The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 6, pp.1-9, Dec. 31, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.6.1
JIIBC 2015-6-1

모바일 가상화 TYPE-I을 이용한 보안 기술 연구

A Study on Security Technology using Mobile Virtualization TYPE-I

강용호*, 장창복*, 김주만**

Yong-Ho Kang*, Chang-Bok Jang*, Joo-Man Kim**

요 약 최근 스마트 장치 확산과 이러한 장치들을 이용한 다양한 서비스들의 도입으로 모바일 보안 및 스마트 TV 보안에 대한 관심이 증가하고 있다. 스마트폰 사용자들은 클라우드 서비스, 게임, 뱅킹 서비스, 모바일 서비스 등의 다양한 서비스를 사용한다. 하지만 현재의 모바일 보안 솔루션과 스마트 TV 보안은 단순히 악성코드를 탐지하거나 모바일 단말 관리, 자체 보안 시스템을 이용하는 수준에 머무르고 있다. 이에 인증서, 법인 문서, 개인의 신용 카드 번호와 같은 보안에 민감한 정보에 대해 서비스 해킹 및 누설을 방지하는 기술이 필요하다. 이러한 문제를 해결하기 위해서 모바일 가상화, ARM TrustZone, GlobalPlatform, MDM과 같은 다양한 모바일 장치의 보안 기술이 연구되었다. 따라서 본 논문에서는 가상화 TYPE-I 기반의 ARM TrustZone 기술을 이용한 효율적 보안 기술 구현 방법을 제시한다.

Abstract Recently, with smart device proliferation and providing the various services using this, they have interested in mobile and Smart TV security. Smartphone users are enjoying various service, such as cloud, game, banking. But today's mobile security solutions and Study of Smart TV Security simply stays at the level of malicious code detection, mobile device management, security system itself. Accordingly, there is a need for technology for preventing hacking and leakage of sensitive information, such as certificates, legal documents, individual credit card number. To solve this problem, a variety of security technologies(mobile virtualization, ARM TrustZone, GlobalPlatform, MDM) in mobile devices have been studied. In this paper, we propose an efficient method to implement security technology based on TYPE-I virtualization using ARM TrustZone technology.

Key Words : Mobile Security, Smartwork, Mobile Virtualization

Ⅰ. 서 론

최근 기업들이 스마트폰과 태블릿 PC 등 모바일 장치를 업무에 직접 활용하기 시작하면서 스마트 장치 보안의 관심이 증가되고 있다. 특히 모바일 악성 어플리케이션이 크게 증가하고 있으며, 이러한 위협이 기업으로까지 번지고 있다. 스마트폰에는 다양한 개인정보가 저장되어 있기 때문에 이를 관리하는 것은 중요하며, 더불어 개인정보 및 기타 주요 정보를 안전한 저장 공간을 확보하여 저장하고 이를 암호화하여 저장함으로써 보호해야할 필요가 있으며, 이 저장 매체에 접근 시 접근권한을 설정하고 각종 인증 및 개인정보를 안전하고 손쉽

*정회원, (주)알투소프트
**정회원, 부산대학교 IT응용공학과(교신저자)
접수일자: 2015년 10월 8일, 수정완료: 2015년 11월 7일
게재확정일자: 2015년 12월 11일

Received: 8 October, 2015 / Revised: 7 November, 2015 / Accepted: 11 December, 2015
**Corresponding Author: joomkim@pusan.ac.kr
Dept. of Applied IT Engineering, Pusan National University, Korea

