한국컴퓨터정보학회 하계학술대회 논문집 제31권 제2호 (2023. 7)

모바일 운영체제의 보안 매커니즘과 새로운 공격 경로 탐지

김애솔*, 박재경O
*강서폴리텍대학 사이버보안학과,
O강서폴리텍대학 사이버보안학과
e-mail: qpsbdj1028@gmail.com*, jakypark@kopo.ac.krO

A Study on the Security Mechanisms of Mobile Operating Systems and the Detection of New Attack Paths

A.S Kim*, Jae-kyung ParkO
*Dept. of Cyber Security, Korea Polytechnis,
ODept. of Cyber Security, Korea Polytechnis

● 요 약 ●

본 논문은 모바일 운영체제의 보안 매커니즘을 조사하고, 현재까지 알려진 공격 경로뿐만 아니라 새로운 공격 경로를 탐지하기 위한 방법에 대해 연구하였다. 모바일 운영체제 보안은 사용자의 개인 정보와 중요한 데이터를 보호하는 데 매우 중요하며, 이에 대한 이해와 공격 경로의 탐지는 보안 강화에 필수적이다. 본 연구에서는 iOS와 Android를 중심으로 모바일 운영체제의 주요 보안 매커니즘을 분석하고, 샌드박스 환경, 권한 관리, 암호화 등의 보안 매커니즘에 대해 상세히 살펴보았다. 또한, 이전 연구들에서 파악된 공격 경로 외에도 새로운 공격 경로를 발견하고 탐지하기 위한 방법과 도구를 개발하였다.

키워드: 모바일(Mobile), iOS, 안드로이드(Android), 샌드박스(Sandbox), 암호화(Encryption)

I. Introduction

최근 몇 년 동안 모바일 장치는 일상 생활의 필수적인 부분이 되어 전례 없는 편리함과 연결성을 제공합니다. 그러나 모바일 운영체제의 급속한 성장과 광범위한 채택으로 인해 취약성을 악용하고 민감한 정보에 대한 무단 액세스를 시도하는 악의적인 행위자의 주요 표적이 되었습니다. 결과적으로 모바일 운영 체제의 보안을 보장하는 것이 중요한 문제가 되었습니다.

Android 및 iOS와 같은 모바일 운영 체제는 다양한 보안 메커니즘을 사용하여 사용자 데이터를 보호하고 잠재적인 위협을 완화합니다. 이러한 메커니즘은 알려진 공격 벡터와 새로운 공격 벡터 모두에 대해 강력한 방어를 구축하는 것을 목표로 하드웨어, 펌웨어 및 소프트웨어를 포함한 여러 계층을 포함합니다. 그러나 끊임없이 진화하는 사이버 위협 환경은 보안 조치의 지속적인 발전을 필요로 합니다.

II. Preliminaries

1. 국내 동향

현재 모바일 운영체제는 우리의 일상생활에 크게 기여하는 중요한 기술입니다. 모바일 기기는 개인정보, 금융 정보, 비즈니스 데이터 등 다양하고 중요한 정보를 저장하고 전송하는 역할을 한다. 그러나 모바일 기기는 해커나 악성 소프트웨어의 공격에 취약하며, 새로운 공격 경로가 지속적으로 등장하고 있다. 이에 따라 모바일 운영체제의 보안 매커니즘을 강화하고, 새로운 공격 경로를 탐지하고 대응할 수 있는 연구가 필요하다. 그림 1에서와 같이 기존 운영체제를 이해하고 보안상 문제를 발견할 수 있는 새로운 경로를 연구하는 것이 필요하다고 판단한다.

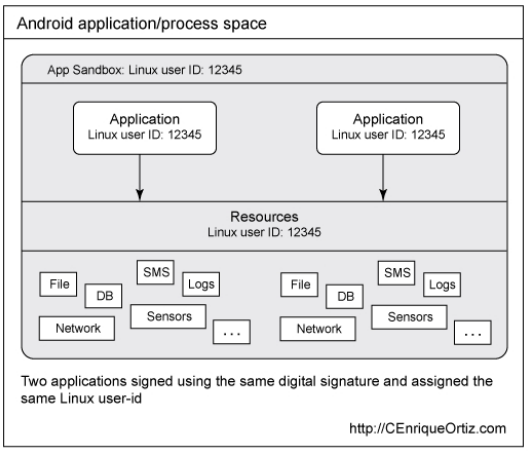

Fig. 1. Android OS Architecture

2. 연구 목적

본 연구의 목적은 모바일 운영체제의 보안 매커니즘을 분석하고, 새로운 공격 경로를 탐지하고 대응하는 방법을 탐구하는 것이다. 우리는 기존의 보안 매커니즘에 대한 이해를 바탕으로 모바일 기기의 취약성과 공격 경로를 식별하고, 이를 탐지하고 방어하기 위한 새로운 알고리즘과 기술을 개발하고자 한다.

