WLAN 인증서버의 인증서 폐지상태 확인 기술

박동국* · 조경룡*

Efficient and Practical Appraoch to Check Certificate Revocation Status of the WLAN Authentication Server's Public Key

DongGook Park* · Kyung-Ryong Cho*

요 약

WLAN 사용자 인증을 위한 EAP (Extensible Authentication Protocol) 프로토콜에 결합하여 쓰는 인증 메커니즘으로 최근에 공개키 기반의 EAP-TTLS(EAP-Tunneled TLS)나 PEAP(Protected EAP) 방식이 등장하였다. 이는 패스워드 추측 공격을 막을 수 있는 훌륭한 대안이지만, 상용화된 관련 솔루션 및 시스템에는 인증 서버의 인증서가 노출되었을 때를 대비한 인증서 갱신 처리 방법이 전혀 제공되고 있지 않은 실정이다. 본 논문에서는 이런 문제를 해결할 수 있는 매우 경제적인 메커니즘을 제안하였다.

ABSTRACT

WLAN user authentication is mostly based on user password resulting in vulnerability to the notorious "offline dictionary attack". As a way around this problem, EAP-TTLS and PEAP protocols are increasing finding their way into WLANs, which are a sort of combination of password protocols and the TLS public-key protocol. This leads to the use of the public-key certificate of the WLAN authentication server, and naturally the concern arises about its revocation status. It seems, however, that any proper soulution has not been provided to address this concern. We propose a very efficent and proper solution to check the certificate revocation status.

키워드

WLAN 인증서버, 공개키 인증서, 폐지상태 확인, CRL, EAP-TTLS

Ⅰ. 서 론

현재 중소 규모 이상의 WLAN(Wireless LAN) 망에서 가장 널리 쓰이고 있는 인증 프로토콜은 IETF 표준인 EAP(Extensible Authentication Protocol) 프로토콜[1],[2]이며 이는 특정 인증 메커니즘 또는 프로토콜이라기보다는 각종 인증/보안 프로토콜을 탑재할 수 있는 일반적 인증 체계라고 할 수 있다. 즉, 흔히 말하는 "plug-in" 개념을 인증 프로토콜에 적용한 것으로 볼 수 있으며, 이는 다양한 인증 프로토콜의 수용과 특정 프로토콜의 향후 개선에 손쉽게 대처할 수 있다는 장점이 있다. 또한, 인증/보안 프로토콜의 수행 주체가, 무선 링크 계층의 두 망요소인 WLAN 카드와 AP(Access Point)로부터 더 상위계층을 이루는 WLAN 단말기 또는 이용자와 인증 서버로 변경됨으로써 중앙집중식 인증/보안 관리가 가능하게 되었다.

* 순천대학교 정보통신공학부 전임강사
** 순천대학교 정보통신공학부 부교수

접수일자 : 2005. 7. 4

국내의 대표적 WLAN 서비스인 KT NESPOT 서비스에서도 EAP 프로토콜이 적용되고 있다. 다만, 그 서비스 초기에 기존 CHAP(Challenge Handshake Authentication Protocol) 프로토콜을 이용하는 EAP-MD5 프로토콜을 채택하였는데[3], 이 프로토콜은 가장 먼저 표준화된 EAP용 패스워드 인증 프로토콜이라 할 수 있다. 널리 알려진 바와 같이, 이런 패스워드 인증 프로토콜의 결정적인 약점은 바로 "오프라인 패스워드 추측 공격 (offline password guessing attack 또는 dictionary attack)"에 매우 취약하다는 것이다[4],[5].

