정 보 보 호 학 회 지
제27권 제4호, 2017. 8

모바일 게임 보안 동향

김 은 진*

요 약

온라인 게임 내 가상재화를 현실 세계의 재화로 교환할 수 있다는 점 때문에, PC기반 온라인 게임 내 가상세계는 많은 작업장(Gold-farmer)들로 인한 부정행위가 빈번히 일어나고 있다. 사이버 재화를 현금거래하는 RMT (Real Money Trading)은 과거에는 PC기반 온라인게임, 특히 고포류 게임이나 MMORPG와 같은 장르들에 주로 존재했으나, 모바일 게임에서도 최근 몇 년 간 거래시장이 활발해 지고, 가치가 높은 아이템들이 출현하기 시작하면서 거래 규모가 비약적으로 성장하고 있다. 이로 인해, PC게임에서만 존재하던 작업장이 모바일 게임에도 출현하고, 게임계정 도용을 위한 모바일 악성앱이 등장하는 등 모바일 게임 내의 부정 행위 및 공격 시도 역시 증가하고 있다. 모바일 게임은 하드웨어의 성능 제약 문제, 네트워크 통신의 항상성이 보장되지 않는 문제, 안드로이드 등 플랫폼 OS 자체의 보안 문제, 앱 자체의 디컴파일 문제와 같이 근본적으로 해결하기 어려운 취약점이 존재하는 환경에서 구동되기 때문에 PC기반 게임에서의 게임 봇 및 작업장 탐지와 같은 기법을 적용하기에는 적합하지 않다. 본 연구에서는 모바일 게임 보안과 PC 게임 보안 기법들을 비교하고, 향후 모바일 게임 보안 향상을 위해 할 수 있는 방안을 제시해 보도록 한다.

Ⅰ. 서 론

1.1. 개요

온라인게임, 특히 모바일 게임은 스마트폰의 폭발적인 보급과 더불어 빠른 성장을 하였으며, 모바일 앱 중에서 가장 많은 연령층이 즐기고 있는 응용 서비스 중 하나로 자리매김하고 있다.

Unity 사의 2016년 보고서 [1]에 따르면 2016년 모바일 게임 시장은 4백 6억 달러의 수익을 창출하였고, 설치하는 앱 3개 중 1개는 게임앱이었다고 한다. 국내의 경우 2015년 콘텐츠 진흥원의 통계에 의하면 게임시장의 규모는 2015년 10조 7222억 원으로, 2014년 대비 7.5% 성장했으며, 모바일 게임시장은 약 20%의 성장률을 기록하며 3조 4844억 원의 매출액으로 시장점유율 32.5%를 기록했다.

하지만 모바일 게임 앱 자체 및 모바일 게임 서비스를 대상으로 한 공격들 역시 증가하고 있다. 모바일 게임이 첫 태동하던 시기에는 스미싱이나 리패키징된 게임앱 배포를 통해 휴대폰 자체의 권한을 탈취하여 정보유출 등 2차피해를 유발하는 형태가 많았다. 즉, 휴대폰을 공격하기 위하여 게임앱을 이용, 소셜엔지니어링과 결합하여 개인정보유출에 활용하는 형태가 많았다면, 현재는 게임앱 자체를 공격하고 이를 이용하여 모바일 게임서비스를 악용하여 금전적인 이익을 취하려는 형태로 공격의 방향성이 바뀌고 있다.

물론, 초기부터 유행하였던 공격 유형들 역시 현재 시점에도 상당 부분 존재한다. 여전히, 유료로 구매하여야 하는 모바일 게임앱을 리패키징하여 무료로 배포하고, 이를 다운로드 받게 하여 광고앱 부정삽입, 개인정보탈취에 이용하는 경우 역시 많기 때문이다. 다만, 이러한 형태의 공격에 감염되는 비율은 장르 및 지역적 특성을 가지고 있다. 기본적으로 무료게임서비스를 이용하면서 유료 아이템을 in-app purchase 로 구매하는 방식의 과금체계를 선호하는가, 아예 게임의 풀버전을 초기에 유료구매하는 형태 (즉, 모바일 게임이기는 하나 준 패키지 형태의 게임으로서, 상시 온라인으로 유료컨텐츠 이용을 하거나 타 이용자와 상호작용을 할 필요가 거의 없는 장르의 게임)를 선호하는가에 따라 감염율 및 피해가 지역적으로, 시기별로 다르기 때문이다.

