파일 시그니처 기반의 안티디버깅 방식을 이용한 게임 어뷰징 방지에 대한 연구

*정준영
*안양대학교
e-mail : dsph9245@naver.com

A Study on the Prevention of Game Abuse Using File Signature-Based Anti-Debugging Method

*Jeong JunYoung
*Anyang University

Abstract

최근 게임 산업에서는 특정 유저 혹은 무특정 다수를 기반으로 하는 어뷰징 공격이 점점 늘어나고 있다. 수많은 게임 서비스와 이를 플레이하는 유저들이 늘어남에 따라, 어뷰징에 대한 피해는 나날이 늘어가고 있으며, 어뷰징 공격으로 인하여 작게는 게임 플레이어의 피해를 시작으로 크게는 게임 회사의 금전적인 문제 또는 앞으로의 서비스 운영 결과를 좌지우지할 수 있는 상황을 만들 수도 있다. 따라서 본 논문에서는 윈도우에서 쓰이는 실행 파일 형식인 PE (.EXE) 파일에 대하여 파일시그니처를 기반으로 안티디버깅 방식을 설계하여 어뷰징을 방지하기 위한 방법을 제시하고자 한다.

I. 서론

프로그램에 대한 어뷰징은 게임 뿐만이 아니라 다양한 프로그램에서 발생하고 있으며, 이러한 어뷰징은 단순하게 크랙을 통한 유료 프로그램을 무료로 사용하는 것뿐만이 아닌 개인 혹은 기업에 막대한 피해를 입힐 수 있는 수단이 되기도 한다. 최근에도 많은 플레이어가 플레이하는 게임인 “리그오브레전드”, “발로란트” 등의 게임에서도 어뷰징이 발생하여 사용자의 게임 플레이를 방해하는 데에 이어서 사용자의 추가적인 외부 소프트웨어 사용에도 영향을 끼치는 모습을 보여주었다. 이러한 예시를 보았을 때 게임 어뷰징은 단순히 게임 순위, 게임 플레이와 관련된 문제를 벗어나서, 게임이 설치된 사용자의 PC에 대해서 추가적인 권한 즉, Exploit을 실행할 수 있다고 여겨지며, 이는 곧 사용자의 PC 사용을 방해할 수 있고, 제2, 제3의 영향으로도 작용할 수 있다. 실사례를 보자면, 게임 스트리머들이 특정 게임을 플레이할 때 외부 프로그램인 “디스코드”나 다른 외부 방송 프로그램 작동에 문제를 겪었으며, 이는 앞서 말한 사용자의 PC 사용을 방해하는 행위라고 말할 수 있다. 따라서 본 논문에서는 2장에서는 어뷰징이 발생하는 원인과 현재 어뷰징을 막기 위해서 사용되고 있는 기술들을 설명하고, 3장에서 새롭게 제시하는 어뷰징 방지 방안을 설명할 예정이다.

II. 본론

2.1 어뷰징 발생 원인

[2] 게임에 대한 어뷰징이 발생하는 원인으로는 먼저 게임 시스템에 대하여 취약점이 존재하기 때문에 이를 이용하여 공격자가 어뷰징을 시도하는 사례가 많이 있다. 이 경우에는 특별한 이유 없이 어뷰징을 시도하는 경우가 많은데, 해당 경우 외에도 어뷰징이 발생하는 주요 원인으로는 경쟁에서 우위를 차지하기 위해서 상대 플레이어의 플레이를 방해하여 자신이 더 우위에 올라가기 위해 어뷰징을 이용하고나 경제적인 이득을 얻기 위해 게임 내에서 아이템, 게임 머니 등을 얻기 위해 어뷰징을 이용한다.

2.2 어뷰징으로 인한 피해

어뷰징으로 인한 피해가 발생한 사례로는 게임 내 경제 파괴, 즉, 일부 플레이어들이 게임 내에서 아이템을 대량으로 획득하거나 아이템의 가격을 조작하는 행위를 통해 게임의 경제 시스템을 파괴하거나, 자신이 이러한 게임의 경제 시스템을 어뷰징하여 얻은 자산을 실제 화폐로 교환하는 행위를 통하여 이득을 얻고, 게임 회사에 피해를 주는 사례도 있었다, 그 외에도, 게임의 랭킹 시스템을 조작하여, 자신의 랭킹을 고위 랭킹에 위치시키거나, 다른 플레이어의 플레이를 방해하는 행위도 보고되고 있다.

