http://dx.doi.org/10.3745/KIPSTC.2011.18C.5.293

모바일 플랫폼에서 MTM을 이용한 보안영역 제공 및 인증에 관한 연구

이 선 호[†] · 이 임 영[††]

요 약

무선 통신 기술의 발달을 통해 스마트폰을 이용한 다양한 정보 서비스를 빠르게 받을 수 있게 되었다. 스마트 폰은 기존에 사용되고 있던 피처폰에 비하여 더 강력한 컴퓨팅 능력을 제공하며, 웹서핑, 문서 편집, 비디오 시청 그리고 게임과 같은 다양한 기능을 제공한다. 스마트폰의 높은 활용성에 따라 수많은 개인정보가 단말기에 저장되고 있으며, 이의 분실 및 도난에 따른 개인정보 유출은 큰 문제가 될 것으로 예상된다.

따라서 본 연구는 기존에 제공되는 스마트폰 모바일 플랫폼의 보안영역 제공 및 인증 방법에 대하여 분석하고 요구사항을 도출하였으며, 보안 요구사항을 만족하는 보안 기술을 제안한다. 제안방식은 인증 우회가 불가능한 보안영역을 제공하며, 보안영역에 접근하기 위해 필요한 정보의 손상으로부터 가용성을 제공한다.

키워드 : 모바일 플랫폼, 보안영역, 인증

A Study on Providing Secure Storage and User Authentication Using MTM on Mobile Platform

Sun-Ho Lee[†] · Im-Yeong Lee[††]

ABSTRACT

The various information services can be delivered by smartphone through advanced high-speed mobile communication. A smartphone is a mobile device that offers more powerful computing capacity than feature phone. Therefore this device can provide such as web surfing, editing documents, playing video, and playing games. A lot of personal information stored on smartphone. Because it has High usability. Personal information Leaks if the smart phone is lost or stolen may become a big problem.

In this paper we have analyzed existing method for providing secure storage and user authentication on mobile platform and derived security requirement. Therefore we propose the following scheme that satisfy security requirement. Proposed scheme providing secure storage with preventing authentication bypass, and availability from damaged data to access secure area.

Keywords : Mobile Platform, Secure Storage, Authentication

1. 서 론

이동통신은 사용자가 무선단말기를 통해 음성이나 영상, 데이터 등을 장소에 구애받지 않고 이용할 수 있도록 이동성을 제공하는 통신 서비스를 말한다. 국내에서는 1984년 단순 음성 통신서비스를 제공하는 FDMA(Frequency Division Multiple Access)기반 1세대 이동통신 서비스를 시작으로 CDMA(Code Division Multiple Access)기반의 2세대, IMT(International Mobile Telecommunication)-2000의 3세대를 거쳐 현재 음성과 영상뿐만 아니라, 데이터 통신을 제공하는 3.5세대 이동통신 서비스가 제공되고 있다.

이와 같은 이동통신의 발달과 함께 이동통신 서비스를 제공하는 단말기 또한, 빠르게 발전하였다. 단순 통신 기능만을 제공하는 바널라폰을 시작으로 모바일뱅킹, 게임 등의 기능을 제공하는 피처폰이 대중적으로 사용되었으며, 현재 스마트폰이 출시되어 많은 사용자로부터 각광을 받고 있다. 스마트폰은 일반 모바일 단말기와 다르게 OS를 내장하여 사용자가 App스토어에서 다양한 응용프로그램을 설치해 사용할 수 있는 차별화된 서비스를 제공하고 있다[10].

스마트폰은 사용자의 생활에 밀접한 기능들을 제공하여 기존 무선단말기에 비하여 민감한 개인 정보 및 주요정보가 단말기에 빈번히 저장되고 있다. 따라서 이를 분실 및 도난

† 준 회 원 : 순천향대학교 컴퓨터학부 박사과정
†† 종신회원 : 순천향대학교 컴퓨터소프트웨어학과 교수
논문접수 : 2011년 4월 11일
수 정 일 : 1차 2011년 5월 30일
심사완료 : 2011년 5월 30일

당하게 될 경우 스마트폰에 저장되어 있는 연락처, 사진, GPS 좌표 목록, 문자 및 통신 목록 등 사용자의 개인 정보와 주요 정보가 유출될 수 있는 심각한 문제성을 가지고 있다. 현재 이를 해결하기 위한 보안 솔루션이 요구되고 있으며, 다양한 기술이 연구되고 있다.

모바일 환경에서 안전성을 제공하기 위한 방법으로 현재 신뢰컴퓨팅 기술이 연구되고 있다. 신뢰컴퓨팅은 컴퓨팅 능력을 가지는 단말기가 의도된 대로 동작할 수 있도록 신뢰성을 부과하는 기술로서 하드웨어 기반의 보안 칩을 신뢰의 근원으로 사용 한다[4]. 현재 신뢰 컴퓨팅 관련 표준을 정의하는 단체인 TCG(Trusted Computing Group)에서 모바일 환경에서 신뢰의 근원으로 활용할 수 있는 MTM(Mobile Trusted Module)을 개발하였으며, 이는 차후 다양한 모바일 기기에 적용될 것으로 전망된다[5].

본 논문에서는 이러한 신뢰 컴퓨팅기술을 무선단말기에 제공하는 MTM을 이용하여 무선단말기의 주요 정보 유출 방지를 위한 안전한 저장소 제공기술을 제안한다. 또, 보안영역에 접근하기 위해 필요한 보안영역 정보 복호화 키를 생성하기 위한 복구 값을 모바일 서비스 제공자에게 안전하게 위탁, 사후 이를 통하여 복호화 키를 생성하는 사용자 인증기술을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 모바일 플랫폼에서 안전한 사용자 인증을 위해 필요한 보안요구사항을 도출하고 3장에서는 기존에 제공되고 있는 무선단말에서의 안전성 제공에 관련된 연구를 분석하며, 4장에서는 보안요구사항을 만족하는 방식을 제안한다. 5장에서는 제안방식을 분석하며, 마지막으로 6장에서 결론을 맺도록 한다.

2. 보안요구사항

모바일 플랫폼에서는 기존의 무선단말기와 달리 개인정보 및 주요 자료가 저장되는 사례가 빈번함에 따라 무선단말기에 저장되는 데이터에 보안이 제공되어야 한다. 따라서 다음과 같은 요구 사항을 고려해야 한다.

• 기밀성(Confidentiality)
개인정보 및 민감한 정보자원은 정당한 객체만이 확인할 수 있어야 한다. 또한, 서비스 제공자에게 저장되는 무선단말 보안영역 정보 복호화 키를 생성하기 위한 복구 값으로부터 복호화 키의 평문을 유추할 수 없도록 하는 기밀성이 제공되어야 한다.

