스마트폰을 위한 안전하고 효율적인 무결성 검증 방법

한진희, 전용성
한국전자통신연구원 사이버보안연구본부 사이버보안시스템연구부
e-mail : hanjh@etri.re.kr

A Method for Safe and Efficient Integrity Verification of Smartphones

Jin-Hee Han, YongSeong Jeon
Cyber Security Research Department, ETRI

요 약

본 논문에서는 MTM(Mobile Trusted Module)과 커널상에 저장된 무결성 검증 파일을 이용하여 스마트폰의 부트로더 이미지 및 커널 이미지, 커널이 로딩되며 실행되는 실행파일, 라이브러리 파일 등의 무결성을 안전하고 효율적으로 검증하는 방법을 제안한다. 부트로더 이미지와 커널 이미지, 외부로부터 악의적으로 변경되거나 수정될 경우 심각한 문제를 일으킬 수 있는 실행 파일이나 라이브러리 파일 등의 무결성 검증은 MTM 을 이용하여 안전하게 처리하고, 그 외 파일들의 무결성 검증은 커널상에 저장된 무결성 검증 파일을 이용하여 처리함으로써 MTM 기반 무결성 검증 기능을 모든 파일에 적용하는 경우에 발생될 수 있는 처리 시간 지연, 성능 저하 등의 문제점을 방지할 수 있다.

1. 서론

최근 단말의 프라이버시 데이터 보호 위협, 단말 내 악성 코드 삽입, 사용자의 부주의로 인한 시스템 분실 혹은 악의적인 외부 제 3 자에 의한 시스템 도난 등을 통해 단말 복제, 도청 및 악용, 등의 보안 위협이 급증하면서 그 해결 방안을 다양한 각도에서 분석하며 개발하고 있는 추세이다[1][2]. 하지만, 여전히 소프트웨어적인 보안 방식이 대다수를 이루는데 실제로 소프트웨어적인 보안 방식은 데이터가 저장되어 있는 메모리가 분실되거나 외부로부터 악의적으로 해킹될 경우, 메모리에 저장되어 있던 중요 데이터 및 키 값들이 고스란히 유출될 수 있기 때문에 단말 해킹 시 아무런 보호 기능을 제공해주지 못하는 문제점을 지닌다. 이러한 문제점을 해결하기 위한 방안으로서 하드웨어 기반의 보안 방식에 대한 요구가 제기되었으며, TCG (Trusted Computing Group)에서 모바일 환경에 적합한 하드웨어 보안 모듈인 MTM 을 발표하였다. MTM 은 모바일 단말에 장착되어 단말 자체에 대한 플랫폼 무결성 검증 기능은 물론 차폐 영역과 보호 능력 및 안전한 키 관리 체계, 물리적인 안전성 등 다양한 보안 기능을 제공하기 때문에 단말 플랫폼의 무결성 검증 및 단말 내부에서 사용되는 파일들을 안전하게 처리하고 관리해 줄 수 있는 환경을 제공한다[3][4].

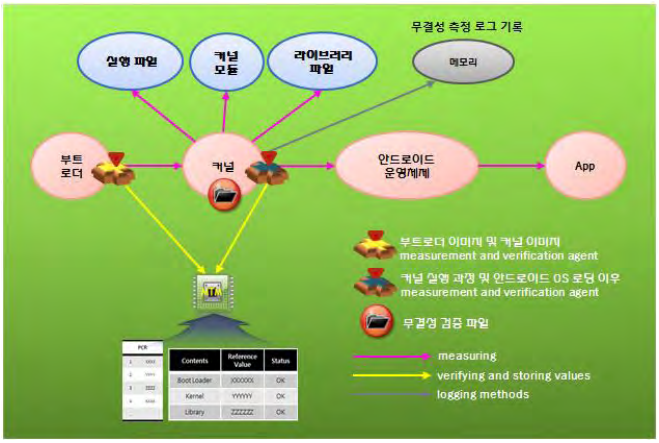
본 논문에서는 이러한 다양한 보안 기능을 제공해주는 MTM 과 커널상에 저장된 무결성 검증 파일을 이용하여 무결성 검증 방법을 파일의 중요도에 따라 MTM 기반 또는 무결성 검증 파일 기반으로 분류하여 보다 안전하고 효율적인 스마트폰의 무결성 검증 방법을 제안한다.

