제주교육대학교 논문집 (2004)
제33집 pp. 359~374

온라인 게임의 보안에 관한 연구
A Study on Security of Online Game

김종훈*, 이면재**, 김종진**

〈목 차〉

〈개 요〉

국내 온라인 게임 산업은 초고속 인터넷의 보급으로 지속적으로 성장하고 있고 이러한 온라인 게임 산업은 국가와 온라인 게임을 개발한 기업에 큰 경제적 이익을 제공하고 있다. 그러나 온라인 게임 산업의 경제적인 이득과 온라인 게임의 아이템을 획

* 제주교육대학교 컴퓨터교육과 교수
** 홍익대학교 컴퓨터공학과 박사과정 수료

득하기 위한 목적으로 행해지는 불법적인 해킹은 국내 게임 산업의 발전에 방해 요소가 되고 있다. 따라서 본 논문에서는 국내 온라인 게임에서 발생되고 있는 해킹의 공격 유형을 살펴보고 이에 대한 보안 방법을 연구하였다. 이 논문은 개발된 게임을 보안하려는 온라인 개발 업체에게 도움이 될 수 있다.

〈ABSTRACT〉

As high speed internet is widely used, industry of online game has been increasing. And, industry of online game has been important gains of our country, company of online game. But illegal hacking to gain of economical profits and items has been a obstructive factor of industrial development for online game. This paper shows kinds of hacking in online game in our country and researches security method of it. This paper should be helpful to secure the online game which developed the it.

1. 서 론

해킹을 시도하지 않는 분야로 알려져 왔던 온라인게임 업계에 최근 크래킹 사건이 잇달아 발생하였다. 인기 온라인 게임 위드를 서비스하고 있는 조이임팩트에서는 최근 중국인으로 추정되는 해커의 서버 공격으로 3일 동안 서비스를 중단하는 피해를 입었다. 그리고 3D 온라인게임 라그나로크를 서비스하고 있는 그라비티는 해커에 의해 서버 실행 파일과 데이터 파일이 유출되는 피해를 입었다. 코스닥 등록업체 액토즈소프트도 온라인 게임 미르의 전설 2의 게임 소스가 유출되는 사건을 겪기도 했다. 조이임팩트의 경우에는 해커의 공격을 막고 3일만에 서버 복구에 성공하여 큰 피해를 입지 않았으나 서버 복구 기간 동안 게임 이용이 불가능해 게이머들의 항의가 있었다. 그러나 그라비티와 액토즈의 경우 실행 파일과 게임 소스 유출 이후 무료로 게임을 서비스하는 불법 서버가 등장해 경제적인 피해를 입고 있다. 액토즈는 유럽 서비스 업체에서 미르의 전설 2의 게임 소스가 유출되면서 유럽과 중국에서 불법 서버가 개설됐다. 그라비티는 대만에서 시범 서비스 중이던 데이터가 유출되면서 현재 독일에서 무료

서버가 운영되고 있다. 해당 업체는 유출된 게임 소스가 현지화 초기 버전인데다 업그레이드가 불가능하기 때문에 더 이상 피해는 확대되지 않을 것으로 보고 있다. 그러나 업계 일각에서는 이번 사태를 계기로 근본적인 대책을 마련해야 한다고 주장하고 있다. 실제 국내 온라인 게임 업계는 지난해 해외 진출을 본격화하면서부터 크고 작은 크래킹 피해를 입고 있다. 국산 온라인 게임이 대만, 중국, 그리고 일본 등에서 인기를 끌자, 이 지역 해커들의 집중 공격을 받고 있기 때문이다. 한국 온라인 게임들이 해커들의 표적이 되고 있는 것은 온라인게임 특성상 서버 접근이 용이하고, 유명 게임을 해킹할 경우 실적이 되기 때문이다. 국내 온라인 게임 업체들의 보안 기술은 최근 몇 년 사이 상당한 수준으로 높아졌으나, 크래킹 방법과 기술이 대범해지면서 그 피해 정도가 점차 심각해지고 있다. 온라인 게임 서비스 초기에 나타난 해킹 양상은 야한 사진을 홈페이지에 올린다거나, 더 많은 게임 아이템을 얻기 위해 스피드핵을 사용하는 정도였으나, 최근에는 서버를 다운시키거나 소스코드를 노리는 악의적인 크래킹이 시도되고 있다. 특히 크래킹에 의한 게임 소스 유출은 국내 온라인 게임 업체들이 쌓아온 게임 개발 노하우를 한꺼번에 잃어버릴 수 있다는 측면에서, 단순한 해킹이 아니라 산업적인 위협으로까지 인식되고 있다. 액토즈소프트만 해도 중국 내 불법 서버가 생겨나면서 현지 라이선스 업체와 책임 소재를 놓고 마찰을 빚었고, 급기야 계약을 파기하는 사태를 맞기도 했다[1]. 따라서 이러한 해킹을 막기 위해 보안 장비 또는 보안 소프트웨어를 구입하거나 보안 사항을 고려하여 온라인 게임 서버를 운영해야 한다. 온라인 게임의 보안을 고려하지 않고 온라인 게임을 운영하는 경우에 만약 해킹을 당하게 되면 게이머들의 아이템이 없어지거나 네트워크 또는 네트워크 자원, 그리고 게임 서버가 정상적으로 작동을 할 수 없어 게임의 충성도가 낮아질 수 있고 온라인 게임 소스가 유출되는 경우에 게임 경쟁력이 저하될 수 있다.