• 무결성(Integrity)
사용자 인증 값 및 데이터 암호화 등에 사용되는 킷값은 위/변조되거나 파괴되지 않도록 해야 한다. 만약 위조, 삭제 및 변화가 되었다면 그 사실을 확인할 수 있어야 한다.

• 인증(Authentication)
Sandbox의 허술한 규칙과 탈옥 등을 통하여 인증되지 않은 사용자가 주요 자료에 접근하는 것을 차단해야 하며, 그 신원이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다.

• 접근제어(Access Control)
개인 정보 및 민감한 정보자원에 대한 읽기나 변경 등의 모든 접근 행위에 대해 그 권한을 명백히 구분해 허가되지 않은 접근시도를 사전에 차단할 수 있도록 하는 통제가 필요하다. 인증 우회를 통한 정보자원의 접근을 제어하기 위해 분리된 저장 공간이 제공되어야 한다.

• 효율성(Efficiency)
무선단말기에 제공되는 제한적인 컴퓨팅 능력을 고려해야 하며, 과도한 연산으로 인한 배터리 소모를 줄이기 위해 서비스 제공에 요구되는 연산량의 효율성이 제공되어야 한다.

• 가용성(Availability)
다양한 모바일 플랫폼에 적용 가능해야 한다. 또, 저장소 접근을 위해 필요한 키가 손상되지 않아야 하며, 손상되어도 지속적인 서비스를 제공할 수 있어야 한다.

3. 기존 연구

스마트폰에서 제공되는 다양한 서비스로 인하여 기존의 모바일 단말에 비하여 스마트폰에 저장되는 개인 정보의 비율이 상당히 높아지고 있다. 따라서 스마트폰의 도난 및 분실, 모바일 악성코드 등으로 단말기에 저장된 개인정보가 유출되는 것을 방지하기 위해 데이터를 보호하고 접근을 제어하는 보안기술이 적용되고 있다. 본 장에선 이러한 기술들에 대해서 알아보고 분석하고자 한다.

3.1 Sandbox 기술

먼저 모바일 플랫폼에서 애플리케이션 및 데이터에 대한 접근제어를 위해 사용되는 기술 Sandbox에 대하여 알아보도록 한다. 컴퓨터 보안에서 Sandbox란 응용프로그램을 분리 시켜 구동시키는 것을 말한다. 즉, 외부의 프로그램이 단절된 영역에서만 동작하여 시스템의 자원에 함부로 접근하거나 부정하게 조작, 다른 응용프로그램의 데이터에 접속하는 것을 방지하는 기술로서 검증되지 않은 코드라던가 신뢰할 수 없는 업체 혹은 사람으로부터 개발된 프로그램을 실행할 때 자주 사용된다. 일반적으로 디스크 및 메모리에서 게스트 프로그램의 실행을 위해 강력하게 제어된 자원을 제공하며, 네트워크 접근, 호스트 시스템을 검사하거나 입력장치로부터의 읽기 동작은 일반적으로 강력하게 제한된다. 이러한 Sandbox기술은 Applets, Jail, Rule-based Execution, Virtual machine, Sandboxing on native hosts, Capability system, Online judge와 같은 예를 가지고 있다.

안드로이드 OS에서 Sandbox는 App들 간의 서로의 영역을 침범할 수 없도록 하는 기술로 활용된다. App이 설치되

는 시점에서 안드로이드 OS는 각 App에 고유의 UID, GID를 부여하여 각각의 권한으로 실행되도록 한다. 즉, App들은 리눅스에서 서로 다른 사용자가 상대방의 작업에 관여하지 못하는 것과 같이 실행되는 것이다. 이러한 App들은 루트디렉토리에 있는 "AndroidManifest.xml"에 서비스를 등록한다. 이는 App이 단말이 가지는 다양한 정보 자원에 접근하기 위한 권한을 표현하고 있다. "AndroidManifest.xml"의 경우 루트권한을 획득하면 얼마든지 xml파일을 추출 및 조작할 수 있는 보안 취약점을 가지고 있다[11].

iPhone역시 안드로이드와 유사한 Sandbox기술을 적용하고 있다. App스토어에서 다운 받아 설치된 각종 응용프로그램들은 무선단말기 저장소 안의 "/private/var/mobile/Applications/"에 설치되고 서로 다른 프로그램들을 보는 것을 방지한다. iPhone의 Sandbox기술은 커널레벨에서 구현되며 SandboxTemplate.sb라는 파일에 표시된 일련의 규칙을 따르게 된다. 해당 규칙에 따라 무선단말기의 응용프로그램들은 "sandboxed"되어 다른 응용프로그램에서 저장한 데이터에 접근할 수 없다. 또한, 시스템 파일, 리소스, 그리고 커널은 사용자의 응용프로그램 공간으로부터 단절되어 있다고 말하고 있다. 하지만 실제로 수많은 시스템과 응용프로그램의 환경 설정 파일이 읽을 수 있다는 사실이 밝혀졌다[12].

설정 파일을 기반으로 하는 Sandbox 기술의 경우 다양한 포렌식 기반 기술을 통하여 우회가 가능하게 된다. 따라서 설정파일의 유출 및 조작으로부터 개인 정보 및 주요자료 유출을 방지 할 수 있는 분리된 저장 공간이 필요하다.

3.2 KeyChain 기술

핸드폰에 저장된 데이터들을 사용자 인증 없이 PC와 연결해 직접 접근하는 것을 방지하기 위해 모바일 플랫폼에서는 KeyChain을 사용해 저장소를 암호화한다.

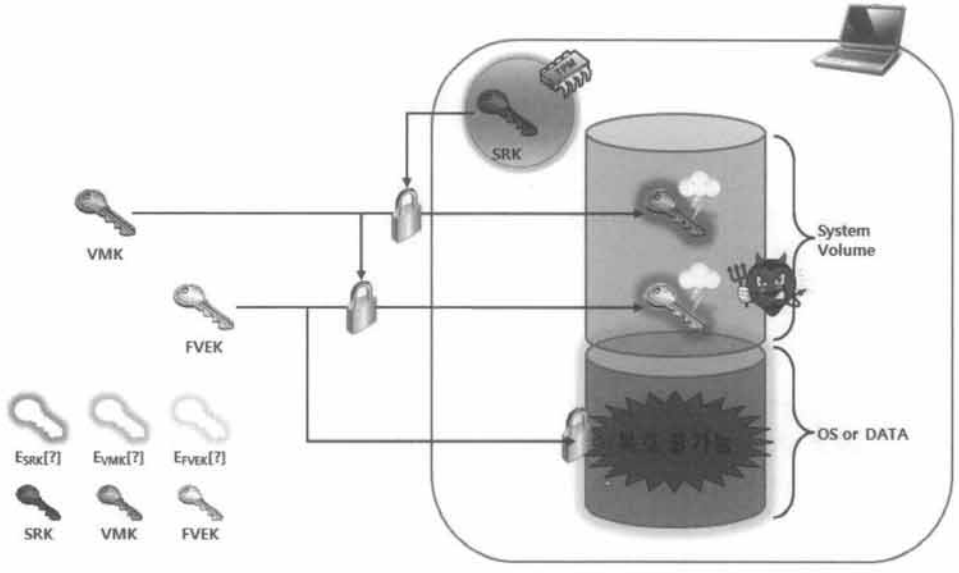
iPhone의 경우 KeyChain방식을 이용하여 사용자에게 투명한 인증을 제공하고 있다. 모든 응용프로그램은 사용자의 로그인 계정을 통해 인증을 제공한다. 기본적으로 Mac OS의 로그인 계정으로 로그인을 했을 시 로그인 계정의 비밀번호를 KeyChain에 입력하고, 차후 같은 응용프로그램을 이용할 경우 별도의 로그인 절차 없이 자동으로 KeyChain에서 비밀번호를 찾아 인증을 시도한다.

