안전한 스마트 단말을 위한 가상화 기반 도메인 분리 보안 플랫폼 구현

(Implementation of Virtualization-based Domain Separation Security Platform for Smart Devices)

김정녀*

(Jeong Nyeo Kim)

요 약

최근 들어, 스마트 단말에서 오피스, 화상회의 등 스마트워크 업무와 관련된 중요한 정보들을 다루는 경우가 많아졌다. 또한 스마트 단말의 실행환경이 공개 소프트웨어 환경 위주로 발전하면서, 사용자들이 임의의 응용소프트웨어를 다운받아 사용하는 것이 용이하게 됨에 따라, 스마트 단말이 보안적 측면에서 취약하게 되었다. 본 논문에서는 TEE(Trusted Execution Environment) 기반의 격리된 안전실행환경 영역을 가지는 모바일 단말 플랫폼인 가상화 기반 스마트 단말 보안 기술의 특징을 알아본다. 또한, 본 논문에서는 스마트 단말에서 실행되는 응용프로그램을 위한 도메인 분리 기반의 안전한 스마트 단말 보안 플랫폼에 대한 구현 방법을 제안한다.

■ 중심어 : 스마트 단말 보안; 가상화; 도메인 분리; 안전실행환경(TEE); 신뢰 군사 영역(TMZ)

Abstract

Recently, important information related with smart work such as office and video conference are handled in smart device quite a lot compare with before. Also, execution environment of smart devices is getting developed as open software environment. It brought convenience to download and use any kind of application software. By that, security side of smart devices became vulnerable. This paper will discuss characteristics of smart device security technology based on virtualization that is a mobile device platform with isolated secure execution area based on TEE (Trusted Execution Environment). Also, this paper will suggest an implementation method about safe smart device security platform based on domain separation for application software which can be executed in smart devices.

■ keywords : Smart Device Security ; Virtualization ; Domain Seperation; Trusted Execution Environment; Trusted Military Zone;

Ⅰ. 서 론

스마트 단말의 보급이 급격하게 증가하고 있는 현실에서 모바일 환경에 대한 개인정보 침해, 모바일 악성코드 등 새로운 모바일 위협의 확대가 예상되고 있다. 특히, 스마트폰 등 모바일 장치에서 실행되는 웜, 바이러스는 모바일 장치의 성능저하, 모바일 사용자의 개인 정보 불법 수집, 다른 서비스로의 바이러스 전파 등을 야기할 수 있어 이에 대한 대비가 무엇보다 중요하다. 또한, 모바일 장치의 도난/분실 시 모바일의 복제, 모바일 장치 내부에 저장된 정보의 유출에 대한 우려가 제기되고 있다. 뿐만 아니라, 개방형 모바일 플랫폼에 대한 시장 선호도가 높아짐에 따라 안드로이드와 같이 모바일 장치의 개방형 플랫폼이 주요 해킹의 표적이 될 가능성이 많아지고 있다. 이와 같이, 스마트 단말에 대한 개방형 플랫폼을 중심으로 하는 서비스 확대와 함께 보안 위협의 증대는 Anti-Virus 와 같은 기존 소프트

* 종신회원, 한국전자통신연구원, 모바일보안연구실

이 논문은 MSIP(미래창조과학부)의 IT R&D 프로그램의 지원을 받아 작성되었습니다.[10043959, 모바일 단말의 비인가 접근 차단 및 안전한 운영환경 보장을 위한 EAL 4급 군사용 융합 보안 솔루션 개발]

접수일자 : 2016년 10월 12일 게재확정일 : 2016년 12월 27일

수정일자 : 1차 2016년 12월 21일, 2차 2016년 12월 26일

교신저자 : 김정녀 e-mail : jnkim@etri.re.kr

웨어 기반 솔루션으로는 대응에 한계가 있으며, 모바일 백신, MDM 등과 같은 응용서비스 수준의 보안 대책으로는 사용자가 모르는 상태에서 스마트 단말이 루팅되어 내부의 중요한 정보가 유출되는 등의 피해에 대해서는 방지를 할 수가 없다. 특히, 국내 스마트 단말 보안 기술은 안티 바이러스, 방화벽 기능, 디바이스 잠금 기능 등과 같은 어플리케이션 수준의

