온라인게임 계정도용 탐지모델에 관한 연구

최화재, 우지영, 김휘강
고려대학교 정보보호대학원
{chj870809, jywoo, cenda}@korea.ac.kr

Online Game Identity Theft Detection Model based on Hacker's Behavior Analysis

Hwa Jae Choi, Jiyoung Woo, Huy Kang Kim
Graduate School of Information Security, Korea University

요 약

온라인상에서 사용자의 개인정보를 불법적으로 취득, 악용하는 계정도용 문제는 금전적인 이득을 얻을 수 있는 MMORPG(Massively Multi-player Online Role Playing Games)에서 특히 빈번하게 발생하고 있다. 많은 사람들이 게임을 이용하여 심각한 피해로 이어질 수 있기 때문에 이에 대한 대책마련이 시급함에도 불구하고, 이를 예방하거나 탐지하는 기법에 대한 연구가 많이 부족한 실정이다. 본 연구에서는 온라인게임에서 발생했던 실제 계정도용 사례 분석을 통해 계정도용의 유형을 체계적으로 정의하고, 유형별로 계정도용을 분류하는 자동화된 탐지모델을 제안한다. 실 계정도용 사례를 분석한 결과 속전속결형, 신중형, 대담무쌍형의 3가지로 구분되었으며 이 분류 체계와 탐지모델을 국내 주요 온라인게임회사 중 한 곳에 적용하였다. 본 연구에서 제시한 유형별 탐지모델은 해킹의 유무만을 판정하던 기존의 모델보다 탐지에 있어서 향상된 성능을 보였다.

ABSTRACT

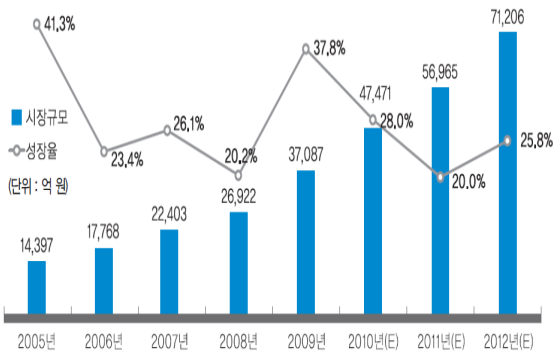
Identity theft happens frequently in popular MMORPG(Massively Multi-player Online Role Playing Games) where profits can be gained easily. In spite of the importance of security about identity theft in MMORPG, few methods to prevent and detect identity theft in online games have been proposed. In this study, we investigate real identity theft cases of an online game and define the representative patterns of identity theft as the speedy type, cautious type, and bold type. We then propose the automatic identity theft detection model based on the multi-class classification. We verify the system with one of the leading online games in Korea. The multi-class detection model outperforms the existing binary-class one(hacked or not).

Keywords : Online Game Security, Identity Theft Detection, MMORPG, Neural Network, Behavior Analysis

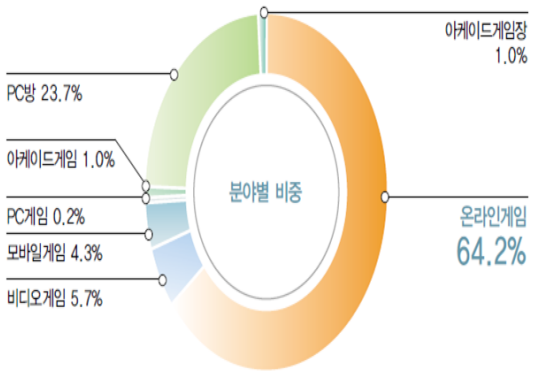
접수일자 : 2011년 10월 28일 심사완료 : 2011년 11월 22일
교신저자(Corresponding Author) : 김휘강

1. 서 론

오늘날 많은 사람들이 게임을 여가활동으로 즐기고 있다. 이에 따라 게임은 점점 하나의 문화로서 세계 곳곳에 자리 잡기 시작하고 있다. 특히나 국내의 온라인게임시장의 경우 잘 형성된 네트워크 인프라에 힘입어 1990년대 후반부터 활성화되기 시작하여 해마다 그 규모가 증가하고 있는 추세이다[그림 1]. 온라인게임은 2010년 게임시장의 64.2%를 넘어섰고 아케이드 게임장과 PC방을 제외하면 전 게임 플랫폼 중에서는 85.2%를 차지해 사실상 현 게임시장의 성장을 견인하고 있다고 봐도 과언이 아니다. 2012년에는 약 7조원정도의 규모를 형성할 것이라고 추정되고 있다[그림 2].



[그림 1] 국내 온라인게임시장 규모 및 향후 전망
(2010 대한민국 게임백서, 한국콘텐츠진흥원)



[그림 2] 2010년 국내 게임시장 분야별 비중
(2011 대한민국 게임백서 요약, 한국콘텐츠진흥원)

이렇게 온라인게임시장이 커져감에 따라 금전적인 이득을 취하려는 불법적인 행위들 또한 급격하게 증가하였으며 그 기법 역시 점점 다양화되었다[5,13]. 게임을 하면서 얻게 되는 게임아이템과 게임머니는 본래 게임 내에서만 가치를 가지나, 한정된 게임머니나 게임아이템을 손쉽게 얻길 원하는 사람들이 늘어나면서 현금거래시장이 형성되게 되었다[14].

아이템베이, 아이템매니아 등 국내 현금거래 사이트에서 거래된 자료를 집계한 내용에 따르면, 국내 게임아이템시장의 규모는 2009년 1조 5천억을 넘었으며 당시 온라인게임시장 규모 3조 7천억([그림 1] 참조)의 약 41%, 2010년에는 2조에 근접하는 거대한 시장을 이루었다. 또한 리서치회사인 Park Associates에 의해 2010년에 수행된 조사에 따르면 전 세계적으로 온라인게임 아이템 구입을 통해 발생될 수익은 2015년까지 60억 달러(한화 약 6조 7천억)가 될 것으로 예상되고 있다. 이는 거의 한 국가의 게임 시장 규모와 맞먹는 수준이다. 보다 쉽고 빠르게 게임자산을 모을 수 있도록 게임봇[1]을 사용하거나, 계정도용을 통하여 다른 사용자 계정의 자산을 훔치는 등의 부정행위를 하는 사람들이 생겨나기 시작하였다. 이에 따라 온라인게임을 안전하게 사용자들에게 서비스하기 위해 온라인게임 보안은 필수적인 요소가 되었다. 온라인게임 보안의 목표는 크게 2가지로 나눌 수 있다. 첫째는, 온라인게임회사의 시스템, 네트워크, 데이터베이스, 프로그램과 같은 IT 자산을 보호하는 것, 둘째는 사용자의 개인정보, 게임자산 등과 같은 고객의 정보를 보호하는 것이다. 온라인게임 보안을 위협하는 다양한 요인들이 있지만, 그중에서 고객에 대해 행해지는 부정행위 중 가장 빈번하고 큰 피해를 유발할 수 있는 것이 바로 계정도용이다. 온라인상에서 사용자의 개인정보를 불법적으로 취득, 악용하는 계정도용 문제는 특히나 쉽게 금전적인 이득을 얻을 수 있는 MMORPG(Massively Multi-player Online Role Playing Games)에서

