모바일 플랫폼에서 MTM을 이용한 안전한 사용자 인증 방법+

이선호, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[sunho431, imylee]@sch.ac.kr

Secure User Authentication Method using MTM on Mobile Platform Environment

Sun-Ho Lee, Im-Yeong Lee
Department of Computer Software Engineering, Soonchunhyang University

요 약

이동통신은 사용자가 단말기를 통해 음성이나 영상, 데이터 등을 장소에 구애받지 않고 통신할 수 있도록 이동성을 제공하는 통신 서비스로 이동이 자유롭지 못한 유선통신과 달리 언제 어디서나 서비스를 받을 수 있어 사용자가 지속적으로 증가하고 있다. 국내의 경우 단순 음성통화 서비스만 가능한 1세대 이동통신 서비스가 1984년에 시작되었으며 2세대, 3세대를 거쳐 현재 데이터 통신 기능이 강화된 3.5세대 통신이 사용되고 있다. 통신의 발달과 함께 모바일 디바이스 역시 점차 발전되어 스마트폰이 등장하게 되었다. 여러 가지 기능을 제공하는 스마트폰의 장점으로 인해서 스마트폰 사용자 수가 급격히 증가하고 있으며, 앞으로도 지속적으로 증가할 것으로 전망하고 있다.

하지만, 스마트 폰은 일반 모바일 디바이스와 다르게 개인 정보 및 주요 정보가 디바이스에 저장되는 경우가 많아 이를 분실할 경우 심각한 개인정보 유출 사고로 확대될 수 있는 문제점을 가지고 있다. 따라서 이를 해결할 수 있는 보안 기술의 필요성이 높아지고 있으며 이러한 모바일 환경에서 안전성 제공 방안의 하나로 신뢰 컴퓨팅 기술을 적용하는 연구가 진행되고 있다. 본 논문은 이러한 신뢰 컴퓨팅 기술을 제공하는 MTM을 이용하여 모바일 디바이스의 주요 정보 노출을 방지하며, 비밀번호 손상 시 가용성을 제공하기 위한 사용자 인증 기술을 제안한다.

1. 서론

이동통신은 사용자가 단말기를 통해 음성이나 영상, 데이터 등을 장소에 구애받지 않고 통신할 수 있도록 이동성을 제공하는 통신 서비스를 말한다. 이동이 자유롭지 못한 유선통신과 달리 모바일 디바이스를 이용하여 언제 어디서나 서비스를 받을 수 있는 이동통신은 사용자가 지속적으로 증가하고 있다.

국내의 경우 단순 음성통화 서비스만 가능한 FDMA (Frequency Division Multiple Access) 기반의 1세대 이동통신 서비스가 1984년에 시작되었다. 이어서 CDMA(Code Division Multiple Access) 방식의 2세대, IMT-2000으로 불리는 3세대를 거쳐 현재 데이터 통신 기능이 강화된 3.5세대 통신이 사용되고 있다. 통신의 발달과 함께 모바일 환경에서 다양한 서비스를 받고자 하는 사용자의 요구에 따라 모바일 디바이스 역시 점차 발전되었으며, 스마트폰이 등장하게 되었다. 스마트 폰은 PC와 같은 고급기능을 제공하는 휴대전화로 일반적인 음성 통화는 물론, 무선 인터넷, 워드프로세서나 엑셀과 같은 문서 작성도 가능한 장점을 가지고 있다[1-4].

+ 본 연구는 한국전자통신연구원 부설 연구소의 위탁 연구과제 지원으로 수행되었음

하지만, 스마트 폰은 일반 모바일 디바이스와 다르게 개인 정보 및 주요 정보가 디바이스에 저장되는 경우가 많다. 따라서 이를 분실할 경우 심각한 개인정보 유출 사고로 확대될 수 있는 문제점을 가지고 있어 이를 해결할 수 있는 보안 기술의 필요성이 높아지고 있으며, 이러한 모바일 환경에서 안전성 제공 방안의 하나로 신뢰 컴퓨팅 기술을 적용하는 연구가 한창 진행 중이다. 신뢰 컴퓨팅이란 신뢰성 제공을 목표로 하는 개체에 최소한의 신뢰 개체를 두는 개념이다. 이 최소한의 신뢰할 수 있는 개체로부터 시작하여 해당 모바일 디바이스에 대한 신뢰성을 점차 이루어 나아가 전체적인 신뢰성을 제공할 수 있도록 하는 것이 신뢰 컴퓨팅의 개념이다[5][7-8].

