情 報 保 護 學 會 誌
第 13 券 第 1 號, 2003. 2

무선랜 환경에서의 PKI 구축

이 종 후*, 서 인 석**, 윤 혁 중**, 류 재 철*

요 약

무선랜에서의 보안문제는 크게 두가지 측면에서 지적할 수 있는데, 첫 번째는 승인된 사용자에게만 접속을 허용하는 접속에 관한 보안이며, 다른 하나는 스니퍼 등을 이용해 무선랜을 통해 전송되는 내용 자체를 몰래 보는 도청 행위를 방어할 수 있는 보안이다. 특히 유선 네트워크와 달리 무선랜에서는 AP(Access Point)만 설치되어 있는 곳이면 누구나 쉽게 AP를 통해 네트워크를 이용할 수 있다. 이에 따라 무선랜에서 보다 중요성이 강조되는 보안문제는 접속에 관한 보안, 즉 사용자 인증이라고 할 수 있다.

그러나 무선랜 표준인 IEEE802.11b에서의 인증은 사용자 인증이 아닌 디바이스 인증에 머물고 있는 실정이며, 이 또한 매우 취약하다. 이에 따라 IEEE802.1x가 강력한 사용자 인증을 제공할 수 있는 메커니즘으로 개발되었다. IEEE802.1x에서는 EAP-TLS, LEAP, PEAP 등의 다양한 사용자 인증 메커니즘의 사용이 가능하다. 이러한 사용자 인증 메커니즘은 모두 공개키 암호기술을 이용하고 있어 무선랜 환경에서의 PKI 구축이 요구된다. 본 고에서는 무선랜에서의 사용자 인증 메커니즘에 대해서 알아보고, 유선 네트워크와는 다른 특성을 갖는 무선랜 환경에서 PKI 구축시 고려해야 할 사항들에 대해서 분석하였다.

Ⅰ. 서 론

인터넷 및 이동통신 기술의 발전과 함께 사무실 내에서뿐만 아니라 자동차나 거리, 공항이나 지하철역 등 다양한 환경에서 인터넷에 접속이 가능해지고 있다. 이러한 환경의 구축은 PDA나 휴대전화 등에서 인터넷 접속이 가능하게 되면서 실현되고 있는데, 최근 들어 사용의 폭이 급격하게 증가하고 있다.

이러한 가운데, 최근에는 우리에게 익숙한 이더넷(Ethernet) 랜 기술을 사용하는 무선랜(WLAN: Wireless Local Area Network) 서비스가 주목을 받고 있다. 무선랜은 무선랜카드를 노트북이나 PDA 등에 장착하고 인터넷과의 접점이 되는 AP(Access Point)를 이용해 인터넷을 이용할 수 있게 해주는 기술로, 이동전화를 이용해 인터넷을 이용할 경우에 비해 속도가 빠르고, 장비의 비용이 10배정도 저렴하기 때문에 무선인터넷 시장에서 경쟁력을 갖추고 있다고 보여지며, 향후 많은 이용이 예상되고 있다.

무선랜 기술이 각광을 받고 있는 이유는 주로 설치 비용이 낮고 사용이 편리하기 때문인데, 무선랜 기술이 갖는 장점을 살펴보면 다음과 같다[1].

- ◉ 사용자 이동성: 물리적으로 유선상의 네트워크에 접속하지 않은 상태에서도 인터넷을 비롯한 네트워크에 접속이 가능하며, 이 때 속도면에서 유선 네트워크를 사용할 때와 비슷한 수준의 통신이 가능하다.
- ◉ 빠른 설치: 물리적인 네트워크 선의 설치가 필요 없기 때문에 네트워크 구축에 드는 시간이 적게 소요된다.
- ◉ 유연성: 네트워크 사용이 어려운 장소에서도 AP만 설치하면 바로 네트워크 사용이 가능하다.
- ◉ 확장성: 여러 개의 AP 설치를 통해 네트워크 사용 범위를 쉽게 확장할 수 있다.

* 충남대학교 정보통신공학부
** 국가보안기술연구소

이와 같은 무선랜 기술은 주로 IEEE (Institute of Electrical and Electronics Engineers)에서 주도하는 표준화 작업에 기반하여 개발이 진행되고 있는데, 현재 가장 많이 사용되는 기술은 2.4GHz 대역에서 최대 11Mbps까지 전송이 가능한 IEEE 802.11b이다.

IEEE802.11b는 비교적 최근에 표준화가 완료되었음에도 불구하고 면허가 필요 없는 2.4-2.5GHz ISM(Industrial, Scientific, and Medical) 주파수 대역을 사용하기 때문에 현재 가장 널리 사용되고 있다. 그러나 향후에는 좀 더 좋은 서비스를 제공할 수 있는 802.11a의 사용도 증가할 것으로 예상되고 있다[1].

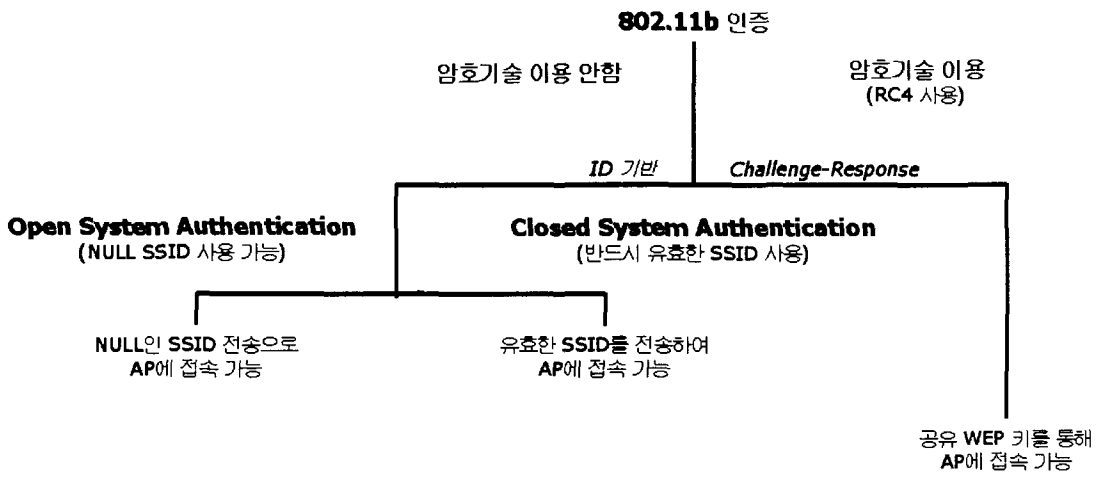
보안 문제는 현재 서비스 초기 단계라고 할 수 있는 무선랜 기술이 활성화되는데 있어서 반드시 해결해야 할 문제점으로 지적되고 있다. 무선랜에서의 보안 문제는 크게 두가지 측면에서 지적할 수 있는데, 첫 번째는 승인된 사용자에게만 네트워크 접속을 허용하는 접속에 관한 보안(접근제어 및 사용자 인증)이며, 다른 하나는 스니퍼(sniffer) 등을 이용해 무선랜을 통해서 전송되는 내용 자체를 몰래 보는 도청 행위를 방어할 수 있는 보안(기밀성)이다.

유선 네트워크와 달리 무선랜은 AP만 설치되어 있는 곳이면 누구나 쉽게 AP를 통해 네트워크를 이용할 수 있다는 특징이 있다. 이에 따라 무선랜에서 보다 중요성이 강조되는 보안 문제는 접속에 관한 보안, 즉 사용자 인증이라고 할 수 있다. 특히 공중 무선랜 서비스가 제공될 경우, 자신이 가입한 사업자가 아닌 다른 사업자가 제공하는 AP를 이용할 경우, 과금 등에 있어서 많은 문제점이 발생할 수 있다.