2. 본론

RoT (Root of Trust) 기능을 제공해주는 MTM 은 tamper-resistant 컴포넌트로써 데이터를 안전하게 저장 하는 RTS (Root of Trust for Storage), 시스템 상태를 신뢰할 수 있는 방법으로 증명하는 RTR (Root of Trust for Reporting) 역할을 담당하며, power-on 시에 가장 먼저 실행되고, 항상 신뢰할 수 있는 컴포넌트인 CRTM (Core Root of Trust for Measurement)이 시스템의 상태를 점검한 뒤 PCR (Platform Configuration Register)에 기록하는 RTM 역할을 담당 한다. CRTM 은 PC 의 경우 BIOS 에 포함될 수 있으며 임의로 수정할 수 없는 특징을 갖는다. 또한, MTM 은 중요한 데이터 및 키를 외부로 절대 유출시키지 않으며, MTM 내에 데이터나 키를 저장할 수 있는 공간이 부족할 경우 SRK (Storage Root Key)를 이용하여 MTM 외부에 중요한 데이터나 키 값을 저장하는 안전 저장(protected storage) 기능을 제공한다[5].

모바일 단말, 즉 안드로이드 기반 스마트폰의 경우 power-on 시에 가장 먼저 실행되는 프로그램이 부트로더이며, 부트로더 로딩 후 커널이 로딩되고 이후 안드로이드가 로딩되어 실행된다. (그림 1)은 본 논문에서 제안한 MTM 과 커널상에 저장된 무결성 검증 파일을 이용한 안드로이드 기반 스마트폰의 무결성

검증 과정을 보여준다.

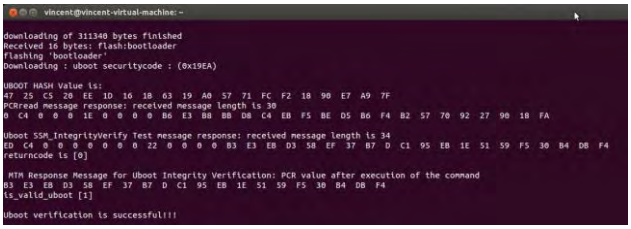


(그림 1) 제안한 스마트폰의 무결성 검증 과정

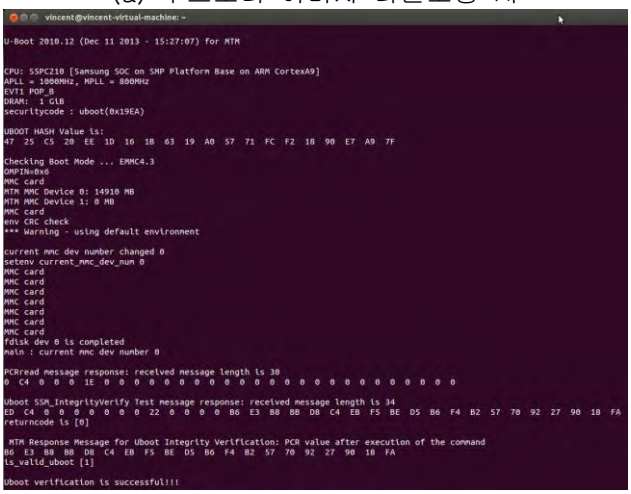
단계별로 이루어지는 각 구성요소 별 무결성 측정 과정은 chain of trust 라고 불리는데, (그림 1)에서 보는 바와 같이 부트로더상에서 MTM 을 이용하여 부트로더 이미지와 커널 이미지에 대한 무결성 측정 및 검증 기능을 차례대로 수행하는 에이전트는 MTM 으로부터 무결성 검증 성공 메시지를 전달받은 후 부트로더 실행 및 커널 실행을 허가한다. 부트로더 이미지와 커널 이미지의 경우, 스마트폰에 다운로딩 시, 스마트폰상에서 실행 시 두 가지 상황 모두에 무결성 검증 에이전트가 동작하도록 구현되었으며, 에이전트는 부트로더 프로그램내에 포함되도록 설계하였다. (그림 2)는 다운로딩 및 실행 시점에 MTM 을 이용하여 수행되는 부트로더 이미지와 커널 이미지에 대한 무결성 측정 및 검증 메시지를 보여준다.