패스워드의 편리성은 그대로 살리면서 동시에 이러한 단점을 보완하기 위한 방법으로는 첫째, 소위 "strong password authentication" 프로토콜을 쓰는 방법[2], 둘째, SSL/TLS와 같은 공개키 (public-key)[5] 기반 인증 프로토콜과 패스워드 인증을 결합하는 방법이 있다. 그러나 크게 보자면 이 두 가지 방법 모두 "공개키 기법"을 패스워드 인증에 가미함으로써 패스워드 프로토콜의 약점을 보완한다는 점에서는 서로 다르지 않다. 현재, 널리 보급되고 있는 방안은 위의 후자, 즉 TLS 프로토콜[6]과 패스워드 인증을 결합하는 것으로, 그 전형적인 예가 바로 그림 1에서 보인 EAP-TTLS (Tunneled TLS) 프로토콜이다[7]. 이 프로토콜의 기본 개념은 공개키 방식으로 서버를 인증하는 TLS 프로토콜과 이용자를 패스워드로 인증하는 임의의 패스워드 인증 프로토콜을 결합하는 것인데 전자의 수행 결과로 얻어지는 암호키를 이용하여 TLS 터널을 구성하고 후자 즉 패스워드 프로토콜을 이 TLS 터널 안에서 (즉 암호화되어 교환) 수행하게 된다. 결국, 이 프로토콜은 현재 인터넷 서버와 웹브라우저 간 인증/키설정 프로토콜로 가장 널리 쓰이는 기존 SSL/TLS 프로콜 사용과 그 개념이 사실상 동일하다. 다만 차이는 기존 방법에서는 TLS 터널을 통하여 패스워드를 단순히 전달만 하던 것이 EAP-TTLS에서는 TLS 터널 안에서 임의의 패스워드 프로토콜을 수행할 수 있다는 것이다.

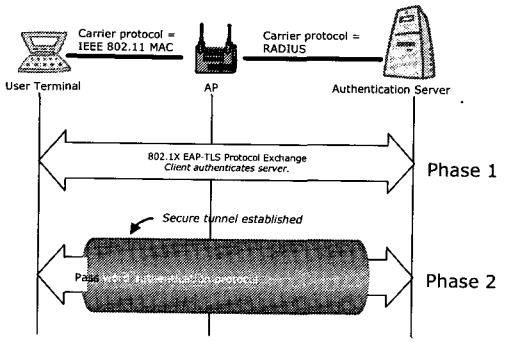


그림 1. EAP-TTLS 프로토콜의 전형적인 사용 환경 및 개념적 절차

Microsoft 등이 제안한 PEAP (Protected EAP) 프로토콜[8]도 EAP-TTLS와 대동소이하다고 할 수 있다. 현재 KT NESPOT 서비스에는 EAP-TTLS가 도입되고 있으며 기타 사업자들도 동일한 경향을 따를 것으로 보인다.

이와 같이, 패스워드 인증의 약점을 해결하기 위해 도입된 TLS 프로토콜은 필연적으로 "서버 공개키 인증서 (public-key certificate)" 사용으로 이어지게 되는데 이는 TLS 프로토콜을 통하여 이용자가 서버를 인증하는 데 필수 데이터가 된다. 더구나 이 서버 공개키는 그 역할이 서버 인증에서 그치는 것이 아니라 TLS 터널 생성을 위한 암호키, 소위 "session key"를 안전하게 생성하고, 따라서 후속되는 이용자 패스워드 인증의 보안과도 연결되므로 서버 공개키 값에 대한 "신뢰성"은 매우 중요하다. 공개키의 신뢰성 관리를 위한 기술로 잘 알려진 "CRL(Certificate Revocation List)"는 이 논문에서 다루는 WLAN 인증서버-이용자 간 인증에 대한 답이 될 수 없다. 이것은 기술적으로 불가능해서가 아니라, 효율성, 경제성 등의 타당성 측면을 볼 때 적절하지 않다는 것이다.

Ⅱ. 인증서 폐지 상태 (Certificate Revocation Status) 확인

신용카드가 분실되면 카드 유효기간이 아직 남아 있어도 그 카드는 더 이상 사용될 수 없도록 폐지/취소된다. 그리고 이러한 폐지 정보를 누구나 알 수 있도록 지원해야 하며, 상점은 카드 결제할 때마다 해당 카드의 유효기간 확인은 물론, 폐지/분실 신고 된 카드인지 아닌지도 확인해야 한다.

공개키 인증서도 해당 비밀 개인키(secret private key)가 노출되었다고 판단되는 즉시 신용카드처럼 폐지/분실 신고를 인증서 발급 CA(Certificate Authority)에 신고하고, CA는 이 공개키 인증서를 폐지목록 즉 CRL에 추가하고 이 정보를 공개하여 누구나 이용할 수 있

도록 지원해야 한다. 그러나 공개키 방식 프로토콜을 수행하는 각 개체는 예를 들면 SSL 프로토콜을 돌리면서 또 별도의 CRL 확인을 위해 공개 디렉토리를 접속하거나 아니면 주기적으로 CRL을 갱신하는 등의 적지 않은 부담을 져야한다.

