게임 서비스 침해유형에 따른 기술적 대응방안 연구

The Study of Information Security Technologies for Security Incidents in Online Game Service

장 항 배 (Hang Bae Chang) 대진대학교 경영학과 교수, 교신저자
김 경 규 (Kyung Kyu Kim) 연세대학교 정보대학원 교수, 공동저자
이 시 진 (Si Jin Lee) 대진대학교 컴퓨터공학과 교수, 공동저자

요 약

본 연구에서는 최근 급속한 속도로 발전하고 있는 게임 산업에 비하여 상대적으로 미진한 상태에 있는 게임 서비스에 관한 정보보호 기술 연구를 진행하였다. 연구수행을 위하여 현재 온라인으로 서비스되고 게임들을 대상으로 침해현황을 조사하여 이를 유형별로 분류하였다. 정리된 게임 서비스 침해유형에 따라 서비스 침해를 발생시키는 원인을 분석하여 이를 해결할 수 있는 기술적 방안을 설계한 다음 현재 제공되고 있는 게임 서비스로의 적용가능성을 검증하였다. 본 연구의 결과는 게임 서비스 보호를 위한 연구의 방향성을 제시함과 동시에 게임 서비스를 포함하는 일반 응용소프트웨어에 대한 정보보호 기술개발에도 적용될 수 있을 것으로 기대한다.

키워드 : 게임 보안, 오토 프로그램, 소프트웨어 위변조, 스피드 핵

Ⅰ. 서 론

관련 자료에 의하면 국내 게임 서비스 산업의 규모는 2006년 8조 6천억 원으로 매년 10% 이상 성장할 것으로 예상하고 있다. 이렇게 급속한 속도로 성장하고 있는 게임 서비스 산업은 다음과 같이 몇 가지 특징을 가지고 있다. 먼저 게임 서비스는 문화적 특징을 지닌다. 게임 서비스는 말·그림·소리·움직임 등과 같은 문화의 4가지 요소를 모두 갖추고 있으며, 이러한 구성 요소와 함께 기술이 합쳐진 종합적인 문화로 볼 수 있다. 두 번째 특징으로 게임 서비스는 산업적 성격을 가지고 있다. 게임 서비스 산업은 짧은 시간동안 초고속 성장을 해온 산업으로 부가가치가 매우 높으며 모험성이 강한 산업이다. 따라서 개발도상국처럼 경제문제에 국가역량이 집중되는 국가보다는 경제문제와 함께 삶의 질을 개선하기 위하여 노력을 기울이는 선진국에 보다 적합한 산업으로 볼 수 있다. 세 번째로 게임 서비스는 사회적 특징을 지닌다. 게임 서비스는 다른 어떤 매체보다도 사용자가 스스로 원하도록 만드는 힘이 강하기 때문에 게임 서비스 중독증을 일으킬 정도로 강한 친화력을 발휘하고 있다. 마지막으로 게임 서비스는 학습적 특징을 지닌다. 게임 서비스는 노동과 학습에 필요한 감성을 배양시킬 수 있으며 창의력을 확장시키는

계기를 제공함으로써 개인의 상상력과 능력을 향상시키는 데 기여한다.

그러나 이러한 게임 서비스 산업 규모의 성장 속도와 게임 서비스 산업이 미치는 경제·사회·문화적 영향 등을 고려하여 볼 때, 상대적으로 게임 서비스 역기능 방지를 위한 정보보호 기술연구는 일반적인 정보시스템 대한 정보보호 기술연구에 비하여 게임 서비스에 관한 차별화된 체계적인 연구는 아직 미진한 상태이다. 이에 따라 게임 서비스 취약성을 공격하는 게임 서비스 침해사고 건수는 지속적으로 증가하고 있으며 이러한 침해사고는 게임 서비스 동작중단과 게임 서비스 소스유출 등의 다양한 피해로 이어지고 있다. 본 연구에서는 게임 서비스에 특화된 정보보호 기술을 개발하기 위하여 현재 서비스되고 있는 온라인 게임 서비스에 대한 침해현황 조사와 함께 사례분석을 진행함으로써 게임 서비스 침해유형을 정의하고 유형별 침해원인 분석을 통한 기술적 대응방안을 설계하고자 한다.

Ⅱ. 게임 서비스 침해현황 조사연구

게임 서비스 침해에 대한 피해 사례수가 증가되면서 피해 유형도 다양화 되고 있으며 사회범죄로까지 확대되고 있다. 본 장에서는 국내 게임 서비스 침해에 관한 구체적인 사례(아이템 복사, 이중 로그인, 공격 및 이동 속도 증가, 공격력 및 방어력 조작 등)와 함께 이에 대한 대책수립 현황을 조사하였다. 게임침해에 관한 현황조사를 위하여 정보보호 실태조사 및 수준평가에 관한 선행연구를 기초로 하여 설문지를 작성하였으며 이를 관련분야 전문가 검토와 예비 설문조사를 실시하여 설문지의 타당성을 얻고자 하였다.

한국정보보호진흥원이 매년 실시하고 있는 정보화 역기능 실태조사 연구는 인터넷 사용자의 정보화 역기능 실태현황 및 추이분석을 통하여 정보화 역기능 방지를 위한 정책대안 수립을 목적으로 객관적 현황자료 확보측면에서 진행되었다. 이 조사에서는 정보화 역기능 현황을 알아보기 위하여 개인정보 및 프라이버시 침해, 스팸메일, 불건전 정보유통(음란물), 컴퓨터 바이러스, 정보시스템 불법침입 및 파괴(해킹), 무선 인터넷 보안 등 6가지 영역으로 분류하여 사용자 피해경험, 태도 및 인식, 방지 및 대처방안 등을 조사하였다. 중소기술정보진흥원이 진행한 중소기업 정보화 역기능 실태조사 연구에서는 정보보호 관리체계(Information Security Management System)를 기초로 하여 정보보호 조직 및 인력현황, 정보보호 지침수립 및 이행현황, 정보보호 투자 및 운영현황, 보안사고 경험 및 대응현황, 정보보호 추진에 따른 문제점 및 정부지원 요구사항 등을 조사하였다.

이러한 선행연구는 서비스(정보시스템, 인터넷 등) 사용자를 대상으로 일반적인 사용현황과 정보화 역기능 피해사례 경험을 조사했을 뿐 역기능을 발생시키는 원인분석과 함께 정보서비스에 대한 체계적인 침해유형 정리는 진행되지 않았다. 또한 조사를 위한 설문지 응답대상이 서비스 사용자에게만 한정되어 있을 뿐만이 아니라 1회에 많은 내용을 조사하다보니 조사항목 수가 많은 단점을 가지고 있다. 본 연구의 진행을 위한 게임 서비스 침해 현황조사 항목은 기본적으로 선행연구와 함께 비슷한 구조를 설계하되 게임 서비스 침해를 유발하는 원인분석을 위하여 별도의 게임 서비스 침해 사례조사를 진행하였으며, 게임 서비스 사용자뿐 만이 아니라 게임 서비스 개발자 및 운영자에 대한 조사항목도 별도로 설계하여 최종 20여개 미만의 설문문항을 구성하였다. 게임 서비스 개발자 및 운영자를 위한 설문은 게임 서비스 침해에 관한 대응책 수립현황을 조사하고자 하였으며, 게임 서비스 사용자 설문은 사용자가 느끼는 게임 서비스 침해 현황을 조사할 목적으로 진행하였다.