본 논문에서는, 게임 개발사가 처리하기 어려운 문제로 인해 발생되는 문제에 대해서는 다루지 않는다. 예컨

이 논문은 2016학년도 경기대학교 연구년 수혜로 연구되었음.
* 경기대학교 국제산업정보학과 (ejkim777@kgu.ac.kr)

데, 이용자들의 보안마인드 개선을 통해서만 해결될 수 있는 문제, 즉, 정식 스토어에서 다운로드 받지 않은 불법 앱을 이용하지 않도록 계도하는 것, 게임 퍼블리싱 플랫폼들 (예: 구글플레이, 앱스토어)에서 보안검증이 엄격하지 않아 원래 게임과 유사한 짝퉁 게임이 유통되어 피해가 발생하는 경우들은 제외하도록 한다.

Ⅱ. 모바일 게임 서비스의 위협 요소 및 대응방안

2.1. 모바일 게임 서비스의 위협 요소

모바일 게임 서비스의 위협 요소들을 발생 지점에 따라 분류를 해보면 다음과 같이 나눠 볼 수 있다.

- 게임클라이언트 단
  - 위치: 게임앱 및 게임앱이 실행되는 디바이스 단
  - 위협요소: 게임앱 메모리 변조, 게임앱 디컴파일, 게임앱 내 지적재산권이 포함된 음원 및 아트 리소스 추출, 게임앱에서 전송되는 패킷 변조, 모바일게임용 봇, 결제 모듈 우회, 루팅된 디바이스에서 동작하는 경우 OS관리자 권한 탈취 후 개인정보 유출 및 시스템 제어
- 네트워크 단
  - 위치: 게임앱이 실행되는 디바이스가 접속해 있는 네트워크 (3G, LTE, Wi-Fi 등)
  - 위협요소: 취약한 인증 및 암호화가 적용되어 운영되는 Wi-Fi 서비스를 이용 중일 경우, 전송되는 패킷의 도감청에 의한 조작
- 게임서버 단
  - 위치: 게임서비스 회사의 IDC 또는 호스팅 서비스
  - 위협요소: 모바일 웹페이지에 대한 웹공격, 게임서버에 DDoS 공격, 서버에 대한 remote exploit 등 전통적인 원격 서버 공격들과 대동소이
- 플랫폼 단 (게임결제, 앱유통 등)
  - 위치: 게임퍼블리싱 플랫폼 (예: 카카오, 라인)에 대한 계정도용 공격, 게임앱 유통 및 결제 플랫폼 (예: 구글플레이, 애플 앱스토어) 상에서의 부정결제 (void purchase 등), 부정 환불 등

2.2. 모바일 게임 보안 기법 및 한계

최근 몇 년간 이러한 위협으로부터 모바일게임서비스를 보호하기 위해 게임퍼블리셔, 게임개발사, 게임개발툴 및 플랫폼 차원에서의 많은 노력들이 있었다.

본 절에서는 게임클라이언트 단, 네트워크 단, 게임서버단, 플랫폼 단 각 위치 별로 모바일 게임과 관련된 보안기술에는 어떠한 것들이 있는지 간단히 살펴보고, 이러한 기술을 적용하는데 어떠한 기술적, 환경적 제약사항들이 있는지 살펴보도록 한다.

- 게임클라이언트 단

  - 1. 디컴파일 방지 및 난독화

Java 와 같이 개발언어의 특성상 디컴파일을 근본적으로 막기 어려운 언어들이 있다. Object C와 같이 상대적으로 디컴파일이 어려운 언어도 있지만, 시간의 문제일 뿐 분석을 못하게 근본적으로 막을 수는 없다. 하지만 최대한 이를 지연시키기 위해 안티디버깅 기법과 난독화 (obfuscation)를 적용하는 것이 일반적이다.

게임앱 패키지 파일 (예: apk)을 추출하여 디컴파일을 통한 분석을 하고, 이를 통해 특정 보안 기능이 bypass 되거나 삭제된 리패키징 앱을 만들어 재배포를 하는 방식도 있고, 게임앱의 구동 중에 게임앱의 프로세스를 제 3의 해킹프로세스가 제어를 하거나, 게임앱이 사용하고 있는 메모리 대역을 스캔하여 체력, 승패여부, 아이템 정보와 같이 게임 결과와 자산 변동량과 같은 민감한 변수값들을 조작할 수도 있다.

이를 막기 위해 게임 개발사에서 자체적으로 난독화 솔루션을 개발하는 경우도 상당 비율을 차지하고 있고, DexGuard, ProGuard, ArXan, TOAST Cloud AppGuard, AppSealing 과 같은 다양한 국내외 무료 또는 상용 보안솔루션들이 존재한다.

  - 1. 이에 대한 한계

기본적으로 난독화된 게임앱들을 실행할 때, 그렇지 않은 게임앱에 비하여 모바일 디바이스의 CPU 및 메모리를 추가로 사용하게 되어 있다. 이로 인해 발열, 속도 지연이 발생할 수 밖에 없는 문제가 있다.