더구나 EAP-TTLS처럼 신호부하와 계산부하가 작지 않은 프로토콜을 수행하면서, 접속프로그램이 서버 공개키 인증서의 폐지 상태 정보를 확인하기 위해 인터넷상의 CRL 정보에 접근한다는 것은 사실 매우 번거롭고 접속시간이 더 길어져야 하는 단점이 있다.

사실 웹브라우저를 이용한 인터넷 SSL 프로토콜 이용 환경에서조차 이 CRL 확인은 거의 하지 않고 있는 실정이다. 다만, 특정 이용 분야, 예를 들면 e-banking 과 같이 보안 요구 정도가 매우 큰 경우는 CRL 확인을 위한 별도 프로토콜이나 메커니즘을 운용하고 있는 실정이다.

Ⅲ. 서버 인증서 유출시의 공격

CRL 확인을 하지 않았을 때 일어날 수 있는 폐지된 공개키 인증서 관련 공격은 어떤 모양이 될 것인가? 유효기간 이전에 공개키 인증서가 폐지되었다는 것은, 해당 비밀 개인키가 노출되었을 가능성이 있기 때문이다. 즉, 어떤 공격자의 손에 그 개인키가 들어갔다는 것을 말한다. 이 때 가능한 공격으로는 데이터의 기밀성에 대한 공격에서부터 이용자에 대해 인증서버 행세를 하는 "impersonation attack"까지 가능하게 된다.

3.1. 기밀성에 대한 공격

공격자가 인증 서버의 공개키 및 그 개인키마저 알게 되면 인증서버와 임의의 이용자 간 EAP-TTLS 프로토콜 교환 메시지만 분석해도 세션 암호키를 알아낼 수 있다. 국내외를 불문하고 기업 환경에서의 도청 공격이 문제인 것을 감안하면 이 기밀성 관련 공격을 무시할 수 없게 된다.

3.2. 인증 측면의 공격 (impersonation attack)

인증서버의 공개키/개인키 쌍을 알아낸 공격자는 어떤 제삼자에게 이 공개키/개인키 쌍의 진짜 주인(key owner)인 것처럼 행세할 수 있게 된다. 즉, 소위 "impersonation attack"을 할 수 있게 된다. EAP-TTLS 환경이라면 EAP 서버인 것처럼 행세할 수 있다는 뜻이다. 제삼자(여기에서는 WLAN 이용자 단말기)는 인증서버 행세를 하는 공격자가 TLS 프로토콜 메시지를 통해 보낸 폐지된 공개키 인증서를 서명검증 하겠지만 아무런 이상을 발견할 수 없기 때문에 공격자는 인증에 성공하게 되고 이용자 단말기는 자신이 EAP 인증서버를 상대로 TTLS 프로토콜을 수행한 것으로 믿게 된다. 즉, 단말기는 인증서버가 아닌 공격자와 TLS 터널을 만들고 이 터널 상으로 패스워드를 전달하거나, 패스워드 프로토콜을 돌리게 된다. 따라서, 이용자가 입력한 이용자 패스워드가 공격자의 수중에 떨어질 수 있다. 즉, 패스워드가 TLS 암호키로 암호화되어 있다면 이 키는 공격자도 알고 있으며 (서버의 개인키를 알고 있으므로) 패스워드를 복호화 할 수 있게 된다. 비록, 패스워드가 단순한 암호화가 아니라 CHAP 프로토콜 등으로 보호된다고 하더라도 이 CHAP 프로토콜 교환 메시지를 이용하여 공격자는 off-line dictionary attack을 가하여 패스워드를 알아 낼 수 있게 된다.

EAP-TTLS 운용환경의 특성상 이런 공격을 시도하거나 성공할 가능성은 사실 그리 크지 않다. 왜냐하면, 기밀성 측면의 공격 타당성이 인증 측면의 공격 가능성에 비해 워낙 클 뿐 아니라 인증 측면의 공격 실현이 훨씬 더 번거롭기 때문이다. 어쨌든 이 공격의 구현은 다음 두 가지로 나눠 볼 수 있다.