조사 대상은 게임 서비스 기업의 경우 한국게임산업진흥원에서 발간한 '2005년 대한민국 게

임백서' 내용 중에서 국내 게임 서비스 이용현황 자료를 기초로 하여, 많은 수의 게임 서비스 사용자를 확보하고 있는 80개의 게임 서비스 기업과 이들의 게임 서비스를 사용하고 있는 대학교 이상의 게임 서비스 사용자 350명 등을 추출하여 설계되었다.

설문방법은 간접설문(전화, 전자메일, 팩스 등)과 방문설문의 방법을 통하여 15일 동안(2006년 12월 1일~15일) 수거된 유효설문을 대상으로 결과를 분석하였다. 최종적으로 수거된 유효설문 개수는 게임 서비스 개발자 및 운영자에 대해서 50개, 게임 서비스 사용자에 대해서 200개가 수거되었다. 조사된 게임 서비스 종류는 게임 서비스 현황조사에 관한 선행연구를 참고로 하여 일반적인 롤플레잉 게임(Roll Playing Game), 캐주얼 게임(Casual Game), 웹보드 게임(Web Board Game), 슈팅 게임(Shooting Game) 등을 대상으로 게임 서비스 침해 에 따른 대응책 수립현황을 조사하였다. 수집된 설문에 대한 검증을 위하여 통계적 방법을 적용한 신뢰성을 측정하였다.

신뢰성은 유사한 조건아래에서 같은 대상을 반복하여 측정하였을 경우 비슷한 결과가 얼마나 자주 나타나는 지를 알아보는 것이다. 본 연구에서는 재검사나 상호 교환적 방법과 달리 여러 번에 걸친 측정을 요구하지 않으며, 반분법과 같이 전체문항을 반문함으로 인하여 불확정성 문제가 발생하지 않는 신뢰성 계수(Cronbach Alpha) 값을 통한 한 번의 측정으로 신뢰성을 얻는 내적일관성 검사방법을 적용하여 게임 서비스 산업에 종사하는 게임 개발자와 운영자들에 대한 설문조사 결과를 통계 프로그램(SPSS 12.0)에 입력하여 신뢰성을 분석하였다. 내적일관성 검사방법에서는 신뢰성 계수 값으로서 신뢰성의 정도를 평가하게 되며, 선행연구에 의하면 신뢰성 계수 값이 0.6이상이면 충분(기초연구 분야에서는 0.8이상, 중요한 의사결정 시에는 0.9이상)하다고 설명하고 있다. 신뢰성을 분석하기에 앞서 수집된 자료에 대한 전반적인 분포형태를 살펴본 후 분석방향에 대하여 정리하였다. 일반적으로 정규분포를 따르게 되면 다른 분포에 비하여 좀 더 정확한 결과 값을 가지게 된다. 이에 따라 수집된 자료를 가지고 정규분포 검정을 실시한 결과 정규분포에 가까운 값을 얻을 수 있었으며, 개발자(운영자) 침해사고 대응현황 항목(게임 서비스 침해사고 대응을 위한 중요성 인식, 환경조성 등)에 관한 항목의 신뢰성 계수 값을 산출한 결과 0.7223을 얻게 되어 설문 분석할 내용들에 대한 신뢰도가 통계적으로 문제가 없음을 알 수 있었다.

게임 서비스 침해 현황조사에 관한 주요결과 내용으로서 게임 서비스에 대한 침해경험은 서비스 개발자 및 운영자응답자 수의 70%(35명), 서

〈표 1〉 게임 서비스 침해현황 조사항목

조사대상	조사 항목	세부 조사 항목
개발자 (혹은 운영자)	일반정보	이름, 소속, 연락처 등
	게임 서비스 업무 현황	업무분야, 게임 서비스 이름, 게임 환경 등
	게임 서비스 침해사고 현황	침해사고 경험, 침해사고 발생영역, 침해사고 사례 내용 등
	게임 서비스 침해사고 대응 현황	침해사고 대응 인식수준, 침해사고 대응 시스템 구축현황 등
사용자	일반정보	이름, 소속, 연락처 등
	게임 서비스 이용 현황	이용 장소 및 시간, 이용하는 게임 서비스 현황 등
	게임 서비스 침해사고 현황	침해사고 경험, 게임 서비스에 대한 자발적인 침해시도 경험, 침해사고 대응책 수립수준 등

비스 사용자 응답자 수의 38.5%(77명)가 게임 서비스 침해경험이 있다고 답하였다. 서비스 사용자에 대한 침해경험 응답 수가 서비스 개발자 및 운영자의 응답 수에 비하여 상대적으로 적은 이유는 전문가 성격의 서비스 개발자 및 운영자에 비하여 서비스 사용자는 게임침해 자체사실도 느끼지 못하는 것으로 예상할 수 있다. 게임 침해 영역에 있어서는 클라이언트 영역에서의 침해사례가 가장 많은 것으로 집계되었으며, 이는 서버 및 네트워크 중심의 일반적인 정보보호 기술 발전방향과 배치되고 있다는 것을 보여준다. 이러한 이유는 일반적인 정보시스템에 대한 침해는 정보자산에 대한 침해공격을 목적으로 발생하지만 게임 서비스 분야에서는 사용자 스스로 좀 더 편리하고 쉽게 게임 서비스를 즐기기 위한 목적으로 게임 서비스 침해를 발생시키는 것에 기인할 수 있다.

게임 서비스 침해에 대한 게임 서비스 개발자 및 운영자가 생각하는 정보보호에 대한 인식의 중요성에 비하여 실제적인 정보보호 시스템의 구축 및 대응책 수립현황은 설문 응답수의 58% 이하(29명)로 나타났다. 이와 같이 정보보호 환경 구축이 미흡한 이유는 정보보호 전담인력 부재와 함께 현재 발생하고 있는 게임 서비스 침해현상에 대하여 정확하게 차단할 수 있는 정보보호 시스템이 부재하기 때문인 것으로 조사되었다. 본 연구에서는 게임 서비스 침해사고를 사전에 방지할 수 있는 정보보호 기술을 개발하기 위하여 게임 서비스 침해유형별 사례분석을 통하여 침해발생 원인을 먼저 분석하였다.

Ⅲ. 게임 서비스 침해유형 정의

게임 서비스 침해에 대한 현황조사를 바탕으로 실제적인 게임침해 사례조사를 진행하기 위해서는 게임 서비스 침해현상에 따른 분류과정이 선행되어야 한다. 본 장에서는 일반적인 정보보호 침해유형 분류체계와 함께 게임 서비스 침해에 대한 특성을 분석하여 게임 서비스 분야에 적합한 게임 서비스 침해유형을 정의하고자 한다.

