안드로이드 멀웨어 분석을 통한 액티비티 삽입 공격에 대한 이해

김영석 [1], 황성재 [1]
[1] 성균관대학교 소프트웨어학과
kys00514@skku.edu, sungjaeh@skku.edu

Empirical Study of Activity Injection Attacks in Android Malware

Youngseok Kim[1] , Sungjae Hwang[1]
[1]College of Computing, Sungkyunkwan University

요 약

액티비티 삽입(Activity Injection) 공격은 공격자가 만든 악의적인 화면을 사용자에게 강제로 표시되게 하는 공격으로, 이를 악용하여 다양한 피싱(Phishing) 공격이 가능하다. 액티비티 삽입 공격은 특별한 권한없이 수행될 수 있으며 사용자가 정상적인 앱을 실행했을 때 공격이 수행되기 때문에 사용자 입장에서는 공격의 수행 여부를 판단하기 쉽지 않다. 이렇게 액티비티 삽입 공격이 강력한 반면, 안드로이드 멀웨어(Malware)에서 이러한 공격을 어떻게 활용하고 있는지에 대한 연구 결과가 없어, 액티비티 삽입 공격을 활용하는 멀웨어를 대응하기가 쉽지 않은 실정이다. 본 논문에서는 1,498 개의 안드로이드 멀웨어를 정적 및 동적 분석하여, 안드로이드 멀웨어에서 액티비티 삽입 공격의 활용도를 분석하고 이해하고자 한다.

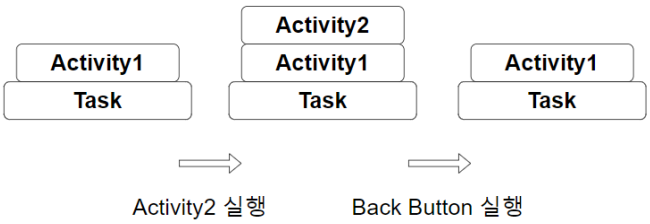
1. 서론

액티비티(Activity)는 사용자와 직접적으로 상호작용하는 컨포넌트로, 공격자가 악의적인 액티비티를 강제로 사용자에게 띄울 수 있다면 다양한 피싱(Phishing) 공격이 가능하게 된다. 이는 개인정보 유출과 같은 심각한 사고로 이어질 수 있어, 액티비티를 안전하게 보호하는 것은 안드로이드 보안의 중요한 부분으로 볼 수 있다.

그러나 선행 연구에서 안드로이드 프레임워크의 취약점을 악용한 액티비티 삽입 공격(Activity Injection Attack)을 소개하였고, 정상적인 안드로이드 앱에서 액티비티 삽입 공격(이하 “AIA”이라 함)을 활용하는 케이스를 조사하였다[1]. AIA 공격은 특별한 권한없이 수행될 수 있어 강력하다. 또한, 기존 액티비티를 활용하는 공격들은, 정상 액티비티의 흐름을 가로채어 공격자의 액티비티를 보여주게 하는 방법으로, 공격을 수행하는 타이밍이 중요하였다. 하지만 AIA 는 사용자가 정상적인 앱을 실행했을 때 자동으로 공격이 수행되기 때문에 타이밍을 고려하지 않아 공격의 성공이 보장된다.

이렇게 AIA 는 강력한 공격인 반면, 선행 연구에서는 정상적인 앱을 대상을 분석하였고, 안드로이드 멀웨어(Malware)에서 AIA 를 어떤 용도로 활용하고 있는지에 대한 연구 결과가 없다. AIA 를 활용하는 멀웨어가 발생하고 있는 시점에[2], 이러한 정보가 없어 멀웨어를 대응하는데 어려움이 있다. 본 논문에서는 멀웨어 분석을 통해 AIA 를 악용하는 빈도수 및 활용도를 이해하고자 한다.

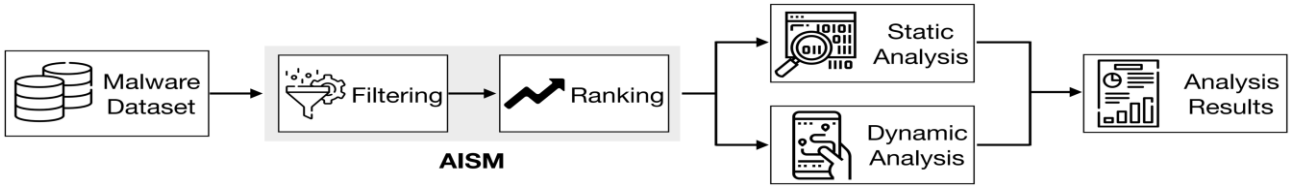
2. 액티비티, 태스크, 액티비티 삽입 공격



(그림 1) 액티비티 및 태스크 설명

액티비티는 안드로이드 기본 컨퍼넌트 중 하나이며, UI 를 제공하여 사용자와 상호작용하는 역할을 담당한다. 예를 들어 카카오톡 앱 안에서도 로그인 화면과 대화창을 나타내는 화면이 있고, 이들은 각각 다른 액티비티로 개발된다.