단품형 기술로 구성되어 있으며, 비교적 초기 단계의 기술이라고 할 수 있다.[1] TCG (Trusted Computing Group)에서 모바일 환경에 적합한 하드웨어 보안 모듈인 MTM을 발표하였다. MTM은 모바일 단말에 장착되어 단말 자체에 대한 플랫폼 무결성 검증 기능은 물론 차폐영역과 보호능력 및 안전한 키 관리 체계, 물리적인 안전성 등 다양한 보안기능을 제공하기 때문에 단말 플랫폼의 무결성 검증 및 단말내부에서 사용되는 파일들을 안전하게 처리하고 관리해 줄 수 있는 환경을 제공한다[3][4]. 스마트 단말의 저전력, 저용량, 멀티미디어 서비스, 실행환경 등의 특성을 고려하여, 위에서 언급한 다양한 보안 위협으로부터 개방형 플랫폼 환경의 스마트 단말을 보호하기 위한 시스템 수준의 보안 플랫폼 기술 개발이 최우선적으로 요구되고 있다.

모바일 단말 기능과 성능의 눈부신 발전으로 인해, 모바일 단말 기반의 다양한 신규 서비스가 증가하고 있으며, 이와 더불어 사용자의 모바일 단말 의존도는 점점 높아지고 있다. 증가하는 신규 서비스는 삶의 편의성을 제공함과 동시에 다양한 보안위협을 초래하고 있어, 보안 위협과 악의적인 공격에 대비할 수 있는 보안 플랫폼의 개발이 필요하다[5]. 보안 플랫폼 구조는 일반적인 모바일 운영체제(예, 안드로이드 OS)와 응용들로부터 분리된 신뢰된 실행 환경을 의미하는 Global Platform의 TEE(Trusted Execution Environment)가 대표적이다[6]. TEE는 안드로이드와 같은 일반적인 운영체제보다 높은 수준의 보안을 제공하는 운영 환경을 제공하여, 하드웨어 기반의 SE(Secure Elements)를 장착하지 않더라고 저비용으로 높은 보안 수준을 제공할 수 있는 방법을 제공한다. TEE 구조에서 일반적인 모바일 운영체제 영역의 응용이 TEE의 보안 서비스(암호 및 안전저장 등)을 이용하기 위해서는 TEE에서 정의한 API를 통해서만 이용이 가능하지만, API가 오픈되어 있기 때문에 악의적인 목적의 앱이 TEE API를 통해 TEE 영역으로 침범할 가능성이 존재한다.

본 논문에서는 TEE 기반의 격리된 안전실행영역을 가지는 모바일 보안 단말 구조와 스마트 단말에 대하여 플랫폼 수준의 보안 기능을 제공하는 가상화 기반의 스마트 단말 보안 기술의 구현에 대해 알아본다.

