회사로 송출할 수 있도록 함 - Mail 또는 HTTP 를 통해 전달할 정보에는 IP 주소, 도메인 정보, 사용자, 게이트웨이 IP 정보, 역추적 정보 등 추적에 필수적인 정보를 담도록 함 - 특히 서버 바이너리 배포대상 국가, 빌드넘버, 빌드일자 를 포함하여 증거로 활용 가능하도록 함	
	◦ 원격에서 운영되는 사설서버에서 회사의 게임 서버 실행파일이 구동 중일 때, 이를 원격에서 접속하여 조회/통제할 수 있는 기능이 구현되어 있는가?	
	◦ 게임서버가 특정 IP에 구동중인 것을 안 경우 해당 게임 서버에 접속하여 버전 정보 및 빌드넘버, 빌드 일자 등 증거에 활용할 수 있는 정보를 조회할 수 있도록 되어 있는가?	

네트워크 장비, 해당 네트워크에 구축된 보안장비 및 소프트웨어, 게임 클라이언트 및 서버 프로그램 부속물들로 게임 서비스가 구성되어 있다.

이들을 상용화가 된 후에, 이미 내재되어 있는 취약점을 발견하기 위하여 게임 서버, 웹 및 인증 서버, 결제 서버, 관련네트워크 장비, 관련 보안장비, 게임 응용프로그램(게임 클라이언트 프로그램, 서버 프로그램 부속물) 등을 진단한다면 실제적으로 많은 비용이 소요된다.

하지만, 정보보호 사전진단을 통해 설계 및 구축단계에 진단을 통해 불필요한 설계 요소와 필요한 정보보호 부분을 반영할 경우 많은 비용을 줄일 수 있다. 정보보호 사전진단의 비용산정 방식은 다음과 같다[2].

상기 산식을 바탕으로 상용화와 사전진단에 따른 비용산정 결과는 <표 5>와 같다.

<효과분석 산식>

$$TC = \sum_{i=1}^{l} \alpha_i + (\sum_{i=1}^{m} \beta_i + K) + \sum_{i=1}^{n} \gamma_i$$

◦ αi = i번째 장비의 시장 대체가격
◦ l = 대체 장비 수
◦ βi = i번째 장비의 교체 및 수거에 대한 인력파견 비용
◦ m = 대체 장비 수,
◦ K = 서비스 개통일 지연에 대한 보상비용
◦ γ = 비밀유출에 따른 손해배상 비용
◦ n = 서비스 가입 및 이용자 수

상기 비용산정 결과를 보면, 상용화를 기준으로 사전진단을 통해 웹/인증 설계, 보안장비, 게임 응용프로그램에 대하여 교체 및 설계 변경 등의 교체 및 수정 비용이 사전진단 미수행의 경우와 비교해볼 때 최소 60%의 비용절감 효과를 발생시키는 것을 알 수 있다.

〈표 5〉 사전진단 비용효과 산정표

구 분	서비스 구축 기준	진단비용
일반 상용화	게임 유관서 버 50대 웹/인증, 결제 서버 20대 네트워크 장비 5대 보안장비 3대 게임 응용 프로그램 4식	1억 5천만 원
정보 보호 사전 진단	교체장비(웹/인증 2대)× 교체장비 단가(2,000만 원)	4천만 원
	응용 프로그램 수정 (1,000만 원)× 4식	4천만 원
	응용프로그램 취약점 진단(500만 원) × 4식	2천만 원

이는 국내 대표적인 온라인 게임 서비스 기업들에서 매년 취약점 분석에 소요되는 진단예산이 평균적으로 1개의 게임 서비스 점검에 1억 5천만 원 가량 매년 집행하고 있는 것에 근거하여, 기존 선행연구에서 제시된 효과분석 산식을 활용하여 산정한 결과이다[2]. 시뮬레이션 결과에서는 실제 상용화 이후에 발생하는 설계상의 보안 문제를 해결하는데 소용되는 교체 및 수정 비용에 대해서 살펴보았고, 실제 상용화시에는 서비스 개시 후에 서비스 신뢰성 하락 및 서비스 이용자의 피해보상 부분이 발생할 경우 사전진단을 통해서 절감할 수 있는 비용에 대한 효과성은 더욱 증가할 수 있다.