게 관리하는 시스템이 요구된다. 이러한 위협에 대응하고자 사내에 불법으로 설치된 액세스 포인트(AP)를 비롯해 외부에서 접근할 수 없도록 통제할 수 있는 무선 침입방지시스템(WIPS), 무선네트워크접근관리(WNAC) 솔루션이 개발되었다. WIPS, WNAC 등의 무선보안 솔루션을 구축한 기관에서는 외부로부터 들어오는 무선 침입을 방지하기 위해 공개 액세스 포인트를 모두 제거하여, 외부 침입을 원천적으로 막을 수 있는 장점이 있지만, WIPS, WNAC 등이 구축되지 않은 곳에서 모바일 기기를 통해 모바일 오피스를 사용할 경우 중요 데이터의 유출을 방지할 수 없는 문제점이 존재한다[1-3]. 이러한 모바일 오피스 단말에 대한 관리·보안의 필요성이 요구됨에 따라 모바일단말관리(MDM) 솔루션이 개발되었으며, MDM (Mobile Device Management) 솔루션이란 OTA(휴대폰무선전송기술, Over The Air)를 이용하여 언제 어디서나 원격으로 모바일 단말기를 관리할 수 있는 시스템을 의미한다. 모바일 디바이스 관리 및 관련 정보 수집, 분실/도난 시 추적관리, 보안 정책 적용을 위한 사용 제한, 소프트웨어 패치 배포 등을 총괄하는 통합 솔루션이다. 만일 MDM 솔루션이 탑재되지 않은 스마트폰의 경우, 분실했을 때 사내 데이터가 외부로 유출될 가능성이 있지만 MDM 솔루션이 적용된 스마트폰의 경우 바로 공장 초기화시켜 데이터를 전부 삭제할 수 있으며, 많은 업무 영역이 기존의 PC 환경이 아닌 모바일 기기를 통해서도 가능해짐에 따라, 회사 내에서만 유통되던 문서가 이제는 회사 외부로 자유롭게 유통될 수 있어 기기 자체에 대한 보안도 중요하지만 기기를 통해 활용되고 유통되는 콘텐츠 자체를 보호하는 것이 매우 중요하다. 하지만, MDM 솔루션의 경우 근본적으로 중요데이터를 암호화하거나 패스워드를 설정한다고 해도 암호화된 데이터와 패스워드 정보를 외부로 유출하지 못하게 하는 방법을 제공하지 못한다. 따라서, 언제든지 중요 데이터가 외부로 유출될 수 있는 위험이 존재하는 문제점을 가지고 있다. 따라서, 기존의 보안 문제를 해결하기 위한 다양한 연구들이 이루어지고 있으며, 특히 최근에는 가상화 기술을 이용한 보안 연구가 이루어지고 있다.

II. 관련연구

1. 가상화 기술 연구

모바일 가상화 기술은 임베디드 시스템에서 사용되어져 왔다. 이 기술은 가상 머신 모니터(VMM, virtual machine monitor) 또는 하이퍼바이저라고 불리우는 작은 소프트웨어 추상 계층이라고 할 수 있다[1][2][6][7]. 일반적인 플랫폼은 하드웨어, 운영체제, 그리고 사용자 어플리케이션과 같은 수직적 계층 구조를 갖지만, 하이퍼바이저는 단일 디바이스에 다양한 디바이스들이 존재하는 것처럼 보이게 할 수 있다. 그러므로 서로 다른 운영체제가 독립적 및 동시적으로 동작할 수 있다. 이러한 가상화 기술을 이용하는 주요 목적은 단일 장치에서 하드웨어의 사용률을 극대화 시키는데 있었다[1][2].

일반적으로, 이러한 영역은 각각 독립되어 있으며, 서로 간의 접근이 허락되지 않는다. 이러한 독립된 영역은 소프트웨어의 신뢰성과 보안성을 제공할 수 있다. 이러한 이유로 가상화 기술을 이용한 보안 기술들이 활발하게 연구되고 있다[1][2][4][5][14][16].

2. 모바일 보안 기술

최근 모바일 가상화 기술이 시스템의 보안성과 신뢰성을 강화할 목적으로 연구가 이루어지고 있다[1][2][11][12]. 몇몇 연구들은 악성코드를 분석하거나 해킹으로부터 모바일 장치를 보호하기 위한 효율적 가상화 방법을 제안하고 있다[9][10][16].

최근에는 어플리케이션 프로세서와는 별도로 하드웨어에서, 엄격한 보안 정책을 제공하는 근거리 무선 통신(NFC)을 사용하는 연구가 이루어지고 있다. 이러한 기술은 보안 기능이 전용 USIM 카드 내에 존재하여 모바일 결제, 은행 등의 서비스에서 높은 수준의 보안 환경을 제공한다. 그러나, 모바일 장치의 자원과 전원은 다양한 서비스를 처리하기에 한계를 갖는다는 문제점을 가지고 있다[12][15]. 데스크톱 또는 서버 컴퓨팅 상에 기존의 신뢰할 수 있는 컴퓨팅 플랫폼들은 보안 코프로세서를 사용하거나 암호화 프로세서를 사용하였다. 그 중, TCG의 Mobile Trusted Module이 모바일 장치가 제공해야 하는 보안 사양을 발표하였으며, 이러한 TPM은 모바일 하드웨어 모듈이 무결성 측정을 위한 기능을 제공하고 있으며 암호화 기능에 대한 key 정보 등을 제공하고 있다[13]. 또한 보안 서비스 도메인에서 Virtual Trusted Module을 제공

하는 MTM 기술이 연구되고 있다[8][17].