Ⅱ. 관련 연구

본 논문과 유사한 운영환경 분리를 위한 기존의 기술은 ARM의 TrustZone, Cellrox의 ThinVisor, Fraunhofer의 BizzTrust 등이 있다. ARM의 TrustZone은 HW 기반의 실행 도메인을 분리하는 기능을 제공하며 실제적으로는 HW 기반의 구조 확장이다. TrustZone 자체는 실행 도메인 분리 기능만을 제공하고 분리된 영역에서 운영하는 보안 모듈은 별도로 제공되어 분리된 영역의 이용 가능 자원이 한정적이다. 무엇보다 ARM 사의 프로세서에 내장된 기술로 특정 벤더 및 특정 프로세서 기반의 기술에 종속이 된다. Cellrox의 ThinVisor는 OS 상위 계층의 가상화로 응용 수준의 영역을 분리하여 가상화된 시스템 자원을 제공하여, 영역 간의 보안성을 제공하고 있다. 응용 수준 영역의 분리 기능에 충실하고 각 영역 간 완전한 격리를 통해 한 영역의 보안 취약점이 다른 영역에 영향을 주지 않는 구조이다. 특히 영역 간 분리로 서로 다른 영역에 영향을 주지는 않지만 각각의 영역이 동작하는 운영 환경은 공유하고 있으므로 각각의 영역이 같은 보안취약점을 가질 수 있다. Fraunhofer의 BizzTrust는 커널 내 접근제어 구조를 수정하여 업무용 앱과 개인용 앱을 구분하는 논리적인 앱 수행 영역을 분리하는 구조이다. 업무용 앱은 앱 설치시 회사의 인증서를 통한 인증을 통해 구분되고, 앱에 업무용앱 식별자를 부여하여 커널 내부에서 업무용 앱과 개인용 앱이 다루는 데이터의 접근을 강제적으로 제어한다. 업무용 앱과 개인용 앱이 접근제어에 의해 논리적으로 분리되어 운영되지만 동일한 OS 영역에서 동작하므로, OS 보안취약점으로 인해 개인용 앱에 의한 업무용 데이터의 침범 가능성이 항상 존재한다. 이와 같이 기존의 정보 유출 방지를 위한 모바일 단말 기술은 주로 업무용으로 스마트 단말을 사용할 때 기업 데이터의 유출 방지를 위해 업무 영역과 개인 영역을 분리하는 기술이 주를 이루어 있다. 운영 환경 영역 분리를 통한 보안 구조는 업무 영역이 좀 더 보안 사고에 노출될 가능성이 적지만, 개인 영역과 동일한 OS 환경을 가지므로 OS에 대한 보안 취약점에 항상 잠재적인 위협을 가지고 있다고 할 수 있다.

Ⅲ. 스마트 단말 보안 위협

스마트 단말에서의 보안 위협은 크게 네 가지로 나눌 수 있다. 첫째는 개방형 플랫폼으로 보안 취약점 노출위협이 증대되고, 두 번째는 앱스토어를 통한 애플리케이션 유통에 따라 악의적인 바이러스 제작 및 유포 기회가 확대되고 있으며, 세 번째는 다양한 네트워크 접속환경을 지원하고 있어 감염경로의 다양성을 제공하며, 마지막으로 이동 편의성 및 모바일 오피스 지원에 의해 개인 및 기업 정보 유출 위협이 증대한다는 것이다.

그 피해 또한 악성코드 감염, 기업/개인정보 유출, 서비스

거부 공격, 금융사고 등으로 이어지고 있다. 전 세계 모바일 악성코드 감염경로 비율을 보아도 블루투스 67.1%, MMS(24.4%), 외부저장장치 (3.7%), PC플러그인 (2.4%), 인터넷 다운로드(2.4%) 등으로 이루어진다. 이러한 다양한 보안 위협으로부터 스마트 단말을 보호하기 위해 플랫폼 보안 기술이 필요하다. 본 보안 플랫폼을 위하여 자체 개발한 하이퍼바이저인 ViMo를 기반으로 일반 도메인과 안전 도메인으로 분리하기 위하여 안드로이드 운영체제와 실시간 운영체제 기반의 보안 운영체제를 분석하였다. 또한 이를 위하여 보안 API를 제공하기 위하여 ARM에서 제공하는 TrustZone API와 Global Platform이라는 업체 컨소시엄에서 제공하는 TEE(Trusted Execution Environment) API를 분석하여 본 보안 플랫폼에 알맞은 보안 API를 정의하였다.

그림 1. 스마트 단말 보안 위협

이 필요하다.

IV. 가상화 기반 스마트 단말 보안기술 구현

1. 분석

본 논문은 다양한 용도로 활용되는 스마트 단말의 운영환경을 분리하여, 보안을 필요로 하는 서비스의 처리를 일반 운영영역과 분리된 보안 영역에서 실행하도록 하여, 철저한 보안이 요구되는 군사용 환경에서 사용이 가능한 CC EAL* 4급의 보안 등급을 보증하는 스마트 단말 기반 융합 보안 기술이다. 본 보안 플랫폼에서 제공하는 암호 알고리즘은 KCMVP** Level 1 인증을 준수하여 암호 모듈의 안전성과 호환성을 제공한다.