KeyChain에는 각 응용프로그램과 Mac OS에서 사용하는 모든 동작들의 패드워드가 입력되어 있으며 사용자는 자신이 사용하고자 하는 응용프로그램과 KeyChain의 패스워드를 입력하면 KeyChain에 저장되어있는 비밀번호가 자동으로 각 응용프로그램에 전달되어 인증 절차가 수행된다. KeyChain 패스워드는 Mac OS에서 자동으로 부여되는 패스워드로 수정되지 않고, 사용자는 별도의 KeyChain 패스워드를 입력하지 않아도 자동으로 인증되어 KeyChain을 이용할 수 있다.

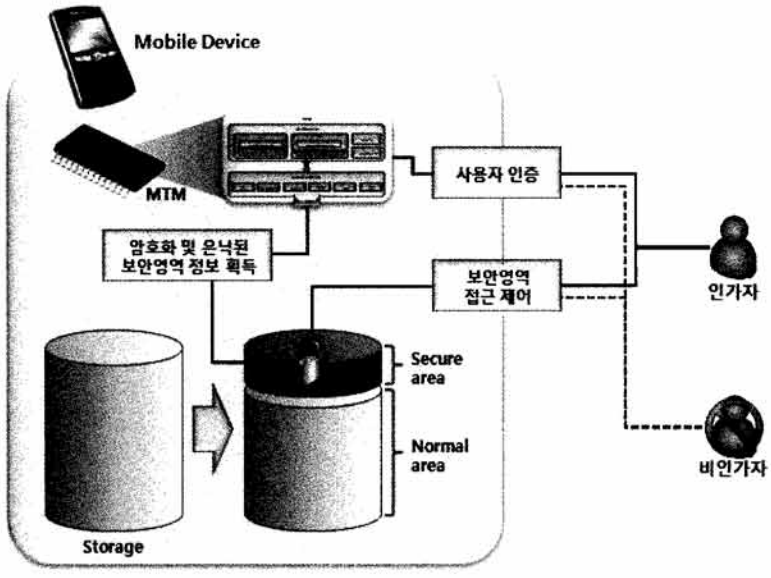
사용자가 iPhone의 데이터를 백업하면 KeyChain 데이터는 백업파일에 KeyChain의 패스워드를 키로 사용하여 암호화되어 있다. 그러나 KeyChain의 패스워드는 백업파일에 포함되지 않는다. 따라서 백업파일을 다른 iPhone에 전송하여도 KeyChain의 키가 없기 때문에 백업파일을 복호화 할 수 없다. 이러한 이유로 KeyChain은 보안 웹 사이트에 로그인 정보와 기타 데이터를 저장하기 위하여 사용되고 있다. 하지만 McAfee의 연구원 Jonathan Zdziarski는 이를 우회할 수 있음을 보여주었다[14].

3.3 Bit-Locker 기술

모바일플랫폼에서 이용되는 기술은 아니지만 TPM을 사용하여 PC에서 강력한 사용자 인증 및 데이터 접근제어를 제공하는 기술인 Bit-Locker에 대하여 알아보도록 한다. Bit-Locker는 Microsoft의 운영체제인 Windows Vista 및 Windows 7에서 사용되는 TPM 기반의 디스크 암호화 솔루



(그림 1) Bit-Locker 구조 및 취약점



(그림 2) 제안방식 개념도

션으로서 TPM(Trusted Platform Module)을 사용하여 사용자 인증 및 디스크의 암호화를 수행하여 앞의 두 방식과 다르게 강력한 안전성을 제공한다.

해당 기술은 디스크를 보호하기 위해 256bit의 FVEK (Full Volume Encryption Key)를 이용한 AES암호화를 이용하며, 암호화에 사용되는 키들은 TPM에 의해 보호되며 해당 TPM에 의해서만 복호화가 가능하여, 암호화키의 노출을 방지하였다. 그 밖에 FVEK를 보호하기 위해 256bit 대칭키 VMK(Volume Master Key)가 사용되며 VMK는 TPM 저장소의 암호키인 2048bit 공개키 SRK(Storage Root Key)로 암호화 되어 있는 구조를 가지고 있다. 하지만 해당 구조는 공격자에 의해 TPM 외부에 저장되어 있는 VMK나 FVEK가 손상될 경우 암호화된 파티션을 복호화 할 수 없는 가용성의 문제를 가지고 있다(그림 1 참조). 따라서 안전한 저장소에 접근하기 위해 필요한 키가 손상될 경우 이를 복원할 수 있는 기술이 요구된다.

4. 제안방식

본 장에선 MTM과 무선단말기의 파일시스템 구조를 이용하여 앞서 도출된 보안 요구사항을 만족하는 데이터 보호 기술을 제안한다. 제안방식은 여러 플랫폼에 독립적으로 동일한 구조를 가지는 파일시스템의 구조를 이용하였기 때문에 다양한 플랫폼에 본 보안기술을 적용할 수 있는 장점을 가진다.

제안방식은 무선단말기 저장소의 파티션을 2개로 분할하여 그중 하나의 파티션 정보를 암호화하여 숨겨진 보안영역으로 이용한다. 오직 MTM을 이용한 인증에 통과한 사용자만이 보안영역의 파티션 정보를 획득, 해당 정보를 통하여 보안영역에 접근 가능하며, 비인가자 및 공격자는 보안영역의 정확한 위치와 정보를 획득하지 못해 접근하지 못하도록 하는 구조를 가지고 있다(그림 2 참조). 또한 제안방식은 BitLocker에서 키가 공격을 당하였을 경우 저장소에 접근하지 못하는 문제를 해결하기 위해서 보안영역에 접근하기 위한 복호화 키를 복구하는데 필요한 값을 서비스 제공자에게 위탁하고, 이를 사용자 인증 시 요청하여 MTM에 안전히 저장된 값과 함께 보안영역의 정보를 복호화 할 수 있는 키를 생성하도록 한다. 이는 무선단말기가 항상 네트워크에 연결되어 있는 환경을 고려하여 제안되었다.