3. TEEMO 기술

TEEMO는 ETRI에서 제안된 모바일 플랫폼을 위한 가상화 기반 보안 실행 환경이다[1][2][16]. 이 기술은 서로 다른 보안 정책을 두 개의 별도의 도메인을 제공하고 안전한 방법으로 격리된 가상 머신에서 보안 서비스를 제공하는 것이다. 실행 안전 영역에서 다양한 보안 서비스를 제공하고 사용자는 이러한 서비스를 이용할 수 있는 보안 API를 통해 보안 서비스를 제공받도록 제한되었다. 아울러, 두 개의 영역을 분리하기 위해 TYPE-II 기반의 하이퍼바이저를 이용하였다. 일반적으로 TYPE-II 기반의 가상화 기술은 에뮬레이터 방식으로 가상화를 하기 때문에 TYPE-I 가상화 기술에 비해 처리속도가 느리다는 단점을 가지고 있다.

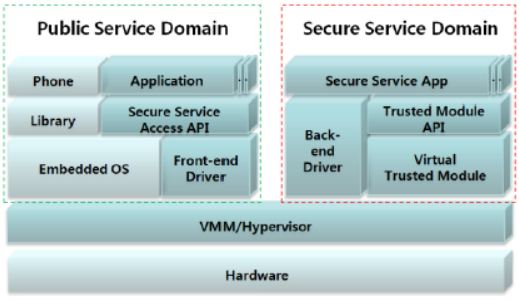

그림 1. TEEMO 구성도
Fig. 1. TEEMO Architecture

4. MDM(Mobile Device Management) 기술

모바일 장치 관리(MDM) 소프트웨어는 모바일 장치를 보호, 관리, 모니터링 하는 기능을 제공하는 기술이다. 이러한 MDM 기능은 스마트폰, 태블릿 컴퓨터, 휴대용 프린터, 휴대 POS 장치를 포함한 모든 종류의 모바일 디바이스에서 사용되는 어플리케이션, 데이터, 환경 설정 등을 보호하는 기능을 제공한다. MDM은 이동 통신 네트워크의 기능 및 보안을 최적화하는 것으로 모바일 디바이스의 사용 증가로 인한 보안 문제에 따라 빠르게 성장하고 있다[16].

5. TrustZone 기술

TrustZone은 ARM에서 제공하고 있는 보안 기술로써, 클라이언트 어플리케이션이 보안 환경과 보안 서비스를 사용할 수 있도록 추상 보안 서비스와 통신 인터페이스를 제공하며, 지원 가능한 하드웨어 플랫폼 상의 상위층에 위치하고 있다[16].

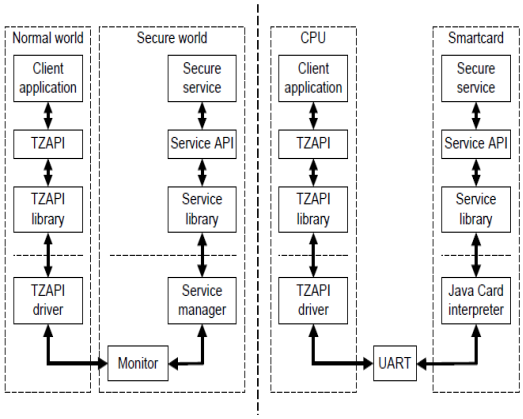

그림 2. TrustZone API를 이용한 시스템 구성도
Fig. 2. Two possible systems using the Trust Zone API

클라이언트의 관점에서, TZAPI는 네 개의 기능 블록으로 보안 환경을 구성한다[16].

가. TrustZone API

TZAPI은 특정 플랫폼을 요구하지만, 일반적으로 클라이언트 메모리 공간이나 호스트 운영체제의 특권 메모리 영역에 존재하는 라이브러리 코드로써의 컴포넌트이다. 일반적으로 드라이버라고 불리우는 운영체제 내의 컴포넌트는 클라이언트 메모리 영역 내에 있으며 몇몇 제한된 보안 기능을 제공하는 컴포넌트보다 좀 더 신뢰될 필요가 있다.

나. 장치

단일 논리적 장치는 시스템 내 각각의 보안 환경을 제공하는 기본 요소이다. 장치는 보안 환경으로의 엔트리 포인트를 제공하고, 클라이언트와 다른 컴포넌트 사이의 연결을 관리한다.

다. 서비스 매니저

제공할 서비스를 구성하거나 장치 내에 설치된 서비스를 변경하기 위한 기능을 제공한다.

라. 서비스

많은 수의 서비스들이 보안 환경에서 실행되어지고 있지만 높은 수준의 보안 기능을 클라이언트 어플리케이션에 부여하고 있다. ARM의 TZAPI는 구조화된 메시지 및 공유 메모리를 통해 클라이언트와 서비스 간의 통신을 제공하고 있다. 공유 메모리는 서비스의 메모리 공간에 직접 매핑되는 클라이언트 메모리이다.