본 연구의 최종 결과물은 운영환경을 분리하는 가상화 플랫폼 기술과 EAL 4급의 보안 등급을 보증하는 가상화 기반의 보안 플랫폼 기술과 일반 영역의 서비스로부터 보안 플랫폼의 보안 기능을 안전하게 접근할 수 있도록 하는 보안 API 기술 등으로 이루어진다. 이를 위하여서는 일반 영역과 보안 영역을 분리하여 실행 할 수 있는 가상화 기능을 제공하는 하이퍼바이저

본 논문은 TEE 기반의 안전실행영역 구조를 가지는 모바일 보안 플랫폼으로 개발된 TeeMo를 기반으로 설계되었다[7][8]. TeeMo는 가상화 기술을 기반으로 안드로이드 영역과 안전실행영역을 가지며, 안드로이드 영역의 응용이 안전실행영역의 서비스를 이용할 때는 자체 정의된 보안 API를 통해 접근한다.

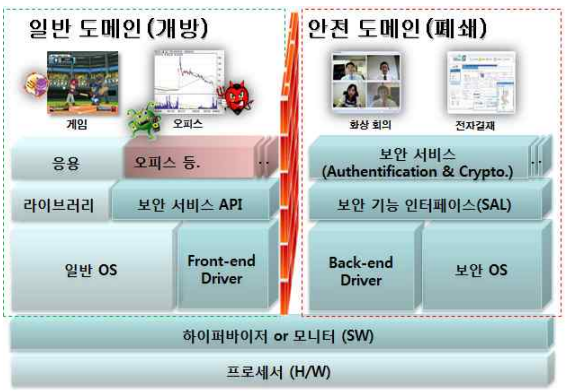

그림 2. 본 논문에서 제안하는 가상화 기반의 모바일 보안 실행환경

* CC EAL : Common Criteria Evaluation Assurance Level

** KCMVP : Korea Cryptographic Module Validation Program

2. 설계

본 논문에서는 그림 2 와 같이 모바일 장치에서의 중요한 정보를 보호할 수 있는 TEE 기반의 안전한 실행환경을 제안한다. 이 모바일 장치용 안전 실행환경은 모바일에서 실행되는 응용프로그램을 위한 TEE 기반의 다양한 보안 기능을 제공할 수 있다.

가. 도메인 분리 가상화 플랫폼 핵심 모듈 SW

먼저 가상화 하이퍼바이저 상에서 두 개의 분리된 영역을 제공하기 위한 핵심 모듈 SW를 설계하였다. 두 가지 기능으로 첫 번째는 다중 도메인용 메시지 처리 및 관리 모듈을 설계하였다. 이는 영역 간 데이터 전송을 위한 메시지를 생성하고 관리하는 기능 제공하며 다중 앱의 보안 서비스 이용을 위하여 멀티채널 및 동시 접속 기능을 제공한다. 일반 영역에서 필요한 보안 영역의 서비스를 사용하기 위해 전송할 데이터 및 보안 프로시저를 호출하기 위한 메시리를 처리하고 관리하는 기능을 담당한다. 두 번째는 다중 도메인용 프로세스 간 통신 모듈을 설계하였다. 다중 도메인 간 통신을 위한 일반 영역 및 보안 영역의 통신 드라이버를 제공하며 설정된 통신 채널을 활용하여 보안 세션 및 보안 서비스 호출이 가능한 데이터 송수신 기능을 제공한다.

나. 가상화 기반 보안 플랫폼 핵심 모듈 SW

본 모듈은 크게 세 가지로 비인가 접근차단 모듈, 다중 도메인 기반 인증 서비스 모듈, 안전저장장치 모듈로 나누어 설계되었다.

비인가 접근차단 모듈은 일반영역의 앱이 보안영역의 보안서비스를 요청할 때, 허가된 앱인지 확인하는 보안영역의 접근 차단 기능을 제공하며 접근판단 및 제어기능과 보안 정책관리 기능으로 나누어 설계되었다. 이를 위해 보안 정책 DB를 설계하여 보안 영역으로의 접근을 허용하는 앱을 관리하는 DB로 사용하였다. 다중 도메인 기반 인증 서비스 모듈은 단말 및 앱을 사용하는 사용자를 인증하는 것으로 사용자가 미리 설정한 PIN 번호를 통해 사용자 인증 기능을 수행하도록 설계되었다. 게이트 앱을 통해 군사용 보안 서비스에 접근 시 한번의 PIN 인증이 이루어지며 일정 Idle Time이 지나면 재인증하도록 설계되었다. 안전저장장치 모듈은 시스템 또는 서비스에 사용되는 중요 데이터를 보안영역에서 안전하게 저장 및 관리하기 위해 보안 파일시스템을 제공하도록 설계하였다. 대용량 파일 처리가 가능한 임베디드 OS위에서 수행되는 경량화된 보안 파일 시스템으로 앱별 파일 관리를 통해 앱별 파일 공유 및 파일 검색 시간을 최소화할 수 있도록 설계되었다. 안전저장장치 모듈의 기능은 파일 시스템에 대한 암호화 및 무결성 검증 기능과 파일 시스템 메타데이터에 대한 암호화 및 무결성 검증 기능을 제공한다.