초기 정보보호 침해유형에 관한 분류체계 연구는 Bisbey(1978) and Brain Matick(1990)등이 진행하였으나, 분류체계가 다소 명확하지(mutually exclusive) 않고 외부로부터의 공격(attack)보다는 정보자산의 취약점(vulnerability)을 중심으로 침해유형을 정리하였다. Bishop(1995)의 연구에서는 유닉스 환경에서 발생 가능한 취약점들을 기존연구에서 사용했던 계층구조(tree-like taxonomy)에서 탈피하여 6가지의 속성(Nature, Time of Introduction, Exploitation Domain, Effect Domain, Minimum Number, Source) 축(axe)에 따라 정리하였다. Howard(1997)연구에서는 컴퓨터 또는 네트워크 공격들을 외부 침입자가 정보자산에 공격하기까지 각 단계를 정의(Attackers, Tools, Access, Results, Objectives)하고 단계별 특성에 따라 침해유형을 정리하였으며, Lough(2001)연구에서는 외부공격의 특성(Improper validation, Improper exposure, Improper randomness, Improper deallocation)에 따라 침해유형을 분리하였다. Ray Hunt(2005) 연구에서는 외부 공격의 유형을 더욱 자세히 분석하여 4차원(Attack Vector, Attack Target, Vulnerabilities and Exploits, Attacks Payloads or Effects)

〈표 2〉 게임 서비스 종류별 침해현황 조사

	롤플레잉 게임	캐주얼	보드	슈팅
서버	70.0%	72.0%	62.5%	0%
네트워크	20.0%	20.0%	25.5%	33.3%
클라이언트	10.0%	8.0%	12.5%	66.7%

로 분류하고, 각 차원 별로 단계를 세분화 시켰다.

현재까지 게임분야 침해사례에 대하여 세부적인 원인분석을 진행한 연구는 아직 초기단계에서 진행되고 있기 때문에 본 연구에서는 Ray Hunt(2005)가 제시한 4차원 분류기준 중에서 첫 번째 및 두 번째 기준(Attack Vector, Attack Target)을 가지고 침해유형을 분류하고자 하였다. 첫 번째 기준에 해당되는 침해유형 분류방법은 공격대상에 대한 침해방법에 따른 분류이다. 예를 들어 1단계에서 바이러스, 웜, 서비스 거부공격, 비밀번호 공격 등으로 분류하고, 2단계에서 바이러스는 일반 파일 감염, 시스템 주요정보 감염, 매크로 등으로 세분화 되며, 서비스 거부공격은 호스트 기반과 네트워크 기반으로 다시 나누어진다. 두 번째 기준에 따라 침해유형을 분류하는 방법은 침해대상을 기준으로 분류하는 것이다. 예를 들어 1단계에서 침해대상을 하드웨어와 소프트웨어로 분류하고, 2단계에서는 하드웨어를 컴퓨터시스템으로 소프트웨어는 운영체제, 응용소프트웨어, 네트워크로 구분한다. 3단계에서 컴퓨터시스템은 하드디스크, 네트워크장비, 주변장치 등으로 세분화 되며, 운영체제는 윈도우즈 운영체제, 유닉스 운영체제, 맥 운영체제(Mac OS), 응용소프트웨어는 서버와 사용자, 네트워크는 프로토콜 등으로 나누어진다. 이와 같이 Ray Hunt(2005) 방법론은 정해진 기준에 따라 단계별 세분화를 지속적으로 진행하면서 침해유형을 분류하게 된다. 본 연구에서는 게임 서비스 침해사례들에 대하여 먼저 침해방법에 따라 분류를 진행하고, 그 다음 침해대상에 따라 침해유형을 계층화하였다. 침해방법은 침해사례가 발생하는 주요 원인에 따라 게임 서비스 자체 취약점으로 생기는 침해현상(Vulnerability)과 외부공격으로부터 발생하는 침해현상(Attack), 그리고 정보기술이 아닌 사람이나 외부환경에 의하여 발생하는 침해현상(Social Engineering) 등으로 분류하였다.

게임 서비스 침해유형에 관한 세부적인 체계를 설계하기 위하여 조사된 침해사례와 함께 관련된 선행연구 결과를 정리하여, 전문가 집단에게 이를 단계별로 제시하면서 델파이 방법론을 통하여 최종적으로 침해유형을 정리하였다. 델파이 방법은 전문가 집단으로부터 설문을 통하여 의견을 듣고 통계분석 결과를 다시 설문하여 의견을 수렴 집계하는 반복과정을 말한다. 이 방법은 각자의 전문가 의견을 수정할 기회가 주어지고, 다른 전문가의 의견을 활용할 수 있다는 점에서 매우 긍정적이며, 현재 기술 예측연구 분야에서는 90% 이상이 델파이방법을 사용할 정도로 보편적인 방법으로 자리 잡고 있다. 또한 전문가 집단의 참여를 통하여 신뢰성 있는 결과를 얻을 수 있으며, 비교적 광범위하고 분석적인 견해를 제시하여 줄 수 있다.

이 방법을 통하여 총 3회의 설문조사를 실시하였으며, 1차는 2007년 2월 11일에서 13일까지, 2차는 2월 18일에서 20일까지, 3차는 3월 1일에서 3일까지 실시하였다. 각각의 게임 서비스 침해사례들을 앞서 소개한 방법론에 따라 침해유형을 설계하여 전자우편 및 팩스의 방법으로 전달하였다. 검토 대상자인 전문가 집단은 정보보호를 연구하는 교수 3명과 게임 서비스 기업에서 정보보호 업무를 총괄하는 관리자 2명을 선정하여 진행하였다. 설문 대상자 수가 5명으로 한정되어 있었기 때문에 매회 설문 응답률은 100%였으며, 의견차이가 매우 컸던 초기 설계와는 달리 반복보정 횟수가 증가하면서 점차 안정화 되어가는 모습을 볼 수 있었다. <표 3>은 최종 설계된 침해방법과 침해대상에 따른 게임 서비스 침해유형을 정리한 것이다.

게임 서비스 침해유형은 일반적인 프로그램에서 발견될 수 있는 침해유형과 비교하여 볼 때 서버나 네트워크 영역에는 상호 유사한 침해유형이 존재하고 있으나, 클라이언트 영역에서는 좀 더 세분화된 침해사례들이 발견되고 있다는 것을 알 수 있다. 게임 서비스에서 발견되는 클라이언트 영역에서 발견되는 세부적인 게임

