情報保護學會論文誌
第13券 第4號, 2003. 8

공중 무선랜에서의 이중요소 인증된 키교환 프로토콜

박 영 만*, 박 상 규**

Two-factor Authenticated and Key Exchange(TAKE) Protocol in Public Wireless LANs

Young Man Park*, Sang Kyu Park**

요 약

본 논문에서, 우리는 이중 요소 인증과 사전 계산(precomputation)을 사용하여 공중 무선랜(Public Wireless LANs)에서 노트북뿐만 아니라 PDA에도 적용할 수 있는 새로운 이중 요소 인증된 키교환(TAKE) 프로토콜을 제안한다. 이 프로토콜은 상호 인증, 세션키 설정, 사용자 신원 보호, 그리고 실용적인 half forward secrecy를 제공한다. 프로토콜 수행 중에 가입자 무선단말에 필요한 연산량은 한번의 대칭키 암호와 다섯번의 해쉬함수 뿐이다.

ABSTRACT

In this paper, we propose a new Two-factor Authentication and Key Exchange(TAKE) protocol that can be applied to low-power PDAs in Public Wireless LANs using two factor authentication and precomputation. This protocol provides mutual authentication, session key establishment, identity privacy, and practical half forward-secrecy. The only computational complexity that the client must perform is one symmetric key encryption and five hash functions during the runtime of the protocol.

keyword :

Ⅰ. 서 론

최근, 네트워크 서비스 사업자(NSPs)들은 핫스팟(hot spot)이라고 일컬어지는 공공장소에서 가입자들에게 초고속 무선 네트워크 접속을 제공하는 공중 무선랜(Public WLAN) 서비스를 시작하고 있다. 공중 무선랜은 일반 기업내의 무선랜(WLAN)과는 달리 사업자간 로밍, 신호 간섭(interference), 과금 등 여러 가지 고려해야 할 사항이 많이 있으며, 특히 적대적인 공격자들의 공격에 훨씬 더 취약하므로 무선 보안(wireless security)에 대한 고려가 중요시된다. 무선 보안은 공중 무선랜 서비스의 활성화에 있어 아주 중요한 기술적 장애물이 되고 있다.

그리하여 IEEE 802.11 워킹 그룹은 무선랜 시스템의 보안성을 개선하기 위해 802.1x 규격을 2001년에 확정하여 통과 시켰다. IEEE 802.1x 규격은 사용자 인증을 위한 다양한 인증 프로토콜을 수용하면서 접속 포트에 기반한 접근 제어 기능을 정의하고 있다.[1] 802.1x는 사용자와 인증 서버 사이의 인증 데이터를 전달해 주는 확장 가능한 인증 프로토콜인 EAP (Extensible Authentication Protocol)[2]를 표준 프로토콜로 이용하고 있다. 현재 무선랜 인증을 위한 EAP 방식(EAP-method)으로는 인증서를 이용하는 방식인 EAP-TLS(Transport Layer Security)와 패스워드를 이용

* 한국통신(KT) 서비스개발연구소(youngman@kt.co.kr)
** 한양대학교 전자전기컴퓨터공학부(skpark@hanyang..ac.kr)

하는 방식인 EAP-MD5(Message Digest 5), EAP-SRP (Secure Remote Password) 그리고 인증서와 패스워드를 모두 사용하는 터널(tunnelled) 인증 프로토콜 방식인 PEAP(Protected EAP)와 EAP-TTLS(Tunneled TLS) 등이 있다. 그러나 현재의 EAP 인증 방식들은 각각 단점들을 가지고 있다. 즉, EAP-MD5는 상호인증과 세션 키가 제공되지 않고, EAP-TLS는 PKI(Public Key Infrastructure) 기반을 요구하고, EAP-SRP는 가입자측 단말에 많은 계산량을 요구하며 EAP-TTLS와 PEAP는 man-in-the-middle attack에 취약한 것으로 알려져 있다.[11] 공중 무선랜에서 무선보안을 해결하기 위한 방안으로 TLS, SRP와 같은 유선 보안 솔루션들을 이용하는 방법은 무선 단말 측에 과다한 계산량을 요구하여 좋은 방법이라고 할 수 없다. 특히, PDA (Personal Digital Assistant)를 공중 무선랜에 사용할 경우 PDA에 적합한 안전하고 효율적인 EAP 인증방식을 찾기가 쉽지 않다. 왜냐하면, PDA는 지수화(exponentiation)와 역원(inverse element) 계산과 같은 복잡한 연산량을 수행하는데 시간이 많이 걸리고 전력(power)이 많이 소비되기 때문이다.

