무선 네트워크에서의 EAP

한경헌[1] · 박규진[1]· 최동유[1] · 한승조[1*]

[1]조선대학교

WLAN of Extensible Authentication Protocol

Kyong-heon Han[1] · Kyu-jin Park[1] · Dong-you Choi[1] · Seung-jo Han[1*]

[1] Dept. of Information and Communication Engineering, Chosun University

[1*]Corresponding author (Email: sjbhan@chosun.ac.kr)

요 약

본 논문에서는 증명프로토콜(EAP)을 분석하는 것에 중점을 두고 있다. 무선네트워크 환경에서 안전하게 통신하기 위해 사용되는 EAP 방법을 검토하여 그 방법들의 이점과 취약점을 분석하며, 새로운 프로토콜을 제안한다. 제안된 프로토콜은 무선 네트워크인 802.11에 맞추어 설계하였다. 그리고 802.11 환경이 아닌 다른 무선 네트워크 환경인 RFID와 WiMAX 환경에서 EAP가 가져야 하는 특징을 제시하며 3G네트워크 환경에서 가져야 할 새로운 특징을 제안한다.

키워드

EAP-TLS, LEAP, EAP-SIM, EAP-AKA

Ⅰ. 서 론

현재 무선 랜의 사용이 급증하면서 개인 또는 기업의 사용자들에게 빌딩이나 캠퍼스에서 전자상거래, 전자 메일과 같은 중요한 정보를 비밀리에 전달하고자 하는 보안성 요구가 더욱 증가하게 되었다. 그리고 무선 랜은 사용의 편리성을 주는 대신 해킹의 용이성, 단말의 이동에 대한 복잡성이라는 문제를 주었다. 이런 문제의 해결을 하기 위해 무선 랜 보안 방법과 보안 프로토콜이 발전하게 되었다.[2]

네트워크 보안을 고려할 때 기본적인 이슈 중의 하나는 증명과 승인이다. 네트워크에 가입하고 서비스와 리소스에 접근하도록 허락 받을 것인지 아닌지 결정할 뿐만 아니라 사용자나 네트워크에 접근하려고 하는 장치의 유효한 신원을 증명한다. 증명 방법은 모든 네트워크를 안전하게 하는 것이 필수적이고 각 개인적인 네트워크의 독특한 요건에 관심을 기울이면서 만들어 져야 한다.[2] 인증유형들에는 EAP-MD5, EAP-TLS, LEAP등이 있지만 이 프로토콜 또한 문제점을 가지고 있다. 본 논문에서는 IEEE 802.1x 기반의 EAP 인증의 문제점을 알아보고 이 문제점을 보안하여 새로운 프로토콜을 설계하고자 한다.

Ⅱ. 본 론

EAP의 인증 유형을 간단히 살펴보겠다.

EAP-MD5는 IEEE 802.1x에서 가장 기본적인 수준의 인증을 하는 방법이다. 패스워드 기반의 인증 방식은 사용자와 서버사이에 상호인증이 없

이 무조건 서버를 믿는 방식이다. [3,4,5]

EAP-TLS는 각각의 인증서를 이용하여 상호 인증하고, 그 결과에 의해 쌍방 간에 공유하는 비밀키를 생성하여 이후 전송되는 데이터들을 보호하는 프로토콜이다. TLS의 가장 큰 특징은 안전한 터널을 기반으로 세션 기반의 동적인 WEP키를 생성하여 분배한다는 것이다.

EAP-TTLS와 PEAP는 서로 비슷한 인증 프로토콜이다. 단말과 서버 모두 인증서가 사용하는 가장 확실한 인증 방법이지만 모든 단말에 인증서를 설치하는 것이 비용이 많이 들어간다는 문제점을 가지고 있다.

LEAP는 시스코 무선 랜 AP에 주로 사용되는 인증 프로토콜이다. 사용자와 서버의 인증을 모두 수행하는 상호 인증절차가 사용된다. 하지만 사용자 입장에서는 무조건 서버인증을 믿어야 하는 일반향성 인증이 문제점이다.

EAP 방법의 기술과 기본 요건에 대한 내용은 다음 표에서 나타내었다.

EAP type	Dynamic rekeying	User ID and password	Comment
EAP-MD5	NO	YES	· Easy to implement · Support on many servers, but insecure · Requires clear text transmission · Uses databases
EAP-TLS	YES	NO	· Requires client as well as server side certificates · Increases maintenance costs
LEAP	YES	YES	· Proprietary solution from CISCO · AP must have LEAP support
EAP-SIM	YES	NO	· Uses SIM card and authentication method from · GSM wireless standards
EAP-TTLS	YES	NO	· Creates secure SSL tunnel · Supports legacy authentication method · User identity is protected
PEAP	YES	NO	· Similar to EAP-TTLS · Creation of a secure SSL tunnel · User identity is protected
EAP-SPEKE	YES	NO	· Proprietary solution from Interlink Network · Based on Diffie-Hellman algorithm