1) 게임자산 취득을 목적으로 사람을 대신해 자동으로 게임을 플레이하도록 설계된 인공지능 프로그램

빈번하게 발생하고 있다. MMORPG는 수많은 사람들이 게임에 참여하기 때문에 상대적으로 현금거래에 대한 수요도 높기 때문이다. 게임회사에서 계정도용의 예방과 그 피해에 대해 적절히 대응하지 못하면 사용자는 게임에 불만을 느껴 게임을 떠나버리게 되고, 회사의 이익에도 큰 손해를 끼치게 된다. 더불어, 이때 도난당한 사용자의 아이디와 패스워드는 은행 사이트와 같은 타 웹사이트 해킹으로 이어져 2차적인 피해를 유발할 가능성을 가지고 있다. 따라서 온라인서비스를 제공하는 회사들은 자신의 고객을 보호하고 서비스의 경쟁력을 확보하기 위해 계정도용을 예방하고 발생 시 적절한 대응을 취해야만 한다. 빈번하게 계정도용 문제가 발생하는 여러 서비스 영역들 중에서, 주로 금융권의 계정도용 탐지와 관련해서는 많은 연구가 이루어져 왔으나, 온라인게임에 대해서는 그 중요성과 파급력에도 불구하고 많은 연구가 이루어지지 못한 실정이다.

게임회사는 일반적으로 사용자의 아이템 복구나 데이터의 소실과 같은 비상 상황을 대비해 사용자와 게임 시스템에 관련된 중요한 정보와 상태들을 로그로 기록하고 있다. 온라인게임에서 계정도용을 일으키는 해커는 일반 사용자의 계정에서 아이템과 게임머니를 훔쳐 자신의 계정으로 옮기는 일련의 행위들을 하게 되는데 이런 흔적들 역시 시스템에 의해 기록이 된다. 따라서 로그분석을 통해 해커의 흔적을 발견할 수 있는 메커니즘이 구축된다면 계정도용에 보다 능동적으로 추적하고 대응할 수 있을 것이다. 로그 분석을 통한 계정도용 탐지 접근은 추가적인 시스템 장비가 필요하지 않고 서버 측에 남겨진 로그를 이용하기 때문에 시스템에 부하를 거의 주지 않으며 또한 사용자의 편의성을 헤치지 않는다는 강점을 가진다. 이 논문에서는 국내 온라인게임회사 게임로그와 그 게임에서 실제로 발생했던 계정도용 사례들의 로그를 분석하여 계정도용이 발생할 때 나타나는 특징들을 연구하였다. 이 특징들은 정상적인 사용자들에게서는 발견되지 않는 비정상적 행위들이며, 이를 통해 온라인게임에서 발생하는 계정도용 유형을 분류하는 기준을 제시한다. 또한, 이런 해커의 행동패턴을 반영한 자동화된 계정도용 탐지모델을 제시하여 효율적으로 계정도용을 탐지해낼 수 있도록 하였다.

2. 관련 연구

온라인게임 상에서 발생하는 부정행위는 본 논문에서 연구한 계정도용 이외에도 사기, 게임봇, 사설서버[2], 골드파밍[3] 등 다양하다. 최성락[2]은 경영학적 관점에서 이런 부정행위들의 주목적인 현금거래가 왜 발생하는 가를 아이템 수요자와 공급자 관점에서 분석하였다. 게임 내에서도 현실과 마찬가지로 각 입장 사이의 욕구에 대한 합의의 일환으로 현금거래가 발생한다고 말한다. 한창희[3] 등은 캐릭터간의 거래, 게임 외부에서의 사용자간 거래, 전문 중개상을 통한 거래 등과 같은 현금거래 방식의 변화와 발전에 대해 정리하고 현금거래와 관련되어 발생할 수 있는 다양한 이슈들을 언급하고 있다.

온라인게임에서 발생하는 범죄 유형을 연구하고 이에 대한 대응방법을 개발하기 위해, 범죄 유형을 체계적으로 분류하기 위한 시도들이 있었다. Yan과 Randell[16]은 근본적인 취약점과 부정행위의 원리, 그리고 그 부정행위의 결과 관점에서 온라인게임에서 발생할 수 있는 부정행위를 분류했다. 이 분류체계는 온라인게임 상에서 발생하는 대부분의 부정행위를 포함하고 있으며, 계정도용은 이 분류체계의 "Compromising passwords" 항목에 속한다. Hu와 Zambetta[9]는 MMORPG (Massively Multi-player Online Role Playing Game) 의 속성, 속성에 따른 위협, 그리고 위협에 대한 수단의 관점에서 부정행위 분류체계를 제안했다. 이들은 Yan과 Randell의 분류체계를 사용하였으며[16], 기

2) 게임회사에 의해 정식으로 서비스되는 서버가 아닌 제3자에 의해 운영되는 서버, 사용자를 빼앗아가 게임회사에 손실을 끼침

3) 정상적인 게임플레이는 하지 않고 계속적으로 게임머니만 생성하는 행위, 이렇게 생성된 게임머니를 시장에 판매

본적인 결함의 근원들과 이 근원들로부터 결함이 발생하게 되는 가능한 경로들, 그리고 이러한 결함들을 완화하기 위한 대응책들을 언급하였다. 그러나 이들은 모두 계정도용이 속한 “Compromising passwords”에 대한 구체적인 내용은 다루지 않았다. 이와 같은 분류체계들은 온라인게임에서 발생하는 부정행위들을 체계적으로 이해할 수 있는 틀을 제시했다는 데 의미가 있지만, 각 부정행위들의 특징에 대한 보다 심도 있는 분석이 필요하다.