본 논문의 2장에서는 온라인 게임의 해킹 유형을 살펴보고, 3장에서는 이에 대한 보안 대책을 논하고, 4장에서는 결론 및 추후 연구 방향을 기술하였다.

2. 온라인 게임의 해킹 유형

온라인 게임은 여러 게이머간의 상호 작용을 통해 게임이 진행되므로 인터넷 상에 존재하는 각종 해킹과 그에 사용하는 보안 기법은 동일하다. 특히 MMORPG[2]는 동일

한 공간과 시간에서 게이머들의 상호 작용에 의해서 진행되므로 온라인 게임에만 적용되는 특징적인 현상들은 존재한다. 예를 들어 온라인 게임에 대한 해킹, 네트워크를 통한 공격, 시스템을 공격하는 방법 등이 이러한 특징에 포함될 수 있다[2].

2.1 아이템 해킹

아이템이란 게임 내 캐릭터가 소유한 창, 칼, 물건등으로 수량이 극히 한정적이며 오랜 시간동안 이를 획득하기 위해 노력해야 하는 것이다[3]. 그러므로 상대방과 대전하거나 다른 게이머들과 함께 몬스터를 사냥하는 등 게이머의 상호 유기적인 관계를 맺는 온라인 게임에서 아이템이 해킹되면 많은 게이머들이 큰 피해를 당할 수 있다. 아이템 해킹은 계정을 도용하여 사용자의 아이템을 훔치는 것이다. 이러한 아이템 해킹 방법에는 Key Stroke Hooking, 운영자 사칭, 그리고 게임의 버그를 주로 이용하는 것이 있다.

- **Key Stroke Hooking[6, 7]**

클라이언트 PC에 키보드 입력을 가로채어 비밀 공간에 보관하거나 실시간으로 공격 대상의 PC에 설치된 스니핑(Sniffing) 프로그램을 이용하여 사용자 계정과 비밀 번호를 가져가는 방법이다. 주로 여러 사람이 공유하는 PC에 많이 사용되며 인터넷에서 쉽게 구할 수 있는 해킹 프로그램을 이용하여 PC의 모든 키보드 사용을 파일로 저장시켜 사용자의 ID와 패스워드를 빼내간다. 어떤 특정한 상황에서만 작동하는 인터넷 웜이나 바이러스를 이용하여 원격에서 상대 시스템을 조작하거나 모니터링을 하여 게이머의 자료를 유출하는 방법도 있다.

- **운영자 사칭[6, 8]**

이것은 사회 공학적인 해킹 방법으로 온라인 게임의 게시판등에 운영자를 사칭하여 사용자의 각종 정보 즉 게임의 내용, 서버, 계정, 비밀번호를 속기 쉬운 메일 계정으로 전송하도록 속여 유출시키는 방법이다.

---

2) MMORPG(Massively Multi-player Online Role Playing Game)는 인터넷상에서 많은 게이머들이 게임을 플레이 할 수 있는 게임

● 게임 버그 이용[6, 7]

운영체제나 온라인 게임 프로그램의 알려지지 않은 버그를 이용하여 아이템을 복사하거나 획득하는 방법이다.

● 게임 방해

공격자가 다른 게이머들이 정상적으로 게임을 진행하지 못하는 환경을 구축하여 공격자의 의도대로 게임을 진행하는 행위로써 공성전을 할 때 적 혈맹이 사용중인 PC방쪽에 대량의 네트워크 트래픽을 유발시키는 방법이 이에 포함될 수 있다. 이렇게 하기 위해서 공격자는 사전에 바이러스 프로그램이나 DDoS(Distributed Denial of Service)에 관련된 프로그램을 해당 PC방 PC에 설치해야 한다.

● 사기(Fraud)

온라인 게임 안에서 각종 거짓, 술수, 그리고 음모를 통하여 아이템을 취득하는 행위이다.

