Journal of Korea Multimedia Society Vol. 12, No. 8, August 2009(pp. 1120-1127)

게임 서비스 보호를 위한 소프트웨어 위변조 방지기술 연구

장항배[†], 강종구[††], 조태희[†††]

요 약

게임 산업의 급격한 성장과 사회적 영향은 그에 비례하여 게임 서비스의 취약성을 공격하는 침해사고 건수는 지속적으로 증가하고 있다. 하지만, 게임서비스 역기능 방지를 위한 차별화된 정보보안 기술연구는 아직 미진한 상태이다. 따라서 본 연구에서는 현재 서비스되고 있는 온라인 게임서비스에 대한 침해현황을 조사하고, 가장 큰 보안 취약점으로 도출된 게임서비스 위변조에 기술적 대응 방안을 설계하였다. 게임 서비스의 위변조 방지를 위하여 실행파일을 암호화하고 실시간으로 복호화하며 게임서비스 역 분석 방지를 위하여 디버깅, 디스어셈블, 자체 메모리 덤프를 방지하고 모듈 의존성에 대한 정보를 은닉하도록 하였다.

The Study on Software Tamper Resistance for Securing Game Services

Hangbae Chang[†], Jonggu Kang[††], Taehee Joe[†††]

ABSTRACT

The commensurate number of the attacks and infringement targeting a vulnerability of the game service has been increasing constantly, due to the dramatic growth and expansion of the impact of the game industry. However, there exist no subsequent researches for the differentiated technology, which is to prevent the reverse function of the game service. Therefore, in this study, we examined the current status of infringement toward online game services which are provided in the market currently and designed the proper technical measures for a manipulation of the game service which is the most vulnerable part. We have encrypted an execution file and decrypted it in real time process. Furthermore, we conducted debugging, disassemble, and prevented a its own memory dump, also concealed the information to overcome the module dependency to preclude a manipulation.

Key words: u entertainment(u 엔터테인먼트), software tamper resistance(소프트웨어 위변조), debugging(디버깅), disassemble(디스어셈블리), memory dump(메모리덤프)

1. 연구개발의 필요성

게임서비스 산업은 짧은 시간동안 초고속 성장을 해온 산업으로서 부가가치가 매우 높으며 모험성이 강한 산업이다. 게임서비스는 다른 어떤 매체보다도 사용자가 스스로 원하도록 만드는 힘이 강하기 때문에 게임 중독증을 일으킬 정도로 강한 친화력을 발휘하고 있으며, 노동과 학습에 필요한 감성을 배양시켜 창의력을 확장시키는 계기를 제공함으로써 개인의 상상력과 능력을 향상시킨다[1-3].

※ 교신저자(Corresponding Author) : 장항배, 주소 : 경기도 포천시 선단동 산 11-1(487-711), 전화 : 031)539-1752, FAX : 031)539-1750, E-mail : hbchang@daejin.ac.kr
접수일 : 2009년 5월 25일, 완료일 : 2009년 8월 18일
[†] 종신회원, 대진대학교 경영학과 조교수
[††] 대진대학교 대학원 경영학과 석사과정 (E-mail : jgkang@daejin.ac.kr)
[†††] 준회원, 연세대학교 정보대학원 석사과정 (E-mail : johee@yonsei.ac.kr)
※ 본 논문은 '2008년 한국멀티미디어학회 추계학술대회' 발표논문에 대한 후속연구를 통하여 수행되었습니다.

그러나 게임서비스의 산업성장 속도와 사회적 영향 등에 비하여 게임서비스 역기능 방지를 위한 차별화된 정보보안 기술연구는 아직 미진한 상태이다. 이에 따라 게임서비스의 취약성을 공격하는 침해사고 건수는 지속적으로 증가하고 있으며, 이러한 침해사고는 게임서비스 동작중단과 게임서비스 소스유출 등의 다양한 피해로 이어지고 있다. 따라서 본 연구에서는 현재 서비스되고 있는 온라인 게임서비스에 대한 침해현황 조사결과, 가장 큰 보안취약점으로 도출된 게임서비스 위변조에 기술적 대응방안을 설계하였다.

