모바일 클라우드를 위한 Extensible Authentication Protocol(EAP) 연구

황문영*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail : myhwang@sch.ac.kr, jkwak@sch.ac.kr

A Study of Extensible Authentication Protocol for Mobile Cloud

Moon-Young Hwang*, JinKwak**
*ISAA Lab, Department of Information Security Engineering, Soonchunhyang University
**Dept of Information Security Engineering, Soonchunhyang University

요 약

인터넷의 발달은 다양한 인터넷 서비스들을 등장시켰고, 클라우드 컴퓨팅이란 용어가 처음 생겨난 이후 클라우드 컴퓨팅은 차기 비즈니스의 핵심 기술로 주목을 받고 있다. 그 후 클라우드 컴퓨팅을 기반으로 모바일 기술을 결합한 모바일 클라우드 서비스가 등장을 했다. 또한 최근 '모바일화', '개인화', '개방화'의 IT 산업 트렌트에 맞춰 다양한 신규 서비스들이 제공되고 있으며 앞으로도 확대될 전망이다. 사용자의 민감한 정보가 많이 다루어지는 모바일 클라우드의 특성상 보안적인 측면이 많이 고려되어야 하지만 무선 인터넷 환경의 인증 과정은 유선에 비하여 취약점이 존재하고 있다. 그래서 모바일 클라우드 환경에 적합한 인증 프로토콜을 개발하기 위해 현재 사용되고 있는 무선인터넷 프로토콜의 인증 취약점을 분석하고자 한다.

1. 서론

2006년 클라우드 컴퓨팅의 개념이 등장한 이후 현재 클라우드 컴퓨팅과 모바일 기술이 결합된 모바일 클라우드가 새로운 이슈가 되고 있다. 더군다나 최근에는 3G 이동통신, 무선랜 등 무선 통신 인프라의 보급과 스마트폰 등 다양한 모바일 기기의 확산으로 인한 '모바일화', 개인 맞춤형 사용 환경을 구축하고 개인 콘텐츠의 생성과 배포로 인한 '개인화', 사업자의 독자적인 플랫폼으로 발생하는 상호 호환 문제를 해결하기 위한 개방형 기술 적용과 표준화에 대한 요구에 의한 '개방화' 등 IT 산업 트렌트에 맞춰 다양한 신규 모바일 클라우드 서비스들이 제공되고 있으며 앞으로도 확대될 전망이다.[1]

사용자가 모바일 단말을 이용하여 모바일 클라우드 서비스를 제공받고자 할 때 사용자는 스스로 인증을 해야 한다. 이러한 모바일 클라우드 서비스의 인증을 위해 EAP(Extensible Authentication Protocol) 기반의 IEEE 802.1x 표준이 많이 사용되고 있다.[2] EAP 프로토콜을 기반으로 제안되어진 인증 프로토콜은 많지만 제안된 프로토콜들은 각각의 장, 단점이 존재하기 때문에 어느 프로토콜이 모바일 클라우드에 적합한지 알기 어렵다. 또한 대부분의 EAP 인증 프로토콜은 인증과 중간자 공격에 취약점을 가지고 있다.[3] 이런 취약점들은 기존의 모바일 통신에 비해 사용자의 개인정보가 많이 다루어지는 모바일 클라우드 서비스의 특성상 사용자의 프라이버시 침해나 다른 커다란 피해로 확산이 될 수 있다.

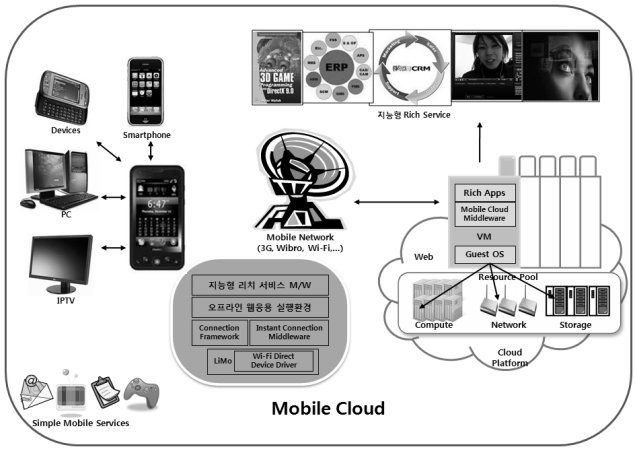
본 논문에서는 현재 제공되고 있는 EAP 기반의 인증 프로토콜보다 모바일 클라우드 서비스를 안전하게 제공하기 위한 프로토콜 개발을 위하여 모바일 클라우드에서 필요한 보안 요구 사항들을 알아보고 취약점들 분석한다.