다. 핵심 모듈용 보안 API

본 보안API는 일반 영역의 보안서비스들이 보안 영역의 보안 요소들을 접근하기 위한 보안 서비스API를 제공하며 보안 영역의 보안 기능을 이용할 수 있도록 보안 기능을 추상화하여 제공하는 보안API 추상화 모듈을 제공한다.

보안 API는 다섯 가지로 분류하여 설계하였다. 첫 번째는 채널 관리 API로 일반 영역과 보안 영역 사이의 채널을 생성하고 종료하는 API이며, 두 번째는 세션 관리 API로 PIN을 이용한 사용자 인증을 수행하여 일반 영역과 보안 영역 사이의 인증된 세션을 생성하거나 인증된 세션을 종료하기 위한 API이다. 세 번째는 파일 관리 API로 보안 영역의 파일시스템에 파일을 암호화하여 저장/수정/삭제하고 암호화된 파일을 검색하는 등 파일을 관리하는 API이며, 네 번째는 접근제어 API로 사용자의 보안 영역 접근 시 PIN 인증을 통해 접근제어를 하기 위해 필요한 API이고, 마지막으로 서명 관리 API는 서비스 레벨의 사용자 인증을 위해 PKI기반의 인증 메커니즘에 따라 FIPS-196을 준수하여 서명 관련 기능을 수행하는 API이다.

라. 군사용 보안 서비스 앱

본 보안 서비스 앱은 안전한 보안 서비스에 접근 가능하도록 하는 게이트 앱인 TMZ(Trusted Military Zone)를 제공한다. 군사용으로 사용하기 위해서는 서비스가 안전하여야 하므로 게이트 앱을 통하여 실행되도록 하였다. TMZ를 통하여 제공되는 서비스는 인증관리, 주소록, 카메라, 사진, 문자, 상황전파 등의 앱을 설계하였다. 사용자와 응용을 통한 2 단계 인증을 위한 보안 서비스를 제공하고 사용자 인증 후 일정 Idle Time이 지나면 타임아웃 되어 사용자에게 PIN 재인증을 요구하도록 설계하였다.

그림 3. TMZ 스크린샷

3. 구현

본 논문의 구현을 위하여 플랫폼은 갤럭시 S3 상용단말을 선정하였고, ViMo 하이퍼바이저를 설치하여 그 위에 안드로이드와 보안 운영체제를 구현하였다.

먼저 가상화 플랫폼 핵심 모듈을 구현하였는데, 먼저 다중 도메인 간 통신을 위한 일반 영역 및 보안 영역의 통신 드라이버를 구현하고, 설정된 통신 채널을 활용하여 보안 세션 및 보안 서비스 호출이 가능한 데이터 송수신 기능을 구현하였다. 이렇게 구현한 모듈을 검증하기 위해 메시지 송수신 처리에 대한 성능을 측정하였다. 일반영역에서 2MB크기의 대용량 메시지 송수신 처리 시간을 측정하였더니 10회 수행시 평균 3초로 측정되었다.

가상화 기반 보안 플랫폼 핵심 모듈은 먼저 비인가 접근차단 모듈을 구현하였다. 다중 도메인 간 통신을 위한 일반 영역 및 보안 영역의 보안 서비스를 요청할 때, 허가된 앱인지를 확인하여 보안 영역에 대한 접근을 차단하는 기능을 구현하였다. PIN 번호 입력시 번호가 정렬된 일반 키패드가 아닌 아래와 같이 여러 번호가 섞인 보안 키패드로 구현하였다. 안전저장장치 모듈은 보안영역 내에서 보안 파일시스템 관련 총 10가지 기능 시험을 수행하였다. 보안 파일시스템 초기화, 포맷 및 사용정보 기능 시험, 파일 쓰기, 읽기, 지우기, 리스트 및 관리 기능 시험, 메모리 단편화율 및 메모리 정리 기능 시험 등을 수행하였다.

