온라인 게임의 사설서버 피해와 방어

배정일*, 오상석**, 민성기**
*고려대학교 컴퓨터정보통신대학원 소프트웨어공학과
**고려대학교 컴퓨터 전파통신공학과
e-mail : jungila@korea.ac.kr, ssoh94@korea.ac.kr, sgmin@korea.ac.kr

Damage and Defense of Online game private servers.

Jung-Il Bae*, Sang-Seok Oh**, Sung-Gi Min**
*Dept. of Software Engineering, Computer Information and Communications, Korea University
**Dept. of Computer & Radio Communications Engineering, Korea University

요 약

사설서버는 개발사의 동의 없이 게임 서버를 제작 및 운영 하여 게임에 대한 저작권 침해와 서비스의 권리 없이 영리나 비영리 목적으로 단체 또는 개인이 온라인 게임을 즐길 수 있도록 서비스 하는 행위 또는 서버 자체를 뜻한다. 본 논문에서는 이러한 사설서버에 대한 기술적인 대응 방법인 사설서버 방어코드에 대해서 제안 한다. 본 연구는 사설서버로 인한 게임 개발사의 피해와 사설서버에 대한 방어 방법, 그리고 실제 온라인 게임에 사설서버 방어 기술을 도입한 후 사설서버 방어의 효과에 대해서 조사를 한다.

1. 서론

사설서버는 정상적으로 온라인 게임을 서비스하는 운영사의 서버가 아닌 다른 목적으로 만들어서 개인 또는 일부 집단이 이용하는 서버를 의미 한다. 이러한 사설서버는 기존 게임의 기획 의도와 다르게 컨텐츠의 내용을 다른 내용으로 바꾸거나 경험치, 게임머니등을 많이 지급 하면서 기존의 정상적으로 서비스를 하는 온라인 게임에 지루함을 느낀 이용자들로 하여금 사설서버로 몰리게 하고 있다. 또한 일부 사설서버의 경우는 실제 돈을 목적으로 유료로 운영 하거나 게임 아이템이나 게임 머니를 실제 돈으로 판매하는 행위도 이루어 지고 있다. 이로 인해서 정상적으로 서비스 하는 운영사의 서버에는 이용자 수가 줄어 든다. 그래서 운영사의 매출을 감소시키고 저작권을 침해 하는 등 영업방해를 하게 된다.

본 논문에서는 사설서버의 운영 방식을 분석하고 사설서버에 접속 하지 못하도록 클라이언트에 사설서버 방어코드를 설계 및 구현한다. 그리고 사설서버 방어코드를 변조 할 수 없도록 코드 가상화 기술에 대해서 이야기를 한다. 마지막으로 사설서버 방어코드를 실제 온라인 게임에 반영하였을 때 실제 운영중인 불법 사설서버의 변화에 대해서 분석 한다.

2. 관련 연구

2.1. 사설서버 현황

사설서버는 프로그램 언어에 대한 지식 및 네트워크 관련된 지식이 부족하더라도 특정 프로그램만 다운로드 받아서 설치하면 사설서버를 쉽게 만들 수 있다는 점에서 큰 문제가 되고 있다. 인터넷에서 "프리 서버" 라고 검색하면 쉽게 많은 블로그를 검색할 수 있다. [1]

<표 1> 주요 인터넷 포털사이트의 "프리서버" 검색어 검색 결과

구분	검색 건수
Naver	284,686
Daum	12,199
Nate	28,207
Yahoo	101,219
Paran	4,042

<표 2> 주요 인터넷 검색 포털사이트의 'A 게임 프리서버' 검색결과 게시물 수

구분	지식검색	블로그/카페	웹문서	계
Naver	19,626	2,969	17,069	39,664
Daum	186	496	29,300	29,982
Nate	642	6,182	905	7,729
Yahoo	718	6,662	44,100	51,480
Paran	162	464	14,841	15,467

인터넷 뉴스에 따르면 이러한 사설서버로 인해 게임 운영사의 피해는 연간 약 15000 억원대라고 추정하고 있다. 예를 들어 엔씨소프트의 자체 조사 결과 '리니지' 불법 사설서버의 경우는 약 330 개가 넘고 회원 수는 15 만명이라고 공개하였으며, 이를 금액