〈표 4〉 침해방법 및 대상에 따른 게임 서비스 침해사례 유형분류

침해대상 / 침해방법	서버	네트워크	클라이언트
정보자산 취약점 공격	• 서버 초기화를 통한 경험치(MOB) 생성 • 백 도어(Back Door)를 통한 부적절한 접근 • 유니코드 취약점을 이용한 IIS(또는 ASP) 공격 • 게임 커뮤니티 웹 사이트를 통한 데이터베이스 변경 • 버퍼 오버프로우(Buffer Overflow) 취약점 공격 • 서비스 거부공격(Denial of Service Attack)	• 포트 스캐닝(Port Scanning)을 통한 정보획득 • 패킷 스니핑(Packet Sniffing)을 통한 회선 도청 • 스푸핑(Spoofing)을 통한 위장 • 통신 프로토콜(Protocol) 취약점 공격 • 서비스 거부공격(Denial of Service Attack) • 분산 서비스 거부공격(Denial of Service Attack)	• 소프트웨어 위변조 • 키보드 입력정보(Key Log) 탈취 • 맵 핵(Map Hack) 사용(카드게임 상대 패보기) • 게임 아이템(Item) 복사 • 메모리 위변조
외부로부터 악성 프로그램 사용	• 바이러스(Virus) 배포 • 웜(Worm) 프로그램 실행 • 봇(Bot) 프로그램 실행 • 트로이 목마(Trojan)를 통한 비인가 된 기능수행 • 서비스 거부공격(Denial of Service Attack)	• 웜(Worm) 프로그램 실행 • 피싱(Phishing) 프로그램 실행	• 오토 마우스 입력 • 매크로(Macro) 사용 • 스피드 핵(Speed Hack) 사용
사회 공학	• 내부 자에 의한 게임자료 유출 • 외부 자에 의한 게임자료 갈취 • 운영자 사칭	• 외부 자에 의한 물리적인 게임운영 방해	• 사기(Fraud) • 아이디(ID) 및 패스워드(Password) 유출

서비스 침해사례는 다음과 같다.

- 소프트웨어 위변조: 게임 서비스 실행프로그램을 변조하여 실행환경이 모두 갖추어져 있지 않은 상태에서도 게임 서비스가 실행될 수 있도록 하는 변경
- 키보드 입력정보(Key Log) 탈취: 사용자가 입력한 키보드 입력정보 또는 이벤트 메시지를 텍스트 파일로 저장
- 맵핵(Map Hack) 사용(카드게임 상대 패보기): 보이지 않게 설정된 상대편의 위치나 카드 패를 가시화
- 게임 아이템(Item) 복사: 게임 서비스에서 사용하는 아이템을 게임 서비스 버그나 취약성을 사용하여 개수를 늘리는 행위
- 메모리 위변조: 허가되지 않은 프로세스가 메모리에 접근하여 게임 서비스 프로세스의 메모리를 조작하는 시도
- 오토 마우스 입력 및 매크로(Macro) 사용: 게임 서비스 진행에 필요한 입력을 자동으로 입력하여 반복적인 게임 서비스 진행을 수행
- 스피드 핵(Speed Hack) 사용: 사용자의 컴퓨터를 비정상적으로 빠르게 만들어 줌으로써 게임 서비스 내에서 사용자의 이동 및 공격속도를 증가시키도록 조절
- 사기(Fraud): 게임 서비스를 이용하고 있는 상대편을 거짓으로 속여가면서 아이템을 획득하는 방식
- 아이디(ID) 및 패스워드(Password) 유출: 상대방의 권한을 가져오기 위하여 비 도덕적인 방법으로 아이디와 패스워드를 탈취

위와 같이 게임 서비스 침해유형 분류기준을 가지고 게임 서비스 침해사례에 대한 설문을 게임 서비스 개발자 혹은 운영자와 게임 서비스 사용자를 대상으로 10일간(2007년 3월 10일~20일)진행한 결과, 수거된 유효 설문(게임 서비스 개발자 혹은 운영자에 대해서는 20개, 게임 서비스 사용자에 대해서는 100개) 중 68.9% 이상이 클라이언트 영역에서의 게임 서비스 침해사례를 경험한 것으로 조사되었으며, 클라이언트 영역 내에서는 오토 프로그램(28.3%), 소프트웨어 위변조(28.0%), 스피드 핵(20.0%) 순으로 게임 서비스 침해사례가 많이 발생하는 것으로 나타났다. 그리고 네트워크 영역(20.9%)에서는 패킷 스니핑(Packet Sniffing), 서버 영역(9.3%)에서는 백 도어(Back Door) 공격이 주된 게임보안 침해사례로 조사되었으나 그 비율은 그리 높지 않았다. 클라이언트 영역에서 게임 서비스 침해사례가 많이 발생하고 있는 이유는 일반적인 정보보호에서는 외부 침입자가 정보자산에 대한 침해공격을 통하여 서비스 운영방해와 정보획득을 진행되지만 게임 서비스 분야에서는 사용자가 좀 더 쉽고 편하게 게임 서비스를 즐기기 위해서 사용자 스스로 게임 서비스 침해도구를 사용하는 특성에 기인한다.

이러한 게임 서비스 침해를 방지하기 위한 게임 서비스 운영기업의 실제적인 대응은 아직 미진한 상태(50%)이며, 대응방안을 수립한 서비스 기업들도 단순한 정보보호 시스템 도입(42.0%)에만 한정되어 정보보호를 추진하고 있었다. 이러한 이유는 게임 서비스를 위한 정보보호 기술 개발은 게임 서비스의 특성과 시스템에 관한 경험적 지식을 요구하기 때문에 기존의 일반적인 응용소프트웨어를 대상으로 하는 정보보호 연구 내용을 게임 서비스 정보보호 분야에 그대로 적용시키기에는 한계성을 가지고 있기 때문이다.

Ⅳ. 게임 서비스 유형별 사례분석

본 연구에서는 <표 4>와 같이 국내에서 가장 많은 사용자 분포를 보이고 있는 게임 서비스를 대상으로 클라이언트 영역에서 가장 많은 침해사례를 발생시키고 있는 오토 프로그램, 소프트웨어 위변조, 스피드 핵 등에 관하여 세부적인 침해사례 분석을 진행하였다.

〈표 4〉 게임 서비스 침해사례 분석대상 분포

기준	게임 서비스 종류	분 포	비 율(%)
운영 환경	온라인 게임 서비스	27	90.0
	PC 게임 서비스	3	10.0
장르별	롤플레잉	19	63.3
	캐주얼	8	26.7
	슈팅	2	6.7
	전략 시뮬레이션	1	3.3
서비스 단계	시범 서비스	10	33.3
	무료 서비스	12	40.0
	유료 서비스	8	26.7
합 계		30	100

주) 조사대상 게임 서비스: 2007년 1월 30일 현재, 국내에서 서비스 되고 있는 온라인 게임 서비스

오토 프로그램 사례로서 사전에 입력을 한 대화 내용을 게임 내에서 동일한 글자를 주기적으로 반복하여 생성하거나, 게임 캐릭터가 사냥을 하게 되는 경우 마우스로 매번 클릭하지 않아도 설정한 시간에 따라 자동적으로 창을 휘두르는 반복적인 행동이 진행되는 것을 볼 수 있다. <표 5>는 조사대상 서비스에서 추출한 오토 프로그램과 기능을 정리한 것이다.

소프트웨어 위변조 프로그램을 사용하면 <그림 1>과 같이 무작위로 생성된 정품 인증번호를 사용하여 게임을 실행하게 하거나 이와 같은 행위를 차단하기 위한 보호 프로그램의 실행을 중지시킬 수 있다.