2. 게임서비스 침해유형

먼저 게임서비스 침해유형에 대한 분석을 위하여 선행연구를 바탕으로 침해영역별로 다음과 같이 정리하였다. 게임서비스에서 발견되는 클라이언트 영역에서 세부적인 게임서비스 침해유형으로서 '소프트웨어 위변조'는 게임서비스 실행프로그램을 변조하여, 실행환경이 모두 갖추어져 있지 않은 상태에서도 게임서비스가 실행될 수 있도록 하는 변경하는 행위를 말하며, '키보드 입력정보(Key Log) 탈취'는 사용자가 입력한 키보드 입력정보 또는 이벤트 메시지를 텍스트 파일로 저장되는 것을 의미한다. '맵 핵(Map Hack) 사용'(카드게임 상대 패보기)은 보이지 않게 설정된 상대편의 위치나 카드 패 등을 가시화하는 것을 의미하며, '게임 아이템(Item) 복사'는 게임서비스에서 사용하는 아이 템을 게임서비스 버그나 취약성을 사용하여 개수를 늘리는 행위를 말한다. '메모리 위변조'는 허가되지 않은 프로세스가 메모리에 접근하여 게임서비스 프로세스의 메모리를 조작하는 시도를 말하며, '오토 마우스 입력 및 매크로(Macro) 사용'은 게임서비스 진행에 필요한 입력을 자동으로 입력하여 반복적인 게임서비스 진행을 수행하는 것이다. '스피드 핵(Speed Hack) 사용'은 사용자의 컴퓨터를 비정상적으로 빠르게 만들어 줌으로써 게임서비스 내에서 사용자의 이동 및 공격속도를 증가시키도록 조절하는 행위이며, '사기(Fraud)'는 게임서비스를 이용하고 있는 상대편을 거짓으로 속여가면서 아이 템을 획득하는 방식이다. 마지막으로 '아이디(ID) 및 패스워드(Password) 유출'은 상대방의 권한을 가져오기 위하여 비도덕적인 방법으로 아이디와 패스워드를 탈취하는 것을 말한다.

게임서비스에서 발견되는 서버영역의 세부적인 게임서비스 침해유형은 일반적인 정보시스템 침해유형과 유사하며, 최근 들어 새롭게 발견된 내용은 다음과 같다. '게임 커뮤니티 웹 사이트를 통한 데이터베이스 변경'은 데이터베이스에 불법적인 질의 문을 사용하여 저장되어 있는 내부 정보를 유출하는 것을 의미하며, '백 도어(Back Door)를 통한 부적절한 접근'은 정식의 인증 절차 및 로그기록 없이 시스템에 접근하는 행위이다.

마지막으로 게임서비스에서 발견되는 네트워크 영역의 세부적인 게임서비스 침해유형은 일반적인 정보시스템 침해유형과 유사하며, 최근 들어 새롭게 발견된 내용은 다음과 같다. 먼저 '서비스 거부공격'은 표적 시스템이나 네트워크에 과다한 데이터를 통하여 성능을 저하시키는 행위를 말하며, '분산 서비스 거부공격'은 분산 설치된 해킹 프로그램들이 통합된 형태로 네트워크 공격을 통한 성능 저하 및 시스템을 마비시킨다. '패킷 위변조'는 네트워크 선을 단락시키거나 특성 소프트웨어를 통하여 패킷 송수신을 방해한다.

게임서비스에 대한 주요 침해유형 중 '소프트웨어 위변조 프로그램'이 사용되면, 그림 1과 같이 무작위로 생성된 정품 인증번호를 사용하여 게임을 실행하게 하거나, 이와 같은 행위를 차단하기 위한 보호 프로그램의 실행을 중지시킬 수 있다.

또한 게임서비스에 '스피드 핵 프로그램'이 설치되

그림 1. 소프트웨어 위변조 사례 (정품 인증번호 자동생성 및 보호 프로그램 차단)

그림 2. 스피드 핵 사례

면 그림 2의 사례에서 특정장소(동그라미 부분)까지의 도착시간이 정상적으로는 약 10초정도 걸리던 것을 1초 안으로 단축할 수 있게 되며, 또 다른 게임서비스에서는 오른쪽 끝에서 왼쪽 끝까지 정상적으로는 20초 이상이 걸리지만 스피드 핵을 사용할 경우에는 약 10초 안에 이동할 수 있으며 목표물(몬스터)에 대한 공격속도도 2배 이상 빨라지게 된다[4-10].

