NGN을 위한 EAP의 요구사항에 관한 연구*

이성용, 김락현, 염흥열*

*순천향대학교 정보보호학과

A Study on EAP Requirements for NGN

Sung-Yong Lee, Rack-Hyun Kim, Heung-Youl Youm*

*Department of Information Security Engeneering, Soonchunhyang University.

요 약

확장 가능한 인증 프로토콜(EAP, Extensible Authentication Protocol)은 일반적으로 네트워크를 접근하려는 사용자를 인증하는 프로토콜로써, 인증을 요청하는 인증 요청자와(supplicant)와 인증을 수행하는 인증서버 (authentication server) 간에 수행되는 프로토콜이다. 현재 여러 국제표준화기구들에서 확장 가능한 인증 프로토콜에 대한 표준화가 진행되고 있다. 특히 ITU-T의 SG17 Q.9에서는 안전한 패스워드 인증 프로토콜에 대한 가이드라인 표준이 제안자에 의하여 수행되고 있고, SG17 Q.5에서는 NGN을 위한 인증 및 키관리 프레임워크에 대한 표준화가 제안자에 의하여 수행되고 있다. 본 논문에서는 EAP의 표준화 동향과 NGN를 충족시키기 위한 EAP의 요구사항에 대하여 알아본다.

I. 서론

현재 IETF에서는 확장 가능한 인증 방식에 대한 표준화가 EAP 작업반을 중심으로 추진 중에 있고, 또한 갱신된 EAP 작업반이 최근 구성되어, 이에 대한 표준화와 연구가 수행될 예정이다. 현재 5가지 정도의 후보 프로토콜이 제시되고 있으며, 다양한 방식에 대한 연구가 수행될 예정이다.

ITU-T 에서도 SG17 Q.9에서 안전한 패스워드 인증 프로토콜에 대한 가이드라인 표준이 제안자에 의하여 수행되고 있고, SG17 Q.5에서 NGN을 위한 인증 및 키관리 프레임워크에 대한 표준화가 저자에 의하여 수행되고 있다.

II. EAP 표준화 동향

① EAP(Extensible Authentication Protocol): 이 표준은 1998년 3월 IETF RFC 2284로 표준화된 프로토콜로서, 인증자와 신청자 간에 특정의 인증 메카니즘에 무관하게 관련 인증 메시지를 교환하기 위한 프로토콜이다. EAP 패킷의 종류는 요구(request), 응답(response), 성공(success), 실패(failure)의 네 가지 유형을 갖는다. 이 표준은 다양한 하부 인증 메커니즘을 수용하는 확장 가능한 인증 프로토콜이다. 구체적으로 확장 가능한

* 본 연구는 국가보안기술연구소의 확장 가능한 인증방식 연구 사업의 연구결과로 수행되었음.

주요 EAP는 EAP-MD5, EAP-TLS, EAP-SRP, EAP-TTLS 등이다

② IETF : 현재 IETF에서는 확장 가능한 인증 방식에 대한 표준화가 EAP 작업반을 중심으로 추진 중에 있고, 또한 갱신된 EAP 작업반이 최근 구성되어, 이에 대한 표준화와 연구가 수행될 예정이다. 현재 5가지 정도의 후보 프로토콜이 제시되고 있으며, 다양한 방식에 대한 연구가 수행될 예정이다. 또한 IETF에서도 EAP에 대한 안전성을 검토하기 위하여 2005년 11월 BOF를 만들어 이에 대하여 연구하고 있다. 여기서 고려하고 있는 확장 가능한 인증 방식은 (1) 현재 유일하게 RFC로 표준화 되어 있는 EAP-TLS에, (2) 공개키 기반으로 동작하는 EAP-IKEv2, 공유 비밀 방식으로 동작하는 EAP-IKEv2, EAP-PAX, EAP-SKL, EAP-PSK, EAP-MAKE, EAP-Double-TLS, EAP-TLS with TLS-PSK, (3) 터널 방식으로 동작하는 EAP-FAST, EAP-TTLSv0, EAP-TTLSv1, PEAP v0, PEAP v1, PEAP v2, (4) 일회용 패스워드로 동작하는 OTP, EAP-OTP, (5) 셀루라 망을 위한 EAP-SIM, EAP-AKA 등이다. 이에 대한 표준화와 연구는 앞으로도 계속 수행될 것이다.