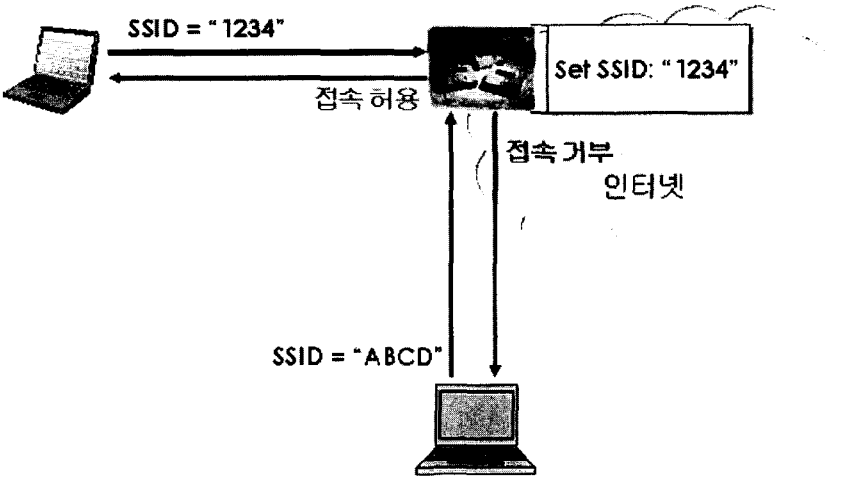
사용자 인증 및 암호화와 관련하여 IEEE802.11b에서는 SSID(Service Set Identifier), MAC (Media Access Control) 주소, WEP(Wired Equivalent Privacy) 등의 메커니즘을 통해 보안 서비스를 제공하고 있다[2].

그러나 현재 이와 같은 IEEE802.11b의 보안 메커니즘들의 많은 취약성들이 알려지고 있는 실정이다. 이에 따라 IEEE802.11b의 보안 메커니즘을 보완하기 위한 메커니즘들이 개발되고 있다. 이 가운데 대표적인 것이 사용자 인증 메커니즘을 강화하기 위한 IEE802.1x EAP(Extended Authentication Protocol)이다. 802.1x에서는 해쉬 함수를 이용한 Challenge/Response, kerberos, 인증서를 기반으로 하는 TLS(Transport Layer Security), One-time Password 등 다양한 사용자 인증 메커니즘들이 사용될 수 있다[3-5]. 특히 TLS의 경우 가장 널리 사용되고 있는 웹 보안 메커니즘으로 인증서 기반의 강력한 사용자 인증을 제공하고 키 교환이 가능하다는 점 등 많은 장점을 가지고 있어 많은 사용이 기대된다.

기존 IEEE802.11b의 보안 메커니즘의 경우, 단순한 사용자 인증 및 관용 암호 알고리즘을 사용하기 때문에 PKI(Public Key Infrastructure)에 대한 고려가 필요하지 않았으나, 802.1x를 기반으로 해서 TLS 등의 보안 메커니즘을 사용할 경우에는 PKI의 구축이 필수적이다. 그러나 유선랜과 다



[그림 1] 802.11b의 사용자 인증 방법



〔그림 2〕 SSID를 이용한 사용자 인증

른 특성을 가지는 무선랜 환경을 감안할 때 PKI 구축을 보다 효율적으로 하기 위해 여러 가지 사항을 고려해야 한다.

이에 본 고에서는 802.1x 및 802.11b를 이용하는 무선랜 환경에서 PKI를 효율적으로 구축할 수 있는 방안에 대해서 살펴보고자 한다.

본 고의 2장에서는 802.11b의 사용자 인증 메커니즘의 동작 원리 및 이의 취약성에 대해서 살펴보고, 3장에서는 802.1x 기반의 좀 더 강화된 사용자 인증 메커니즘에 대해서 살펴본다. 그리고 4장에서 무선랜 환경에서 PKI를 구축할 때 고려해야 할 사항들을 분석하고 5장에서 결론을 맺는다.

Ⅱ. 무선랜 보안기술

1. IEEE802.11b 사용자 인증

802.11b에서 유선 네트워크에 접속하려는 무선 사용자를 인증할 수 있는 방법은 그림 1과 같이 크게 두 가지로 구분할 수 있는데, 첫번째는 암호기술에 기반한 방법이며 다른 하나는 그렇지 않은 방법이다[1-2].

우선 암호기술에 기반하지 않은 인증 방법에 대해서 살펴보면 SSID(Service Set Identifier)를 이용한 방법이다. 즉, 어떤 무선랜카드에서 AP에 접속하기 위해서는 SSID를 미리 알고 있어야 한다(그림 2 참조). 이 때, 반드시 유효한 SSID를 사용해야만 인증이 이루어지는 경우도 있지만, NULL 값을 갖는 SSID를 이용해서 접속이 가능한 경우도 있는데, NULL인 SSID를 이용해 접속이 가능한 경우를 개방형 인증 (Open System Authentication)이라고 한다.

AP 및 무선랜카드 업체에서는 SSID를 각각의 업체에서 정한 기본값으로 설정하여 판매하는 것이 일반적이다. 예를 들어 3COM의 제품은 SSID가 "101"로 설정되어 있으며, Cisco의 제품은 "tsunami"로 설정되어 있다. 물론 사용자는 이 값을 변경하여 사용할 수 있다. 또한 AP에서는 주기적으로 SSID를 브로드캐스트(broadcast) 할 수 있다. 이 경우 무선랜카드에서는 AP에 접속 가능한 지역 내에서 AP로부터 브로드캐스트되는 SSID를 수신한 뒤 이를 이용하여 AP에 접속할 수 있다.

암호기술에 기반한 인증은 사용자(무선랜카드)와 AP가 공유하는 WEP 키를 이용해서 인증하는 방법으로 간단한 형태의 Challenge-Response 방식이다. 이는 그림 3과 같이 이루어진다.

① 무선랜카드는 네트워크 접속을 위해 AP에 인증을 요청한다.
② AP는 임의로 생성한 난수인 Challenge를 무선랜카드에게 전송한다.
③ 무선랜카드는 수신한 Challenge를 자신이 저장하고 있는 WEP 키를 이용해서 암호화한 결과인 Response를 AP에게 전송한다. 이 때, 암호 알고리즘은 WEP 암호화와 마찬가지로 RC4 가 사용된다.
④ AP는 자신이 생성한 Challenge를 무선랜카드가 사용한 것과 동일한 WEP키로 암호화한 뒤, 무선랜카드로부터 전송된 Response와 비

교하여 동일하면 인증에 성공한 것으로 한다.

이러한 두가지 인증 방법 외에 무선랜에서 사용되는 인증 방법으로 MAC 주소 필터링(MAC address filtering)이 있다. 이 방법은 무선랜카드마다 유일하게 할당되는 MAC 주소를 인증에 이용하는 것으로 그림 4와 같이 이루어진다.

AP는 접속이 허용된 MAC 주소의 목록을 저장하고 있으며 이는 관리자의 조작에 의해서 편집이 가능하다. 무선랜카드에서 접속을 위해 자신의 MAC 주소를 전송하면 AP는 접속이 허용된 MAC 주소 목록에 포함된 주소인지 여부를 확인하고 접속의 허용 또는 거부를 결정한다.

2. IEEE802.11b 사용자 인증의 취약성

1) SSID

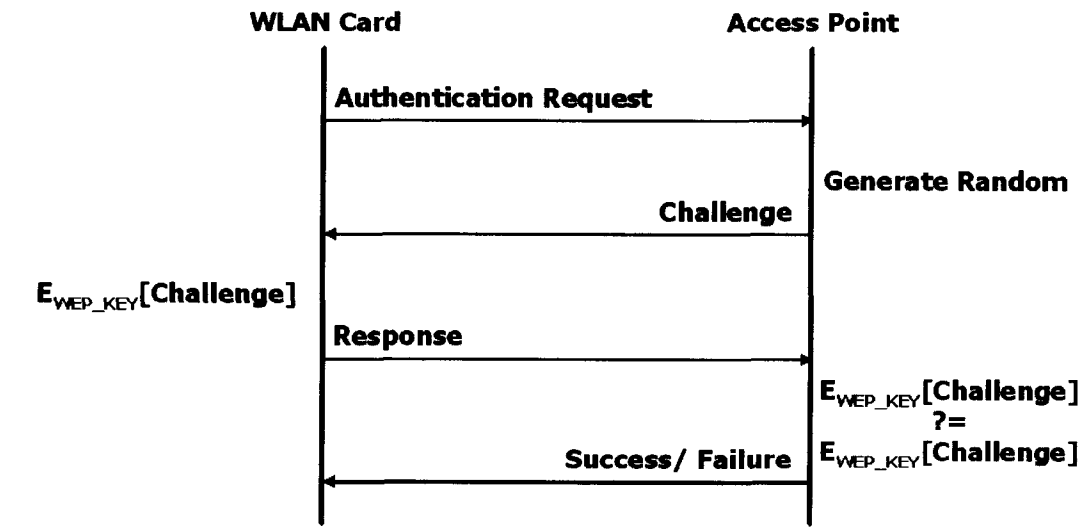
무선랜카드에서 AP로 전송되는 SSID는 단순한 평문이다. 따라서 제3자가 전송되는 SSID를 도청하여 사용하는 것이 가능하며, 공격자는 도청한 SSID를 이용해 자신의 신원을 위장하여 AP에 접속할 수 있다. 또한 AP에서 SSID를 "ANY" 로 설정하거나 브로드캐스트하도록 설정하는 경우, 누구든지 AP에 접속이 가능하다.