3. 게임서비스 위변조 방지기술 개발

3.1 기술 개요

소프트웨어 위변조 방지기술은 전자상거래, 디지털콘텐츠 관련 산업, 온라인 게임 등 불법적으로 수정되거나 삭제되는 등의 행위로부터 보호되어야 할 소프트웨어가 사용되는 다양한 응용분야에서 요구되는 소프트웨어에 대한 변조 및 분석을 방지하기 위한 기술이다. 소프트웨어 위변조 방지기술이 적용된 게임서비스는 악의적인 사용자가 게임서비스의 역 분석 및 변조를 통하여 불법적인 이득을 취하는 것을 원천적으로 방지함으로써, 해당 게임서비스 개발사 및 사용자의 피해를 미리 예방할 수 있다.

3.2 전체적인 시스템 구성

게임서비스 위변조 방지기술 기술(이하 'TRS')은 Portable Executable(이하 'PE') 구조를 가진 모든 파일(EXE, DLL, OCX, SCR 등)에 대하여 세부기능을 직접 파일에 삽입하는 방식으로 진행된다. TRS는 암·복호화를 수행하는 부분과 기계어 바이트 코드를 분석하기 우한 디스어셈블러, 소프트웨어 위변조 방지기술이 적용된 PE에 대한 동작 코드를 담당하는 TRS Loader 코드, 그리고 TRS의 사용자 인증과 사용자 인터페이스 부분으로 구성된다.

일반적인 PE 구조를 지닌 파일이 TRS를 통하여 각 기능별로 작업을 완료하면 PE 파일의 헤더를 조작하고 텍스트 섹션과 데이터 섹션을 암호화한 후, TRS Loader를 추가하여 새로운 파일을 생성하게 된다[11-13].

3.3 세부적인 기술 구성

3.3.1 Program Executable File

마이크로소프트에서 제공하는 파일 형식은 여러

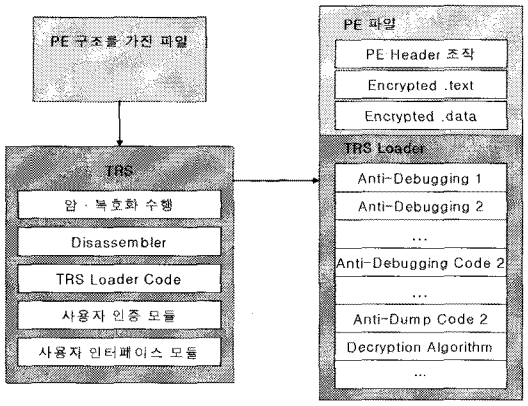


그림 3. TRS 구성도 및 동작 흐름도

가지가 존재하는 데 그 중 실행과 관련된 특정 파일의 표준형식은 PE 구조로 구성되어 있다. PE구조에서 암호학적 알고리즘이 적용되는 곳은 .text Section이나 .data Section이며, .text Section은 소프트웨어의 실행코드가 있으며 .data Section은 실행에 필요한 데이터를 저장한 곳이다. 코드영역과 데이터 영역을 암호화 혹은 packing하여 소프트웨어의 분석(disassembly)이 불가능하게 되는 것이다. 그림 4는 실행과 관련된 PE의 구조를 보여주고 있다.

그림 5처럼 PE 구조를 가진 파일은 메모리로 적재될 때 복호화 또는 unpacking 되며, 메모리에 적재된 소프트웨어는 보호되지 않는다.

3.3.2 소프트웨어 위변조 방지

① Loader Section Trap

Anti Debug와 Anti Soft Ice를 위하여 디버거 동작 유무를 확인할 수 있는 코드를 통하여 디버거 발견 시 종료 또는 임의의 주소로 분기하고 디버거가 breakpoint를 설정하게 되면, 메모리 코드가 변하는 것을 이용하여 Loader의 특정 부분의 올바른 check-sum인 경우만 다음 명령어가 실행될 수 있도록

