한국컴퓨터정보학회 동계학술대회 논문집 제23권 제1호 (2015. 1)

안드로이드 취약점을 이용한 공격 시나리오 연구

박재경°
°한국과학기술원 사이버보안연구센터
e-mail:wildcur@kaist.ac.kr°

A Study of Attack Scenario using Android Vulnerabilities

Jae-kyung Park°
°Cyber Security Research Center, Korea Advanced Institute of Science & Technology

● 요 약 ●

본 논문에서는 고성능 컴퓨팅 시스템의 성능 향상을 위한 효율적인 동적 작업부하 균등화 정책을 제안한다. 이 정책은 시스템 자원인 CPU와 메모리를 효율적으로 사용하여 고성능 컴퓨팅 시스템의 처리량을 최대화하고, 각 작업의 수행시간을 최소화한다. 또한 이 정책은 수행중인 작업의 메모리 요구량과 각 노드의 부하 상태를 파악하여 작업을 동적으로 할당한다. 이때 작업을 할당 받은 노드가 과부하 상태가 되면 다른 노드로 작업을 이주시켜 각 노드의 작업부하를 균등하게 유지함으로써 작업의 대기시간을 줄이고, 각 작업의 수행시간을 단축한다. 본 논문에서는 시뮬레이션을 통하여 제안하는 동적 작업부하 균등화 정책이 기존의 메모리 기반의 작업부하 균등화 정책에 비해 고성능 컴퓨팅 시스템의 성능 향상 면에서 우수함을 보인다.

키워드: 안드로이드(Android), 악성코드(Malware), 취약점(Vulnerability), 루팅(Rooting)

I. 서 론

스마트폰 사용자가 증가함에 따라 스마트폰 사용자를 노리는 악성코드 또한 증가 하고 있다. 국내 외 다양한 스마트폰 운영체제 중, 특히 안드로이드의 경우 오픈소스 정책 및 다양한 기기의 보급을 통해 사용자가 증가하고 있다. 스마트폰은 데스크탑 PC와 매우 유사한 형태의 서비스를 사용자에게 제공하여 데스크탑 PC에서 발생할 수 있는 보안 위협들이 스마트폰에서도 유사하게 발생하고 있다. 따라서 스마트폰 사용자의 보안을 위해 전문적인 보안기술을 연구하고 대응방안을 마련하는 것이 필요하다[1,2].

안드로이드(Android)는 휴대 전화를 비롯한 휴대용 장치를 위한 운영 체제와 미들웨어, 사용자 인터페이스 그리고 표준 응용 프로그램(웹 브라우저, 전자우편 클라이언트, 단문 메시지 서비스(SMS), 멀티미디어 메시지 서비스(MMS)등)을 포함하고 있는 소프트웨어 스택이자 모바일 운영 체제이다. 안드로이드 사용자가 증가함에 따라 해커들의 공격이 늘어나고 있으며 개인정보 및 휴대폰 소액 결제 등을 이용한 피해가 증가하고 있다[3,4]. 본 보고서에서는 최근 주목 받고 있는 안드로이드 플랫폼 상에서의 안드로이드 OS환경, 보안 기능, 보안 모델, 취약점 등에 대한 항목별 내용 및 취약점 들을 정리하고 이를 통해 발생할 수 있는 문제점들에 대해서 고찰하였다.

공개용 모바일 운영체제 환경에서 애플리케이션의 제작이 쉬운 반면에 운영체제의 취약성과 애플리케이션의 취약점을 이용한 공격이 많아지고 있는 것을 파악하고 취약점을 통한 공격 시나리오를 분석함으로써 보다 안전한 스마트폰 환경을 연구할 수 있을 것으로 판단한다[5,6,7]. 그리고 보안 취약성에 대한 시나리오 구성을 통해 모바일 기기에서 발생할 수 있는 문제점을 각 단계별로 파악하고 제시함으로써 취약점에 대한 대비를 철저히 할 수 있도록 연구하였다.

II. 관련 연구

1. 관련연구

1.1 국내 동향

안드로이드는 자바로 작성된 응용프로그램을 수행하며 모바일 환경에 적합하게 수정된 고유의 보안 메커니즘을 가진 리눅스 기반의 플래폼이다[8,9]. 리눅스를 기반 운영체제로 사용함으로써 선점형 멀티태스킹, 효율적인 공유 메모리, Unix의 사용자 ID/그룹 ID, 그리고 파일접근 권한과 같은 기능들을 상속받아 사용한다. 또한 자바의 특성인 Type-safe와 가상기계 개념을 그대로 사용함으로써 샌드박싱과 같은 보안기능도 가지고 있다[10].