또한, 우리는 공중 무선랜에서 패스워드를 이용한 단일 요소(single factor) 인증만으로 가입자 인증을 수행하는 것은 충분히 안전하다고는 생각하지 않는다. 비록 EAP-SRP와 같은 패스워드 인증된 키설정(PAKE) 프로토콜이나, EAP-TTLS 및 PEAP 등이 사전 공격(dictionary attack)에 안전한 프로토콜이라 할지라도 패스워드는 키스트로크 모니터링(keystroke monitoring)이나 사기, 협박 등과 같은 사회 공작(social engineering)적 공격으로 인해 적들에게 패스워드를 노출시킬 수 있기 때문이다 .

따라서 우리는 앞에서 기술한 문제점들을 해결하기 위해 패스워드와 토큰(token)을 이용하여 사용자를 인증하는 이중 요소 인증 방식과 오프라인에서 복잡한 연산을 수행하는 사전계산 방식을 사용하여 새로운 상호 인증 및 키교환 프로토콜을 제안한다.

본 논문의 구성은 Ⅱ장에서 무선랜 보안체계와 공중 무선랜 보안 요구사항들을 알아보고, Ⅲ장에서는 이중 요소 인증에 대하여 살펴본다. Ⅳ장에서는 제안된 TAKE(Two-factor Authentication and Key Exchange)프로토콜의 동작을 설명하고 안전성을 분석한다. 마지막으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. 무선 보안(wireless security)

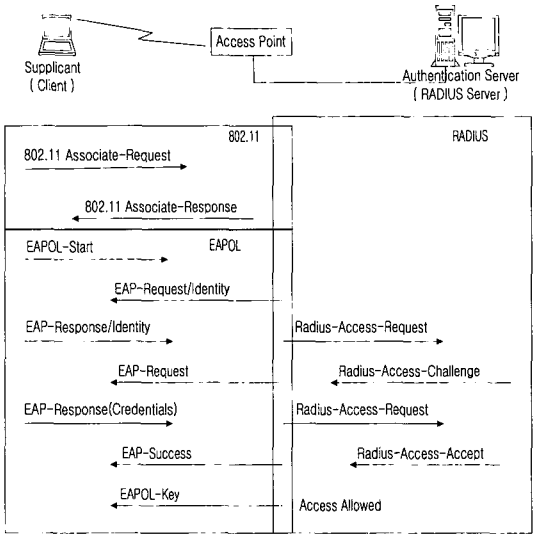
2.1 무선랜(WLAN) 보안

일반적으로 유선 랜(LAN)에서는 물리적으로 포트에 연결된 유선이 공격자가 랜을 해커(hack)하려는데 주요 장애물이 된다. 그러나 무선랜(WLAN)에서는 이런 장애물이 사라진다. 무선랜은 기본적으로 브로드캐스팅 망이므로 무선전파를 수신할 수 있는 영역 내에 있는 단말은 다른 사람의 송수신 데이터 내용을 청취할 수 있다. 따라서 무선랜에서는 데이터 프라이버시와 인증 서비스가 매우 중요하다. IEEE 802.11b[4] 표준은 이러한 보안 문제점을 해결하기 위해 사용자 인증과 WEP(Wired Equivalent Privacy) 알고리즘을 사용하여 데이터 암호화를 수행하도록 정의하고 있다. 그러나 불행하게도 WEP 알고리즘은 여러 보안상의 취약점으로 인해 공격자가 암호문으로부터 평문을 유도할 수 있는 것으로 알려져 있다.[5] 따라서 무선랜의 보안성을 더욱 강화하기 위하여 새로운 암호 알고리즘의 정의와 동적인 키분배 및 인증에 대한 표준화 작업이 필요하다. IEEE 표준화 그룹에서는 802.11b 무선랜 사용자들에게 강화된 보안을 제공하기 위해 802.1x 규격을 표준화하였고, 현재 WEP의 취약점을 해결하고 대체할 수 있는 새로운 알고리즘의 표준화를 추진하고 있다.

2.1.1 IEEE 802.1x(Ported based Authentication)

IEEE 802.1x는 무선랜에서의 인증방법과 무선 구간 보안에 필요한 세션 키를 동적으로 분배하기 위한 방법을 정의한다. 무선랜 인증에는 3가지 주요 개체인 supplicant(client), Authenticator(Access Point), 인증서버(AS)로 되어 있다. 인증서버는 802.1x에서는 정의하지 않았지만 주로 RADIUS(Remote Authentication Dial In User Service)[6]서버를 사용하고 있다. 802.1x에서는 IETF의 EAP 표준 프로토콜을 사용하여 무선랜 사용자의 인증 데이터를 전송한다. 무선랜 인증에 사용될 수 있는 EAP 인증 방식은 Ⅳ장에 있는 [표 1]과 같이 IETF에서 표준화 및 표준화 추진 중에 있다.

