AP 인증 및 동적 키 분배를 이용한 안전한 무선랜 시스템 구현

이 종 후[†] · 이 명 선[††] · 류 재 철[†††]

요 약

현재의 무선랜 표준인 IEEE802.11b가 많은 보안 취약성을 가지고 있는 것은 잘 알려진 사실이다. 특히 IEEE802.11b에서의 인증은 사용자 인증이 아닌 디바이스 인증에 머물고 있으며, 제공되는 인증 메커니즘들 역시 여러 가지 면에서 취약하다. 한편, IEEE802.1x는 IEEE802.11b 인증의 취약한 부분을 보완하고 강력한 사용자 인증을 제공할 수 있는 메커니즘으로 개발되었으나 이 역시 AP에 대한 인증을 수행하지 않는 등, 취약한 부분이 있다. 또한 WEP을 통해 제공되는 기밀성 및 무결성 역시 키 스트림 재사용 공격, IV 재사용 공격 등에 취약하다. 이에 따라 본 논문에서는 무선랜 환경에 적합한 안전한 사용자 인증 메커니즘 및 기밀성을 제공하는 무선랜 보안 시스템을 제안한다. 제안하는 시스템은 IEEE802.1x를 기반으로 하고 TLS를 통해 무선랜의 구성요소인 클라이언트, AP, 인증서버에 대한 사용자 인증을 모두 수행한다. 그리고 동적인 키 분배를 통해 암호통신의 안전성을 향상시킨다.

Implementation of a Secure Wireless LAN System using AP Authentication and Dynamic Key Exchange

Jong-hu Lee[†] · Myung-sun Lee[††] · Jae-cheol Ryou[†††]

ABSTRACT

The existing wireless LAN standard IEEE802.11b has many vulnerabilities from security point of view. The authentication mechanisms in IEEE802.11b have many vulnerabilities. As a result to complement the weak of IEEE802.11b authentication, the IEEE802.1x had been developed in the sense of providing strong user authentication with appropriate mechanism. But this mechanism does not perform AP authentication and there are also some weak points. And in confidentiality and message integrity case, WEP is weak from key stream reuse attack, IV reuse attack and so on. For that reason, in this paper we propose secure wireless LAN system. Our system provides strong user authentication, confidentiality, and message integrity based on existing IEEE802.1x framework and TLS.

키워드 : 무선랜(WLAN), IEEE802.11b, IEEE802.1x, 사용자 인증(User Authentication), 키 분배(Key Exchange)

1. 서 론

무선랜은 개발 초기에는 높은 가격과 낮은 데이터 전송 속도 등으로 인해 널리 사용되지 못했으나, 1990년대 들어서면서 IEEE(Institute of Electrical and Electronics Engineers)에서 802.11 프로젝트를 시작하면서부터 본격적인 개발이 이루어지기 시작했다. IEEE는 1997년에 처음으로 802.11 국제 표준을 승인하였으며 이는 1999년에 802.11a와 802.11b로 분리되었다. 802.11의 목표는 802.3 이더넷(Ethernet) 표준과 동일한 수준의 무선통신을 제공하는 표준을 제정하는 것이다[1, 2].

무선랜 기술이 최근 들어 각광을 받고 있는 이유는 주로 설치 비용이 낮고 사용이 편리하기 때문인데, 무선랜 기술의 주요 장점을 살펴보면 다음과 같다[3].

- 사용자 이동성 : 물리적으로 유선 상에서 네트워크에 접속이 가능하지 않은 상태에서도 인터넷을 비롯한 네트워크에 접근이 가능하며, 유선 네트워크를 사용할 때와 비슷한 수준의 통신이 가능하다.
- 빠른 설치 : 물리적인 네트워크 선의 설치가 필요 없기 때문에 네트워크 구축에 소요되는 시간을 줄일 수 있다.
- 유연성 : 네트워크 사용이 불가능한 장소에서도 AP(Access Point)만 설치하면 바로 네트워크 사용이 가능하다.

※ 본 연구는 대학 IT연구센터 육성지원사업의 연구결과로 수행되었음.
† 준 회 원 : (주) 시큐컴 대표이사
†† 정 회 원 : 한남대학교 대학원 컴퓨터공학과
††† 종신회원 : 충남대학교 정보통신공학부 교수
논문접수 : 2003년 12월 8일, 심사완료 : 2004년 3월 25일

- 확장성 : 여러 개의 AP 설치를 통해 네트워크 사용 범위를 쉽게 확장할 수 있다.

