情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

가상화를 이용한 모바일 플랫폼 보안성 향상 기술*

김 정 한,[1†] 김 지 홍,[2] 신 은 환,[1] 엄 영 익[1‡]
[1]성균관대학교 전자전기컴퓨터공학과, [2]성균관대학교 휴대폰학과

Enhancing Mobile Platform Security with Virtualization Technologies*

Junghan Kim,[1†] Jee-hong Kim,[2] Eunhwan Shin,[1] Young Ik Eom[1‡]
[1]Department of Electrical and Computer Engineering, Sungkyunkwan University,
[2]Department of Mobile Systems Engineering, Sungkyunkwan University

요 약

모바일 장치의 성능 향상과 네트워크 인프라의 확산 그리고 개방형 어플리케이션의 등장으로 스마트폰이 빠르게 보급되고 있다. 이러한 모바일 환경의 변화는 다양한 선 작용과 동시에 보안 문제를 야기하고 있다. 이를 해결하기 위한 다양한 방법 중 하나로 가상화를 이용한 보안 기술이 주목받고 있다. 이에 본 논문에서는 가상화를 이용한 모바일 플랫폼 보안성 향상 기술을 제안한다. 제안하는 Secure execution 기술과 프로세스 은닉 기술을 통하여 가상 머신 보호 및 프로세스 보호가 가능함으로써 보다 더 안전한 모바일 환경을 제공한다.

ABSTRACT

Smartphone devices are widely used because of recent improvements in hardware device, network infrastructure, and emergences in open mobile platforms. These changes provide various advantages and cause security problems. One of the solutions to prevent these problems is that applying of the virtualization technology to mobile environment has attracted attention. In this paper, we proposed the virtualization technology which is based on security-enhanced mobile platform scheme, for secure mobile environment based on the secure execution and process concealing technology.

Keywords: Mobile Virtualization, Mobile Platform, Mobile Security, Secure Execution, Process Concealing

I. 서 론

모바일 장치의 성능 향상과 네트워크 인프라의 확산 그리고 누구나 개발하여 설치가 가능한 모바일 애플리케이션 환경의 제공으로 스마트폰이 빠르게 보급되고 있다. 이러한 모바일 환경의 변화는 다양한 선 작용과 함께 보안 문제를 야기하고 있으며 이러한 보안 문제는 날로 커지고 있는 상황이다[1,2]. 더구나 모바일 환경은 특유의 휴대성을 바탕으로 개방형 모바일 플랫폼을 통해 상시 네트워크에 연결되어있어 보안 문제의 확산 속도가 크기 때문에 이러한 문제들에 빠르게 대응하기 위해서 관련 보안 기술 연구가 시급히 필용하다.

이에 따라 모바일 플랫폼을 보호하기 위한 다양한 보안 기술들이 제안 되고 있다. 모바일 전용 백신, 모바일용 하드웨어 보안모듈인 MTM(Mobile Trusted Module), ARM 기반 모바일 프로세서 보안기술인 Trustzone, 공개된 컴퓨팅 환경을 보호하기 위한 PCPP(Private Computing on Public Platforms), 가상화 기술을 이용한 Secure execution

접수일(2010년 12월 05일), 수정일(2011년 02월 14일), 게재확정일(2011년 02월 23일)
* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (No.2010-0022570)
† 주저자, junghan@ece.skku.ac.kr
‡ 교신저자, yieom@ece.skku.ac.krr

기술 등이 현재 제안되었다[3,4,5,6]. 그러나 이들 기술은 각각의 장점 및 단점이 존재하며 이에 각각의 기술들을 통합할 수 있는 모바일 플랫폼 보안 기술이 필요한 상황이다.

최근 IT 산업에서 주목받는 기술 중에 하나인 가상화 기술은 서버 및 데스크톱 가상화, 클라우드 컴퓨팅을 넘어 모바일 환경에도 적용되어 컴퓨팅 환경의 유연성을 제공하고 있다[7]. 또한 가상화 기술은 이미 악성 코드 탐지 시스템, 시스템 모니터링 등의 보안 기술로도 널리 사용 중에 있다[8]. 이에 더해 Secure execution과 같은 가상화 응용 기술도 모바일 보안 기술로 최근 주목받고 있다.

이에 본 논문에서는 가상화 기술을 이용한 모바일 플랫폼 보안 기술을 소개한다. 성균관대학교에서 제안한 MyAV 가상화 엔진을 이용하여 효율적인 Secure execution 환경을 제공함과 동시에 프로세스 은닉기술을 통하여 가상 머신에서 특정 프로세스 보호 및 모바일 클라우드 환경에 대비한 원격지 프로세스 보호 기술을 제공한다[9]. 또한 취약점 모델링을 통하여 보안 유형을 분석하고 제안 기술과 관련 기술과의 비교를 통하여 본 가상화 보안 기술의 장점을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 모바일 플랫폼의 보안과 모바일 가상화 기술을 소개한다. 이후 3장에서는 모바일 플랫폼 보안을 위한 관련 연구들을 살펴보고, 4장에서는 모바일 플랫폼 보안을 위한 가상화 기술을 제안한다. 5장에서는 보안 모델링을 통하여 제안 기술을 검증하고 마지막으로 6장에서 결론을 맺는다.

II. 배경 지식

본 장에서는 최근 이슈가 되고 있는 모바일 플랫폼 상의 보안 문제들과 본 논문의 바탕이 되는 모바일 가상화 기술에 대해 소개한다.

2.1 모바일 플랫폼 보안

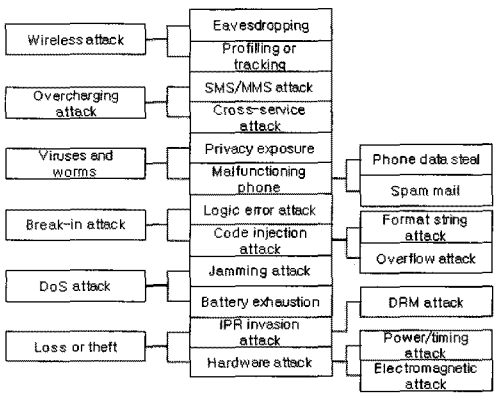
모바일 장치의 성능 향상과 네트워크 인프라의 확산 그리고 누구나 개발하여 설치 가능한 모바일 애플리케이션 환경의 제공으로 스마트폰은 빠르게 보급되고 있다. 또한 애플사의 아이폰OS 모바일 플랫폼과 구글사의 안드로이드 모바일 플랫폼은 타블렛, Ebook 등의 모바일 장치에도 적용되어 기존 컴퓨팅 환경을 대체하는 빠른 성장을 보이고 있다. 앞으로의 모바일 환경은 개방성을 바탕으로 더 나아가 다양한 전자 장치에 적용 될 것으로 전망되고 있다.