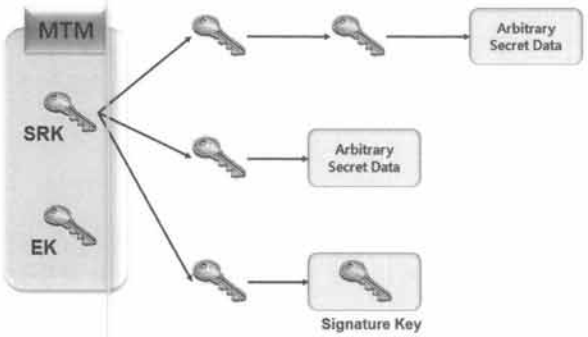
4.1 관련연구

무선단말에서 안전한 보안영역 제공을 위해서 MTM의 기능, 저장소의 논리구조, 겹선형 사상에 대한 연구를 진행하였으며, 해당 내용을 활용하여 모바일 플랫폼에서 MTM을 이용한 보안영역 제공 및 인증 방법을 제안하였다.

4.1.1 Mobile Trusted Module

MTM은 모바일 환경에서 신뢰 컴퓨팅 환경을 구축하기 위해서 TCG의 MPWG(Mobile Phone Working Group)에 의해 표준화된 모바일 TPM이다. 이는 TPM을 기반으로 하여 기본적 구성과 기능이 매우 흡사하며 TPM과 명령어 역시 호환가능하다.

MTM은 무선단말기에 보안성을 제공하기 위해 플랫폼 무결성 검증, 디바이스 인증, 데이터 보호, 안전한 통신채널 생성, 모바일 지불과 같은 다양한 서비스 모델을 가지고 있다. 특히 제안방식에서는 보안영역 정보 보호 및 사용자 인증을 위해 MTM의 데이터 보호기술을 활용하며, 해당 내용은 다음과 같다. MTM은 2048비트의 개인키/공개키 쌍으로 구성되어 있는 EK(Endorsement Key)와 SRK를 내장 하고 있다. 즉 이 두 개의 키는 MTM 내부에서만 참조되며, 안전하게 저장되어 신뢰의 근원이 된다. MTM은 저장소를 위한 최상위 키인 SRK를 이용하여 (그림 3)과 같이 하위 키들을



(그림 3) MTM의 키관리 구조도

암호화 저장하고 하위 키들로 데이터를 암호화 저장하여 개념적으로 무제한의 보호된 저장소를 제공하는 역할을 수행한다[4].

4.1.2 저장소의 논리적 구조

무선단말기에서 안전한 저장소 즉 보안영역을 제공하기 위해 제안방식은 단말기의 플래시 메모리가 가지는 저장소의 논리적 구조를 분석 및 이용하고자 하며, 해당 내용은 다음과 같다. 플래시 메모리 및 다양한 저장매체는 모두 섹터라 불리는 512Byte의 구조체로 구성이 되어 있다. 이중 저장매체의 첫 번째 섹터인 MBR(Master Boot Record)은 해당 저장매체가 가지는 파티션의 정보를 표현하는 4개의 파티션 테이블을 가지고 있다(그림 4 참조). 저장소에 접근하는 장치는 각 저장소의 MBR을 참조하여 각 파티션을 논리 드라이브로 인식한다.

4.1.3 겹선형 사상

겹선형 사상(bilinear map)은 본래 타원곡선 상의 이산대수 문제를 유한체상의 이산대수 문제로 축소시켜 그 어려움을 줄여 타원곡선 암호시스템을 공격하는 도구로 제안되었다. 하지만 최근에는 공격 도구가 아닌 정보보호를 위한 암호학적 도구로 사용되고 있으며 제안방식에서는 다음과 같은 겹선형 사상의 계산가능(Computable)한 특성을 활용하여 사용자인증에 발생되는 연산을 경량화 한다.

$$e(aP,bQ) = e(P,bQ)^a = e(aP,Q)^b = e(P,Q)^{ab} = e(abP,Q) = e(P,abQ)$$

- q : 매우 큰 소수
- G_1 : 위수가 q인 타원곡선 위의 덧셈군
- G_2 : 위수가 q인 유한체 위의 곱셈군

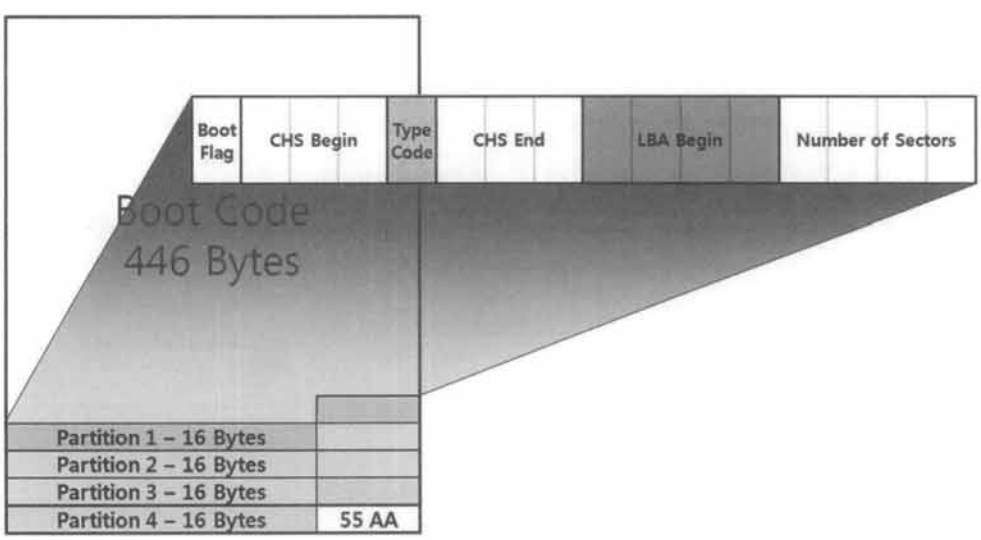
$$e : (G_1 \times G_1 \rightarrow G_2)$$

- $P, Q, R \in {}_rG_1$
- $a, b, c \in {}_rZ_q$

4.2 시스템 계수

본 제안 방식에서 사용되는 시스템 계수는 다음과 같다.