그러나 이와 같은 여러 가지 장점에도 불구하고 현재의 무선랜 기술표준인 IEEE802.11b의 보안상 취약성은 무선랜 확산의 걸림돌로 작용하고 있다. IEEE802.11b에서는 기밀성 및 무결성 제공을 위해서 WEP(Wired Equivalent Privacy)이라는 보안 메커니즘을 제공하고 있으나, 이 메커니즘은 키 스트림 재사용 공격, IV 재사용 공격 등으로부터 취약하다. 사용자 인증 또한 도청, 키 스트림 재사용 공격 등에 취약하다. 특히 사용자 인증의 취약성을 보완하기 위해 개발된 IEEE802.1x 역시 AP 인증의 부재로 인해 취약성이 들어나고 있다.

이에 따라 본 논문에서는 무선랜 환경에서 AP 인증을 포함해 강력한 사용자 인증을 제공하고 동적인 키 분배를 통해 안전한 암호통신을 가능케 하는 안전한 무선랜 통신 시스템을 제안하고자 한다.

본 논문의 2장에서는 기존 IEEE802.11b 및 IEEE802.1x의 내용을 기술하고 취약성을 분석한다. 3장에서는 제안하고자 하는 안전한 무선랜 통신 시스템의 설계 내용을 기술하고, 4장에서는 제안 시스템의 분석 및 구현 내용에 대해서 기술한다. 마지막으로 5장에서 결론을 맺는다.

2. 무선랜 보안

본 장에서는 기존의 무선랜 시스템에서 제공되는 보안 기능에 대해서 분석한다. 크게 사용자 인증과 기밀성 및 무결성 관점에서 IEEE802.11b와 IEEE802.1x에서 제공하는 보안기능의 취약성을 분석한다.

2.1 사용자 인증

2.1.1 SSID 및 MAC 주소 필터링

IEEE802.11b에서 사용자 인증은 암호기술을 이용하는 경우와 그렇지 않은 경우가 있다. 우선 암호기술에 기반하지 않은 인증 방법에 대해서 살펴보면 SSID(Service Set Identifier)를 이용하는 방법과 MAC 주소를 이용하는 방법이 있다[1].

우선 SSID를 이용하는 방법에 대해서 살펴보면, 무선랜 카드에서 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" 또는 "NULL"로 설정하거나 브로드캐스트하도록 설정하는 경우, 누구든지 AP에 접속이 가능하다[1, 4].

MAC 주소 필터링은 AP에서 접속이 허용된 MAC 주소의 목록을 저장하고 있으며, 무선랜카드에서 접속을 위해 자신의 MAC 주소를 전송하면 AP는 접속이 허용된 MAC 주소 목록에 포함된 주소인지 여부를 확인하고 접속의 허용 또는 거부를 결정하는 방법이다. MAC 주소를 이용한 인증의 경우도 SSID를 통한 인증과 마찬가지로 MAC 주소가 평문 형태로 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. 또한 MAC 주소가 무선랜카드마다 유일하게 할당되는 값이지만, 외부에서 조작이 쉽게 이루어진다는 문제도 지적할 수 있다. 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[4].

2.1.2 공유키 인증

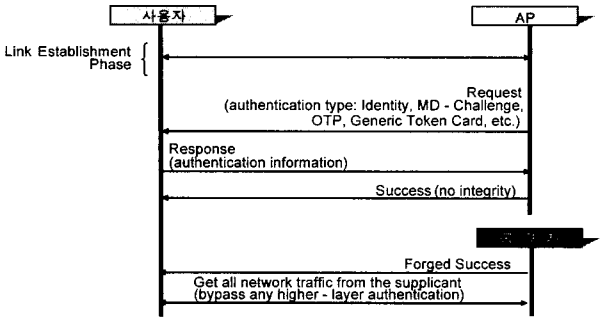
암호기술을 이용한 사용자 인증은 사용자(무선랜카드)와 AP가 공유하는 WEP(Wired Equivalenct Privacy) 키를 이용해서 인증하는 방법으로 Challenge-Response 방식이다.