이후, 커널상에서 MTM 과 무결성 검증 파일을 이용하여 커널이 실행될 때 로딩되는 실행 파일, 커널 모듈 및 라이브러리 파일 등에 대한 무결성 측정 및 검증 기능을 수행하는 에이전트는 중요 파일에 대한 무결성 검증 결과는 MTM 으로부터 전달받아 처리하고, 그 외 파일들에 대한 무결성 검증은 무결성 검증 파일에 기록된 정보를 바탕으로 수행하여 처리한다. (그림 3)은 MTM 을 이용한 커널상의 실행 파일, 커널 모듈 및 라이브러리 파일 등에 대한 무결성 측정 및 검증 기능을 수행하는 에이전트의 내부 구조이며, (그림 4)는 MTM 을 이용하여 setup_fs, app_process 파일의 무결성 측정 및 검증을 수행한 결과와 커널상에 저장된 무결성 검증 파일을 이용하여 libandroid_runtime 파일의 무결성 측정 및 검증을 수행한 결과를 보여준다.

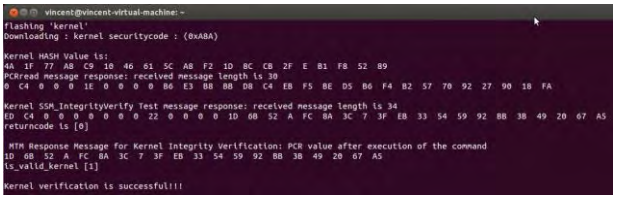
(그림 2)와 (그림 4)에서 보는 바와 같이 MTM 을 이용한 무결성 검증을 수행할 경우 에이전트는 무결성 검증 요청 메시지를 생성하여 MTM 에게 전달하게 되는데 이때 SSM_IntegrityVerify 메시지 형태를 사용한다. SSM_IntegrityVerify 메시지는 본 논문에서 제안한 파일의 무결성 검증 처리를 위해 별도로 정의한 메시지 형태로 MTM 은 해당 메시지가 전송될 경우, 무결성 검증에 필요한 데이터를 추출하여 내부에



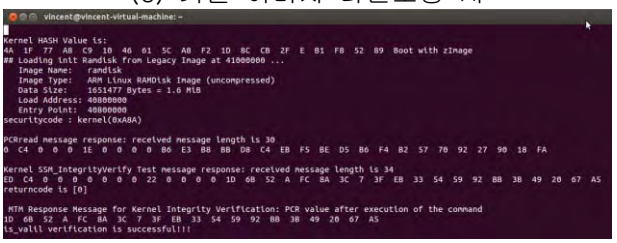
(a) 부트로더 이미지 다운로딩 시



(b) 부트로더 이미지 실행 시



(c) 커널 이미지 다운로딩 시



(d) 커널 이미지 실행 시

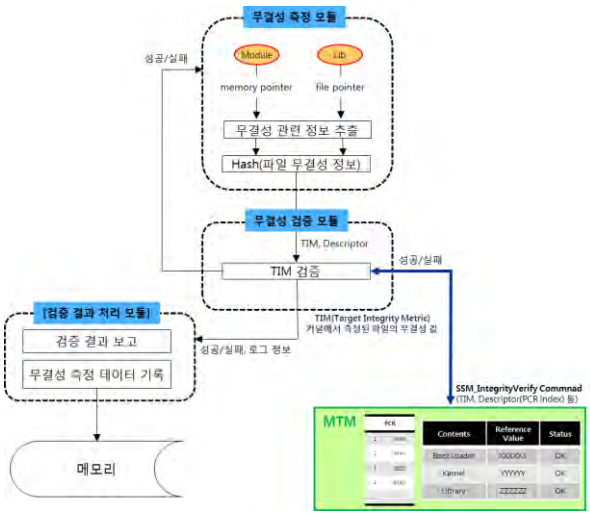
(그림 2) MTM 을 이용한 부트로더 이미지 및 커널 이미지 무결성 검증 과정

저장된 참조 값과 비교 검증을 수행한 후 검증 결과를 에이전트에게 전달하게 된다. MTM 은 검증 결과가 성공적일 경우 결과 값으로 0 을 보내주며 실패할 경우 결과 값으로 9 를 전달한다.

