스마트폰 환경에서 이동 통신사 AP 접속을 위한 효율적인 인증 기법에 관한 연구

민대기, 전문석
숭실대학교 컴퓨터학과
e-mail : {daegi_min, mjun}@ssu.ac.kr

A Study on Effective Authentication Method for Mobile Agency AP Connection in Smart Phone Environment

Dae-Gi Min, Moon-Seog Jun
Dept of Computer Science, Soongsil University

요 약

현대 사회에서 스마트폰은 손안의 PC라는 말이 있을 정도로 작지만 많은 기능들을 제공하고, PC와 마찬가지로 개인적이고 중요한 정보들을 저장할 수 있다. 스마트폰의 활성화로 인해 좋은 부분도 있지만 모바일 환경의 무선 보안 문제 또한 부각되고 있다. 본 논문에서는 스마트폰 환경에서 무선 AP를 통해 무선 네트워크 서비스를 이용할 시 문제점들을 보완하고자 3G망을 통하여 암호화된 값을 보내주고 대칭키, PKI, 전자서명을 사용하였다.

1. 서론

오늘날 활발히 연구되어지고 있는 스마트폰의 기술과 기능들은 생활 전반에 걸쳐 많은 영향을 주고 있고 앞으로 미래의 생활과 IT산업에도 큰 영향을 줄 것으로 예측된다.

최근 스마트폰을 이용해서 인터넷 통신이나 자료 전송 등의 무선 서비스가 확대되고 있으며, 인터넷을 통해 음악, 영상, 방송, 인터넷 뱅킹 등 멀티미디어 기능을 통한 스마트폰 시장이 점차적으로 발전하고 있다.

이처럼 무선 네트워크 서비스를 통해 다양하고 편리한 기능들이 수행되어지나 무선 전파의 특성으로 인해 악의적인 공격자가 데이터를 도청하거나, 서비스 거부 공격, 중간자 공격 등이 가능해서 단말기 안에 있는 개인적이면서 중요한 정보들은 더욱 쉽게 노출되어진다.

본고에서는 기존 방법들의 취약점을 보완하고 안전한 무선 네트워크 서비스를 위한 프로토콜을 제안한다. 2장에서는 스마트폰의 보안 요구사항과 기존의 인증 프로토콜을 살펴보고, 3장에서는 제안하는 프로토콜을 소개한다. 마지막으로 4장에서 결론을 맺도록 하겠다.

2. 관련연구

2.1 스마트폰 보안 요구사항

방송통신위원회에서 스마트폰의 보안 위협이 높아짐에 따라 발표한 10대 안전 수칙은 다음과 같다.

1) 의심스러운 애플리케이션은 다운로드를 하지 않는다.
2) 신뢰할 수 없는 사이트는 방문하지 않는다.
3) 발신인이 의심스러운 메시지는 삭제한다.
4) 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호를 변경한다.
5) 무선 인터페이스 기능은 사용시에만 켜놓는다.
6) 악성코드 감염여부를 확인한다.
7) 다운로드한 파일은 바이러스 유무를 검사한 후 사용한다.
8) PC에도 백신프로그램을 설치하고 정기적으로 바

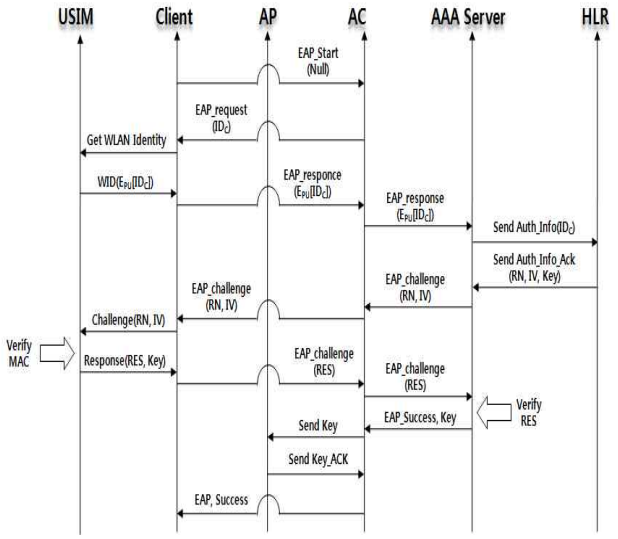
이러스 검사를 한다.