이 방법은 하나의 키를 이용해서 Response를 생성하기 때문에 키 스트림 재사용 공격이 가능함이 이미 잘 알려져 있다[1, 4].

2.1.3 IEEE802.1x

앞에서 살펴본 바와 같이 IEEE802.11b에서의 사용자 인증 방식은 신뢰하기 어렵다. 이에 따라 IEEE802.11b에서의 사용자 인증 문제를 해결하기 위한 방법으로 IEEE802.1x가 개발되었다[5].

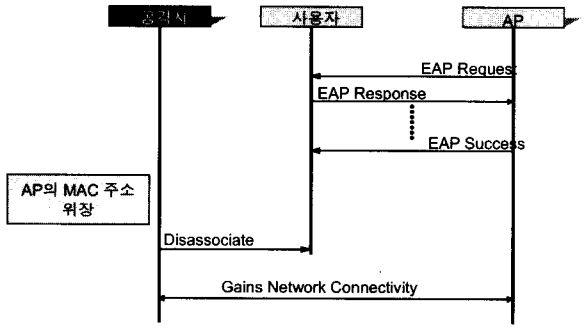
그러나 IEEE802.1x의 사용자 인증 메커니즘 역시 클라이언트에 대한 인증만을 정의하고 있으며, AP에 대한 인증은 정의하고 있지 않다. 즉, 상호인증(mutual authentication)을 제공하지 않는다. AP는 EAP 요청 메시지를 사용자에게 보내고 EAP 응답 메시지를 수신하는 역할만을 수행하지 EAP 응답 메시지를 송신하는 역할은 수행하지 않는다. 이와 같이 상호인증을 제공하지 않을 경우에는 다양한 형태의 스푸핑 공격이 가능하다. (그림 1)은 EAP Success 메시지 스푸핑을 통한 Man-in-the-middle 공격 방법이 가능함을 보여준다[8].



(그림 1) EAP SUCCESS 메시지 스푸핑

(그림 1)에서 사용자에 대한 인증이 성공하였음을 알리는 EAP Success 메시지는 암호기술을 통해 보호되지 않는다. 따라서 공격자가 이미 인증이 완료된 후에 AP가 전송하는 Success 메시지를 가로챈 후, 다시 AP로 위장하여 Success 메시지를 사용자에게 전송하는 공격이 가능하다. 이 공격이 성공하게 되면 공격자는 사용자로부터 전송되는 모든 데이터의 내용을 알 수 있다. 이 공격은 IEEE802.1x 인증방법으로 EAP-TLS 등 상호인증 메커니즘을 제공하는 방식이 사용된다 하더라도, 얼마든지 공격이 가능하다는 점에서 위험성이 크다.

또한 이 공격을 좀 더 발전시켜 (그림 2)는 IEEE802.1x에서 세션 가로채기(session hijacking) 공격이 가능함을 보여준다[8].



(그림 2) Disassociate 메시지 스푸핑에 의한 세션 하이재킹

(그림 2)에서 모든 인증과정이 완료되고 사용자가 AP와 통신을 하고 있는 가운데, AP의 MAC 주소로 위장한 공격자가 사용자에게 통신 종료를 알리는 Disassociate 메시지를 전송한다. 이 메시지 역시 보호되지 않음으로 위장이 가능하고, 따라서 사용자는 더 이상 통신을 수행할 수 없다. 이 후, 공격자는 다시 사용자의 MAC 주소를 이용해 사용자로 위장하여 AP와의 통신을 계속할 수 있다. 이 공격 역시 상호인증을 지원하는 인증 메커니즘이 사용된다 하더라도 가능한 공격이다.

2.2 기밀성 및 무결성

IEEE802.11b에서의 기밀성 제공을 위한 보안 메커니즘인 WEP은 스트림 사이퍼(stream cipher) 관용 암호 알고리즘인 RC4를 이용한다[2].

WEP을 통한 암호화에 사용되는 키의 크기는 64비트 혹은 128비트이며, 이 때 24비트는 IV(Initialization Vector)이기 때문에 실질적인 키의 크기는 40비트와 104비트라고 할 수 있다. 일반적으로 키의 크기가 커질수록 암호의 강도는 높아진다고 할 수 있는데, 그 동안의 연구에 의하면 80비트 이상의 키를 사용할 경우 전수조사(brute-force)에 의한 키 크랙(crack)은 사실상 불가능한 것으로 받아들여지고 있다[9].