802.1x 프로토콜의 동작 절차는 [그림 1]과 같다. AP가 단말(supplicant)에게 사용자 정보를 요구하면 이에 대한 응답인 EAP-Response패킷이 단말로부터 AP에게 전달되고, 이것은 RADIUS의 Access-Request 패킷에 수납되어 인증 서버에 전달된다. 이러한 요청



〔그림 1〕 802.1x를 이용한 EAP 인증 절차

을 수신한 인증서버는 사용자의 신원을 검정하기 위하여 일련의 인증 과정을 수행하여 인증 결과를 단말에게 전달하게 된다. 그리고 AP는 그 인증결과를 참조하여, 자신의 controlled 포트의 활성화를 결정한다.

2.1.2 IEEE 802.11i(Advanced Encryption Standard)

무선랜 보안 관련 표준화를 주도하는 IEEE 802.11i는 무선접속 구간의 데이터 암호화 알고리즘에 대한 표준화 등을 추진하고 있다. 현재 암호화 알고리즘으로는 TKIP(Temporary Key Integrity Protocol)와 AES(Advanced Encryption Standard) 등이 제안되어져 있다. TKIP는 패킷당 키 믹싱(key mixing), Michael MIC(message integrity check), 확장된 IV(Initialization Vector), 그리고 re-keying 메카니즘을 제공하여 기존 WEP의 알려진 취약점을 보완한다. 그리고 무선랜의 시스팀의 하드웨어 변경 없이 소프트웨어 업그레이드를 통해 TKIP를 구현할 수 있게 한다. 아직 크래킹 됐다는 보고가 없는 AES 알고리즘은 새로운 하드웨어가 필요하며 암호화가 하드웨어적으로 처리되어 한층 더 빠르고 안전한 무선랜을 구현할 수 있게 한다.

2.2 공중 무선랜(PWLAN) 보안

공중 무선랜 서비스는 IEEE 802.11b와 같이 국제적으로 표준화된 무선랜 기술을 활용하여 공항, 역, 커피숍, 전시장 등 이른바 핫스팟(hot spot)이라고 일컬어 지는 공공장소에서 일반인을 대상으로 하는 초고속 무선 네트워크 접속 서비스이다. 공중 무선랜 서비스는 현재 셀룰러 이동통신 서비스가 제공하지 못하는 광대역 전송속도로 무선 인터넷 서비스를 제공할 수 있고 유선랜이나 ADSL 통신서비스와 달리 공공장소에서 휴대 및 이동하면서 인터넷이나 인트라넷에 접속할 수 있어 무척 경제적이고 편리한 서비스이라 할 수 있다. 그러나 무선랜 기술은 본래 공중망 서비스를 염두에 두고 개발된 기술이 아니기 때문에 본격적인 서비스 활성화를 위해서는 특히 보안에 관련된 문제점들을 해결하여야 한다.

공중 무선랜에서 인증 및 키교환 프로토콜의 보안 요구사항은 다음과 같다.

① 신원 보호(identity protection) : 공중 무선랜에서 도청과 같은 수동적 공격으로부터 가입자의 신원을 보호하는 것은 개인의 통신비밀(privacy)을 위해 필요하다. 특히, DHCP(Dynamic Host Configuration Protocol)로 IP 주소를 할당받는 사용자에게는 유용한 것이다.

② 강력한 상호인증(strong mutual authentication) : 공격자들은 가입자와 인증서버 사이에 rouge AP(또는 rouge radio NIC)를 설치하여 Man-in-the-Middle(MitM) 공격을 수행할 수 있기 때문에 가입자와 네트워크에 대한 강력한 상호인증이 필요하다.

③ 세션 키 설정 : 가입자와 AP(access point)사이에 교환되는 데이터를 보호하기 위해서 마스터 세션 키가 설정되어 동적인(dynamic) WEP key를 지원하여야 한다.

④ Forward Secrecy(FS) : 프로토콜에 참여하는 개체의 정적인(static) 비밀키가 노출되더라도 공격자가 이전에 도청된 세션으로부터 과거 세션 키를 계산할 수 없는 성질인 FS가 제공되어야 한다.

⑤ 오프라인 사전(offline dictionary) 공격에 안전: 공격자가 오프라인 사전 공격을 수행하더라도 가입자와 인증 서버간에 공유된 비밀정보는 얻지 못하여야 한다.

⑥ Replay 공격에 안전: 공격자가 정상적으로 사용된 메시지를 재전송하여 인증 및 키 설정을 시도하는 replay 공격에 안전하여야 한다.

⑦ 키 확인(key confirmation) : 프로토콜에 참여한 합법적인 사용자가 자신이 의도한 상대방과 실제로 공통의 비밀 세션 키를 공유하였음을 확인하여야 한다.