본 논문에서는 이러한 신뢰 컴퓨팅 기술을 제공하는 MTM(Mobile Trusted Module)을 이용하여 모바일 디바이스의 주요 정보 노출을 방지 및 비밀번호 손상 시 가용성을 제공하기 위한 사용자 인증 기술을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존방식의 취약점을 분석하고 모바일 플랫폼에서 안전한 사용자 인증을 위해 필요한 보안요구사항을 도출하며, 3장에서는 보안요구사항을 만족하는 방식을 제안한다. 4장에서는 제안방식을 분석하며, 마지막으로 5장에서 결론을 맺도록 한다.

2. 기존방식

본 장에선 TPM을 이용하여 PC에 안전한 저장소를 제공하는 Microsoft 사의 BitLocker의 취약점을 분석하고, 취약점을 해결하기 위해 필요한 보안 요구사항을 도출한다.

2.1 BitLocker

Microsoft 사의 BitLocker는 (그림 1)과 같이 스토리지를 FVEK(Full Volume Encryption Key)로 암호화하고 FVEK를 VMK(Volume Master Key)로 암호화, VMK를 MTM에 안전하게 저장된 SRK(Storage Root Key)로 암호화하여 시스템 볼륨에 저장하는 방법으로 안전한 저장소를 제공하고 있다[6].

이와 같은 방법은 저장소의 손상이나 공격자로부터 시스템 볼륨이 손상당했을 경우 암호화된 스토리지를 복호화할 수 없는 가용성의 문제점을 가지고 있다.

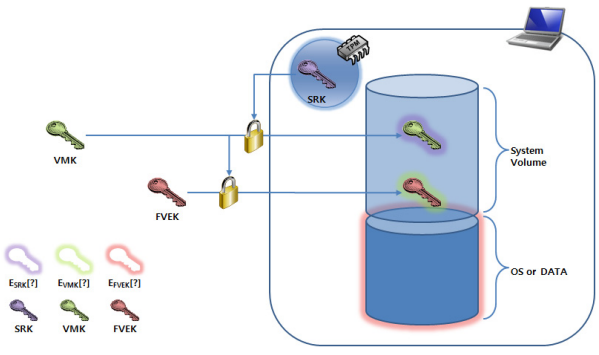
2.2 보안요구사항

따라서 본 논문은 스토리지 보안을 위해 필요한 사용자 인증 과정에 가용성을 제공하기 위해 아래와 같은 보안요구사항을 도출하였다.

- 인증: 기기 인증 및 안전한 사용자 인증을 받은 사용자만이 안전한 저장소에 접근 가능해야 한다.
- 무결성: 통신 간 주고받는 내용이 변조되지 않아야 하며, 변조될 경우 이를 감지할 수 있어야 한다.
- 가용성: 스토리지 손상 및 공격자의 공격에도 지속적인 서비스가 제공되어야 한다.
- 기밀성: 클라이언트와 서버와의 통신 내용으로부터 비밀번호를 알아낼 수 없어야 한다.

3. 제안방식

본 논문에서는 MTM의 기능 및 겹선형 쌍곡선을 이용하여 안전하고 가용성을 제공하는 사용자 인증 방식을 제안한다.



(그림 1) BitLocker 개념도

3.1 시스템계수

제안방식은 다음과 같은 시스템 계수를 이용한다.

- G_1 : 덧셈군
- G_2 : 곱셈군, $G_2 \leftarrow G_1 * G_1$
- p : 큰 소수 값
- g : G_1생성자
- X : 개인키
- Y : 공개키
- KU_{SP} : 서비스 제공자의 공개키
- $H[\,]$: 일방향 해시함수
- $H_1[\,]$: 덧샘군 원소를 반환하는 해시함수
- PCR : Platform Configuration Register
- $IMSI$: International Mobile Subscriber Identity
- SP : 서비스 제공자
- STK : 스토리지 암호화 키
- PWD : 사용자 인증 비밀번호
- r_1 : 임의 난수값
- r_2 : 임의 난수값

3.2 설정 단계

사용자 인증을 위하여 다음과 같은 설정 단계를 거치게 된다.

Step 1. 모바일 디바이스에 장착된 MTM에서 PCR 값을 획득한다.

Step 2. 사용자가 모바일 디바이스에 사용자 인증을 위한 비밀번호를 입력한다.

Step 3. 기기 및 사용자 인증을 확인하기 위해 비밀번호의 해시 값으로 Step 1.에서 획득한 PCR 값을 암호화하여 모바일 디바이스기에 저장한다.