최근 게임들은 전세계에 동시 발매 및 업데이트를 지향하고 있어서 개발도상국들에서 많이 이용하는 저사양 스마트폰에서도 원활히 구동될 수 있도록 성능저하 요

인을 최소화 하고 있다. 이로 인해 강력한 난독화 알고리즘을 적용하기는 어려운 현실적인 문제가 있다.

대부분 현존하는 모바일게임 앱 보안솔루션 들이 난독화에만 초점을 두는 경우가 많고, PC기반 게임들에 적용되어 있는 다양한 역공학 방지 기법들은 상대적으로 디바이스 성능상의 한계로 인해, 모바일 게임에는 적용하기 어렵다.

- 2. 리패키징 탐지 및 방지

역공학에 의해 분석되고 다시 제작된 리패키징 앱들은 유료 앱을 무료로 이용할 수 있도록 하거나, 게임 봇과 같은 악성 프로그램이 동작하기 쉽도록 보안 기능을 삭제 또는 무력화 하거나, 리패키징 앱을 다운받아 실행하는 이용자들의 디바이스 내에서 개인정보를 탈취하기 위해 악성 기능이 은밀히 추가되거나, 광고를 통한 부가 수입을 얻기 위해 리패키징 앱 제작자가 고의로 광고를 삽입하는 경우들이 존재한다.

기본적으로 원래 배포한 게임앱을 위변조한 것이므로 무결성 체크를 통하여 리패키징된 앱을 탐지할 수 있다. 하지만, 초기 구동 때에만 무결성 체크를 하고 런타임 때 주기적, 반복적으로 무결성 체크를 하지 않는 경우가 많아 초기 무결성 체크 모듈만 우회하면 여전히 리패키징 앱들이 동작하는 경우가 많다. 또는 네트워크 기반 게임이 아닌 패키지 성격의 모바일 게임의 경우에는 아예 네트워크를 꺼두어 원격 서버에 의한 무결성 탐지를 무력화 시키고 구동시키는 경우가 많다.

- 2. 이에 대한 한계

초기 구동 또는 런타임 때 이용자의 스마트폰이 항상 안정적인 네트워크 통신 환경이라는 것은 담보할 수 없는 사항이다. 이용자가 느린 네트워크 환경에서 접속할 수도 있고, 고속으로 이동 중에 게임을 플레이 하고 있는 상황일 수도 있으며, 또 모든 이용자가 무제한 데이터 요금제에 가입한 것은 아니기 때문에 주기적, 반복적인 무결성 체크를 위해 데이터 트래픽을 발생시키는 것이 이용자에게 별도의 데이터 이용 요금을 발생시킬 수 있으므로 강제화 하기는 어렵다고 할 수 있다.

원격에서 게임 이용자가 어떠한 통신 환경에서 플레이 중인지를 알 수 없기 때문에, 단순히 무결성 체크를 위한 통신 패킷이나 체크 모듈이 원할히 결과값을 응답하지 않았다는 이유로 제재를 할 수 없다는 정책적인 문제가 있다.

- 3. 루팅탐지

안드로이드 SDK가 설치되어 있어 'su' 명령어가 실행이 되는가와 같이 아주 간단한 루팅 탐지를 하던 방식에서 출발하여, 다양한 형태로 권한을 체크하는 방식으로 진화되었다. 루팅을 허용한 상태에서는 모바일용 게임 봇의 개발 및 동작이 더 용이하기 때문에, 잠재적인 피해 및 공격을 예방하는 차원에서 루팅을 탐지/차단하는 것이 필요하다고 할 수 있다.

- 3. 이에 대한 한계

루팅된 스마트폰을 이용하여 앱을 실행시키는 것이 불법적인 행위는 아니다. 스마트폰의 소유권은 이용자에게 있고, 이용자는 자신 소유의 스마트폰에 루팅을 할 수 있기 때문에, 뱅킹앱과 같이 특수한 용도의 크리티컬한 앱을 제외하고는 루팅을 탐지하더라도 이를 근거로 서비스에 접근을 차단시키는 경우는 거의 발견하기 어렵다.

루팅된 스마트폰에서 게임을 이용시 악성코드에 감염될 확률도 높고, 게임 이용자가 직접 게임앱을 해킹하는 데 이용할 수도 있지만, 루팅된 스마트폰을 모두 탐지하여 차단하는 것에 대한 실익보다 이용자 감소 및 매출 감소로 인한 피해가 훨씬 크기 때문에, 사업적인 이유에서도 이는 향후 적용되기 어려운 보안정책이라 할 수 있다.

- 4. 에뮬레이터 탐지

전통적으로 모바일 게임들은 터치 방식으로 조작되어 마우스나 키보드를 통해 조작을 하는 방식에 비해 조작 속도의 한계가 있어 빠른 속도로 자동화된 프로그램이 게임앱을 구동하여 경제적인 이익을 얻기에는 제약사항들이 많았다.