이와 같은 경우 외에도 기본값으로 설정된 SSID를 변경하지 않고 사용하는 경우가 많기 때문에, 업체별로 설정된 SSID를 이용해서 AP에 접속을 시도하는 경우도 발생할 수 있다.

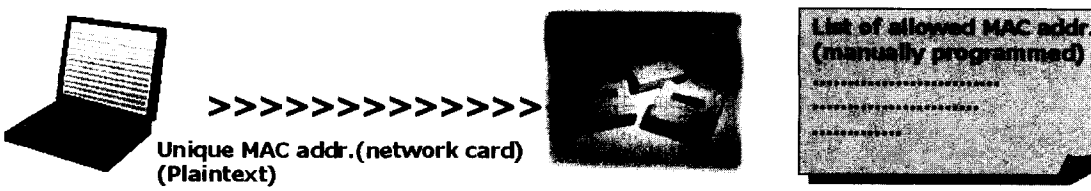
또한 조직내 홈페이지 등을 통해 무선 네트워크를 사용하는 구성원이 쉽게 알 수 있도록 SSID를 공개하는 경우도 많아 SSID를 통한 사용자 인증은 거의 무의미하다고 할 수 있다.

2) MAC 주소 필터링

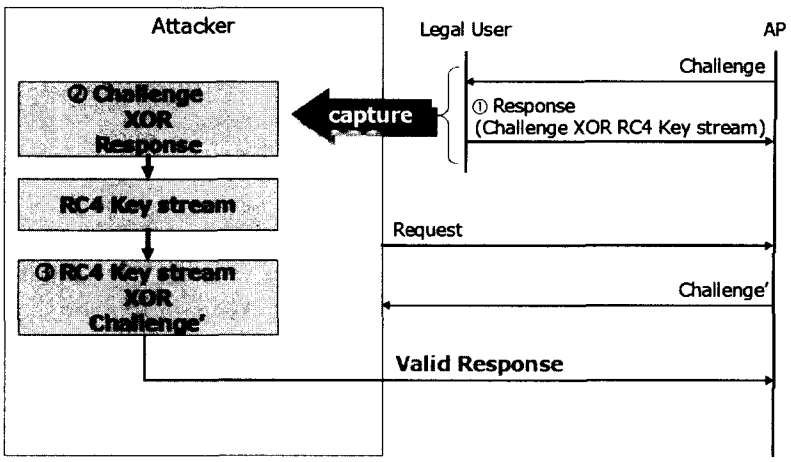
MAC 주소를 이용한 인증의 경우도 SSID를 통한 인증과 마찬가지로 MAC 주소가 평문으로 전송되기 때문에 얼마든지 도청이 가능하다는 문제점이 있다. 또한 AP에서 MAC 주소를 관리하는데 있어서도 확장성이 떨어지기 때문에 이동이 많거나 불특정 다수가 접속하는 환경에서는 관리가 거의 불가능하다는 단점이 있다.



〔그림 3〕 WEP을 이용한 사용자 인증



〔그림 4〕 MAC address filtering



〔그림 5〕 IEEE802.11b 공유키 인증에 대한 공격

그리고 MAC 주소 필터링이 본래는 사용자 인증의 목적으로 고안된 것이나, 이는 사용자 인증이라기 보다는 무선랜카드라는 하드웨어에 대한 인증이라고 할 수 있다. 이는 SSID의 경우에도 마찬가지이다.

또한 MAC 주소가 무선랜카드마다 유일하게 할당되는 값이지만, 외부에서 조작이 쉽게 이루어진다는 문제도 지적된다. 리눅스(Linux)나 유닉스(UNIX) 환경에서는 root 권한이 있는 경우에 MAC 주소의 변경이 가능하며, 윈도우즈(Windows) 환경에서는 레지스트리(registry) 조작을 통해 MAC 주소의 변경이 가능하다.

3) 공유키 인증

RC4와 같은 스트림 사이퍼의 경우 동일한 키를 사용할 경우에는 평문이 노출될 위험이 있다. 무선랜에서 사용되는 공유키 인증의 문제점에 대해서 분석하기 전에 스트림 사이퍼의 키 재사용에 대해서 먼저 살펴보면 다음과 같다.

$$\text{만약, } C1 = P1 \oplus RC(IV,K)\text{이고, } C2 = P2 \oplus RC(IV,K) \text{ 이라면,}$$
$$C1 \oplus C2 = (P1 \oplus RC(IV,K)) \oplus (P2 \oplus RC(IV,K)) = P1 \oplus P2$$

가 되어 2개의 암호문을 획득할 수 있다면 2개의 평문의 XOR 연산 결과를 알아낼 수 있다.

이 때, 만약 공격자가 2개의 평문 가운데 하나를 알고있다면 키에 대한 정보 없이도 나머지 하나의 평문을 쉽게 얻어낼 수 있다.

802.11b에서의 공유키 인증은 하나의 키를 이용해서 Response를 생성한다. 따라서 스트림 사이퍼에서 키를 재사용하는 경우에 발생하는 문제점을 이용하면 그림 5와 같은 공격이 가능하다.

① 우선 공격자는 정당한 사용자가 AP와 인증을 수행할 때 사용된 Challenge와 Response를 가로챈다. 이 때, Challenge는 AP가 임의로 생성한 난수이며, Response는 다음과 같다.

$$Response = Challenge \oplus RC4\_Key\_stream$$

② 공격자는 다음과 같은 연산을 통해 Challenge와 Response로부터 RC4_Key_stream 값을 알아낼 수 있다.

$$RC4\_Key\_stream = Challenge \oplus Response$$

③ 키 스트림을 얻어낸 공격자는 정당한 사용자로 위장이 가능하다. 즉 AP에게 인증 요청을 전송한 후 수신하게 되는 Challenge로부터 다음과 같이 유효한 Response를 생성할 수 있다.

$$Response' = Challenge' \oplus RC4\_Key\_stream$$

이와 같이 키 스트림의 재사용이 가능한 이유는 WEP에서는 하나의 동일한 키가 모든 암호통신에 사용되고, Challenge를 공격자가 가로채기가 쉽기 때문이다.

이와 같이 공유키 인증을 무력화시킬 수 있는 공격이 가능하기 때문에, 802.11b 표준에서는 인증이 이루어질 때마다 IV(Initialization Vector)를 임의로 생성하여 사용하도록 하여 동일한 키 스트림이 재사용되는 상황이 발생하지 않도록 할 것을 권고하고 있다. 그러나 이 IV도 재사용 되기 때문에 이 절에서 설명한 공격을 완전히 차단하지는 못한다. 이에 대해서 보다 자세하게 살펴보면 다음과 같다.

스트림 사이퍼를 통한 암호 통신에서 동일한 키를 사용할 경우 공격자가 키에 대한 정보 없이도 암호문에 대한 평문을 얻어낼 수 있다는 것을 이미 앞에서 설명하였다. 이러한 공격을 피하기 위해서는 전송되는 데이터마다 키 스트림을 다르게 해야하는데, WEP에서는 이를 위해 전송되는 패킷마다 다른 IV를 사용하도록 하고 있다.

WEP은 모든 패킷에 대해서 동일한 암호키와 각 패킷마다 임의로 생성되는 공개된 IV를 사용하여 패킷마다 다른 RC4 키 스트림을 생성한다. 이러한 키 스트림을 사용하여 암호화된 패킷을 받은 수신자는 암호화된 패킷을 복호화하기 위하여 암호화에 사용된 키 스트림과 동일한 키 스트림을 생성해야 하는데, 이를 위해서는 암호화에 사용된 것과 동일한 IV를 생성해야 한다. 동일한 IV 공유를 위해서 패킷 전송시 평문의 IV를 암호화된 패킷 앞에 붙여서 전송한다. IV는 암호화되지 않기 때문에 공격자에게 쉽게 노출될 수 있느나, 공격자가 암호키를 알지 못하기 때문에 키 스트림은 안전하다.