보안 API는 핵심 보안 API와 군사용 서비스 앱으로 나누어서 구현하였다. 보안 API는 5가지 API를 구현하여서 기능시험을 마쳤다. 그중 인증 서비스는 FIPS-196 준수를 위하여 공개키/개인키 쌍에 대한 바인딩 검증과 난수를 이용한 전자서명 검증 등의 인증 항목을 구현하였고 공개키 암호화를 이용한 엔티티 인증은 단 방향 인증과 양방향 인증 중의 하나를 만족하면 되어서 인증서를 통한 양방향 인증을 구현하였다. 군사용 보안 서비스 앱은 게이트앱과 내부 6개의 앱을 구현하였는데, 특히 군요구에 의해 구현된 상황전파앱이 많이 사용될 예정이다. 상황전파 서비스는 긴급 상황이 발생하였을 때 카메라 앱과 사진 앱 기능과 함께 문자로 상황을 전파 할 수 있는 서비스로 별도의 군사용 상황전파 서버를 구축하여 상황전파 앱을 실행 시킬 때마다 상황전파 서버와 FIPS-196 기반의 양방향 인증을 수행하게 된다. 상황전파 시 카메라 앱 기능을 통해 사진을 첨부할 수 있으며 첨부된 사진에는 사진 촬영 시점의 GPS정보와 Time 정보, 사진 전송 시점의 GPS 정보와 Time 정보가 포함되어 군사용 상황 전파 서버에 전송이 되며 상황전파 서버는 상황전파 문자가 도착하면 수신자 그룹에 포함된 군 관계자들의 단말에 상황전파 문자를 전송한다. 상황전파 서버는 수신된 GPS정보를 지도와 매핑하여 수신자 및 사진의 위치를 인지하는데 용이하며 송신자의 이동경로를 쉽게 파악할 수 있다.

그림 4. 상황발생 스크린샷

4. 테스팅

대부분의 모바일 악성코드는 SMS 메시지나 이메일을 보내는 것으로 감염된다. 모바일 악성코드는 보통 정상적인 앱처럼 가장하여 사용자의 스마트 단말에 다운로드 되고 설치된다. 공격자는 앱에 악성코드를 삽입하여, 악성앱이 성공적으로 설치되고 실행된다. 악성코드는 SMS 메시지, 주소록, 그림, 인증서 등과 같은 스마트 단말내의 민감 데이터를 수집해서 가져간다. 특별히 인증서는 국내에서 모바일 뱅킹이나 지불에 널리 쓰이는 가장 중요하고 민감한 데이터이다. 본 기술은 모바일 악성코드에 감염이 되더라도 스마트 단말로 부터의 정보 유출을 방지한다. 탐지한다. 모든 보안 서비스는 게이트앱인 TMZ를 통해서만 접근이 가능하며 실행이 된다. 특히 TM 문자, TM 주소록, TM 인증 관리를 통해 안전한 군용 문

그림 5. 도메인 분리 기반 모바일 보안 플랫폼 프로토타입

자/상황 전파 응용서비스를 제공한다. 이를 통해 문자, 주소록, 공인인증서 등의 정보 유출을 방지한다.

그림 5는 도메인 분리 기반 스마트 단말 보안 플랫폼의 프로토타입을 보여 준다. 본 플랫폼은 상용 스마트 단말에 설치된 하이퍼바이저, 가상화 플랫폼, 암호 SW를 포함한 가상화 기반 보안 플랫폼, 보안 API를 포함한다.