2장에서는 모바일 클라우드 서비스에 대해 설명하고 3장에서는 EAP 기반의 인증방식을 알아보고 보안 이슈에 대해 분석하였다. 마지막으로 4장에서는 결론을 맺는다.

2. 모바일 클라우드 서비스 개요

모바일 클라우드란 모바일 단말을 이용해서 클라우드 컴퓨팅 서비스를 지원받는 개념이라고 할 수 있다. 대표적인 모바일 서비스로는 애플의 '모바일미(MobileMe)'를 꼽을 수 있는데 이 서비스는 클라우드 환경을 통해 사용자의 메일 및 연락처, 일정 정보들을 관리하고 모바일 기기와 웹 사이트 간에 동기화를 통해 언제 어디서든, 어떤 모바일 디바이스를 사용하든 사용자에게 동일한 데이터와 서비스를 제공한다. 그 외에도 Microsoft의 My Phone, Soonr, Google의 Sync, Motorora, Webex등 다양한 모바일 클라우드 서비스들이 제공되고 있다.

모바일 클라우드는 모바일 단말, 어플리케이션, 모바일 클라우드 이렇게 3개의 구성요소로 이루어져 있다[4].



(그림 1) 모바일 클라우드 구성도

사용자는 모바일 어플리케이션을 통하여 모바일 클라우드 환경에 접속을 하고 클라우드 서비스를 제공 받는다.

3. EAP 기반 인증 방식과 보안 이슈

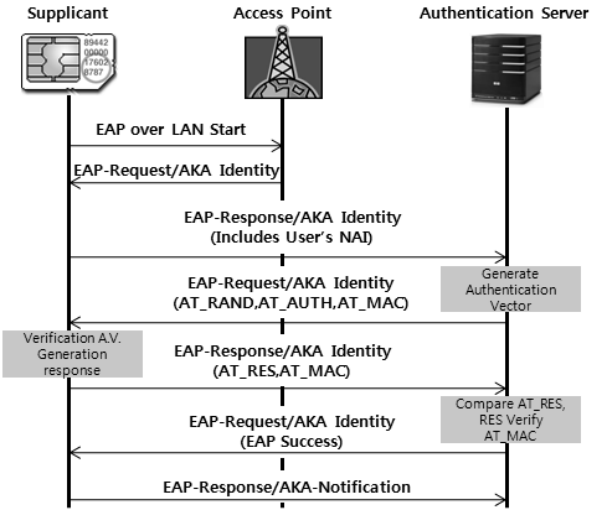
3.1 EAP 개요

EAP는 IEEE 802.1x 포트 기반의 가입자 인증 데이터 전송을 위한 표준 프로토콜이다. 다중 인증 메커니즘을 지원하는 프로토콜로써 스마트카드, Kerveros, OTP(One Time Password) 등 많은 인증 방식을 지원한다.

3.1.1 EAP-AKA(Authentication and Key Agreement)

3GPP에서 제안한 AKA 방식을 EAP의 인증 프로토콜에 적용하여 3GPP와 무선랜과의 연동을 제공하는 보안 인증 프로토콜이다.

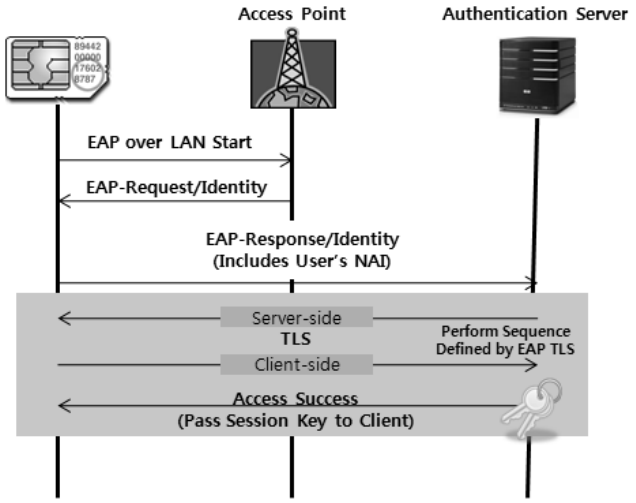
국내에서는 EAP gateway의 기능을 단말장치가 수행하고 나머지 기능을 스마트카드가 수행하는 방법이 휴대 인터넷의 표준으로 채택되어 사용되고 있다. EAP-AKA의 인증 메시지 흐름은 다음 그림과 같다.[5]