또한, 루팅을 하지 않을 경우 특정 앱의 프로세스를 후킹하여 조작하는 것 역시 불가능했기 때문에 게임 봇 제작자들은 전통적으로 블루스택이나 녹스와 같은 안드로이드 에뮬레이터를 이용하여 게임앱을 제어하는 방식을 선호해 왔다.

이럴 경우 PC상에서 구동되기 때문에 성능상의 제약, 배터리를 이용 시 가동시간의 제약, 프로그램적인 게임앱에 대한 접근 제약 사항들을 쉽게 극복할 수 있

기 때문에 많은 모바일 게임 봇 프로그램들 및 치팅 프로그램들이 PC기반 에뮬레이터를 통해 구현되어 왔다.

이러한 문제로 인해 모바일 게임 회사들은 원격의 접속자가 현재 순수 디바이스에서 접속을 한 것인지, PC상에서 에뮬레이터를 구동하여 접속을 한 것인지를 탐지하려고 machine ID, OS정보, 버전 정보, 하드웨어 정보와 같은 기기식별정보를 활용하여 에뮬레이터를 탐지하여 왔다. 하지만 이러한 단편적인 정보들의 조합을 통한 시그너쳐 탐지는 가상 디바이스 정보를 조작하여 쉽게 우회가 될 수 있는 문제점들이 있었다.

- 4. 이에 대한 한계

모바일 게임의 초창기에는 대부분의 모바일 게임이 캐쥬얼 게임이나 보드게임과 같은 장르가 대부분이어서 대형 화면을 요구하거나, PC기반 MMORPG 와 같이 장시간 플레이를 하는 경우는 거의 없었다. 하지만 점차 모바일 게임의 장르가 다양해지고, MMORPG 장르의 게임이 인기를 얻어감에 따라 모바일 게임에서도 플레이 시간 역시 점차 길어지는 추세이다. 아예 상시로 전원을 연결한 채로 게임 플레이를 하거나, 삼성DEX 와 같은 별도 디바이스를 이용하여 배터리 시간의 제약, 마우스 및 키보드 입력, 화면 크기와 같은 입출력 상의 제약을 모두 극복하여 새로운 게임경험을 추구하는 유저들도 늘어나고 있다.

이러한 이용자들의 선호도 변화에 따라, 온라인 게임사 역시 최근에는 에뮬레이터로부터의 접속을 특별히 차단하지 않고 있으며, 오히려 PC기반 안드로이드 에뮬레이터를 이용하여 입출력 조작이 편리한 환경에서 접속하는 유저들이 플레이 타임이 긴 만큼 매출발생량도 많다는 점에 주목하여, 에뮬레이터로부터의 접속을 권장하는 경우 역시 존재한다.

- 5. 모바일 게임 봇 탐지 및 차단

초창기 모바일 게임은 대부분 싱글 플레이 방식에, 플레이가 간단한 캐쥬얼 게임 및 보드 게임들이어서, 플레이 시간이 짧고, 플레이 내 이벤트 및 플레이 패턴이 단순하여 사용자들을 패턴인식 방식으로는 명확히 식별해 낼 수 없었다.

그렇기 때문에 PC기반 게임들의 경우처럼 풍성한 feature를 가진 플레이 로그를 기반으로 서버단에서 데이터마이닝과 머신러닝 기법을 이용하여 게임 봇 및 작업장을 탐지해 내는 방식은 모바일 게임에 적합하지 않았다.

하지만, 모바일 게임에서도 PC기반 게임들처럼 풍성한 이벤트와 플레이 스타일을 갖는 MMORPG 장르가 인기를 얻고, 장시간의 플레이를 하는 이용자층이 늘어남에 따라 PC기반 MMORPG 와의 차이가 점차 없어지고 있다.

이에, 모바일 게임에서도 서버 단에 플레이로그를 상세히 남겨 데이터마이닝과 머신러닝 기법을 적용하여 게임 봇을 이용한 유저들을 탐지해 내는 방식들이 점차 보편화 되고 있다.

- 5. 이에 대한 한계

먼저 기술적인 한계로는, 데이터마이닝 기반의 탐지 기법들이 공통적으로 갖는 문제로, 분석에 시간이 소요되어 실시간 탐지가 불가능하다는 한계가 있다. 하지만 이러한 점은 모바일 게임만의 한계는 아니고 데이터마이닝 방식 자체의 한계점으로, stream 방식으로 학습을 하는 신경망 기법들이 접목되면서 극복되어질 것으로 예상하고 있다.

하지만, 모바일 게임의 한계 상 플레이 로그를 상세하게 남길 경우 클라이언트 단에서도 이벤트 발생을 서버와 동기화하기 위해 관련 정보를 네트워크 단과 서버단으로 지속적으로 전송하여야 하므로 통신 데이터 발생으로 인한 과금 유발 문제가 발생할 수 있다.