〈표 1〉은 아이템이 해킹된 게임의 예이다[4,5].

〈표 1〉 아이템이 해킹된 게임 예

게 임	예
포트리스 3	무한 폭격 해킹 프로그램을 이용하여 일방적인 공격을 할 수 있음
미르의 전설 3	몬스터를 사냥하지 않고 단 시간내 많은 아이템을 획득할 수 있는 아이템 복사 해킹 프로그램으로 자신의 공격 속도를 1.45배 정도 향상시키면서 빠른 시간내 많은 몬스터를 사냥하는 스피드 해킹 프로그램
스타크래프트	지도를 해킹한다는 뜻의 맵핵'(Maphack)은 게임내 지도에 까맣게 가려진 부분을 없앰으로써 상대방이 어디에서 무엇을 할 수 있는지 한눈에 알 수 있는 프로그램으로 상대방의 위치와 전략을 명확하게 알 수 있음
포커게임	인터넷 온라인 포커 게임에서 상대방의 패를 볼 수 있는 해킹 프로그램

2.2 네트워크, 서버에 대한 해킹

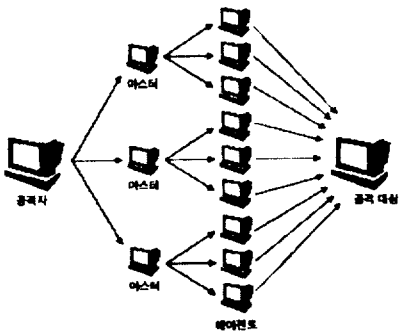
인터넷의 본격적인 활동이 시작된 이후, 우리나라에는 새로운 용어로 대변되는 변화의 물결이 나타나고 있으며, 동시에 해킹, 웜[3]의 역기능도 나타나고 있다. 즉 오프라인에서 가능했던 많은 경제 활동들이 인터넷 상에서 이루어지는 환경으로 변화되면서 이에 대한 정상적인 흐름을 방해하려는 시도가 나타나고 있다. 게임도 개인용 PC 게임에서 온라인 게임으로 변화되면서 정상적인 게임 진행을 막거나, 온라인 게임 서버에 대한 해킹이 본격화 되고 있다. 현재 네트워크 또는 서버를 해킹하기 위해 주로 시도되는 공격 방법은 DDoS[4]와 바이러스[5]에 의해 라우터나 서버의 CPU 또는 메모리, 그리고 하드 디스크와 네트워크 대역폭을 낭비하도록 유도하는 것이다. 님다, 코드레드, SQL 슬래머등 최근의 가장 큰 이슈가 되었던 해킹들은 모두 DDoS 형태의 바이러스이다. 이러한 DDoS공격과 바이러스들은 서버 컴퓨터가 과부하로 인해 작동이 중지되는 서버다운(Server Down) 또는 일시적으로 게임 속도가 느려지는 랙(Lag) 현상을 발생시켜서 게이머의 데이터를 유실시키거나 정상적으로 게임 진행을 못하게 만드는 원인이 된다. 특히, 경험치가 누적되는 성장형 게임에서 아이템에 대한 유실은 게이머에게 정신적 또는 물질적 손해를 크게 입히는 경우가 많다. (그림 1)은 DDoS 해킹 공격의 형태의 예이다[8]. 공격자는 공격을 주도하는 해커의 컴퓨터이고, 마스터는 공격자에게서 직접 명령을 받는 시스템으로 여러 대의 에이전트를 관리하는 시스템이고 에이전트는 공격 대상에 직접적인 공격을 가하는 시스템이다. 공격자는 공격 대상의 네트워크 또는 운영체제의 취약점을 파악하고 마스터에 공격대상을 공격할 수 있는 프로그램과 공격 방법과 순서등에 관련된 스케줄을 저장한다. 이러한 과정을 통해 공격자는 계획된 시간에 마스터를 이용하여 공격 대상을 공격한다.