(그림 2) EAP-AKA의 인증과정

3.1.2 EAP-TLS(Transport Layer Security)

EAP-TLS는 클라이언트 및 네트워크에 대한 인증서 기반 상호 인증 기능을 제공한다. 이 인증 방법은 클라이언트의 인증서와 서버의 인증서를 통해 인증을 수행하게 되는데 통신에 대한 보안을 강화하기 위해 사용자 기본 키 및 세션 키를 동적으로 생성한다.



(그림 3) EAP-TLS의 인증과정

EAP-AKA, EAP-TLS 외에도 EAP-TTLS, PEAP, EAP-SIM 등 여러 가지 프로토콜이 사용되고 있지만 각 프로토콜의 특징은 모두 다르다. 여러 가지 프로토콜들의 특징은 아래의 표와 같다.

늑징	EAP-AKA	EAP-TLS	EAP-TTLS	PEAP	EAP-SIM
암호타입	대칭키	공개키	공개키	공개키	대칭키
사용자 관리	모바일 사업자	WLAN 사업자	WLAN 사업자	WLAN 사업자	모바일 사업자
IMSI 보호	X	X	O	O	X
중간가 공격 보호	X	O	X	X	X
모바일-WLAN간 로밍	O	X	X	X	O

<표 1> EAP기반 프로토콜의 비교

3.2 EAP 기반 인증 방식의 보안 이슈

EAP 인증 방식에서는 AKA, TLS 방식을 제외한 그 외의 여러 가지 인증 방식을 수용할 수 있다. 여러 가지 인증 방식 중에 모바일 클라우드에 적합한 인증 방식을 선택하기 위해서는 먼저 무선랜 환경에서 요구되는 보안 요구사항들을 분석해야 한다. 다음은 RFC 4017에서 정의되어 있는 보안 요구사항 항목이다.

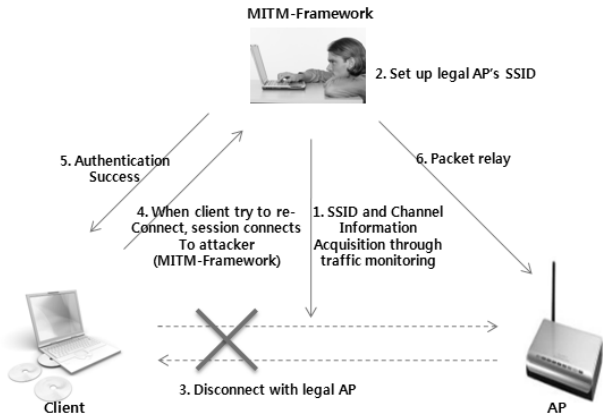
- 상호인증(Mutual authentication) : 클라이언트와 인증 센터는 상호간의 인증을 수행해야 한다.
- 자기보호(Self-protecting) : 악의적인 또는 불법적인

공격으로부터 정보의 기밀성을 보장해야 한다.
- 사전공격(Dictionary Attack) : 사용자의 비밀번호 등을 알기 위하여 challenge-response등 반복되는 사전 공격에 대하여 안전해야 한다.
- 세션 키(Session Key) : 메시지 인증, 기밀성, 무결성 등을 보장하기 위해 동적인 세션키를 생성하고 사용해야 한다.
- 전방향 안전성(Perfect forward secrecy) : 사용자의 비밀정보가 공격자에 의해 노출되지 않는 시점을 말하는데 최초 인증단계에서 획득한 세션 정보 값으로는 그 이후의 인증과정에서도 사용자의 정보를 얻을 수 없어야 한다는 것을 말한다.