- PWD : 사용자 인증 비밀번호
- $SINF$: 보안영역 파티션 테이블 정보
- SRK : MTM의 비휘발성 메모리에 저장되는 최상위 저장소 암호화 키
- $NONCE$: 비밀번호 저장 위치의 노출을 막기 위한 난수
- $FLAG$: 보안영역 정보 시작을 알리는 특정 코드
- PCR : Platform Configuration Register
- $IMSI$: International Mobile Subscriber Identity
- SP : 서비스 제공자
- STK : 보안영역 정보 암호화 키
- RV : SP에 저장되는 STK의 복구값
- r : 임의 난수
- $H[\,]$: 안전한 일 방향 해시 함수
- $H_1[\,]$: 덧셈군 원소를 반환하는 해시함수
- $E_*[\,]$: $*$의 키로 암호화



(그림 4) MBR 및 파티션 테이블의 구조

- $D_*[\,]$: $*$의 키로 복호화
- G_1 : 덧셈군
- G_2 : 곱셈군, $G_2 \leftarrow G_1 * G_1$
- p : 큰 소수 값
- g : G_1 생성자
- x : 사용자 인증에 사용되는 개인키
- y : 사용자 인증에 사용되는 공개키
- SK : 모바일 단말의 MTM과 서버간의 상호 인증을 통해 생성된 세션키

4.3 보안영역 제공 방법

4.3.1 보안영역 설정 단계

모바일 플랫폼에서 보안영역을 설정하기 위해 다음과 같은 단계를 거친다. 해당 과정은 무선단말기에 장착된 저장소의 파일 시스템 구조를 이용한다(그림 5 참조).

Step 1. 먼저, 무선단말기의 저장소인 플래시 메모리에 보안영역으로 사용될 파티션을 생성해야 한다. 따라서 플래시 메모리의 1번 섹터에 저장되어 있는 MBR(Master Boot Record)값을 메모리로 읽어온다.

Step 2. MBR에 저장된 파티션 테이블 값을 보안영역과 일반영역으로 나누어 파티션 정보를 생성하고 각 파티션에 해당하는 파티션 테이블을 생성하여 파티션을 분할한다. 이때 일반영역의 파티션 정보만 첫 번째 파티션 테이블에 기록한다.

Step 3. 보안영역의 파티션 정보 앞에 보안영역 정보의 시작을 표시하는 플래그를 추가하고 앞뒤를 $NONCE$ 값을 붙여 예약영역에 보안영역 정보 암호화 키 STK로 암호화 저장한다. 이때 보안영역 파티션 테이블 정보의 저장 위치는 예약영역 내 랜덤 위치에 저장하여 보안영역의 정보를 은닉하게 된다.

$E_{STK}[NONCE \| FLAG \| SINF \| NONCE]$

Step 4. 무선단말기는 메모리에서 사용자 인증 값 및 암호화된 보안영역 정보가 추가된 MBR 값을 플래시 메모리에 기록, 변경된 플래시 메모리의 MBR 정보를 플랫폼에 인식 시킨다.

4.3.2 보안영역 접근 단계

사용자 인증을 거친 뒤 설정된 보안영역에 접근하기 위하여 다음과 같은 단계를 거친다. 해당 과정은 모바일 플랫폼에 장착된 저장소의 파일 시스템 구조를 이용한다(그림 6 참조).

Step 1. 무선단말기는 사용자 인증을 위해 플래시 메모리의 1번 섹터에 저장되어 있는 MBR(Master Boot Record) 값을 무선단말기의 메모리로 읽어온다. 그 뒤 무선단말기 MBR 정보의 사본을 저장한다.

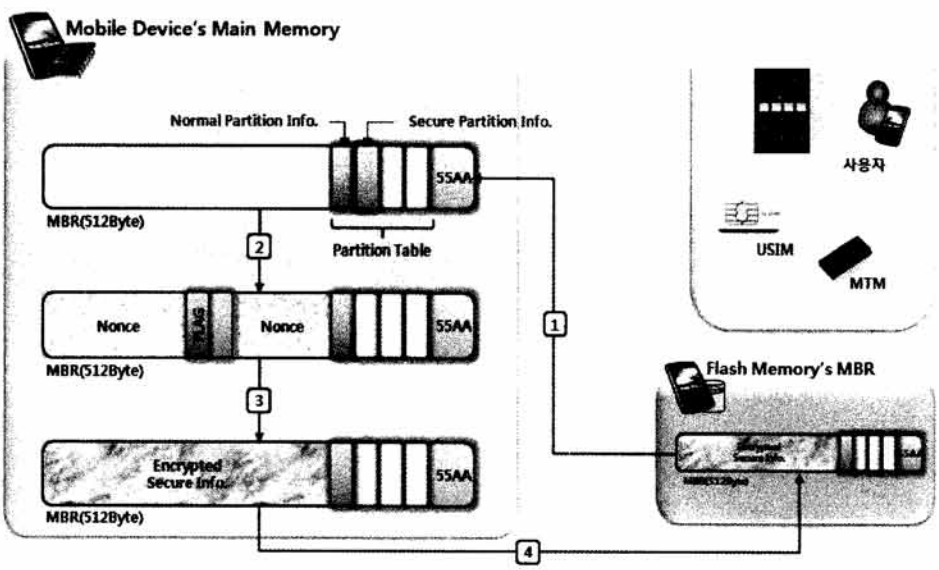
Step 2. 무선단말기는 사용자 인증과정에서 생성된 STK로 예약영역에 저장된 보안영역 정보가 포함된 암호문을 복호화 한다.

$D_{STK}[E_{STK}[NONCE \| FLAG \| SINF \| NONCE]']$
$= NONCE \| FLAG \| SINF \| NONCE$

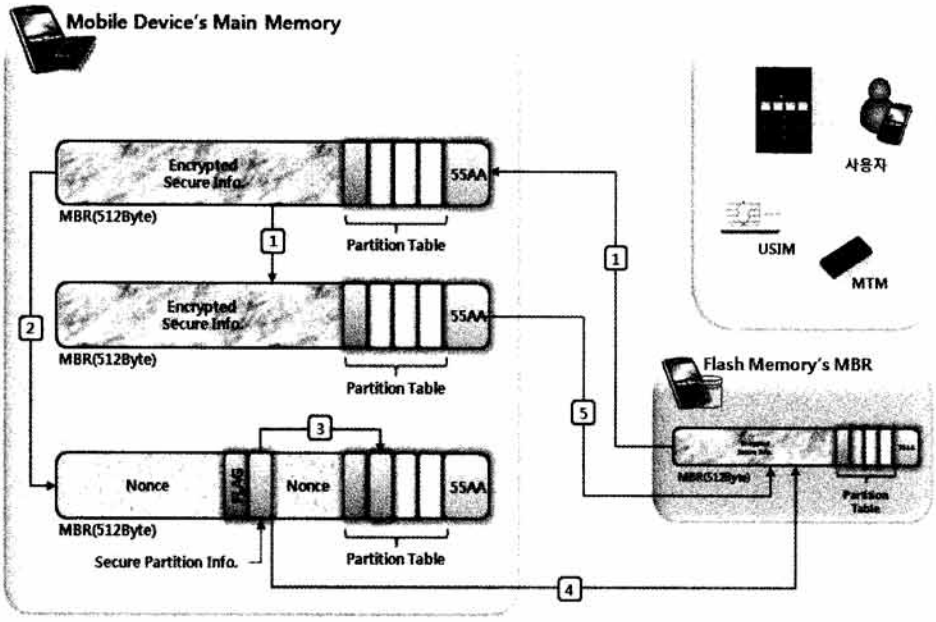
Step 3. 무선단말기는 Step 2.에서 복호화된 값에서 플래그를 추출하여 랜덤 위치에 저장된 보안영역 정보를 찾아 파티션 테이블 2번에 기록한다.