⑧ 효율성(efficiency)
- 연산 부하의 최소화 : 가입자의 PDA에 적용할 수 있을 정도의 적은 연산량을 요구하여야 한다. 그리고 사전 계산(precomputation)을 이용하여 온라인(online) 계산의 부하를 최소화 하여야 한다.
- 메시지 교환 횟수의 최소화 : 네트워크 자원의 효율성과 네트워크 상의 지연(delay) 등을 고려할 때 통신 라운드(round) 수가 적을수록 장점이 있다. 따라서 가입자와 인증서버 사이에 교환하여야 할 메시지의 횟수를 가능한 적게 하여야 한다.
- 통신 대역폭 사용의 최소화 : 프로토콜 메시지의 크기를 가능한 작게 유지하여야 한다.

Ⅲ. Two-Factor 인증

본 논문에서 사용되는 이중 요소 인증은 (1) 사용자가 알고 있는 것(패스워드)과 (2) 사용자가 가지고 있는 것(토큰이나 무선기기), 이 2개의 요소를 결합하여 개체를 인증하는 인증 방식이다.

패스워드를 이용한 단일 요소(single factor) 인증 방식은 다음과 같은 여러 가지 문제점으로 인해 결코 안전하지 않다. 첫째는 사용자가 패스워드를 입력할 때 누군가가 사용자의 어깨너머로 패스워드를 훔쳐 볼 수 있고, 키스트로크(keystroke) 모니터링으로 패스워드가 노출될 수 있다. 둘째는 사기, 협박 등과 같은 사회 공작(social engineering)적 공격방법으로 패스워드를 공격자에게 노출시킬 수 있다. 셋째는 패스워드는 정보량 측면에서 낮은 엔트로피(entropy)를 가지고 있어 사전 공격(dictionary attack)에 취약하다. 넷째는 패스워드를 물리적으로 기록하거나 유사 패스워드를 여러 곳에 갱신 없이 사용하는 것과 같은 사용자들의 나쁜 습관으로 인해 패스워드가 노출될 수 있다. 그리하여 우리는 이중 요소 인증방식을 사용하여 새로운 인증 및 키 설정(AKE) 프로토콜을 제안하는데, 이 방식은 단일 요소 인증 방식보다 훨씬 더 강력한 인증 방식이며 공격자들은 이중 요소를 모두 다 획득해야 인증에 성공할 수 있다.

그러나 이중 요소 인증에는 두 번째 요소인 토큰과 토큰을 읽을 수 있는 입력장치(카드 리더기)가 필요하다는 단점이 있다. 두 번째 요소인 토큰은 스마트 카드, USB(Universal Serial Bus)기반의 스마트 키, 그리고 PDA와 같은 무선 기기(wireless devices) 등이 될 수 있는데 공중 무선랜 환경에서는 무선기기나 USB기반의 스마트 키를 토큰으로 사용하면 특별히 하드웨어를 추가하지 않아도 된다. 단, 토큰은 대칭키 및 개인의 인증 관련 비밀 정보가 저장되어야 하므로, 어느 정도의 불법 변조 방지(temper resistant)특성을 가진 보안 모듈에 저장되어야 한다.

지금 현재의 이중 요소는 사용자가 알고 있는 것과 가지고 있는 것으로 구성되지만 앞으로는 사용자가 알고 있는 것과 지문, 홍채와 같은 사용자 자신의 것, 이 2개의 요소를 결합하는 방식으로 나아갈 것으로 예상된다.

Ⅳ. 제안한 TAKE 프로토콜

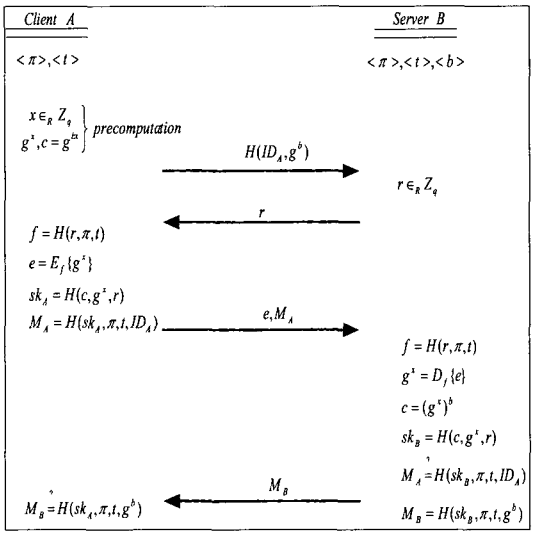
4.1 프로토콜 동작

TAKE 프로토콜은 이중 요소(패스워드와 토큰) 기반의 상호 인증과 세션 키 설정을 제공하는 보안 프로토콜이다. TAKE는 유한체 상의 이산 대수를 이용한 암호 스킴(scheme)으로 세션 키 생성에 있어서는 DH(Diffie-Hellman) 키 교환 방식을 사용한다.그리고 복잡한 모듈라 지수승 계산은 오프라인에서 사전 계산(precomputation)을 통하여 처리하게 하여 PDA와 같은 낮은 연산 처리능력과 제한된 전원을 가지는 무선 기기에 적합하도록 설계되었다. 또한, 온라인에서는 효율성을 위해 통신 패스 수와 연산 부하를 최소화하여 빠른 실시간 인증을 제공하도록 하였다.