9) 스마트폰 플랫폼의 구조를 임의로 변경하지 않는다.

10) 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 한다.

2.2 EAP-AKA 프로토콜

EAP-AKA 프로토콜이란 EAP 개념을 기존 AKA 인증에 도입을 하여 사용자가 자신의 USIM과 단말기를 이용하여 무선 네트워크에 접속할 때 인증을 하기 위한 프로토콜이다. EAP-AKA 프로토콜의 인증과정은 [그림 1]과 같다.



[그림 1] EAP-AKA 프로토콜 인증 과정

1) Client는 AC에게 무선 네트워크에 접속할 것을 요청한다.

2) AC가 Client의 ID_C를 요구하면 USIM 칩에 저장된 ID_C를 AAA Server의 공개키로 암호화하여 EAP_response/AKA_identity를 통해 AC로 보낸다.

3) AC는 AAA Server로 전송하여 인증 요청을 하면, AAA Server는 개인키로 복호화한 후 HLR에 Client의 ID_C를 전송한다.

4) HLR는 ID_C를 이용하여 RN, IV, Key 생성을 하여 RN, IV는 EAP_request/AKA_challenge를 이용해 USIM 칩으로 보내고 Key는 AAA Server에 저장한다.

5) USIM 칩에서는 MAC값을 검증하여 결과가 성공적일 경우 결과 값(RES)를 AAA Server로 보내고 실패할 경우 재접속을 요청한다.

6) AAA Server는 RES 값을 비교하여 인증을 수행한다.

7) 인증이 성공적이면 AC로 Key를 전송하여 실패하면 Client에게 재전송 요청을 한다.

8) AC는 AP로 Key를 보내고 AP는 수신된 Key가 올바른 Key라고 신호를 보낸다.

3. 제안 프로토콜

3.1 용어 정리 및 기법 설명

AP_MAC : AP의 맥주소

ISP : 이동 통신사 서버(Internet Service Provider)

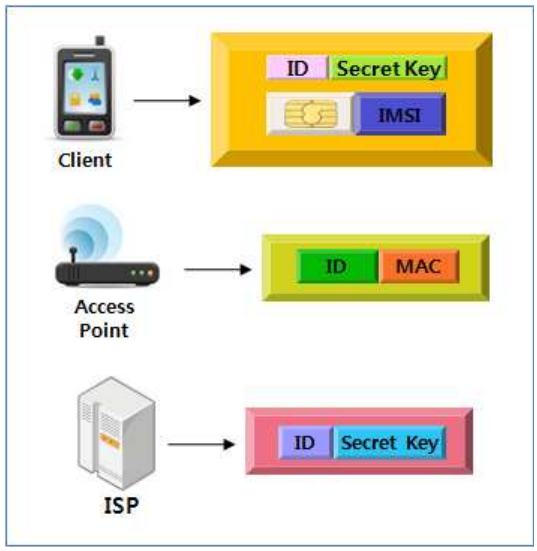
SecretKey : Client와 ISP가 사전에 공유한 비밀 키

IMSI : 국제 모바일 가입자 인증번호(International Mobile Station Identity)

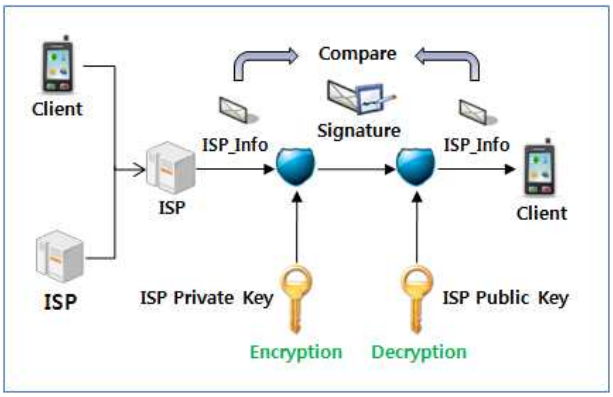
EISP_Pr[AP_MAC] : AP의 맥주소를 ISP의 개인키를 전자서명한 이동 통신사 정보 값

