SE-Android 보안 기술 동향*

최정호·양승제·김기범 (한국전자통신연구원 부설연구소)

목차

1. 개 요

스마트폰 보급률이 급증하면서 2014년 말부터 스마트폰 보급률은 PC 보급률을 앞지르고 있다[1]. 갈수록 스마트폰에 대한 의존도가 늘어가면서 스마트폰을 이용한 각종 보안 사고들이 잇따르고 있다. 애플사의 대표 스마트폰인 아이폰은 보안성이 뛰어난 것으로 알려져 있고 아직까지 보안 사고에 대한 우려가 적은 편이지만 국내에서 80% 이상의 점유율을 차지하는 안드로이드 스마트폰은 초기 버전에서 각종 취약점으로 인한 보안 사고들이 종종 발생하여 보안성에 대한 신뢰도가 강하지 않았다. 이에 따라 안드로이드 진영에서는 새 OS를 출시하면서 강화된 보안 솔루션을 탑재하여 애플사만큼의 보안 신뢰성을 쌓아가고 있다.

최근 안드로이드에 탑재되기 시작한 대표적인 보안솔루션 중 하나인 SE-Android는 안드로이드의 커널 계층에 탑재된 보안 플랫폼이다. 이는 SE-Linux를 기반으로 하여 안드로이드의 보안 강화를 위해 만들어진 것으로 정식 명칭은 Security Enhancements for Android(이하 SE-Android)이다. 본 기고문에서는 안드로이드 장치의 보안을 강화하는 기술 중 대표적인 기술인 SE-Android에 대해 소개한다. 대표적인 안드로이드 장치 제조회사인 삼성전자에서 SE-Android를 어떻게 활용하여 보안을 강화하고 있는지 살펴본 뒤, 안드로이드 장치 보안 강화 기술의 연구 방향에 대해 논하며 본 기고문을 마치고자 한다.

2. SE-Android 보안 기술 개요

2.1 정의

SE-Android는 SE-Linux를 기반으로 개발된 안드로이드의 보안 강화 플랫폼이다[2]. SE-Linux는

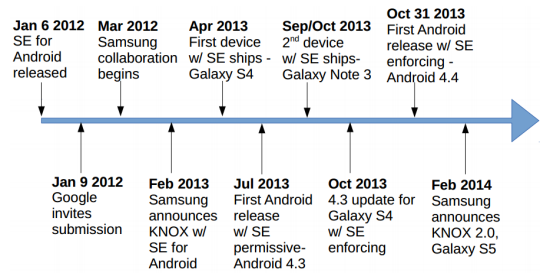
* 편집자 주) Android 스마트폰은 시장 점유율에 나타난 바와 같이 IoT의 End-point로 널리 사용될 것이므로 IoT보안의 주요 기기가 될 것이다.

리눅스에서 보안성을 최대한으로 유지하기 위한 플랫폼 중 하나다[3]. 안드로이드는 리눅스를 기반으로 만들어진 OS이고 안드로이드 보안강화에 대한 요구가 커짐에 따라 SE-Linux를 기반으로 한 SE-Android가 등장하였다. 안드로이드 OS가 점차 업그레이드됨에 따라서 SE-Android를 채택하고 있는 제조회사가 늘고 있다. 안드로이드 OS 버전 4.3 인 젤리빈을 기점으로 SE-Android가 보안 솔루션으로써 본격적으로 탑재되는 추세를 보이고 있다. SE-Android가 탑재된 스마트폰의 설정 화면에는 SE-Android의 설정상태를 확인할 수 있고 이 상태는 SE-Android의 유무 및 기능 활성화 상태 확인과 관련 있다.

삼성전자의 경우 SE-Android는 안드로이드 OS 버전 4.2.2 부터 탑재 계획 중이었으며 안드로이드 OS 버전 4.3부터 본격적으로 탑재하였다.