이와 같이 WEP에서는 패킷마다 다른 IV를 사용하여 키 스트림 재사용 공격을 방지하도록 하고 있다. 그럼에도 불구하고 WEP은 이러한 목적을 이루고있지 못하다.

이는 주로 잘못된 IV 관리에서 비롯된다. 일반적으로 공유되는 비밀키는 자주 변경되지 않음으로 IV의 재사용은 키 스트림의 재사용의 원인이 된다. IV는 평문으로 공개되는 정보이기 때문에 공격자는 IV의 재사용 여부를 쉽게 알 수 있다. IV의 잘못된 관리에 대해서 좀 더 살펴보면 다음과 같다.

WEP 표준은 매 패킷마다 IV를 변경하여 사용하도록 권고하고 있다(강제적인 요구사항은 아니다). 그러나 IV의 생성 방법에 대해서는 정의하고 있지 않다. 또한 구현 방법에 대해서도 기술하고 있지 않다. 따라서 업체에 따라서 무선랜카드를 탈착후 다시 장착할 때마다 IV를 '0'으로 초기화하고 데이터가 전송될 때마다 '1'씩 증가하도록 구현한 경우도 있다. 이 경우 동일한 IV가 자주 재사용될 위험이 매우 높다.

또한 WEP 표준은 IV의 크기를 24비트로 제한하고 있는데, IV의 크기가 비교적 작기 때문에 동일한 IV가 여러 패킷에서 사용될 위험이 크다. 이와 관련해서 [4]에 의하면 무선랜카드에서 1500바이트의 패킷을 AP에 계속 보내고 평균 5Mbps의 대역폭을 사용한다면 (최대 대역폭은 11 Mbps) 12시간만에 IV로 유효한 공간이 모두 소진된다. 또한 각 패킷에서 임의의 24비트 IV를 사용한다면 5000개의 패킷을 전송한 후에 충돌이 발생하게 되는데, 5000개의 패킷은 몇 분이면 전송이 가능하다.

이와 같은 방법들을 통해서 동일한 IV를 사용하는 2개의 암호문 패킷을 찾아내고 암호문에 대응되는 2개의 평문 가운데 하나를 알아낸다면 다른 하나의 평문은 바로 찾아낼 수 있다.

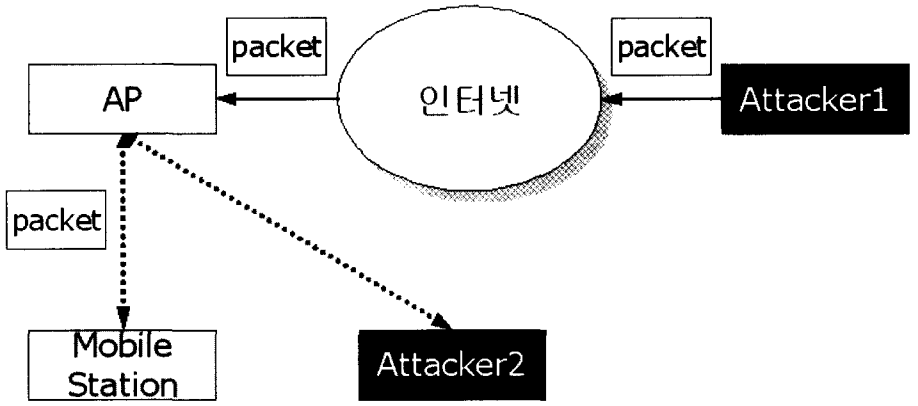
2개 가운데 하나의 평문을 알아내기 위한 방법은 다음과 같은 3가지로 정리할 수 있다.

첫 번째 경우는 AP를 잘못 구현한 경우이다. 어떤 AP는 비콘(beacon) 등의 정보를 브로드캐스트할 때 암호문 패킷과 평문 패킷을 동시에 브로드캐스트하도록 구현된 경우가 있다[4]. 이 경우, 암호문에 대응되는 평문을 쉽게 알아낼 수 있기 때문에 무선랜카드와 AP가 데이터를 암호화하는 단계에서 평문을 전송하지 않지만, 이전에 알아낸 평문을 이용하여 암호화된 데이터에 대응되는 평문을 쉽게 얻어낼 수 있다.

두 번째 경우는 2개의 평문 가운데 하나를 추측하는 방법이다. 즉, 쉽게 추측이 가능한 평문을 통해 추측이 어려운 다른 평문을 찾아내는 방법이다. 추측에 이용되는 패킷은 로그인 메시지, NFS(Network File System)에서의 공유 라이브러리(shared library) 등을 이용할 수 있다.

세 번째 방법은 좀 더 적극적인 공격방법으로 그림 6과 같이 공격자의 인터넷 호스트에서 무선 호스트로 패킷을 전송하여 평문을 알아낸다.

① 인터넷 상의 공격자(attacker 1)은 WEP을 사용하는 무선 호스트에 데이터를 전송한다. 이 무선 호스트는 AP와의 통신에서 WEP 암호화 기능을 이용하기 때문에 AP는 인터넷



〔그림 6〕 IV 재사용 공격

상의 공격자로부터 수신한 데이터를 암호화하여 무선 호스트에게 전송한다.

② 무선 네트워크 상의 공격자(attaker 2)는 AP로부터 무선 호스트에게 전송되는 암호 패킷을 가로챈다. 이를 통해 공격자들은 평문과 이에 대응하는 암호문을 모두 알 수 있다.

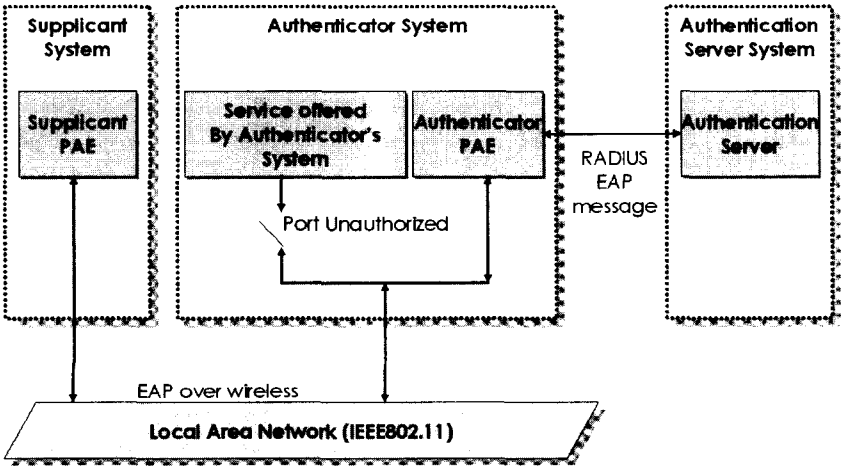
③ 이 후, 무선 호스트가 AP를 통해 암호 통신을 할 때, 이전에 가로채서 알고 있는 암호문과 평문을 이용해서 무선 호스트와 AP 간의 암호 패킷에 대응되는 평문을 알아낼 수 있다.

Ⅲ. IEEE802.1x 기반의 사용자 인증

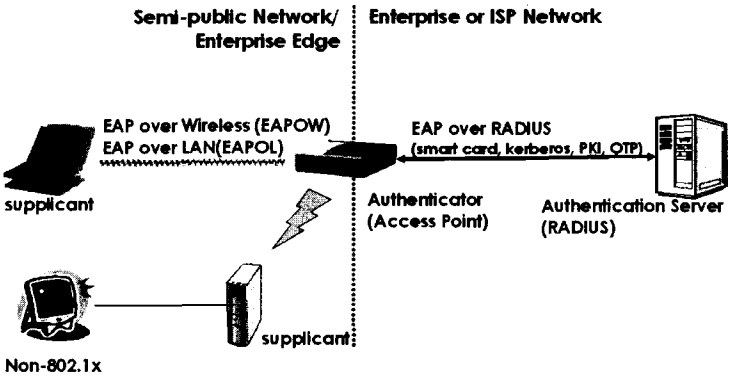
1. IEEE802.1x 개요

앞서 기술한 바에 의하여 SSID나 공유키 인증 방식에서 사용하고 있는 방식은 신뢰하기 어렵다는 것을 알 수 있었다. 802.1x는 이와 같이 802.11b에서의 사용자 인증 문제를 해결할 수 방법으로 고안되었다. 802.1x가 동작하는 구조를 살펴보면 그림 7과 같다.