위와 같은 보안 요구사항들을 만족시키고 안전한 통신을 제공해야 하지만 실제로 EAP의 대표적인 EAP-AKA 방식에서는 다음과 같은 문제점들이 존재한다.[5]

- IMSI(Interational Mobile Subscriber Identity)의 노출
- 중간자 공격
- 전방향 안전성
- 네트워크 대역폭의 소비
- SQN 동기화

그 중에서도 대표적인 취약점으로 뽑히고 있는 중간자 공격의 경우 아래의 (그림 4)와 같은 과정을 통해 클라이언트와 AP간의 정보를 쉽게 얻는 것이 가능하다. 사용자의 민감한 데이터들이 많이 다루어지는 모바일 클라우드 경우 사용자는 심각한 프라이버시 침해를 받을 수 있다.[6]



(그림 4) 중간자 공격의 과정

(1) AP와 클라이언트 사이의 통신을 도청하면서 SSID나 AP의 채널 같은 정보를 수집한다.
(2) 공격자는 수집한 정보를 통해 SSID와 채널을 만든다.
(3) 클라이언트와 정상적인 AP사이의 세션을 차단한다.
(4) 클라이언트는 재접속을 위해 AP를 스캔하고 공격자의 로그 AP(MITM-Framework)에 연결이 된다.
(5) 공격자는 클라이언트를 인증하고 연결 성공 메시지를 포함한 패킷을 클라이언트에게 전송한다.
(6) 클라이언트로 받은 패킷들을 정상 AP로 전송한다.

위에 그림에서 볼 수 있듯이 MITM 모듈은 무선 클라이언트와 정상적인 AP사이의 패킷을 살피고 가로채는 기능, 로그 AP를 가지고 클라이언트를 공격자에게 연결시키는 기능, 정상적인 AP에게 패킷을 전달하는 기능을 가지고 있다.

중간자 공격(MITM) 외에도 EAP에 대한 Denial of Service(DOS) 공격이 충분히 가능하다는 분석도 나와 있다.[6]

4. 시사점 및 결론

본 논문에서는 모바일 클라우드 서비스에 대한 일반적인 정의와 서비스 종류, 또 그에 따른 보안 문제점을 분석하고 현재 사용되고 있는 EAP 기반의 여러 가지 프로토콜을 비교하였다. 모바일 클라우드 서비스는 역사가 짧기 때문에 모바일 클라우드 서비스만을 위한 시스템이나 보안 기술들에 대한 연구는 미미하다. 현재 해외 대기업들이 소비자 시장과 IT구매시장을 중심으로 사업을 확장하고 있으며, 국내에서도 정부가 앞장서서 모바일 클라우드 시장을 키우려고 노력중이기 때문에 모바일 클라우드 컴퓨팅 환경이 확대 될 경우 이에 따른 보안 문제는 더욱더 많은 취약점을 수반할 것으로 예상 된다.

현재 모바일 클라우드 서비스는 여러 가지 보안성의 문제로 사용자들에게 신뢰를 얻지 못하고 있다. 하지만 기존의 네트워크 기술을 분석하고 다양하고 새로운 기술을 연구·개발을 한다면 우리나라가 모바일 클라우드 서비스 시장에서의 위치를 확고히 할 수 있을 것으로 기대된다.

참고문헌

[1] 최우석, “클라우드 컴퓨팅 서비스 전개와 시사점”, SERI경영노트, 삼성경제연구소, 2010
[2] 손영설 외, “휴대인터넷에서의 UICC 기반 EAP-AKA 인증처리 기술에 관한 연구”, 한국통신학회, 2006
[3] Yuh-Min Tseng, “Usim-based EAP-TLS authentication protocol for wireless local area networks”, ScienceDirect, 2009
[4] 김학영 외, “모바일 클라우드 기술 동향”, ETRI, 2010
[5] Hyeran Mun 외, "3G-WLAN Interworking: Security Analysis and Authentication and Key Agreement based on EAP-AKA", IEEE, 2009
[6] Mina Malekzadeh 외, "Vulnerability Analysis of EAP DOS Attack over Wireless Networks, ICGST, 2009
[7] Hyunnuk Hwang 외, “A Study on MITH Vulnerability in Wireless Network Using 802.1x and EAP”, ICISS, 2008