계정도용과 관련해서는, Ki[12]의 연구에서 저자들은 사회공학(Social Engineering)이 아이디와 패스워드를 탈취하는데 악용된다고 말하고 있으며, Chen[7]의 연구에서는 실제 계정도용 당한 사례들에 대한 조사를 통해 온라인게임에서 계정도용이 얼마나 심각한 피해를 초래하는지를 보였다.

온라인게임에서 계정도용 보안이 점점 중요해지면서, 계정도용을 예방, 탐지하기 위한 방법들이 제안되기 시작했다. 안면인식(Facial recognition), 지문인식(Fingerprint recognition), 그리고 필기인식(Handwriting)과 같은 바이오메트릭(biometrics)을 활용한 방법들이[11] 계정도용을 예방하기 위한 방법으로 제안되었으며, 탐지를 위한 방법론으로는 키보드 타이핑 패턴(Keyboard typing patterns), 마우스 움직임(Mouse movement dynamics)을 분석하는 방법들이[8,15] 제안되었다. 또, Chen과 Hong[6]은 게임 사용자들의 게임 플레이 중 연속적인 움직임 사이의 대기 시간(사용자로부터 아무런 입력이 없는 상태)의 패턴을 통해 사용자 개개인을 판별하는 특정 개체의 인식이라는 새로운 바이오메트릭 방식을 제시했다. 이렇게 여러 예방 및 탐지에 관한 방법들이 제안되어졌지만, 계정도용이 실제 어떤 형태로 일어나고 있는가를 연구하고 이 계정도용을 체계적으로 분류, 실제 탐지모델에 적용시켜 계정도용을 탐지한 예는 지금까지 없었다. 본 논문에서는 온라인게임에서의 계정도용 유형을 분류하고, 이 분류체계를 통해 계정도용을 탐지해내는 모델을 제안한다.

3. 방법론

3.1 계정도용 유형의 체계적인 분류

실제 발생한 계정도용 사례들을 관찰해 본 결과, 대부분 금전적인 이익을 노리고 도용한 계정 내 게임머니나 게임아이템을 이동시키는 과정이 특징적으로 나타난다. 이를 상세히 분석하기 위해 게임 내 경제 활동과 관련된 게임 로그 데이터를 주요 분석대상으로 하였으며, 이를 통해 정상 사용자들과 구분되는 계정도용의 특징들을 찾고 이 특징들에 근거하여 3가지 계정도용 유형을 정의하였다. 각 유형을 분류하는 기준으로 해킹속도(Acting speed), 거래패턴(Trading pattern), 트랜젝션 빈도(Transaction Frequency)와 거래채널(Trading channel)이 사용되었다.

● 해킹속도(Acting speed)
- 빠른 속도(Fast speed) : 이 특성을 가지는 해커는 짧은 시간 내에 원하는 목적을 달성하고 접속을 종료한다. 보통 수십 초 이내의 접속시간을 가진다.
- 보통 속도(Normal speed) : 약 수백 초 정도의 접속시간을 가진다.
- 느린 속도(Slow speed) : 짧은 시간 내에 해킹이 일어날 것이라는 일반적인 기대와 다르게 상당히 긴 시간에 걸쳐 해킹을 하는 사례들도 있다. 이 특성을 가지는 해커는 만족하는 목표에 도달할 때까지 접속을 계속 유지한다. 원 사용자에게 발각되는 것도 개의치 않으며, 수천 초 정도의 접속 시간을 가진다.

● 거래패턴(Trading pattern)
: 일반적으로 온라인게임 자산은 게임 내에서 일정한 가치를 지니는 돈(게임머니)과 물건(게임아이템)의 2가지 형태로 존재한다.
- 게임머니 탈취 : 자산을 취하기 위한 가장 쉬운 방법으로 해커들은 피해 계정이 현재

소유하고 있는 게임머니를 갈취한다.

- 아이템을 게임머니로 변환 : 계정 내의 캐릭터는 게임자산을 고가의 게임아이템의 형태로 가지고 있는 경우가 많다. 캐릭터가 착용하고 있는 장비(고가 아이템의 일종)를 해제하고 인벤토리(캐릭터가 가지고 있는 게임 내의 개인 창고)를 살펴 고가의 아이템이 있는지를 확인한다. 이 아이템들을 게임 내의 다양한 방법(아래 설명 참조)을 통해 게임머니로 바꾼다. 요즘은 온라인게임에서 계정도용 발생 시 아이템을 쉽게 다른 캐릭터로 옮길 수 없도록 하기 위해 보호조치를 취한다(예, 귀속 시스템 - 직접적인 캐릭터 간 거래를 통한 교환은 불가능). 그러나 게임머니는 그 화폐적 특성상 특별한 제약을 받지 않기 때문에 해커는 아이템을 쉽게 옮길 수 있는 게임머니로 바꾸는 작업을 거치게 된다. 또한 보호 메커니즘이 없다하더라도 많은 아이템들을 모두 옮기는 것은 매우 불편한 일이고 해커 자신의 계정 캐릭터의 아이템을 보관할 수 있는 창고의 공간에도 한계가 있기 때문에 거래 및 보관이 용이한 게임머니로 바꾸는 것이 유리하다. 게임머니로의 변환 작업은 게임 내 상점 NPC(Non-Player Character)[4]에게 시세보다 낮은 가격에 판매하여 짧은 시간 내에 간단하게 처리할 수 있는 방식과 판매대행[5], 개인상점[6], 거래(1대1 판매)를 통해 일반 사용자들에게 높은 가격으로 팔지만 팔리기까지 시간이 오래 걸리는 방식의 두 가지가 있다. 이 두 가지를 혼합한 방식도 존재한다(값싼 아이템은 상점에 팔고, 비싼 아이템은 일반 사용자들에게 팔아 이윤을 취하는 방식).

● 트랜젝션 빈도(Transaction Frequency)

: 대부분의 경우 1~2번 이내의 트랜젝션을 통해 계정의 자산을 해커의 계정으로 옮기지만, 특정 해킹 사례들의 경우 반복적인 갈취 행위가 발생한다. 이는 언제 원 사용자에 의해 발각될지 모르기 때문에, 현재 계정에 있는 게임머니를 먼저 옮겨 이득을 취하고, 이 후 아이템을 게임 내 상점이나 일반 사용자에게 팔아 일정량의 게임머니가 모이면 다시 옮기는 방식을 취하기 때문이다.

● 거래채널(Trading channel)

: 거래채널은 해킹의 주 목적인 게임머니를 어떤 경로를 통해 해커 자신의 계정으로 옮기는 가에 대한 것이다.