게임 서비스에 스피드 핵 프로그램이 설치되면 <그림 2>의 사례에서 특정장소(동그라미 부분)까지의 도착시간이 정상적으로는 약 10초 정

〈표 5〉 게임 서비스에서 추출된 오토 프로그램

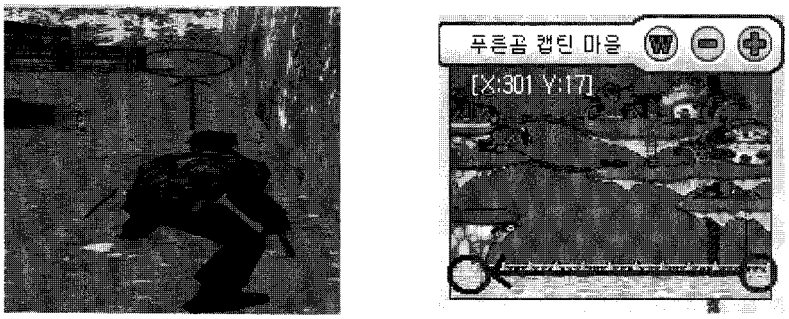
추출한 게임 서비스	오토 프로그램	동작 방식
군*	G-Chat_v1	일정시간을 간격으로 반복적으로 동일한 글자를 입력
라****	sinroo_jansa	
실***	Macro G	자동으로 특정 키 값을 입력함으로써 아이템 자동적용
칼***	playKAL	
탄**	G Macro	특정 마우스 좌표 값이나 키 입력 값을 자동으로 반복해서 입력
나*****, 천**	ZleGEMc	일정시간을 간격으로 마우스 클릭과 특정 문구를 반복해서 입력
데**	QMouse	
클***	AutoCloverSetup	자동으로 공격 수행 및 아이템 적용
한**	AutoClickProject	자동으로 낚시를 하기 위한 던지기 및 들어올리기 기능수행

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

〈표 6〉 게임 서비스에서 추출된 소프트웨어 위변조 프로그램

추출한 게임 서비스	소프트웨어 위변조 프로그램	동작 방식
니* * ***	Keyzen	정식제품 번호를 생성하여 인증을 통한 게임실행
쯔**	zweipet	실행 CD ROM이 없어도 게임을 실행
던*****	!FullScreen	전체화면크기의 게임진행 화면을 작은 화면으로 변경
마***	gcdown	마비노기 보안프로그램인 'Guard CAT'의 실행을 차단
스******	loader	정식제품 인증을 거치지 않고 배틀넷에 접속
요***	팅~욕	클라이언트의 은어 사용금지 정책을 차단

도 걸리던 것을 1초 안으로 단축할 수 있게 되며, 또 다른 게임 서비스에서는 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 빨라졌다. <표 7>은 조사대상 서비스에서 추출한 스피드 핵 프로그램과 기능을 정리한 것이다.



〈그림 2〉 스피드 핵 사례

〈표 7〉 게임 서비스에서 추출된 스피드 핵 프로그램

추출한 게임 서비스	스피드 핵 프로그램	동작 방식
대****	SPSF	게임의 진행 속도를 일정 배수만큼 증가 혹은 감소시킴
데**, 빨****, 코**, 탄**	Speed Gear	단축키를 통하여 특정시점에서 게임 진행속도를 일정 배수만큼 증가 혹은 감소시킴
드** *, 바****, 카*****, 칸***, 컴***, 콩****	Speeder	

V. 게임 서비스 침해유형별 기술적 대응방안

게임 서비스 침해유형에 따른 기술을 개발하기 위해서는 게임 서비스를 침해하는 프로그램에 대한 내부구성과 동작원리에 대한 분석이 선행되어야 한다. 이를 위한 분석도구로서 본 연구에서는 현재 시스템에서 실행되는 프로세스의 상세정보(사용하는 모듈, 커널 객체, 파일 등)를 보여주는 'Process Explorer(정보수집단계)', 프로세스를 구성하는 모듈에 대한 상세정보(모듈이름, 파일 종류, 크기 등)와 모듈이 사용하는(또는 제공하는) 함수목록 등을 보여주는 'Dependency Walker (정보수집단계)', 실행 중인 모듈에 대한 상세정보(어셈블리 코드정보, 레지스터 상태정보, 메모리 정보, 콜 스택 정보 등)를 제공함으로써 윈도우 프로그램 바이너리 디버거로 사용되는'Olly Dbg(분석단계)' 등을 사용하였다.

오토 프로그램(G_Chat_v1)이 실행되면, 'Process Explorer'을 통하여 현재 시스템에서 실행되고 있는 프로세스들의 목록과 상세정보를 획득할 수 있다. 프로그램 목록의 아래 부분에 오토 프로그램 프로세스가 발견되었으며, 프로세스가 클릭되면 선택된 프로세스에 대한 세부적인 설명이 기술된다.

그 다음 'Dependency Walker'를 사용하여 오토 프로그램이 사용하는 함수들을 분석하여 가상의 키보드 동작을 발생시키는 함수(SendKeys, keybd_event, mouse_event, SendInput, SetCursorPos, SendMessage, PostMessage 등)를 호출하는지 함수구성 연관도를 점검한다. 점검결과 오토 프로그램을 구성하는 모듈 중에서 특정모듈(USER32.DLL)이 키보드 동작을 발생시키는 함수(keybd_event)를 호출하고 있는 구조를 확인하였다

마지막으로 오토 프로그램 실행과정에서 가상의 키보드 동작을 발생시키는 함수를 실제로 사용하는지를 'OllyDbg'를 통하여 분석하였다. 'OllyDbg'의 실행정지(Break Point) 기능을 사용하여

<표 8> 침해유형에 따른 보호대상 함수

침해유형	보호대상 함수	저장 위치	함수 주요기능
오토 프로그램	keybd_event	User32.dll	키 입력을 생성
	mouse_event	User32.dll	마우스 움직임과 버튼 클릭을 생성
	SendInput	User32.dll	키 입력 또는 마우스 움직임과 버튼 클릭을 생성
	SetCursorPos	User32.dll	마우스의 커서를 명시된 스크린 좌표로 이동
	rtcSendKeys	msvb60.dll	입력된 키보드 값을 전송
	SendMessage	User32.dll	윈도우 특정 메시지를 전송
	PostMessage	User32.dll	
스피드 핵	SetTimer	User32.dll	일정 간격으로 특정 함수가 계속 실행되도록 타이머를 설정
	GetTickCounter	Kernel32.dll	시스템이 시작한 경과 시간을 수신
	QueryPerformanceCounter	Kernel32.dll	실행할 명령어의 위치를 지정하는 레지스터(PC Counter)의 현재 값을 가져오는 함수
	timeGetTime	winmm.dll	시스템 시간을 가져오는 함수
	timeSetEvent	winmm.dll	설정된 시간에 특정 함수를 실행
소프트웨어 위변조	EXE 파일 자체	실행파일	

가상의 키보드 동작을 발생시키는 함수에 적용시킨다. 이 기능이 적용된 함수는 실행될 때 프로그램의 동작을 일시정지 시키게 된다. 스피드 핵과 소프트웨어 변조에 대해서도 게임 서비스 침해 프로그램을 분석한 결과로서 보호해야하는 함수들을 <표 8>에서 간략한 설명과 함께 정리하였다. 특히 보호대상 함수의 주요기능을 살펴봄으로써 향후 개발될 함수의 적용 위험성을 예측할 수 있도록 하였다.