이러한 기술적인 문제 외에, 게임 봇을 탐지, 제재하는 정책과 관련된 문제가 심각하게 대두되고 있다.

도탑전기 이후에 출시된 대부분의 모바일 게임들이 도탑전기의 성공요인을 분석하여, 자동전투와 같은 이용자에게 편리한 기능을 적극 제공해 주고 있다. 이러한 게임 스타일을 적극 도입한 중국 게임들의 대규모 성공을 벤치마킹하여 다수의 모바일 게임들이 자동전투 기능을 점차 수용하게 되었다. 또한 이용자들의 성향 역시 PC기반 게임에서처럼 직접 모든 부분을 통제하고 플레이를 하려는 성향 보다는 간단히 task 지시를 하고, 결과를 피드백 받는 메타성 플레이 (meta play)를 더 선호하기 시작했다.

더불어 AI기술의 발전 역시 자동전투 및 자동플레이를 원활히 하는데 영향을 끼쳤다.

이러한 유저들의 플레이스타일 선호도의 변화, AI기술의 발전 및 게임회사들의 적극적인 수용이 결국 게임

앱 내에 공식적인 자동플레이, 자동전투를 포함하게 하는 계기가 되었으며, 대부분의 대작 게임들이 이러한 기능들을 포함함에 따라, 게임 봇을 이용하였다는 이유로 제재를 하는 것에 대한 명분이 약해지고 있다.

동시대에, PC기반 MMORPG 게임에서 자동사냥을 게임 봇을 이용할 경우 강력한 제재를 하는 반면, 모바일 게임의 경우에는 공식적으로 자동전투, 자동사냥을 지원하고 있기 때문에, 자동화된 정도의 차이와 게임 장르 및 플랫폼 상에 차이가 있다고는 하지만, 오히려 모바일 게임에서 이를 허용하기 시작함에 따라 PC기반 온라인게임에서의 게임 봇 제재의 명분에도 악영향을 주기 시작했다. 이러한 정책적 충돌은 향후 더욱 강해질 것이며, 이용자들에 의해 제재 정책과 약관을 개정하도록 요구하는 움직임 역시 커질 수 있다는 점에서 주목할 만 하다.

더불어 에뮬레이터 상에서 모바일 게임앱을 동작시키는 것을 게임회사들에서 점차 차단하지 않게 됨에 따라, 고사양의 PC에서 동시에 대량의 에뮬레이터를 동시에 구동하고, 봇을 이용하는 대신에 게임앱에서 공식적으로 제공하는 자동전투, 자동사냥을 이용하는 경우가 늘고 있다.

이에 따라 대량으로 계정을 생성하여 에뮬레이터 상에서 대규모로 정상 게임 앱을 이용한 아이템 생산 및 거래를 하는 유형의 플레이가 늘어나게 되고, 모두 허용한 범위 내에서 이루어지는 합법적인 플레이이기 때문에 모바일 게임 상에서의 게임 봇 및 작업장 탐지는 점차 기술적, 정책적 문제에 부딪히게 될 것으로 예상된다.

● 네트워크 단

- 1. 통신 암호화

게임클라이언트 단과 서버 단 사이에 전송되는 데이터의 안전한 통신을 위해 기밀성과 무결성을 확보하여야 하고 end-to-end 암호화를 적용하는 것이 가장 보편적인 보안기법이라 할 수 있다.

더불어 안전한 통신을 셋업하기 위해 검증된 키교환 방식과 인증방식을 이용하여야 한다.

대부분의 모바일 게임앱에서 이러한 원칙을 준수하여 개발툴에서 제공하는 암호화 라이브러리를 적용하고 있다.

- 2. 이에 대한 한계점

우선 암호화 적용시 성능저하가 발생할 수 있다. 암호화 연산은 기본적으로 CPU를 사용하기 때문에 스마트폰의 CPU사용으로 인한 발열, 배터리 소모, 스마트폰의 성능 저하가 유발될 수 있다. 이러한 점 때문에 일부 온라인게임 개발사의 경우 자체적으로 개발한 경량 암호화 알고리즘을 적용하는 경우도 있다. 또한 일부 보안에 대한 인식이 부족한 온라인 게임사의 경우 XOR과 같은 단순한 연산에 의존하여 데이터를 인코딩 시키는 정도에 그치는 경우가 있어 보안에 심각한 허점을 발생시키고 있다. 더불어 네트워크 단에서 도청될 수 있는 가능성을 무시하고 3G, LTE 의 통신 알고리즘 자체가 안전하다는 가정하에 데이터 통신 암호화를 적용하지 않는 등 보안상 문제점이 많은 게임앱들 역시 다수 존재한다.