2.1 연구 범위

이 연구의 범위는 주로 주요 모바일 운영체제(예: 안드로이드, iOS)에 대한 보안 매커니즘과 공격 경로를 중점적으로 다룰 것이다. 우리는 보안 패치 정책, 앱 권한 관리, 데이터 암호화 등의 주요 보안 기능을 조사하고 분석하며, 현재 존재하는 새로운 공격 경로를 조사하고 탐지하기 위한 방법을 개발할 것입니다. 그러나 다른 플랫폼이나 보안 시스템에 대한 연구는 이 연구의 범위를 벗어나므로 제외될 것이다.

2.2 관련 기술

a) 샌드박스 환경

샌드박스 환경은 모바일 운영체제에서 중요한 보안 매커니즘 중 하나이다. 이는 앱이 독립적인 환경에서 실행되도록 하여 다른 앱이나 운영체제에 악영향을 미치지 않도록 합니다. 샌드박스는 앱이 자체적인 리소스, 파일 시스템 및 메모리 공간을 할당받아 작동하며, 앱 간에 데이터 공유나 악성 코드의 전파를 방지합니다. 또한, 앱이 외부 시스템에 대한 접근 권한을 제한함으로써 보안을 강화한다.

3. 모바일 결제 시스템으로 인해 일어날 수 있는 보안문제

1) 악성 앱 : 기기 내 설치된 악성 앱으로 인해 정보 탈취할 수 있다.

2) 네트워크 스니핑 : 공용 네트워크를 통해 데이터가 전송될 때, 해커는 스니핑 기술을 이용하여 데이터 탈취가능하다.

3) 피싱 : 악성 메일이나 메시지를 통해 결제 정보를 입력하도록 유도하는 피싱 사기가 일어날 수 있다.

라. 탈옥된 기기 : 탈옥된 IOS나 루팅 된 안드로이드 기기를 사용시 보안에 취약하다.

마. 결제 서비스의 취약점 : 결제 서비스 업체의 보안 취약점으로 인해 사용자 정보가 유출 가능성이 있다.

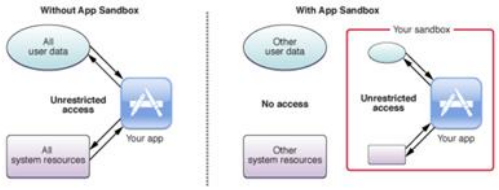

Fig. 2. SandBox

b) 권한 관리

모바일 운영체제에서는 권한 관리를 통해 앱이 사용자의 개인 정보와 기기 기능에 접근하는 권한을 제어한다. 사용자는 앱을 설치할 때 앱이 요구하는 권한을 확인하고 승인할 수 있습니다. 권한 관리는 사용자의 개인 정보 보호를 위해 중요한 역할을 수행하며, 앱이 불필요한 권한을 요구하는 경우에는 사용자에게 경고를 주고 거부할 수 있는 기능을 제공한다.

c) 암호화

암호화는 모바일 운영체제에서 중요한 보안 기능으로, 데이터의 기밀성과 무결성을 보장합니다. 암호화는 저장된 데이터, 통신 데이터, 인증 정보 등을 암호화하여 외부에서의 불법적인 접근이나 탈취를 방지합니다. 또한, 데이터 암호화를 통해 잠금 해제된 장치에 대한 보안을 강화하고, 데이터 유출이나 변조를 방지한다.

d) 기타 보안 기능

모바일 운영 체제는 다양한 기타 보안 기능을 제공한다. 예를 들면, 안전한 부팅 프로세스를 통해 장치의 안전한 시작을 보장하고, 앱 서명 기능을 통해 앱의 신뢰성을 검증할 수 있습니다. 또한, 취약점 패치 정책을 통해 운영체제의 보안 결함을 보완하고, 네트워크 보안 기능을 통해 안전한 데이터 통신을 제공한다.

이러한 보안 기능들은 모바일 운영체제의 핵심적인 매커니즘으로 작용하며, 개인 정보 보호와 시스템 보안에 대한 중요한 역할을 수행한다. 이러한 기능들은 사용자의 개인 정보와 기기의 안전성을 보호하고, 악성 소프트웨어의 공격으로부터 시스템을 방어하는 데 도움을 준다. 또한, 이러한 보안 기능들은 모바일 앱 개발자들에게도 중요한 역할을 한다. 개발자는 보안 기능을 올바르게 구현하여 사용자의 개인 정보를 보호하고, 새로운 공격 경로에 대비할 수 있도록 해야 한다. 따라서, 이러한 샌드박스 환경, 권한 관리, 암호화, 그리고 기타 보안 기능들은 모바일 운영체제의 핵심적인 보안 매커니즘으로서 연구와 개발의 주요 대상이 된다. 본 논문에서는 이러한 보안 기능들을 분석하고, 새로운 공격 경로를 탐지하고 대응하는 방법을 탐구하여 모바일 운영체제의 보안 강화에 기여하는 것을 목표로 한다.

III. The Proposed Scheme

새로운 공격 경로 탐지 방법 중 알려진 공격 경로 분석, 새로운 공격 경로 식별 등이 선행되며 본 연구에서는 새로운 공격 경로 탐지 방법과 기법에 대해 간략히 제안하고자 한다.

