모바일 환경에서의 안전한 사용자 인증을 위한 MTM과 USIM의 연동 방안에 관한 연구

강동완*, 이임영*
*순천향대학교 컴퓨터학부
e-mail:lupin428@sch.ac.kr

A Study on Interoperability between MTM and USIM for Secure User Authentication on Mobile Environment

Dong-Wan Kang*, Im-Yeong Lee*
*Division of Computer Science and Engineering, Soonchunhyang Univ.

요 약

현제의 서비스들은 점점 온라인화 되어 가고 있으며 특히 무선 통신의 발전에 따라 현대 사회인들은 다양한 모바일 기기들을 사용하여 여러 서비스를 제공 받고 있다. 하지만 서비스들을 제공하기 위한 기존 패스워드 기반의 사용자 인증은 스니핑과 피싱 및 악성코드에 의한 개인정보 유출 등으로 인하여 안전성을 보장받지 못하고 있다. 특히 모바일 단말기의 분실 및 불법적인 복제와 점차 증가하고 있는 모바일 악성코드로 인한 모바일 환경의 보안 위협은 기존의 소프트웨어 보안으로는 감당할 수 없게 되었다. 따라서 본 논문에서는 신뢰컴퓨팅을 위한 TCG의 보안기술로써 플랫폼 인증을 제공하는 MTM을 사용자 인증 모듈인 USIM과 연동하여 다양한 모바일 환경의 보안 위협에 대응할 수 있는 사용자 인증 방안을 제안한다.

1. 서론

모바일 환경의 보안은 기존의 유선 환경보다 훨씬 열약한 환경을 가지고 있다. 무선의 특성으로 통신 트래픽을 쉽게 얻을 수 있으며, 모바일 단말기의 분실 및 물리적인 해킹은 모바일 환경의 주된 보안 위협으로 볼 수 있다. 특히 현재 사용하고 있는 모바일 단말기의 한 종류로써 핸드폰의 경우, 사용자는 자신의 4자리 숫자로 비밀번호를 걸어 놓지만 이는 사용자의 개인정보를 모른다고 하더라도 일반적인 전사적 공격에 의해 매우 취약하다. 이러한 패스워드 기반의 인증 방법은 사용자가 직접 기억해야 하는 패스워드를 사용해야 하므로 그 패스워드의 암호학적 강도가 높지 않은 것이 사실이다.

따라서 USIM(Universal Subscriber Identity Module)를 사용하여 사용자를 인증하는 방안이 연구되고 있으며, 우리나라에서도 이동 전화 서비스를 위한 가입자 인증 방안으로 고려되고 있다. USIM은 사용자를 인증하기 위한 인증정보를 하드웨어적으로 안전하게 저장하기 때문에 사용자는 그것을 자신이 기억하지 않아도 되며 단지 USIM에 대한 사용자의 소유자 인증을 수행하면 된다. USIM은 모바일 단말기와 서로 독립적인 사용자 인증을 위한 다른 하드웨어적 보안 요소이기 때문에 USIM을 사용함으로써 내가 사용하고자 하는 단말기가 정당한 단말기인지 판단할 수 있어야 한다. USIM은 사용자의 인증정보가 저장되어 있기 때문에 불법적인 단말기나 악의적인 목적을 가진 단말기를 사용하게 될 경우 사용자의 개인 정보가 유출되거나 악용될 우려가 있기 때문에 모바일 단말기에 대한 인증을 위한 보안적인 요소가 필요하다.

현제의 보안은 점차 하드웨어 기반의 요소를 요구하고 있기 때문에 모바일 환경의 안전한 보안을 위해서 하드웨어적인 보안 모듈이 필요하며 이는 개방형 보안 프레임워크를 표준화하고 있는 TCG(Trusted Computing Group)의 MTM(Mobile Trusted Module)를 사용하여 제공될 수 있다. 본 논문에서는 사용자 인증을 위한 USIM과 모바일 단말기에 대한 인증으로써 MTM을 사용하여 안전한 사용자 인증 방안에 대하여 제시한다.

2. 보안 요구 사항

본 장에서는 사용자가 모바일 단말기를 사용하여 서비스를 제공받기 위한 보안 요구사항에 대해서 기술한다.

- 사용자 인증 : 단말기를 이용하고자 하는, USIM을 사용하고자 하는 사용자에 대해서 정당한 사용자인지 검증해야한다.
- 단말기 인증 : 사용하고자 하는 단말기가 불법적으로 복제 된 것이거나 사용자 개인정보를 빼내기 위한 악의적인 목적을 가진 단말기 인지 검증할 수 있어야 한다.
- 기밀성 : 사용자의 인증 정보와 이를 사용한 인증 절차

에 있어 관련 데이터를 정당한 객체만이 확인할 수 있어야 한다.