2.3 게임 어뷰징 방지를 위한 기술

현재 게임 어뷰징을 막기 위해서 쓰이고 있는 기술로는 취약점 패치, 어뷰징 감지 및 모니터링, 실시간 데이터 분석, 유저 신고 및 검토 등이 있다. 실제 어뷰징은 메모리 상에서 발생하는 취약점을 기반으로 주로 일어나기 때문에 취약점에 대한 패치가 매우 중요한데, 해당 경우는 이미 취약점이 발현되고 나서 패치하는 경우가 많기 때문에 어뷰징 공격 방지에 조금은 미흡하다고 할 수 있으며, 감지 및 모니터링 시스템도 어뷰징이 이미 발행하고 난 후 감지하여 악성 유저를 셧다운 시키거나, 정지시키는 등의 조치를 하게 된다. 마찬가지로 실시간 분석 혹은 사용자 신고 또한 이와 유사하며, 어뷰징 자체를 무력화하는 솔루션은 아직 알려지지 않았다고 볼 수 있다.

2.4 파일 시그니처를 이용한 EXE 파일의 악성 행위 방지

파일 시그니처를 이용하여 EXE 파일의 악성 행위를 방지한 사례가 있는데, 대표적으로 안티바이러스 및 보안 소프트웨어를 예로 들 수 있다. 안티바이러스 및 보안 소프트웨어는 파일 시그니처를 사용하여 시스템에 다운로드 되는 파일을 검사하고, 악성 코드 혹은 악성 행위가 발견되면 해당 파일을 삭제하거나, 차단하는 등의 행동을 실행하게 된다. 또한, 이러한 기술을 기반으로 파일 시그니처를 이용하여 시스템에 이미 존재하는 파일의 변조나 침임을 탐지하여 방지하는연구도 진행되고 있다.

2.5 안티 디버깅을 이용한 EXE 파일의 악성 행위 방지

안티 디버깅을 이용하여 EXE 파일의 악성 행위를 방지하기도 한다. 보통의 소프트웨어 제조사는 자신의 소프트웨어를 어뷰징하지 못하게 하기 위해서 안티 디버깅을 걸어놓는데, 보통 디버거 탐지를 통해서 안티 디버깅 행위를 탐지해서 악성 행위를 방지한다. 즉, 프로그램에 대해서 디버거가 감지되면 실행을 중단하거나 비정상적인 동작을 수행하는 방식으로 악성 행위를 방지하는 것이다. 또한, 난독화를 통하여 EXE 파일을 암호화하여 사용자가 해당 EXE 파일을 분석하려고 하였을 때 이를 어렵게 만들어 분석하지 못하도록 하여 악성 행위를 방지한다. 즉. 안티 디버깅을 이용하여 디버깅 (EXE 파일의 악성 행위)을 방지한 방법은 디버거 탐지와 난독화가 대표적이라고 할 수 있다.

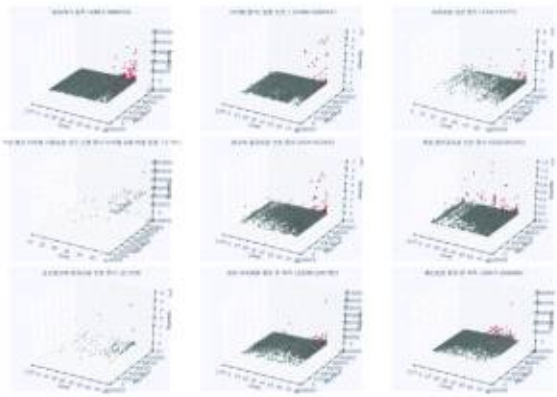
2.6 머신러닝을 이용한 게임 어뷰징 방지

머신러닝을 이용하여 게임 어뷰징을 방지할 수 있다. 예를 들어 하둡과 파이썬을 사용하여 데이터 수집, 지표 및 통계를 분석한 후, 추가로 탐색적 데이터를 분석하여 간단한 통계적 아이디어로 스팸 (광고)를 검출하거나 라이브 게임에서 각종 해킹 툴을 사용하여 어뷰징 플레이를 Decision

Tree 방식으로 지도 학습하여, 평균 정확도 80% 정도의 결과를 보여주었다. 교차 검증 (Cross Validation)을 위해 데이터 셋을 분리하고, GridSearch를 통해 최적의 하이퍼 파라미터를 찾은 경우는 91%까지 정확도가 향상되었다.

[그림 1] 머신러닝 어뷰징 결정 트리

또한, 이러한 어뷰징 트리를 학습하는 것뿐만이 아니라 이상 탐지 후 차단을 해야 하는데, 방법은 특이치 검출 (데이터가 오염되지 않았으며, 자주 발생하지 않는 이상 탐지)과 이상치 검출 (데이터가 오염되었을 가능성이 있으며, 표준 분포를 따를 때)로 나누어진다. 이를 머신러닝을 통해서 학습한 후, 이상 검출을 한 결과를 보자면, 정상 범위 밖의 값들이 검출되긴 하지만, 이들이 부정 플레이를 하였다는 명확한 증거를 찾을 수 없으면, 모니터링을 통해서 이중으로 검증을 해야하는 문제점이 존재한다.