ECA-Pu[ISP_Certificate] : Client에서 통신사 정보의 인증을 CA에게 요청하기 위해 CA의 공개키로 암호화한 값

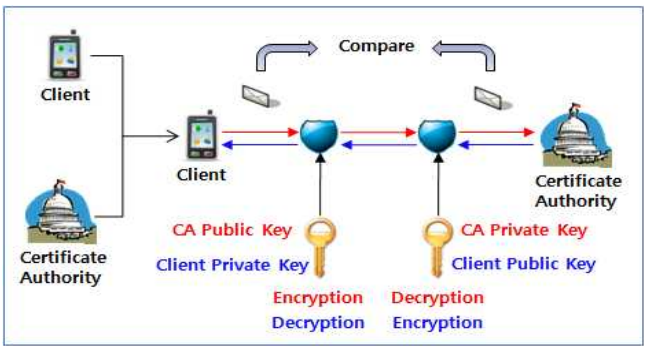
EC_Pu[ISP_Certificate] : CA에서 통신사 정보의 인증을 Client에게 응답하기 위해 Client의 공개키로 암호화한 값



[그림 2] Client, AP, ISP에서 사용되는 용어



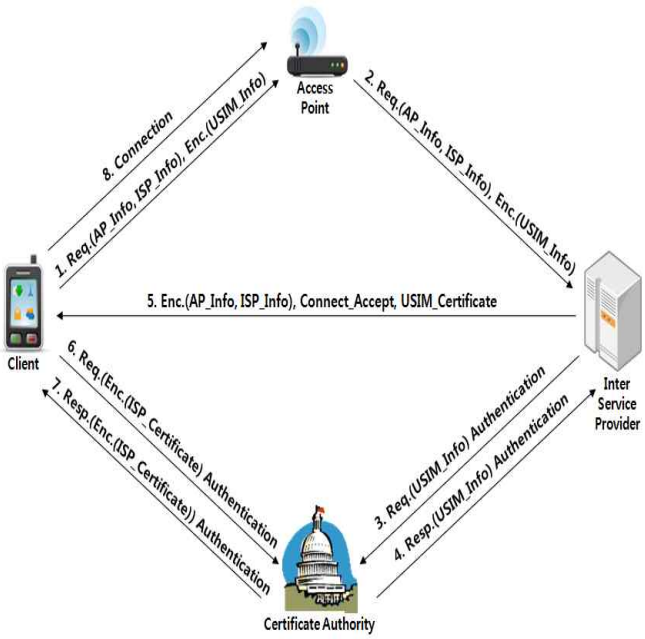
[그림 3] E_{ISP_Pr}[AP_MAC]의 암복호화 과정



[그림 4] E_{CA_Pu}[ISP_Certificate], E_{C_Pu}[ISP_Certificate] 암복호화 과정

3.2 제안시스템 구성도

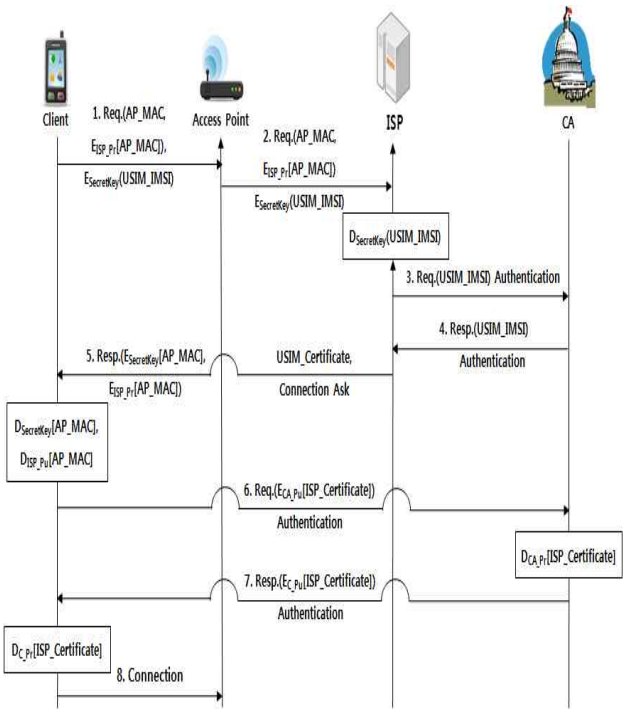
본 절에서는 제안하는 AP 접속을 위한 인증 과정에 대해 기술한다. [그림 5]는 제안하는 전체 시스템 구성도 이며, 다음의 과정을 거쳐 인증이 이루어진다.