그림 6는 스미싱 기법을 이용하여 악성 코드를 배포하고 실행하여 스마트 단말의 보안 취약성을 확인하는 과정을 보여준다. 먼저 일반적인 스마트 단말을 사용하는 사용자가 스미싱에 의해 악성코드가 있는 ①SMS 링크를 클릭하게 되면 해커에 의해 ②앱이 배포되고 설치되어 ③악성코드가 동작하게 되고 이에 따라 ④단말에 있는 인증서, 사진, 주소록, 메일 등의 주요정보가 유출되게 된다. 그러나 도메인 분리 기반 스마트 단말 보안 플랫폼이 설치된 군사용 보안 단말은 이러한 ①,②, ③ 과정을 다 거치더라도 인증서, 사진, 주소록, 메일 등의 주요정보가 보안 영역에 있어서 정보를 가지고 갈 수 없음을 알 수 있다.

만 각각의 영역이 동작하는 운영 환경을 공유하고 있으므로 각각의 영역이 같은 보안 취약점을 가질 수 있다. Fraunhofer의 BizzTrust는 업무용 앱과 개인용 앱이 접근제어에 의해 논리적으로 분리되어 운영되지만 동일한 OS영역에서 동작하므로, OS 보안 취약점으로 인해 개인용 앱에 의한 업무용 데이터의 침범 가능성이 항상 존재한다. 그러므로 기존의 이 모든 솔루션 들은 도메인을 분리하지 않은 기존 운영체제 환경과 같이 그림 6의 악성 코드 배포 시험에서 모두 악성코드에 감염되어서 개인 정보가 유출될 수 있는 위험성이 존재한다.

마지막으로 모바일 백신의 경우에는 SW기반의 보안 솔루션으로, 접근 허용된 시스템 라이브러리의 변경을 탐지할 수 없다. 또한 모바일 백신은 알려지지 않은 악성코드 패턴이 DB에 존재하지 않기 때문에 새로운 모바일 악성코드를 탐지 할 수 없다. 그런 반면 본 기술을 통해 모바일 백신의 한계점을 극복이 가능하다.

그림 6. 스미싱 기법에 의한 악성코드 배포 및 실행 과정

모바일 악성코드가 스마트 단말의 보통 영역에서 실행이 되어서 스마트 단말 내에 있는 정보를 탈취해 가려고 하더라도 군사용으로 사용되는 중요한 정보들이 안전 도메인에 저장되어 있어서 아무것도 없는 것으로 알고 있다.

기존 기술인 ARM의 TrustZone의 경우는 분리된 영역의 이용 가능 자원이 한정적이어서 본 논문의 운영환경의 안전성 보장 기능을 제공하기 어려우며, Cellrox의 ThinVisor의 경우에는 영역간의 분리로 서로 다른 영역에 영향을 주지는 않지

V. 결 론

본 논문에서는 스마트 단말에서 필요로 하는 도메인 분리 기반의 단말 보안 플랫폼 기술들에 대해 알아보았다. 또한, 기존의 하드웨어기반 보안 기술이 모바일 장치에 대한 신뢰의 근원 기능만을 제공한 반면, 본 논문에서 제시하는 도메인 분리 기반 스마트 단말 보안 플랫폼은 모바일 장치에서 실행되는 응용프로그램이 필요로 하는 다양한 보안 기능을 제공할

수 있다. 본 도메인 분리 기반 스마트 단말 보안 플랫폼 기술은 단말내의 민감 정보 유출과 비인가 접근을 차단한다. 본 논문은 분리된 보안 영역의 보안 플랫폼을 통해 개인 정보 및 중요 정보의 비인가 접근을 차단하고 정보 유출 기능을 제공할 수 있어 보안이 철저히 요구되는 군 내부에서 작전용이나 지휘체계용으로 활용할 수 있는 기반 기술이 될 것으로 기대된다. 또한, 군사용 뿐만 아니라 민간에서 사용될 경우 스마트 단말의 보안이 보장되어야 가능한 다양한 모바일 단말 기반 보안 서비스의 신뢰 단말 기술로 활용이 가능함(금융 보안 단말, 원격 관리 단말 등). 단, 군사용으로 사용될 때 적용된 암호알고리즘 및 보안 API 등 본 기술 결과물에 대한 보안 기능에 대해 민간용으로 이전 가능한 기술에 대한 범위는 과제 및 국방 관련 관계자와 협의를 거쳐 진행할 예정임