가짜 인증서버 공격 (인증 서버만을 가장한 공격): 이용자/단말기-RADIUS 클라이언트 (AP)-RADI US 서버 구조에서는 공격자가 인증서버 즉 RADI US 서버 행세를 하기 위해서는 먼저 인증서버- AP 간에 서로 공유하는 RADIUS 비밀공유키(shared secret)를 알고 있어야 한다(RADIUS 프로토콜은 RADIUS 클라이언트가 RADIUS 서버를 인증하는 단방향 인증 프로토콜로 볼 수 있다). 즉, 서버가 이용자 단말기를 직접 상대하는 일반 인터넷 환경과는 달리, 일단 AP라는 RADIUS 클라이언트를 거쳐서 상대해야 하며, 이용자 단말기를 속이기 이전에 먼저 AP를 먼저 속여야 하는 어려움이 있다. 사실상 이는 불가능하다고 할 수 있다. 물론, 공격자가 인증 서버를 해킹하여 서버 공개키/개인키 쌍은 물론 RADIUS shared secret 조차 알아내버렸다면 이용자는 물론 AP까지 속일 수 있긴 하다.

가짜 AP-Server 조합 공격: 이런 용어는 쓰인 적이 없으나 이러한 공격이 시도될 가능성은 얼마든지 있다. 사실 WLAN 보안의 취약점을 앞 다투어 외치던 보안 솔루션 업체들이 늘 얘기하던 것 중의 하나가 바로 가짜 (bogus) AP 공격이다. 앞에서 가짜 서버가 진짜 AP를 속이기 힘들다고 했지만 만약 AP도 공격자가 설치한 가짜라면? 이럴 때는 막을 방법이 사실상 없다. 물론, 이러한 공격이 성공하기 위한 전제조건은 인증서버의 공개키에 상응하는 개인키가 노출되었고 이러한 사실을 단말기가 알 수 있는 방법이 없다는 것이다. 따라서, 이런 공격의 성공 가능성이 높기 때문에 아무리 서버 개인키의 노출 가능성이 적다고 하더라도, 단말기 차원의 "인증서 폐지 상태" 관련 정보의 관리 방법을 마련할 필요가 있다고 하겠다.

Ⅳ. WLAN 서비스 환경의 특수성

어떤 방법이나 기술도 그 적용환경을 떠나서 얘기할 수는 없듯이 PKI(Public Key Infrastructure) 관련 CRL도 맹목적으로 적용할 것이 아니라 그 이용 환경을 고려하여 적용여부를 결정해야 한다. 결론부터 말하자면, CRL을 WLAN 서버 인증서에 적용한다는 것은 엄청난 과다지출이 되는 셈이며 이런 까닭에 어떤 상용 솔루션도 CRL 관련 기능을 지원하지 않고 있다. 그러나, 그렇다고 해서 앞에서 살펴 본 인증서 유출시 발생할 수 있는 공격이 없어지는 것은 아니므로 적절한 대비 기술을 마련해야 하나, 실상은 그렇지 못한 실정이다. 심지어는, 이용자 접속 프로그램을 구현할 때, 서버 인증서의 유효기간 확인조차 하지 않는 식으로 구현될 우려도 없지 않다.

해결방법을 살펴보기 전에 먼저, 공개키 사용 측면에서 볼 때 WLAN 서비스 환경의 특수성을 몇 가지 짚어 볼 필요가 있다.

첫째, 이용자 단말기가 상대하는 TLS 서버가 불특정 다수의 서버가 아닌, 고정된 특정 서버, 즉 RADIUS/EAP 인증서버다.

둘째, 이용자 단말기와 인증서버가 서로 직접 상대하는 것이 아니라 AP라는 RADIUS 클라이언트를 매개로 삼고 있다.

셋째, EAP-TTLS가 적용되는 WLAN 접속 보안은 e-banking 등의 거래 보안과는 비교할 수 없을 정도로 덜 치명적이다.

첫째로 기술한 특수성은, 이용자를 상대하는 인증서버가 하나로만 고정되어 있다는 것이고 이것만으로도 CRL 이용이 적절치 않다는 것을 알 수 있다. 대신, 뒤에 가서 알 수 있듯이 이 "고정된 특정 서버"라는 점을 서버 인증서 폐지상태 확인 방법 구현에 최대한 활용할 수 있게 된다.