SE-Android는 기존 안드로이드의 자유재량 접근 제어 (DAC; Discretionary Access Control) 환경 대신 의무 접근 제어(MAC; Mandatory Access Control)를 구현할 수 있도록 한다. 또한 SE-Android는 특정 SE 정책을 정의하는 것을 기반으로 시스템 및 객체에 특별 권한을 부여할 수 있다. 의무 접근 제어 환경에서는 SE-Android가 커널 리소스의 액세스를 제어하기 때문에, 사전에 정의한 SE 정책에 부합되지 않는 행동을 하는 어플리케이션을 수행되지 않게 하여 보안성을 강화하는 역할을 수행한다. SE 정책에는 사용자, 프로그램, 프로세스 그리고 이들의 동작 대상인 파일과 디바이스를 포함한 시스템 전체, 즉, 모든 주체와 객체에 대한 접근허가(access permissions)에 대한 내용이 포함된다[4].

SE-Android는 2012년 처음으로 릴리즈 되었으며 삼성전자의 대표 안드로이드 장치인 갤럭시 시리즈를 주축으로 점차 채택이 확장되고 있는 추세이다. 2015년 4월 발매 예정인 갤럭시S6 시리즈에도 여전히 SE-Android를 탑재할 예정이다. (그림 1)은 SE-Android의 기술 발전 순서를 보여준다[5].



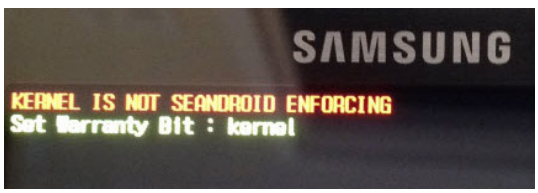
(그림 1) SE-Android 기술 발전 순서

2.2 개발 목적

SE-Android는 안드로이드의 보안 강화를 위해 NSA(National Security Agency, 미 국가안보국)에서 개발되었으며 삼성전자가 갤럭시S4의 안드로이드 OS 4.3 업그레이드 시 SE-Android를 정식 탑재함으로써 본격적으로 안드로이드 스마트폰에 탑재되고 있다.

SE-Android는 SE-Linux와 마찬가지로 루트 관리자 권한 이상으로 보안을 유지하며, 커널, 파일 시스템 등의 보안을 강화할 수 있다. 예를 들면 (그림 2)와 같이 SE-Android가 탑재된 스마트폰에서 인증되지 않은 커널을 탑재한 후 부팅하게 되면 해당 파일은 보안성에 위배된다고 판단하여 부팅을 보류하고 순정 커널로 교체하도록 권하는 메시지를 출력함으로써 보안 취약성이 있을 수 있는 변조된 커널을 탑재하는 것을 방지한다.

SE-Android는 현재 오픈 소스로 공개되어 있으며, 모든 안드로이드 장치에 탑재할 수 있도록 되어있다[2]. 그러나 탑재하기 위해서는 전문적인 지식과 실력을 바탕으로 진행해야하기 때문에 개발목적이 아닌 이상 개인이 임의로 안드로이드 기기에 SE-Android를 탑재하는 것은 쉽지 않다.



(그림 2) 순정이 아닌 커널 이미지를 넣었을 경우 메시지 출력

일반적으로 안드로이드 장치 제조업체에서 SE-Android를 탑재할 기기에 맞게 커널을 제조한 후 탑재하고 있다. SE-Android의 주요 사용 목적은 악의적으로 만들어진 어플리케이션을 통한 데이터 유출 방지 및 보안 모듈 강화, 그리고 어플리케이션과 데이터의 무결성 유지 등으로 요약할 수 있다.

2.3 SE-Android 상태별 기능 수행

SE-Android를 탑재한 후 기능 수행 상태를 설정할 수 있는데, Enforcing, Permissive, Disabled의 세 가지 중 하나의 상태로 설정할 수 있다. 각각의 상태별 기능 수행 내용은 다음과 같다[6].

첫 번째로 Enforcing 상태는 제조사가 정의한 SE-Android 정책 파일이 적용되어 보안 강화 정책을 수행하는 상태를 의미한다. 이 상태로 설정된 SE-Android는 그것이 탑재된 안드로이드 장치를 여러 보안 위협으로부터 적극적으로 보호하며 정의된 SE 정책 파일에 따라 악성 코드가 포함된 어플리케이션의 액세스 권한을 거부하는 등의 보안 강화 정책을 수행한다.