모바일 환경의 변화는 다양한 신 작용과 동시에 가장 큰 문제로 보안 문제를 야기하고 있다. 이러한 보안 문제는 다음의 몇 가지 모바일 상의 위협 요소로 기인한다[1]. 스마트폰은 무선 네트워크상에 상시 연결이 되어있으며 모바일 플랫폼에서 제공하는 SDK (Software Development Kit)을 통하여 누구나 어플리케이션 개발과 배포가 가능하다. 이러한 개방성은 현재 모바일 환경의 변화의 가장 큰 성공 요인과 동시에 보안상의 위협요인이 되고 있다. 또한 모바일 장치의 휴대성은 항상 도난 및 분실 사고의 위험요소를 내포하고 있으며 피쳐폰과 달리 개인 정보 및 모바일 오피스 환경을 제공하는 스마트폰의 특성상 모바일 위협요소는 크다고 볼 수 있다.

이러한 스마트폰의 보안 위협은 아래 그림 1과 같이 분류할 수 있다.

모바일 공격 유형은 기존 데스크톱 환경에서의 보안 문제들을 포함하며 더 나아가 분실 및 도난으로 인한 문제와 24시간 전원이 켜진 상태로 무선 네트워크 연결로 인해 발생하는 문제, 사용자 위치를 알 수 있는 GPS 신호를 이용한 보안 문제 등이 있다. 그로 인해 현재 모바일 상의 보안 문제는 심각한 위험에 노출되어 있으며 보안 문제를 야기하는 악성 프로그램의 수는 가파르게 증가하고 있다. 대표적으로 단말 장애를 유발하는 악성코드, 배터리 소모를 촉진하는 악성코드, 과금을 발생시키는 악성코드, 사용자 정보 유출하는 악성코드, 연결된 이기종 장치를 감염시키는 악성 코드 등이 있으며, 그 종류는 점차 다양해지고 있으며 위험성은 커지고 있는 상황이다.

모바일 플랫폼 상의 보안 문제는 기존의 보안 문제



[그림 1] 모바일 공격 유형 분류[1]

와 달리 모바일 기기의 특성상 보호 및 해결에 더 큰 어려움이 있다. 모바일 기기는 배터리를 이용하여 동작하며 한정된 저장공간 및 컴퓨팅 자원을 바탕으로 동작한다. 그러기 때문에 컴퓨팅 자원을 많이 소모하는 백신과 같은 형태의 보호 기술은 모바일 상에서 한계점을 지니고 있다. 또한 모바일 플랫폼의 운영체제 영역에까지 공격에 침해되었다면 모바일 장비의 특성상 개개인의 복구하기에 어려움이 따른다.

모바일 기기는 24시간 켜진 상태로 무선 네트워크 상에 연결되어있으며 사용자의 이동에 따라서 계속 무선 네트워크를 달리 사용한다. 이와 같이 위험성의 확산도가 기존 데스크톱수준의 문제 보다 크기 때문에 이러한 모바일 플랫폼 상의 보안은 상당한 위험성을 갖고 있으며 보다 근본적인 보안 체계가 필요하다.

2.2 모바일 가상화

1970년대 초부터 연구가 시작된 가상화 기술은 물리적인 컴퓨팅 자원을 논리적인 컴퓨팅 자원으로 추상화함으로써 컴퓨팅 자원 활용의 유연성을 제공한다[10]. 이를 통하여 컴퓨팅 자원의 효율성을 증대시킴과 동시에 다양하게 응용되어 새로운 컴퓨팅 패러다임을 만들고 있다. 이러한 가상화 기술이 서버 가상화, 클라우드 컴퓨팅에 적용 및 안정화를 통하여 최근 모바일 환경에서도 새로이 주목받고 있다. VMware, VirtualLogix, Open Kernel Labs 등에서 상용 솔루션 개발에 성공하였으며 기존 서버 가상화로 널리 사용되고 있는 Xen, KVM 등도 모바일 플랫폼에 적용되어 다양한 연구 및 개발을 이끌고 있다[11,12,13,14].

이러한 모바일 가상화의 등장은 모바일 장치의 성능 향상 및 데스크톱 수준의 컴퓨팅 환경을 제공하는 모바일 플랫폼 보급으로 가능해졌으며 이후 다양한 형태로 응용이 가능 할 것으로 보인다. 특히 현존하는 모바일 가상화 솔루션들은 유연하고 안전한 컴퓨팅 환경을 만드는데 주로 활용되어 오고 있으며, 대표적으로 가상화의 격리 기술을 이용하여 악의적인 공격에 대응하는 Secure execution 및 하나의 단말을 이용하여 개인용 및 업무용 모바일 플랫폼 환경을 배타적으로 동시에 제공하는 SW 망분리를 예로 들 수 있다. 현재의 모바일 가상화 기술은 기존 서버/데스크톱 가상화 기술을 대부분 차용하고 있으며 보다 더 모바일 환경에 적합한 형태의 가상화 기술이 개발되어야 할 필요가 있다.

VMware사는 2008년 말 실시간 임베디드 가상화 기술 개발 업체인 TRANGO를 인수하여 2009년 MVP를 출시하였다[11]. MVP는 하나의 물리적인 모바일 장치 안에서 여러 개의 가상의 모바일 플랫폼을 운영하는 것이 가능하다. 이를 위해서 모바일 플랫폼 내의 운영체제 환경에는 가상화를 지원하기 위한 추가적인 소프트웨어 계층이 필요하다. 모바일 가상화 솔루션은 제한적인 모바일 환경에서 보다 더 높은 효율성을 제공하기 위해 가상 머신 내의 운영체제 코드를 수정하는 반가상화 기술이 주로 활용되고 있다. 또한 컴퓨팅 자원의 가용성을 높이는데 주된 목적이 있는 기존 가상화 기술과 달리 적은 자원 내에서 보안, 특수한 응용기술 지원 등을 주로 지원하는데 목적이 있다.

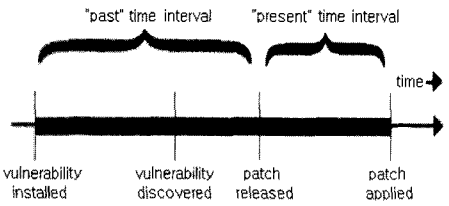
III. 관련 연구

본 장에서는 모바일 보안을 목적으로 연구되고 있는 보안 기술들을 소개한다. 기존에 널리 사용되어오는 소프트웨어 기반의 보안 기술인 백신, 하드웨어 암호화 모듈을 이용한 보안 기술인 MTM(Mobile Trusted Module), 프로세서 차원에서 제공되는 보안 기술인 Trustzone, 네트워크 상의 원격지의 프로세스를 보호하는 PCPP(Private Computing on Public Platforms), 가상화 기술을 이용한 보안 기술인 Secure execution을 차례로 소개한다.

3.1 모바일 백신

백신(vaccine)은 기존 데스크톱환경에서부터 가장 널리 사용되고 있는 보안 소프트웨어 중의 하나이다. 다양한 악성 프로그램 패턴의 DB화를 통하여 시스템 전체를 지속적으로 모니터링 함으로써 악성코드로부터 시스템을 보호한다. 악성 프로그램은 지속적으로 자신의 패턴을 변형하여 발생하기 때문에 이를 위해서 백신은 보다 더 많은 패턴DB를 관리함과 동시에 다양한 예측 알고리즘을 통하여 백신의 신뢰성을 높이고 있다. 그로인해 백신의 업데이트가 주기적으로 이루어지지 않는다면 보안성을 확보하기 어렵다.