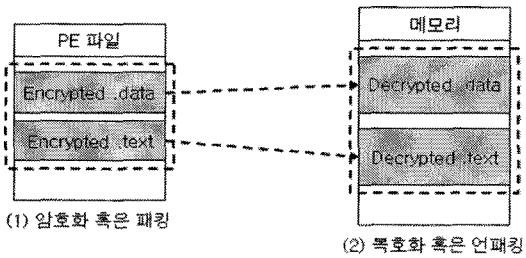


그림 4. 메모리에 적재된 PE 구조

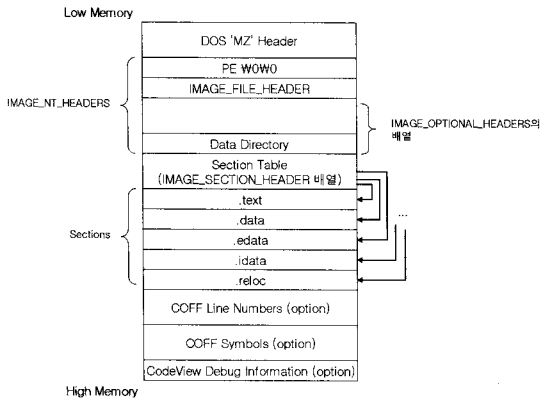


그림 5. 실행과 관련된 PE 구조

Partial Checksum을 이용하여 조정한다. Loader에서 사용되는 옵션을 얻기 위해서 XOR Trap을 이용하여 암호화된 옵션에서 정상적인 옵션을 구하고 디버거 또는 디스어셈블러를 사용하여 Loader Section의 Loader 복호화 코드 테이블을 참조하는 것을 방지하기 위한 목적으로 Loader Decryption Code를 치환한다.

② Loader Section and Text Section En(De)cryption: Cryptographic Wrapper

Loader 암·복호화 방식은 그림 6처럼 Section Encryption방식에서 Relocation Flag Table을 참조하는 것을 제외하고 동일하며 복호화는 복호화 명령어 코드를 통해 암호화 방식과 동일하게 동작한다. 암호화 과정은 파일에 위치한 .text Section 영역 찾은 후에 .text Section 영역의 크기를 계산하고 암·복호화 함수 코드를 생성하여 암호화를 실행한다. 복호화 과정은 PE 파일에 대한 암호화 명령어 테이블을 생성할 때 함께 생성한 복호화 명령어 테이블의 위치를 검색하고 PE 파일의 코드영역의 위치와 크기를 얻어온 후 코드영역을 복호화 명령어 테이블과 Relocation Flag Table을 참조하여 복호화 한다.

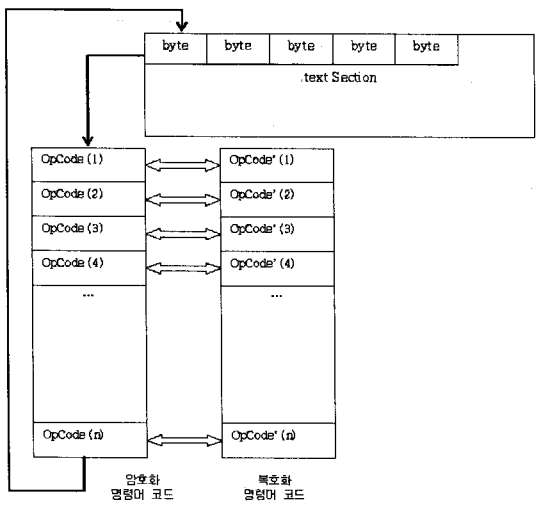


그림 6. Loader Section 암·복호화 과정

③ Data Section Encryption: Cryptographic Wrapper

.data Section의 암·복호화는 .text Section 영역의 암호화 방식과 같으나 사용자의 컴퓨터에서 수집한 하드웨어 정보의 해시 값(hash Vender Key)을 암호화 연산의 키 재료로 사용함으로써 키 재료가 일치하지 않으면, 정상적으로 동작하지 않는 차이점이 있다.

④ Self Integrity Check

정상적인 파일의 Check Sum 값을 암호학적으로 내포하여 숨긴 뒤 메모리에 적재될 때 다시한번 Check Sum 검사하여 파일의 무결성을 검사하도록 한다.

3.3.3 소프트웨어 역 분석 방지

① Anti Debugging

디버거를 통해 PE 파일을 실행시키거나 실행 중인 PE 파일(프로세스)을 디버깅하는 것은 역 분석의 기본이다. 악의적인 사용자는 디버깅을 통하여 프로세스의 동작을 분석하며 의도하지 않은 동작을 유도하기 위해 코드를 삽입, 삭제 그리고 수정한다. 따라서 이러한 프로세스 디버깅을 방지하기 위하여 구조화된 예외처리(Structured Exception Handler), 인터럽트 Handler 조작, 프로세스 실행 환경 블록(Process Environment Block) 수정과 같은 기술을 사용하여 디버거의 동작을 감지한다. 다음 a단계에서 e단계는 그림 7처럼 Entry Point를 숨김으로써