표 1. EAP 특징

Requirement	EAP-MD5	EAP-TLS	EAP-TTLS	LEAP	PEAP	EAP-SPEKE
Mandatory						
Generation of keying material	NO	Not required	YES	YES	YES	YES
Mutual authentication	NO	YES	YES	YES	YES	YES
Self protection	YES	YES	YES	YES	YES	YES
Resistance to dictionary attack	Only with long passwords	YES	YES	NO	YES	YES
Protection to MITM attack	NO	YES	YES	YES	YES	YES
Protected cipher suite negotiation	NO	Not required	YES	YES	YES	YES
Recommended						
User identity hiding	NO	NO	YES	NO	YES	NO
Faster reconnect	NO	YES	YES	NO	YES	NO

표 2. 무선 랜을 위한 EAP 요건

기존 인증 유형은 여러 가지 문제점을 가지고 있다. EAP-MD5의 문제점은 인증을 위하여 사용자의 이름과 패스워드를 전송할 때 암호화 되지 않는 상태에서 전송을 한다. 그리고 단방향으로만 인증이 된다는 것이 문제점이다. EAP-TLS의 문제점은 인증 절차가 완료되기 전까지 네트워크를 이용할 수 없기 때문에 인증서의 유형성 검증을 요청할 수 없으므로 클라이언트는 인증 서버를 실시간으로 인증할 수 없다. EAP-TTLS와 LEAP의 문제점은 클라이언트 인증은 공인이 되지 않은 인증이라는 것이다. 그리고 EAP-TLS와 같이 클라이언트는 인증 서버를 실시간으로 인증할 수 없다. [6]

이렇듯 안전하게 네트워크에서 EAP 방법의 사용으로 사용자나 장치가 진품임을 증명할 인증 보안을 제공하는 것은 아니다. EAP의 공격 방법은 몇가지로 표현할 수 있다.

EAP는 공격을 받을 수 있고 그 공격에 대해 보호하는 방법이 현재 많이 연구 되고 있다. EAP에 대한 공격이 가능한 방법은 다음 표와 같다.

EAP method	Encryption technologies	Possible attacks
EAP-MD5	• One-way message digest	• Dictionary attack • Man-in-the-middle attack
EAP-TLS	• Digital certificates	• Strong authentication, resistant to attacks
EAP-TTLS	• Digital certificates • Diffie-Hellman algorithm to generate keying material • Symmetric key for data encryption	• Strong authentication, resistant to attacks
EAP-SIM	• Symmetric key generated using GSM authentication key	• Possible spoofing • Does not provide session independence
PEAP	• Digital certificates • Diffie-Hellman algorithm to generate keying material • Symmetric key for data encryption	• Strong authentication, resistant to attacks
LEAP	• Diffie-Hellman algorithm to generate keying material • Symmetric key for data encryption	• Dictionary attack

표 3. EAP 암호화 기술과 가능한 공격 비교

III. 프로토콜 제안

기존의 EAP 방법은 여러 가지의 문제점을 발생하기 때문에 현재는 PKI를 적용한 인증방법이 연구되어지고 있지만, 높은 보안성을 제공한는 EAP-TLS의 경우에는 실시간 인증이 되지 않지 않아 인증서 교환의 효율성이 떨어진다는 것이 문제가 되어 실시간 상호 인증이 가능하고 시간차 문제를 해결해주는 효율적인 프로토콜의 필요성을 느끼게 되었다.

그래서 제안하는 프로토콜은 EAP-TLS와 EAP-SIM의 장점을 혼합 시킨 프로토콜이다. 상호 증명과 고도의 보안을 제공하기 위해 기존의 EAP-TLS 프로토콜을 사용한다. 이 프로토콜의 특징을 살펴보면 클라이언트 증명은 SIM을 통해서 하며 사용자 신원 보호는 강하며 Cellular network와 WLAN를 둘 다 접속이 가능하다는 것이다.

다음 다이어그램에서 나와 있는 용어는 다음과 같다.

- MT: Mobile Terminal
- AP: Access Point
- W-AS: WLAN Authentication server
- C-AS: Cellular network Authentication server

다이어그램에 보듯이 1번에서 4번까지의 인증 절차는 기존 EAP-TLS와 같다. 하지만 5번부터 7번까지의 인증 절차가 변화 시켰는데 그것은 다음과 같다.

5. Response/CTLS
(Client-Hello, MT-Cert-Rqst-Msg)
Clinet_Hello는 기존 TLS와 같은 메시지이지만 MT-Cert-Rqst-Msg 는 다음과 같은 $(pk_A, TID_A, E_{PKC}(ID_A, R_A), N, H)$을 전송하게 된다.

5.1 MT_Cert_Rqst_Msg
W-AS가 인증 요구 메시지를 무시할 경우 C-AS는 3번 인증과정(Reponses/Identity)을 통해서 전송을 받는다.

5.2 MT_Tem Certificate
전송을 받으면 C-AS는 W-AS에게 Temporary Certificate을 보내게 된다.

6. Request/CTLS
(Server_Hello, Certificate,
Server_key_Exchange, Client, Tem Certificate,
Server_Hello_Done)
MT의 Temporary Certificate을 알게된 W_AS는 EAP응답 메시지를 보낸다. 여기서 알게된 Temporary Certificate는 오직 6번 인증과정에서만 쓰이게 된다.