(그림 2)는 2002년도와 2003년도의 해킹 피해 유형 분류를 보여준다[9]. 주로 DDoS 공격이나 바이러스에 의한 공격에 의한 불법 자원 사용이 2002년도에 비해 2003년도가

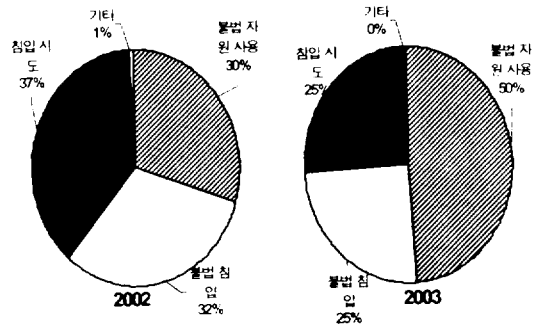
3) 컴퓨터 시스템을 파괴하거나 작업을 지연 또는 방해하는 악성프로그램. 실행코드 자체로 번식하는 유형을 말하며 주로 PC상에서 실행되는 악성 프로그램

4) 인터넷에 연결된 일련의 시스템들을 이용해 단일 사이트에 대해 서비스 거부 공격(DoS) 공격을 시도하는 것이다. 해커들이 일단 취약한 인터넷 시스템에 대한 액세스에 성공하면 침입한 시스템에 소프트웨어를 설치하고 이를 실행시켜 원격에서 공격을 개시하는 방법을 이용한다.

5) 컴퓨터 프로그램이나 실행 가능한 부분을 변형하여, 여기에 자기 자신 또는 자신의 변형을 복사하여 컴퓨터 작동에 피해를 주는 명령어들의 조합



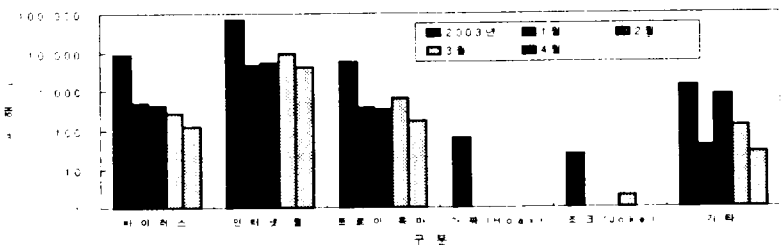
(그림 1) DDoS 해킹 공격의 예



(그림 2) 2002년과 2003년의 해킹 유형 분류

크게 증가된 것을 볼 수 있다. 그러므로 인터넷이라는 공간에서 실행되는 온라인 게임의 특성상 DDoS 공격과 바이러스에 의한 공격을 예방해야 한다.

(그림 3)은 2003년부터 2004년 4월까지 바이러스에 의한 피해 분석이다[10]. 2003년도와 2004년도 현재까지 인터넷 웜 바이러스로 인한 피해가 가장 많은 것을 알 수 있다. 따라서, 인터넷 웜에 대한 각별한 보안이 필요함을 알 수 있다[10].



(그림 3) 2003년부터 2004년 4월까지의 바이러스 피해 분석

〈표 2〉는 2004년도 4월에 KrCERT에 접수된 공격 수법에 따른 해킹 유형이다[10]. 네트워크 자원 또는 서버의 구성 설정 오류와 악성 프로그램[6], 그리고 취약점 정보 수

6) 사용자가 컴퓨터를 정상적으로 사용하지 못하게 방해하는 프로그램으로 웜, 바이러스, 트로이 목마 등이 포함된다.

집을 통해 가장 많이 공격했다는 것을 알 수 있다[10]. 그러므로 네트워크 자원 또는 서버에 대한 취약점을 보완하는 작업은 온라인 게임 보안에서 중요할 수 있다.

〈표 2〉 공격 유형에 따른 해킹 피해

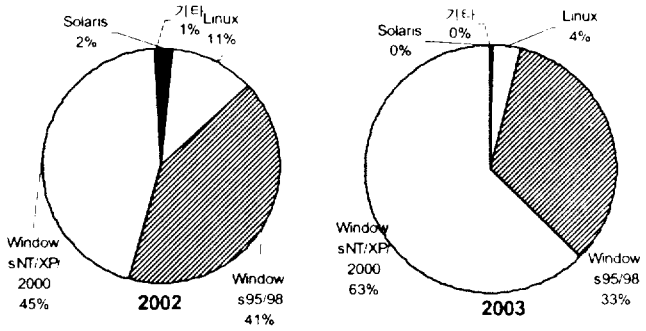
구 분	건 수	비 고
사용자 도용	3	개인 사용자 계정 도용
S/W 보안 오류	0	-
버퍼 오퍼플로우 취약점	1	SNMP, Named/Bind취약점 이용
구성 설정 오류	36	사용자 권한 설정 오류
악성 프로그램	1,066	윈도우즈 트로이 목마 등
프로토콜 취약점	0	-
서비스 거부 공격	0	-
E-mail 관련 공격	0	스팸 릴레이 등 스팸메일 관련 공격
취약점 정보 수집	1,083	named/bind,ftpd,rpc,LSASS
사회 공학	1	-
총 계	2,190	

〈표 3〉은 대표적인 해킹 사례와 경향의 변천을 보여준다[9]. 단순한 개인 지식의 과시에서 도구를 이용하거나 특정한 공격 대상을 선정하여 공격하는 유형으로 변화되고 있다.