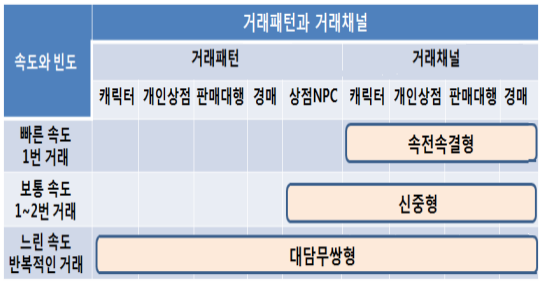
- 미리 대기시켜둔 해커 자신의 캐릭터에게 게임 아이템과 게임머니를 옮기기 위해 거래를 요청한다.
- 해커는 미리 만들어 둔 자신의 판매대행 NPC, 개인상점, 경매 등에 거래를 요청한다. 해커는 이러한 채널을 통해 팔 아이템에 비정상적으로 높은 가격을 설정해 놓기 때문에, 해커가 조종하는 피해자의 캐릭터를 제외하고 아무도 이 아이템을 사지 않는다. 즉 직접적으로 주고받는 1대1 거래를 통하지 않고도 게임머니를 이동시킬 수 있다. 게임 내 거래시스템이 어떻게 구현되었냐에 따라 이 방식이 정상적인 거래보다 더 편리할 경우, 이 방식을 해커가 더 선호하기도 한다.

위에서 제안한 기준에 따라, 계정도용에서의 유형을 [그림 3]과 같이 속전속결형, 신중형, 대담무쌍형의 3가지로 구분하였다.

4) 사용자들에게 게임을 플레이하는데 기본적으로 필요한 게임아이템들을 판매하는 인공지능 캐릭터

5) 일정량의 수수료를 받고 사용자가 원하는 가격에 다른 사용자에게 아이템을 자동으로 광고, 판매해주는 인공지능 캐릭터, 옥션 시스템과 비슷하고 게임마다 다른 형태로 존재

6) 자신의 캐릭터로 상점을 만들고 아이템을 판매하기 위한 광고 문구를 자신의 캐릭터 근처의 사용자들에게 자동적으로 반복해서 전달할 수 있는 시스템, 개인상점은 판매대행과 다르게 사용자의 캐릭터가 게임에 접속해있어야 한다는 단점을 가짐

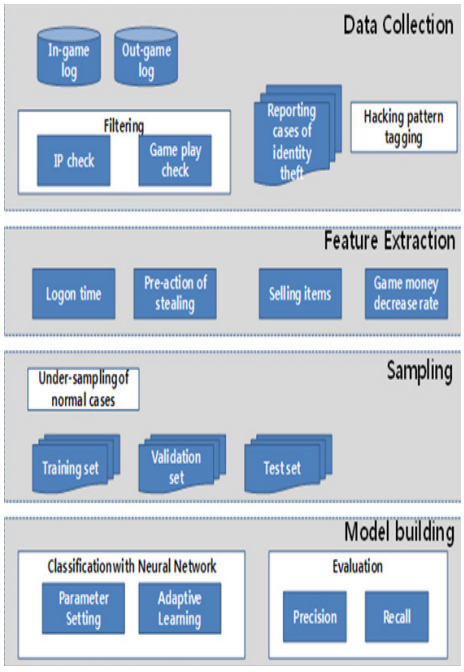


[그림 3] 계정도용의 세 가지 유형

1. 속전속결형
   : 이 유형은 표적 캐릭터가 접속 당시부터 소유하고 있는 게임머니만을 빠르게 훔치기 때문에 매우 짧은 시간 내에 발생한다. 해커는 미리 준비해 둔 해커의 캐릭터, 개인상점, 판매대행 등을 통해 게임머니를 갈취한다.
2. 신중형
   : 이 유형은 표적 캐릭터의 인벤토리를 살피고 아이템들을 상점 NPC에게 판매한다. 이 같은 짧은 시간 내에 간편하게 게임아이템을 게임머니로 바꾸는 작업을 한다. 얻을 수 있는 이득은 일반 사용자에게 파는 것보다 낮지만 처리 속도가 빠르고 리스크가 적다. 게임머니를 옮기는 거래채널은 역시 캐릭터, 개인상점, 판매대행 등이었다.
3. 대담무쌍형
   : 일반적인 기대와 다르게, 특정 해킹은 짧은 시간 내에 일어나지 않는다. 이 유형의 해커는 판매대행과 개인상점을 통해 고가의 아이템을 비싼 가격으로 일반 사용자들에게 파는데, 그렇기 때문에 아이템이 팔리기까지 어느 정도 시간이 필요하지만 해커는 개의치 않는다. 해커는 아이템이 팔리기를 계속 기다리거나 접속을 잠시 끊고 일정 시간이 지난 후 다시 접속해서 아이템이 팔렸는지를 확인하는 식의 로그인, 로그아웃을 반복한다. 계속해서 같은 식으로 고가의 아이템을 팔고 게임머니가 일정량 모이면 사전에 준비해둔 자신의 캐릭터로 옮기고 다시 파는 식의 반복적인 방식을 취한다. 저가 아이템들은 상점에 팔아버리는 흔적 역시 발견된다.

3.2 계정도용 유형기반 탐지모델

분류된 계정도용의 유형에 따라 계정도용 접속을 자동적으로 탐지해내는 계정도용 탐지모델을 제안한다. 세 가지 계정도용 유형을 시스템에 학습시키기 위한 학습알고리즘으로는 높은 탐지 성능을 얻기 위해 인공신경망을 사용하였으며, 이를 이용하여 각 계정도용 유형에 따른 특징을 학습시켰다. [그림 4]와 같이 데이터 수집(Data collection), 특징 추출(Feature extraction), 샘플링(Sampling)과 모델수립(Model development)의 4단계를 거쳤다.



[그림 4] 자동화된 계정도용 탐지 시스템 디자인

데이터 수집 단계에서 게임 내부로그(in-game log), 게임 외부로그(out-game log), 그리고 게임회사에 계정도용으로 신고 된 계정도용 사례들을

수집하였다. 게임 내부로그는 게임 플레이 시 게임 서버 내에서 발생한 이벤트들을 기록한 로그로, 전투, 사냥, 채집, 경제활동 등의 모든 액션을 포함한다. 게임 내부로그에서 계정도용 사례 분석을 통해 정상적인 사용자와 해커를 구별할 수 있는 비정상적인 행동들을 선별하여 정의했다. 게임 외부로그는 게임 플레이와 관련된 내부 액션로그는 아니지만, 로그인시 최종 접속지 IP 주소, 웹접속 로그와 같은 게임서비스를 운영하는데 있어 발생되는 로그를 의미한다. 이 로그들 중에서 IP주소와 같은 해당 접속 시에 남겨지는 연결정보를 계정도용 탐지에 필요한 정보로 활용하였다. 계정도용 사례들은 실제 해킹 피해 사례들로, 고객 센터를 통해 신고된 목록을 받아 방대한 규모의 게임 내부로그와 게임 외부로그 안의 해킹의 흔적을 추적하였다. 이 세 가지 데이터 분석을 통해 3.1장에서 정의한 대로 계정도용의 유형을 분류하고, 각 특징을 정의하였다. 이 분류체계는 계정도용 탐지모델을 구축하기 위해 사용되었다.