으로 환산 하면 200 억원 정도로 '리니지' 전체 매출의 약 8.5% 가 된다고 한다. 이러한 운영사의 매출에 영향을 미치는 것 뿐 아니라 운영자가 기획한 게임 내용을 임의로 수정하여 폭력성과 선정성 수위를 높이고 성인용 게임도 무방비로 노출이 되어 있다는 점이 큰 문제가 되고 있다. 조작된 온라인 게임 속의 캐릭터는 서로 전투를 하거나 전투 도중에 피가 보이며, 여성 캐릭터의 경우 반라 또는 심하면 전라로 등장 하는 경우도 있다. [2]

대한민국 저작권법상 사설서버로 온라인 게임 운영이 적발되면 5 년 이하의 징역 또는 2 천만원 이하의 벌금형에 처하도록 규정이 되어 있으나 사설서버는 국내와 해외에서 계속해서 그 수가 증가 하고 있으며, 특히 외국의 경우는 사설서버에 대한 법적 대응을 하기에 어려움이 있어 제대로 된 대처가 이뤄지지 않고 있다.

2.2. 사설서버 분석 및 방어 대책

온라인 게임을 일반적으로 서버와 클라이언트 구조로 이루어 진다. 온라인 게임의 특성상 대부분 컨텐츠와 리소스는 클라이언트에 포함이 되어 유저에게 배포된다. 정상적으로 배포된 클라이언트에서 리버스 엔지니어링을 통한 코드분석 및 리소스파일 암호해독을 통한 데이터 추출, 그리고 클라이언트가 서버로 전송 하는 패킷(packet) 을 분석하여 사설서버가 제작되게 된다.

클라이언트에는 서버의 IP 또는 DNS 가 소스코드 또는 데이터 파일에 포함되는 경우가 많은데 리버스 엔지니어링 툴 등을 이용하여 IP 를 변경하거나, 프록시(proxy) 서버 또는 게이트웨이(gateway) 에서 정식 서비스를 하는 서버로 접속하는 IP 를 임의로 변경하여 사설서버에 접속하도록 제작한다. 변경된 코드 또는 불법프로그램을 일반유저에게 배포하여 정상적으로 다운로드 받은 클라이언트에 적용을 하게 되면 쉽게 일반유저도 사설서버에 접속을 하게 되는 것이다.

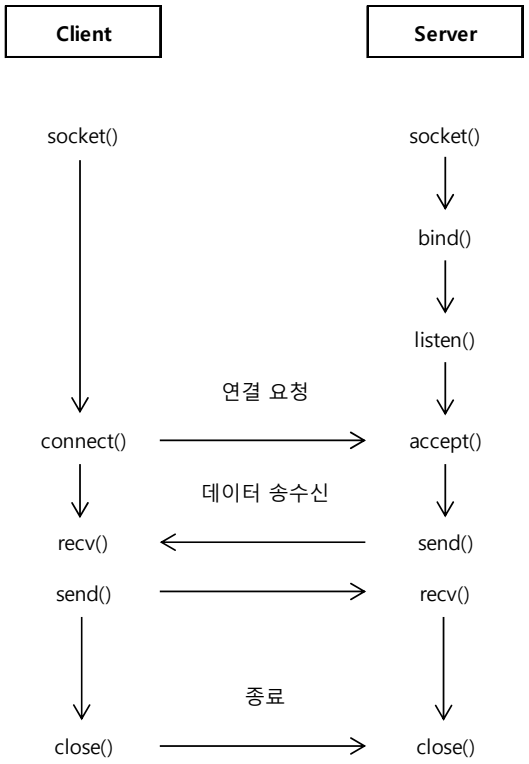
본 연구에서는 클라이언트가 서버로 접속하여 통신하는 과정에서 접속하고 있는 서버의 IP 를 분석 하여 운영사에서 정식으로 서비스하는 서버가 맞는지 주기적으로 검사를 한다. 만약에 사설서버로 접속이 되어 있는 경우는 클라이언트를 강제 종료하여 사설서버에서 게임을 할 수 없도록 사설서버 보안코드를 구현한다. 하지만 사설서버 보안코드도 리버스 엔지니어링을 통해 우회가 될 수 있기 때문에 코드 가상화 작업으로 사설서버 보안코드를 다시 한번 보호한다. 보호된 코드를 변경 할 경우 클라이언트가 정상적으로 실행이 되지 않도록 대응 한다.