기본적으로 802.1x에는 제어된 포트(Controlled port)와 제어되지 않은 포트(Uncontrolled port)가 있다. 제어되지 않은 포트는 AP나 브리지 상에서 가상적으로 정의한 것으로 사용자(supplicant)가 네트워크를 사용하기 위해서는 AP의 뒷단에 있는 인증 서버(Authentication server)로 인증을 요구할 수 있는 포트이다. 이 하나의 포트만으로 특정 네트워크 자원(인증 서버)에 접근이 가능한데, 이 포트를 통하여 인증을 받게되며, 인증 서버와의 통신 이외에는 네트워크 자원으로 접근이 허용되지 않는다.



〔그림 7〕 802.1x 구조



〔그림 8〕 EAP를 이용한 인증

제어된 포트는 인증이 성공했을 때 마치 문처럼 열리는 포트라고 보면 된다. 인증 받은 사용자는 이 포트를 통해서 모든 네트워크 자원에 접근할 수 있다. 이 때, 인증 서버로는 현재는 RADIUS(Remote Authentication Dial In User Service)라는 AAA (Authentication Authorization Accounting) 서버가 이용되고 있으며, 향후에는 Diameter 서버의 이용이 예상되고 있다[5-7].

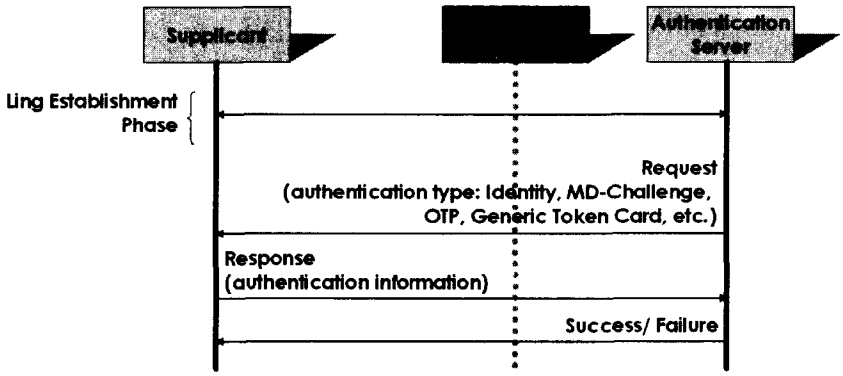
802.11b에서는 사용자 인증을 AP에서 수행하였지만, 802.1x EAP에서는 그림 8과 같이 AP는 단순히 사용자와 인증 서버 간의 통신의 중개 역할만을 하게되며, 사용자 인증은 인증 서버에서 수행한다.

사용자와 AP, 인증 서버 간에 주고 받는 메시지는 EAP 규격을 따르게 된다. 즉, 802.1x를 사용할 경우 기존에 지원하지 않던 인증 방식이 확장된 다른 프로토콜을 사용해야 한다. 따라서 일반 패킷을 EAP 프레임으로 캡슐화하여 강화된 사용자 인증에 사용한다. 사용자와 AP 간의 통신은 EAPOL(EAP over LAN) 또는 EAPOW(EAP over Wireless)를 사용하게 되는데, 무선랜에서는 EAPOW를 사용한다.

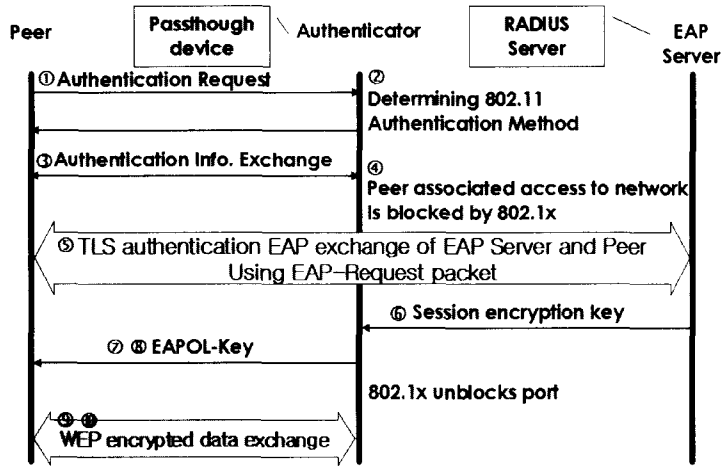
또한 802.1x에서는 구체적인 인증 방법은 정의하고 있지 않으며 인증을 수행할 수 있는 골격만 제공하게 되는데, 따라서 인증은 스마트 카드를 이용한 인증, 커버로스(Kerberos), TLS(Trnasport Layer Security), OTP(One Time Password) 등 다양한 방법 가운데 하나를 통해 수행될 수 있다.

802.1x EAP에 의해서 인증이 이루어지는 과정을 살펴보면 그림 9와 같다.

사용자로부터의 네트워크 연결 요청이 있으면 AP는 이를 인증 서버에게 알린다. 이 상태에서는 사용자는 AP를 통해 인증 서버와의 통신만이 가능하며, 다른 네트워크 자원에는 접근할 수 없다. 다음 단계에서 인증 서버는 인증 방법을 지정하여 사용자에게 인증에 필요한 정보를 요구한다. 이 요구를 받은 사용자는 인증에 필요한 정보를 인증 서버



〔그림 9〕 802.1x EAP 인증 구조



〔그림 10〕 EAP-TLS 동작

에게 전송하고, 인증 서버는 이 정보를 통해 성공 또는 실패 여부를 판단한다. 실패할 경우에는 사용자의 네트워크 접근은 거부되며, 성공할 경우에 사용자는 AP를 통해 모든 네트워크 자원을 이용할 수 있다.

앞서 설명한 바와 같이 802.1x EAP에서는 다양한 인증 메커니즘을 사용해 인증을 수행할 수 있다. 이 가운데 가장 대표적인 것은 인증서를 이용해 인증을 수행하는 TLS를 이용하는 방법이다. 이는 그림 10과 같은 구조로 이루어진게 된다.

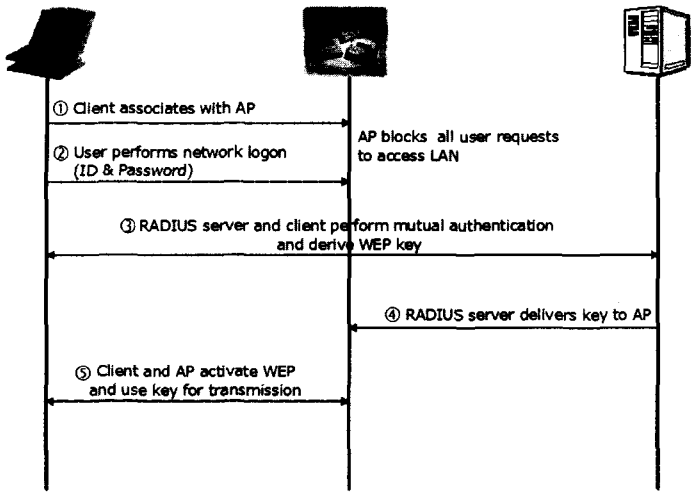
우선 사용자와 AP는 기존의 802.11b 방식에 의한 인증을 수행한다. 즉, SSID 또는 MAC 주소 필터링에 의한 인증을 수행한다. 그리고 나서 802.1x 인증에 필요한 정보를 주고받는다. 아직까지는 802.1x EAP에 의한 인증이 이루어지기 전이기 때문에 사용자는 네트워크 자원을 이용할 수 없다. 이후에 TLS를 통한 사용자 인증이 이루어지게 되며, TLS의 키 공유 메커니즘을 통해 생성된 암호키를 사용자와 AP가 공유하게 된다. 인증이 완료되었기 때문에 사용자는 AP를 통해 네트워크 자원을 이용할 수 있게 되고, WEP 암호화에는 인증 과정에서 공유된 키가 이용된다. 이를 좀 더 자세히 살펴보면 다음과 같다.