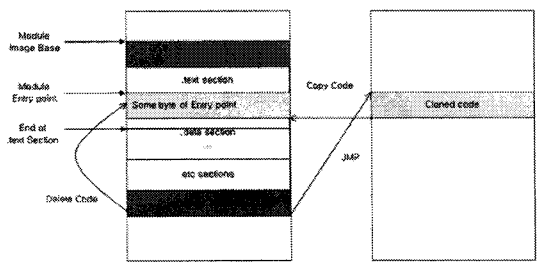


그림 7. Anti Debugging 과정

디버깅을 방지하는 절차이다.

a. Loader가 .text Section, .data Section을 복호화하고 실행에 필요한 Win32 시스템이나 DLL이나 사용자 정의 DLL에 대한 정보를 가지고 있으며, 특정 프로세스가 어떤 Win32 API를 호출하는지에 대한 직접적인 정보를 담고 있는 Import Address Table 값을 채운다.

b. Loader는 Original Entry Point로 옮겨가기(jump) 전에 .text Section의 Entry Point에서 임의의 길이의 어셈블리 코드 값을 버퍼에 복사한다.

c. 복사되는 코드의 크기는 Well Formed byte 만큼의 길이 정보가 이미 구해져 있다.

d. .text Section에서 복사된 크기만큼의 byte를 지운다.

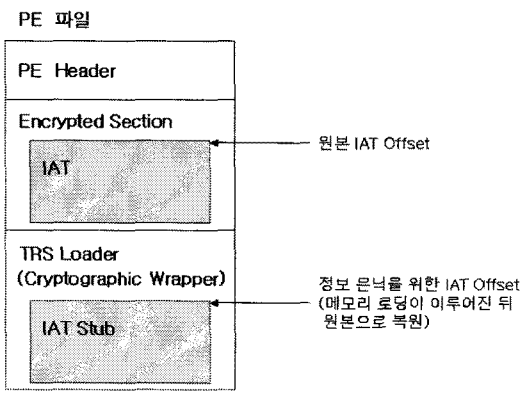
e. Loader는 Cloned Code로 이동하여, 복사된 크기의 어셈블리 코드를 실행한 다음 삭제된 코드 이후 위치로 이동한다.

② Anti Disassembly

PE 파일의 .text Section과 .data Section은 앞서 설명한 바와 같이 Cryptographic Wrapper로 암호화하므로, 디스어셈블러를 통한 분석은 불가능하다.

③ Dependency Hiding

악의적인 사용자는 Import Address Table에서 얻은 정보를 사용하여 디버거의 breakpoint를 설정하거나 API hooking과 같은 기술을 사용하여 프로그램에서 의도하지 않은 동작을 유도할 수 있다. 따라서 PE 파일의 정보를 수정하여 Import Address Table 통한 직접적인 정보를 숨긴 다음, 메모리에 적재 되었을 때 복원함으로써 악의적인 사용자의 의도치 않은 상황을 회피하도록 하였다. 그림 8은 복호화 직후의 PE 파일의 checksum을 보여준다.



※ IAT: Import Address Table

그림 8. 복호화 직후의 PE 파일 checksum

④ Anti Memory Dump

TRS에서 암호화한 PE 파일은 메모리에 로드되면 복호화 되기 때문에 메모리에 로드된 프로세스를 덤프하게 되면 원본 바이너리를 얻을 수 있게 된다. 따라서 본 연구에서는 PE 파일의 헤더 정보를 조작 또는 속임수(Tricky) 코딩으로 dump 유틸리티로부터 dump를 방지하였다.

4. 게임서비스 위변조 방지기술 실험

본 연구를 통하여 개발된 게임서비스 위변조 방지기술의 적용가능성을 실험하기 위하여 실행파일을 그림 9와 같이 암호화 하였다.

① EXE 파일 Anti Debugging 보안성 실험

실행파일을 debugging 하는 프로그램인 'OllyDbg 프로그램'을 이용하여 본 연구의 기술을 적용한 암호화된 EXE 파일이 debugging이 불가능 한 것을 확인하였다. 암호화 되지 않은 메모장 프로그램을 사용하면 그림 10과 같이 debugging이 가능하였다.

그러나 암호화된 실행 파일의 경우에는 그림 11과 같이 debugging을 방지할 수 있었다.