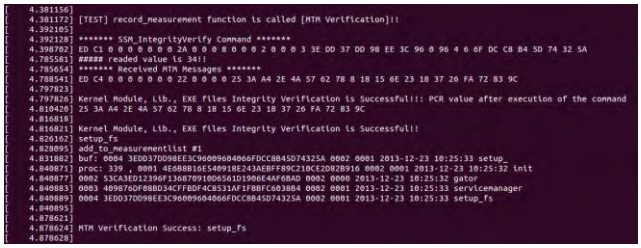
부트로더 이미지와 커널 이미지, 커널상에서 중요파일로 분류된 파일들의 무결성 검증 참조 값은 MTM 내에 안전하게 저장되어 있으며, 각 구성요소를 식별하기 위한 식별자를 MTM 과 에이전트가 공유하여 사용한다. 무결성 검증 결과가 성공적으로 수행될 경우, MTM 은 구성요소에 따라 사전에 할당된 PCR 인덱스에 무결성 측정 값을 기록(extend 과정)한다. 무결성 검증 파일에 저장된 파일들의 무결성 검증 참조 값은 (그림 5)에 보이는 바와 같은 형태로 사용한다.

또한, 커널상에 탑재된 에이전트는 무결성 측정 및

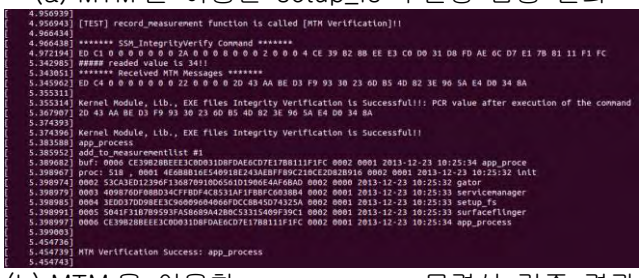
검증 정보를 수행 순서에 따라 파일에 기록하는데, 수행 순서, 무결성 측정 값, 검증 성공 후 extend 된 PCR 인덱스, 무결성 검증 결과(성공: 1, 실패: 0), 날짜 및 시간, 검증 파일 이름 등의 정보가 파일에 저장되게 된다. (그림 6)은 무결성 측정 및 검증 과정 시 생성되는 로그 정보를 보여준다.