공유 메모리가 큰 데이터 버퍼들을 사용하는 서비스들에서 오버헤드를 최소화하는데 유용한 반면에, 구조화된 메시지는 작은 양의 데이터를 전달하는데 사용될 수 있다.

Ⅲ. 모바일 가상화 TYPE-I을 이용한 보안 시스템

모바일 가상화 TYPE-I 기반의 보안 시스템은 스마트 워크 서비스 및 각종 보안 서비스를 안전하게 제공하기 위해서 안드로이드 OS 기반의 '일반 영역'과 Secure OS 기반의 '안전 영역', 그리고 모바일 하이퍼바이저, 스마트 워크용 어플리케이션으로 구성된다. 안드로이드 OS의 개방성은 사용자에게 편리함과 폭넓은 활용성을 주지만, 반면에 보안 취약점을 가진다. 따라서 이를 해결하기 위한 방안으로 기존의 안드로이드 OS가 설치된 단말과 동일한 환경인 '일반 영역'외에, 일반 사용자에게 노출되지 않고 모바일 단말의 안전성을 확보하기 위한 핵심 보안 기능을 수행하는 '안전 영역'을 가지며, 두 도메인은 하이퍼바이저를 통해서 연결된다.

그림 3에서 볼 수 있듯이 모바일 가상화 TYPE-I 기반의 보안 시스템은 프로세서 위에 일반 영역과 안전 영역을 연결하기 위한 하이퍼바이저를 두고, 일반 영역이 안전 영역에서 제공하는 보안 기능을 이용하고자 할 때 하이퍼바이저를 통해서 안전 영역과 통신하는 구조로 되어 있다. 스마트워크 서비스를 비롯한 다양한 서비스 구현 시, 기존의 안드로이드 OS만이 설치된 모바일 단말 구조에서와 거의 유사한 방법으로 모바일 가상화 TYPE-I 기반의 보안 시스템 환경에서 구현할 수 있도록 하기 위해서 모바일 보안 서비스 API가 존재하며 서비스에서 필요로 하는 보안 기능이 동작할 수 있는 Secure OS, 각종 보안 관련 기능을 제공하는 모듈로 구성된다.

1. 보안 서비스

본 논문에서는 모바일 가상화 TYPE-I 기반의 보안기술을 이용하여 보안 서비스를 제공하기 위해 요구되는 요소들을 연구하였으며, 그 내용은 다음과 같다.

가. 인증 요소

모바일 환경에서 보안 서비스를 제공하기 위해서는

그림 3. 모바일 가상화 TYPE-I 기반의 보안 시스템
Fig. 3. Security System based on Mobile Virtualization TYPE-I

사용자의 인증 또는 어플리케이션 인증과 같은 수단을 통해 사용자의 접근을 확인하기 위한 요소가 필요하다. 모바일 가상화 TYPE-I 기반의 보안 시스템에서는 모바일 가상화 기술에 의해 분리된 두 개의 영역 중 일반 영역의 사용자 혹은 어플리케이션이 안전 영역의 시스템 리소스 및 보안 기능을 이용하고자 할 때, 사용자 혹은 어플리케이션을 인증하고, 접근제어에 사용할 데이터를 생성하는 기능을 수행한다. 사용자 혹은 어플리케이션을 인증한 후, 해당 사용자 혹은 어플리케이션에 대한 접근 제어를 통해서 안전 영역에 속한 시스템 리소스 및 보안 기능의 이용 가능 여부를 결정할 수 있어야 한다.

나. 보안정책/접근제어 요소

모바일 환경에서 보안 서비스를 제공하기 위해서는 안전 영역의 보안 기능을 이용하거나 중요 데이터를 포함한 리소스에 접근하고자 할 때, 이를 보호하기 위한 요소가 필요하다. 비록 인증 과정에서 성공을 하더라도 보안정책 및 접근제어 요소에 의해서 해당 보안 기능 및 시스템 리소스에 대한 접근이 차별적으로 이루어지도록 해야 한다. 보안정책 및 접근제어 요소는 크게 보안정책관리, 접근권한결정, 접근제어권한실행 기능으로 분류할 수 있다.

다. 암호/키관리 요소

모바일 환경에서 중요한 정보를 보호하기 위한 핵심적인 기능 중 하나인 다양한 암호 알고리즘 및 키관리 기능을 보안 서비스로 제공해야 한다. 일반적으로 사용되고 있는 보안 알고리즘은 다음과 같다.