〈표 3〉 해킹 사례와 경향의 변천

년 대	대표적인 해킹 사례	해킹의 경향
1980년대	1988년 모리스 웜	개인지식의 과시/실험, 자기 복제 기술 이용, 컴퓨터의 가용성 파괴
1990년대	1990년 캐빈 폴슨의 전화망 해킹 1995년 캐빈 미트릭 신용정보 해킹	개인지식의 과시/경제적 이득, 특정 대상을 향한 해킹
2000년대	네트워크와 운영체제에 대한 약간의 기술적인 지식을 갖고 있는 해커	개인지식의 과시/특정 대상을 향한 해킹, 게임 사이트, 이웃집 등을 자동화된 툴을 이용, 취약점 분석 도구등
2003년	1월 Slammer 웜 8월 MS-Blast 9월 Sobig-F	개인 지식의 과시, 불특정 다수를 대상, 자기 복제 기술, 자동화된 공격 대상 선정, 해킹+웜의 형태

(그림 4)는 해킹 피해 OS별 분류이다[9]. 2002년도와 2003년도에는 MS SQL 및 RPC 취약점이 집중적으로 부각된 마이크로 소프트웨어사에서 개발된 윈도우즈 95/98/NT/2000/XP에 대한 피해가 많이 발생되었다. 그러므로 마이크로 소프트웨어사에서 개발한 윈도우즈 운영체제에 대한 보안은 필요하다.



(그림 4) 2002년도와 2003년도의 해킹 피해에 대한 OS별 분류

〈표 4〉는 KrCERT에 접수된 월별 해킹 피해이다[5]. 일반 해킹은 전월의 1,946건에서 918건으로 절반 이상 감소하였으나 웜에 의한 신고 건수는 715건에서 1,437건으로 급증하였다. 스팸 릴레이[7]는 전월의 43건에서 89건으로 증가되었지만 2004년에 감소되고 있음을 보여준다.

〈표 4〉 2003년도와 2004년도 현재까지 월별 해킹 피해

구 분	2003	2004			
		1월	2월	3월	4월
일반 해킹	13,184	1,408	1,589	1,946	918
일반 웜	4,719	45	45	715	1,437
스팸 릴레이	8,276	617	326	43	89
합 계	26,179	2,070	1,960	2,704	2,444

7) 발신자가 자신과 아무런 관계가 없는 수신자에게 발송하는 전자 메시지를 보안이 허술한 PC방이나 학교에 설치된 서버를 통하여 불법적으로 불법 광고물을 유포하는 것을 말함

3. 온라인 게임의 보안 대책

현재 온라인 게임에 대한 해킹은 보다 지능적이고 조직적인 해킹 방법을 사용하고 있으며 경제적인 이득 또는 개인의 실력 과시를 위한 목적으로 해킹을 하고 있다. 그러므로 게이머 또는 게임 개발 회사의 경제적인 가치를 보존하기 위해서는 해킹에 대한 적절한 보안 대책을 강구해야 한다.

3.1 아이템 해킹에 대한 보안 대책

(1) PC방 해킹 방지 시스템 구축

현재 전국적으로 2만여곳에 달하는 PC방은 국내 온라인게임 산업의 근간을 이루고 있지만, 해킹이 만연하고 있다. 특히 이러한 해킹은 타인의 아이템을 불법으로 취득하여 매매하기 위한 수단이 되므로, 이대로 방치할 경우 게임 서버에 대한 해킹 가능성도 있어 사이버 범죄 온상으로 PC방이 전락될 수 있다. 따라서, PC방 관련단체 및 게임제공업체 공동으로 해킹 방지 시스템을 만드는 대책이 필요하며, 특히 해커들의 게임 서버에 대한 침투를 방지하기 위한 자체 방화벽 및 전송보안 체계도 마련하여야 한다.

(2) 해킹 툴 감지 프로그램 운영

실시간 해킹 감지 및 차단 프로그램에는 게임 자체에 대한 해킹이나 변칙적인 게임 진행을 막아주고, 해킹 툴 탐지 및 차단 프로그램 파일을 위조하거나 변조하는 것을 방지하거나 메모리 해킹 방지, 스피드 핵 방지, 디버깅 방지, 오토 마우스 방지, 자체 프로그램 보호 등의 기능을 가지고 있어야 한다. 대표적인 예는 안철수 연구소에서 개발한 온라인 게임용 해킹 차단 솔루션인 핵 실드와[11], 잉카 인터넷에서 개발한 PC 보안 솔류션 엔프로텍트이다[12].