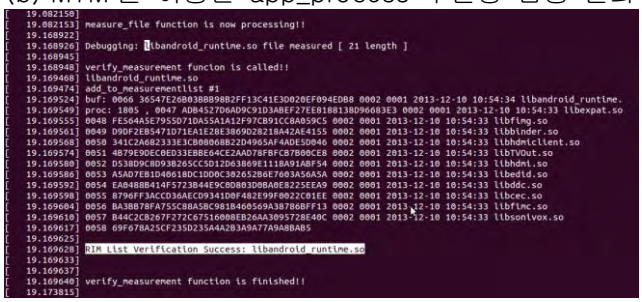
(그림 3) 커널상에 탑재된 에이전트 내부 구조



(a) MTM 을 이용한 setup_fs 무결성 검증 결과

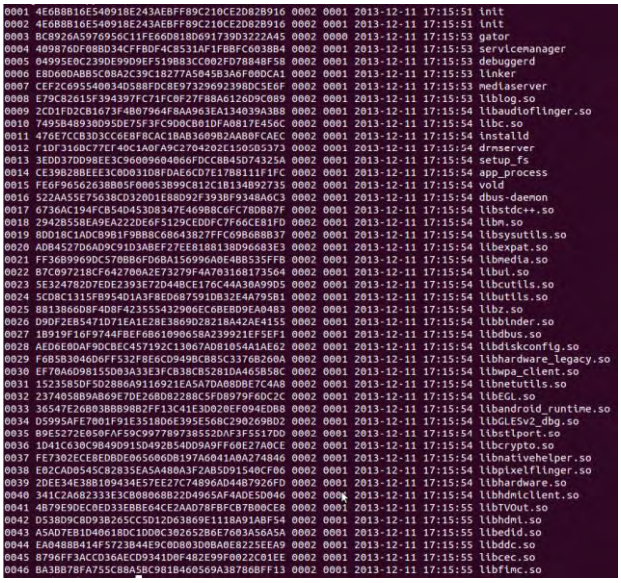


(b) MTM 을 이용한 app_process 무결성 검증 결과



(c) 무결성 검증 파일을 이용한 libandroid_runtime 무결성 검증 결과

(그림 4) MTM 을 이용한 부트로더 이미지 및 커널 이미지 무결성 검증 과정



(그림 5) 무결성 측정 및 검증 로그 정보

(그림 6) 무결성 측정 및 검증 로그 정보

논문에서 제안한 무결성 검증 방법을 테스트하기 위해 사용한 단말은 현재 MTM 을 장착할 수 있도록 자체 제작된 스마트폰으로 커널 버전은 3.0.15 SMP PREEMPT, 안드로이드 버전 4.0.4, ARM Cortex-A9 기반 듀얼 CPU 코어, 1.2GHz 클럭 속도, 128MB 내부 RAM, 모바일 DDR2 1GB 메모리, 임베디드 멀티미디어 카드(eMMC) 16GB 사양을 갖추고 있다. ADB 용 케이블과 minicom 출력용 케이블을 인터페이스 보드 및 시험 단말에 연결하여 부트로더 및 커널, 안드로이드 이미지 파일을 퓨징한 후, 무결성 측정 및 검증 정보를 확인하였다.

부트로더와 커널에 현재 구현되어 동작하는 에이전트는 동적(dynamic)인 특성보다는 정적(static)인 특성을 갖고 있으며. 커널상에 저장되는 무결성 검증

파일의 무결성 참조 값은 커널이 실행되기 전에 파일의 측정 값을 미리 측정한 후 측정 된 값을 입력하여 사용하였다. 그리고, 커널상에 탑재된 에이전트가 무결성 측정 및 검증 정보를 기록하는 파일은 proc 파일 시스템을 이용하여 생성된 파일로 커널모드가 아닌 유저모드에서도 쉽게 접근할 수 있도록 하였다.

3. 결론

본 논문은 MTM 과 커널상에 저장된 무결성 검증 파일을 이용하여 스마트폰의 부트로더 이미지 및 커널 이미지, 커널이 로딩되며 실행되는 실행파일, 라이브러리 파일 등의 무결성 측정 및 검증을 안전하고 효율적으로 수행할 수 있는 방법을 제안하고, 이에 대한 시험 과정 및 결과를 소개하였다.

향후, 정적 특성만을 제공하는 에이전트에 기능을 추가하여 동적 특성까지 포함할 수 있도록 개발 할 예정이며 스마트폰에 탑재되는 애플리케이션을 위한 무결성 검증 기능도 추가할 예정이다.

또한, 커널상에 저장되어 사용되는 무결성 검증 파일과 무결성 측정 및 검증 정보를 기록하는 파일은 접근 제어 기능을 강화하여 외부에서 악의적으로 조작하거나 변경할 수 없도록 안전하게 저장하여 관리할 있도록 설계할 것이다.

ACKNOWLEDGMENT

본 연구는 미래창조과학부의 방송통신기술개발사업 과제 “ MTM 기반 단말 및 차세대 무선랜 보안 기술 개발”의 일환으로 수행되었음(12-912-06-001)

참고문헌

[1] 서승현, 전길수, “ 스마트폰 보안 위협 및 대응 전략”, TTA 저널 132 호, pp. 44-48, 2010 년 11 월

[2] 강동호 외 6 명, “ 스마트폰 보안 위협 및 대응 기술”, 전자통신동향분석 제 25 권 제 3 호, pp. 72-80, 2010 년 6 월

[3] Siani Pearson, “ Trusted Computing Platforms”, 2003.

[4] TCG, “ TCG Mobile Trusted Module Specification. Version 1.0, Revision 7.02, April 28, 2010

[5] S. Choi, J. Han, J. Lee, J. Kim, S. Jun, “ Implementation of a TCG-based trusted computing in mobile device”, TrustBus 2008 pp.18-27