Wi-Fi 환경내의 모바일 단말기와 컨텐츠 제공서버간의 상호 인증 방안

황재연*, 이경석*, 전문석*
*숭실대 대학원 컴퓨터 공학과
e-mail : eyestorys@ssu.ac.kr

A Mutual Authentication Method between Mobile device and Server for Contents on Wi-Fi

Jae-Yeon Hwang*, Kyung-Seok Lee*, Moon-Seog Jeon*
*Dept. of Computer Science, Graduate School of Soong-Sil University

요 약

차세대 무선 통신 기술인 Wi-Fi 는 이동통신사를 거치지 않고 근처의 AP(Access Point)를 통하여 여러 컨텐츠 제공서버에 접근한다. 그에 따라 사용자는 컨텐츠 제공서버로 위장한 피싱이나, 인증되지 않은 사이트를 통해 악성코드 배포, 사용자 정보유출등과 같은 취약점에 노출되고, 컨텐츠 제공서버 또한 타인으로 위장한 위장공격등과 같은 취약점에 노출된다.

본 논문에서는 Wi-Fi 환경 내에서 사용자 단말기와 컨텐츠 제공서버간의 상호 인증 방안을 모색하고, 모바일 환경의 특성을 고려한 상호 인증 방안을 제안한다.

1. 서론

최근 스마트 모바일 단말기는 사용자의 편의성을 고려한 기능부터 기존의 PC 에서 가능했던 다양한 기능들을 지원함으로써 사용자들에게 높은 인기를 받고 있다. 2009 년 5 월 시장조사 업체에서 만 19 세 ~50 세 미만의 남녀 1000 명을 대상으로 "스마트 단말기 구매 의향과 기능 이해 및 선호도 조사"를 실시한 결과 약 40%에 해당하는 이들이 향후 1 년 이내에 구입할 의사가 있는 것으로 조사되었다.

그리고 최근 스마트 모바일 단말기는 Wi-Fi 와 같은 무선 인터넷 플랫폼을 탑재하여, 인터넷을 활용한 많은 기능들을 사용할 수 있는 반면, 단말기의 처리속도나 저장공간 등과 같은 제한된 환경문제로 기존의 유/무선망에서의 PKI 를 활용하는데 제약이 있다.

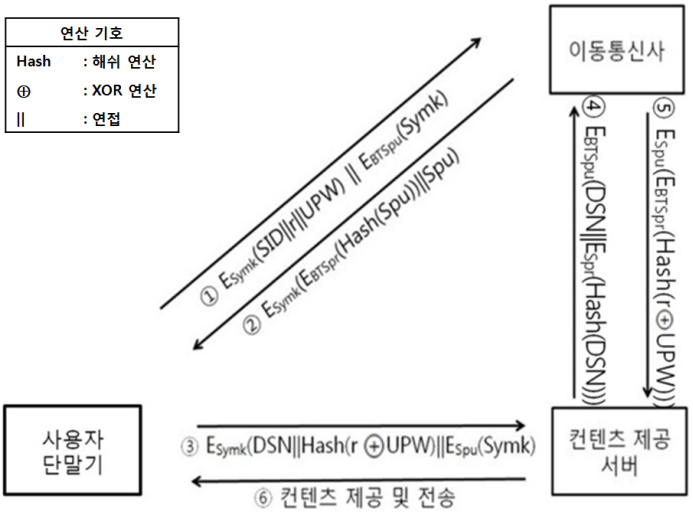
2. 모바일 단말기와 서버의 상호인증 방안

모바일의 특성을 살려 W-PKI 환경에서 단말기와 서버와의 상호인증을 이동통신사의 공증을 통하여 수행하기 위해, 다음과 같은 4 가지 전제 조건이 필요하다.

- 이동통신사는 단말기 사용자로부터 신뢰받는 기관임.
- 단말기는 이동통신사의 공개키를 소유하고 있어야 함.
- 단말기 사용자의 컨텐츠 사용 비밀번호는 사전에 이동통신사에 등록하고, 이동통신사는 사용자의 비밀번호를 노출되지 않게 보관함.