최근 모바일 악성 프로그램은 2004년 카비르웜이 발생한 이후 2009년까지 600여종의 스마트폰 악성코드가 발생된 바 있으며 발생 빈도는 점점 빠르게 증가하고 있다. 이를 해결하기 위해 다양한 기존 백신들의 모바일 버전이 개발되어 스마트폰에 탑재되고 있다.



[그림 2] 취약성 생명 주기

그러나 백신을 통한 보안은 모바일 환경에서의 근본적인 어려움이 있으며 이는 다음과 같다[3].

위 그림과 같이 취약점이 노출, 발견되고 적절한 패치가 나오기까지에는 반드시 일정 기간이 필요하다. 또한 패치가 실제 사용자들에게 적용되어 취약점을 극복하기까지는 마찬가지로 시간이 필요하다. 그로 인해 시스템 전체가 취약점에 노출될 경우 전체 시스템에 대한 사용자의 자가 복구가 어려운 스마트폰 환경에서는 위와 같은 대비는 완벽한 보안 해결책이 되기 어렵다. 또한 배터리 사용의 제한이 있는 모바일 디바이스에서는 주기적으로 시스템을 모니터링하는 백신 소프트웨어의 적용은 많은 전력 소모를 가져올 수 있다.

3.2 MTM(Mobile Trusted Module)

TCG(Trusted Computing Group)는 신뢰 할 수 있는 컴퓨팅 환경을 구축하기 위해 2003년 설립된 컨소시엄으로써 암호화 하드웨어인 TPM(Trusted Platform Module)을 이용한 보안 기술을 제안하였다[15]. 또한 기존 TPM을 컴퓨팅 환경의 제약이 존재하는 모바일 환경에 보다 더 적합한 형태로 개량한 MTM을 2006년 공개하였다. MTM은 내부적으로 RSA 키 및 암복호화기, 난수 발생기, SHA-1 해쉬 모듈 등을 하드웨어에서 지원하며 모바일 환경에 적합하도록 전력소비 및 칩의 크기 등을 고려하여 제안되었다[4].

MTM은 외부에서 공개 될 수 없는 유일한 RSA 공개키/개인키를 통하여 플랫폼의 무결성을 검증, DRM 보호, 디바이스 사용자 인증, 과금 시스템 보호, 안전한 소프트웨어 다운로드, 개인 데이터 보호 등에서 활용이 가능하다. 특히 플랫폼의 무결성 검증을 위해서 안전한 부팅(secure boot) 기능을 제공하는데 이는 MTM에 저장된 해쉬 값을 이용하여 부트로더, 커널, 프로세스들의 무결성을 확인하는 과정을 통하여 이루어진다.

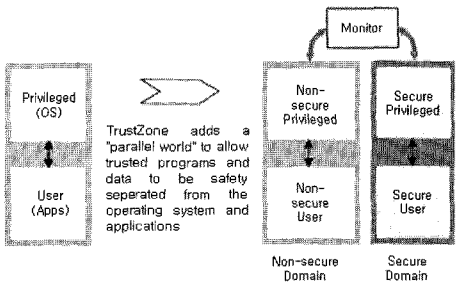
그러나 MTM은 현재까지 출시된 모바일 기기에서는 적용 사례가 드물며 널리 사용되는 구글사의 안드로이드 플랫폼 및 애플사의 아이폰 모바일 플랫폼이 탑재된 스마트폰의 경우 현재 적용사례가 없다. 또한 MTM 하드웨어를 이용한 방법으로는 기 설치된 코드의 검증은 가능하나 코드 자체에 갖고 있는 취약성에는 대처가 어렵다는 문제가 있다. 그로인해 MTM을 사용하는 경우 소프트웨어마다 코드의 신뢰성의 차이가 있으므로 TCB(Trusted Computing Block)의 크기를 최소화 하는 노력이 필요하다.

3.3 Trustzone

최근 컴퓨팅 환경의 보안을 위해서 프로세서 차원에서의 기술 지원이 늘어나고 있다. 특히 인텔 vPRO 기술에서는 TXT(Trusted Execution Technology) 기술을 제안하여 안전한 부팅 및 메모리 격리(isolation), 개인 데이터 유출 차단 등을 용이하도록 지원하고 있으며 이는 앞서 언급한 TPM 하드웨어 모듈과 연동하게 제공된다[16]. 이와 유사하게 ARM에서는 시스템의 보안성을 향상을 목적으로 ARMv6 아키텍처부터 프로세서 내에 Trustzone 기술을 제공하고 있다[5].

Trustzone은 다음 그림3와 같이 프로세서의 동작 모드를 일반 모드와 보안 모드로 나눈다. 이와 같은 하드웨어상의 지원을 통하여 가상적으로 2개의 분리된 환경에서 프로그램이 동작 할 수 있도록 지원한다. 이를 통하여 하나의 프로세서 상에서 보안 관련 어플리케이션과 일반 사용자 어플리케이션을 별도로 운영할 수 있게 함으로써 메모리의 보다 강력한 보호가 가능하다.

본 기술은 최근 x86 호환 프로세서에서 제공되는 VT(Virtualization Technology) 기술과 유사하



[그림 3] ARM사의 Trustzone 기술

다. VT 기술의 경우 2개의 동작 모드를 제공함과 동시에 가상화에 필요한 다양한 기술을 프로세서 상에서 지원 한다. 그러나 Trustzone은 보안성 향상이 목적이였으나 최근에는 가상화 기술과 융합하여 VT 기술과 유사한 형태의 하드웨어 지원 가상화 기술로도 주목받고 있다.

3.4 PCPP(Private Computing on Public Platforms)

PCPP는 공개된 컴퓨팅 환경 내에서 특정 어플리케이션을 다른 어플리케이션과 운영체제, 관리자로부터 보호하기 위해서 2007년 제안된 기술이다[6]. 다른 보안 기술들과 다르게 네트워크상에 공개된 플랫폼상의 있는 원격지 프로세스에 대한 보호기술을 정의하고 있으며 이와 관련하여 실행 코드 및 데이터 변경 방지, 실행 코드 복사 방지, 데이터 기록 방지, 프로그램 모니터링 방지에 대한 위협에 대응하기 위한 기술을 제안한다.

위와 관련하여 PCPP에서는 Executable guard, Secure context switch, Secure IO, Encryption key protection 기술을 제공한다. 먼저 Executable guard는 원격지의 보호 대상이 되는 메모리상의 로딩된 프로세스의 실행 파일 이미지를 암호화하는 기술이다. 마찬가지로 Secure context switch 기술은 메모리상의 보안 프로세스를 다른 프로세스로부터 보호하는 기술로써 실행/대기 시 메모리 암/복호화를 통하여 제공한다. Secure IO와 Encryption key protection은 각각 암호화를 이용하여 파일 시스템 보호하고 시스템 내 존재하는 보안키를 관리하는 기술이다.