• 무결성 : 통신 채널에서의 송수신 되는 정보가 위조 및 변조가 되지 않아야 한다.

• 패스워드 추측 : 특정 암호문 혹은 인증 정보에 대해서 사용된 비밀 정보를 추측할 수 없어야 한다.

• 물리적 단말기 해킹 : 모바일 단말기의 특성상 분실이 되었을 때 물리적인 해킹에 안전해야 한다.

• 사용자 프라이버시 : 모바일 단말기에 사용된 사용자의 인증 정보 및 개인 정보 등의 비밀 정보는 안전하게 관리되어야 한다.

3. 관련 연구

본 장에서는 기반 연구로써 USIM과 MTM에 대해서 분석하고 모바일 환경의 사용자 인증 프로토콜로써 3G-AKA와 EAP-AKA에 대해서 살펴본다.

2.1 USIM

USIM은 사용자 인증 모듈로써 사용자의 인증 정보를 하드웨어 적으로 안전하게 보관하고 있다. USIM은 안전한 저장소와 공개키 암호화 및 전자서명 등의 다양한 암호학적 기능을 가지고 있으며 USIM으로써 단말기에 강한 사용자 인증을 제공한다. 하지만 USIM을 사용하려면 USIM의 소유자로써 사용자 인증이 추가적으로 필요하고 USIM이 여러 단말기에 삽입 될 수 있으므로 각 단말기 자체의 보안성을 검증하여 불법적인 개인정보의 유출을 보호할 필요가 있다.

2.2 MTM

개방형 보안 플랫폼을 표준화 하고 있는 TCG에 의해 제정된 산업 규격을 기초로 한 마이크로 컨트롤러인 TPM(Trusted Platform Module)의 모바일 버전이다. MTM은 다양한 암호학적 기능을 가지는데 신뢰 모듈로써 외부로부터 인증된 유일한 2048bit의 개인키/공개키 쌍을 가지고 있고, MTM 내부의 안전한 저장소와 함께, 단말기 내부에 임베디드 되어 단말기의 하드웨어 구성 및 소프트웨어 상태를 점검 할 수 있는 PCR(Platform Configuration Register)을 가지고 있어 플랫폼에 대한 무결성 검사 및 인증을 수행 할 수 있다. 또한 자신의 고유한 개인키/공개키 쌍을 사용하여 외부로부터 검증할 수 있는 AIK(Attestation Identity Key)를 비롯한 개인키/공개키 쌍을 생성할 수 있으며 이러한 키들은 안전한 저장소에 저장되어 외부로부터 안전하다.

2.3 3GPP-AKA

모바일 환경에서 사용자 인증 및 암호화 등을 제공하기 위해 3GPP(3rd Generation Partnership Project)에서 AKA(Authentication and Key Agreement) 표준을 개발하였다. 여기서는 사용자와 외부 등록 서버, 홈 등록 서버가 있으며, 단말과 등록 서버간의 상호 인증 및 키 생성을 정의하고 있다. 하지만 악의적인 제 3자로부터 등록 서버가 위장되었을 경우에 이 위장된 등록 서버로부터 보안 위협이 존재한다. 즉, 단말과 등록 서버 간에 상호인증을 제공하지 못한다는 단점이 있다.

2.4 EAP-AKA

EAP(Extensible Authentication Protocol)-AKA는 IETF RFC 4187에 정의 되어 있으며, 현재 무선 인터넷, 3GPP 및 WiBro 보안 기술로써 연구가 되고 있다. EAP-AKA는 USIM을 사용하여 사용자에 대한 인증정보를 안전하게 저장하고 칩의 복제, 위조가 어려운 특성을 가지고 있다. EAP-AKA는 인증을 통해 데이터 암호화 키를 설립하며 단말기 내에서 다른 도메인간의 이동을 위한 인증 서버간 통신이 필요하다.

4. 제안 방식

제안방식은 크게 플랫폼 인증단계와 사용자 인증단계, 서비스 이용단계로 나뉜다. 사용자는 자신의 USIM을 모바일 단말기에 삽입하고 자신의 USIM 패스워드를 넣기 전에 플랫폼에 대한 인증을 수행하며 플랫폼 인증은 인증서버(AS)와 이루어진다. 사용자 인증은 플랫폼 인증이 통과된 이 후에 사용자가 USIM의 소유자임을 검증하는 단계로써 모바일 단말기와 USIM간에 이루어진다.