TAKE 프로토콜 동작은 등록(enrollment) 단계와 사전계산(precomputation) 단계, 그리고 실행 단계로 나누어 설명한다.(이후 mod p 표기는 생략함)

TAKE는 [그림 2]와 같다.

■ 기호 정의 :
A : 가입자(supplicant)
B : 인증 서버(authentication server)
π : 패스워드
x, r : [1 ~ q-1]범위의 랜덤 넘버
t : 대칭키 암호에서 사용되는 비밀키
ID_A : 가입자 A의 식별자(identifier)
$E_K\{\ \}$, $D_K\{\ \}$: 대칭키 암호화 및 복호화
e : g^x를 키 f로 대칭키 암호화($e = E_f\{g^x\}$)
H( ) : 일방향 해쉬함수
sk_A : A가 생성한 세션 키(session key)
p : 큰 소수
q : (p-1)을 나누는 큰 소수인 수
g : 위수(order)가 q인 Z_p^*의 원소인 생성원



〔그림 2〕 제안된 TAKE 프로토콜

b, g^b : 인증서버 B의 DH static 비밀키 및 공개키
c : 사전 계산인 $c = g^{bx}$

■ 등록 단계 :

가입자 A와 인증서버 B는 3D ES나 Rijndael과 같은 대칭키 암호 알고리즘에 사용되는 대칭키(t)와 패스워드(π)를 결정하여 서로 공유한다. 그리고 서버는 특정 가입자에 대한 서버의 비밀키로 [1 ~ q-1] 범위의 임의의 수 <b>를 선택하여 안전한 데이터베이스(DB)에 저장하고 가입자에게 서버의 공개키(g^b)와 도메인 파라메터(p, q, g)를 알려준다. 가입자는 대칭키(t)를 토큰에 저장한다. 여기서 서버의 공개키(g^b)와 도메인 파라메터(p, q, g)는 공개될 수 있는 성질의 정보이므로 반드시 안전한 장소에 저장되어야 하는 것은 아니다.

■ 사전계산 단계 :

사전계산은 프로토콜 수행전인 오프라인 상에서 이루어지는 단계로 프로토콜 수행 중에 소요되는 시간과 계산량을 감소시킨다. 가입자의 무선 단말기는 무선 네트워크를 사용하지 않는 빈 시간(idle time)이나 단말기 파워 온(power on)시에 사전계산을 수행한다. 즉, 가입자 A는 임의의 수 $x \in_R Z_q$를 선택하고 g^x와 $c = g^{bx}$를 사전계산 한다.

■ 실행 단계 :

실행 단계는 상호 개체 인증과 세션 키 설정을 수행하는 단계로 다음과 같은 절차로 이루어진다.

① 가입자 A는 공중 무선랜 서비스 접속을 위하여 자신의 식별자 ID_A와 인증서버 B의공개키(g^b)를 해쉬한 값인 $H(ID_A, g^b)$를 B에게 보낸다. 만일, 가입자 ID가 글로벌 로밍과 과금을 지원하기 위해 NAI(network access ID) 형식[7]을 사용하는 경우에는(예 : userid@realm.com) 사용자 이름 부분과 g^b를 해쉬한 값인 H(userid, g^b)와 영역 이름 부분을 함께 보낸다.

② $H(ID_A, g^b)$를 받은 인증서버 B는 데이터베이스(DB)에서 $<H(ID_A, g^b)>$, $<ID_A>$, <π>, <t>, <b>를 검출해 낸다. B는 임의의 수 $r \in_R Z_q$을 선택하여 A에게 보낸다.

③ A는 r을 수신하면 f=H(r, π, t)를 계산한다. 이 f는 g^x를 대칭키 암호화하는 대칭키로 사용하여 $e = E_f\{g^x\}$를 계산한다. 그리고 세션키 $sk_A=H(c, g^x, r)$를 계산하여 인증자 $M_A=H(sk_A, \pi, t, ID_A)$를 생성한다. 그런 다음 A는 e와 M_A를 B에게 보낸다.

④ e와 M_A의 메시지를 받은 B는 f=H(r, π, t)를 계산하고 수신된 e를 대칭키 f로 복호화하여 $g^x = D_f\{e\}$를 구한다. 그 후, B는 $c = g^{bx}$와 $sk_B=H(c, g^x, r)$를 계산하고 수신된 M_A와 B가 계산한 $H(sk_B, \pi, t, ID_A)$가 같은지를 검사한다. 만일, 그 값이 동일하면 A의 인증은 성공적이고, B는 M_A을 받아들인다. 그리고 B는 $M_B=H(sk_B, \pi, t, g^b)$를 계산하여 A에게 보낸다.