② 실행파일 Anti Disassembling 보안성 실험

실행파일을 대상으로 'OllyDbg 프로그램'을 이용한 결과 본 연구의 기술을 적용한 암호화된 실행 파일이 disassembling이 안 되는 것을 확인하였다. 암호화 되지 않은 메모장 프로그램을 사용하면 그림 12와 같이 assembly 언어로 변환되고, 암호화된 실

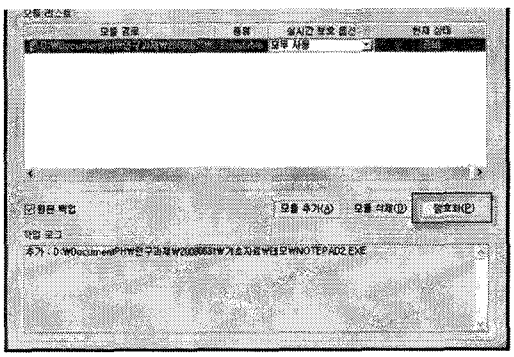


그림 9. 실행 파일 암호화

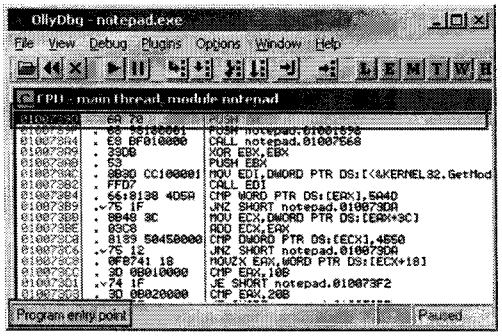


그림 10. 암호화 되지 않은 EXE 파일에 대한 debugging 결과

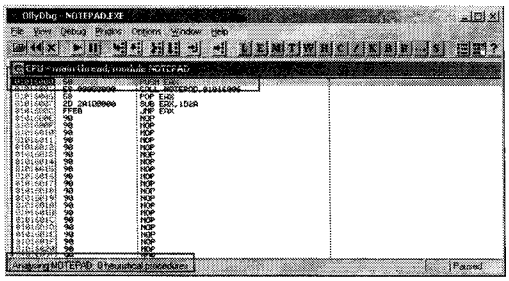


그림 11. 암호화 된 실행 파일에 대한 debugging 방지 결과

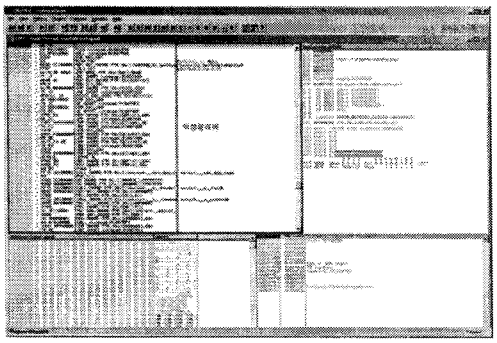


그림 12. 암호화 되지 않은 실행 파일에 대한 disassembling 결과

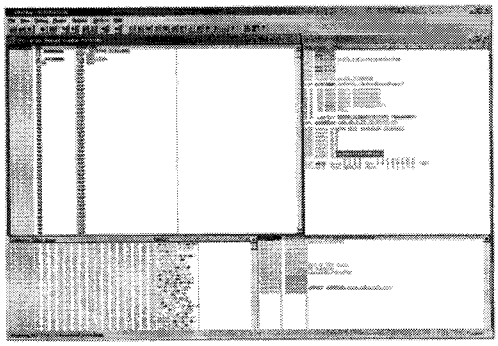


그림 13. 암호화 된 실행 파일에 대한 disassembling 방지 결과

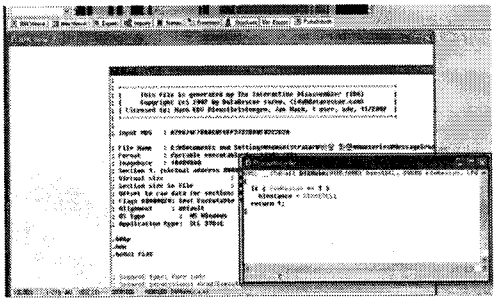


그림 14. 암호화 되지 않은 파일에 대한 disassembling 결과

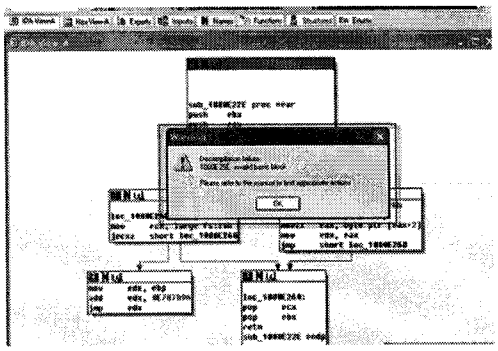


그림 15. 암호화 된 파일에 대한 disassembling 방지결과

행 파일의 경우에는 그림 13과 같이 disassembling을 방지할 수 있었다.