PCPP 보안 기술은 원격지의 보안 프로세스를 보호하는 기술로써 최근 클라우드 컴퓨팅 환경이 대두되면서 네트워크상의 원격지의 시스템 보호의 필요성이 높아짐에 따라 주목받고 있다. 최근 클라우드 컴퓨팅 기술이 모바일에도 적용됨에 따라 앞으로는 모바일 환경에 적합한 클라우드 보안 기술을 필요로 하는 경우가 많아 질 것이다[17].

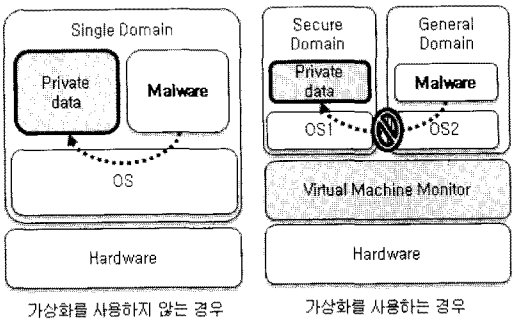
그러나 PCPP 기술은 클라우드 컴퓨팅의 기반 기술인 가상화 기술에 대해서 고려된바가 없다. 원격지의 가상 머신을 보호하고 가상 머신 내의 프로세스 또한 보호하는 기술이 새로이 주목받고 있으며 모바일 상에서도 필요로 하고 있다. 이와 관련하여 데스크톱 클라우드 컴퓨팅 환경에서 PCPP 기술을 가상화에 보다 적합하게 개량한 Local execution 기술이 제안된바 있으며 앞으로 모바일 환경에서도 관련 기술에 대한 연구가 필요하다[18]

3.5 Secure Execution

하나의 물리머신에서 생성 된 여러 개의 가상머신은 각각 격리되어 있어 서로 임의의 접근이 불가능하다. Secure execution은 위와 같은 점을 이용하여 안전한 실행환경을 제공하는 기술이다. 이를 위해 가상머신을 보안 정책에 따라 보안 가상머신(Secure Domain)과 범용 가상머신(General Domain)으로 구분한다. 보안 가상머신에는 전화, 주소록 등의 꼭 필요한 기본 프로그램과 인터넷 뱅킹 등의 보안에 민감한 프로그램을 사용하며, 범용 가상 머신에는 사용자 임의로 사용이 가능하도록 한다. 다음은 가상화 사용 유무에 따른 Secure execution의 동작 예를 보인다.

먼저 가상화를 사용하지 않는 경우의 시스템에서는 악성 프로그램의 공격 방법에 상당히 취약한 구조를 갖고 있다. 기존의 백신 등의 보안 기술 등이 위와 같은 기존 시스템에서 활용되고 있지만 결과적으로 한번 취약성이 노출되면 보안 문제는 발생한다. 그러나 가상화를 사용하는 경우, 가상 머신에 의해 사용상의 제약을 줌으로써 근본적인 보안성의 유지가 가능하다. 악성 프로그램의 공격 패턴은 계속 변화하고 진화하고 있으며 발생 후 해결하는 방법의 기존 연구에서는 보안성의 근본적인 한계를 갖고 있는 것이 사실이다. 모바일의 특성상 약간의 사용상의 제약이 따르더라도 근원적인 보호가 보안 문제에 있어서는 무엇보다도 중요하다.

가상화 기술을 이용하는 기존의 서버 및 데스크톱 가상화, 클라우드 컴퓨팅의 경우는 보안성 보다는 전체 시스템의 유연성을 높이는 노력을 하는 반면 현재



[그림 4] Secure execution

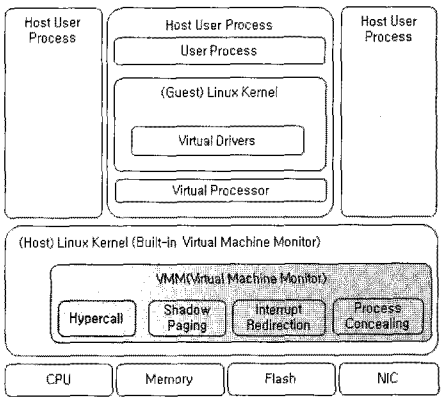
모바일 가상화의 흐름은 보안성에 보다 더 집중하고 있다. 상용 솔루션인 Open Kernel Labs의 OKL4 및 VMware의 MVP 경우, 모바일 가상화의 가장 중요한 사용예로 보안성 향상을 제시하고 있으며 이는 Secure Execution 기술과 맥락을 함께한다. 또한 서버 가상화로 유명한 오픈소스 Xen을 모바일에 적용한 삼성전자의 Xen on ARM의 경우도 Secure execution 기술을 소개하고 있으며 이와 관련하여 보안성 관리를 위한 Access control, Secure boot, Secure storage 기술 등을 제안하고 있다[14].

IV. 가상화를 이용한 모바일 플랫폼 보안 기술

가상화 기술은 기존 컴퓨팅 환경의 패러다임을 바꾸는 핵심 기술로 주목받고 있다. 대표적으로 가상화 기술은 서버 및 데스크톱가상화, 실시간 시스템 가상화, 시스템 모니터링, 클라우드 컴퓨팅과 같이 컴퓨팅 환경의 가용성, 실시간성, 확장성을 제공한다. 이와 더불어 가상화 기술은 보안성 향상을 위해서도 널리 사용되고 있다. 그 예로 동적 코드 분석기를 이용하여 악성 코드 탐지 시스템, 가상머신의 시스템 재생 기능을 이용한 악성코드 동작 분석, 가상 머신을 이용한 악성코드 수집을 위한 허니팟(honeypot) 시스템 운용, Secure execution에서 사용되고 있다[8]. 이와 같이 가상화 기술은 컴퓨팅 환경의 유연성과 보안성을 제공하고 있으며 기존의 연구된 다양한 응용 기술과 융합하여 보다 효과적인 기술로써 활용이 가능하다.

본 논문에서 제안하는 가상화 기술은 MyAV 가상화 엔진을 기반으로 모바일 환경에서 보다 높은 수준의 보안 기술의 제공을 목적으로 한다[9]. 본 가상화 기술은 커널/사용자 주소 공간 분리 기술을 사용하여 구조적으로 모바일 환경에 적합하도록 설계되었다. 더 나아가 가상 머신 간에 격리 기술을 기반으로 하는 가상 머신 보안기술을 제공하며 이 뿐만 아니라 가상 머신 내외의 프로세스 보안 기술을 지원한다. 다음은 MyAV 가상화 엔진의 구조를 보인다.