두 번째 특수성 역시 일반적인 인터넷 서버 운용 환경과 많이 다른 점이라 할 수 있다. 이용자가 방문하는 임의의 인터넷 사이트의 인증서버는 중간매개체인 인터넷 망과 특별한 신뢰 관계를 형성할 필요가 없다. 더구나, 이용자 단의 접속망과는 더더욱 그러하다. 반면, WLAN 서비스 환경에서는 인증서버는 이용자 접속망의 최첨단에 있는 AP와 비밀키를 서로 공유해야 하는 특수한 관계에 있다. 이것은 앞 장에서도 살펴 본 봐와 같이 impersonation attack이 그만큼 더 번거롭거나 어렵다는 것을 뜻한다.

세 번째 특수성은, WLAN 서비스의 특성에 기인한다고 할 수 있다. 단순히 망 접속 서비스에 그치는 WLAN에서의 보안 관련 위협이 은행거래나 전자상거래 등에 비해 경미함은 말할 것도 없다. 이러한 특수성과 앞의 두 번째 특수성을 함께 고려할 때, WLAN 환경에 적합한 서버 인증서 관리 방법은 CRL 확인과는 달리 구현상의 경제성과 운용상의 동작성능 향상을 위해 어느 정도의 구현 관련 융통성(흔히 말하는 granularity 측면에서)이 허용되는 것이다.

이러한 WLAN 서비스 환경의 특수성을 감안할 때, 서버 인증서 폐지상태 확인 방법이 만족시켜야 할 요구사항으로 다음 세 가지를 생각해 볼 수 있다.

- 폐지상태를 위해 서버-단말기 간에 별도의 추가 메시지 교환이 없을 것.
- 망 접속 시간에 추가 지연을 초래하지 않을 정도로 그 처리 부하가 작을 것.
- 이용자의 개입 없이 이용자 접속 프로그램 차원에서 자동으로 처리될 것.

이 요구사항들은 일견 무리일 것처럼 보이나,

사실은, WLAN 접속 서비스 환경의 특수성 때문에 충분히 만족시킬 수 있으며, 본 논문에서 제안하는 방법이 이를 입증한다.

V. 인증서 폐지 상태 확인을 위한 방법

WLAN 이용자/단말기와 WLAN 인증서버 간의 관계가 일반적인 인터넷 환경의 다대다 환경이 아니라 다대일 환경임을 고려하면, CRL이라는 무겁고 부적절한 방법이 아닌 훨씬 더 간단하고 오히려 더 적절할 수 있는 대안이 있다. 그것은 바로 인증서 내에 담긴 유효기간 (validity period) 정보를 이용하는 것이다. 그림 2에 나타낸 것처럼, X.509 인증서는 그 버전에 관계없이 늘 유효기간 정보를 담고 있다[9]. 즉, 유효 기간의 시작일자(not before) 데이터와 종료일자(not after) 데이터가 있다.

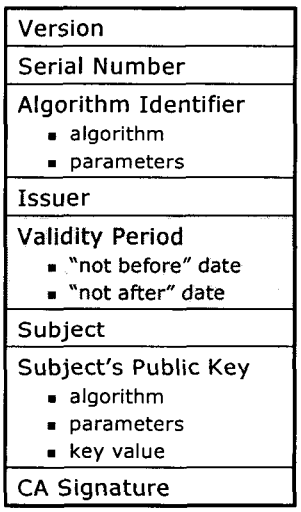


그림 2. X. 509 인증서 구조

인증서 유효기간 데이터는 원래, 인증서의 주기적 갱신/재발급을 위해 쓰이며, 유효기간 내에서 일어나는 예기치 못한 인증서 폐지를 처리하기 위한 것은 아니다. 그러나, WLAN 접속 서비스 환경에서는 관련 서버가 보통은 오로지 하나 있을 뿐이므로 유효기간 정보가 CRL보다 오히려 더 적절한 대안이 될 수 있다. 왜냐하면, WLAN 이용자 접속 프로그램이 이 WLAN 인증서버의 유효기간 정보 중에서 시작일자(not before) 데이터를 기억해 둘 수 있기 때문이다. 이는 바로 관련 대상 서버가 오로지 하나뿐이기 때문에 가능하다. 물론, 특정 이용자가 여러 개의 WLAN 망과 관계를 가질 경우에도 접속 프로그램이 각각의 해당 인증 서버의 시작일자 정보를 기억하는 것은 충분히 가능하다. 즉, 대상 서버가 불특정 다수가 아닌 고정된 두 세 개의 WLAN 인증서버일 뿐이기 때문이다.