⑤ A는 수신된 M_B와 자신이 계산한 $H(sk_A, \pi, t, g^b)$가 동일한 값인지를 검사한다. 만일, 그 값이 동일하면 B의 인증은 성공적이고 A는 M_B를 받아들인다. 이렇게 하여 A와 B가 M_B와 M_A를 각각 받아들이면 상호 인증은 성공적으로 이루어진 것이다.

4.2 안전성 분석

공중 무선랜 환경에서 인증 및 키 설정 프로토콜의 보안 요구사항을 기술한 앞 2.2절의 요구 조건을 TAKE 프로토콜이 만족하는지를 분석한다.

① 신원 보호(identity protection) : 가입자는 AP(access point)로부터 ID 요청을 받으면 자신의 ID_A 대신에 $H(ID_A, g^b)$를 전송하여 도청자와 같은 수동적 공격자(passive attacker)들이 가입자의 신원을 알

수 없게 한다. 단, 인증서버는 가입자의 익명과 실제 신원을 매칭시킬 수 있도록 하여야 한다.

② 강력한 상호 인증 : 가입자는 패스워드(π)와 대칭키(t), 그리고 가입자 식별자(ID_A)를 알아야 인증자 M_A를 유도할 수 있어 가입자 인증을 받을 수 있다. 서버는 패스워드(π)와 대칭키(t), 가입자 식별자(ID_A) 그리고 서버의 비밀키(b)를 알아야 M_B를 유도할 수 있어 네트워크 인증을 받을 수 있다. 그리하여 강력한 상호 인증을 제공하게 되며 이것은 rouge AP(또는rouge radio NIC)를 이용한 DoS(Denial of Service) 공격을 어느 정도는 방지하여 준다.

③ 세션 키 설정 : 생성된 세션키는 랜덤성과 신규성(freshness)을 제공하는데 이것은 각 개체의 동적인(dynamic) 임의의 수 x와 r의 선택에 기인한다. 그리고 일반적인 DH 키 교환 방식은 MitM 공격에 취약할 수 있으나, TAKE는 이중요소(토큰과 패스워드)로 인증된(authenticated) DH 키 교환 방법을 사용하므로 MitM 공격에 안전하다.

④ Forward Secrecy(FS) : 가입자가 소지한 비밀 정보 <ID_A>, <π>, <t>, <g^b>가 공격자에게 모두 노출되었을 경우, 공격자는 e 암호문을 복호하여 g^x를 알 수 있겠지만, $c = g^{bx}$ 값은 DDH(Decision Diffie-Hellman) Problem에 의해 계산하기가 어렵다.[10] 따라서 가입자 측면(client side)의 FS는 제공한다. 반면에 인증 서버에 있는 가입자의 비밀 정보 <b>, <π>, <t>, 그리고 <ID_A>가 공격자에게 모두 노출되었을 경우에는 세션 키를 계산할 수 있다. 따라서 인증서버 측면(AS side)의 FS는 제공되지 않는다. 결국 TAKE 프로토콜은 가입자가 소지한 비밀정보가 모두 노출되더라도 공격자가 과거 세션 키를 계산할 수 없는 half FS를 제공한다. 그러나 실제로 공중 무선랜 서비스를 제공하는 네트워크 서비스 사업자(NSP)들은 자체의 강력한 보안 체제를 가지고 있기 때문에 인증서버의 비밀정보가 공격자에게 누설될 가능성은 아주 낮을 것으로 생각된다.

⑤ 오프라인 사전(offline dictionary) 공격 : 공중 무선랜 환경에서 공격자들은 성공적인 인증에 필요한 비밀정보들을 얻기 위하여 오프라인 사전 공격을 시도할 수 있다. 엔트로피가 적은 패스워드는 이러한 공격에 취약할 수 있으나, TAKE에서는 토큰에 저장된 엔트로피가 높은 대칭키와 패스워드가 임의의 값 g^x를 암호화하는 키로 함께 사용되므로 이러한 공격은 사실상 불가능하다. 즉, 공격자는 패스워드와 비밀키 그리고 임의의 값 g^x까지 추측하여야 한다.

⑥ Replay 공격 : Replay 공격은 공격자가 사용된 메시지를 재 전송하여 이전 세션 키를 다시 설정하려는 공격 방법이다. TAKE에서는 가입자와 서버가 매 세션 마다 임의의 수 x와 r을 각각 생성하여 세션 키를 생성하기 때문에 replay 공격에 안전하다.