본 가상화 엔진은 리눅스 커널에 커널 모듈 형태로 내장된 하이브리드(hybrid) 구조로 설계되었다. 내장된 VMM(Virtual Machine Monitor) 역할을 하는 커널 모듈에는 프로세서 가상화를 위한 하이퍼콜(hypercall) 및 인터럽트 전달(interrupt redirection) 기능, 메모리 가상화를 위한 섀도우 페이징(shadow paging) 기능을 갖는다. 이와 별도로 본 논문에서 제안하는 보안 기술을 제공하기 위해서 각각



[그림 5] MyAV 가상화 엔진의 구조

의 세부 컴포넌트에 대해서 Secure execution을 고려한 추가적인 기능을 포함하며, 프로세스 보안을 위한 프로세스 은닉(process concealing) 기능을 포함한다.

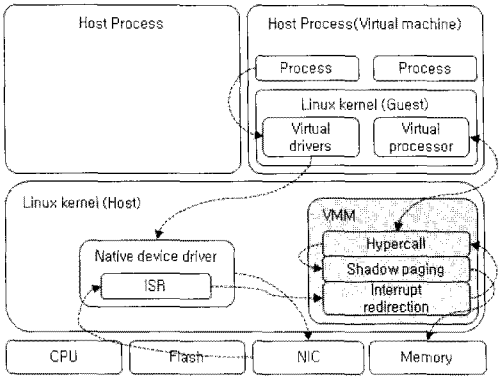
게스트 가상 머신에는 가상 프로세서(virtual processor), 가상 드라이버(virtual drivers)를 포함하여 특권 명령어, 인터럽트, 메모리 관리, 디바이스 관리 등을 VMM과 연동하여 처리한다.

위와 같은 하이브리드 구조를 통하여 기존의 VMware MVP 가상머신의 호스트(hosted) 구조의 성능 문제와 OKL4 및 Xen on ARM에서 사용되는 Bare-metal구조가 갖는 개발상의 어려움, 유지 보수 문제를 개선하였다. 이처럼 본 가상화 엔진은 구조적으로 TCB(Trusted Computing Base)의 크기, 성능, 개발 편의성 등을 고려하였다. 본 가상화 엔진은 반가상화 기술을 사용하기 때문에 게스트 가상 머신으로는 소스가 공개되어있는 리눅스 기반 커널 기반의 안드로이드 모바일 플랫폼을 적용하였다[19].

4.1 가상화 엔진의 세부 동작 과정

가상화 엔진 기술은 특수권한 명령어(privileged instruction), 처리 호스트-게스트 전환, 인터럽트 처리 등을 담당하는 프로세스 가상화와 메모리 주소 변환 및 보호를 담당하는 메모리 가상화, 가상의 장치를 관리하는 장치 가상화 기술로 나뉜다. 다음은 인터럽트 처리, 메모리 매핑, 장치 요청 처리의 예를 통하여 본 가상화 엔진의 세부적인 동작 과정을 소개한다.

기존의 가상화 SW의 경우, 메모리 맵 상에 상주하고 있고 실행 권한이 가장 높은 VMM을 호스트와 게스트가 공유하는 구조이다. 이러한 구조에서는 호스트



〔그림 6〕 가상화 엔진 동작 과정

-게스트 전환, 인터럽트 처리 등의 프로세스 가상화를 처리하기 위해서는 먼저 VMM으로 전환하고 그 뒤에 호스트, 게스트로 처리루틴을 전달하는 과정이 필요하다. 이에 따르는 스택 및 주소 공간의 전환 과정은 호스트 및 게스트에 전체적인 오버헤드를 가져온다. 그러나 제안하는 가상화 엔진의 경우 VMM에 별도의 메모리 맵을 할당하지 않고 호스트가 직접 처리 과정을 통해서 게스트에 전달하는 구조이다. 그로인해 위 그림6과 같이 NIC에서 인터럽트가 발생했을 경우, 호스트의 ISR에서 직접 수신하여 만약 게스트의 인터럽트라면 인터럽트 리다이렉션을 통해 게스트로 전달한다. 그 결과 VMM 전환이 필요하지 않게되어 호스트의 경우 가상화 제공으로 인한 추가적인 오버헤드가 미미하다.

가상 머신은 메모리 관리에 있어서 직접 메모리 관리 장치(MMU)에 접근 할 수 없기 때문에 VMM의 도움이 필요하다. 본 가상화 엔진은 코드 수정이 적고 관리가 용이한 섀도우 페이징 기법을 사용하고 있다. 위 그림과 같이 게스트의 메모리 매핑이 필요한 경우, 하이퍼 콜을 통하여 물리 페이지 테이블에 대한 매핑을 요청한다. 이 요청은 섀도우 페이징 기술을 통하여 VMM에서 관리하는 가상의 페이지 디렉토리에 동기화하고 실제 물리 메모리를 매핑한다.

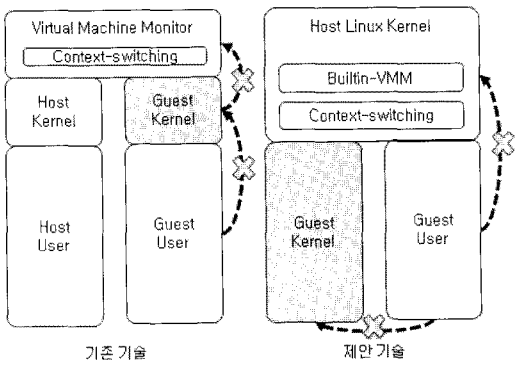
게스트는 실제 물리적인 장치의 직접 접근이 불가능하기 때문에 그래픽, 네트워크, 입력장치, 블록장치와 같은 각각의 장치에 대해서 가상의 장치 드라이버를 제공받아야 한다. 기존 가상화 엔진을 VMM이 독립적인 SW로써 존재하기 때문에 장치 지원에 있어 어려움이 있다. 이와 같은 경우 VMM이 모든 장치 드라이버를 관리하는 방법과 하나의 가상 머신에게 장치 관리를 위임하는 방법을 사용한다. 대부분의 가상화 엔진의 경우, 후자의 관리 방식을 따른다. 이는 모든 가상 머신의 장치 처리가 VMM를 경유하여 백엔드로 전달되므로 오버헤드가 상당히 크다. 그러나 본 가상화 엔진은 호스트 커널에서 관리하는 디바이스의 장치 파일을 가상 머신에서 읽고 쓰는 과정을 통하여 편리하게 장치 관리가 가능하다는 장점이 있다.

4.2 커널/사용자 주소공간 분리 기술을 이용한 Secure Execution 기술

일본 가상화 기술은 새로운 메모리 관리 기술을 이용하여 보다 효과적인 격리 기술을 바탕으로 Secure execution 환경을 제공한다. 다음은 기존 가상화 엔진과 제안하는 가상화 엔진의 메모리 맵을 비교한다.