더불어, 스마트 폰이 루팅되어 있는 경우, 해커가 네트워크 패킷을 분석하거나, 암호화가 해제된 상태로 메모리 상에 적재된 데이터를 이용하여 암호화 된 결과를 사실상 무력화 시킬 수 있는 문제가 존재한다.

또한 개발 단계에서 개발자들이 암호화 알고리즘을 적용하는 경험의 부족으로 인해, 암호화 키를 하드코딩하여 게임 앱에 포함시키는 문제점이 존재한다. 이럴 경우 게임 클라이언트 단에서 해커가 디컴파일을 하여 게임앱에 적용된 암호화 알고리즘을 알아내고, 하드코딩된 키값을 추출해 낼 수 있게 된다.

패킷분석을 통해 실제로 플레이를 하지 않고 게임서버에서 원하는 결과값을 받을 수 있도록 입력값 조작을 시도할 수 있다. 예를 들어 게임을 플레이하지 않고 아이템 습득 결과를 알리는 메시지를 일방적으로 전송하거나, 게임 승리 시 리턴되는 값을 강제로 서버로 전송하여 플레이 결과를 조작하는 것을 들 수 있다.

요컨대, 네트워크 단 보안은 네트워크 단 보안 그 자체적으로는 한계가 있고 클라이언트 단에서의 난독화, 실행 중 프로세스 보호가 같이 보장되어야 기밀성과 무결성을 담보할 수 있는데, 게임 클라이언트 단의 보안은 보장할 수 없다는 점으로 인해 네트워크 단 보안 역시 담보하기 어렵다는 한계점을 갖는다.

● 게임서버 단

게임 서버 운영체제 설정들에 보안강화 (Hardening)를 하는 것, DDoS 공격 대비를 위해 Anti-DDoS 장비

를 설치 운영하는 것, 원격에서 해커가 서버에 exploit을 수행하는 것을 탐지/차단하기 위해 IPS를 설치 운영하는 것 등 게임서버단의 보안상 이슈는 모바일 게임이라고 하여 전통적인 서버 보안과 다르지 않다.

게임서버 단에서는 시스템 및 네트워크 레벨의 보안 외에도, 계정도용을 탐지하고 게임 내부에 부정행위를 하는 불량이용자들을 적발할 수 있도록 FDS (Fraud Detection System)을 개발, 구축하는 것이 중요하다고 할 수 있다.

- 1. 클라우드 화

스케일업, 스케일아웃 등 손쉬운 확장기능, 관리상 편의성이 있기 때문에 최근 모바일 게임들의 경우 퍼블릭 클라우드를 통해 서비스가 제공되는 경우가 많아지고 있다.

- 2. 이에 대한 한계점

모바일 게임 개발의 특성 상, DevOps 와 같이 개발자들이 직접 앱개발에서부터 테스트 및 서비스 운영까지 직접 수행할 경우 AWS 와 같은 퍼블릭 클라우드를 이용하여 게임서비스를 할 때, AWS 가상머신들의 접근권한을 잘못 설정하는 등 클라우드 관리상의 실수로 인한 문제가 발생할 수 있다.

기술적인 문제점은 물론 아니며, 대형 게임회사를 제외한 많은 모바일 게임 개발 회사들이 소수 인원에 의해 개발과 운영을 하는 경우, 소수의 개발자에 과도한 접근권한이 허용되어 개발과 운영의 분리가 명확히 이루어지지 않아 취약점이 발생할 수 있는 소지가 있다.

● 플랫폼 단

- 1. 결제부정

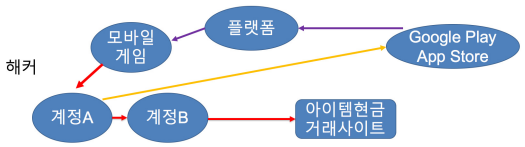
게임회사와 카카오와 같은 게임퍼블리셔와, 결제를 대행하는 앱마켓으로 온라인게임에 참여하는 멀티파티가 있는 경우, 결제부정은 게임생태계 상의 구조적인 문제로 인해 대응하기 어려운 큰 문제점으로 지속되어 왔었다. 국내 온라인게임회사들에 심각한 경제적 타격을 주고 있는데, 이러한 결제부정은 [그림 1]과 같은 절차로 이루어진다.