3. 사설서버 방어코드 구현 및 코드 보호 적용

3.1. 사설서버 방어코드 구현

일반적으로 게임 클라이언트에서 서버로 먼저 접속하고 데이터 송수신을 하게 된다. 클라이언트 코드에서 접속 하고자 하는 서버의 IP 를 변경하여 사설서버로 접속하게 되는데 클라이언트가 서버로 접속 하고 있는 소켓(socket)의 정보를 추출 하여 정상적으로 운영사에서 서비스하고 있는 서버가 아니라면 클라이언트를 비정상 종료시켜 사설서버에 접속을 차단 하고자 한다.

클라이언트에서 소켓(socket)을 이용하여 서버에 접속 및 데이터 송수신을 하는 순서는 다음과 같다.[3]



(그림 1) 클라이언트 서버 통신에 사용되는 함수 호출

여기서 두 곳에 사설서버 방어코드를 도입하고자 한다. 하나는 connect() 함수가 호출이 될 때 정상적인 IP 로 연결하는지 체크하고, 또 하나는 데이터 송수신을 하는 과정에서 주기적으로 정상적인 IP 로 연결이 되어 있는지 체크를 한다. 주기적으로 하는 이유는 패킷 전송할 때 마다 체크를 한다면 속도 저하 문제가 발생할 수 있기 때문이다.

소켓(socket) 통신에서 연결된 IP 확인을 하는 방식은 getpeername() 이라는 함수를 이용 하면 확인이 가능 하다. getpeername() 함수는 소켓이 연결되어 있는 원격지 상대방(peer)의 이름(인터페이스 어드레스와 포트번호)를 얻을 수 있는 함수 이다. 함수의 구성은 다음과 같다. [4]

<표 3> getpeername 함수 인자

```
int getpeername(
    _In_      SOCKET s,
    _Out_     struct sockaddr *name,
    _Inout_   int *namelen
);
```

그럼 getpeername() 함수를 이용하여 원격지의 IP 와 Port 를 얻을 수 있는 방법을 예제 코드를 통해 확

인해보자.

<표 4> 사설서버 검출 예제 코드

```
struct sockaddr_in peer;
int peer_len;
peer_len = sizeof(peer);
if (getpeername(hsock, reinterpret_cast<SOCKADDR*>(&peer), &peer_len) == -1)
{
        perror("getpeername() failed");
        return -1;
}

DWORD dwAddr = peer.sin_addr.s_addr;
BYTE* pByte = (BYTE*)&dwAddr;

if ( *pByte == 14 && *(pByte+1) == 52 && *(pByte+2) == 209 ) {        // Server IP 대역 14.52.209.xxx
        dwAddr = 0;
}
else {
        CLEAR_STACK;
}
```

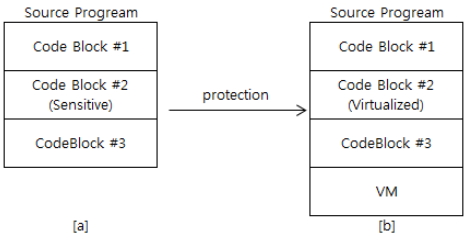
getpeername() 함수를 이용하여 소켓(socket) 핸들인 hsock 을 인자로 받고, SOCKADDR 구조체를 얻어 온다. 그리고 상대방의 인터페이스 어드레스를 얻어와서 비교하여 정상적인 서버인지 확인한다. 일반적으로 MMORPG 의 경우는 여러 대의 서버를 사용하고 있으며, IP 는 C Class 로 구성이 되어 있는 경우가 많다. 그래서 IP 주소를 바이트(Byte)단위로 분리하여 IP 대역으로 체크한다.

예제 코드에서는 14.52.209.xxx 대역의 서버에만 접근이 가능 하도록 처리하였다. 그 외에 IP 인 경우는 CLEAR_STACK 을 통해 클라이언트가 비정상 종료가 되도록 하였다.

하지만 일반적으로 클라이언트는 유저에게 배포 되고 사설서버 보안코드는 리버스 엔지니어링을 통해 쉽게 우회가 될 수 있다. 그래서 이러한 사설서버 보안코드를 코드 가상화 기술을 이용하여 쉽게 변조 할 수 없도록 보호한다.