가상 머신에서의 메모리 보호는 VMM과 가상 머신 사이의 보호와 가상 머신 내의 커널과 사용자 프로세스 보호로 크게 나뉜다. 이는 상당 부분 프로세서에서 제공하는 하드웨어 보호 기능에 의존적이다. 서버 및 데스크톱에서 널리 사용되는 x86호환 프로세서(32비트)의 경우, 4단계 실행 레벨과 세그멘테이션, 페이징 메커니즘을 통하여 손쉽게 메모리 보호가 가능하다. 그러나 ARM과 같은 모바일 프로세서의 경우 2단계 실행 레벨 및 페이징만을 지원하고 있다. 그러므로 위 그림7과 모바일 환경에서 기존 가상화 엔진의 구조를 사용 할 경우 VMM과 가상 머신 사이의 보호는 가능하지만 가상 머신 내의 커널과 사용자 프로세스 사이의 메모리 보호에는 어려움이 따른다. 그러므로 기존 메모리 맵을 따를 경우 완벽한 형태의 Secure execution 기술의 지원이 어렵다.

그러나 제안하는 가상화 엔진은 위 그림과 같이 커널/사용자 주소공간 분리 기술을 이용하여 게스트의



〔그림 7〕 메모리 보호를 위한 메모리맵 비교

커널과 사용자 프로세스가 독립적인 가상 주소 공간에서 동작한다. 그러므로 VMM과 가상 머신간의 보호는 하드웨어 지원을 통하여 가능하며 가상 머신 내의 사용자 프로세스가 임의로 커널 영역에 대한 접근이 불가능하므로 앞서 언급한 가상 머신에서의 메모리 보호가 추가적인 하드웨어 지원 없이도 가능하다. 이를 통해 Secure execution에서 요구하는 가상화 기술간의 격리를 효과적으로 지원 할 수 있다.

4.3 프로세스 은닉기술을 이용한 보안기술

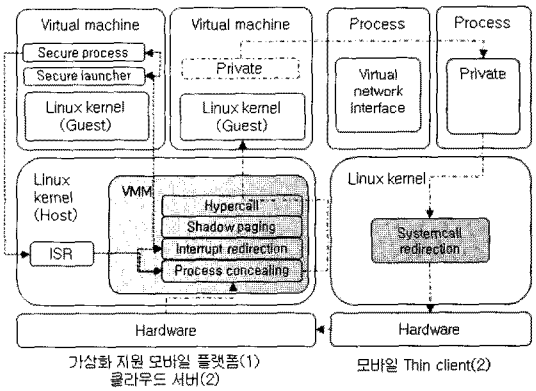
제안하는 프로세스 은닉기술은 가상화 환경 내에서 특정 프로세스를 보호하기 위한 기술이다. 본 기술은 VMM에 의한 가상 머신 내의 특정 프로세스를 다른 악의적인 프로세스로부터 보호하는 기술과 모바일 클라우드 환경에서 원격지 클라우드 서버에 있는 특정 프로세스를 보호하는 기술로 나눌 수 있다.

먼저, VMM에 의한 가상 머신 내의 특정 프로세스를 보호하는 기술로는 2008년 VMware에서 제안한 Overshadow라는 기술이 있다[20]. 이 기술은 Intel VT(Virtualization technology)를 지원하는 서버/데스크톱 환경에서 특정 프로세스를 Shim이라는 보안 프로세스 런쳐를 이용하여 런타임시 암/복호화를 통하여 가상 머신 내의 악의 적인 프로세스로부터 공격을 막는다. 또 다른 연구로는 2010년 CMU에서 제안한 TrustVisor라는 기술이 있다[21]. 본 기술을 TPM 하드웨어를 이용한 DRTM(Dynamic Root of Trust for Measurement) 제공한다. 이를 통해 보안에 민감한 프로세스의 데이터 및 코드 영역의 무결성을 제공한다. 위 두 가지 기술은 특정 하드웨어 기술에 의존적이며 모바일 환경에서 적용된 사례는 아직 없다.

클라우드 환경에서 원격지의 서버에 있는 특정 프로세스를 보호하는 기술로는 2010년 성균관대학교에서 제안한 Local execution 기술이 있다[18]. 이는 클라우드 서버 내의 관리자에 의한 보안 위협을 해결하고자 원격지 서버의 보안 프로세스의 코드 및 데이터를 런타임 시 Thin client의 로컬로 옮겨와서 실행하는 기술이다. 이를 통해 원격지의 관리자로부터의 메모리 덤프 및 기타 악의적인 프로세스로부터 안전하게 보안 프로세스를 보호 할 수 있다.

본 논문에서는 위의 두 가지 기술을 모바일 환경에 적용하였으며 구조는 다음 그림 8과 같다.

VMM에 의한 가상 머신 내 특정 프로세스를 보호하는 기술은 (1)과 같다. Secure process를 실행



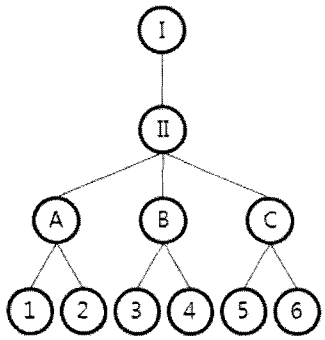
[그림 8] 제안하는 프로세스 은닉 기술

시 Secure launcher를 이용하여 메모리상에 로딩함으로써 프로세스 메모리 영역에 대한 암/복호화를 통하여 Secure process를 보호한다. Secure process는 동작 시 매번 페이지 폴트를 발생하게 되며 이는 VMM 내의 Process concealing에서 관리되며 Interrupt redirection 루틴을 통하여 Secure launcher의 복호화 과정을 통해 Secure process를 실행한다. 이는 Overshadow에서 제안한 시나리오와 유사하며 제안하는 모바일 가상화 엔진에 적용하였다.

클라우드 상에서 원격지 서버의 특정 프로세스를 보호하는 Local execution 기술은 (2)와 같다. 가상 머신 내의 Private 프로세스는 실행 시 네트워크를 통하여 Thin client에게 스택 포인터, 프로세스 시작 주소 등의 정보를 전달한다. 이를 통해 로컬 내의 프로세스는 원격지의 프로세스 컨텍스트를 가져와서 실행한다. Private 프로세스에서 페이지 폴트나 시스템 콜을 호출하는 경우, Systemcall redirection을 통하여 원격지 서버로 요청을 전달한다. 이 과정은 네트워크 패킷을 통하여 이루어지며 원격지 가상 머신 내의 커널에서는 커널 컨텍스트 관리를 통하여 요청을 처리 후 결과를 Thin client로 전달한다. 이를 통해 메모리에 로딩된 유저 공간을 안전하게 보호하는 것이 가능하다. 본 가상화 엔진에서는 기존 KVM 기반 서버 가상화 기술로 구현된 Local execution 기술을 제안하는 모바일 가상화 엔진에 적용하였다.