삼성 스마트폰의 경우 안드로이드 OS 4.3 부터 Enforcing 상태로 SE-Android가 수행되도록 설정되었다. SE 정책을 주기적으로 업데이트함으로써 시시각각 변하는 보안 위협에 발 빠르게 대응하고 있다.

두 번째로 Permissive 상태는 SE-Android 정책 파일을 로드하지만 안드로이드 장치가 이를 적용하지 않는 상태를 의미한다. 악성 코드가 포함된 어플리케이션이 허용되지 않는 리소스에 대한 접근을 시도하면 해당 액세스에 대한 로그를 기록하여 시스템에 남기지만 액세스 자체를 금지하지 않는다. 즉, Permissive 상태는 SE-Android를 본격적으로 적용하기 전에 그것을 테스트하고 디버깅하기 위한 상태임을 알 수 있다. 기존 SE 정책을 위반하였다고 판단된 어플리케이션의 수행과정이 로그 파일로 만들어지고, 추후 그것을 분석하여 새로운 어플리케이션의 보안 위협을 파악하고 사전에 방지하는 새로운 SE 정책 파일을 만들어 안드로이드 장치에 배포하고 적용 할 수 있다. 물론 이러한 정책 업데이트 과정은 Enforcing 상태에서도 진행되지만, 안드로이드 장치에 공식적으로 SE-Android를 탑재하기 전에 테스트를 진행하기 위해서는 Permissive 상태로 수행해야 한다.

삼성전자에서 SE-Android를 공식적으로 첫 탑재한 갤럭시S4의 경우 안드로이드 OS 버전 4.2.2에는 Permissive 모드로 SE-Android를 탑재하였는데, 이로 미루어보아 그 당시에는 SE-Android를 사전에 테스트한 것이었음을 알 수 있다.

마지막으로 Disabled 상태는 SE-Android 시스템이 활성화되지 않고 SE 정책 파일도 로드되지 않은 상태를 의미한다. 악성행위를 하는 어떠한 어플리케이션에 대해서도 그것에 대한 로그 파일이 생성되지 않으며, 따라서 안드로이드 시스템이 전반적으로 보안 위협에 취약한 상태이다. SE-Android가 탑재된 시스템에서 Disabled 상태는 거의 적용되지 않는다.

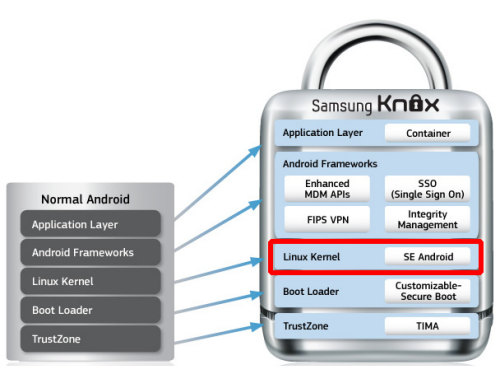
(그림 3)은 삼성전자의 갤럭시노트3의 디바이스 정보 메뉴에서 확인할 수 있는 SE-Android 상태를 보여준다. 안드로이드 OS는 4.4.2 이고 SE-Android가 Enforcing 상태로 설정되어 있는 것을 확인할 수 있다.

(그림 3) SE-Android가 탑재된 갤럭시노트3 (Enforcing 상태)

3. 삼성전자의 SE-Android 적용 방법

3.1 KNOX플랫폼과 결합한 SE-Android

본 절에서는 삼성전자가 어떠한 방식으로 SE-Android를 적용하여 보안성을 강화하였는지에 대하여 알아보도록 한다. 삼성전자는 안드로이드 진영에서 SE-Android를 처음 본격적으로 채택한 회사이다. 삼성전자는 자체 개발 보안 솔루션인 KNOX와 SE-Android를 결합하여 강화된 보안성을 제공하고 있다[6]. KNOX 내부의 커널 계층에서 SE-Android는 기 설정된 SE 정책을 기반으로 다양한 보안 정책을 설정 및 수행할 수 있다. 삼성전자는 커널 계층의 무결성을 보장하기 위한 SE 정책을 설정하여 SE-Android를 탑재하였다. (그림 4)와 같은 계층 구조로 KNOX 플랫폼에 SE-Android를 결합하여 탑재 및 운용하고 있다[6].