- 블록 암호
  · 평문을 일정 단위로 나누어서 각 단위마다 암호화 과정을 수행하여, 블록단위로 암호문을 얻는 대칭 암호화 방식으로 현재 세계적인 표준 암호알고리즘으로 사용되고 있는 AES와 국산암호알고리즘인 ARIA, SEED 알고리즘, 현재는 많이 사용되고 있지 않지만, 기존의 암호시스템에서 사용되고 있는 DES, T-DES등이 있다.
- 해쉬 함수
  · 임의의 길이의 입력 메시지를 고정된 길이의 출력 값으로 압축시키는 함수로써, SHA 방식이 가장 많이 사용되고 있으며, 인터넷 응용에서는 default 해쉬 알고리즘을 사용하고 있다. 또한 최근에는 많이 사용되고 있지는 않은 MD5등이 있다.
- 공개키 암호
  · 공개키 암호 방식으로는 가장 대표적인 RSA 알고리즘이 있으며, RSA와 같은 기존의 암호화 시스템에 비해 크기가 작은 키를 사용하여 동등한 보안 기능을 제공하는 ECC 알고리즘이 있다. ECC 알고리즘은 작은 키를 사용하므로, 계산 속도가 빠르고 전력 소모가 적을 뿐만 아니라 메모리와 대역폭도 절약되어, 모바일 또는 무선 환경에 적합한 특징을 갖는다.
- 전자서명
  · 전자서명 알고리즘은 인증서를 생성하는 경우와 전자문서에 전자서명을 하는 경우에 사용한다. 전자서명은 위조불가, 서명자 인증, 부인불가, 변경 불가, 재사용 불가 조건을 만족하게 구현되어야 한다.

라. 안전 저장 요소

안전 저장 요소는 모바일 장치 내에 존재하는 민감 정보를 저장하기 위한 것으로, 기업 정보, 문서 등을 안전 영역에 저장함으로써, 일반 영역의 해킹 위험으로부터 주요 정보를 보호하기 위해 필수적으로 요구되는 요소이다. 아울러 안전 저장소에 대한 임의의 사용을 제한하기 위하여, 인증에 따라 허가된 응용 프로그램(서비스)만이 안전 저장소의 데이터를 저장(또는 인출)할 수 있도록 설계할 필요가 있다.

Ⅳ. 실험 및 결과

본 논문은 모바일 가상화 TYPE-I 기반 보안 시스템의 실험을 위해 모바일 단말에 모바일 단말용 OS(안드로이드 OS)와 보안서비스를 위한 시큐어OS(uCOS)가 올라가 있는 시스템을 고려하였으며, 본 논문에서 제안한 보안 기능 요소를 구현하여 동작 여부를 실험하였고 아울러 보안 서비스를 처리하는데 소요되는 시간을 측정하였다. 시험대상은 본 논문에서 제안한 모바일 가상화 TYPE-I 기반 보안 시스템과 TYPE-II 기반 보안 시스템이며 시험에 사용한 도구는 다음과 같다.

- 컴파일러
  • arm-2010q1(TeeMo 컴파일러), arm-2009q1

(r2mvm 컴파일러), Sourcery G++ Lite arm-2010q1-188 for ARM(Host 커널 컴파일러)
  - android-ndk-r8b-linux-x86(TCM, libTeeMo 컴파일러)
- 개발자 보드와 PC컴파일러 연결을 위한 드라이버
  - Teraterm : PC와 개발 장비 연결을 통한 동작 내용 확인
  - adb 및 fastboot : 커널 및 bootloader 탑재를 위한 프로그램
  - usb 드라이버(SiliconLab) : 개발 장비의 usb 연결을 위한 장치 드라이버

또한, 실험에 이용된 보안 기능과 실험 방법은 다음과 같다.