③ DLL 파일 Anti Disassembling 보안성 실험

Anti Disassembling에 관한 보안성 실험을 위하여 DLL파일을 대상으로 DLL 파일의 Disassembler인 'IDA Pro 프로그램'을 이용하여 본 연구의 기술을 적용한 암호화된 DLL 파일이 disassembling이 안 되는 것을 확인하였다. 암호화 되지 않은 msgsndr.dll 파일은 IDA Pro 프로그램에 의하여 그림 14와 같이 assembly 언어로 변환됨을 볼 수 있다.

암호화된 DLL 파일의 경우에는 그림 15와 같이 disassembling을 방지할 수 있다.

④ 실행파일 Anti Memory Dump 보안성 실험

실행파일을 대상으로 실행 파일을 dump 시켜주는 'M Dump 프로그램'을 이용하여 본 연구의 기술을 적용한 암호화된 실행 파일이 dumping이 안 되는 것을 확인하였다. 암호화 되지 않은 응용 프로그램을 사용하면 그림 16과 같이 assembly 언어로 변환된다.

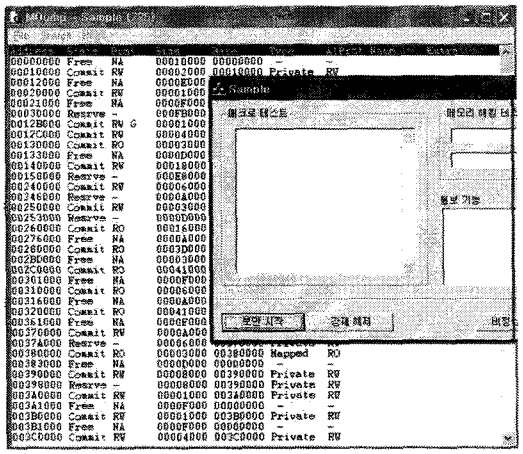


그림 16. 암호화 되지 않은 파일에 대한 dumping 결과

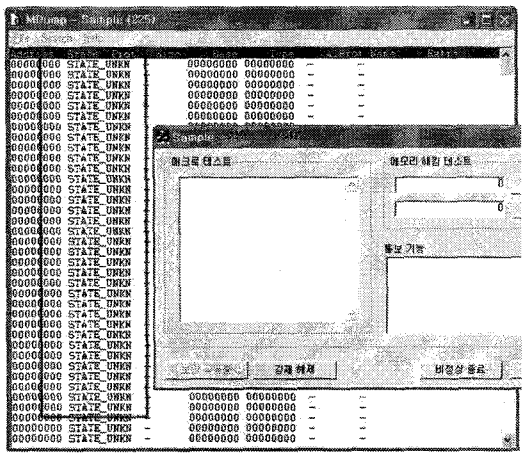


그림 17. 암호화 되지 않은 파일에 대한 dumping 결과

암호화된 EXE 파일의 경우에는 그림 17과 같이 dumping을 방지할 수 있었다.

5. 결 론

게임서비스 산업은 산업성장 속도 및 사회적 영향 등에 비하여 게임서비스 역기능 방지를 위한 차별화된 정보보안 기술연구는 아직 미진한 상태이다. 이에 따라 본 연구에서는 현재 서비스되고 있는 온라인 게임 서비스에 대한 침해현황 조사결과, 가장 큰 보안취약점으로 도출된 게임서비스 위변조에 기술적 대응방안을 설계하였다. 게임서비스 위변조 방지기술은 게임서비스에 관한 역 분석 및 위변조를 방지를 하기 위한 기술로서, Anti Debugging, Anti Disassembling, Anti Memory Dump 등으로 구성된다.