[그림 2] 특이값 검출

2.7 지속적인 어뷰징으로 인한 위험성

먼저, 현재 어뷰징으로 발생하는 문제점은 사용자의 게임 플레이가 원활하지 않다는 점이다. 보통의 어뷰징 공격은 디도스 공격을 바탕으로 발생하게 되는데, 이 경우, 게임 플레이에 지장을 주거나 심할 경우, 게임 외적인 다른 외부 프로그램에도 영향을 줄 가능성이 존재한다. 이러한 경우, 특정 유저를 대상으로 어뷰징을 발생시키게 된다면, 특정 유저의 게임 플레이를 아예 망쳐버릴 수 있으며, 사용자가 실행하고 있는 서드파티 프로그램에도 영향을 끼칠 가능성이 있다.

프로게이머나 게임 방송인 등의 PC를 대상으로 어뷰징을 발생시키면 단순한 게임 서비스 방해가 아닌 금전적인 문제 등 복잡한 문제가 일어날 수 있다. 따라서, 어뷰징에 대한 문제가 해결되지 않고 지속될 경우, 개인적인 문제부터, 결과적으로는 금전적인 문제로까지 이어질 수 밖에 없다. 또한, 어뷰징이 해당 사용자를 노리는 것인지 혹은 전체 사용자를 대상으로 하는지 알 수 없기 때문에 빨리 대응하지 않는다면, 서비스에 큰 피해를 줄 수 있으며, 크게는 서비스 종료까지 일으킬 수 있기에 대응과 방어가 필요하다.

Ⅲ. 해결 방안 제시 및 구현

4.1 파일 시그니처를 이용한 안티디버깅 기법

[3~4] 파일 시그니처를 이용한 안티디버깅 기법으로는 공격자가 어떠한 어뷰징 혹은 악의적인 공격을 하기 위해서 파일을 분석하거나 파일의 시그니처 혹은 Hex값에 접근을 하게 될 것인데, 이러한 부분을 탐지해서 프로그램을 공격자가 디버깅하지 못하게 한다면, 어뷰징 공격에 필요한 정보들을 수집하지 못하게 될 것이고, 어뷰징 공격을 성공할 확률도 많이 줄어들게 될 것이다. 즉, 대상 파일에 대한 디버깅이 발견되었을 때, 파일의 시그니처를 임의의 시그니처로 변경하거나 파일 시그니처에 대한 접근이 발견된다면 디버깅을 탐지하여 차단하는 등의 방법을 사용할 수 있다.

4.2 파일 시그니처를 이용한 어뷰징 방지

파일 시그니처를 이용한 어뷰징 방지는 4.1에서 설명한 것과 같이 파일 시그니처 즉, 분석을 시작할 때 EXE 파일을 다른 임의의 확장자로 변경시켜서 공격하지 못하게 하거나 아예 분석을 하지 못하게 하는 것이다. 본 논문에서는 Python 코드를 이용하여 악용되면 안되는 EXE 파일이

특정 디버거나 에디터에서 실행되었을 때, EXE의 파일 시그니처를 임의의 파일 시그니처로 변경하거나 아예 해당 시그니처 값을 암호화시키는 방식을 사용하여 어뷰징을 방지하는 연구를 수행하였다.

4.3 머신러닝을 이용한 파일 시그니처 변경 탐지 기법

[1, 5] 머신러닝을 이용한 파일 시그니처 변경 탐지 기법은 4.1, 4.2에서 설명한 방식에 머신러닝의 이점을 추가해서 어뷰징 발생의 원인을 제거하는 방법이다. 즉, 파일 시그니처를 이용한 안티 디버깅, 어뷰징 방지에 대한 내용을 기계학습을 이용하여 학습을 시킨 후, Loss율을 최소화하여 이를 더욱 정확한 방법으로 차단시키는 방법으로, 이를 적용할 시 어뷰징에 대한 유동적인 대응이 가능할 것으로 보인다. 하지만, 아직까지는 머신러닝을 이용한 어뷰징 탐지는 87 ~ 95% 정확도를 가지고, 오차 범위가 존재하기 때문에 오차가 발생하게 되면 정상적인 사용자도 파일에 접근할 수 없게 되는 문제점이 발생할 여지가 있다. 여기에 파일 시그니처와 안티디버깅을 적용하게 되면, 정확도가 더 낮아질 수도 있어 이에 대한 연구가 더 필요하다.