게임 서비스를 침해하는 프로그램에 대한 내부구성과 동작원리에 대한 분석을 마친 후에 는 실제적인 기술적 대응방안을 수립할 수 있다. 오토 프로그램은 시스템에서 제공하는 가상으로 입력을 발생시키는 함수를 통하여 게임 서비스 내에 키보드 또는 마우스 입력 이벤트(event)를 발생시켜 게임 서비스에 적용되도록 한다. 따라서 오토 프로그램을 차단하기 위해서는 침해 프로그램의 가상입력 발생함수의 사용을 감지한 다음 이 함수가 게임 서비스에 전달되는 입력정보를 처리할 경우 이를 차단할 수 있도록 해야 한다. 한편 스피드 핵 프로그램은 시스템에서 제공하는 타이머(Timer) 관련 함수를 가로채어(Hooking) 지정된 증감 값만큼 반영한 다음 게임 서비스에 전달하여 게임 서비스에서 인지하는 시간을 빠르게(또는 느리게) 반응하도록 한다. 따라서 스피드 핵 프로그램을 차단하기 위해서는 타이머 관련 함수의 반환 값을 가로채어 조작여부를 확인한 다음 값이 변경되었을 경우 게임 서비스의 실행을 중단시켜야 한다.

오토 프로그램 및 스피드 핵 등과 같은 침해 프로그램은 게임 서비스 침해를 발생시키는 특정 함수의 동작을 감지한 다음, 특정함수가 게임 서비스에 영향을 미치는 것으로 확인되면 이를 차단하는 과정을 통하여 게임 서비스를 안전하게 보호할 수 있다. 이러한 차단방법으로서 침해 프로그램의 특정함수 사용을 응용 프로그램 수준에서 제어하는 방법(API Hooking)과 시스템 수준(Kernel Level)에서 제어하는 방법(System Ser-

vice Hooking)등이 있다.

응용 프로그램 수준에서 침해 프로그램을 제어하는 방법은 'Import Address Table[1]'을 사용한다. 침해 프로그램이 실행되면 프로그램 내부에서는 가상입력 발생함수의 실제 실행코드(Executable Code)가 저장되어 있는 주소를 가리키고 있는 'Import Address Table'로 프로그램의 제어를 넘기게 된다. 이때 이 테이블에 저장되어 있는 주소를 게임 서비스 침해 프로그램 판단함수의 주소로 교체하여 침해 프로그램의 유무 및 동작차단 기능을 수행 할 수 있다(IAT Patching).

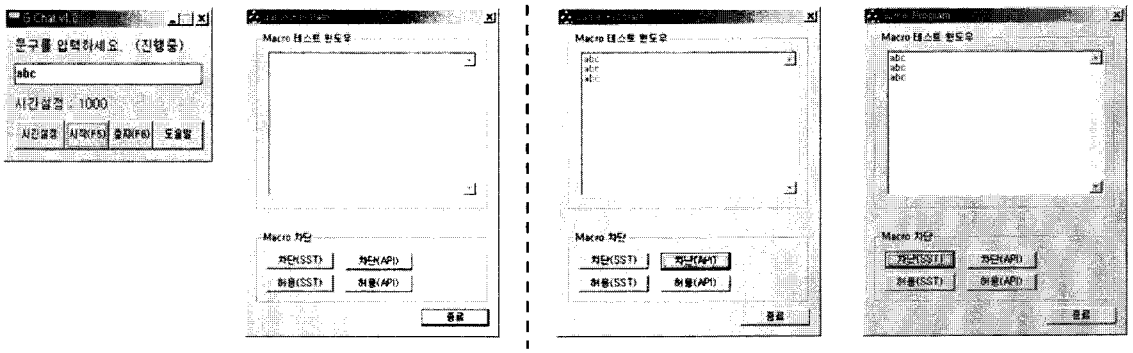
예를 들어 오토 프로그램이 가상의 입력을 발생시키는 'keybd_event' 함수를 사용하기 위해서는 메모리(main memory)에 적재된(load) 'USER 32.dll' 파일에서 해당함수의 실제 주소 값인 'Ox 01056341'을 가져와야 한다. 그러나 게임 서비스가 실행되기 전에 이 주소 값이 침해 프로그램 판단함수의 주소 값 'Ox00452000'으로 변경되었기 때문에 프로그램의 제어는 가상입력 발생함수가 아니라 침해 프로그램 판단함수로 이동하게 된다. 침해 프로그램 판단함수에서는 'keybd_event' 함수를 사용하는 프로그램이 게임 서비스가 아니라면 게임 서비스를 침해할 수 있는 프로그램으로 판정하고, 'keybd_event' 함수를 호출한 프로세스로 복귀 명령어(Return)를 수행한다(프로세스 내 다음명령어 주소 값 'Ox00004 856'으로 이동). 만약 'keybd_event' 함수를 사용하는 프로그램이 게임 서비스 프로세스이면 게임 서비스 진행에 사용되는 정상적인 동작으로 판단하고 'keybd_event' 함수의 원래주소인 'Ox01056341'로 이동하여 동작을 수행하게 된다. 이와 유사한 방법으로 'Import Address Table'의 주소를 변경하지 않고, 'keybd_event' 함수의 실제 실행코드가 있는 부분을 변경하여 원래 코드가 실행되기 전에 게임 서비스 침해 프로그램 함수를 삽입함으로써 침해 프로그램의 유무 및 동작차단을 차단하는 방법도 사용될 수 있다(Code Patching).

시스템 수준에서 가상입력 발생함수를 제어하는 방법은 응용 프로그램 수준의 가상입력 발생함수가 운영체제(Kernel Mode)에서 실행될 수 있는 함수로 변환해주는 시스템 서비스 테이블의 주소를 변경함으로써 가능하다. 침해 프로그램이 실행되면 프로그램 내부에 있는 가상입력 발생함수는 'Import Address Table'를 거친 다음 실제 함수코드가 저장되어 있는 주소로 프로그램의 제어를 넘기게 된다. 함수코드 실행을 진행하면서 가상입력 발생함수는 'KiSystemService'를 사용하여 운영체제에서 동작될 수 있는 함수이름으로 변환된다(예를 들어, sys_kbd_event). 변환된 함수이름은 시스템 서비스 테이블을 참조하여 실제 함수코드가 저장되어 있는 주소로 제어를 넘기게 되는데, 이때 게임 서비스가 실행되기 전에 변경되어진 게임침해 판단함수 주소로 제어가 이동되면서 침해 프로그램의 유무 및 동작차단을 차단하게 된다.