(3) 게이머의 컴퓨터에 방화벽 설치

게임 프로그램을 내려 받을 때 게이머의 PC에 설치되고 이후에 온라인 게임을 시작할 때마다 자동으로 실행되는 개인용 방화벽 프로그램을 제공한다. 대표적인 예로는 안철수 연구소의 게임용 마이파이어월이 있다[13].

3.2 네트워크, 서버 해킹에 대한 보안 대책

온라인 게임은 인터넷에서 실행되므로 온라인 게임 서버로부터 게이머까지의 네트워크 트래픽이 정상적이어야 한다. 따라서 네트워크와 네트워크 자원의 보안이 필요하며 이를 위해 다음과 같은 요소가 충족되는 것이 바람직하다[6,7].

● **네트워크와 네트워크 자원에 대한 보안 대책**

(1) 네트워크 지연 시간이 중요한 게임 트래픽과 기타 트래픽을 분리

네트워크 지연 시간이 중요한 게임 트래픽과 그렇지 않은 데이터에 대한 트래픽의 회선 및 라우터를 분리하여 라우터의 보안에 대한 부담을 감소시킨다.

(2) 라우터에 대한 접근에 대한 보안 강화

라우터 접근에 대한 AAA(Authentication, Authorization, Accounting)를 통하여 인증, 권한, 로깅을 시행하여 라우터 자체에 대한 보안을 강화한다

(3) 네트워크 자원들에 대한 지속적인 업그레이드

보안 관련 문제가 발견되고 그에 대한 IOS[8]가 발표되면 검증을 통하여 단계적인 업그레이드를 한다.

(4) 별도의 제어망 구축

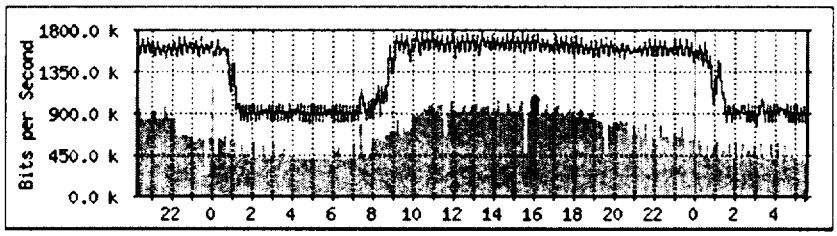
인터넷은 전화망에서 사용하는 것과 같은 신호 네트워크를 별도로 가지지 않고 일반 정보나 제어 정보 모두 동일한 네트워크를 통해 전달되기 때문에 트래픽 폭주와 같은 비상 상황이 발생하여 네트워크에 긴급 조치가 필요한 경우 긴급 제어 정보를 효과적으로 전달할 수 있는 방법이 없어 네트워크의 장애 상태의 회복을 어렵게 만든다. 따라서 현재의 인터넷 통신 구조를 유지하면서 제어 정보를 효과적으로 전달할 수 있는 논리적인 네트워크를 인터넷에 도입할 필요가 있다.

(5) MRTG[9]를 통하여 정상 상태에 대한 수준을 정확히 파악

백본 주요 구간 및 ISP 회선에 대한 pps[10], bps[11]를 측정하여 시각적으로 볼 수 있도

8) internetworking operating system으로 네트워크 운영체제를 말한다.
9) Multi Router Traffic Grapher로써 네트워크 트래픽을 실시간으로 모니터링 하는 툴이다.
10) packet per second로써 1초에 몇 개의 패킷을 처리하는지를 나타낸다.
11) bit per second로써 1초당 몇 개의 비트를 처리하는지를 나타낸다.

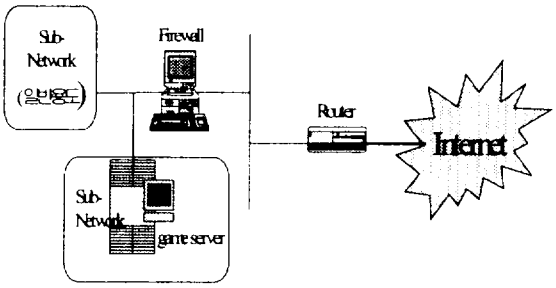
록 MRTG를 사용하여 상시 모니터링을 시행하고 최고, 최저, 평균등의 정상 서비스 상태를 파악하고 있으면서 이상 징후가 발견될 때를 발견하도록 한다. (그림 5)는 MRTG의 예이다[17].