계정도용 탐지에 앞서 전체 접속에서 확실하게 계정도용이 아니라고 판단되어지는 접속을 제거하기 위해(즉, 용의자를 줄이기 위해) 2가지 필터링 과정을 거쳤다. 첫째, 계정도용 탐지를 수행하는 시점 전 5일 간의 각 계정에 접속했던 IP를 계정별로 모아서 계정별 IP 기록 리스트를 만들었다. 탐지 시점에 계정에 접속한 IP가 이 기록 리스트에 있는 해당 계정의 과거 IP들 중 같은 것이 있다면 정상적인 사용자의 접속으로 판단한다. 그렇지 않다면 의심되는 접속으로 판단하고 다음 탐지 작업을 수행한다. 매 접속 시 이용되는 IP는 이용중인 ISP를 변경하였거나, 지역을 바꾸어서 접속하지 않는 한 큰 변경은 발생하지 않는다. 즉, 가정내 PC, 회사의 PC, 주로 이용하는 PC방이 특정되어 있는 경우라면, 이 사용자의 접속IP는 3~4개의 IP대역으로 좁혀질 수 있다. 둘째, 캐릭터를 육성하는 행위를 했다고 판단되는 사용자 역시 필터링하였다. 해커의 목적의 특성 상 경제적인 활동만을 하게 되어서 일반적으로 사냥과 같은 경험치를 얻는 행위를 하지 않기 때문이다.

또한, 탐지모델을 수립하기 위해 '세션(session)'이라는 개념을 정의하였다. 로그분석 결과, 해커는 탐지되는 것을 피하기 위해 잦은 로그인과 로그아웃을 하는 경향을 보였다. 또한 위에 언급했던 대담무쌍형과 같은 이유로 로그인과 로그아웃을 반복하는 경우가 있었기 때문에, 이를 통합적으로 분석하기 위해, 동일 해커가 행한 모든 행위들을 모아 종합적으로 분석한다. 즉, 세션은 해커가 하루 동안 동일 IP로 같은 캐릭터의 최초 접속부터 마지막 접속까지의 모든 행위를 포함하는 기간을 나타내는 개념이다. 한 계정에는 여러 개의 캐릭터를 만들어서 육성할 수 있는데 계정도용의 흔적들은 캐릭터 단위로 남기 때문에 캐릭터를 기본 단위로 사용하였다. 이 정의된 각 세션 당 계정도용이라 판단할 수 있는 비정상적인 행위들이 일어났는가를 체크하는 특징들(Feature set)을 추출하였으며, 이 특징들은 필터링을 거친 의심 접속들을 다시 검사하는데 사용되었다.

분석을 통해 발견된 계정도용의 특징으로는 먼저 계정을 해킹하는 주된 목적은 게임머니와 아이템을 훔치고, 현금거래 시장에서 현금화 하는 것이기 때문에, 해커는 보통 고가의 아이템을 보유하고 있는 높은 레벨의 캐릭터 계정을 표적으로 삼게 된다는 것이다. 실제 해킹 사례 분석을 통해서도, 계정도용이 캐릭터 레벨과 상관관계가 높은 경향성을 확인할 수 있었다. MMORPG에서, 캐릭터는 장비 형태의 아이템을 소유하거나 인벤토리에 아이템을 보관한다. 아이템을 게임머니로 바꾸기 위해, 해커는 보통 인벤토리를 훑어보거나 장비를 해제하는 것과 같은 게임머니를 훔치기 위한 사전 행동을 한다. 그리고 다양한 방법들을 통해 이 아이템들을 팔아 게임머니로 변환시킨다. 경제적인 행위에 편향된 해커의 행위를 반영하기 위해, 캐릭터가 아이템을 추출하거나 다양한 방법을 통해 아이템을 팔았는가에 대한 체크를 특징 셋에 포함시켰다. 아이템 추출은 고가의 장비를 보석으로 바꾸는 것으로, 보석은 장비와는 다르게 용도가 다양하여 고가

에 쉽게 거래될 수 있기 때문에 속전속결형을 제외한 두 유형에서는 모두 발생했다. 장비탈착율(장비를 해제한 횟수를 장비를 장착한 횟수와 장비를 해제한 횟수의 합으로 나눈 비율, 장비탈착횟수 / (장비장착횟수 + 장비탈착횟수))을 고안하여 이 값을 특징 셋의 하나로 사용하였다. 일반적인 경우에 장비해제 횟수는 장비장착 횟수보다 많지 않다. 만약 이 비율이 0.5를 초과하면, 이 캐릭터는 해킹당했을 가능성이 있다고 간주할 수 있다.

마지막으로, 분석결과 일반적인 사용자의 경우 모든 게임머니를 한 번에 소모하는 경우가 흔치 않은 반면에, 해킹당한 계정들은 한 번의 거래를 통해 게임머니가 0으로 감소(100%)하거나 거래채널에 따라 80%이상의 감소율이 나타났다(판매대행이나 개인상점을 거래채널로 사용할 경우 해커는 하나의 아이템에 보통 백만, 천만의 큰 단위의 규칙적인 숫자를 설정해놓는 것이 게임머니를 빼가기가 수월하다. 따라서 이런 경우 게임머니 감소율이 100%가 될 수가 없다). 이런 게임머니의 급격한 감소를 반영하기 위해 게임머니 감소율을 정의하여 사용하였다. 일반적으로 캐릭터가 보유하고 있는 게임머니의 80%가 한 번의 거래를 통해 없어진다는 것은 부자연스러운 현상이다. 또한, 위에서 언급한 바와 같이 반복적으로 아이템을 팔고 게임머니를 옮기는 양상을 보이는 공격적인 유형의 해커를 탐지하기 위해 80% 이상 게임머니 감소가 2번 이상 일어났는가를 체크하여 특징 셋에 포함시켰다(판매대행으로 아이템을 팔아 게임머니로 변환하기 위해서는 수수료가 필요하므로). 더불어 해커는 원 사용자에게 발각되는 걸 피하기 위해, 해킹에 필요한 일만 빠르게 처리하는 경향을 보였다. 이런 점을 고려하여 접속 유지시간(Logon time)을 포함시켰다. 지금까지 설명한 특징들을 [표 1]에 정리했다.