⑦ 키 확인(key confirmation) : TAKE에서는 인증자 M_A와 M_B에 세션 키를 포함시켜 키 확인을 수행한다.

〔표 1〕 EAP 인증 방식별 특성

프로토콜	인증 방법	사회 공작적 공격	개체인증		신원 보호	세션키 지원	MitM 공격	기 타(단점)
			Client인증	Sever인증				
TAKE	-이중 인증(패스워드 및 토큰)	안전	제공	제공	제공	제공	안전	-서버에 저장할 정보량 이 많다.
EAP-TLS	-인증서	-	제공	제공	-	제공	안전	-인증패킷의 크기가 크고 계산량이 많다.
EAP-MD5	-패스워드	취약	제공	미 제공	미 제공	미 제공	취약	-단방향 인증 및 세션 키 미 제공
EAP-TTLS	-패스워드(가입자), 인증서(서버)	취약	제공	제공	제공	제공	취약	-많은 round trip이 필요하고 MitM 공격에 취약
PEAP	-패스워드(가입자), 인증서(서버)	취약	제공	제공	제공	제공	취약	-많은 round trip이 필요하고 MitM 공격에 취약
EAP-SRP	-패스워드	취약	제공	제공	미 제공	제공	안전	-단말 측에 과다한 계산량을 요구함.

⑧ 효율성(efficiency)

- 연산 부하의 최소화 : DH(Diffie-Hellman) 프로토콜은 FS를 제공할 수 있기 때문에 인증 및 키 설정(AKE) 프로토콜에서 많이 사용되고 있지만, 지수화(exponentiation) 계산을 요구하여 연산량이 많아진다. 해쉬 함수, 대칭키 암호화/복호화에 걸리는 시간은 아주 작기 때문에 연산에 소요되는 시간의 대부분은 지수화(exponentiation)와 역원 계산, 그리고 곱셈에서 주로 소요된다. 특히, PDA에서는 연산량이 많아지면 실시간 인증에 걸리는 시간이 많이 소요된다. TAKE에서는 온라인시에 가입자 측이 대칭키 암호 1번과 해쉬 5번의 연산량이 필요하고, 오프라인시에 사전계산으로 2번의 지수화 계산이 필요하다. 서버 측에서는 지수화 1번, 대칭키 복호 1번, 그리고 해쉬 4번의 연산량이 필요하다.
- 메시지 교환 횟수의 최소화 : 일반적으로 빠른 재연결(reconnect)을 위해서는 6 라운드 수(신원 교환 포함)이내가 바람직하며 TAKE에서는 4라운드 수가 필요하다.
- 통신 대역폭 사용의 최소화 : 5개의 메시지 중 3개는 해쉬의 출력 비트 수이고, 한개는 랜덤 넘버의 비트 수이고, 다른 하나는 g^x의 암호문 출력 비트 수이다.

⑨ 기존의 EAP 인증방식과 특성 비교 : EAP 인증방식으로는 EAP-TLS, EAP-MD5, EAP-TTLS, PEAP, EAP-SRP 등이 있는데 각 방식별 특성은 [표 1]과 같다. EAP-TLS는 사용자와 인증서버가 인증서를 이용하여 상호인증하고 동적인 WEP 키를 생성 분배하는 방식이다. 이 방식은 MitM 공격에는 안전하나 신원보호가 제공되지 않으며 인증서 관리 시스템 및 PKI 기반이 필요하다. EAP-MD5는 패스워드를 이용하여 가입자 측의 인증만을 제공하며 서버에 대한 인증과 세션키를 제공하지 않는다.

EAP-TTLS는 EAP-TLS의 확장형태로 가입자인증은 패스워드로, 서버인증은 인증서를 이용하여 인증하는 방식이다. PEAP는 EAP-TTLS와 유사한 형태의 인증방식으로 가입자 인증정보를 TLS 프로토콜을 통해 안전하게 터널링한 후에 가입자 인증을 처리하는 방식이다. 그러나 EAP-TTLS와 PEAP는 TLS 설정시에 가입자에 대한 인증 미비로 MitM 공격에 취약하고 많은 round trip이 요구되는 단점이 있다. EAP-SRP는 상호인증 및 Perfect FS를 제공하는 패스워드 인증된 키 설정(PAKE) 프로토콜이나 가입자 단말 측에 과다한 계산량을 요구하며 2-for-1 guess 공격에 취약하다. 본 논문에서 제안된 TAKE는 이중 요소(two factor) 인증방식을 이용하기 때문에 패스워드와 같은 단일요소 인증방식의 문제점인 키 스트로크 모니터링이나 사회공작적 공격 등에 취약한 점을 해결하였으며, 정적인(static) 익명성과 상호 개체 인증을 제공한다. 그러나 이 방식은 서버에 저장해야 할 비밀 정보량이 다소 많다는 단점이 있다.