본 연구에서는 게임서비스 위변조 방지를 위하여 게임서비스와 별도로 독립된 컴파일러 및 하드웨어가 필요하였던 선행연구를 개선하여, 실행파일 자체가 스스로 자신의 역 분석 및 위변조 방지를 할 수 있는 기술을 개발하였다. 세부적으로 본 연구를 통하여 제안한 방식은 실행파일 내 data section 과 code section을 분리하여 암호화하고 이를 복호화 할 수 있는 loader를 이중으로 설치하였다. 또한 Anti Debugging을 위하여 외부 debugger의 동작이 감지되면 게임서비스가 자동으로 종료되게 하였으며, Anti Disassembling을 위하여 Disassembling 프로그램이 참조하는 실행파일의 헤더를 변경하여 이를 불가능하게 하였다. 마지막으로 Anti Memory Dump를 위하여 보호하고자 하는 데이터는 임시 할당 메모리에 복사함으로써 이를 해결하였다.

본 연구의 결과는 게임서비스 침해유형을 파악하고 침해유형에 따른 대응기술에 따라 게임 기획 및 개발이 이루어짐으로써 게임콘텐츠 내부로직에 대한 침해를 예방할 수 있으며 이것은 내부 로직의 침해에 따른 국가 및 기업의 피해비용, 더 나아가 그에 따른 파급 효과를 줄일 수 있다. 또한 경쟁력 있는 게임 콘텐츠를 안전하게 보호함으로써 국가 및 기업 경쟁력을 보장할 수 있으며, 이것은 게임 콘텐츠 시장의 활성화를 가져올 수 있을 것으로 예상된다.

향후 연구에는 본 연구를 통하여 조사된 게임 서비스 침해 유형 중 게임 서비스 사용자의 아이디나 비밀번호 등을 유출하여 정상적인 게임서비스 운영을 방해하는 키보드 입력정보 보호기술에 대한 연구를 진행함으로써, 클라이언트 영역의 통합적인 게임 보안 환경을 구축할 예정이다.

참 고 문 헌

[1] Bernard L. and Solms R., "A Formalized to the Effective Selection and Evaluation of Information Security Controls," Computer & Security, Vol. 19, No. 2. 2000.

[2] Norton Peter and John Paul Mueller, "Complete Guide to Microsoft Windows XP," SAMS, 2002.

[3] Otwell K. and B. Aldridge, "The Role of

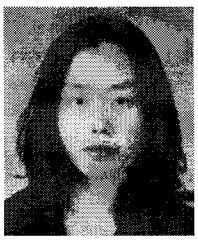
Vulnerability in Risk Management," IEEE Proceedings of the 5th Annual Computer Security Applicant Conference, 1989.
[4] Peltier T., "Information Security Risk Analysis," Auerbach, 2001.
[5] Rajeev Nagar, "Windows NT File System Internals : A Developer's Guide," O'Reilly & Associates, 1997.
[6] Eloff J. and M. Eloff, "Information Security Management - A New Paradigm," Proceedings of SAICSIT, 2003.
[7] Joan Daemen and Vincent Rijmen, "The Design of RijndaeL: AES - The Advanced Encryption Standard", Springer-Verlag, 2002.
[8] Liming and Sean D., "Windows NT Embedded Step-By-Step", Annabooks, 2000.
[9] Bott, Ed, Carl Siechert and Craig Stinson, "Microsoft Windows XP Inside Out," Microsoft Press, 2001.
[10] Knittel and Brian, "Windows XP Under the Hood", QUE, 2003.
[11] Norton Peter and John Paul Mueller, "Complete Guide to Microsoft Windows XP," SAMS, 2002.
[12] Art Baker and Jerry Lozano, "The Windows 2000 Device Driver Book: A Guide for Programmers," Prentice Hall, 2001.
[13] Edward N. Deker, Joseph M. and Newcomer, "Developing Windows NT Device Drivers: A Programmer's Handbook," Addison-Wesley, 1999.
[14] Inca Internet, "Method to cut off an Illegal Process Access and Manipulation for the Security of Online Game Client by Real Time," Korean Patent 10-0483700, 2005.

장 항 배

2006년 2월 연세대학교 정보대학원(정보시스템 박사)
2007년 3월~현재 대진대학교 경영학과 조교수
관심분야 : 산업보안 기술 및 관리 체계, u 비즈니스 전략 및 기술

강 종 구

2008년 2월 대진대학교 경영학과 학사
2009년 3월~현재 대진대학교 경영학과 석사과정
관심분야 : 산업보안 기술, u 비즈니스 모델링



조 태 희

1998년 8월 경북대학교 전자공학과 학사
2008년 3월~현재 연세대학교 정보대학원 석사과정
관심분야 : 정보보호, 내부자정보 유출방지