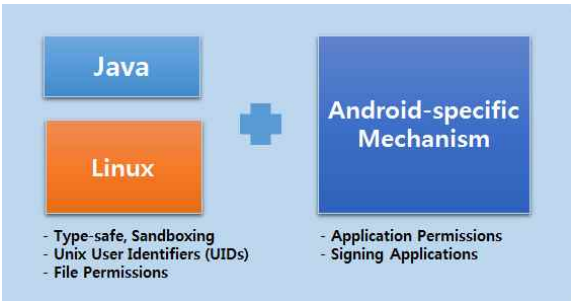

그림 275. 안드로이드 보안모델

또한 안드로이드 시큐리티 모듈(ASM) 프레임워크 개발자와 사용자들이 별도 루트 권한(관리자 권한)을 갖지 않고도 새로운 보안툴을 사용할 수 있게 하고, 서드파티 앱 개발사들이 자사 앱에 최신 보안기능을 실시간으로 제공할 수 있게 한다[11,12]. 다시 말해 안드로이드에서 정기적인 OS나 펌웨어 업데이트 없이도 보안기능을 활용할 수 있는 프레임워크로 정기 업데이트에 의존한 보안 대응 방안에서 벗어나 조금 더 빠르게 대응 할 수 있는 것이다.

III. 본 론

기존 악성코드는 대부분 불특정 다수를 대상으로 하고 개인정보 탈취가 주 목적이였으나 해당 악성코드는 대량의 개인정보유출 사고를 통해 유출된 개인정보 중 주민번호와 전화번호를 이용해 특정한 공격대상을 정하여 기존 악성코드보다 진보된 형태라 볼수 있으며 통신사 정보, 전화번호, 인증 SMS을 탈취하여 소액결제 피해를 발생 및 인증 번호 문자메시지를 사용자가 볼 수 없어 피해가 확산된다[13].

다음의 구체적인 단계를 통해 악성코드가 스마트폰을 장악하고 이로 인한 금전적 피해가 발생하는 것을 파악할 수 있으며 간략한 대응 방안도 기술한다.

1. 악성코드 공격 시나리오

다음 그림 1과 같이 악성코드에 감염된 스마트폰을 통해 소액결제에 필요한 정보를 탈취한 후 해커가 소액 결제를 하여 피해를 입힌 사례이다[14].

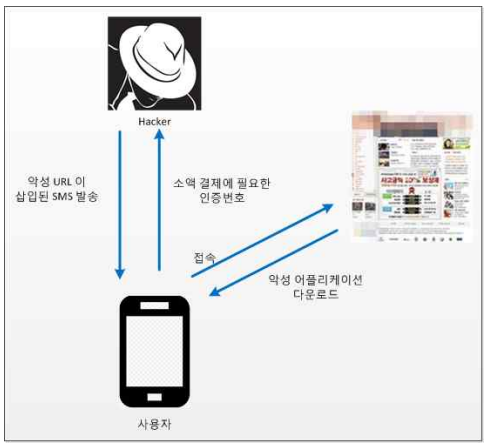

그림 276 스마트폰 소액결제 공격 구조

- 악성 어플리케이션 설치 유도 단계[15]

① 공격자는 스마트폰 소액 결제 공격을 하기 위해 어둠의 경로에서 개인정보를 입수한다.

② 공격자는 SMS를 통하여 악성 앱을 다운받을 수 있는 서버를 구축한다.

▶ 공격자는 서버 추적을 피하기 위해 국내가 아닌 외국에 서버를 구축해 둔다.

③ 공격자는 사전에 입수한 개인정보를 목록에 있는 공격대상에게 악성 어플리케이션을 유도하는 SMS를 발생한다.

▶ 공격자는 이름, 주민등록번호, 전화번호를 입수하여 추후 소액결제 공격을 할 수 있도록 한다.

③ 공격자는 사전에 입수한 개인정보를 목록에 있는 공격대상에게 흥미를 유발할 수 있는 문구를 SMS 통해 발송하여 악성 어플리케이션을 설치할 수 있도록 유도한다[16].

▶ 공격자는 입수한 전화번호 정보를 통하여 이벤트 관련(외식 영화 및 기타 유명 브랜드 무료쿠폰 등) SMS를 보낸다.

"OOO입니다. 새해 따듯하게 보내세요. 아메리카노 2잔 무료 http://xxx.xxx/xxxx"

"O월 명세표가 발송되었습니다. 바로확인하러 가기 http://www.xxx.xxx/xxxx"

"(O월 행사) OOOO에서 행운의 2만원 무료쿠폰받기 http://www.xxx.xxx/xxxx"

- 앱 다운로드 단계

① 공격자가 보낸 SMS를 받은 일부 사용자는 아무 의심없이 해당 어플리케이션을 다운 받는다.