6. 결 론

본 논문에서는 정보보호 사전진단 방법론을 알아보고, 이를 온라인게임에 적용하여, 온라인게임 서비스에서 가장 문제가 되고 있는 불법행위인 게임 봇 프로그램, 계정도용, 사설서버를 각각 게임 클라이언트 측면, 네트워크 측면, 게임 서버 측면으로 나누어 각 단계와 각 측면에서 보안성을 사전에 점검할 수 있는 체크리스트를 제안하였다. 이 체크리스트를 통하여 각 온라인게임 개발사 및 서비스 회사에서 고객의 개인정보를 지키고, 게임 봇 프로그램 및 사설서버와 같은 불법 프로그램 및 불법행위로부터 자신들의 중요한 자산을 지켜 안전한 온라인게임 개발 및 서비스를 가능케 할 것이다.

또한 온라인게임 서비스 보안에 대한 노하우가 없는 신생 온라인게임 개발 및 서비스 회사에서 어떠한 사항을 점검해야 하는지에 대해 참고자료로써 활용될 수 있을 것이다.

본 논문에서는 온라인게임 서비스 분야에 대하여 정보보호 사전진단에 따른 상용화시의 보안 진단 비용에 대한 효과성을 제안하였다.

정보보호 사전진단의 비용효과 분석은 단순히 장비 교체 및 프로그램 수정의 1차원적인 피해이외에도 기업의 가치하락 및 서비스 이용자 감소와 같은 2차적인 피해가 발생할 가능성이 크다. 향후 본 연구의 개선 분야는 2차 피해에 대한 경제적 분석을 통해 사전진단의 효과성에 대한 추가 검증이 필요하다.

아울러, 본 논문의 사전진단 결과는 온라인게임 서비스 보안에 대한 노하우가 없는 신생 온라인게임 개발 및 서비스 회사에서 어떠한 사항을 점검해야 하는지에 대해 참고자료로써 활용될 수 있을 것이다.

참 고 문 헌

[1] 「2010 대한민국 게임 백서」, 한국 컨텐츠 진흥원, 2010.

[2] 신동훈, "정보보호 사전진단 방법론을 활용한 u-City 보안 모델 연구", 박사학위논문, 단국대학교, 2010.

[3] 신동훈, "서비스 개발단계에서의 정보보호", 「한국IT서비스 학술대회논문집」, 제1권(2010), pp. 384-391.

[4] 신동훈, 김국태, 이강신, "신규 IT서비스의 정보보호 사전평가 모델 : RFID 서비스 적용 중심", 한국정보처리학회, 제25회 춘계학술발표대회, 2006.

[5] 동아일보, "中서 불법생산 온라인 게임머니 현금바꿔 420억 밀반출", http://www.donga.

com/fbin/output?n = 200810220106.

[6] 안철수연구소, 2010년 3월 신종악성코드 감염 보고 top 20, http://www.ahnlab.com/kr/site/securitycenter/asec/asecView.do?groupCode = VNI001&webNewsInfoUnionVo.seq = 15952.

[7] 중앙일보, "리니지 명의도용 피해신고 22만건 넘어", http://article.joinsmsn.com/news/article/article.asp?ctg = 16&Total_ID = 2208595.

[8] 김휘강, 「Online game security」, Codegate, 2009.

[9] 김휘강, 「Online game security-new approaches for the endless battlefront」, Korea Security Seminar (KSS), 2010.

[10] Ahmad, M. A., B. Keegan, J. Srivastava, D. Williams, and N. Contractor, "Mining for Gold Farmers : Automatic Detection of Deviant Players in MMOGS", International Conference on Computational Science and Engineering, 2009.

[11] Chen, K. T. and L. W. Hong, "User Identification based on Game-Play Activity Patterns", The International Journal of Virtual Reality, 2007.

[12] Chen, K. T., J. W. Jiang, P. Huang, H. H. Chu, C. L. Lei, and W. C. Chen, "Identifying MMORPG Bots : A Traffic Analysis Approach", *EURASIP Journal on Advances in Signal Processing archive*, Vol.2009(2009).

[13] Golle, P. and N. Ducheneaut, "Preventing Bots from Playing Online Games", Computers in Entertainment (CIE), 2005.