③ ITU-T : ITU-T에서도 SG17 Q.9에서 안전한 패스워드 인증 프로토콜에 대한 가이드라인 표준이 제안자에 의하여 수행되고 있고, SG17 Q.5에서 NGN을 위한 인증 및 키관리 프레임워크에 대한 표준화가 제안자에 의하여 수행되고 있다

Ⅲ. EAP의 개요 및 인증 유형

1. EAP 개요

EAP는 패킷내의 다양한 인증방식을 내부적으로 캡슐화 하여 여러 인증방식을 선택적으로 적용하는 것이 가능하기 때문에 NAS(Network Access Server) 의 부담을 덜어준다. 인증방식에는 EAP-MD5, EAP-TLS, EAP-TTLS, OTP(One Time Password), GTC(Generic Token Card), EAP-SRP, EAP-AKA(Authentication and key Agreement) 등이 있고 사용자들은 이들 인증방법 중에서 협상을 한 후 인증절차를 수행한다. EAP는 확장성이 좋고 하위 계층에 많은 기능을 요구하지 않아, 802.1x에서 응용하기에 적합한 프로토콜이다. IEEE 802.1x에서는 다양한 프로토콜 중에서 EAP, TLS, RADIUS를 사용하도록 권고하고 있고, 앞으로는 EAP-TLS, 혹은 EAP-TTLS를 사용할 것을 권고안을 심의 중에 있다.

IEEE 802.1의 스택(stack)에서 EAP를 처리하는 흐름은 다음과 같다: 가입자(user, 단말)와 브리지 간에 TLS, EAP 가 Ethernet에서 전달될 수 있도록 MAC 계층 프로토콜인 EAPoL을 사용한다. 인증자와 인증서버 간에는 EAPoL에 실려온 EAP부분을 뽑아낸 후 RADIUS 또는 Diameter 패킷(EAP over RADIUS)으로 전환되어 전송된다. 가입자에서 보내어지는 인증정보는 EAP over EAPoL에 의해 브리지로 전달되고 브리지에서는 EAP 패킷을 유선망을 사용한다면 RADIUS 패킷 전환하고, 무선망을 이용하여 인증을 수행한다면 Diameter 패킷으로 전환하여 인증서버로 전달된다.

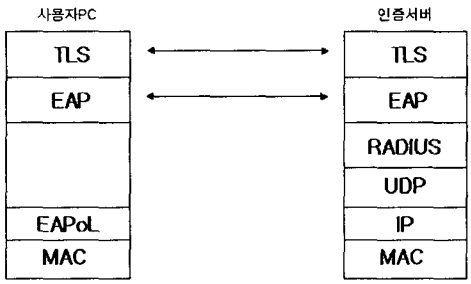

그림 1 IEEE 802.1x에서 사용하는 프로토콜 스택

802.1x를 구현하는 방식에는 EAP에 따라 여러 방식(EAP-TLS, EAP-TTLS, EAP-SRP, EAP-MD5)으로 분류된다.

- EAP-MD5(Message Digest 5) : EAP-MD5 인증 방식은 패스워드 기반의 네트워크 인증 방식이다. EAP-MD5는 인증서버에 사용자 이름과 패스워드 정도의 데이터만 관리함으로서 관리의 편리성을 제공하는 반면 무선 LAN에서 암호화 키를 만들지 않아 다른 EAP 방식보다 보안에 취약하다.

- EAP-TLS(Transport Level Security) : EAP-TLS(RFC2716) 방식의 802.1X 프로토콜은 가장 일반적인 인증서 기반의 인증 방식이다. EAP-TLS 프로토콜은 인증서를 기반으로 하는 무선 클라이언트와 인증서버 간의 세션키를 만드는 상호 인증을 지원한다. EAP-TLS를 사용했을 때 장점은 최종 사용자의 신원을 확인하는 방법으로 인증서를 사용한다는 것이다. 그러나 이는 규모가 큰 WLAN을 설치하는 경우 복잡한 인증서 관리 체계를 지녀야 한다.

- EAP-TTLS(Tunneled TLS) : EAP-TTLS 방식은 EAP-TLS방식과 CHAP(Challenge Handshake Authentication Protocol) 또는 OTP(One Time Password)와 같은 전통적인 암호 기반의 결합 방식이다. 이 방식은 무선 클라이언트에서 인증서가 아닌 패스워드를 사용한다. 인증서는 오직 TTLS 서버에서만 필요하기 때문에 인증서의 개수를 줄일 수 있는 동시에 관리도 간소화할 수 있다. TLS 터널은 처음에 무선 클라이언트와 인증서버 간에 만들어진다. 무선 클라이언트는 TTLS 서버로부터 부여되는 인증서를 인증함으로서 연결되는 네트워크를 인증한다. 일단 인증된 터널이 만들어지면 최종 사용자에 대한 인증이 수행된다. EAP-TTLS는 무선 네트워크에서의 최종 사용자에 대한 동일성을 보장하는 장점을 지니고 있으며, 또한 EAP-TTLS의 최종 사용자의 익명성이 보장되며 기존 어떤 RADIUS 서버와도 연동 가능하다.