7. Response/CTLS
(Client_Key_Exchange, Certificate_Verify,
Change_Cipher_Spec, Finished)
MT는 기존의 EAP-TLS와 같이 행동을 한다.
W-AS에게 Certificate에 대한 응답을 하지 않는다. 그 이유는 이미 인증과정 5.2에서 W-AS는 MT의 Certificate를 가지고 있기 때문이다.

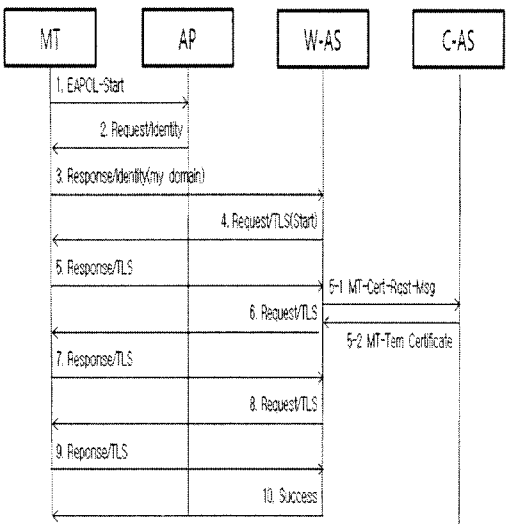


그림 1. 프로토콜 제안 다이어그램

Ⅳ. 결과 분석

무선 네트워크 환경은 OPNET 10.0 시뮬레이터를 이용하여 설계하였으며 이를 이용해 기존의 EAP-TLS 인증 방식과 제안한 시스템과 비교 하였다. 시뮬레이션 환경은 다음 그림과 같이 만들었다. [1]

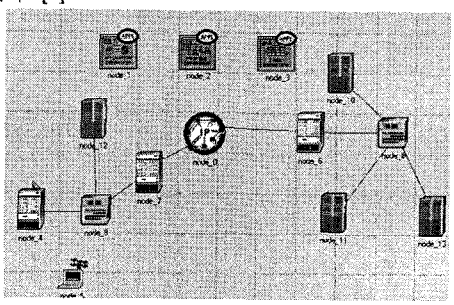
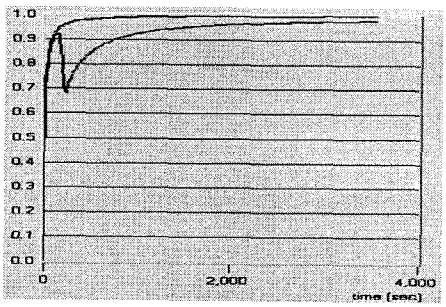


그림 2. 시뮬레이션 환경

Application 영역에서는 시뮬레이션 환경값을 기존의 EAP-TLS와 같이 적용하여 아래 그림과 같은 결과를 얻게 되었다.



위에 나타난 선은 제안한 프로토콜의 전송 효율을 시간에 따라 나타낸 것이고 아래선은 기존의 EAP-TLS의 전송 효율을 나타낸것이다.

단위는 packet/sec으로 결과값을 보듯 기존의 프로토콜보다 약 10%정도 효율이 좋아 진 것을 볼 수 가 있다. 하지만 이것은 EAP-TLS 특성상 인증 도중에는 네트워크를 이용할 수 없다는 문제점 때문에 나타난 결과값의 차이이므로 EAP-TLS의 문제점인 인증과정 도중에 네트워크를 할수 없다는 것을 어느 정도 해결할 수 있는 결과라고 본다.

Ⅴ. 결 론

본 논문에서 제안하는 방식은 인증 서버를 WLAN과 Cellular network 두 개를 사용함으로써 안전성, 효율성 측면에서 기존 시스템의 문제점이 개선되었음을 분석하였고, 시뮬레이션 결과에서 볼 수 있듯이 성능 또한 EAP-TLS의 대기 시간보다 단축되었음을 볼 수 있다. 향후 인증 시스템이 802.11환경에서만 쓰이는 것이 아니라 다른 무선 네트워크 환경에서도 사용될 경우 무선 네트워크에서 보다 안전적이고 효율적으로 인증을 할 수 있는 방법이 매우 중요하다고 볼 수 있다. 무선 네트워크 환경에서 보다 나은 EAP 시스템을 설계하기 위해 많은 참고 사항이 되었으면 한다.

참고문헌

[1] OPNET Modeler Simulation Software, htttp://www.opnet.com

[2] S. K. Miller "facing the challenge of Wireless security", Computer.org pp.16-18, 2001

[3] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", IETF RFC 2284, Mar. 2001

[4] R.Rivest, "The MD5 Message-Digest Alogorithm:, IETF RFC 1321, April 1992

[5] L. Blunk, "PPP Extensible Authentication Protocol", IETF RFC2284, Mar. 1998

[6] W. Diffie and M. E. Hellamn, "New directions in cryptography", IEEE Transactions on Information Theory, pp.644-654 1976

※ This work was supported by research funds from chosun university, BK21