(그림 4) 삼성의 SE-Android 탑재 방법 (with KNOX)

3.2 삼성전자의 SE-Android 운용 방식

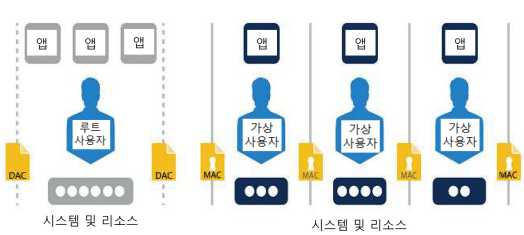
안드로이드 운영체제의 기반이 되는 리눅스에서는 자유재량 접근 제어(DAC) 방식으로 사용자가 임의로 파일 읽기, 쓰기 및 실행 권한을 부여할 수 있다. 이러한 환경에서 악의적인 사용자가 자유재량 접근 제어 권한을 획득하면 데이터 파일 및 어플리케이션 리소스에 무단으로 접근할 수 있다. 보안 솔루션이 적용되지 않은 일반 안드로이드 장치에서도 기본적으로 자유재량 접근 제어 방식으로 리소스를 관리하고 있다. 악의적인 사용자는 장악된 안드로이드 장치에 비밀번호를 읽는 어플리케이션 또는 스팸을 보내는 메일 클라이언트 등 각종 악성 어플리케이션을 설치하여 기밀문서를 인터넷에 업로드하거나 카메라 또는 마이크를 몰래 켜는 등의 작업을 수행할 수 있는 문제점이 발생할 수 있다.

삼성전자는 SE-Android를 다음과 같이 활용하여 안드로이드 장치에서 발생할 수 있는 각종 보안 관련 문제들로부터 운영 체제를 보호한다. 먼저, 운영 체제를 보안 도메인으로 파티셔닝(partitioning)한다. 각 도메인 내에서 작동하는 데 필요한 최소한의 권한만 어플리케이션에 부여한다. 이로써 악성 코드가 포함되거나 결함 있는 어플리케이션으로 인한 손상을 억제하며 한 도메인

내의 문제가 다른 도메인으로 퍼지는 것을 방지한다. (그림 5)에 이러한 과정이 도식화되어있다[6].

또한 SE 정책 파일을 사용하여 파일 및 리소스에 접근할 수 있는 사용자와 어플리케이션을 각각 정의한다. 사용자는 이 정책 파일을 재정의 할 수 없다. 예를 들어 다른 방법으로 제한되어 있는 파일 또는 리소스 접근 권한을 자신에게 부여할 수 없다. 안드로이드 장비가 새로운 보안 정책이 반영된 최신 정책을 항상 사용하도록 하려면 SE 정책 파일이 자동으로 업데이트되도록 설정하면 된다. SE-Android가 탑재된 삼성 안드로이드 장치에서 허가되지 않은 접근을 감지하면 사용자에게 알림 메시지가 표시되며, 보안 정책 업데이트에 대한 정보 제공에 동의한 사용자들로부터 수집한 이러한 보안 위협 행위를 추후 SE 정책 파일에 반영한다. 삼성전자는 SE-Android의 보안정책을 주기적으로 업데이트함으로써 점차 안드로이드 장치의 보안을 강화하는데 활용하고 있다.

삼성전자에서 개발한 안드로이드 보안 시스템인 KNOX 2.0 플랫폼에는 SE-Android 정책 에 제어된 접근 권한을 제공하는 SEAMS(SE for Android Management Service)라는 새로운 기능이 추가되었다[6]. SEAMS는 KNOX 2.0 워크스페이스에 의해 내부적으로 사용되고, 타사 공급업체가 자체 컨테이너 솔루션을 보호하는 데 사용할 수도 있다. 또한 SEAMS를 통해 기업은 개별 SE-Android 정책 파일을 교체할 수 있다. KNOX 2.0 플랫폼에 탑재된 SE-Android는 어플리케이션 또는 프로세스가 허용되지 않은 데이터 및 리소스에 접근하지 못하도록 한다. 예를 들어, KNOX 컨테이너 외부의 어플리케이션은 컨테이너 내부의 어플리케이션 데이터에 접근할 수 없도록 제한된다.