- EAP-SRP(Secure Remote Password)[14] : Thomas Wu는 검증자 기반 SRP[7]프로토콜을 제안하였다. SRP는 비대칭형(검증자, verifier) 메커니즘의 키분배 프로토콜로서 분할 공격(partition attack)에 안전하고 부분군 제한 공격에도 강한 특성을 지닌다. SRP는 인증서버가 검증자 를 알고 있고 있는가에 대한 확인과정과 클라이언트가 패스워드를 알고 있는가에 대한 확인과정이 시도-응답 방법으로 처리된다. SRP에 바탕 둔 EAP-SRP는 상호인증 및 전방향 안전성(forward secrecy)을 제공하는 패스워드 기반 인증된 키교환으로서 개체인증 및 세션키 생성이 동시에 이루어진다. EAP SRP 인증서버는 인증서 대신 가입자의 패스워드 검증자만을 저장하기 때문에, 인증서 관리에 따르는 성능 저하를 막을 수 있으나 단말측에 많은 연산을 필요로 한다.

2. EAP의 기본 흐름

EAP는 PPP(Point-to-Point Protocol, 두 지점 간 프로토콜)에서 규정된 인증방식의 확장을 용이하게 하기 위하여 제안되었다. 일반적인 접속서비스 장치인 NAS는 단말간에 PPP 연결시에 LCP(Link Control Protocol)을 교환하여 링크설정과정을 수행한다. 링크 설정과정에서는 데이터링크의 동작변수, 즉 인증프로토콜의 종류를 협상한다. NAS는 자신에게 연결된 인증서버가 사용하는 인증프로토콜의 종류를 미리 알고 있어야하는 한다. 만일 NAS가 n개의 다른 인증서버를 사용 한다면, n개의 다른 인증프로토콜의 종류를 명시하는 영역을 LCP에 명시해야 하는 문제점이 발생한다. 이러한 문제점을 해결하기 위하여 별도의 인증프로토콜을 규정하고 헤더부분에 인증방법의 종류를 구분해 놓는다. 이렇게 하므로 NAS는 인증방법에 상관없이 단순히 EAP만 인증서버에게 전달한다. NAS는 인증을 위한 정보만을 통과 시켜주고 최종적으로 인증 성공/실패 결과만 인증서버로부터 받게 된다.

Ⅳ NGN을 위한 확장 가능한 인증 방식 요구사항

1. NGN

NGN(Next Generation Network)은 패킷 기반의 통신 서비스를 제공하기 위한 네트워크로서, 광대역 고속 통신이 가능하고, 처리능력 및 전송지연 등의 서비스 품질이 보장되며, 전달 기술과 서비스 기술이 독립적이며, 완전한 이동성을 지원

하는 ITU-T가 개발중인 차세대 통신망이다.

2. NGN 보안 위협

NGN에서의 보안 위협으로는 크게 다음과 같은 것들이 있다.

- 사용자 관점에서의 보안 위협 : 메시지의 도청, 패스워드 등의 중요 기밀 정보의 도난 및 손실, 원하지 않은 스팸, 아이디 도용, 바이러스/웜/스파이웨어로부터의 단말 오염, 사용자에 대한 프라이버시 손실, 서비스 가용성 부재, 그리고 공격자에 의한 과도한 트랙픽 집중을 통한 단말에 대한 트래픽 플루딩(flooding) 공격

- 서비스 제공자 관점에서의 보안 위협 : 서비스의 도용, 서비스 거부 공격 등의 망에 대한 사이버 공격, 네트워크 구조의 인가되지 않은 공개, 그리고 비인가된 네트워크 설정 및 구조 변경

3. NGN을 위한 확장 가능한 인증 방식 요구사항

- 대칭키 재료 생성: 확장 가능한 인증 방식은 프로토콜을 완료하고 나서 상대방을 서로 인증함과 동시에 추후의 세션을 위한 암호키 생성을 위한 마스터 키를 생성 할 수 있어야 한다.