3.1 새로운 공격 경로 탐지 방법

a) 공격 시나리오 분석

공격 시나리오 분석은 모바일 운영체제에서 새로운 공격 경로를 발견하고 탐지하기 위해 필요한 첫 번째 단계이다. 이 단계에서는 기존에 알려진 공격 시나리오뿐만 아니라 새로운 공격 경로에 대한 특징과 잠재적인 위협 요소를 조사한다. 공격 시나리오 분석은 보안 전문가들이 현실적이고 실제 가능성이 있는 공격 시나리오를 모델링하고 평가하는 과정을 포함한다.

b) 새로운 공격 경로 시뮬레이션

새로운 공격 경로 시뮬레이션은 분석된 시나리오를 실제로 재현하여 시스템 내에서의 공격 경로를 모의하는 것을 의미한다. 이를 통해 실제 공격을 수행하지 않고도 시스템의 취약점과 잠재적인 위협을 파악할 수 있다. 새로운 공격 경로 시뮬레이션은 다양한 시나리오와 전략을 시험하며, 모바일 운영체제의 보안 취약점을 탐지하는 데 도움이 된다.

3.2 방어 및 탐지 기법 제안

a) 새로운 취약점 분석 및 보안

모바일 운영체제의 보안을 강화하기 위해서는 새로운 공격 경로에서 발생할 수 있는 취약점을 분석하고 보완해야 한다. 이를 위해 보안 업데이트와 패치를 제공하여 이미 알려진 취약점을 해결하고, 보다 견고한 보안 매커니즘을 구현하는 작업이 필요하다.

b) 행위 기반 탐지

행위 기반 탐지는 모바일 운영체제에서 실행되는 앱의 동작을 모니터링하고, 비정상적인 동작 패턴을 감지하는 기법이다. 예를 들어, 앱이 민감한 사용자 정보에 접근하거나, 알려지지 않은 네트워크 연결을 시도하는 경우에는 이를 즉시 탐지하여 적절한 조치를 취할 수 있다. 행위 기반 탐지는 기존의 시그니처 기반 탐지 방법과는 달리 알려진 공격 패턴을 기반으로 하지 않고, 앱의 동작과 행위에 초점을 맞춘다. 이는 새로운 공격 경로에 대응할 수 있는 유연성과 탐지의 정확도를 향상시킬 수 있다.

c) 정적 및 동적 분석

정적 및 동적 분석은 앱의 코드와 실행 과정을 분석하여 잠재적인 취약점과 악성 행위를 탐지하는 기법이다. 정적 분석은 앱의 소스 코드를 검사하여 보안 위협을 식별하고, 동적 분석은 앱을 실제로 실행하여 실행 중에 발생하는 행위를 분석한다. 이러한 분석을 통해 앱의 취약점과 악성 행위를 탐지하고, 이를 이용한 새로운 공격 경로를 사전에 차단할 수 있다.

d) 기계 학습 기반 탐지

기계 학습은 모바일 운영체제에서 새로운 공격 경로 탐지에 유용한 도구로 사용될 수 있다. 기계 학습 모델을 사용하여 정상적인 앱 동작과 악성 행위의 패턴을 학습하고, 이를 기반으로 새로운 공격 경로를 식별할 수 있다. 이는 정확도와 탐지율을 향상시키며, 실시간으로 변화하는 공격 기술에 대응할 수 있도록 도와준다.

e) 협업적 탐지

협업적 탐지는 여러 모바일 장치나 서버 간의 정보 공유와 협업을 통해 새로운 공격 경로를 탐지하는 기법이다. 예를 들어, 모바일 장치에서 탐지된 악성 행위의 패턴이 서버로 전송되어 분석되고, 이를 기반으로 다른 장치에서도 적절한 대응을 취할 수 있다. 이러한 협업적 탐지는 실시간으로 변화하는 공격에 대응하는 데 도움이 된다.

IV. Conclusions

본 연구는 모바일 운영체제의 보안 매커니즘을 조사하고, 새로운 공격 경로를 탐지하기 위한 방법을 연구하였다. 모바일 운영체제의 보안은 개인 정보와 중요한 데이터의 보호에 매우 중요하며, 보안 매커니즘의 이해와 새로운 공격 경로의 탐지는 보안 강화를 위해 필수적이다. 제안된 방어 및 탐지 기법의 실험 결과와 분석을 통해 이를 검증하였으며, 향후 연구 방향을 제시하여 모바일 운영체제의 보안을 더욱 강화할 수 있는 방향을 제시하였다.

REFERENCES

[1] Jain, A., & Kumaraguru, P. (2017). A survey of mobile malware in the wild. IEEE Communications Surveys & Tutorials, 19(2), 1347-1381.

[2] Kim, D. H., Cho, S., Park, S., Park, H., & Park, Y. (2018). Survey on Android security threats and malware detection techniques. Journal of Information Processing Systems, 14(2), 411-426.

[3] Islam, S., Ahmed, R., & Kalam, A. (2015). Mobile operating systems security: A comparative analysis between Android and iOS. Procedia Computer Science, 72, 619-627.

[4] Cao, H., & Liu, Z. (2016). A survey on Android security and privacy protection mechanisms. Proceedings of the 11th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 692-696.