4.1 시스템 계수

- * : 각각의 개체(USER : 사용자, USIM : 사용자 인증 모듈, MTM : 모바일 단말기에 부탁된 인증 모듈, AS : Authentication Server(인증서버))
- $E_*[]$: 키 *로 암호화
- $Sign_*[]$: *의 개인키로 전자서명
- $h()$: 안전한 일 방향 해쉬 함수
- $K_{USIM.AS}$: 객체 USIM, AS간에 비밀리에 공유된 대칭키
- pw : USIM에 저장된 사용자 패스워드
- pw' : 사용자가 입력한 패스워드
- r_1 : 플랫폼 인증 단계를 위한 USIM이 생성한 난수
- r_2 : 사용자 인증 단계를 위한 USIM이 생성한 난수
- TS : 일련의 순서를 가지는 타임스탬프
- $PRAIK_{USER}/PUAIK_{USER}$: 인증된 사용자를 위해 MTM이 생성한 개인키/공개키 쌍
- $Platform\ Info$: 모바일 단말기에 대한 하드웨어 밀 소프트웨어 정보로써 제조사 및 장치 구성 운영체제등의 시스템 정보
- PIV_{AS} : AS가 가지고 있는 Platform Integrity Value로써 모바일 단말기의 $Platform\ Info$에 따라 신뢰할 수

있는 PCR 값에 대한 AS의 전자서명

- PIV_{MTM} : MTM이 계산한 PIV로써 현재 단말기의 $Platform\ Info$에 따라 PCR을 검사하여 얻은 PCR 값에 대한 MTM의 전자 서명 값
- $PIVReq$: USIM의 PIV_{AS}요청 메세지
- $AuthReq$: USIM의 사용자 인증 요청 메세지

4.2 프로토콜

프로토콜은 총 세 단계로 단말기 인증, 사용자 인증, 서비스 이용 단계로 구분된다. 사용자의 USIM과 MTM은 AS를 통해 이미 인증된 개인키/공개키를 가지고 있다고 가정한다.

4.2.1 단말기 인증 단계

단말기 인증 단계는 USIM이 사용자가 단말기를 사용하기 전에 단말기가 안전한 상태인지 확인하는 과정이다. AS는 단말기의 $Platform\ Info$에 따른 PIV값을 자신의 데이터베이스에 저장하고 있다고 가정한다. 이 과정은 MTM의 PCR Reporting을 사용하여 이루어지며 프로토콜의 시작은 사용자가 USIM을 단말기에 삽입하고 나서 USIM으로부터 시작된다.

step 1 USIM은 자신의 아이디와 난수 r_1을 생성하여 AS와의 공유된 비밀키 $K_{USIM,AS}$로 암호화하여 $PIVReq$와 함께 MTM에 전달한다.

$$M1: ID_{USIM}, PIVReq, TS, E_{K_{USIM,AS}}[r_1 \| h(ID_{USIM}, TS)]$$

step 2 MTM은 USIM으로부터 받은 메시지 M1을 자신의 $Platform\ Info$과 서명을 함께 AS로 전달한다.

$$M2: ID_{MTM}, M1, Platform \infty o, TS, \\ Sign_{MTM}[h(M1 \| Platform \infty o \| TS)]$$

step 3 AS는 USIM의 $PIVReq$에 따라서 MTM의 $Platform\ Info$에 따른 PIV를 자신의 데이터베이스에서 찾아 자신의 서명을 첨부한 PIV_{AS}를 생성하고, USIM과의 비밀키로 암호화된 난수 r_1을 복호하여 새로운 비밀키 $K'_{USIM,AS}$를 계산한다.

$$M3.1: K'_{USIM,AS} = h(K_{USIM,AS} \oplus r_1)$$

그리고 키 $K'_{USIM,AS}$로 PIV_{AS}와 r_1을 암호화 하여 자신의 서명과 함께 MTM에 전송한다.

$$M3.2: ID_{AS}, E_{K'_{USIM,AS}}[r_1, \Pi V_{AS}], TS, \\ sign_{AS}[h(ID_{AS}, E_{K'_{USIM,AS}}[r_1, \Pi V_{AS}], TS)]$$

step 4 MTM은 자신의 $Platform\ Info$에 대한 PCR을 검사하여 PIV_{MTM}를 생성하고 AS로부터 받은 메시지 M3.2의 암호화된 PIV_{AS}를 함께 USIM에게 전달한다.