3.2. 코드 가상화

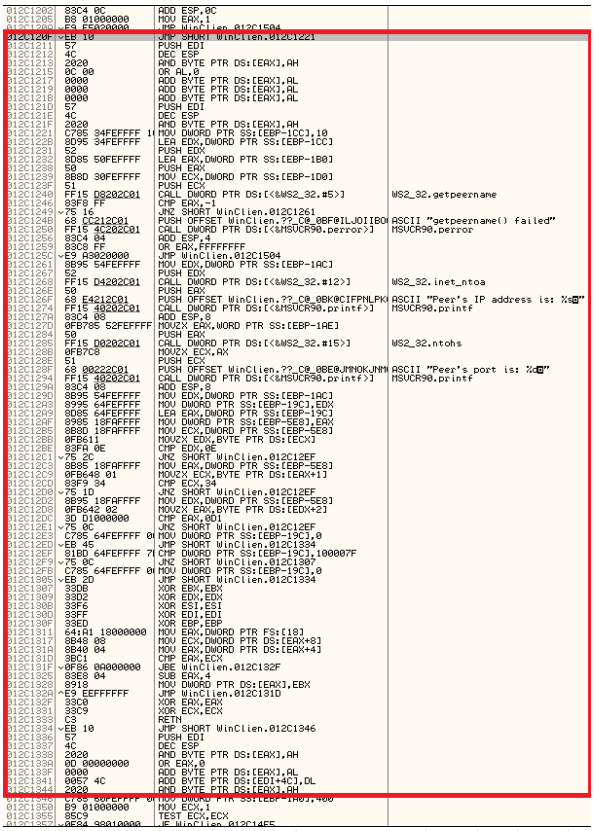
코드 가상화란 프로그램의 주요 코드 영역 (Sensitive Code Block) 을 리버스 엔지니어링으로 부터 보호하기 위해, VM 만이 해석할 수 있는 가상화된 코드 영역 (Virtualized Code Block) 으로 변환하는 기술이다. 변환은 런타임에 이루어 지는 것이 아니라 그 이전에 이루어 지기 때문에 일반적인 디스어셈블러로는 해석을 할 수 없다. 변화된 코드 영역의 해석 및 실행은 CPU 대신 VM 이 처리하게 된다. [5][6]



(그림 2) 코드 가상화를 이용한 변환과정

<표 4> 에서 작성한 예제 코드는 리버스 엔지니어링 툴을 이용하여 확인하면 (그림 3)과 같이 어셈블리어 코드를 볼 수 있다. 어셈블리어 코드를 수정하면 사설서버 보안코드를 우회 할 수 있다. 하지만 가상화 기술을 도입한 이후 일반적인 디스어셈블러로는 해석 할 수 없기 때문에 리버스 엔지니어링 툴을 이용하더라도 어셈블리어 코드 변경이 불가능하게 되어 사설서버 방어에 효과적이다.

코드 가상화를 하는 프로그램은 유료, 무료 여러 가지가 있지만 실제 현업에서 사용하고 있는 데미다 (Themida) 프로그램을 이용하여 코드 가상화를 하였다. 코드 가상화를 하게 되면 코드분석 및 변조하기에 많은 시간이 소요 되어 해커들로 하여금 사설서버 제작을 방해 할 수 있다.



(그림 3) 리버스 엔지니어링 툴을 이용한 어셈블리어

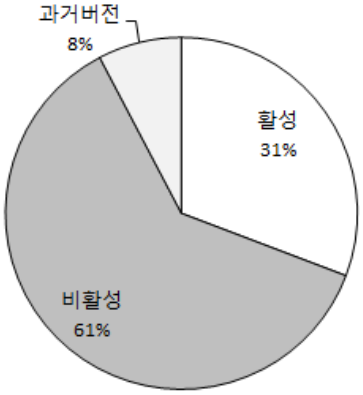
4. 결과

사설서버 방어코드를 도입 후 실제 사설서버의 운영 상태를 모니터링 하였다. <표 5> 자료를 실제 미국에서 서비스 중인 M 게임의 불법 사설서버 운영상태를 모니터링 하여 사설서버 방어코드를 도입 후 변화되는 현황을 보고한 내용이다.

모니터링 대상 사이트는 총 13 개의 사설서버이며, 사설서버 방어코드가 도입 된 후 모니터링을 한 결과 8 개의 사설서버는 더 이상 운영이 되고 있지 않음을 확인 할 수 있었으며, 활성화 되어 있는 사설서버에도 과거 사설서버 방어코드가 도입이 되지 않은 버전의 클라이언트가 이용 되는 것으로 확인되어 실제로 최신 클라이언트로 운영 되는 사설서버는 총 4 개인 것을 확인할 수 있었다.