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

Step 5. 사용자 인증에 사용될 키 쌍 X, Y와 임의 난수 r_1, r_2를 생성한다.

$$X \in Z_p^*$$

$$Y = g^x$$

Step 6. 주요 정보가 저장된 모바일 디바이스기의 스토리지 암호키 STK를 생성하고 스토리지를 암호화한다.

$$STK = e(g, H_1[IMSI])^{H[PWD]*r_1*r_2}$$

Step 7. 모바일 디바이스기는 STK 값을 노출하지 않고 차후 재생성 할 수 있도록 하는 값을 생성하여 SP의 공개키로 암호화하여 전송한다.

$$E_{KU_{SP}}[IMSI \,\|\, e(Y^{H[PWD]}, H_1[IMSI]^{r_1}) \,\|\, H[IMSI]$$

Step 8. SP는 모바일 디바이스로부터 전송 받은 값을 복

호화고 $IMSI$값을 통해 무결성을 검증한 뒤 비밀번호 복구 값을 저장한다.

$e(Y^{H[PWD]}, H_1[IMSI]^{r_1})$

3.3 인증 단계

사용자 인증을 위해 다음과 같은 단계를 거치게 된다.

Step 1. 모바일 디바이스에 장착된 MTM에서 PCR 값을 획득한다.

Step 2. 사용자가 모바일 디바이스에 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 모바일 디바이스에서 USIM에 저장된 가입자 식별 정보인 $IMSI$를 추출한다.

Step 5. 모바일 디바이스는 $IMSI$를 SP의 공개키로 암호화한 값과 $IMSI$의 해시 값을 연접하여 전송한다.

$E_{KU_{SP}}[IMSI] \parallel H[IMSI]$

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

Step 7. SP는 검색된 비밀번호 복구 값을 모바일 디바이스에게 전송한다.

$e(Y^{H[PWD]}, H_1[IMSI]^{r_1})$

Step 8. 모바일 디바이스는 SP로부터 전송받은 비밀번호 복구 값에 r_2/x승을 하여 STK값을 복구하고 스토리지를 암호화한다.

$$e(Y^{H[PWD]}, H_1[IMSI]^{r_1})^{r_2/x}$$
$$= e(g^{x*H[PWD]}, H_1[IMSI]^{r_1})^{r_2/x}$$
$$= e(g^{H[PWD]}, H_1[IMSI]^{r_1})^{r_2}$$
$$= e(g, H_1[IMSI])^{H[PWD]*r_1*r_2}$$
$$= STK$$

4. 제안방식 분석

제안 방식은 다음과 같은 요구사항을 만족한다.

- 인증: 비밀번호 및 MTM의 PCR값을 통한 사용자 인증과정으로 사용자 및 기기 인증을 취득해야만 안전한 저장소에 접근할 수 있다.
- 무결성: 통신 간 주고받는 내용에 해시값을 첨부하여 내용의 변조를 감지할 수 있다.
- 가용성: 스토리지 및 공격자의 공격에도 SP에 저장된 복구 값 및 MTM을 이용하여 STK를 생성할 수 있어 지속적인 서비스가 제공될 수 있다.
- 기밀성: 공개키 암호 방식을 이용한 통신으로 클라이언트와 서버와의 통신 내용으로부터 비밀번호를 알아낼 수 없다.

5. 결론

본 논문은 TPM 및 USIM을 이용한 하여 모바일 플랫폼 상에서 저장소에 접근할 수 있는 안전한 사용자 인증 기술을 제안하였다. 앞으로 이와 같은 저장소의 데이터의 이동성 보장을 위한 연구가 지속되어야 하며, 지속적이고 효율적인 안전성 제공을 위하여 암호키 갱신 연산 효율성을 제공하는 기법에 대한 연구가 필요하다.

또한 TPM을 활용한 다양한 응용 기술의 취약점을 분석하고 신뢰컴퓨팅 기술을 활용한 지속적인 연구 및 개발이 필요할 것으로 본다.

참고문헌

[1] 제갈병직, “스마트폰 시장과 모바일OS 동향”, Semiconductor Insight, 2010.5.

[2] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안기술“, 정보보학회 논문지, 제 10권, 제 5호, 2009.10.

[3] 배근태, 김기영, “모바일 디바이스 보안 운영체제 기술 동향“, 전자통신동향분석, 제 23권, 제 4호, 2008.8.

[4] 윤민홍, 김선자, “글로벌 모바일 디바이스 소프트웨어 플랫폼 동향”, 전자통신동향분석, 제 23권, 제 1호, 2008.2.

[5] 김영수, 박영수, 박지만, 김무섭, 김영세, 주홍일, 김명은, 김학두, 최수길, 전성익, "신뢰 컴퓨팅과 TCG 동향", 전자통신동향분석, 제 22권 제 1호, pp.83-96, 2007.

[6] "BitLocker Drive Encryption", Microsoft Coporation, 2006.

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

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