Step 4. 무선단말기는 Step 3.에서 생성된 보안영역의 파티션 정보가 기록된 MBR값을 플래시 메모리의 MBR에 기록 및 플랫폼에 보안영역 파티션을 인식하도록 한다.

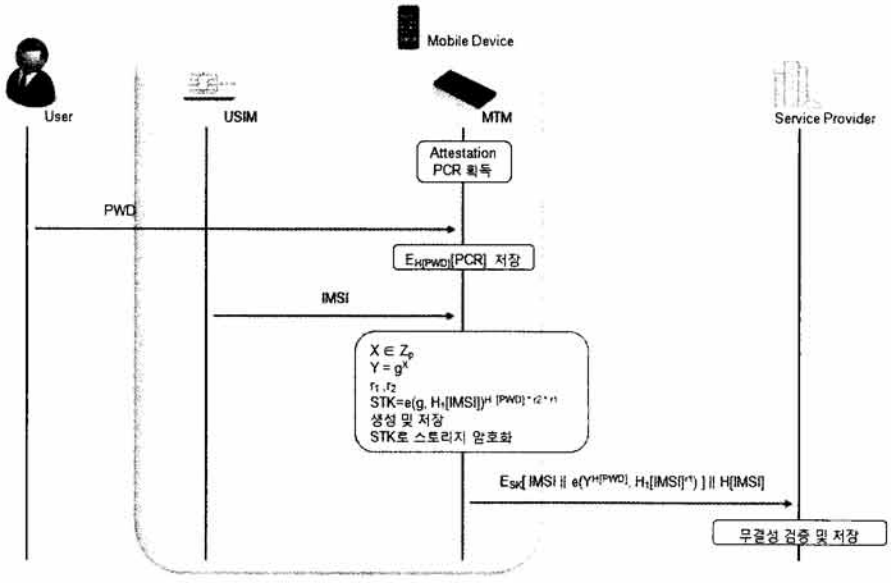
Step 5. 보안영역 파티션이 플랫폼에 정상 되었을 경우 Step 1.에서 저장한 일반영역만 기록된 MBR 사본 값을 플래시 메모리에 기록한다. 모바일 플랫폼은 변경된 MBR의 값을 재인식 요청이 오기 전까지 참조하지 않는 특성을 가지고 있다 본 방식은 이와 같은 과정을 통하여 무선단말기의 비정상 종료 및 불법 접근을 통한 보안영역 정보 유출을 방지한다.



(그림 5) 보안영역 제공을 위한 설정 단계



(그림 6) 보안영역 제공을 위한 접근 단계



(그림 7) 사용자 인증을 위한 설정 단계

4.4 사용자 인증 방법

인증된 사용자만이 보안영역에 접근하기 위해 무선단말기 환경을 고려한 안전한 사용자 인증 방법을 제안한다. 사용자 인증은 무선단말기를 통해 사용자가 인증한 비밀번호와 MTM에 안전하게 저장되어 있는 *EK*를 이용해 보안영역 정보를 복호화 할 수 있는 키 *STK*를 생성 하는 과정으로 구성되어진다.

4.4.1 설정 단계

모바일 플랫폼에서 보안영역에 인증된 사용자만 접근 가능하도록 하는 접근제어 및 인증 값 손상으로부터 가용성을 제공하기 위해 다음과 같은 설정 단계를 거친다. 본 단계는 무선단말기에 장착된 USIM과 MTM 그리고 서비스 제공자의 서버를 이용한다(그림 7 참조).

Step 1. 무선단말기에 장착된 MTM에서 플랫폼의 무결성을 확인한 뒤 해당 상태를 표현하는 *PCR* 값을 획득한다.

Step 2. 사용자가 무선단말기에 사용자 인증을 위한 비밀번호를 입력한다.

Step 3. 차후 기기 및 사용자 인증을 확인하기 위해 비밀번호의 해시 값으로 Step 1.에서 획득한 *PCR* 값을 암호화하여 MTM에 *SRK*로 암호화 저장한다.

Step 4. 무선단말기에서 USIM에 저장된 가입자 식별 정보인 $IMSI$를 추출한다.

Step 5. 사용자 인증에 사용될 키 쌍 x,y와 임의 난수 r을 생성하며, 키 쌍 x,y는 MTM에 SRK로 안전하게 암호화 저장한다.

$x \in Z_p^*$

$y = g^x$

Step 6. 주요 정보가 저장된 무선단말기기의 보안영역 정보 암호화키 STK를 생성하고 보안영역 정보를 암호화한다.

$STK = e(g, H_1[IMSI])^{H[PWD]*r}$

Step 7. 무선단말기기는 STK 값을 노출하지 않고 차후 재생성 할 수 있도록 하는 복구 값을 생성하여 MTM과 SP간의 상호인증을 통해 공유된 세션키 SK로 암호화하여 전송한다.

$RV = e(Y^{H[PWD]}, H_1[IMSI]^r)$

$E_{SK}[IMSI \| RV] \| H[IMSI]$

Step 8. SP는 무선단말기로부터 전송 받은 값을 복호화고 $IMSI$값을 통해 무결성을 검증한 뒤 비밀번호 복구 값RV를 저장한다.

4.4.2 인증 단계

설정된 보안영역에 접근하기 위해 다음과 같은 인증 단계를 거치게 되며, 본 단계는 무선단말기에 장착된 USIM과 MTM 그리고 서비스 제공자의 서버를 이용한다(그림 8 참조).

Step 1. 무선단말기에 장착된 MTM에서 PCR' 값을 획득한다.

Step 2. 사용자가 무선단말기에 사용자 인증을 위한 비밀번호를 입력한다.

Step 3. 기기 및 사용자 인증을 확인하기 위해 비밀번호의 해시 값으로 Step 1.에서 획득한 PCR' 값을 암호화한 값과 사전에 암호화 저장된 PCR값을 비교하여 기기 및 사용자 인증을 수행한다.

Step 4. 사용자 및 기기인증에 성공하면 무선단말기에서 USIM에 저장된 가입자 식별 정보인 $IMSI$를 추출한다.

Step 5. 무선단말기는 $IMSI$를 MTM과 서버가 상호인증을 통해 공유한 세션키 SK키로 암호화한 값과 $IMSI$의 해시 값을 연접하여 전송한다.

$E_{SK}[IMSI] \| H[IMSI]$

Step 6. SP는 무선단말기로부터 전송받은 값을 복호화하고 무결성을 검증한 뒤 복호화된 $IMSI$에 해당하는 비밀번호 복구 값을 검색한다.