V. 제안 기술 검증

본 가상화를 이용한 모바일 플랫폼 보안 구조를 검증하기 위해서 우선적으로 발생 가능한 일반적인 보안



〔그림 9〕 취약성 그래프 모델

〔표 1〕 각 그래프 노드에 대한 정의

그래프노드	설명
I	클라우드 서버의 관리자
II	VMM(Virtual Machine Monitor)
A-C	가상 머신 내부의 커널
1-6	가상 머신 내부의 사용자 프로세스

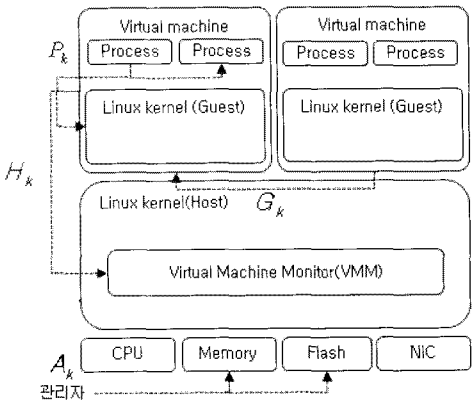
위협 유형들을 정리한다. 이를 통하여 발생 가능한 보안 위협들을 정리하고 관련 연구에서 제안하는 기술들과 제안하는 기술의 보안 범위와 제약 및 장단점 분석 비교 분석한다. 다음은 모바일 클라우드 환경까지 고려한 일반적인 취약성 그래프 모델을 보인다.

본 그래프의 최상위 루트인 관리자 I는 VMM 및 각각의 가상 머신에 대한 권한을 모두 갖는다. 이는 모바일 클라우드 환경을 고려하였을 때의 경우이며, 일반적인 모바일 가상화에서는 관리자는 존재하지 별도로 존재하지 않으며 이 경우 개인 사용자를 의미한다. 클라우드 서버의 관리자I는 VMM을 통하여 사용자의 가상 머신을 분석 및 정보 수집을 할 수 있는 권한을 갖고 있기 때문에 개개인의 모바일 단말에 대한 모든 접근을 갖고 있어 클라우드 서버 내에서 실행하는 모든 경우에 대해서는 모두 보안상의 위협요소를 갖고 있다고 볼 수 있다.

VMM II는 각각의 가상 머신에 해당하는 하위노드에 대한 권한을 갖고 있다. VMM에 대한 취약성이 노출 될 경우 모든 가상 머신에 대한 취약점이 노출되기 때문에 VMM은 최소한의 TCB를 유지하여 보안 위협에 취약점 을 줄일 수 있는 견고한 구조를 갖어야 한다. VMM의 보안성 향상을 위해서는 하드웨어 지원 보호 기술 이용한 메모리 보호 및 특권 명령어의 실행 환경 보호 등이 이용된다.

가상 머신 내부의 커널 A-C의 경우 하위 노드인 각각의 프로세스를 관리하며 커널 자체의 이미 알려진 취약성과 다양한 기능 지원으로 인한 높은 TCB로 인해 취약점이 많다. 각각의 프로세스 1-6은 상위 노드에 대한 접근이 없으며 악의적인 공격의 대한 취약성이 가장 크다.

다음 그림은 위의 취약성 그래프 모델링을 통하여 보안 모바일 가상화 플랫폼에서 발생 가능한 보안 문제들을 정의한다.



〔그림 10〕 가상화 환경에서 발생 가능한 보안 위협 유형별 정의

위 그림과 같이, 가상 머신 내에서 악의적인 프로세스에 의한 다른 프로세스 및 커널 보안 위협을 Pk, 다른 가상 머신에 의한 가상 머신 자체의 보안 위협을 Gk, 가상 머신에 의한 VMM의 보안 위협을 Hk, 모바일 클라우드 시스템에서 외부 관리자에 의한 보안 위협을 Ak로 정의하여 모바일 가상화 플랫폼 상에서 발생 가능한 보안 위협을 정의하였다.

다음은 위 그림을 바탕으로, 기존 플랫폼 보안 연구와 본 제안 기술에 대한 보안 기술 비교 평가표를 보인다.

〔표 2〕 세부 보안 기술 비교

	P_k	G_k	H_k	A_k	HW지원 필요
백신	O	X	X	X	X
MTM	O	O	X	X	O
PCPP	O	X	X	X	X
Trust zone	O	O	X	X	O
Secure execution	O	O	O	X	△
제안기술	O	O	O	O	X

위 표와 같이, 백신의 경우는 악의적인 프로그램으로부터 프로세스 및 커널만을 보호하는 기술이다. 그러므로 가상화 환경에서의 다른 보안 문제에는 대응이 불가능하다. MTM을 이용한 보안 기술은 모바일 디바이스 내에 MTM 하드웨어 보안 모듈을 지원해야하며 이를 이용한 프로세스 보안과 DRTM을 사용한 가상 머신간 보호가 가능하다.

PCPP를 이용한 보안 기술은 프로세스 보안 기술이라는 관점에서는 기존 백신과 같을 수 있으나, 이는 원격지 상의 프로세스를 보호하는 기술로써 백신과 다른 방법의 프로세스 보호 기술이다. 그러나 PCPP는 가상화 및 클라우드 컴퓨팅을 고려하여 제안된 것은 아니기 때문에 원격지 프로세스 보호라는 장점이 있는 반면 다른 보안 기술로는 대체가 불가능하다.

Trustzone을 이용한 보안 기술은 프로세스 차원에서 보안 실행 모드를 지원함에 따라서 이를 이용한 프로세스 보안 및 낮은 수준의 독립된 실행 환경에 대한 보안은 가능하다. 그러나 본 기술은 가상화 환경의 기타 보안 요소를 보호하기 어려우며 다른 소프트웨어 보안기술과 결합 할 경우 보다 더 높은 수준의 보안 기술로 응용이 가능하다.

Secure execution을 이용한 보안 기술은 가상 머신 내의 프로세스 보호 및 가상 머신 사이의 보호가 가능하며, 이를 통하여 VMM을 보호가 또한 가능하다. 보아 더 효과적인 보호를 위해서는 앞서 언급한 Trustzone과 같은 프로세서 차원의 보안 기술이 요구되며 이를 이용 할 경우 더 낮은 성능 저하를 바탕으로 안전한 실행 환경을 제공하는 것이 가능하다.

본 논문에서 제안하는 기술의 경우 커널/사용자 분리 기술을 이용하여 별도의 하드웨어 지원 없이도 Secure execution 환경을 지원한다. 또한 프로세스 은닉 기술을 통하여 모바일 클라우드 상의 원격지 프로세스 보안 기술 및 가상 머신 내의 보안 프로세스 보안이 가능하다. 정리하자면 본 제안 기술은 기타 세부 보안 기술을 상당부분 수용했다는 점에서 이전 연구들을 이용한 보안 융합 기술로도 볼 수 있다.

VI. 결 론

모바일 장치의 성능향상과 네트워크 인프라의 확산, 다양한 사용자 애플리케이션의 지원으로 모바일 플랫폼은 최근 스마트폰을 통하여 빠르게 보급되고 있다. 이러한 모바일 환경의 변화는 다양한 선 작용과 동시에 가장 큰 문제로 보안 문제를 야기하고 있다. 여러 가지 보안을 위한 기술들이 제안되고는 있으나 모바일 플랫폼을 위한 대부분의 기술이 제한적인 환경에서 활용이 가능하다는 단점이 있다.