- 모바일 가상화 관리 기능 : 사용자 PIN정보, 사용자 PIN입력에 사용한 키보드 번호, AppID정보, replay attack 방지를 위한 임의의 값을 이용하여 하이퍼바이저와의 연결 성공 여부를 판단
- 인증서 관리 기능 : 인증서 파일을 입력으로 하며, 인증서를 안전한 영역에 정상적으로 저장 및 삭제 가능한지 여부를 판단
- 암호화 복호화 기능(파일 또는 데이터) : 평문의 문자열을 입력으로 하며, 입력되는 평문이 SEED 암호알고리즘을 이용하여, 정해진 암호문으로 정상적으로 암호화되고, 다시 원래의 평문으로 복호화 되는지를 판단
- PIN 관리 기능(등록, 검색, 비교) : PIN 번호를 입력으로 하여, 기존 PIN 번호를 새로운 PIN 정보로 변경 또는 PIN번호에 따른 사용자 인증 기능이 제대로 되는지 여부를 판단
- 보안정책/접근제어 기능 : AppID정보, 소스 정보, 명령어, 명령어 수행에 필요한 입력 파라미터를 통해 접근제어 코드가 임베디드 시스템에 정상 로딩되어 오류 없이 실행되고, 입력되는 AppID 정보와 명령어 수행 시, 접근권한에 해당하는 데이터 접근으로 명령어 수행이 완료되는지 여부를 판단
- 암호/키관리 기능(대칭키 암호) : 평문 데이터를 입력으로 하여, 암호코드가 임베디드 시스템에 정상 로딩되어 오류 없이 실행되고, 입력되는 평문이 SEED 암호알고리즘을 이용하여, 정해진 암호문으로 정상적으로 암호화되고, 다시 원래의 평문으로 복호화 되는지 여부를 판단
- 암호/키관리 기능(비대칭키 암호) : 평문 데이터를 입력으로 하여 암호코드가 임베디드 시스템에 정상 로딩되어 오류 없이 실행되고, 입력된 평문에 대한 KCDSA, RSA, PKCS 알고리즘에 따라 정상적으로 생성되는지 여부를 판단
- 안전저장 장치 기능 : 임의의 파일을 입력하여, 안전영역에 저장되는지 여부를 판단

이러한 시험 평가 대상 선정 및 절차에 따라 동일한 환경과 조건으로 TYPE-I 가상화 기술을 이용한 시스템과 TYPE-II 가상화 기술을 이용한 시스템에서 보안 기능에 대한 테스트를 수행하였으며, 두 시스템 모두 보안 서비스를 오류 없이 제공하였다. 아래의 그림 4는 제안시스템의 안드로이드에서 실행된 보안 서비스 API 중 인증서 관리 기능 API가 실행된 화면이다. uCOS에 저장된 인증서의 내용을 안드로이드에서 확인할 수 있는 것을 볼 수 있다.

그림 4. 인증서 관리 기능 실행 화면(안드로이드)
Fig. 4. Execution of Certification Manage Function(Android)

그림 5는 제안시스템의 안드로이드에서 요청하는 PIN 관리 기능 중 사용자 인증 보안 서비스를 uCOS에서 인증절차에 따라 인증 서비스를 수행한 결과를 보여주는 화면이다.

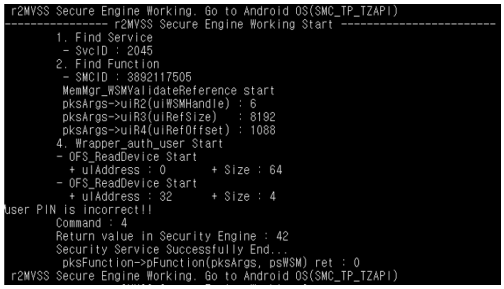

그림 5. PIN 관리 기능 실행 화면(uCOS)
Fig. 5. Execution of PIN Manage Function (uCOS)

이처럼 실험 대상으로 이용된 두 개의 시스템(제안시스템, TYPE-II 기반 시스템) 모두 정상적으로 구현된 기능을 실행하였으나, 처리속도 측면에서는 그림 6에서 보여 지듯이 본 논문에서 제안하는 시스템이 0.03초에서 0.5초 사이의 처리속도를 보인 반면에 TYPE-II 가상화 보안 시스템의 경우는 0.4초에서 1.0초 사이의 처리속도를 갖는 것으로 측정되었다. 그림 6에서 x축은 실행되었던 각 보안 서비스 API를 의미하며, y축은 사용자가 보안 서비스 API를 호출한 후, uCOS에서 해당 기능을 처리하고 다시 호출한 보안 서비스 API로 반환되는데 소요되는 시간을 의미한다.

실험에 이용되었던 두 시스템 모두 비교적 긴 처리 시간을 갖는 API들(API5, API11 ,API12)은 uCOS에서 파일 읽기, 쓰기 등 파일 시스템에 접근하는 경우와 복잡한 보안 알고리즘을 수행하는 API들이였으며, 처리 시간이 비교적 짧은 경우(API1, API2, API3, API4)는 세션 연결, PIN 정보에 다른 사용자 인증, PIN 정보 변경 등 uCOS에서 단순 처리를 요구하는 경우였다.

본 실험을 통해 본 논문에서 제안한 모바일 가상화 TYPE-I을 이용한 보안시스템이 TYPE-II 기반 보안 시스템보다 같은 기능을 제공하면서, 처리속도가 약 2배가량 빠른 것을 확인할 수 있었다.