4.4 파일 시그니처를 이용한 어뷰징 방지 효과

파일 시그니처를 이용한 어뷰징 방지로 얻을 수 있는 효과로 게임 서비스의 원할한 서비스 운영이 제일 큰 장점이 될 것 같다. 그 이유는 어뷰징이 일어나게 되면, 제일 먼저 피해를 보는 것은 게임 회사뿐만 아니라 게임을 플레이하고 있는 유저이기 때문에 어뷰징으로 인해 게임 유저 수도 줄어들게 된다. 따라서 파일 시그니처를 이용한 어뷰징 방지로 어뷰징 원인을 사전에 제거하게 된다면, 게임 플레이를 하는 유저 입장에서도 악의적인 플레이를 하거나 버그를 이용하는 등의 어뷰징 현상 없이 순수하게 게임 서비스를 즐길 수 있어 게임사와 게임 플레이어 둘 다에게 좋은 방법이다. 더 나아가 어뷰징으로 인한 자산 획득 및 악용을 막을 수 있기에 게임사와 플레이어의 자산을 지킬 수 있을 것이다.

4.5 파일 시그니처와 머신러닝을 이용한 어뷰징 방지의 장점

파일 시그니처와 머신러닝을 사용한 어뷰징 방지를 사용하였을 때 기대할 수 있는 사항으로는 제일 먼저 파일 시그니처 변경 여부를 머신러닝을 통해서 학습해놓은 후, 해당 사항이 변조가 되었는지 유동적으로 확인할 수 있어 수동적으로 일일이 검사하는 것보다 더 효율적이다. 대부분의 어뷰징이 메모리 공격으로 인해서 일어나기 때문에 파일 자체 접근을 막아버린다면 어뷰징 방지를 줄일 수 있고, 머신러닝 기반의 학습으로 어떠한 상황에서 접근을 허용하고 어떠한 상황에서 접근을 허용하지 않을 것인지를 명시할 수 있어 관리자와 비관리자의 행위나 접근 범위 수정도 가능할 것이다. 파일 시그니처와 머신러닝을 같이 사용해서 어뷰징 공격을 방지하였을 때 얻을 수 있는 장점은 보다 정확한 어뷰징 탐지 능력과 사용자 여부에 따른 파일 내부 접근 허용 여부이지만 앞서 언급하였듯이 아직은 Loss율이 존재하기에 좀 더 많은 연구가 필요할 것으로 보인다.

Ⅳ. 결론 및 향후 연구 방향

게임 어뷰징은 악의적인 해킹 공격과 마찬가지로 다양한 방법들이 계속 늘어나고 있고, 막으려고 하면 계속 우회를 하여 공격을 하는 공방전 형태가 계속 이루어질 것으로 보인다. 또한, 어뷰징으로 인한 피해 또한 나날이 늘어날 것으로 보이는데, 이러한 위험성에 맞서 조금이라도 해당 위협을 줄이기 위해서 앞으로 더 많은 연구가 필요하다, 머신러닝을 통한 어뷰징 방지도 점차 AI 관련 기술이 발전하면서 Loss율이 감소함에 따라 더욱 정확한 머신러닝 기반의 분석 또한 가능할 것으로 보인다. 앞으로 이러한 어뷰징 방지에 대한 연구가 많이 진행된다면 어뷰징 발생으로 인한 피해가 방지될 수 있을 것으로 기대된다.

사사

해당 논문은 ‘22~’24년 대학혁신지원사업의 부처협업형 인재양성 사업 추진계획에 따라, 신산업 분야 지식재산 융합인재 양성사업의 지원을 받아

수행된 연구임.

참고문헌

[1] Nexon Development Conference. "Game Abuse Prevention Using Machine Learning Techniques." Presented at NDC 2016, Seoul, Korea, November 2016. Available online

[2] 조영신, 유수정, 한영주. (2015-04-25). 어뷰징의 발생 원인에 대한 탐색적 연구. 한국방송학회 학술대회 논문집, 부산.

[3] 박진우, 박용수. "안티디버깅 루틴 자동 탐지 기법." 한국정보과학회 학술발표논문집 2013 한국정보과학회 제40회 정기총회 및 추계학술발표회 (2013): 793-795.

[4] 김종욱, 방지원, 최미정. "악성코드 분석을 위한 안티-디버깅의 이해와 무력화 연구를 위한 안티-안티-디버깅 연구." 한국통신학회논문지 45권 1호 (2020): 105-116.

[5] 전덕조, 박동규. "머신 러닝(Machine Learning)기법을 활용한 실시간 악성파일 탐지 기법." 한국정보기술학회논문지 16권 3호 (2018): 101-113.