<그림 3>은 응용 프로그램 수준과 시스템 수준에서 오토 프로그램 침해 프로그램을 차단하는 결과를 설명하고 있다. 현재 서비스 되고 있는 게임 서비스에 대하여 본 연구결과를 직접 적용하는 것은 한계가 있기 때문에 문자열을 지속적으로 입력하는 침해 프로그램이 동작되면 이를 감지하여 응용프로그램 수준과 시스템 수준에서 허용 또는 차단하는 도구를 별도로 제작하여 연구된 기술을 검증하였다. 침해 프로그램(G_Chat_v1)이 동작되면, 테스트 윈도우(Game_Program)에 지속적으로 문자열('abc')을 입력하게 되는데, 앞서 설명한 기술이 적용된 테스트 윈도우에서는 응용 프로그램 수준(API 버튼)과 시스템 수준(SST 버튼)에서 문자열의 입력을 차단 또는 허용을 조정할 수 있다.

스피드 핵 프로그램은 시스템에서 제공하는 타이머(Timer) 관련 함수의 사용을 감지하고 이

1) 동적 라이브러리(Dynamic Linking Library)가 메모리로 읽어 들여질 때(loading), 관련되는 함수들의 주소를 가리키는 포인터(pointer)를 저장하고 있는 테이블.



〈그림 3〉 응용 프로그램 수준 및 시스템 수준에서 문자열 입력을 제어

를 제어하여 게임 서비스 침해를 방지할 수 있다. 침해 프로그램(Speeder)이 동작을 시작하면 다양한 타이머 관련 함수를 사용하여 시스템의 속도를 조정하게 되는데, 본 연구내용(AntiSpeedHack)을 적용하면 침해 프로그램이 사용하고 있는 타이머 관련 함수를 추출하고 이 함수들의 사용을 차단할 수 있다.

마지막으로 소프트웨어 위변조는 게임 서비스 실행을 위하여 필요한 특정 파일을 다른 파일로 변경함으로써 정상적인 실행환경이 되지 않았음에도 불구하고 불법적으로 게임 서비스가 실행되는 방식이다. 이에 대한 기술적 대응방안으로는 게임 서비스를 구성하는 파일들의 변조를 차단하여야 하며, 변조가 일어났을 경우에는 정상적으로 게임 서비스가 실행될 수 없도록 하여야 한다. 이와 같은 소프트웨어 위변조에 대하여 본 연구에서는 'Tamper Resistant Software(TRS)' 기술을 개발하였다. 이 기술은 실시간 암 · 복호화 기술, 자체 소프트웨어 위변조 방지기술과 역 분석 방지기술 등으로 구성된다. 위변조 방지기술은 실시간 암 · 복호화 기술(Cryptographic Wrapper) 과 자체 무결성 검사(Self Integrity Check), 메모리 덤프 방지기술(Anti Memory Dump) 등으로 구성된다. 소프트웨어 실시간 암 · 복호화 기술은 소프트웨어를 구성하는 실행파일의 구조(EXE, DLL, OCX, SCR 등)를 분석하여 코드 영역(.text)과 데이터 영역(.data)으로 각각 분리하여 암호화(또는 압축)한 다음, 소프트웨어가 메모리에 적재될 때 복호화(또는 해제)를 진행하면서 최종적으로 실행되게 함으로써 소프트웨어의 정적분석(Disassembly) 불가능하도록 하여 방지하는 기술이다. 이 때 코드 영역 및 데이터 영역 복호화를 위한 키 값은 로더(Loader)에 추가되며, 이 로더 또한 다시 암호화 되어 로더코드에 첨가된다.

자체 무결성 검사기술은 파일 형태에서 체크섬(Check Sum)을 진행한 다음 이 값을 암호학적으로 내포하여 숨긴 다음, 메모리에 적재될 때 체크 섬을 또 다시 진행하여 두 값을 비교해 봄으로써 하여 파일의 무결성을 검사하는 방식이다. 메모리 덤프 방지기술은 실행파일의 헤더 정보를 조작하거나 속임수코드(Tricky Code)를 삽입하여 메모리 침해 프로그램으로부터 덤프를 방지한다.

VI. 결 론

본 연구에서는 최근 급속한 속도로 발전하고 있는 게임 산업에 비하여 상대적으로 미진한 게임 서비스 정보보호를 위한 연구를 진행하였다. 이를 위하여 먼저 현재 운영 중인 게임 서비스들을 대상으로 침해현황과 이에 대한 대응방법들을 조사하여 정리하였다. 조사결과 게임 서비스 침해 현황조사에 관한 주요결과 내용으로서

게임 서비스에 대한 침해경험은 서비스 개발자 및 운영자응답자 수의 70%, 서비스 사용자 응답자 수의 38.5%가 게임 서비스 침해경험이 있다고 답하였다. 이에 비하여 게임 서비스 침해를 방지하기 위한 실제적인 정보보호 시스템의 구축 및 대응책 수립현황은 설문 응답수의 58%이하로 나타났다.

조사된 게임 서비스에 대한 침해사례를 체계적으로 분류하기 위하여 일반적인 정보보호 침해유형 분류체계와 함께 게임 서비스 침해에 대한 특성을 종합하여 게임 서비스 분야에 적합한 게임 서비스 침해유형을 먼저 정의하였다. 게임 서비스 침해유형은 일반적인 응용소프트웨어에서 발견될 수 있는 침해유형과 비교하여 볼 때 서버나 네트워크 영역에는 상호 유사한 침해유형이 존재하고 있으나, 클라이언트 영역에서는 좀 더 세분화된 침해유형을 정의할 수 있었다. 그 결과 소프트웨어 위변조, 키보드 입력정보(Key Log) 탈취, 맵 핵(Map Hack) 사용, 게임 아이템(Item) 복사, 메모리 위변조, 오토 마우스 입력 및 매크로(Macro) 사용, 스피드 핵(Speed Hack) 사용, 사기(Fraud), 아이디(ID) 및 패스워드(Password) 유출 등으로 정의되었으며, 이 중 오토 프로그램, 소프트웨어 위변조, 스피드 핵 순으로 게임 서비스 침해사례가 많이 발생하는 것으로 나타났다.

이를 참고로 하여 본 연구에서는 국내에서 가장 많은 사용자 분포를 보이고 있는 게임 서비스들을 대상으로 클라이언트 영역에서 가장 많은 침해사례를 발생시키고 있는 오토 프로그램, 소프트웨어 위변조, 스피드 핵 등에 관하여 사례분석을 진행하였다. 사례분석 과정을 통하여 게임 서비스 침해를 발생시키는 침해 프로그램들을 추출하였으며 다양한 분석도구를 사용하여 침해 프로그램의 내부구성과 동작원리를 정리하였다. 그 결과 다양한 게임 서비스 침해 프로그램으로부터 보호되어야 하는 시스템 함수들의 목록들이 정리될 수 있었고, 침해 프로그램이 보호대상 함수들을 사용할 때 이를 감지하여 차단하는 연구를 응용 프로그램 수준과 시스템 수준에서 설계하고 검증하였다.