그리고 이동통신사와 컨텐츠 제공서버는 사전에 제휴를 통하여, 상호 신뢰성을 확보하고 양방간의 공개키를 교환한다.

제안하는 상호 인증 방안은 (그림 1)과 같으며 세부 내용은 다음과 같다.



BTS_{Pu}	: 이동통신사 공개키	Symk	: 임의의 대칭키
BTS_{Pr}	: 이동통신사 개인키	UPW	: 컨텐츠 사용 비밀번호
S_{Pu}	: 서버 공개키	r	: 난 수
S_{Pr}	: 서버 개인키	DSN	: 단말기 제품번호
SID	: 컨텐츠 서버 식별자		

(그림 1) 제안하는 상호 인증 프로세스

상호인증 프로세스는 단말기 사용자가 Wi-Fi 환경 내에서 단말기를 통해 컨텐츠 제공서버로부터 컨텐츠 제공 서버 식별자 SID 를 받으면서 시작한다.

① 사용자는 컨텐츠 제공서버로부터 받은 식별자 SID 와 사용자의 컨텐츠 사용 비밀번호 UPW 를 이동통신사로 전송하는 과정이다. 서버 식별자를 이동통신사에게 전송함으로써 사용자 단말기는 컨텐츠 제공서버의 공개키 S_{Pu} 를 이동통신사에 요청하게 되고, 사용자의 컨텐츠 사용 비밀번호를 통해 사용자 인증을 다음과 같이 수행한다.

- UPW 와 동일한 비트수의 임의로 선정된 난수 r 과, 사용자에게 입력받은 UPW 및 SID 를 병합.
- 임의로 선정된 대칭키 Symk 로 (SID||r||UPW)를 대칭키 암호화 알고리즘을 통한 암호화.
- Symk 는 이동통신사의 공개키 BTS_{Pu} 로 암호화.
- 두 결과값 E_{Symk}(SID||r||UPW), E_{BTSpu}(Symk)를 병합하여, 이동통신사에 전달.

위의 데이터를 전달받은 이동통신사는 개인키 BTS_{Pr} 을 사용하여 Symk 를 취득하고 UPW 를 복호화하고, 전제 조건에서 이동통신사에 등록된 UPW 와 비교하여 사용자에 대한 인증을 수행한다. 같이 전달된 난수 r 은 임시 DB 에 저장하고, 컨텐츠 제공서버의 공개키 S_{Pu} 를 검색한다.

② 서버공개키 S_{Pu} 는 이동통신사가 안전성을 보장하는 키임을 증명하고, 또 그에 대한 부인 봉쇄를 위해 개인키 BTS_{Pr} 로 서명한 값을 사용자 단말기에 전송한다.

- 컨텐츠 서버의 공개키 S_{Pu} 를 해쉬하고, 그 결과값을 이동통신사의 개인키 BTS_{Pr} 로 서명.
- 서명값 E_{BTSPr}(Hash(S_{Pu})) 및 S_{Pu} 를 병합하여 ①에서 전달받은 대칭키 Symk 로 암호화한 E_{Symk}(E_{BTSPr}(Hash(S_{Pu}))||S_{Pu})를 사용자의 단말기로 전송.

사용자 단말기는 대칭키 Symk 와 이동통신사의 공개키 BTS_{Pu} 로 S_{Pu} 를 추출하여 해쉬한 Hash(S_{Pu})값과 이동통신사에게서 직접 전달받은 Hash(S_{Pu})값의 비교를 통해서 무결성을 검증한다.

③ 컨텐츠 제공서버의 공개키 S_{Pu} 의 무결성이 보장되면 사용자 단말기는 자신의 제품번호 DSN 과 정당한 사용자임을 인증할 UPW 를 컨텐츠 제공서버로 전송한다. 그리고 컨텐츠 사용 비밀 번호 UPW 는 ①에서 생성한 난수 r 을 사용하여 사용자 UPW 의 노출을 막으며, 그 과정은 다음과 같다.