[표 1] 계정도용 탐지모델 특징 셋

특징들(Features)
접속 유지시간(Logon time)
캐릭터 레벨
게임머니 감소율 80%이상
게임머니 감소율 100%이상
게임머니 감소율 80%이상이 2번 이상 발생
아이템 추출유무
장비탈착율
아이템들을 NPC에게 판매
아이템을 판매대행으로 판매
아이템들을 개인상점을 통해 판매
해커가 게임머니를 옮긴 경로 (거래, 판매대행, 개인상점)

이와 같이 특징 셋을 구성한 뒤, 신경망에 계정도용 특징을 학습시키기 위한 학습 데이터와 학습된 신경망으로 자동화된 탐지를 실험하기 위한 검증 데이터를 구축하였다. 정상적인 사례수가 계정도용 사례수보다 훨씬 많은 샘플 수의 불균형 문제를 해결하기 위해 Undersampling을 수행했다. Hulse와 Khoshgoftaar의 연구결과에 따르면[10], 분류작업에서 클래스 사이의 불균형 문제를 해결하기 위한 Undersampling 방법은 실험결과 다른 방법에 비해 좋은 성능을 보인다. 정상 세션과 실제 계정도용 당한 세션으로 구성된 학습 데이터를 신경망을 이용해 지도학습(Supervised learning)하여 자동화된 분류 시스템을 구축하였다. 신경망은 금융사기 탐지나 파산예측과 같은 다양한 분야에서 자동화된 예측 모델을 구축하는데 사용되어 왔다. 신경망은 모델 복잡도를 증가시키고 계산량이 많다는 단점을 가지고 있지만 다른 지도학습 방법에 비해 변화에 적응력이 높은 모델을 생성하며[4], 높은 정확도를 보장한다. 제안한 모델의 성능을 평가하기 위해, 정밀도(Precision)와 재현율(Recall)의 두 가지 지표를 설정했다. 재현율은 게임회사로부터 받은 실제 계정도용 사례들이 탐지모델을 통해 어느 정도 탐지가 되는가를 나타내는 비율이고, 정밀도는 탐지된 결과들이 실제로 계정도용이 맞는가에 대한 비율이다. 두 가지 지표는 아래와 같이 정의된다.

$$Precision = \frac{TP}{TP+FP} \qquad Recall = \frac{TP}{TP+FN}$$

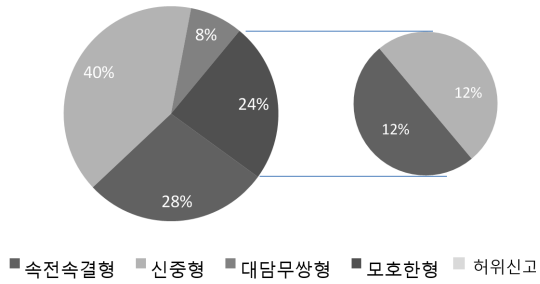
TP: $True\ Positive$
($correctly\ identified\ as\ identity\ theft$)
FP: $False\ Positive$
($wrongly\ identified\ as\ identity\ theft$)
FN: $False\ Negative$
($wrongly\ identified\ as\ normal\ case$)

(식 1) Precision과 Recall

4. 실 험

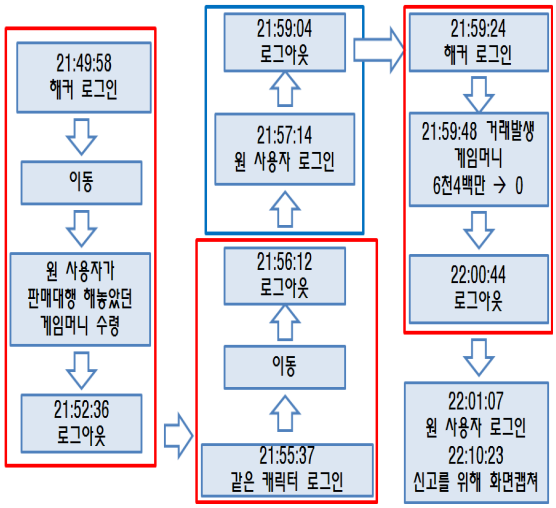
4.1 계정도용유형 분석

국내의 주요 MMORPG 회사 중 한 곳에서 데이터 셋을 얻어 사례 연구를 진행했다. 이 게임에서는 2010/6/25 ~ 2010/7/4 동안 총 25개의 계정도용 사례가 고객센터를 통해 접수되었다. 각 사례를 면밀히 조사하여 비정상적인 특징을 정의, 추출하고 제안한 분류 체계를 구성하였다. [그림 5]는 이 분류 체계에 따라 25개의 계정도용 사례의 분류결과를 나타낸다.



[그림 5] 계정도용 사례 해킹 패턴 분류

위 그림에서 신중형의 해킹이 가장 많이 발생한다는 것을 알 수 있다. 25개의 사례들 중 3개의 허위신고와 3개의 모호한 경우를 제외하고 총 19개 중에서 10개가 신중형, 7개가 속전속결형, 그리고 2개가 대담무쌍형이었다. 모호한 사례의 경우, 해커는 해당 계정의 모든 캐릭터에 접속했으나 아무 행위도 하지 않고 접속을 끊었다. 사용자의 직접적인 피해는 없었지만 누군가 자신의 계정에 접속했기 때문에 신고를 한 것이라 추측된다. [그림 6,7,8]은 각 해킹 유형의 대표적인 사례이다.