정보보호 기술개발을 위하여 게임의 특성과 시스템에 관한 경험적 지식을 요구하고 있기 때문에 기존의 정보보호 연구내용을 그대로 적용시키기에는 한계성을 가지고 있다. 따라서 본 연구의 결과는 게임 서비스 정보보호를 위한 연구의 방향성을 제시함과 동시에 게임 서비스를 포함하는 응용소프트웨어 보호기술 개발에도 적용될 수 있을 것으로 기대한다. 그러나 게임 산업이 발전하면서 다양한 형태의 게임 서비스 침해사례가 발견되고 있으며, 특히 최근에는 키보드 입력정보(Key Log) 탈취, 맵 핵(Map Hack) 사용, 게임 아이템(Item) 복사, 메모리 위변조 등의 침해사고들이 급격히 증가하고 있기 때문에 이에 대한 기술적 대응방안 수립은 필수적으로 요구되고 있다.

한편 게임 서비스 사용자에 대한 이러한 보안성 강화는 다른 측면에서 바라볼 때에는 상대적으로 기능성의 약화를 가져올 수 있다. 다시 말하면 게임 서비스 침해 프로그램에 대한 기술적 대응방안이 적용됨으로써 사용자는 게임 서비스 속도 저하, 부가적인 저장장소 필요성 대두, 게임 서비스와 정보보호 프로그램 사이의 충돌 등과 같은 불편함을 느낄 수 있다. 따라서 향후 연구과정에서는 본 연구에서 제시한 기술적 대응방안 적용에 따른 제한점을 별도로 추출하여 기능성 지원방안과 조화를 이루는 방법연구가 필요하며, 정보보호 요소기술 개발과 부합되게 정보보호 관리체계(물리적 정보보호, 관리적 정보보호 등)를 설계하는 연구가 병렬적으로 진행되어야 한다.

참 고 문 헌

정윤경, 기준백, 천정희, "온라인 게임 아이템의 안전한 전자 거래 시스템", 한국정보보호학

회논문지, 제13권, 제3호, 2003.

중소기술정보진흥원, "중소기업 정보화 역기능 실태조사 연구", 2004.

한국정보보호진흥원, "정보화 역기능 실태조사 연구", 2003.

한국정보보호진흥원, "정보화 역기능 실태조사 연구", 2004.

한국게임산업진흥원, "2005년 대한민국 게임백서", 2005.

Abbott, R. P., J. S. Chin, J. E. Donnelley, W. L. Konigsford, S. Tokubo, and D. A. Webb, "Security Analysis and Enhancements of Computer Operating Systems", *Institute for Computer Sciences and Technology*, National Bureau of Standards, 1976.

Aslam, T., "A Taxonomy of Security Faults in the Unix Operating System", Master's Thesis, Purdue University, 1995.

Bisbey, II R, Hollingworth D., "Protection Analysis: Final Report", University of Southern California, 1978.

Bishop, M., "A Taxonomy of UNIX System and Network Vulnerabilities", Technical Report CSE-95-10, Purdue University, 1995.

Bishop, M. and D. Bailey, "A Critical Analysis of Vulnerability Taxonomies", Technical Report CSE-96-11, Dept. of Computer Science, University of California at Davis, 1996.

Brian, Marick, "A Survey of Software Fault Surveys", Technical Report UIUCDCS-R-90-1651, University of Illinois at Urbana-Champaign, 1990.

Eugene, H. Spafford, "Common System Vulnerabilities", Proceedings of the Workshop on Future Directions in Computer Misuse and Anomaly Detection, 1992.

Howard, J. D., "An Analysis of Security Incidents on the Internet", Ph. D Thesis, Carnegie Mellon University, 1997.

Lough, D. L., "A Taxonomy of Computer Attacks with Applications to Wireless Networks", Ph. D. Thesis, Virginia Polytechnic Institute and State University, 2001.

Otwell, K. and B. Aldridge, "The Role of Vulnerability in Risk Management", IEEE Proceedings of the 5th Annual Computer Security Applicant Conference, 1989.

Peltier, T., "Information Security Risk Analysis", Auerbach, 2001.

Rajeev Nagar, "Windows NT File System Internals: A Developer's Guide", O'Reilly & Associates, 1997.

Ray, Hunt and Simon, Hansman, "A Taxonomy of Network and Computer Attacks", *Computer & Security*, Vol.24, No.1, 2005.

Wenliang, Du and Aditya, P. Mathur, "Categorization of Software Errors that led to Security Breaches", In Proceeding of the 21st National Information Systems Security Conference (NI SSC'98), 1998.

Information Systems Review
Volume 9 Number 3
December 2007

The Study of Information Security Technologies for Security Incidents in Online Game Service

Hang Bae Chang* · Kyung Kyu Kim** · Si Jin Lee***

Abstract

*This study focused on online game security, which has been considered relatively insignificant when compared to the online game industry's rapid growth. In this study, the state of security incidents in the Korean game industry and security solutions for such cases were examined. At first the security incidents were classified according to the type of game security infringement. Based upon this classification, this study analyzed the causes that give rise to infringement of online game security, and developed technical solutions for such cases. Finally, this study verified whether or not these technical solutions could be applied to online game sites.

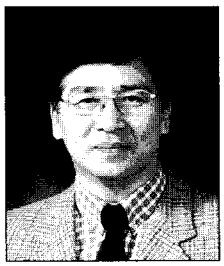
Keywords: Game Security, Auto Program, Speed Hack, System Service Table Hooking

* Department of Business Administration, Daejin University
** Graduate School of Information, Yonsei University
*** Department of Computer Engineering, Daejin University

◐ 저 자 소 개 ◑

장 항 배 (hbchang@daejin.ac.kr)

연세대학교 정보대학원 정보시스템 관리 전공으로 박사를 취득하였으며, 현재 대진대학교 경영학과 교수로 재직 중이다. Lecture Notes in Computer Science, Computing and Informatics, Journal of Computational Information System 등의 국제학술지 및 경영정보학 연구, 중소기업 연구, 한국통신학회 논문지, 한국IT서비스학회 논문지 등의 국내 학술지에 논문을 게재한 바 있다. 주요 관심분야는 유비쿼터스 컴퓨팅, 내부정보 유출방지 기술, 정보보호 관리체계 등이다.



김 경 규 (kyu.kim@yonsei.ac.kr)

미국 Utah 대학에서 경영정보 전공으로 박사를 취득하였으며, 현재 연세대학교 정보대학원 교수로 재직 중이다, MIS Quarterly, Journal of MIS, Information and Management, Accounting Review, Database 등의 국제학술지 및 경영학 연구, 경영정보학 연구, 중소기업 연구 등의 국내학술지에 논문을 게재한 바 있다. 주요 관심분야는 e-Business Strategy, Trust in B2C e-Commerce, Knowledge Sharing in Supply Chain, Ubiquitous Computing 등이다.

이 시 진 (sjlee@daejin.ac.kr)

중앙대학교 전자계산학과에서 박사학위를 취득하였으며, 현재 대진대학교 컴퓨터공학과 교수로 재직 중이다. Lecture Notes in Computer Science, 한국정보과학회 논문지, 한국정보처리학회 논문지 등의 논문을 게재한바 있으며, 주요 관심분야는 분산 시스템 및 시스템 소프트웨어, 리눅스 및 임베디드 시스템, 인터넷 보안, 유비쿼터스 컴퓨팅 등이다.

논문접수일 : 2007년 05월 29일 **게재확정일 : 2007년 11월 07일**
1차 수정일 : 2007년 09월 24일