V. 결 론

무선랜은 무선통신 기술이면서도 고속 통신이 가능하며, 일정 수준의 휴대 및 이동이 가능하다는 점에서 유무선 기술의 장점들을 동시에 가지고 있다고 볼 수 있다. 원래 무선랜 기술은 본래 공중망 서비스를 염두에 두고 개발된 기술이 아니기 때문에 본격적인 공중망 서비스 확대를 위해서는 로밍, 재밍, 보안, 과금 등 여러 기술적인 문제점을 해결하여야 한다. 현재, 공중 무선랜에서 무선 보안을 해결하기 위한 방안으로 TLS, SRP와 같은 유선의 보안 솔루션들을 적용시키는 방법을 시도하고 있으나, 이는 무선 네트워킹의 특징을 고려할 때 좋은 방법이라고 할 수 없으며 무선의 핸디캡을 고려한 무선 보안 프로토콜이 제안 되어야 한다고 생각한다. 본 논문에서 우리는 기존의 단일 요소 인증 및 유선의 보안 솔루션들을 이용한 EAP 인증방식(EAP method)의 근본적인 한계점을 해결하기 위한 방안으로 이중 요소(two factor) 인증과 사전계산(precomputation)을 이용한 상호 인증 및 키 교환 프로토콜을 제안하였다. 제안된 TAKE 프로토콜은 공중 무선랜에서 PDA에 적용할 수 있을 정도로 강력한 보안성과 효율성을 가진다. 프로토콜 수행 중에 가입자 측이 필요로 하는 연산량은 1번의 대칭키 암호와 5번의 해쉬 뿐이다. 가입자의 비밀키 관련 정보들은 PDA내의 보안모듈 혹은 USB기반의 스마트 키 등에 저장할 수 있을 것이다. 서버의 비밀키<b>는 한 개의 키로 모든 가입자에게 적용하기 보다는 여러 개의 비밀 키를 사용하는 것이 더 안전할 것이다.

참 고 문 헌

[1] IEEE, "Standard for local and metropolitan area networks-Port based network access control", IEEE

Std 802.1x, June 2001.

[2] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol(EAP)", RFC 2284, March 1998.

[3] D. P. Jablon, "Strong Password-only Authenticated Key Exchange", *ACM Computer Communications Review*, vol.26, no.5, pp.5~26, October 1996.

[4] IEEE Standard 802.11, "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications", 1999.

[5] W. A. Arbaugh, "Your 802.11 Wireless Network has No Clothes", Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks, December 2001.

[6] C. Rigney, "Remote Authentication Dial In User Service(RADIUS)", IETF RFC 2865, June 2000.

[7] B. Aboba and M. Beadles, "The Network Access Identifier", IETF RFC 2486, Jan. 1999.

[8] D. S. Wong and A. H. Chan. "Efficient and Mutually Authenticated Key Exchange for Low Power Computing Devices", In *ASIACRYPT 2001*, LNCS 2248, Springer-Verlag, Berlin, 2001.

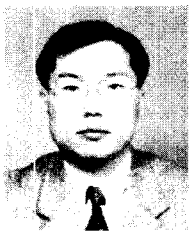
[9] S. Bellovin and M. Merritt. "Augmented Encrypted Key Exchange : A Password-Based Protocol Secure against Dictionary Attacks and Password File Compromise", ACM Conference on Computer and Communications Security 1993, pp.244~250.

[10] D. Boneh, "The Decision Diffie-Hellman Problem", In proceeding of the Third Algorithmic Number Theory Symposium, pp.48~63, 1998.

[11] B. Aboba, "The Unofficial 802.11 Security Web page", http://www.drizzle.com/~aboba/IEEE.

[12] M. Casole, "WLAN security-Status, Problems and Perspective", In Proceedings of European Wireless 2002, Florence Italy, February 2002.

〈著者紹介〉



박 영 만 (Young Man Park)
1986년 2월 : 한양대학교 전자통신공학과 학사
1988년 9월 : 한양대학교 전자통신공학과 석사
1990년 5월~현재 : 한국통신(KT) 서비스개발연구소
<관심분야> 무선 보안, 네트워크 보안, 정보보호

박 상 규 (Sang Kyu Park)
1974년 2월 : 서울대학교 전기 공학(공학사)
1980년 5월 : Duke Univ.통신공학(공학석사)
1987년 5월 : Univ. of Michigan 통신공학(공학박사)
1976년 7월~1978년 10월 : 국방과학연구소
1990년 8월~991년 8월 : Univ. of Southern California 객원교수
1987년 3월~현재 : 한양대학교 공과대학 전자전기컴퓨터공학부 교수
<관심분야> 무선 보안, 디지털통신, 확산대역통신, 부호이론