안드로이드는 사용자가 특정한 목적을 위해 실행한 액티비티들을 태스크(Task)를 통해 관리한다. 따라서



(그림 2) 멀웨어 분석 과정

모든 안드로이드 앱은 Task 를 하나이상 가지고 있다. 그림 1 은 액티비티와 태스크 관계를 보여준다. 태스크에 Activity1 이 저장되어 있는 상태에서 사용자가 Activity2 를 실행하면, Activity2 가 태스크의 가장 위에 위치하게 되며, 사용자는 가장 위에 있는 Acitivity2 를 보게 된다. 이 상태에서 사용자가 뒤로 가기 버튼을 누른다면, Activity2 가 태스크에서 사라지고, Activity1 이 사용자에게 표시된다.

액티비티는 일반적으로 새로 생성될 때, 해당 액티비티를 실행시킨 앱의 태스크에 저장된다. 하지만 안드로이드는 개발자가 액티비티의 전환 흐름을 컨트롤할 수 있게 여러가지 액티비티 속성들을 제공하고, 이러한 속성들을 활용해서 개발자가 원하는 태스크에 액티비티가 저장되게 설정할 수 있다. 이러한 속성들로는 TaskAffinity 와 singleTask, singleTop 과 같은 LaunchMode 와 NEW_TASK, SINGLE_TOP 과 같은 Intent Flag 가 있다. 개발자가 적절하게 LaunchMode 및 Intent Flag 를 설정한다면, taskAffinity 에 명시되어 있는 태스크에 액티비티를 저장하게 할 수 있다. 이 점을 악용하면 멀웨어가 악성 액티비티를 특정 앱의 태스크에 저장할 수 있고, 이를 통해 악성 액티비티가 해당 앱을 실행할 시 사용자에게 보여지는 문제로 이어진다. 이러한 공격을 액티비티 삽입 공격(AIA)이라고 정의하였으며, 공격자는 이를 활용하여 피싱 공격이 가능하다. AIA 는 기존 화면을 가로채는 피싱 공격보다 강력한데, 그 이유는 안드로이드에서 제공하는 정상 기능을 활용하는 공격으로, 어떠한 권한도 요구되지 않기 때문이다. 또한, 기존 공격은 화면을 가로채는 타이밍이 중요한데, AIA 는 사용자가 정상적인 앱을 실행할 시 공격이 수행되기 때문에 타이밍을 고려할 필요가 없어 공격이 용이하다.

3. 안드로이드 멀웨어 분석 방법

AIA 를 활용한 멀웨어의 빈도와 사용 의도를 분석하기 위해 그림 2 와 같은 과정을 거쳤다. 먼저 CIC Dataset[3] 과 AndroidMalware[4]를 통해 1,498 개의 안드로이드 멀웨어를 수집했다. 또한 의미있는 멀웨어만 분석하기 위해, AISM(Activity Injection Search Module)을 개발하였다. AISM 은 Filtering 과 Ranking 모듈로 구성되어 있다. AIA 를 수행하기 위해서는, taskAffinity 속성을 반드시 사용해야 한다. Filtering 모듈에서는 앱 디컴파일 후, AndroidManifest 파일을 추출하고, 이를 파싱하여 taskAffinity 를 사용하는 멀웨어를 찾는다. Ranking 모듈에서는 멀웨어의 기본 태스크 이름과 taskAffinity 로 설정된 태스크의 이름의 유사도를 Levenstein Distance [5] 알고리즘을 활용하여 계산하고, 계산 결과를 기반으로 다른 앱을 타겟으로 AIA 를 수행할 가능성이 높은 멀웨어의 순위를 매긴다. 이 후, 공격 가능성이 높은 멀웨어 순으로 정적 및 동적 분석을 수행하여, 멀웨어에서 AIA 를 어떤 용도로 활용하는지 알아보았다. 정적분석의 경우, JADX 디컴파일러[6]를 활용하였으며, 동적분석의 경우, Bluestacks 에뮬레이터[7]를 활용하여 실제로 멀웨어를 실행해보면서 AIA 에 활용되는 액티비티를 띄워보고, 실시간으로 태스크의 변화를 분석하였다.