(1) 게임 아이템을 in-app purchase 로 결제를 하여 구매

(2) 환불신청을 게임회사에 하는 것이 아닌 앱마켓(구글 플레이 또는 앱스토어)에 함

(3) 환불이 이루어졌지만, 게임아이템은 이미 소비되었거나, 타 이용자에게 선물을 하여 세탁을 함. 이때 선물받은 아이템을 유료 아이템 거래소에서 판매하여 금전적 이익을 취한 상태

(4) 게임개발사는 서비스운영 상 게임아이템을 회수하지 못하게 됨



〔그림 1〕 결제부정 흐름도 (예시)

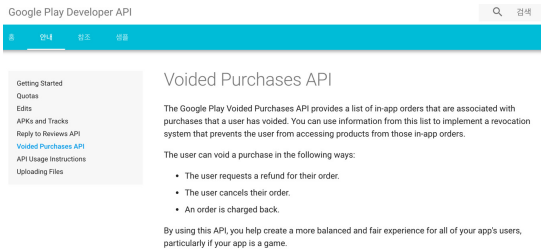
단순한 void purchase 문제인 것 같아 보여도, 탐지와 대응이 어려운 이유는 구글플레이나 앱스토어에서 모바일게임사에 결제 내역 대사 작업에 오랜 기간 (평균 1~2개월)이 소요가 되고, 세부 이용자들의 결제 및 환불 내역이 전달되는 것이 아니라 최종 누적 매출액에 대해 전달하기 때문에 부정행위를 한 이용자를 추적하기 어려운 점이 있다.

더불어 평균 모바일게임의 수명이 2~3개월에 불과하여, 부정이 대량으로 발생했다 하더라도, 성공한 게임이 아니라면 게임수명이 이미 하향세로 돌아서 게임회사의 대응의지가 지속되기 어려운 경우가 많다. 더불어 개발상에 결제루틴 상의 취약점을 사후에 발견한다 하더라도 이를 수정하여 업데이트 하는 과정에서 이미 게임유저들이 대량으로 이탈하여 보안업데이트를 지속할 실익이 없는 경우도 발생한다.

또 공격이 해외에서 들어온 경우에는 수사협조를 원활히 적시에 받기 어렵기 때문에 게임서비스가 유지되는 동안 해커를 추적하기는 현실적으로 한계가 있는 상태이다.

- 2. 이에 대한 한계점

이러한 게임개발사, 퍼블리셔, 플랫폼 사업자 간 비즈니스 로직이 복잡하게 얽혀있고, 실시간 대응이 불가능한 구조라는 점과 게임평균 수명이 2~3개월 밖에 안된다는 점을 이용하였기 때문에, 사실상 게임회사에서 대응할 수 있는 일이 많지 않은 상태였다. 플랫폼 사업자가 2017년1사분기에 void purchase를 탐지하는 API



〔그림 2〕 구글플레이에서 릴리즈한 Void Purchase 탐지용 API

를 개발하여 공개하였으나 [3], 해커들이 5년 가까이 공격을 지속하며 충분히 금전적 부당이익을 얻은 상태이기 때문에 상당히 뒤늦은 대응이라고 할 수 있다.

● 기타 비즈니스 요인

온라인게임, 특히 모바일 게임은 참신한 아이디어로 승부해야 하는 시장이며, 특정 장르와 아이디어를 가진 게임이 성공할 경우 수많은 유사 게임들이 등장하기 때문에 시장에 신속히 진출해야 하는 사업적 특징을 갖는다.

그렇기 때문에, 개발단계에서 개발속도를 늦추는 요인이 되는 시큐어코딩이 무시되는 경우가 많고, 소수의 인원이 개발하는 게임앱들이 많다 보니 보안구현에 전문성을 가지고 개발이 된 앱들이 부족한 상태이다.

더불어 많은 수익을 내기 위해 환금성이 높은 아이템들을 판매할 수 있도록 기획이 되어야 하고, 많은 이용자들을 모집해야 게임 수명이 지속될 수 있기 때문에, 결제 부정과 계정도용이 지속적으로 발생할 수 밖에 없는 생태계적 구조를 가지고 있다.

Ⅲ. 모바일 게임 보안에 대한 예측

3.1. 피씨 게임 봇과 작업장

게임 봇은 사람을 대신하여 게임을 플레이 해주는 AI 프로그램이다 [4]. 이러한 게임 봇은 주로 MMORPG에 존재하며, 환금성이 높은 아이템을 상시 생산한 뒤 현금으로 거래하여 부당이익을 얻게 한다.

이러한 게임 봇을 이용하여 부당이익을 추구하는 기업화된 집단인 작업장들은 [5,6] 지하경제를 형성하며 막대한 이익을 얻고 있다.

작업장들은 이제 PC기반 게임에서 뿐 아니라, 모바일 게임으로 활동 범위를 넓히고 있는데, 이러한 부정행위는 결국 정당한 플레이를 하는 유저들에게 상대적 박탈감을 유발하고, 결국 게임 내 경쟁에서 정상적인 유저들의 도태를 유발, 유저들의 이탈에 큰 영향을 끼치게 된다.