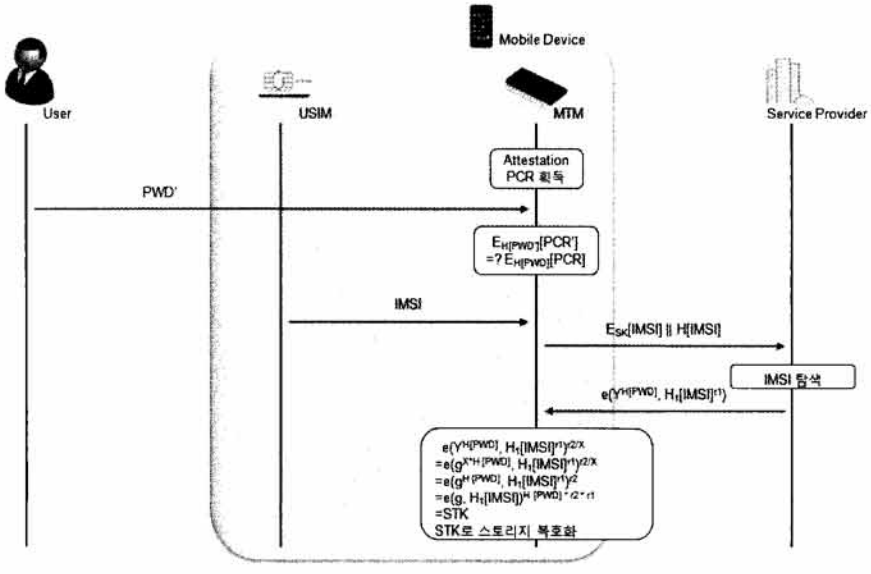
Step 7. SP는 검색된 비밀번호 복구 값 $RV = e(Y^{H[PWD]}, H_1[IMSI]^r)$를 무선단말기에게 전송한다.

Step 8. 무선단말기는 SP로부터 전송받은 비밀번호 복구 값에 $1/x$승을 하여 보안영역 정보를 복호화 할 수 있는 키 STK값을 복구하며, 해당 과정은 MTM내부에서 안전하게 진행된다.

$$
\begin{aligned}
& e(Y^{H[PWD]}, H_1[IMSI]^r)^{1/x} \\
&= e(g^{x*H[PWD]}, H_1[IMSI]^r)^{1/x} \\
&= e(g^{H[PWD]}, H_1[IMSI]^r) \\
&= e(g, H_1[IMSI])^{H[PWD]*r} \\
&= STK
\end{aligned}
$$

5. 제안방식 분석

제안 방식과 기존방식을 앞서 언급한 안전성에 대한 요구사항에 맞추어 분석한 내용은 <표 1>과 같다.



(그림 8) 사용자 인증을 위한 인증 단계

5.1 기밀성(Confidentiality)

Sandbox방식의 경우 사용자의 접근제어만 제공될 뿐 내부 데이터의 기밀성을 제공하지 않으며, KeyChain방식은 루트 키를 통하여 생성된 키들로 데이터 및 인증서, 주요자료들을 암호화하여 기밀성을 제공하고 있다.

제안방식에서의 기밀성은 사용자 인증을 위한 개인키 x를 정당한 사용자만이 알고 있다는 가정 하에 제공된다. 보안영역정보 값이 $STK = e(g, H_1[IMSI])^{H[PWD]*r}$로 암호화 되어 있어 보안영역의 정보가 평문으로 노출되지 않으며, 사용자인증 및 인증으로부터 생성된 STK로 암호화된 보안영역 정보 파티션을 복호화 하여 보안영역을 정상적으로 인식해야만 보안영역에 접근가능하기 때문에 기밀성이 제공된다. 또한, 서버에 저장되는 비밀번호 복구 값을 통해 보안영역 정보 암호키인 STK를 유추할 수 없어 서버 관리자로부터의 기밀성 또한 제공한다.

5.2 무결성(Integrity)

Sandbox방식의 경우 무결성을 제공하지 않으며, KeyChain 방식은 Hash 함수를 이용하여 데이터 및 주요 자료의 무결성 검증체계를 가지고 있다.

제안방식은 무선단말기와 서비스 제공자 간의 통신에서는 $E_{SK}[IMSI] \| H[IMSI]$와 같이 안전하게 공유된 세션키로 암호화된 $IMSI$ 및 이의 해시 값을 첨부하여 무결성이 제공된다. 서버는 이를 통해서 클라이언트로부터 온 $IMSI$의 무결성을 검증하고 이에 해당하는 비밀번호 복구 값을 전송한다.

5.3 인증(Authentication)

서비스를 이용하고자 접근하는 사용자의 신원을 정확히 확인하고, 그 신원이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다. 제안 방식은 사용자 인증을 위해 사용자만이 알고 있는 개인키 x를 통하여 인증을 제공한다.

5.4 접근제어(Access Control)

정당하지 않은 사용자는 서비스를 이용할 수 없어야 한다. Sandbox방식의 경우 Rule-based 접근제어를 제공하고 있다. 하지만 이는 수많은 시스템과 응용프로그램의 환경설정 파일을 메모리에 직접 접근을 통해 읽을 수 있다는 사실이 밝혀졌다[12]. KeyChain방식과 Bit-Locker는 데이터를 암호화하여 키를 소지하고 있는 정당한 소유자만이 데이터의 내용을 확인할 수 있어 접근제어를 제공한다.

제안 방식은 정당하게 인증을 받은 사용자만이 보안영역에 접근할 수 있도록 보안영역의 정보가 STK로 암호화 되어 있기 때문에 사용자 인증을 받지 못한 사용자는 서비스를 제공받을 수 없다.

5.5 효율성(Efficiency)

Sandbox방식은 접근제어를 위한 규칙을 표현하는 파일을 기반으로 접근제어를 제공해 구현이 용이하고 연산량이 적은 장점을 가지고 있다. 따라서 제안 방식은 연산의 효율성을 통하여 연산에 소모되는 배터리 양을 줄이는 효율성을 제공한다. 반면 KeyChain의 경우 키 구조를 생성하고 인증을 통해 접근하고자하는 데이터 복호화 키를 획득하기 위해 여러 번의 복호화 연산이 발생된다.

또, 제안방식은 무선단말기에 쉽게 적용 할 수 있는 파일시스템의 구조를 이용한 방식으로 개발비용이 저렴하고 여러 모바일 플랫폼에 적용 가능하다.