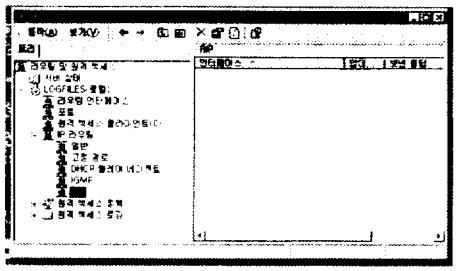
(그림 5) MRTG의 예

(6) Backend network를 구성

게임 서버와 통신을 필요로 하는 시스템들은 인터넷과 분리된 내부 네트워크로 구성하여 연결한다. 내부 네트워크가 복잡해지고 서브넷이 많이 추가된다면 서버에서 라우팅 관련 서비스를 활성화 시켜서 라우팅 정보를 전달한다. (그림 6)은 Backend network의 예이다. 일반적으로 온라인 게임과 관련없이 인터넷에 접속하여 수행되는 서브넷과 게임 서버의 서브넷을 분리하여 게임 서버가 포함된 서브넷에 열려져 있는 포트 또는 프로세스의 기능을 최소화 시킴으로써 보안 기능을 강화한다. (그림 7)은 윈도우 XP에서 라우팅 관련 서비스를 활성화 시키는 그림이다.



(그림 6) Backend network의 예



(그림 7) 윈도우 XP에서 라우팅 관련 서비스를 활성화

(7) 루트 네임 서버의 한국내 유치

국제 회선 장애로 인한 국내 네임 서버의 장애를 예방하기 위해 루트 네임 서버의

국내 유치가 필요하다. 현재 루트 네임 서버는 미국 10개, 유럽 2개, 일본 1개이다. 이는 인터넷 망의 공격에 의해 해외 네트워크가 마비되었다 하더라도 루트 서버가 국내에 있다면 정상적으로 외국에 대한 게임 서비스를 지속할 수 있기 때문이다.

● 악성 프로그램의 보안 대책

악성 프로그램은 해당 게이머의 PC 또는 게임 서버로부터 게이머까지의 네트워크 경로에 있는 자원들을 공격하여 온라인 게임의 정상적인 실행을 방해할 수 있으므로 악성 프로그램에 대한 보안은 필요하다.

(1) 주기적인 시스템 업데이트와 보완 업데이트[12,14].

윈도우즈 계열의 운영체제를 사용하는 게임 업체는 MS와 각종 보안 사이트에서 발견되는 각종 버그와 바이러스에 대한 정보를 획득하고 이에 대해 패치를 수행한다. 또한 서버 관리자 및 일반 게이머의 PC에 보안인식을 제고하여 보안 패치, 백신 업데이트 등 보안 활동을 생활화해야 한다.

(2) 잠재적으로 문제를 야기할 수 있는 설정들 점검[15]

최근 제작되고 있는 악성코드들은 운영체제나 응용프로그램등에서 사용자의 편리를 위해 제공되는 기능들을 악용해, 사용자의 개입 없이 자동으로 실행되는 경우가 많다. 그러므로, 잘못된 설정으로 인해 게이머의 의지와 상관없이 악성코드에 의한 피해를 야기할 수 있으므로 설정을 점검하여 활성화를 막을 필요가 있다. 이것은 자동으로 스크립트를 실행시키는 연결 프로그램을 수정하거나 파일 확장자의 숨김 기능 등을 비활성화하여 트로이 목마의 공격이나 E-mail 바이러스등 에 대한 공격을 예방하는 조치이다.

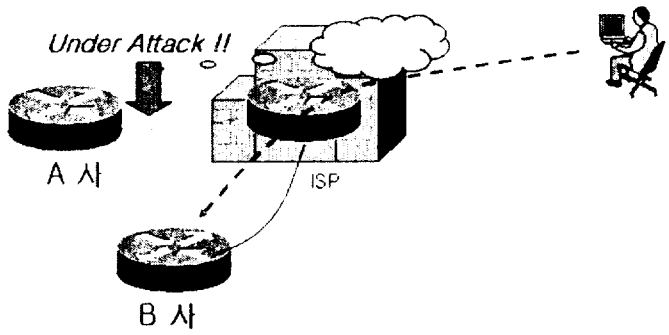
3.3 프로세스 보안 대책

서버 또는 네트워크가 해킹을 당했을 경우 게임 업체간 협조가 필요하며 이를 복구할 때는 정해진 절차를 수행하는 것이 바람직하다[6,12,14].

(1) 게임업계 네트워크 관리자들간의 네트워크를 구축

해킹 또는 바이러스가 발생되면 게임 업계의 네트워크 관리자들간의 신속한 정보와

대책 공유를 통하여 심각한 서비스 중단 사태를 미연에 방지해야 한다. (그림 8)은 A사가 공격을 받는 경우 같은 ISP를 사용하는 B사에도 영향을 끼침을 보여준다. 그러므로 A사에서 공격을 받는 경우 같은 ISP를 사용하는 B사 또는 관련 업체에게 신속하게 이 사실을 알려 대책을 강구할 수 있도록 해야 한다.