① 무선 스테이션(supplicant)이 AP에 참가한다.
② AP는 클라이언트에게 신원 요구를 한다.
③ 클라이언트는 자신의 ID를 응답한다.
④ AP는 EAP 메시지(클라이언트 ID)를 인증 서버로 보내서 인증 서비스를 초기화한다..
⑤ 인증 서버와 클라이언트 간의 인증 프로토콜은 TLS를 사용한다.
⑤-1 인증 서버는 신원 확인을 위해 클라이언트에게 인증서를 요구한다.
⑤-2 클라이언트는 인증서를 AP를 통해 인증 서버에게 보낸다.
⑥ 응답한 인증서가 인증 서버에서 인증이 되면 인증 서버는 클라이언트에게 EAP 성공 메시지를 전송한다.
⑦ AP는 향후 AP와 클라이언트 간의 암호통신에 사용할 WEP 키를 생성한다.
⑧ AP는 생성된 키(WEP 키)를 클라이언트에게 전송한다. 이 때, 서버로부터 받은 키를 WEP 키를 암호화하는데 사용한다.
⑨ 클라이언트와 AP는 WEP 키를 통해 암호 통신을 수행한다.
⑩ 사용자 장비와 AP에서 사용되어지는 WEP 키는 사용자 장비가 로그 아웃(log-out)을 하거나 재인증 타이머가 초과될 때까지 사용되게 된다.

2. LEAP

IEEE802.1x는 802.11b의 인증 메커니즘에 비해서 강력한 사용자 인증을 제공한다. 즉, 802.11b에서 실질적으로 사용자 인증이 아닌 디바이스 인증을 수행하고, 디바이스 인증 또한 앞에서 살펴본 바와 같이 많은 문제점을 가지고 있는데 비해, 802.1x는 좀 더 향상된 사용자 인증을 제공한다.

그러나 802.1x의 EAP-TLS와 같은 경우에는



〔그림 11〕 Cisco LEAP

클라이언트가 모두 인증서를 소지해야 한다는 점이 부담으로 작용한다. 즉, 현재 인터넷에서의 TLS 통신에서도 서버 인증은 인증서를 이용하지만, 클라이언트 인증은 ID/Password를 이용하는 경우가 대부분인데, 무선랜 환경에서 모든 클라이언트가 인증서를 소지한다는 것은 현실적으로 어려움이 많다.

이를 보완하기 위해 Cisco는 EAP-TLS에 비해 구현이 용이하고 클라이언트의 부담을 덜면서도 비슷한 수준의 인증 강도를 제공하는 Cisco LEAP (Lightweight EAP) 인증 알고리즘을 제작하였다. LEAP는 다른 EAP 방법과 마찬가지로 802.1x 프레임워크 상위에서 동작하며 다음과 같은 기능을 제공한다[7].

- 상호인증: 802.11b의 인증 메커니즘은 클라이언트 인증은 있지만 클라이언트에 의한 네트워크 인증은 없다. LEAP은 이를 보강하여 상호인증이 가능하도록 하고 있다.
- 사용자 기반 인증: 802.11b의 인증 메커니즘은 사용자 인증이 아닌 단말기 인증이라고 할 수 있다. 즉, 불법적인 사용자가 정당한 단말기를 훔쳐 네트워크 접속을 시도할 경우, 이를 막을 수 있는 방법이 없다. LEAP은 이를 보완하여 단말기 인증이 아닌 실질적인 사용자 인증이 가능하도록 한다.
- 동적인 WEP 키: LEAP을 통해서 클라이언트별로 유일한 WEP 키를 생성할 수 있으며, 802.1x의 세션이 종료되어 다시 인증을 할 경우, 새로운 WEP 키를 생성하게 된다. 또한 이 과정은 사용자의 입력 없이 자동으로 이루어진다.

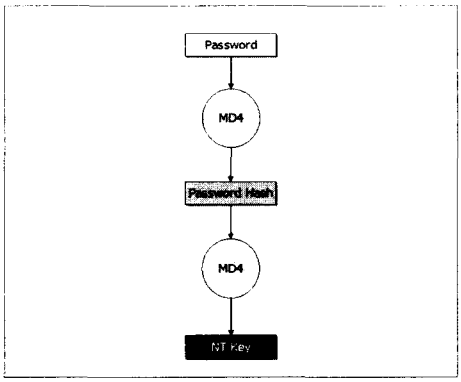
이와 같은 LEAP에 의해 사용자 인증이 이루어지는 과정을 살펴보면 그림 11과 같다.

① 클라이언트는 AP에 접속을 요청한다. 이 과정에서 클라이언트는 접속하고자 하는 AP의 신원을 확인하고, AP 역시 클라이언트의 신원을 확인한다.
② 인증을 위해 ID와 Password를 전송한다.
③ 인증 서버와 클라이언트는 상호인증을 수행하고 WEP 키를 생성한다.
④ 인증 서버는 생성한 WEP 키를 AP에게 전송한다.
⑤ 클라이언트와 AP는 통신을 수행한다.

기술한 바와 같이 LEAP는 패스워드 기반의 인증 메커니즘이다. 이 때, 패스워드를 도청으로부터 보호하기 위해서 사용자가 입력한 패스워드를 암호키로 변환한다. LEAP 암호키는 그림 12와 같이 MD4를 이용하는 WindowsNT 키 형식이다.

WindowsNT 키를 사용함으로써 LEAP에서 Windows 2000 Active Directory와 같은 WindowsNT 도메인 인증 데이터베이스를 사용하는 것이 가능하다. 또한 MS-CHAP(Microsoft Challenge Handshake Authentication Protocol)

패스워드를 사용하는 ODBC(Open Database Connectivity)도 사용할 수 있다.



〔그림 12〕 WindowsNT Key

7. PEAP

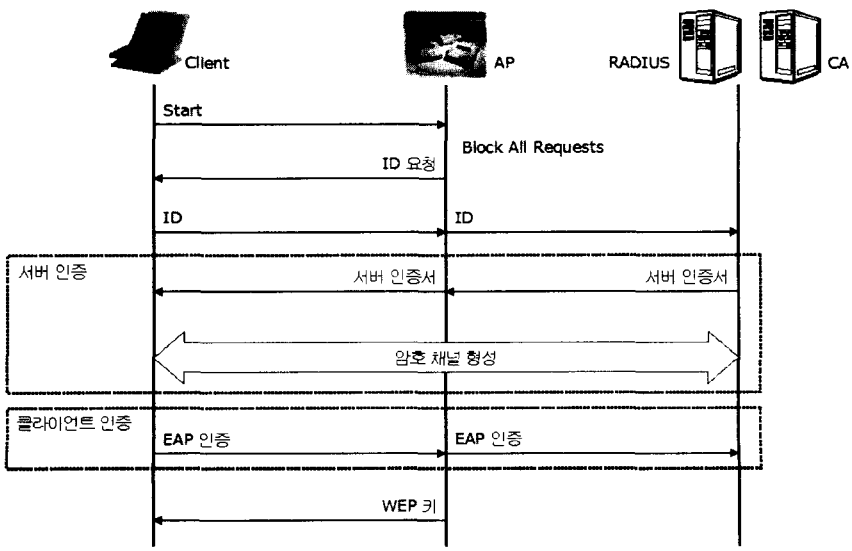
PEAP(Protected EAP)은 Microsoft와 Cisco에서 지원하는 인증 메커니즘으로 IEEE의 표준화 과정에 있다. PEAP는 복합 인증 메커니즘(hybrid authentication)이라고 할 수 있다. 즉, 서버 인증은 PKI 기반의 인증 메커니즘을 사용하며, 클라이언트 인증은 EAP의 여러 가지 인증 메커니즘을 사용할 수 있다. 바꿔 말하면 PKI 기반의 서버 인증을 통해 클라이언트와 인증 서버 사이에 안전한 경로(secure tunnel)을 형성한 후에, GTC(General Tokec Card), OTP, MD5 Challenge/Password와 같은 단방향 인증 방식에 의해 클라이언트 인증을 수행한다. 이 때, PKI 기반의 인증이란 EAP-TLS를 뜻한다.

EAP-TLS에 의해 상호인증을 수행할 경우에는 무선랜을 사용하는 모든 사용자에게 인증서를 발행해야 하는데, 이 경우 관리적인 면이나 확장성 면에서 문제가 발행할 수 있다. PEAP은 이와 같은 부담을 덜고, 효율적으로 클라이언트 인증과 서버 인증을 수행할 수 있도록 해준다.

PEAP에 의한 인증 과정을 보다 자세하게 살펴보면 그림 13과 같다.