(그림 5) DAC와 MAC을 이용한 삼성 KNOX와 SE-Android의 사용자 보호 방법

4. 결 론

본 기고문에서는 SE-Linux를 기반으로 안드로이드를 위해 만들어진 SE-Android 기술에 대하여 살펴보았으며 국내 안드로이드 장치 점유율의 대부분을 차지하고 있는 삼성전자에서 그것을 보안 강화에 어떻게 활용하고 있는지에 대하여 알아보았다.

SE-Android는 오픈 소스 형태로 제공되고 있으며 사용자가 원하는 대로 안드로이드 장치에 설치 할 수 있지만 커널을 수정하는 작업이기 때문에 신중하게 수행되어야 하며 고난도의 기술을 요구한다. 따라서 제조회사에서 SE-Android를 직접 회사의 정책에 맞게 변형하여 제공하고 있다. 삼성전자는 자체 개발한 보안 솔루션인 KNOX의 커널 계층에 SE-Android를 적용하여 커널의 무결성을 보강하는데 활용하고 있다. SE-Android의 보안정책을 주기적으로 업데이트함으로써 안드로이드 장치의 보안을 강화하고 있다.

애플사의 대표 스마트폰인 아이폰은 보안성이 강력하여 보안에 대한 신뢰성이 매우 높은데 반해 국내에서 80% 이상의 비중을 차지하는 안드로이드 장치는 초기 버전에서 발생한 보안 취약점으로 인해 보안에 대한 신뢰가 낮았다. 하지만 해를 거듭하여 안드로이드 OS를 출시하면서 SE-Android를 비롯한 강화된 여러 보안 솔루션을 탑재하여 애플사만큼의 보안 신뢰성을 쌓아가고

있다. 향후 보안성 강화는 스마트폰에서 가장 중요한 과제로 남을 것이며 그것이 곧 스마트폰의 경쟁력이 될 것이다.

참 고 문 헌

[1] 2014년 방송매체이용행태조사결과, 방송통신위원회, http://www.kcc.go.kr/

[2] Security Enhancements (SE) for AndroidTM, http://seandroid.bitbucket.org/

[3] Security-Enhanced (SE) Linux, http://en.wikipedia.org/wiki/ Security-Enhanced_Linux

[4] SELinux의 이해, KLDP, https://kldp.org/files/selinux_140.pdf

[5] Security Enhancements (SE) for Android, Android Builders Summit 2014, http://events.linuxfoundation.org/sites/events/files/slides/abs2014_seforandroid_smalley.pdf

[6] KNOX, 삼성전자, https://www.samsungknox.com/ko/

저 자 약 력

최 정 호

이메일: jhchoi@nsr.re.kr

- 2007년 카이스트 전산학과 (학사)
- 2009년 카이스트 전산학과 (석사)
- 2012년 카이스트 전산학과 (박사)
- 2012년~현재 한국전자통신연구원 부설연구소 선임연구원
- 관심분야 : 모바일 포렌식, 멀티미디어 포렌식, 디지털 워터마킹, 정보보호

양 승 제

이메일: sjyang@nsr.re.kr

- 1997년 2월 한양대학교 컴퓨터공학과(공학사)
- 1999년 2월 한양대학교 컴퓨터공학과(공학석사)
- 2003년 8월 한양대학교 컴퓨터공학과(공학박사)
- 2004년 2월~2005년 3월 뉴욕주립대 박사후과정
- 2005년 3월~2008년 8월 LG전자 MC연구소 책임연구원
- 2008년 9월~현재 한국전자통신연구원 부설연구소 선임연구원
- 관심분야 : 모바일 포렌식, 컴퓨터 포렌식, 정보보호

김 기 범

이메일: kibom@nsr.re.kr

- 1994년 2월 제주대학교 정보공학과 (공학사)
- 1996년 8월 고려대학교 전산과학과 (이학석사)
- 2001년 2월 고려대학교 전산과학과 (이학박사)
- 2001년 1월~2004년 7월 ㈜ECO개발부장
- 2004년 8월~현재 한국전자통신연구원 부설연구소 책임연구원
- 관심분야 : 컴퓨터 포렌식, 모바일 포렌식, 정보보호