(그림 8) A사가 공격받을 때 같은 IPS를 사용하는 B사도 영향을 받는 경우

(2) 표준 설치 가이드와 체크 리스트를 유지

각 게임업체의 특성과 환경에 적합한 시스템의 표준 설치 가이드를 작성하고 각 시스템이 설치될때 반드시 체크 리스트를 이용하여 각각의 항목들을 점검하여 엔지니어의 경험에 의존하여 누락될 수 있는 보안 위협 요소를 최소화해야 한다.

(3) 필요에 따라서 각종 자료에서 권고하는 보안 사항을 적용

각 운영체제, 라우터와 같은 네트워크 장비, 그리고 서버에 관한 보안 교육 및 권고사항을 주기적으로 점검하고 이에 대한 보안 사항을 보완한다.

(4) 보안 전문가 인력 풀(Pool)을 운영

인터넷 망의 침해 사고 발생시 긴급하게 대응하고 효과적인 사후 처리를 위해 산업체, 학교, 연구소등의 전문가 풀을 운영한다.

3. 결론 및 추후 연구 방향

본 논문에서는 온라인 게임에서 발생될 수 있는 아이템을 해킹하거나 네트워크 또는 서버를 해킹하는 경우를 살펴보고 이러한 해킹을 막기 위한 보안 대책으로 아이템에 대한 보안 대책, 네트워크 또는 서버에 대한 보안 대책, 그리고 프로세스적인 보안 대책을 기술하였다. 아이템에 대한 해킹의 보안 대책에는 PC방 해킹 방지 시스템 구축, 해킹 툴 탐지 프로그램 운영, 그리고 게이머의 컴퓨터에 방화벽을 설치하는 것이 있다. 그리고 네트워크 또는 서버에 대한 보안 대책에는 라우터 및 네트워크 자원에 대한 별도의 제어망과 IOS의 지속적인 업그레이드, MRTG를 사용하여 정상적인 트래픽 상태등에 대한 파악이 있다. 프로세스적인 보안 대책에는 게임업계 네트워크 관리자들간의 네트워크를 구축, 윈도우즈 및 바이러스 보안 업데이트, 그리고 표준 설치 가이드와 체크 리스트와 권고 보안 사항등이 있다. 현재 해킹 기술은 점점 지능화되고 있기 때문에 이를 막기 위한 보안 대책 또한 계속적으로 연구해야 한다. 추후에는 온라인 게임에서 발생되는 해킹 사례를 분석할 예정이다.

《참고문헌》

[1] 이택수, 온라인 게임 크래킹 비상, 디지털 타임즈, 2003. 2. 4.
[2] 김동균, 온라인 게임 보안 강화, 2003. 3. 18
[3] 정동영, 온라인 게임 실태, 소비자 시대, 2000. 9.
[4] 송재명, 온라인 게임 업체 해킹 프로그램으로 골머리, 해커뉴스, 2004. 1. 4.
[5] 국순신, 스타크래프트' 이용자 '맵핵' 찾기에 분주, 아이뉴스24, 2004. 6. 7
[6] http://www.game.or.kr/infobank/data/515_온라인 게임 보안
[7] 유병수, 게임사이트에 대한 해킹 수법과 대책, 전자신문, 2001. 9. 27
[8] 양대일, 이승재, 정보 보안 개론과 실습, 한빛 미디어, 2003. 1277
[9] 심원태, 2003년 인터넷 침해 사고 유형 분석, 한국 정보 보호 연구원, 정보 보호 뉴스, 2003. 12

[10] 김승철, 4월 해킹 피해 통계와 주요 특징, 한국 정보 보호 연구원, 정보 보호 뉴스, 2004. 6

[11] 박희진, 안철수연, 팡야 게임 보안 맡는다, 머니투데이, 2004. 6. 23

[12] 박치항, 인터넷 침해 대응을 위한 제언, 정보처리학회 학회지, 2003. 3.

[13] 안연구소, 게임과의 동거... 눈에 띄네, 머니투데이, 2003. 10. 9

[14] 정태명, 인터넷 침해사고 원인과 대책, 정보처리학회 학회지, 2003. 3

[15] http://kin.naver.com/browse/db__detail.php?dir__id=106&docid=35033

[16] http//opendic.naver.com/100/entry.php?entry__id=103316

[17] http://www.stat.ee.ethz.ch/mrtg