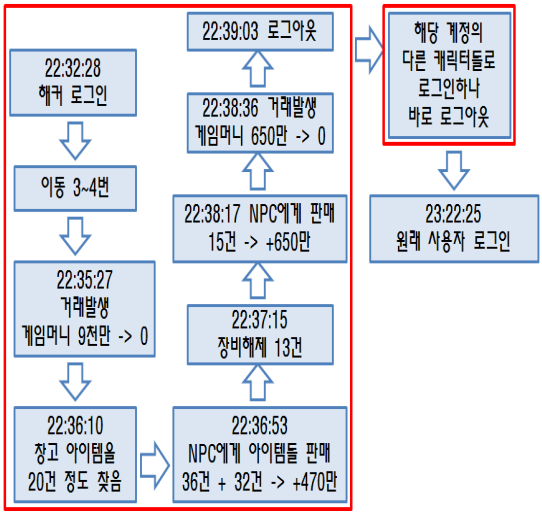


[그림 6] 속전속결형 사례

[그림 6]은 속전속결형으로 해커는 계정의 원 사용자가 잠시 접속해있지 않은 사이에 로그인을 해서 원 사용자가 판매대행을 통해 팔아두었던 아이템의 대금을 수령한다. 이 후 잠시 로그아웃을 했다가 다시 로그인 한다. 해커가 해킹한 계정의 게임머니를 옮기기 위해 자신의 캐릭터를 준비시키는 작업이 필요했기 때문이라고 추측된다. 다시 로그인을 한 해커는 계정의 캐릭터가 가지고 있는 모든 게임머니(100%)를 자신의 계정으로 옮기고 접속을 종료한다. 원 사용자가 곧바로 다시 로그인을 하지만 해킹 당했다는 사실을 깨닫고 약 10분 후에 신고를 위해 화면을 캡쳐를 한 흔적이 발견된다. 이동 흔적이 발견되는 이유는 아이템을 팔거나 거래를 하기 위해서 게임에 존재하는 마을이라는 곳으로 가야하기 때문이다.

[그림 7]은 신중형으로 우선 캐릭터가 가지고 있는 게임머니를 모두 자신의 계정으로 옮긴다. 이동 후 해당 캐릭터의 창고를 살펴 고가의 아이템을 꺼낸다. 아이템을 모두 NPC에게 팔아 빠르게 게임

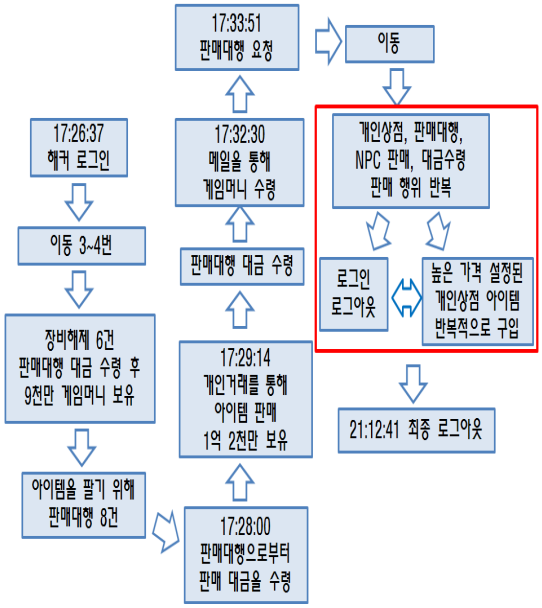
머니로 바꾸고 자신의 계정으로 옮긴다. 즉, 이 타입의 해커는 아이템으로부터 짧은 시간 내에 이득을 얻고 접속을 종료할 수 있는 상점 판매와 같은 판매방법을 택한다.



[그림 7] 신중형 사례

[그림 8]은 대담무쌍형으로 앞의 두 사례와는 다르게 얻을 수 있는 게임머니는 많지만 오랜 시간이 걸리는 판매대행이나 개인상점을 통해 아이템을 파는 흔적이 발견되며, 아이템을 팔고 일정 금액이 모이면 자신의 계정으로 가져가는 반복적인 양상을 보인다. 해당 그림의 사례의 경우 약 4시간이라는 긴 시간 동안 해킹 과정이 지속되었다.

이 계정도용유형 분류결과는 자동화된 계정도용 탐지모델을 구축하기 위해 사용되었다.



[그림 8] 대담무쌍형 사례

4.2 신경망을 통한 계정도용 탐지

Undersampling을 통해 정상적인 사례를 추출, 계정도용 사례와 합쳐 학습 데이터를 구축하였다. 학습 데이터는 각 세션 벡터의 집합으로 13개의 요소([표 1]에 나온 13개의 변수)로 구성되어 있으며, 이 셋으로 학습된 자동화된 탐지 시스템은 탐지 결과를 4개(속전속결형, 신중형, 대담무쌍형, 정상)로 구성되어 있는 출력벡터로 보여준다. 총 31,873개의 세션 가운데 2,094개의 샘플 학습 데이터가 구축되었고, 신경망은 3개의 레이어, 13개의 노드로 구성되었다. [표 2]는 학습한 신경망을 통해 25개의 계정도용 사례를 분류한 결과이다. T1~T4는 각각 속전속결형, 신중형, 대담무쌍형, 정상을 의미한다.

[표 2] 분류 결과

		신경망 분류 결과 유형			
		T1	T2	T3	T4
실제 유형	T1	7/7 (100%)	0	0	0
	T2	0	9/10 (90%)	0	0
	T3	0	0	2/2 (100%)	0
	T4	0	0	0	6/6 (100%)

실험 결과 학습된 신경망은 1개를 제외한 모든 사례를 정확하게 분류하였으며, 3개의 허위신고와 3개의 모호한 경우 모두 T4(정상적인 경우)로 분류하였다. 모호한 형의 경우 피해도 없고 해커가 침입했다는 충분한 흔적이 없기 때문에 정상으로 분류되는 것이 적합하다. 분류되지 않은 1개의 T2 유형의 경우 해커가 어떤 이유로 약간의 경험치를 얻게 되어서 처음 필터링과정에서 제외된 예외 사례이다.

앞의 실험을 통해 분류 시스템이 제대로 동작하는 지를 확인한 후, 실제 계정도용 탐지 성능을 측정하기 위해 검증 데이터를 구축하였다. 전체 세션 중 2가지 필터링 과정을 거치고 특징 셋을 추출한 의심 세션을 탐지 시스템을 통해 분류하고 제대로 분류가 되었는지를 확인하였다. 실험 결과는 [표 3]에 나타내었으며, 계정도용 유형을 분석하고 그 특성에 따라 탐지하는 유형별 탐지 기법과 해킹/정상만을 분류하는 기존의 탐지 기법을 비교하였다. 기존 탐지의 모든 환경은 유형별 탐지와 동일한 조건하에 수행되었다.