V. 결 론

최근 스마트 장치 확산과 이러한 장치들을 이용한 다양한 서비스들의 도입으로 모바일 보안 및 스마트 TV 보안에 대한 관심이 증가하고 있다. 스마트폰 사용자들은 클라우드 서비스, 게임, 뱅킹 서비스, 모바일 서비스 등의 다양한 서비스를 사용한다. 하지만 현재의 모바일 보안 솔루션과 스마트 TV 보안은 단순히 악성코드를 탐지하거나 모바일 단말 관리, 자체 보안 시스템을 이용하는 수준에 머무르고 있다. 이에 인증서, 법인 문서, 개인의 신용 카드 번호와 같은 보안에 민감한 정보에 대해 서

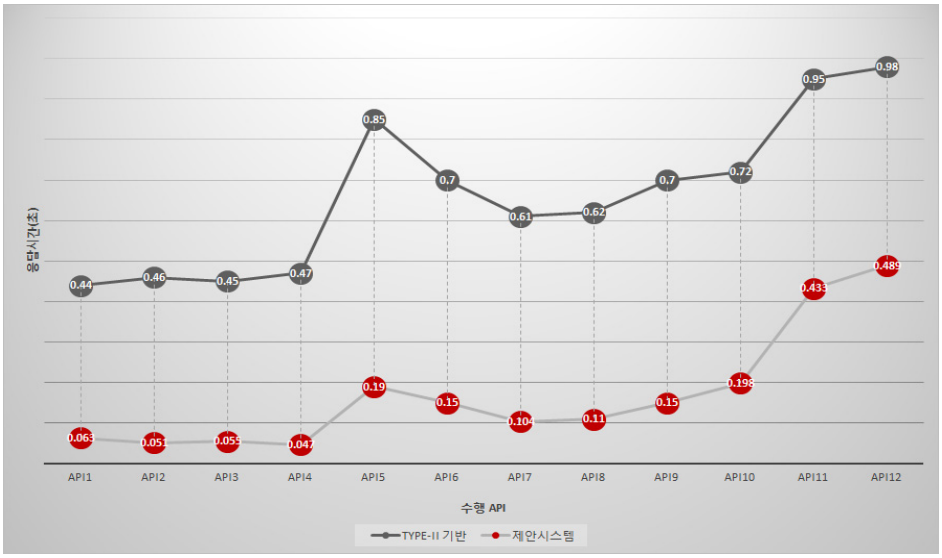

그림 6. 처리속도 측정 시험결과
Fig. 6. Test Result of Execution Time

비스 해킹 및 누설을 방지하는 기술이 필요하다. 따라서 본 논문에서는 현재 제공되고 있는 보안 기술에 대해 연구하였고, 이러한 보안 기술 중에 모바일 가상화 기술을 이용한 형태의 시스템을 조사하였으며, 모바일 가상화 기반의 보안 환경에서 필요한 요소 기술에 대해 연구하였다. 아울러, 이러한 요소 기술을 모바일 가상화 TYPE-I 기반과 TYPE-II 기반 환경에서 구현하여 각 기능을 실험하였다. 또한, 각 TYPE에 따른 처리 속도를 비교함으로써 향후 스마트워크 환경을 채택하기 위한 기업 및 정부 기관들이 고려해야 할 보안 요소들 선정과 보안 환경 구축에 도움이 될 것으로 생각된다.

References

[1] Young-Ho Kim, Jeong-Nyeo Kim, "Building Secure Execution Environment for Mobile Platform Computers", 2011 First ACIS/JNU International Conference, IEEE, pp.119-122, 2011, DOI:10.1109/CNSI.2011.36

[2] Young-Ho Kim, Yun-Kyung Lee, and Jeong-Nye Kim. "TeeMo: A Generic Trusted Execution Framework for Mobile Devices", Computers, Networks, Systems, and Industrial Application International Conference, SERSC, Volume 8, 2012.

[3] J. Bickford, R. O'Hare, A. Baliga, V. Ganapathy, and L. Iftode, "Rootkits on Smart Phones: Attacks, Implications and Opportunities," HotMobile'10, Feb. 2010, DOI:10.1145/1734583.1734596

[4] Trusted Computing Group, TCG Specification Architecture Overview Specification, revision 1.4, http://www.trustedcomputinggroup.org/resources/tcg_architecture_overview_version_14, Aug., 2007.

[5] C. Linn and S. Debray, "Obfuscation of Executable Code to Improve Resistance to Static Disassembly," ACM CCS, Oct. 2003, DOI:10.1145/948109.948149.