[그림 5] 제안시스템 구성도

3.3 제안시스템 상세 프로토콜

본 절에서는 제안시스템 구성도의 상세 프로토콜 과정에 대해 기술한다. [그림 6]는 제안시스템 상세 프로토콜 과정이며, 다음의 과정을 거쳐 인증이 이루어진다.



[그림 6] 제안시스템 상세 프로토콜

1) Client는 AP의 맥주소, 이동 통신사의 정보를 요청하고 자신의 단말 안에 있는 USIM 정보 중에 IMSI 값을 ISP와 사전에 공유하고 있는 SecretKey로 암호화하여 보낸다.
2) AP는 Client로부터 받은 값들을 ISP에게 전송한다.
3) ISP는 Client로부터 받은 정보 값 중에 $E_{SecretKey}$(USIM_IMSI)을 사전에 공유하고 있는 SecretKey로 복호화하여 사전에 신뢰된 기관인 CA에게 USIM_IMSI 값을 확인 요청한다.
4) CA는 ISP로부터 받은 USIM_IMSI 값이 올바른 사용자로부터 전송되어 온 값인지 확인하고 ISP에게 확인 응답을 보낸다.
5) ISP는 Client가 요청한 AP_MAC에 대해 자신이 가지고 있는 AP 맥주소를 사전에 공유하고 있는 SecretKey로 암호화하고 이동 통신사 정보인 EISP_Pr[AP_MAC] 요청에 대해서는 자신의 개인키로 전자서명하여 암호화한다. 동시에 Client가 보낸 USIM_IMSI 값이 확인 되었다는 인증 확인 값과 연결을 할 것인지 메시지를 3G

망을 통하여 보낸다.

6) Client는 SecretKey로 AP_MAC 값을 복호화하고 이동 통신사 정보 값인 E_{ISP_Pr}[AP_MAC]은 ISP의 공개키로 복호화 하여 두 값이 일치하는지 확인한다. 두 값이 일치한다면 CA한테 ISP로부터 받은 이동 통신사 정보가 정확한 것인지 확인을 하기 위해 CA의 공개키를 이용해 암호화하여 인증 요청을 한다.

7) CA는 Client로부터 받은 이동 통신사 확인 요청 값을 자신의 개인키를 이용해 복호화 하여 일치되는 값인지 확인을 하고 일치한다면 Client의 공개키를 이용해 확인 응답 값을 암호화하여 전송한다.

8) Client는 자신의 개인키로 CA한테 받은 값을 복호화하여 이동 통신사 정보의 일치 여부를 확인한다. 동일한 경우 Client는 AP에게 접속을 한다.

4. 결론

본 논문에서 제안하는 시스템은 Client와 ISP가 서로 공유하고 있는 SecretKey를 사용한 대칭키 암호화와 USIM의 IMSI를 사용하여 사용자를 인증하였고, ISP에서는 AP_MAC와 ISP에서 AP_MAC을 전자 서명한 값을 3G망을 통하여 Client에게 전송하고 Client에서는 두 값을 비교 AP를 인증하였다. 마지막으로 Client에서는 CA한테 ISP에 대한 인증 확인 응답을 받음으로서 ISP를 인증한다. 본 논문에서는 Client, AP, 이동 통신사를 인증하고 인증 과정 중에 3G망을 통해서 암호화된 값을 전달하기 때문에 중간자공격(Man in the Middle Attack), Rouge AP공격, Evil Twin 등에 안전하다.

참고문헌

[1] Volker Roth, Wolfgang Polak, Eleanor Rieffel, “Simple and Effective Defense Against Evil Twin Access Points″, Wireless Network Security, 2008.

[2] Janne Lindqvist, Tuomas Aura, George Danezis, “Privacy-Preserving 802.11 Access-Point Discovery″, Wireless Network Security, 2009.

[3] 정병호, 강유성, 김신효, 정교일, “공중 무선랜망에서 인증 및 키관리 기술 동향”, 전자통신동향분석, 제17권, 제4호, 8월, 2002.

[4] 김영세, 이정우, 한진희, 신진아, 전성익, “무선 네트워크 연동 보안 기술 동향”, 전자통신동향분석 제20권, 제1호, 2월, 2005.

[5] 김두환, “3G 네트워크에서 효율적인 인증 관리를 위한 개선된 AKA 프로토콜”, 숭실대학교 석사학위논문, 6월, 2008.

[6] 강봉근, “USIM 카드를 이용한 홈네트워크 인증”, 대전대학교, 2월, 2010.