3.2. 모바일 게임 봇과 작업장의 확산

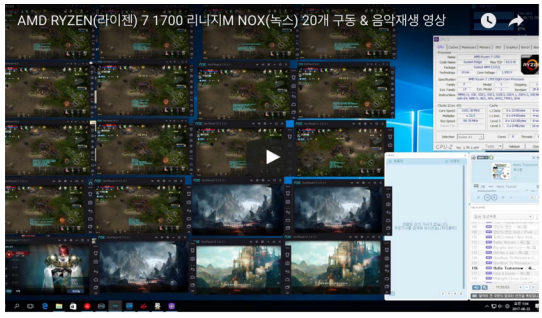
[그림 3]에서 보듯이 에뮬레이터를 이용하여 1대의 PC에서 20개 가까이 모바일 게임을 동시에 실행하는 것을 볼 수 있다.

녹스 및 에뮬레이터를 사용하는데에는 기술적인 제약이나 학습에 필요한 지식이 거의 없기 때문에, 기업화된 작업장 외에도 개인들도 대규모로 게임플레이를 하는 것이 가능하게 되었다.

즉, 기술적 진입장벽이 사라지고 모바일 게임 자체적으로 자동사냥이 지원됨에 따라, 개인화된 작업장이 양산된 상태이다.

향후에는 모바일게임의 성장으로 인해, PC게임보다 모바일게임의 아이템 판매 수익성이 더 높아질 것이고, 기존의 PC게임을 타겟으로 했던 기업형 작업장들이 모바일게임 작업장으로 속속 전환을 하게 될 것이며, 개인들이 직접 개인화된 모바일 게임작업장을 운영하는 일이 급증하게 됨에 따라 게임 생태계를 심각하게 교란시키게 될 것으로 예측된다.

이에 새로운 제재 정책과 이를 뒷받침할 약관, 규정, 법적근거를 준비해야 할 것으로 판단된다.



〔그림 3〕 고사양 PC에서 에뮬레이터를 다수 구동하여 게임플레이를 하는 예

3.3. 랜섬웨어와 결합된 공격 확산

모바일 게임앱을 위장한 스마트폰 용 랜섬웨어가 출현, 증가할 것으로 예상된다. [2] 에서도 살펴보았듯이 전체 앱스토어에 올라가는 앱들 중 1/3 이 게임앱들이라는 점에서 공격자들이 최우선으로 노릴 타겟이 될 것으로 판단된다.

3.4. Intel SGX의 적용

Intel SGX는 하드웨어 기술의 지원을 통해 응용프로그램을 보호하고 기밀성과 무결성을 담보해 주는 Trusted Computing 기술이다 [7].

게임앱이 실행되는 모바일 디바이스는 칩셋이 비 Intel 계가 대부분이므로 게임앱 자체에 Intel SGX 와 같은 하드웨어 기반 보안기술을 적용하는 것은 불가능하다. 하지만, 향후에는 클라우드 기술이 진화함에 따라 게임앱 (게임클라이언트) 단에서는 그래픽 처리와 결과값 디스플레이만을 담당하고, 대부분의 연산 및 게임리소스는 서버에서 이루어지는 클라우드 기반 게임이 늘어날 것으로 예측된다. 이러한 경우, 게임서버 프로그램을 클라우드 환경에서 발생 가능한 위협들로부터 보호하기 위해 Intel SGX와 같은 TEE를 서버사이드에 적용하여 보안성을 높이려는 시도가 확산될 것으로 판단된다.

참 고 문 헌

[1] 안드로이드 환경에서의 모바일 게임 서비스 보안 이슈, 김휘강, 금영준, 한국정보보호학회지, 2013.4

[2] Unity Korea, 2016 모바일 VR 게임 시장 보고서, https://blogs.unity3d.com/wp-content/uploads/2017/02/유니티-코리아-2016-모바일·VR-게임-시장-보고서.pdf

[3] Google, Voided Purchases API, https://developers.google.com/android-publisher/voided-purchases

[4] Jiyoung Woo, Huy Kang Kim. "Survey and research direction on online game security." Proceedings of the Workshop at SIGGRAPH Asia. ACM, 2012.

[5] Hyukmin Kwon et al. "Crime scene reconstruction: Online gold farming network analysis." IEEE Transactions on Information Forensics and Security12.3 (2017): 544-556.

[6] Eunjo Lee et al. "You are a Game Bot!: Uncovering Game Bots in MMORPGs via Self-similarity in the Wild." NDSS. 2016.

[7] Bauman, Erick, and Zhiqiang Lin. "A Case for Protecting Computer Games With SGX." *Proceedings of the 1st Workshop on System Software for Trusted Execution*. ACM, 2016.

〈저 자 소 개〉

김 은 진 (Eunjin Kim)

1999년 2월 : KAIST 산업경영학과 학사
2001년 2월 : KAIST 경영공학과 석사
2007년 8월 : KAIST 경영공학과 박사
2008년 9월~현재 : 경기대학교 국제산업정보학과 부교수
<관심분야> 온라인 게임 보안, 보안 시각화, 보안 경제학, 데이터 마이닝