4. 멀웨어 분석 결과

<표 1> AISM 을 활용한 멀웨어 분석 결과

멀웨어 데이터 셋 범주	멀웨어 개수
전체 멀웨어	1,498
AIA 활용 가능성이 있는 멀웨어	173
AIA 를 활용하여 다른 앱을 공격할 가능성이 있는 멀웨어	92

표 1 은 수집한 멀웨어 데이터 셋을 AISM 에 적용한 결과를 보여준다. 1,498 개의 멀웨어 중 11.55% (173 개)의 멀웨어가 AIA 를 수행할 가능성이 있었다. 이 중, 53.76% (92 개)의 멀웨어가 AIA 를 통해 다른 앱을 공격할 가능성이 있는 것을 확인하였다.

<표 2> 정적 및 동적 분석을 통한 AIA 활용 분석

AIA 활용 의도	멀웨어 개수
광고 창 띄우기	3
라이브러리 사용	4
멀웨어 태스크 회귀	1
분석 불가능	2

AISM 을 통해 다른 앱을 타겟으로 AIA 를 수행할 가능성이 가장 높은 멀웨어 10 개를 정적 및 동적 분석하였다. 분석을 통해, 멀웨어가 액티비티 AIA 를 어떤 용도로 활용하는지 알아보았다.

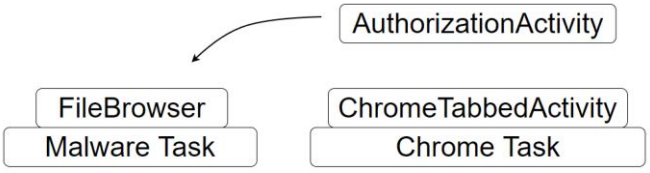
표 2 는 멀웨어를 정적 및 동적 분석한 결과를 보여준다. 총 10 개의 멀웨어 중, 2 개의 멀웨어는 AIA 를 통해 다른 앱의 태스크로 삽입되는 액티비티 코드가 멀웨어에 존재하지 않아 AIA 의 사용 의도를 파악할 수 없었다. 멀웨어에서 동적으로 해당 코드를 다운로드하여 공격을 수행하는 것으로 유추되지만, 공격자 서버에 접근이 되지 않아 필요한 코드를 다운받을 수 없어 분석할 수 없었다. 나머지 8 개의 멀웨어를 분석한 결과 크게 세 가지의 의도로 AIA 를 사용하는 것을 파악하였다.

(그림 3) 광고 화면을 띄우기 위한 AIA 공격 코드

한 가지 의도는 멀웨어에서 특정 앱이 실행되었을 시, 광고 화면을 띄우기 위해 AIA 를 활용하는 것을 알 수 있었다. 하나의 예로, 약 100 개의 중국에서 인기 앱의 태스크에 광고 액티비티를 삽입하는 멀웨어를 확인했다. 그림 3 은 타겟 앱의 태스크에 광고 화면을 삽입하는 코드의 일부를 보여준다. 이를 통해, 해당 앱을 사용자가 실행할 시, 광고가 표시되게 하기 위한 목적으로 보인다. 또한, Unity[8], Startapp[9]과 같은 광고 SDK 를 활용시에 AIA 를 활용하여 다른 앱의 태스크에 광고를 주입하는 멀웨어가 관측되었다.

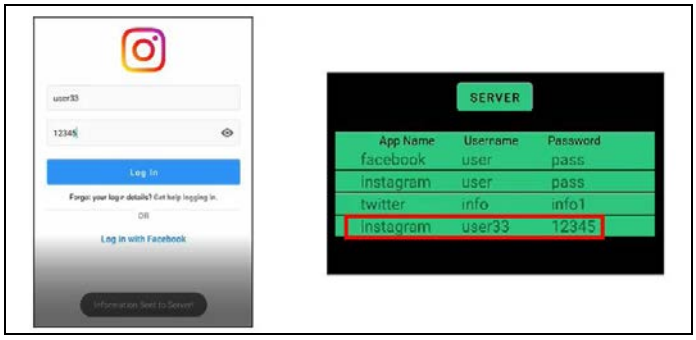
AIA 를 사용하는 다른 이유로 파악된 것은 라이브러리 사용을 위함이다. 하나의 예로, SMS/MMS 전송 및 수신을 편하게 해주는 라이브러리를 사용하는 멀웨어를 확인하였다. 해당 라이브러리의 정상적인 동작을 위해서는 기본 태스크가 아닌 해당 라이브러리에서 지정한 태스크를 사용해야 한다. 이러한 경우에는 공격의 의도로 AIA 를 사용했다고 볼 수 없다.