① 클라이언트는 AP에게 EAP Start 메시지를 보내 네트워크 접속을 요청한다.
② AP는 클라이언트에게 ID를 요청한다.
③ 클라이언트는 NAI(Network Access Identifier), 즉 사용자 이름을 전송한다.
④ AP는 클라이언트의 NAI를 RADIUS 서버에게 전송한다.
⑤ RADIUS 서버는 클라이언트에게 자신의 인증서를 전송한다.
⑥ 클라이언트는 RADIUS 서버의 인증서를 검증함으로서 RADIUS 인증을 수행한다.

여기까지의 과정은 EAP-TLS와 동일하다. 이후 과정이 PEAP과 EAP-TLS가 다른 부분이다.



〔그림 13〕 PEAP 인증

⑦ 클라이언트와 서버는 TLS에 의해 교환된 키를 이용해 암호 채널을 형성한다.
⑧ RADIUS 서버는 새로운 EAP 인증을 클라이언트에게 요청하며, 이는 TLS에 의해 암호화되어 보호된다.
⑨ 클라이언트 인증이 이루어진다. 인증 과정 동안 RADIUS 서버와 클라이언트가 주고 받는 메시지는 TLS에 의해 보호된다.
⑩ RADIUS 서버는 AP에게 클라이언트 성공을 알리는 메시지를 전송한다. 이 메시지에는 WEP 키가 포함되어 있으며, AP는 WEP를 저장함과 동시에 클라이언트에게 전송한다.
⑪ 분배된 WEP 키에 의해 클라이언트와 AP는 암호통신을 수행한다.

Ⅳ. 무선랜 환경에서의 PKI 고려사항

앞서 IEEE802.11b의 사용자 인증 메커니즘이 매우 취약함에 따라, 이를 보완하기 위해 개발된 EAP-TLS, LEAP, PEAP 등 IEEE802.1x 기반의 여러 가지 사용자 인증 메커니즘에 대해서 살펴보았다. 이와 같은 사용자 인증 메커니즘의 특징으로 모두 공개키 암호기술을 이용해서 동작함을 알 수 있다.

따라서 이와 같은 인증 메커니즘들이 동작하기 위해서는 PKI의 구축이 필수적이다. 그러나 무선랜 환경에서 PKI의 구축은 유선 네트워크 환경에서의 PKI 구축과는 다른 양상을 지닐 수 있다. 이는 무선 클라이언트가 유동적인 IP 주소를 갖고 자주 AP의 서비스 범위(셀) 사이에서 이동이 가능하다는 점, 유선 네트워크에 비해 대역폭이 작고 단말기의 종류가 다양해질 수 있다는 점 등, 유선 네트워크와는 다른 서비스 환경을 갖고 있기 때문이다.

본 장에서는 무선랜 환경에서 PKI를 구축할 때 고려해야 할 사항에 대해서 분석한다.

1. 인증서 및 인증서폐지목록 프로파일

IETF PKI 작업반에서는 무선랜 환경을 위한 인증서 프로파일 작성 작업을 진행하고 있다. 이는 무선랜 환경에 적합하도록 확장필드를 추가/변경하는 것을 내용으로 하고 있다. 그러나 현재 이 작업은 초안(드래프트 문서) 상태에 머물고 있는 상황이다.

무선랜 인증서 프로파일에서 우선적으로 고려한 것은 사용자 편의성이다. 즉, 무선랜 사용자의 경우, 이동하면서 서로 다른 네트워크에서 인증서를 사용해야 하기 때문에 여러 개의 인증서를 소지해야 할 필요가 있는데, 이 때 상황에 적합한 인증서를 사용자의 입력 없이 인증서 확장필드에 의해서 선택할 수 있도록 확장필드를 작성해야 한다. 무선랜 사용자가 서로 다른 네트워크를 사용하는 경우에 대해서 좀 더 살펴보면 다음과 같다.

무선랜 사용자는 회사에서 무선랜을 사용하다가 동일한 단말기로 외부에서 공중 무선랜 서비스를 이용할 수 있다. 이 경우, 서비스 제공자가 다르기 때문에 AP에 설정된 SSID도 다를 수밖에 없다. 만약 2개의 네트워크에서 사용자 로밍(roaming)을 허용한다면 하나의 인증서로 2개의 네트워크에 모두 접속할 수 있지만, 그렇지 않다면 사용자는 현재 네트워크에 적합한 인증서를 직접 선택해서 사용할 수밖에 없다. 네트워크 간의 이동이 자주 일어난다면 이 과정은 매우 비효율적일 수밖에 없다.

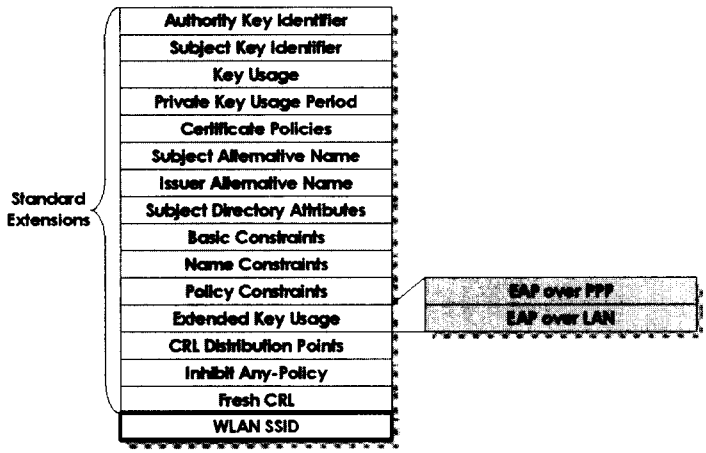
IETF의 무선랜 인증서 프로파일은 이와 같은 사용자의 불편을 덜 수 있도록 인증서를 자동적으로 선택 가능하도록 하는데 중점을 두고 있으며, 이에 따라 그림 14와 같이 표준 확장필드에 WLAN SSID 필드를 추가하고, Extended Key Usage 필드 내에 EAP over PPP 및 EAP over LAN을 추가하였다.

우선 Extended Key Usage 확장필드에 대해서 살펴보면, 이 필드는 Key Usage 확장필드와 함께 공개키의 용도를 나타내는데 사용되며 1개 이상의 용도를 기록할 수 있고, 다음과 같은 구조를 같는다.

```
id-ce-extKeyUsage OBJECT IDENTIFIER
  ::= { id-ce 37 }
ExtKeyUsageSyntax
  ::= SEQUENCE SIZE (1..MAX) OF
      KEY PURPOSE ID
KeyPurposeID
  ::= OBJECT IDENTIFIER
```

무선랜 인증서에서는 이 KeyPurposeID가 다음과 같이 사용된다.

```
id-kp-eapOverPPP OBJECIDENTIFIER
  ::= { id-kp 13 }
id-kp-eapOverLAN OBJECIDENTIFIER
  ::= { id-kp 14 }
```



〔그림 14〕 무선랜 인증서 확장필드

이 확장필드가 critical로 마크될 경우, 공개키는 오직 확장필드에 나타난 용도로만 사용될 수 있으며, non-critical인 경우에는 다른 용도로 사용될 수도 있다.

또한 만약 Key Usage 확장필드와 Extended Key Usage 확장필드 모두가 critical로 마크되었다면, 이 2개의 필드는 독립적으로 처리되기 때문에 공개키는 2개의 확장필드에서 기술된 용도로만 사용될 수 있다.

새롭게 추가된 WLAN SSID 확장필드는 반드시 non-critical이어야 하며, SSID들의 목록을 포함한다. 사용자가 저장하고 있는 인증서 가운데 하나 이상이 Extended Key Usage 확장필드에 의해 현재의 무선랜 환경에 적합한 것으로 나타날 경우, 이 확장필드를 검색해서 적절한 SSID를 포함하고 있는 인증서를 선택하게 된다. 이 확장필드는 다음과 같이 구성된다.

```
id-pe OBJECT IDENTIFIER ::=
  { iso(1) identified-organization(3)
    dod(6) internet(1) security(5)
    mechanisms(5) pkix(7) 1 }
id-pe-wlanSSID OBJECT IDENTIFIER
    ::= { id-pe 13 }
SSIDList ::=
    SEQUENCE SIZE (1..MAX) OF SSID
SSID ::=
    OCTET STRING (SIZE (1..32))
```

2. ID 확인

EAP-TLS를 이용해 사용자 인증을 할 경우, 무선랜 클라이언트 인증은 EAP-TLS에 의한 인증 이전에 사용자가 전송한 ID를 인증서를 통해 인증하는 과정이다. 따라서 클라이언트 인증서 내에 ID를 포함시키거나, 인증서와 저장소에 저장된 사용자 ID를 매핑시켜서 인증을 수행할 수 있다.