또한 이 기술은 스마트 단말뿐만 아니라 인터넷 상의 다양한 IoT 기기를 포함한 다양한 분야에서 악성코드의 실행과 전파를 막을 수 있는 솔루션이 될 것이다. 다양하고 새로운 IoT 서비스가 등장하면서 여러 가지 사양과 특성을 갖는 수많은 기기 간의 연결과 통신의 증가가 예상되고 있다. 이러한 IoT 서비스 환경의 특성으로 인해 발생 가능한 다양한 보안 위협에 대응하기 위해 안전한 서비스 환경 구축 및 서비스의 보안성 강화는 반드시 수반되어야 한다. 향후, 보안 하드웨어와 연동이 가능한 IoT 기기와 게이트웨이 보안 기술과, 도메인 분리 기술인 하이퍼바이저를 활용하여 다양한 IoT 기기에 적용하여 신뢰성과 보안성을 확보하는 방안에 대한 연구를 진행할 예정이다.

References

[1] Mobey Forum Mobile Financial Services, “ Alternatives for Banks to offer Secure Mobile Payments version 1.0,” Aug. 2010.

[2] TCG mobile reference architecture specification version 1.0,(https://www.trustedcomputinggroup.org)

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

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

[5] Bickford J., O’Hare R, Baliga A, Ganapathy V, and Iftode L, “Rootkits on Smart Phones: Attacks, Implications and Opportunities,” *Workshop on Mobile Computing Sys. and Appl. (HotMobile'10). ACM*, Feb. 2010.

[6] Global Platform Device Technology, “The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market,” Global Platform White Paper, Feb. 2011.

[7] Y.H. Kim, Y.G. Lee, and J.N. Kim, "TeeMo: A Generic Trusted Execution Framework for Mobile Devices," *Proc. of International Conference on Computer, Networks, Systems, and Industrial Applications (CNSI)*, pp. 579-583, Jul. 2012.

[8] Y.H. Kim, J.N. Kim, “Building Secure Execution Environment for Mobile Platform,” *Proc. of First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering*, pp. 119-122, 2011

[9] H.I. Joo, S.G. Choi, and S.I. Jeon, “Secure Booting using TPM on Mobile Platform”, NCS2006, Dec. 2006.

[10] M.S. Kim, J.A. Shin, Y.S. Park, and S.I. Jeon, “Common Security Core Module for Mobile Platform,” KIISC, vol.16, no 3, Jun. 2006..

[11] H. Chai, Z. Lu, Q. Meng, J. Wang, X. Zhang, Z. Zhang, “TEEI-A Mobile Security Infrastructure for TEE Integration, ” *Proc. of IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 914-920, 2014.

[12] M. Kim, H. Ju, Y. Kim, J. Park, Y. Park, “Design and implementation of mobile trusted module for trusted mobile computing,” IEEE Transactions on Consumer Electronics, Vol. 56, No. 8, pp. 134-140, 2010.

[13] K.H. Baek, “ Trend of Research and Technology for SEE,” Electronics and Telecommunications Trends, Vol 22, No 5, 2007.10.

[14] D. Oh, I. Kim, K. Kim, S. Lee, and W. Ro, ”Highly Secure Mobile Devices Assisted with Trusted Cloud Computing Environments” ETRI Journal, vol. 37, no. 2, pp. 348-358, Apr. 2015.

[15] M. L. Polla, F. Martinelli, and D. Sgandurra, “A Survey on Security for Mobile Devices,” IEEE Communications surveys & tutorials, vol. 15, no. 1, pp. 446-471, Mar. 2013.

[16] W. Arthur and D. Challener, A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security, Apress, 2015.

저 자 소 개

김정녀(종신회원)

1987년 전남대학교 전산통계학과 학사 졸업.
1996년 OSF/RI 공동연구 파견(미국)
2000년 충남대학교 컴퓨터공학과 석사 졸업.
2004년 충남대학교 컴퓨터공학과 박사 졸업.
2005년 Univ. of California, Irvine Post-Doc.
1988년~현재 한국전자통신연구원 책임연구원
현재 과학기술연합대학원대학교(UST) 정보보호공학과 교수
<주관심분야 : IoT보안, 모바일 보안, 시스템·네트워크 보안, 보안 OS>