AIA 를 사용하는 세번째 목적은 특정 액티비티를 멀웨어의 태스크로 회귀시키기 위함이다. 그림 4 는 이 과정의 동작을 간략하게 보여준다. FileBrowser 액티비티에서 Chrome 브라우저를 실행하고, Chrome 브라우저에서 AuthorizationActivity 를 실행한다. 멀웨어는 AuthorizationActivity 를 자신의 태스크로 가져오기 위해 AIA 를 활용하는 것을 확인하였다.



(그림 4) 타겟 액티비티 회귀 플로우

5. 테스트 멀웨어를 활용한 분석



(그림 5) 테스트 멀웨어를 활용한 검증

10 개의 멀웨어 분석을 통해 도출된 AIA 사용 의도와 더불어 이론적으로 더 다양한 공격에도 AIA 가 활용될 수 있다. 예를 들어 여러 앱의 로그인 창을 모방하여 피해자가 멀웨어의 액티비티에 로그인 정보를 기입하게 속이는 피싱 공격이 가능하다. 다른 공격 방법으로는 각종 권한을 요구하는 액티비티를 정상적인 앱에 주입하여 사용자가 인지하지 못한 채 멀웨어에 치명적인 권한을 허용하는 공격에도 사용될 수 있다. 위 공격들이 최신 안드로이드 환경에서 수행 가능한지 알아보기 위해 선행 연구[1]에서 정리된 AIA 가 가능한 220 가지의 조건을 참고하여 테스트 멀웨어를 만들어서 검증해보았다.

2021 년 가장 많이 사용되는 안드로이드 버전은 Android 10 이였으며[10], 해당 환경에서 앞서 언급한 로그인 창을 모방하는 액티비티와 권한을 획득하는 공격을 성공적으로 수행할 수 있는 것을 확인하였으며, 선행 연구에서 정의한 220 가지의 조건에서 AIA 공격이 가능한 것도 확인하였다. 그림 5 는 AIA 를 통해 공격자가 만든 인스타그램의 화면을 사용자에게 띄우고, 이를 통해 사용자의 로그인 정보를 탈취하는 공격을 성공적으로 수행한 화면을 보여준다.

6. 결론

본 논문에서는 1,498 개의 멀웨어를 분석하여, 멀웨어에서 AIA 를 악용하는 빈도수 및 활용도를 확인해보았다. 본 연구를 통해 멀웨어에서 광고창을 띄우거나, 정상적인 라이브러리 사용, 특정 액티비티를 멀웨어의 태스크로 회귀시키기 위해 AIA 를 활용하는 것을 관찰하였다. 또한, 자체 개발한 테스트 멀웨어를 통해 검증해본 결과, 최신 버전의 안드로이드 환경에서도 AIA 공격이 가능한 것을 확인하였다. AIA 공격은 악의적인 액티비티를 제약사항 없이 사용자에게 띄워주면서 다양한 피싱 공격이 가능하기 때문에 구글과 안드로이드 사용자들의 경각심이 요구된다.

본 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단 및 정보통신기획평가원의 지원을 받아 수행된 연구임 (2022R1F1A1074495, No. 2022-0-01199, 융합보안대학원(성균관대학교))

참고문헌

[1] Hwang, S., Lee, S., Ryu, S, All about activity injection: Threats, semantics, detection, and Defense. *Software: Practice and Experience*,2020, 1061–1086
[2]AIA Malware, https://threatpost.com/strandhogg-2-critical-bug-android-app-hijacking/156058/
[3] CICDataset, http://205.174.165.80/CICDataset/
[4] AndroidMalware, https://github.com/sk3ptre
[5] Levenstein Distance, https://xlinux.nist.gov/dads/HTML/Levenshtein.html
[6] JADX, https://github.com/skylot/jadx
[7] Bluestacks, https://www.bluestacks.com/ko/index.html
[8] Unity, https://unity3d.com/kr/get-unity/download
[9] Startapp, https://www.start.io/
[10] Popular Android Version in 2021, https://www.xda-developers.com/android-distribution-numbers-2021