- 악성 앱 설치단계

① 단말기에 악성 앱이 설치되는 과정에서 단말기 하드웨어 자원 사용 권한의 확인 및 승인을 요구한다.

▶ 기기의 위치 정보

▶ 기기 내 파일(이미지, 동영상, 오디오) 정보

▶ Wi-Fi 설정 여부나 연결된 Wi-Fi 기기의 정보 등

▶ 기기 통신사 정보

▶ 사용자는 정상 앱을 설치할 때처럼 권한에 관련하여 정확히 확인하지 않고 설치한다.

- 악성 앱 이 설치된 단말기 피해 단계

① 사용자의 단말기에 악성 앱이 설치가 되면 악성 앱에 등록되어 있는 공격자의 서버로 사용자의 단말기 전화번호와 통신사 정보를 공격자에게 전송한다.

② 공격자는 전화번호와 통신사 정보를 통해 이미 보유하고 있는 개인정보 중 주민번호와 감염된 스마트폰 사용자의 전화번호를 이용해 소액결제를 시도한다.

▶ 소액결제 두가지 인증

- 주민번호, 통신사 정보, 전화번호 1차 인증
- 소액결제를 신청한 스마트폰으로 발송된 인증문자

③ 소액결제 시 필요한 인증번호가 포함된 문자메시지가 사용자의 단말기로 전송된다.

④ 감염된 사용자 스마트폰은 인증번호가 포함된 SMS가 수신되면 결제사이트의 발신번호인 경우 사용자에게 SMS를 보여주지 않고 공격자에게 다시 전달한다.
⑤ 공격자는 전달받은 인증번호를 입력한다.
⑥ 소액결제가 가능한 사이트에서 정상적인 결제 절차를 완료하고 공격자는 현금화가 가능한 물품 구매를 완료한다.
⑦ 사용자는 정보가 외부 서보로 유출되는 것을 바로 알기 어렵기 때문에 청구서가 나온 후에야 피해 사실을 알 수 있다.

● 대응방법

① 사용자는 수상한 문자메시지로 받은 URL을 실행할 때 주의하는 것이 필수적이다.
▶ URL을 실행했을 때 어플리케션의 설치를 유 도 하면 설치 하지 않는 것이 좋다
② 사용자는 블랙 마켓이나 구글 공식 마켓이라도 안심하지 말고 다른 사용자의 평판을 읽어보고 설치하는 신중함이 필요하다.
③ 사용자는 스마트폰 전용 백신을 업데이트 및 수시로 점검을 하는 습관이 필요하다.

IV. 결 론

스마트폰의 하드웨어 및 운영체제의 기능성능 향상과 무선 통신 기술의 발전으로 스마트폰 사용자가 급증하고 있다. 이와 맞물려서 보안에 관한 문제점들도 함께 증가하고 있는 실정이다. 또한 스마트폰의 특징인 사용자의 편의성, 자율성, 개방성에 따른 장점들이 보안에 있어서 새로운 문제점들을 양산하고 있다. 이에 본 논문에서는 안드로이드 OS 커널 및 모바일 애플리케이션에 대한 신규 취약점을 알아보았다. 취약점은 버전 업이 되면서 줄어들고 있지만 여전히 모바일 기기 자체의 취약점은 많은 피해를 입을 수 있다. 특히 커널 및 서비스 관련 취약점 뿐만 아니라 사용자의 미흡한 권한 관리에서도 치명적인 피해를 입을 수 있다는 것은 사용자의 권한 관리가 얼마나 중요한 것인지 공격 시나리오를 통해서 알 수 있다. 대부분의 취약점은 발견 시 버전 업을 통하여 지속적으로 문제를 해결하고 있으므로 사용자는 지속적인 OS 업그레이드를 통하여 스마트폰 위협에 대응하여야 한다.

참고문헌

[1] Divya Muthukumaran, Anuj Sawani, "Measuring Integrity on Mobile Phone Systems", 2008
[2] SACMAT '08 Proceedings of the 13th ACM symposium on Access control models and technologies pp.155-164, 2008
[3] http://en.wikipedia.org/wiki/Android_version_history
[4] https://github.com/droidsec/droidsec.github.io/wiki
[6] https://github.com/droidsec/droidsec.github.io/wiki/Vuln-Exploit-List
[7] https://github.com/droidsec/droidsec.github.io/wiki/Android-Crackmes
[8] https://github.com/droidsec/droidsec.github.io/wiki/Android-Tools
[9] http://chogar.blog.me/80207139538
[10] http://mutantcell.blog.me/203794743
[11] http://www.trendmicro.co.kr/kr/support/blog/index.html
[13] http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224
[14] http://www.apk-analyzer.net/reports
[15] http://contagiodump.blogspot.kr/
[16] http://www.kernelmode.info/forum/viewforum.php?f=16