$$M4: ID_{MTM}, E_{K'_{USIM,AS}}[r_1, PIV_{AS}], PIV_{MTM}, TS, \\ Sign_{MTM}[h(ID_{MTM}, E_{K'_{USIM,AS}}[r_1, PIV_{AS}], PIV_{MTM}, TS)]$$

4.2.2 사용자 인증 단계

USIM은 M4로부터 단말기에 대한 검증을 확인하고 사용자 인증을 진행한다. USIM은 MTM과 사용자로부터 입력받은 pw', 난수 r_2를 이용하여 사용자 패스워드를 검증한다.

step 1 USIM은 새로운 난수 r_2를 생성하여 임시 패스워드 tpw를 생성한다.

$$M5.1: tpw = h(r_2 \oplus pw)$$

그리고 tpw로 tpw의 해쉬값을 암호화 하고 r_2를 pw로 암호화 하여 MTM에 전송한다.

$$M5.2: ID_{USIM}, UserAuth\ Req, E_{pw}[r_2, h(tpw)], TS$$

step 2 MTM은 사용자로부터 패스워드 입력을 요구하여 사용자 가 입력한 패스워드 pw' 받는다.

step 3 MTM은 사용자가 입력한 패스워드 pw'로 M5.2에 $E_{pw}[r_2, h(tpw)]$를 복호하야 r_2와 $r_2 \oplus pw'$의 해쉬값을 계산하여 $h(tpw)$와 비교 검증 하여 사용자를 인증한다.

4.2.3 서비스 이용 단계

MTM은 보안 모듈로써 안전한 저장소를 제공하고 개인키/공개키 쌍을 생성하여 외부로부터 인증 받은 AIK를 생성할 수 있다. USIM은 MTM이 생성한 공개키를 인증함으로써 USIM이 현재의 단말기를 사용하는 동안 외부로부터 검증이 가능한 MTM이 생성한 공개키를 사용할 수 있다. MTM은 다수의 USIM에 대해서 생성된 암호 키의 안전한 관리를 안전한 저장소와 SRK에 의한 계층적인 키 관리 구조로써 제공한다.

step 1 MTM은 사용자를 인증한 후, 그 결과와 사용자가 사용할 개인키/공개키 쌍 $PRAIK_{USIM}/PUAIK_{USIM}$을 생성하여 AS로부터 AIK로써 인증 받고 그 중 공개키 $PUAIK_{USIM}$를 USIM에게 전송한다. 개인키 $PRAIK_{USIM}$는 MTM 내부의 안전한 저장소에 USIM의 아이디와 연계하여 저장한다.

$$M7: Auth-Accept, PUAIK_{USIM}$$

step 2 USIM은 $PUAIK_{USIM}$를 받아 검증하고, 자신의 서명으로써 단말기 내부의 안전한 저장소와 보안 통신을 위해 사용할 수 있도록 자신의 서명을 MTM에 전달한다. USIM에 의한 서명은 $PUAIK_{USIM}$가 USIM을 나타내는 것이며 해당 USIM이 아니면 $PUAIK_{USIM}$로부터 파생된 데이터에 접근할 수 없음을 의미한다.

$M8: Sign_{USIM}[PUAIK_{USIM}]$

MTM은 사용자가 생성하거나 외부로부터 받은 정보들을 안전한 저장소에 저장하게 되며 사용자가 단말기에서 USIM을 분리할 때 그 정보들은 MTM에 의해 모두 삭제되게 된다.

5. 제안 방식 분석

제안방식은 단말기의 신뢰 모듈로써 하드웨어 기반의 보안 칩인 MTM을 사용하여 단말기 인증을 제공하고 USIM을 사용하여 사용자 인증을 제공한다. 사용자는 자신의 인증 모듈인 USM이 단말기에 삽입되고 나서 단말기에 대한 인증을 인증서버 AS로부터 PIV_{AS} 를 받아 MTM의 PIV_{MTM}로 검증하여 안전한 상태의 단말기임을 검증 할 수 있다. 이후 사용자는 임시 패스워드 tpw를 사용하여 USIM의 소유자 인증을 진행하고, MTM으로부터 개인키/공개키 쌍을 받아 응용 서비스를 이용하는데 있어 안전한 보안 통신을 제공한다. 본 제안 방식을 앞서 보안 요구사항에 따라 분석하면 다음과 같다.