이제 이 유효기간 정보를 이용해서 폐지상태 확인이 어떻게 가능한지를 보기로 하자. 공개키 인증서 내에 있는 유효기간의 "시작일자" 데이터는, 인증서에 있는 다른 정보와 함께 CA 개인서명키로 서명되므로, 그 진위(眞僞) 확인에 아무런 문제가 없으며 (즉, 공격자에 의한 데이터 조작이 불가능함), 갱신될 때마다 그 값이 증가할 수밖에 없다.

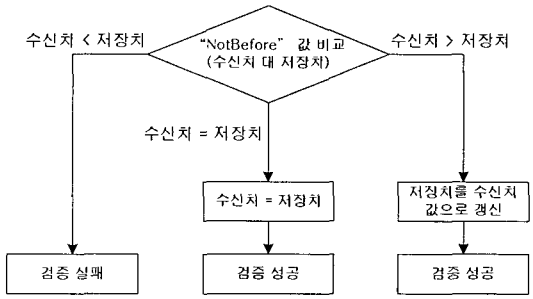


그림 3. 인증서 폐지 상태 관리를 위한 새 방법

그림 3은 본 논문에서 다루는 특수한 환경에서의 인증서 폐지 상태 관리 방법을 보여 준다. WLAN 접속 시마다 인증서버로부터 받은 공개키 인증서의 시작일자 값을 저장해둔 시작일자 값과 비교해보고, 같은 값이면 해당 인증서가 여전히 유효한 인증서로 간주할 수 있다. 만약 수신한 값이 저장된 값보다 크다면 이는 서버 인증서 유효기간이 만료되었거나 혹은 유효기간 안에 폐지되어 CA로부터 새 인증서를 발급 받았다는 것을 뜻하므로 저장된 시작일자 값을 수신한 값으로 대체한다. (물론, 수신한 새 시작일자 값의 진위가 공개키 인증서에 대한 CA 서명 검증을 통해 확인되었다는 것을 전제로 함은 말할 필요도 없다.) 반대로 수신한 값이 저장된 값보다 작다면 즉, 더 옛날 값이라면? 이 경우는 틀림없이 어떤 개체가 폐지된 이전 인증서를 보내 온 것이고 따라서 그 개체는 인증서버가 아니라 서버 행세를 하는 공격자인 것이다. 이럴 경우는, 접속 프로그램은 접속 과정을 즉시 중단해야 한다.

이 방법을 쓸 때 폐지된 이전 인증서를 알아낸 공격자가 공격에 성공할 수 있는 유일한 방법은 바로 공격 대상이 되는 이용자가 서버 인증서 갱신 이후 아직

WLAN에 접속하지 않았을 때를 노리는 수밖에 없다. 즉, 이 이용자 단말기의 접속 프로그램은 폐지된 바로 이전 인증서의 유효기간 시작일자를 기억하고 있으므로, 이 이용자가 WLAN에 접속해 올 때를 기다려 "impersonation attack"을 하면서 폐지된 이전 인증서를 (그것도 가장 최근에 폐지된 인증서라야 함을 주목) 이용자에게 전달하는 수밖에 없다. 그러나 이런 공격의 타당성이나 실현성은 매우 희박할 것이다. 더구나 이 공격이 성공한다 하더라도 해당 이용자가 한 번이라도 진짜 인증서버와 인증 프로토콜을 수행하기만 하면, 새 인증서의 시작일자가 단말기 내에 기억되므로 즉시 그 취약점은 사라져 버린다는 것을 알 수 있다.

결국, 단말기의 접속 프로그램에서 서버 공개키 인증서의 유효기간 시작일자 데이터를 저장해두고, WLAN 접속 시마다 수신한 시작일자 값과 저장된 값을 비교/확인함으로써 CRL 운용도 필요 없고, 단말기가 공개키 인증서 폐지 정보에 액세스할 필요도 없다. 즉, 부하 측면에서 볼 때 추가되는 신호 부하가 전혀 없으며 계산 부하 역시 사실상 거의 제로에 가까우므로 앞 장에서 제시한 요구사항을 모두 만족시킨다고 할 수 있다.