- UPW 와 동일한 비트 수인 r 과 UPW 의 XOR 값에 해쉬 수행.
- XOR 값과 DSN 을 병합하여 대칭키 Symk 로 암호화.
- 컨텐츠 제공서버의 공개키 S_{Pu} 로 대칭키 Symk 를 암호화하여 덧붙인 결과값 E_{Symk}(DSN||Hash(r ⊕ UPW))||E_{Spu}(Symk)을 컨텐츠 제공서버에 전달.

④ 컨텐츠 제공서버는 자신의 개인키 S_{Pr} 을 통해 대칭키 Symk 를 복호화하고, 단말기 제품번호 DSN 과 Hash(r⊕UPW)를 추출한다. 단말기 제품 번호 DSN 은 이동통신사에 전달되며, DSN 에 대한 무결성과 기밀성, 그리고 부인 봉쇄를 위하여 컨텐츠 제공서버는 자신의 개인키 S_{Pr} 로 서명된 Hash(DSN)과 DSN 을 병합하고, 이동통신사의 공개키 BTS_{Pu} 로 암호화한 E_{BTSPu}(DSN||E_{SPr}(Hash(DSN)))을 이동통신사에 전달한다.

⑤ 이동통신사는 자신의 개인키 BTS_{Pr} 를 통해 DSN 을 추출하여 해쉬한 Hash(DSN)값과 컨텐츠 제공 서버의 서명이 담긴 E_{SPr}(Hash(DSN))값을 서버의 공개키 S_{Pu} 로 복호화한 Hash(DSN)값의 비교를 통해 DSN 의 무결성이 입증되면, 다음과 같은 연산을 수행한다.

- ①에서 받은 난수 r 과 UPW 의 XOR 값 (r⊕UPW)에 해쉬 수행.
- 해쉬값 Hash(r ⊕ UPW)를 이동통신사의 개인키 BTS_{Pr} 로 서명한 값 E_{BTSPr}(Hash(r ⊕ UPW))를 다시 S_{Pu} 로 암호화한 E_{SPu}(E_{BTSPr}(Hash(r⊕UPW)))을 컨텐츠 제공서버에 전달.

⑥ 컨텐츠 제공서버는 ③의 Hash(r⊕UPW)값과 ⑤에서 받은 Hash(r⊕UPW)값을 비교하여 두 값이 일치되면 해당 컨텐츠를 사용자에게 제공한다.

3. 분석 및 비교

<표1> PKI와 제안 프로세스의 연산 수행 위치

연산 항목	PKI	제안
공개키 암/복호화	단말기	단말기
대칭키 암/복호화	단말기	단말기
디지털 서명 생성	단말기	이동통신사
디지털 서명 검증	단말기	단말기

제안한 상호 인증 방안과 기존의 공인인증서를 활용한 상호 인증 시스템을 분석 및 비교 한 결과는 <표1>과 같다. 자원의 소모가 매우 큰 디지털 서명의 생성을 이동통신사의 공증을 통하고, 자원의 소모가 적은 서명 검증은 단말기 내부에서 수행하는 것을 알 수 있다.

참고문헌

[1] 김영재 외, "WiFi Phone 의 무선랜 성능 및 음성 품질 측정", KNOM Conference 2008, Session-1, 2008.05
[2] 김흥남, "WIPI 규격 집중 분석" 마이크로소프트웨어, pp.230-235, 2002.10
[3] 박팔현, "와이파이(Wi-Fi)", LG 주간 경제, 706 호, pp.25, 2002.12
[4]이상윤 외 "무선인터넷 표준 플랫폼 WIPI 2.0," TTA 저널, 제 92 호, pp.97-102, 2004. 3
[5] DIGITAL SIGNATURE STANDARD(DSS), FIPS PUB 186-2, 2000.01
[6] "TTA.KO-06.0036 모바일 표준화 규격," 정보통신단체표준, 2004. 6
[7] Wi-Fi Alliance, "WFA 2008 Annual Report public", 2008 년 12 월