본 논문에서는 최근 주목받고 있는 가상화 기술을 이용하여 모바일 플랫폼에서 가상 머신 보안 기술과 프로세스 은닉 기술을 제안하였다. 이를 통하여 추가적인 하드웨어의 지원 없이도 모바일 플랫폼의 보안 수준을 높일 수 있었다. 이후 연구로는 가상화 환경에서 보다 효율적인 보안 기술을 제공하기 위하여 최근 주목받고 있는 보안 하드웨어 기술을 이용한 모바일 플랫폼 보안 기술을 연구 할 계획이다.

참고문헌

[1] 김기영, 강동호, "개방형 모바일 환경에서 스마트폰 보안 기술," 정보보호학회지, 19(5), pp. 21-28, 2009년 10월.

[2] A.D. Schmidt, H.G. Schmidt, L. Batyuk, J.H. Clausen, S. A. Camtepe, and S. Albayrak, "Smartphone malware evolution revisited: android next target?," Proceedings of the IEEE International Conference on Malicious and Unwanted Software, pp. 1-7, Oct. 2009.

[3] A. Joshi, S.T. King, G.W. Dunlap, and P.M. Chen. "Detecting past and present intrusions through vulnerability specific predicates," Proceedings of the 12th ACM Symposium on Operating Systems Principles, pp. 91-104, Oct. 2005.

[4] M. Kim, H. Ju, Y. Kim, J. Park and Y. Park, "Design and implementation of mobile trusted module for trusted mobile computing," IEEE Transactions on Consumer Electronics, vol. 56, no. 1, pp. 134-140, Feb. 2010.

[5] T. Alves and D. Felton, "Trustzone: integrated hardware and software security," ARM white paper, July 2004.

[6] T. Morris and V. Nair, "PCPP: private computing on public platforms a new paradigm in public computing," Proceedings of the IEEE International Symposium on Wireless Pervasive Computing,

pp. 230-235, Feb. 2007.

[7] 김정한, 김인혁, 민창우, 엄영익, "모바일 가상화 기술 동향," 정보과학회지, 28(6), pp. 35-42, 2010년 6월.

[8] 김인혁, 김태형, 김정한, 임병홍, 엄영익, "시스템 보안을 위한 가상화 기술 활용 동향," 정보보호학회지, 19(2), pp. 26-34, 2009년 4월

[9] E. Ryu, I. Kim, J. Kim, and Y. Eom, "MyAV: an all-round virtual machine monitor for mobile environments," Proceedings of the IEEE International Conference on Industrial Informatics, pp. 657-662, July 2010.

[10] R.P. Goldberg, "Survey of virtual machine research," IEEE Computer Magazine, vol. 7, no. 6, pp. 34-45, June 1974.

[11] K. Barr, P. Bungale, S. Deasy, V. Gyuris, P. Hung, C. Newell, H. Tuch and B. Zoppis, "The VMware mobile virtualization platform: is that a hypervisor in your pocket?," Proceedings of the ACM SIGOPS Operating Systems Review, pp. 124-135, Dec. 2010.

[12] VirtualLogix Inc. VirtualLogix VLX for Mobile Handsets, Online at http://www.virtuallogix.com/products/vlx-for-mobile-handsets.html

[13] G. Heiser and B. Leslie, "The OKL4 microvisor: convergence point of microkernels and hypervisors," Proceedings of the ACM Asia-pacific Workshop on Systems, pp. 19-23, Aug. 2010.

[14] J. Hwang, S. Suh, S. Heo, C. Park, J. Rye, S. Park and C. Kim, "Xen on ARM: system virtualization using xen hypervisor for ARM-based secure mobile phones," Proceedings of the International Conference on Consumer Communications and Networking Conference, pp. 257-261, Jan. 2008.

[15] S. Pearson and B. Balacheff, Trusted computing platforms, Prentice Hall, 2003.

[16] J. Greene, "Intel trusted execution technology," Intel Corporation, 2010.

[17] 김학영, 민옥기, 남궁한, "모바일 클라우드 기술 동향," ETRI 전자통신동향분석, 제3호, 2010년 6월.

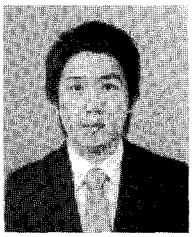
[18] 김태형, 김인혁, 김정한, 민창우, 김지홍, 엄영익, "클라우드 컴퓨팅 환경에서 보안성 향상을 위한 로컬 프로세스 실행 기술," 정보보호학회논문지, 20(5), pp. 69-79, 2010년 10월.

[19] 김정한, 김지홍, 엄영익, "MyAV 가상화 엔진을 이용한 안드로이드 모바일 플랫폼 가상화 기술," 2010년도 대한임베디드공학회 추계학술대회, pp. 22-23, 2010년 11월

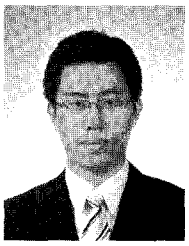
[20] X. Chen, T. Garfinkel, E. Lewis, P. Subahmanyam, C. Waldspurger, D. Boneh, J. Dwoskin and D. Ports," Overshadow: a virtualization-based approach to retrofitting protection in commodity operating systems," Proceedings of the International Conference on Architectural Support for Programming Languages and Operating Systems, pp. 2-13, March 2008.

[21] J. McCune, Y. Li, N. Qu, Z. Zhou, A. Datta, V. Gligor and A. Perrig, "TrustVisor: efficient TCB reduction and attestation," Proceedings of the IEEE Symposium on Security and Privacy, pp. 143-158. May 2010.

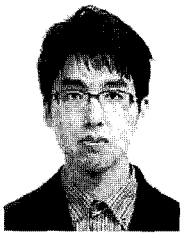
〈著者紹介〉



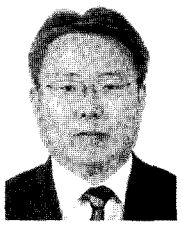
김 정 한 (Junghan Kim) 학생회원
2008년 2월: 세종대학교 컴퓨터소프트웨어공학과 졸업
2010년 2월: 성균관대학교 전자전기컴퓨터공학과 석사
2010년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 박사과정
〈관심분야〉 시스템보안, 가상화, 운영체제



김 지 홍 (Jee-hong Kim) 학생회원
2008년 2월: 광운대학교 전자공학과 졸업
2010년 2월: 광운대학교 전자공학과 석사
2010년 3월~현재: 성균관대학교 휴대폰학과 박사과정
〈관심분야〉 시스템보안, 가상화, 운영체제



신 은 환 (Eunhwan Shin) 학생회원
2010년 2월: 성균관대학교 컴퓨터공학과 졸업
2010년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 시스템보안, 가상화, 운영체제



엄 영 익 (Young Ik Eom) 종신회원
1983년 2월: 서울대학교 계산통계학과 졸업
1985년 2월: 서울대학교 전산과학과 석사
1991년 8월: 서울대학교 전산과학과 박사
2000년 9월~2001년 8월: Dept. of Info. and Comm. Science at UCI 방문교수
1993년 3월~현재: 성균관대학교 정보통신공학부 교수
〈관심분야〉 시스템소프트웨어, 미들웨어, 가상화, 시스템보안