그러나 클라이언트 입장에서 보면 인증서버는 자신의 접속하려는 곳과 일치하지 않으며, 인증서버가 반드시 authenticator (AP)와 같은 시스템에 설치되는 것도 아니다. 이 때문에 인증서버가 전송한 인증서 내의 인증서버 주소와 실제 클라이언트가 접속을 하려는 곳의 주소가 서로 달라서 인증에 실패하는 경우가 발생할 수 있다.

3. 인증서 폐지

앞서 설명한 바와 같이 802.1x에 의해 인증이 이루어지기 전에 클라이언는 인증서버 외의 네트워크 자원에 접속할 수 없다.

이는 인증이 완료되기 전에 클라이언트가 네트워크를 이용할 수 없음을 의미한다. 그러나 인증서버의 인증서 폐지 여부를 확인하기 위해서 클라이언트는 인증서폐지목록(CRL: Certificate Revocation List)을 다운로드 받아야 한다. 즉, 클라이언트가 네트워크에 연결되지 않은 상태에서 인증서버 인증서의 폐지 여부를 확인할 수 있는 방법이 존재하지 않는다.

이 문제는 인증경로 구축에 있어서도 마찬가지로 적용된다. 즉, 클라이언트가 인증서버의 인증서를 검증하고자 할 때, 인증서버에게 인증서를 발행한 CA의 인증서를 비롯해서 필요한 인증서를 미리 저장하고 있지 않아 인증경로를 구축할 수 없다면 필요한 인증서를 저장소나 CA로부터 다운로드 받아야 한다. 그러나 이 과정 역시 클라이언트에 대한 인증이 완료되지 않아 네트워크에 대한 연결이 없는 상태이기 때문에 CA나 저장소로의 접속이 허용되지 않아 수행이 불가능하다.

4. AP 변경시 재인증

무선랜의 특성상 클라이언트가 AP 사용 도중에 AP의 서비스 범위를 벗어나 다른 AP를 이용한 통신을 시도할 수 있다. 이 때, 새로운 AP 입장에서는 클라이언트가 인증되지 않았기 때문에 다시 처음부터 인증을 수행해야 한다. AP 변경이 자주 일어난다면, 이 과정은 매우 비효율적이다. 더 나아가 다시 처음부터 인증을 수행할 경우에, 새로운 AP에서 SSID의 변경 등에 의해서 이전의 인증과정에서 사용한 인증서를 사용할 수 없는 상황이 발생할 수도 있다.

또한 EAP-TLS 등의 인증 메커니즘을 통해 인증을 수행한 후, 여기서 생성된 암호키를 WEP 키로 해서 클라이언트와 AP가 암호통신을 한다면, AP 변경후 WEP 키를 재사용할 수 있는 방안에 대한 고려도 이루어져야 한다.

V. 결 론

무선랜 기술은 물리적인 네트워크 선의 설치가 필요 없어 네트워크 구축에 소요되는 시간이 적고, 높은 사용자 이동성 및 네트워크의 확장성 등의 장점으로 인해 사용자가 급격하게 증가하고 있다.

그러나 현재 무선랜 표준을 통해 제공되는 서비스는 보안상 많은 취약성을 가지고 있다. 특히 인증 메커니즘의 경우에는 사용자 인증이 아닌 디바이스 인증에 머물고 있는 실정이다.

이와 같은 문제를 해결하여 강력한 사용자 인증을 제공하기 위해서는 유선랜과 마찬가지로 PKI에 기반한 사용자 인증 메커니즘의 구축이 필수적이다. 하지만, PKI 구축시에도 역시 무선랜 환경의 특성을 반드시 고려해야 한다.

본 논문에서는 무선랜 환경에서 사용자 인증 메커니즘의 취약성을 알아보고, 무선랜 환경에서 PKI를 구축할 경우에 반드시 고려해야 하는 사항들에 대해서 분석하였다.

무선 클라이언트가 유동적인 IP 주소를 가지고 자주 AP의 서비스 범위 사이에서 이동이 가능하며 유선 네트워크에 비해 대역폭이 작고 단말기의 종류가 다양해 질 수 있는 등, 무선랜 환경과 유선 네트워크 환경은 서로 상이하기 때문에 무선랜 환경에 적용되는 PKI 역시 유선 네트워크에서의 PKI와는 다른 양상을 지니게 된다. 따라서 무선랜에서 PKI 구축은 인증서 및 인증서폐지목록 프로파일, 서버 인증 방안, 인증서 폐지 방안, AP 변경시 클라이언트 재인증 방안 등에 대해 충분한 고려가 선행된 뒤에 이루어져야 한다. 즉 다양한 무선랜 환경 이용을 위해 여러 개의 인증서를 사용해야 하는 사용자의 편의를 위해 무선랜 환경에 따라 자동적으로 인증서 선택이 가능하도록 인증서 프로파일 개발이 이루어져야 하며, 서버 인증시 발생할 수 있는 문제점을 해결해야 한다. 또한 네트워크 연결 이전에 인증서 및 인증서폐지목록을 획득할 수 있는 방안이 개발되어야 하고, 사용자가 사용하는 AP 변경시 사용자 재인증 및 이전에 사용하던 암호키의 재분배 방안 등에 대한 연구도 요구되고 있다.

향후, 무선랜 서비스가 좀 더 넓은 범위에서 안전한 서비스를 제공하기 위해서는 사용자 인증 메커니즘 및 PKI 구축 방안에 대한 지속적인 연구가 필요하다.

참 고 문 헌

[1] Tom Katygiannis, Les Owens, "Draft Wireless Network Security", National Institute of Standards and Technology (NIST), 2002

[2] "IEEE802.11b Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification", IEEE Standard 802.11b, 1999

[3] 'Port-based Network Access Cotrol', IEEE Standard 802.1x, 2001. 6

[4] L. Blunk, J. Vollbrecht, 'PPP Extensible Authentication Protocol (EAP)', IETF RFC2284, 1998. 3

[5] B. Aboba, D. Simon, 'PPP EAP TLS

Authentication Protocol', IETF RFC2716, 1999. 10
[6] Nikita Borisov, Ian Goldberg, David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", Proceedings of the 7th International Conference on Mobile Computing and Networking, 2001. 7
[7] Pejman Roshan, "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite", 2002
[8] Tom Fout, Warren Barkley, "Wireless 802.11 Security with Windows XP", Microsoft Windows XP Technical Article, 2001. 11
[9] R. Housley, T. Moore, "Wireless LAN Certificate Extensions and Attributes", IETF DRAFT, 2002. 9

〈著 者 紹 介〉

이 종 후 (Jong-hu Lee)
학생회원

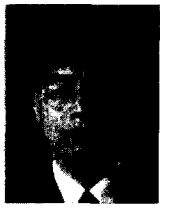
1997년 : 충남대학교 컴퓨터과학과 졸업
1999년 : 충남대학교 컴퓨터과학과 석사
1999년~현재 : 충남대학교 컴퓨터과학과 박사과정
2000년~현재 : (주) 시큐컴
관심분야 : 컴퓨터 및 네트워크 보안

서 인 석 (In-seog Seo)
종신회원

1976년 : 고려대학교 전자공학과 (학사)
1988년 : 충남대학교 계산학 (석사)
2002년~현재 : 충남대학교 박사과정 재학중
1976년 3월~2000년 1월 : 국방과학연구소 중앙전산실장
2000년 2월~현재 : 국가보안기술연구소 키관리센터장
관심분야 : 전산망 보안, 공개키기반구조

윤 혁 중 (Hyuk-Joong Yoon)
정회원

1998년 : 아주대학교 컴퓨터공학과 (학사)
2000년 : 아주대학교 컴퓨터공학과 (석사)
1999년 12월~2000년 7월 : 한국정보보호센터 연구원
2000년 8월~현재 : 국가보안기술연구소 연구원
관심분야 : 네트워크 보안, 공개키기반구조



류 재 철 (Jae-Cheol Ryou)
종신회원

1985년 2월 : 한양대학교 산업공학과 졸업
1988년 5월 : Iowa State Univ. 전산학 석사
1990년 8월 : northwestern Univ. 전산학 박사
1991년 2월~현재 : 충남대학교 정보통신공학부 교수
관심분야 : 인터넷 보안