• 사용자 인증 : USIM은 사용자 인증 모듈로써 정당한 USIM의 소유자 만이 사용자 인증을 수행할 수 있다. 본 제안방식에서는 USIM이 생성한 난수 r_2와 사용자 패스워드 pw의 XOR연산 결과의 해쉬 값으로 임시 비밀번호 twp를 생성하여 MTM이 사용자로부터 입력받은 pw'와 USIM으로부터 받은 r_2로 tpw를 계산하여 검증하는 방식으로 사용자를 인증한다.

• 단말기 인증 : 모바일 단말기는 다양한 하드웨어와 복잡한 운영체제등의 소프트웨어가 동작하고 있다. 이러한 단말기의 기반이 되는 자원 상태인 $Platform\ Info$에 대해서 MTM의 PCR Reporting을 사용하여 PIV로써 단말기의 안전성을 검증하고 정당한 단말기로써 인증할 수 있다.

• 기밀성 : 사용자 인증정보로써 pw는 USIM 내부에 안전하게 저장되어 있다. 사용자 인증 단계에서 USIM은 사용자의 패스워드를 노출시키지 않고 난수 r_2를 사용하여 본래의 pw를 감추었고, AS와의 통신은 사전에 공유된 비밀키 $K_{USIM,AS}$로 기밀성을 제공하였다.

• 무결성 : 통신상의 송수신 되는 메시지의 무결성을 위해 전자서명을 사용하여 메시지 무결성을 제공하였다.

• 패스워드 추측 : 사용자 인증을 위한 pw에 대한 추측은 USIM이 단말기에 삽입된 순간 난수 r_2가 생성되어 임시 패스워드 tpw로써 사용자 인증을 수행하기 때문에 원래의 패스워드 pw를 추측하기 어려우며 난수 r_2는 USIM이 단말기에 삽입된 순간마다 변경되게 되고, 일정 횟수를 초과한 인증 실패는 USIM을 다시 삽입해야 한다.

• 물리적 단말기 해킹 : 단말기에 대한 물리적인 공격은 모바일 환경의 주된 보안 위협중의 하나이다. 제한된 전력과 처리능력으로 가한 보안 시스템일 갖추기 어려운 모바일 단말기의 물리적 공격에 대응하기 위해 MTM을 사용하였다. MTM은 단말기 내부에 임베디드 되어 따로 분리할 수 없으며 안전한 저장소를 제공하고 물리적은 공격에 대응할 수 있다.

• 사용자 프라이버시 : 모바일 단말기는 사용자 프라이버시와 관련된 정보를 다양하게 저장하고 있다. 따라서 이러한 사용자 정보들을 안전하게 관리해야 하며, 다수의 USIM을 상대해야 하는 단말기로써는 각각의 USIM에 대해서 안전한 저장소를 위한 개인키/공개키 쌍을 생성하여 사용자 프라이버시를 보호한다.

6. 결 론

모바일 환경의 보안은 기존의 소프트웨어 보안으로 해결하기에는 너무 다양한 보안 위협이 존재한다. 특히 단말기의 분실 및 물리적인 접근에 의한 공격은 모바일 환경의 대표적인 보안 위협이다. 따라서 기존의 모바일 인증 프로토콜에서 고려하지 않았던 단말기에 대한 보안과 함께 USIM을 사용한 사용자 인증 방안을 제시하였다. USIM과 MTM은 서로 이동성에 따른 차이가 있지만 유사한 성격의 보안 모듈로써 각각 사용자 인증과 플랫폼 인증에 사용하였다. 향후 신뢰 컴퓨팅 기술을 위한 보안 모듈로써 모바일 환경의 MTM에 대한 보안 활용도는 꾸준히 높아질 것으로 전망되며 이에 대한 응용 연구가 필요하다. 따라서 사용자 인증 이 외에 전체적인 서비스에 있어서의 사용자 익명성과 불법 단말기에 대한 대응 방안 등에 대한 연구가 필요한 시점이다.

참고문헌

[1] J. Lindqvist, Laura Takkinen, "Privacy Management for Secure Mobility," WPES'06, 2006.

[3] Third Generation Partnership Project, Technical Specification Group SA, 3G Security, "Security Architecture", Ver 4.2.0, Release 4, 3GPP, TS 33.102, 2001.

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

[4] Trusted Computing Group, "Mobile Trusted Module Specification General Overview FAQ," 2007.

[5] 김무섭, 신진아, 박영수, 전성익, "모바일 플랫폼용 공통보안핵심 모듈 기술," 정보보호학회지, 제 17권, 제 3호, pp.7-17, 2006.