물론, 접속 과정의 신호 및 처리 부하를 줄이기 위해, WLAN 인증서버로부터 이용자 단말기로 가는 인증서 전달 메시지를 생략하고, 단말기 접속프로그램도 서버 인증서에 대한 CA 서명의 검증을 생략할 수도 있다. 다만 이를 위해서는 접속 프로그램에서 반드시 인증서버의 공개키를 기억해 두어야 한다. 또한, 서버 공개키의 인증서가 갱신되었을 때는 WLAN 인증서버가 모든 이용자에 대하여 EAP 인증 프로토콜 수행 시마다 새 인증서를 생략하지 말고 프로토콜 교환 메시지에 포함하여 전달해야 하는데 이는 한 달 이상 정도의 충분한 기간에 걸쳐 계속되어야 한다.

V. 결 론

WLAN 이용자와 인증서버 간 인증/키설정을 위해 EAP-TTLS 등의 "이용자 패스워드/서버 인증서" 결합 프로토콜이 새로이 각광 받기 시작하였지만, 적절한 인증서 폐지 상태 확인 방법이 마련되지 않고 쓰여 왔다. 본 논문에서는 원래 인증서의 주기적 갱신을 지원하기 위해 쓰이던 인증서 "유효기간" 정보를, WLAN 서비스 환경의 특수성을 분석해 볼 때, 서버 인증서의 폐지 상태 확인을 위해 쓸 수 있다는 것을 밝히고 그 구체적 방법을 설명하였다. 더구나, 이 대안은 기존 CRL 방식과 비교할 때 구현 비용이나 신호 및 계산 부하 측면에서 비교할 수 없을 정도로 경제적일 뿐 아니라 오히려 더 적절하다고 할 수 있다. 또한, 이 대안을 쓸 경우 유일한 보안 취약점 역시 무시할 만하다는 것을 알 수 있다.

참고문헌

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

[2] The International Engineering Consortium, "EAP Methods for 802.11 Wireless LAN Security", Web ProForum Tutorials, http:// www.iec.org/online/ tutorials/eap_methods/to pic04.html

[3] W. Simpson, "PPP Challenge Handshake authentication Protocol (CHAP)", IETF RFC 1994, Aug. 1996.

[4] S. Bosworth and M.E. Kabay (editors), Computer Security Handbook, Wiley, 4th Ed., 2oo2.

[5] B. Schneier, Applied Cryptography, 2nd Ed. Wiley, 1996, pp. 171-173.

[6] T. Dierks and C. Allen, "The TLS Protocol", IETF RFC 2246, 1999.

[7] P. Funk and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", IETF draft, July 2004.

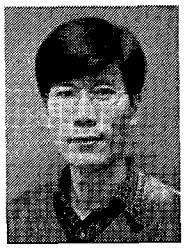
[8] A. Palekar, et al., "Protected EAP Protocol (PEAP)", IETF draft, July 2004.

[9] IETF Public-Key Infrastructure (X.509) charter: www.ietf.org/html.charters/pkix-ch arter.html

저자소개

박동국(Dong-Guk Park)

1986년 경북대학교 전자공학과 졸업(공학사)
1989년 KAIST 전기전자공학과 졸업(공학석사)
2001년. 호주 QUT 데이터통신과 졸업(공학박사)
1989년 ~ 2004년 KT 연구개발본부 선임연구원
2004년 ~ 현재 순천대학교 정보통신공학부 전임강사
※ 관심분야 : 인증/키설정 프로토콜 및 그 응용



조경룡(Kyung-Ryong Cho)

1987년 숭실대학교 전자공학과 졸업(공학사)
1989년 숭실대학교 전자공학과 졸업(공학석사)
1995년 숭실대학교 전자공학과 졸업(공학박사)
1989년 ~ 1990년 한국증권전산(주) 통신시스템부 사원
1990년 ~ 1996년 SK텔레컴 중앙연구원 선임 연구원
1996년 ~ 현재 순천대학교 정보통신공학부 부교수
※ 관심분야 : 채널코딩, 디지털변복조, 이동통신