5.6 가용성(Availability)

Sandbox방식의 경우 접근제어를 관장하는 파일이 노출되

〈표 1〉 제안방식 분석

	Sandbox	KeyChain	Bit-Locker	제안방식
기밀성	×	○	○	○
	제공 안 됨	하위키를 이용한 암호화	데이터 및 키 암호화	**보안영역 정보 암호화, 비밀번호 복구 값 암호화**
무결성	×	○	○	○
	제공 안 됨	Hash함수 이용	Hash함수 이용	**Hash함수 이용**
인증	○	○	○	○
	인증 제공	인증 제공	인증 제공	**인증 제공**
접근제어	△	○	○	○
	Rule-based 접근제어, 파일에 직접접근 가능	데이터 암호화로 인한 접근제어	MTM을 이용하여 정당한 PC 및 사용자만이 접근가능	**보안영역 정보 암호화 분리된 저장소 제공**
효율성	○	△	○	○
	구현용이	키생성 연산량 증가	하드웨어 기반 암호화 연산	**파일 시스템 특성 이용, 타원곡선 이용 경량화 연산**
가용성	×	×	×	○
	접근제어 파일 손상 가능	키 정보 손상 가능	키 정보 손상 가능	**키 복구 정보 SP에 저장**

어 있어 이를 손상시키면 서비스가 정상적으로 제공될 수 없다. KeyChain방식 및 Bit-Locker 역시 데이터 암호화에 사용되는 하위 키들이 노출되어 있어, 해당 값이 손상될 경우 서비스가 제공될 수 없는 문제점이 있다. 하지만 제안방식은 MTM을 이용하여 강력한 안전성을 제공하고, 사용자 인증 값이 손상되어도 이를 복구 할 수 있어 공격자의 공격에도 지속적인 서비스가 가능하다.

6. 결 론

이동통신의 발달로 인하여 무선단말기에 동영상이나 사진, 문서 같은 콘텐츠 파일 등을 저장하고 송수신하기 쉬워졌다. 그로 인하여 사용자들은 더 높은 품질의 고용량 콘텐츠 파일을 추구하게 되었다. 최근 스마트폰 사용자가 급증함에 따라 스마트폰 내부에 저장된 개인 정보의 노출을 막기 위한 보안 솔루션에 대한 중요성이 부각되고 있다. 스마트폰을 통한 개인정보 유출의 원인 분석 결과 바이러스나 웜을 통한 유출 사고보다는 무선단말기의 분실 및 도난을 통하여 개인정보가 유출되는 것을 확인할 수 있다. 따라서 모바일 플랫폼에서의 중요 자료 보호를 위한 보안 솔루션이 필요하다.

본 연구는 무선단말기에서 필요한 데이터 보안기술을 제공하는 방안으로 활용될 수 있으며, 산업계의 경우 본 자료를 이용하여 무선단말기를 위한 보안 솔루션 제공에 대한 연구 기초 자료와 기반 연구 자료로 활용될 수 있으며, 보안기술 향상 및 경쟁력 향상에 기여할 것으로 사료된다. 또한, 제안 방식을 통해 무선단말기의 데이터 보안 취약점을 보완할 수 있는 기술을 제공, 사용자가 손쉽게 강력하고 안전한 보안 영역을 제공 받을 수 있게 되었다. 이로 인하여 안전한 무선단말기 사용의 대중화에 기여할 것으로 본다.

추후에는 더욱 편리하고 안전한 플래시 메모리 사용 환경을 위해 안전한 사용자 인증 방안 및 보안영역 제공방법에 대한 지속적인 연구가 필요하며, 사용자 인증을 위한 비밀번호 분실 시 이를 복구 할 수 있는 비밀번호 복구 서비스 제공 방안에 관한 연구가 필요할 것으로 본다.

참 고 문 헌

[1] 강동호, 한진희, 이윤경, 조영섭, 한승완, 김정녀, 조현숙, "모바일 단말 보안 운영체제기술 동향", 전자통신동향분석, 25(3), 2010.

[2] 김기영, 강동호, "개방형 모바일 환경에서 스마트폰 보안기술", 정보보학회 논문지, 10(5), 2009.

[3] 김무섭, 신진아, 박영수, 전성익, "모바일 플랫폼용 공통보안핵심모듈기술", 정보보호학회지, 제 16권, 제 3호, pp.7-17, 2006.

[4] 김영수, 박영수, 박지만, 김무섭, 김영세, 주홍일, 김명은, 김학두, 최수길, 전성익, "신뢰 컴퓨팅과 TCG 동향", 전자통신동향분석, 22(1), pp.83-96, 2007.

[5] 배근태, 김기영, "모바일 단말 보안 운영체제기술 동향", 전자통신동향분석, 23(4), 2008.

[6] 유지은, "스마트폰의 Key Enabler : 소프트웨어", SW Insight, 2009.

[7] 윤민홍, 김선자, "글로벌 모바일 단말 소프트웨어 플랫폼 동향", 전자통신동향분석, 23(1), 2008. 2.

[8] 이기혁, "Mobile Security 현황과 통신사업자 대응 방안", SIS2009, 2009.

[9] 이선호, 이임영, "USB 메모리를 위한 보안 솔루션에 관한 연구", 멀티미디어학회 논문지, 13(1), 2010. 1.

[10] 제갈병직, "스마트폰 시장과 모바일OS 동향", Semiconductor Insight, 2010.

[11] Andrew Hoog, "Android Forensics". viaForensics, 2009.

[12] Andrew Hoog, Kyle Gaffaney, "iPhone Forensics". viaForensics, 2009.

[13] Apple inc., "iPhone in Business Security Overview", 2009.

[14] Nicolas Seriot, "iPhone Privacy", BlackHatDC2010, 2010.

[15] Trusted Computing Group, "Mobile Phone Work Group Use Cases", 2005.

[16] Trusted Computing Group, "Backgrounder", 2006

[17] Trusted Computing Group, "Mobile Trusted Module Specification FAQ", 2006.

[18] Trusted Computing Group, "Trusted Computing Group Mobile Specification: Securing Mobile Devices on Converged Networks", 2006.

[19] Trusted Computing Group, "TCG Specification Architecture Overview", Revision 1.4, 2007.

[20] Trusted Computing Group, "TCG TPM Specification Version 1.2 Revision 103", 2007.

[21] Trusted Computing Group, "TimeLine", 2007.

[22] U. Kuhn, K. Kursawe, S. Lucks, "Secure Data Management in Trusted Computing", CHES 2005, LNCS 3659, pp.324 - 338, 2005.

[23] iSecPartners, http://www.isecpartners.com/mobile-security-tools/manifes12t-explorer.html

이 선 호

e-mail : sunho431@sch.ac.kr

2009년 순천향대학교 정보기술공학부(학사)

2011년 순천향대학교 컴퓨터학부(석사)

2011년~현 재 순천향대학교 컴퓨터학부 박사과정

관심분야 : 보안USB, 검색가능한 암호

이 임 영

e-mail : imylee@sch.ac.kr

1981년 홍익대학교 전자공학과

1986년 오사카대학 통신공학전공(석사)

1989년 오사카대학 통신공학전공(박사)

1989년~1994년 한국전자통신연구원 선임연구원

1994년~현 재 순천향대학교 컴퓨터소프트웨어학과 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안