[표 3] 탐지 성능 비교

모델	성능 측정	값
기존 탐지 기법	정밀도(Precision) 회귀율(Recall)	0.774 0.874
유형별 탐지 기법	정밀도(Precision) 회귀율(Recall)	0.842 0.970

5. 결 론

본 연구에서는 경제행위와 관련된 로그 분석을 통해, 해킹속도, 트랜젝션 빈도, 거래패턴, 거래채널에 따른 계정도용 유형의 분류체계를 구성하였다. 실제 국내 주요 온라인 MMORPG 회사로부터 데이터 셋을 얻어 사례 연구를 수행하였다. 이를 통해 해커는 서로 다른 행동패턴을 가지고 있다는 것을 밝혔으며, 계정도용의 유형은 속전속결형, 신중형, 대담무쌍형의 3가지 대표적 유형으로 분류됨을 보였다. 또한, 이 분류에 따라 계정도용을 자동적으로 탐지해내는 모델을 제안했다. 각각의 특징적인 계정도용 유형을 반영한 유형별 탐지모델은 기존의 탐지모델보다 정밀도와 재현율에 있어 보다 나은 성능을 보였다. 계정도용의 독특한 특성을 고려한 게임에 특화된 전문 지식과 다양한 특징을 사용하여 정확하고 높은 탐지결과를 얻을 수 있었다.

본 연구결과는 게임회사가 계정도용에 대한 능동적인 전략을 수립할 수 있게 한다. 사전에 사용자로부터 계정도용으로 예상되는 증후가 감지될 경우 긴급조치를 취할 수 있다는 동의를 받은 후에, 속전속결형이 감지가 될 경우 즉시 게임서버에서 접속을 차단하고, 사용자의 비밀번호를 자동으로 변경한 뒤 사용자에게 휴대전화로 알려주는 긴급조치를 취할 수 있다. 대담무쌍형이 탐지될 경우 GM(Game Master)를 통해 행동 패턴을 감시하고, 게임 플레이어 본인여부를 판단하게 할 수 있다. 이와 같이 본 연구 결과를 활용해 계정도용 유형별로, 사용자의 불편을 최소화 하면서도 보안성을 높이는 유연한 대처가 가능하다. 또한 이런 통보조치를 통해서 개인정보 유출에 따른 2차적인 피해를 예방할 수 있는 효과도 얻을 수 있다. 본 논문에서 제안하는 로그 분석을 통한 계정도용 탐지 방법은 단지 서버 측에 기존에 남겨져 있는 로그만을 사용하기 때문에 추가적인 설비나 시스템의 변경이 필요치 않으며, 따라서 직접적으로 시스템의 실시간 서비스나 사용자의 이용에 악영향을 미

치지 않는다. 이는 현재 게임회사에서 제공하고 있는 많은 예방 방법들이 그 불편함 때문에 사용률이 낮고, 낮은 사용률로 인해 발생하고 있는 계정도용 문제에 체계적으로 대응할 수 있는 기반을 제공할 것이다.

본 논문에서 제안하는 탐지모델을 응용하면, 온라인게임회사들은 자신의 시스템 상황에 따른 최적의 탐지 전략을 세워, 고객보안 및 게임보안 향상에 도움을 줄 것으로 기대한다.

참고문헌

[1] 2010 대한민국 게임백서 제1부 산업계 동향 http://www.kocca.kr/center/download_new.jsp?typecd=ics&file=/knowledge/report/kocca/__icsFiles/afieldfile/2011/10/10/3pULQq9k2mr5.pdf

[2] 최성락, "온라인게임 아이템거래 발생 원인 분석", 한국게임학회, 7권, 4호, pp. 125-134, 2007

[3] 한창희, 김정민, 박채희, 홍유진, 김민관, "게임아이템 현금거래의 가치사슬 변화와 동향분석", 한국게임학회, 11권, 2호, pp. 45-56, 2011

[4] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study", Decision Support Systems, 50, pp. 602 - 613, 2011

[5] S. Bono, D. Caselden, G. Landau, and C. Miller, "Reducing the attack surface in massively multiplayer online role-playing games", IEEE Security and Privacy, 7, pp. 13-19, 2009

[6] K. T. Chen, and L. W. Hong, "User identification based on game-play activity patterns", NetGames'07, Melbourne, Australia, 2007.

[7] Y. C. Chen, P. S. Chen, J. J. Hwang, L. Korba, R. Song, and G. Yee, "An analysis of online gaming crime characteristics", Internet Research, 15, pp. 246-261, 2005

[8] D. Gunetti and C. Picardi, "Key stroke analysis of free text", ACM Transaction on Information System Security, 8, pp. 312-347, 2005

[9] J. Hu and F. Zambetta, "Security issues in massive online games", Security and Communication Networks, 1, pp. 83 - 92, 2008

[10] J. V. Hulse, T. M. Khoshgoftaar, A. Napolitano, "Experimental perspectives on learning from imbalanced data", The 24th International Conference on Machine Learning, Corvallis, Oregon, 2007.

[11] Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, 14, pp. 4-20, 2004

[12] J. Ki, J. Cheon, and J. Kang, "Taxonomy of online game security", The Electronic Library, 22, pp. 65-73, 2004

[13] H. K. Kim, "Online game security", Codegate 2009 conference, http://www.hksecurity.net/home/pds/codegate2-1(huykang.kim).pdf, 2009.

[14] G. McGraw, and M. Chow, "Securing online games - Safeguarding the future of software security". IEEE Security and Privacy, 7, pp. 11-12, 2009

[15] X. Peacock, Ke and M. Wilkerson, "Typing patterns: A key to user identification", IEEE Security and Privacy, 2, pp. 40-47, 2004

[16] J. Yan and B. Randell, "An investigation of cheating in online games", IEEE Security and Privacy, 7, pp. 37-44, 2009

최 화 재 (Choi, Hwa Jae)

2011 고려대학교 컴퓨터통신공학부 학사
2011 고려대학교 정보보호대학원 석사과정

관심분야 : 게임보안, 시스템해킹, 웹해킹

우 지 영 (Woo, Jiyoung)

2000 KAIST 산업공학과 학사
2002 KAIST 산업공학과 석사
2006 KAIST 산업공학과 박사
2006 삼성화재 고객관계관리 부서
2008 미국 아리조나대학 인공지능연구실
2011 고려대학교 정보보호대학원 연구교수

관심분야 : 게임보안, 데이터마이닝

김 휘 강 (Kim, Huy Kang)

1998 KAIST 산업경영학과 학사
1999 에이쓰리시큐리티 컨설팅 창업
2000 KAIST 산업공학과 석사
2004 NC소프트 정보보안실장
2009 KAIST 산업 및 시스템 공학과 박사
2010 고려대학교 정보보호대학원 조교수

관심분야 : 게임보안, 침입탐지시스템, 봇넷탐지