[6] P. Barham et al., "Xen and the Art of Virtualization," ACM SOSP, Oct. 2003, DOI:10.1145/1165389.945462

[7] A. Whitaker, M. Shaw, and S. D. Gribble, "Scale and Performance in the Denali Isolation Kernel," ACM OSDI, vol. 36, 2002, DOI:10.1145/844128.844147

[8] TCG, Mobile Trusted Module Specification, ver. 1.0, revision 6, http://www.trustedcomputinggroup.org/files/resource_files/87852F33-1D09-3519-AD0C0F141CC6B10D/Revision_6-tcg-mobile-trusted-module-1_0.pdf, June 2008.

[9] S. M. Lee, S. B. Suh, and B. Jeong, S. Mo, "A Multi-Layer Mandatory Access Control Mechanism for Mobile Devices Based on Virtualization", IEEE Consumer Communications and Networking Conference, Jan. 2008, DOI:10.1109/ccnc08.2007.63

[10] J. Y. Hwang and S. B. Suh, "Xen-On-ARM: System Virtualization using Xen Hypervisor for ARM-based Secure Mobile Phones," IEEE Consumer Communications and Networking Conference, Jan. 2008, DOI:10.1109/ccnc08.2007.64

[11] J. Azema and G, Fayad, "M-Shield Mobile Security Technology", http://focus.ti.com/pdfs/wtbu/ti_mshield_whitepaper.pdf, White Paper, Texas Instruments, 2008.

[12] NFC mobile service standard consortium, "Dynamic management of multi-application secure elements", http://members.nfc-forum.org/resources/white_papers/Stolpan_White_Paper_08.pdf, White Paper, 2008.

[13] R. Sailer, X. Zhang, T. Jeager, and L. Doorn, "Design and Implementation of a TCG-based Integrity Measurement Architecture", https://www.usenix.org/legacy/events/sec04/tech/full_papers/sailer/sailer.pdf, 13th USENIX Security Symposium, Aug. 2004.

[14] T. Garfinkel and B. Pfaff, "Terra: A Virtual Machine-Based Platform for Trusted Computing," ACM SOSP, 2003, DOI:10.1145/945445.945464

[15] Jung-Oh Park and Byung-Wook Jin, "A Study on Authentication Method for Secure Payment in Fintech Environment", The Journal of The Institute of Internet, Broadcasting and

Communication, Vol. 15, No. 4, pp.25-31, Aug. 2015.
[16] Hwi-Min Choi, Chang-Bok Jang, Joo-Man Kim, Efficient Security Method Using Mobile Virtualization Technology And Trustzone of ARM, DOI:10.14400/JDC.2014.12.10.299
[17] Young-Do Joo, "Security Improvements on Smart-Card Based Mutual Authentication Scheme", International Journal of Internet, Broadcasting and Communication, The Journal of The Institute of Webcasting, Internet and Telecommunication VOL. 12 No. 6, DOI:10.7236/JIWIT.2012.12.6.91

저자 소개

강 용 호(정회원)

- 1994년 2월 : 충남대학교 컴퓨터공학 (공학사)
- 1997년 2월 : 충남대학교 컴퓨터공학 (공학석사)
- 2000년 2월 : 충남대학교 공학박사 수료
- 2012년 3월 ~ 현재 : 부산대 IT응-용공학과 박사과정

<관심분야 : 클러스터 컴퓨팅, 모바일 클라우드 컴퓨팅, 모바일 가상화 및 보안>

- E-Mail : kang@r2soft.co.kr

장 창 복(정회원)

- 2003년 2월 : 한남대학교(공학석사)
- 2007년 2월 : 한남대학교(공학박사)
- 2007년 3월 ~ 2011년 2월 : 한남대 BK21 연구교수
- 2011년 3월 ~ 현재 : (주)알투소프트 연구소장

<관심분야 : 상황인식 컴퓨터, 유비쿼터스 컴퓨팅, 모바일 클라우드 컴퓨팅, 모바일 가상화 및 보안>

- E-Mail : chbjang@r2soft.co.kr

김 주 만(정회원)

- 1984년 2월: 숭실대학교 전자계산학 (공학사)
- 1998년 8월 :충남대 컴퓨터공학 (공학석사)
- 2003년 2월 :충남대 컴퓨터공학 (공학박사)
- 1985년 1월 ~ 2000년 2월 : ETRIOS 팀장(책임연구원)
- 1995년 7월 ~ 1996년 6월 : 미국 Novell사 객원연구원
- 2000년 3월 ~ 현재 : 부산대학교 IT응-용공학과 교수

<관심분야 : 임베디드 시스템, 실시간 시스템, 클러스터 컴퓨팅, 병렬분산 시스템>

- E-Mail : joomkim@pusan.ac.kr

※ 본 논문은 중소기업청에서 지원하는 2013년도 기술혁신개발사업(S2131902)의 연구수행으로 인한 결과물임을 밝힙니다.