[14] Hilaire, S., H. C. Kim, and C. K. Kim, "How to deal with bot scum in MMORPGs", IEEE Communications Quality and Reliability (CQR) Workshop, Vancouver, Canada, 2010.

[15] Kesteren, M. V., J. Langevoort, and F. Grootjen, "A step in the right direction : Bot detection in MMORPGs using movement analysis", The 21th Benelux Conference on Artificial Intelligence(BNAIC), 2009.

[16] Kim, H. G., S. W. Hong, and J. T. Kim, "Detection of Auto Programs for MMORPGs", The 18th Australian Joint Conference on Artificial Intelligence, Lecture Notes in Computer Science, 2005.

[17] Lee, I. S., K. H. Hong, G. S. Lee, and J. I. Lee, "Preliminary Diagnosis Model for a New IT Service : Improving the Information Security of u-Services with Zigbee", World Academy of Science, Engineering and Technology, 2007.

[18] Mitterhofer, S., Kruegel, C., Kirda, E., Platzer, C., "Server-Side Bot Detection in Massively Multiplayer Online Games", IEEE Security and Society, 2009.

[19] Shin, D. H., Y. M. Nah, H. S. Kim, G. S. Lee, and J. I. Lee, "Study of Measures to Secure Video Phone Service Safety through a Preminary Evaluation of the Information Security of the New IT Service", World Academy of Science, Engineering and Technology, 2007.

[20] Thawonmas, R., Y. Kashifuji, and K. T. Chen, "Detection of MMORPG Bots Based on Behavior Analysis", The International Conference on Advances in Computer Entertainment Technology, 2008.

[21] Varvello, M. and G. M. Voelker, "Second Life : a Social Network of Humans and Bots", The 20th international workshop on Network and operating systems support for digital audio and video, 2010.

[22] Wikipedia, "Private Server", http://en.wikipedia.org/wiki/Private_server.

◈ 저 자 소 개 ◈

유 동 영 (ydy@kisa.or.kr)

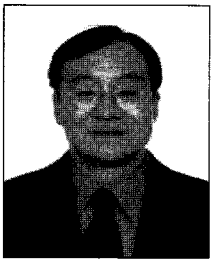
현재 한국인터넷진흥원 팀장으로 재직중이며, 숭실대학교 전자계산과를 졸업하고 숭실대학교 컴퓨터학과에서 석사를 취득하였으며, 고려대학교 컴퓨터·전파공학과 박사과정을 수료하였다. Journal of Intelligent Robotic Systems, Conference of Software Engineering and Data Mining 등의 국제학술지 및 학술대회에 논문을 게재한 바 있다. 주요 관심분야는 정보보호, 정형기법, 소프트웨어 공학, ROBOTICS 등이다.

서 동 남 (deepgust@korea.ac.kr)

현재 고려대학교 정보보호대학원 석사과정으로 재학 중이며, 제주대학교 전산통계과 학사를 졸업하였다. 주요 관심분야는 정보보호, 데이터마이닝, 온라인게임보안, 소셜 네트워크 등이다.

김 휘 강 (cenda@korea.ac.kr)

현재 고려대학교 정보보호대학원 조교수로 재직 중이며, KAIST 산업경영학과 학사, KAIST 산업공학과 석사, KAIST 산업및시스템공학과 박사를 취득하였다. 에이쓰리시큐리티의 창업자이며, 엔씨소프트의 정보보안실장, TD (Technical Director)로 근무하였다. 주요 관심분야는 온라인게임보안, 데이터마이닝 및 머신러닝 기반의 침입탐지, 네트워크보안 등이다.



최 진 영 (choi@formal.korea.ac.kr)

현재 고려대학교 융합소프트웨어 전문대학원 교수 및 고려대학교 컴퓨터통신공학부 겸직교수로 재직중이며, 서울대학교 컴퓨터 공학과 학사를 졸업하고, Dept of Mathematics and Computer Science, Drexel Univ에서 석사를 취득하였으며. Dept of Computer and Information Science, University of Pennsylvania 박사를 취득하였다. 주요 관심분야는 정형기법, 임베디드 실시간 시스템, 프로그래밍 언어, 프로세스 대수, 소프트웨어 공학 등이다.