< 표 5 > 사설서버 방어코드 도입 후 현황

활성화 서버	현황	상태
CelinoSEA (MSEA v.115.2)	웹사이트는 지속적으로 접속이 불가하지만, 게임서버는 활성화 상태입니다.	활성
ExtaliaMS (GMSv.116.1)	게임서버가 활성화 상태이며 웹사이트가 재오픈 된 상태입니다. 게임서버가 v.1161로 업데이트 진행 완료되었습니다.	활성
Zakura MS (GMS v.83/v.115.1)	게임서버가 활성화 상태이며 웹사이트도 접속 가능한 상태입니다.	활성
AncientMESA (GMS v.116..1)	게임 서버가 활성화 상태이며 웹사이트도 접속 가능한 상태입니다.	활성
Exiled MS (GMS v. 114)	게임 서버가 비활성화 상태이며 웹사이트도 접속이 불가능한 상태입니다.	비활성
HydraMS (GMS v.83.1) (Rydah Reborn)	게임 서버가 활성화 상태이며 웹사이트도 접속 가능한 상태입니다. Rydah Reborn 전 버전인 RydahMS 서버가 공식 런칭될 예정이라고 운영자가 페이스북에 발표했습니다.	과거버전
AlchemySea (MESA v.120)	게임 서버는 활성화 상태이며 웹사이트는 복구중입니다.	비활성
My-th story (GMS v.111)	서버는 확인불가 상태이며 웹사이트 또한 접속이 불가합니다.	비활성
Aura MS (MSEA v.106)	포럼이 접속이 되고 있지 않습니다. 서버가 비활성화 상태입니다.	비활성
Bankai (v.55)	포럼이 접속이 되고 있지 않습니다. 서버가 비활성화 상태입니다.	비활성
Pocky MS (v.75)	포럼이 접속이 되고 있지 않으며, 서버 또한 비활성화 상태입니다.	비활성
Arcane MS (GMS v.111.2)	포럼이 접속이 되고 있지 않으며, 서버 또한 비활성화 상태입니다.	비활성
CrypticSEA(MSEA v.118.2/v.119.2.)	포럼이 접속이 되고 있지 않으며, 서버 또한 비활성화 상태입니다.	비활성



(그림 3) 사설서버 모니터링 결과

위 그래프로 볼 수 있듯이 간단한 사설서버 방어코드이지만 절반이상의 사설서버가 비활성화 되거나 사설서버 방어코드가 도입이 되지 않은 과거 배포된 클라이언트로 서비스 하고 있음을 확인 할 수 있었다.

그러나 일부 사설서버에서는 사설서버 방어코드를 우회하여 아직까지도 서버 운영 하고 있다. 이를 해결 하기 위해 운영 중인 사설서버를 분석 하고 지속적으로 사설서버 방어코드를 개선해야 한다.

5. 결론

현업에서는 사설서버에 대해서 법적 대응을 우선시 하는 경우가 많았다. 하지만 법적 대응을 하기 위해서는 증거자료와 수사 과정이 필요 하기 때문에 많은 시간이 소요 된다. 그 사이에 개발된 컨텐츠 및 리소스가 유출 되고 유저는 게임을 떠나게 되어 게임 운영사는 금전적으로 많은 피해를 입고 있다.

본 논문에서는 게임 운영사의 피해를 최소화 하기 위해서 클라이언트에 사설서버 방어코드를 구현하였으며 사설서버 방어코드를 코드가상화 기술로 다시 보호하여 우회되는 경우를 최소화 하였다. 실제 온라인 게임에 적용 후 약 70% 정도의 사설서버가 서비스를 중단하였다. 이로 인해 사설서버 방어코드가 효과가 있었다는 것을 확인 할 수 있었다. 아쉽게도 일부 사설서버에서는 사설서버 방어코드를 우회하여 계속해서 서비스 하고 있다. 서비스 중인 사설서버를 차단하기 위해서 지속적으로 사설서버 방어코드를 개선 할 예정이다.

6. 참고 문헌

[1] 한국게임산업협회, http://www.gamek.or.kr/
[2] 장동준, “온라인 게임의 독버섯 불법 서버”, 전자신문, 2007
[3] 박대우, 서정만, “TCP/IP 공격에 대한 보안 방법 연구”, 한국컴퓨터정보학회, 2005
[4] MSDN, “getpeername function “, http://msdn.microsoft.com
[5] 김정일, 이은주, “유전 알고리즘에 기반한 코드 난독화를 위한 인라인 적용 기법”, 한국 IT 서비스학회, 2011
[6] 이용일, “Design and Implementation of Virtualized Code Protection(VCP) For Anti-Reverse Engineering”, 2008