- 키 강도: 생성된 키 재료는 적어도 암호키 길이가 적어도 128 비트를 지원하는 암호 알고리즘의 키로 사용 가능한 키를 생성해야 한다.

- 상호 인증 지원: 인증서버는 인증 요청자를 인증하고, 인증 요청자는 인증서버를 인증할 수 있어야 한다.

- 사전공격 예방: 만약 패스워드 기반으로 인증이 이루어지는 경우, 교환되는 메시지로부터 통신 당사자가 공유하고 있는 패스워드를 생성할 수 없어야 한다.

- 중간자 공격 예방: 통신로 중간에 존재하는 중간자(man-in-the-middle)는 교환되는 메시지을 이용하여 인증 요청자를 가장할 수 없어야 하고, 또한 인증 서버를 가장할 수 없어야 한다.

- 보호되는 사이퍼슈트 협상: 협상 과정 동안, 인증 프로토콜이 이용하는 암호 슈트를 인증 요청자와 인증 서버는 서로 협상할 수 있어야 한다. 이러한 특성은 하나의 알고리즘이 타협되었을 경우, 신속히 이에 대처할 수 있는 능력을 줄 수 있다.

- 분할 가능: 메시지의 길이가 정해진 MTU를 초과하는 경우, 이를 분할하여 전송할 수 있어야 하고, 수신단에서는 이를 다시 조합할 수 있어야 한다.

- 종단 개체의 신원 보호: 인증 요청자와 인증 서버에 대한 신원 정보를 보호할 수 있어야 한다.

- 채널 바인딩: 인증과 하위 계층인 링크 계층의 변수가 암호학적으로 안전하게 결합될 수 있어야 한다.

- 서버 타협 공격 저항: 인증 서버의 패스워드 보관 파일이 타협되더라도, 공격자는 인증 요청자를 가장할 수 없어야 한다.

- 서버 타협 기반 사전공격(server compromise-based dictionary attack): 서버의 패스워드 파일이 타협되었더라도 공격자는 이를 이용하여 인증 요청자의 패스워드를 구할 수 없어야 한다.

V. 결 론

ITU-T 에서는 SG17 Q.9(Rapporteur : Heung-Youl Youm)에서 안전한 패스워드 인증 프로토콜에 대한 가이드라인 표준이 제안자에 의하여 수행되고 있고, SG17 Q.5에서 NGN을 위한 인증 및 키관리 프레임워크에 대한 표준화가 저자에 의하여 수행되고 있다. 기존의 확장 가능한 인

증 방식은 위에서 제시된 요구사항을 모두 만족하는 방식은 존재하고 있지 않다. 또한 기존의 확장 가능한 인증 방식은 보안 프로토콜 전문가에 의하여 표준화된 것이 아니라, 통신 프로토콜 전문가에 의하여 표준화된 바 있다. 따라서 IETF에서도 이러한 요구사항을 모두 만족하는 확장 가능한 인증 방식에 대한 연구를 추진하고 있다. 그러므로 현재의 제안된 요구사항을 만족하는 확장 가능한 인증 방식에 대한 연구는 추진되어야 할 시점이라고 할 수 있다.

[참고문헌]

[1] T. Wu, "Secure remote password protocol," *Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium*, pp. 97-111 (1998)

[2] P. MacKenzie and R. Swaminathan, "Secure Network Authentication with Password Identification," *Presented to IEEE P1363.2*, Available at http://grouper.ieee.org/groups/1363/passwdPK/contributions.html#MS (1999)

[3] A. Menezes, P. van Oorschot, S. Vanston "Handbook of applied cryptography," *CRC Press, Inc.*, pp 618 (1997)

[4] Xunhua Wang, "Intrusion Tolerant Password-Enabled PKI," *Proceedings of 2nd annual PKI Research Workshop*, Available at http://middleware.internet2.edu/pki03/PKI03-proceedings. html (2002)

[5] Rack-Hyun Kim, Ho-Sun Yoon, and Heung-Youl Youm, "New Password Authenticated Key Exchange Protocols for Mobile Network," The 8th International Conference on Cellular and Intelligent Communications(CIC2003), pp.451-466, 2003.10, Seoul Korea.

[6] 염흥열, "안전한 통신 서비스 표준화 동향 및 향후 전망", 정보보호학회지 16권 1호 (2006)

[7] H.Y.Youm, J.H.Na, B.M.Jin, "Authentication and key management framework for NGN", ITU-T Geneva(2006)