또한 IEEE802.11b에서의 무결성은 CRC(Cyclic Resundancy Check)를 이용해서 제공된다. 송신자는 데이터를 전송하기 전에 CRC 값을 계산하여 원래의 평문과 함께 암호화한다. 수신자는 수신한 암호문을 복호화한 뒤 데이터 부분의 CRC 값을 계산하여 수신한 CRC와 비교하여 동일한 경우에는 전송 도중에 데이터가 변경되지 않은 것으로 간주한다.

앞서 WEP을 이용한 사용자 인증에서 기술한 바와 같이 스트림 사이퍼를 통한 암호 통신에서 동일한 키를 사용할 경우 공격자가 키에 대한 정보 없이도 암호문에 대한 평문을 얻어낼 수 있다. 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 비밀키와 각 패킷마다 임의로 생성되는 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 있으나, 공격자가 비밀키를 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 이루고 있지 못하다.

이는 잘못된 IV 관리에서 비롯된다. 일반적으로 공유되는 비밀키는 자주 변경되지 않음으로 IV의 재사용은 키 스트림의 재사용의 원인이 된다. IV는 공개되어 있음으로 IV의 복사본이 쉽게 공격자에게 노출될 수 있다. 결국 이전에 사용했던 IV를 재사용하는 것은 키 스트림 재사용 공격에 취약해지는 원인이 된다.

WEP 표준은 매 패킷마다 IV를 변경하여 사용하도록 권고하고 있다(강제적인 요구사항은 아니다). 그러나 IV의 생성 방법에 대해서는 정의하고 있지 않으며, 또한 구현 방법에 대해서도 기술하고 있지 않다. 경우에 따라서 무선랜카드를 탈착후 다시 장착할 때마다 IV를 '0'으로 초기화하고 데이터가 전송될 때마다 '1'씩 증가하도록 구현한 예도 있다. 이 경우 동일한 IV가 자주 재사용될 위험이 매우 높다[4]. 또한 WEP 표준은 IV의 크기를 24비트로 제한하고 있는데, IV의 크기가 비교적 작기 때문에 동일한 IV가 여러 패킷에서 사용될 위험이 크다. 무선랜카드에서 1500바이트의 패킷을 AP에 계속 보내고 평균 5Mbps의 대역폭을 사용한다면(최대 대역폭은 11Mbps) 12시간만에 IV로 유효한 공간이 모두 소진되며, 따라서 공격자가 패킷의 복사본을 쉽게 찾을 수 있다. 또한 각 패킷에서 임의의 24비트 IV를 사용한다면 5000개의 패킷을 전송한 후에 충돌이 발생하게 되는데, 5000개의 패킷은 몇 분이면 전송이 가능하다[4].

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

WEP에서는 메시지 무결성 서비스 제공을 위해 체크섬 메커니즘을 사용한다. 체크섬은 CRC32로 구현되며 암호화된 패킷의 일부이다. 그러나 암호 메커니즘이 사용되지 않은 체크섬 메커니즘으로 메시지 무결성을 제공할 수 없다는 것은 이미 잘 알려져 있다[10].

3. 안전한 무선랜 시스템 설계

2장에서 기존 무선랜 기술인 IEEE802.11b와 IEEE802.1x의 보안 취약성에 대해서 살펴보았다. 3장에서는 이와 같은 취약성을 보완하고 강력한 사용자 인증 및 안전한 암호통신을 제공하는 안전한 무선랜 통신 시스템을 제안하고, 그 설계 내용에 대해서 살펴본다.

3.1 운영 환경 및 시스템 구조

3.1.1 운영 환경

본 논문에서 제안하는 무선랜 보안 시스템 가장 큰 목표는 강력한 사용자 인증 및 안전한 암호통신을 제공하는 것이다. 즉, 사용자 인증이라는 관점에서 인터넷과 같은 네트워크 자원을 이용하는데 있어서 접근제어를 수행하고, 클라이언트 입장에서는 자신의 개인정보 보호를 위해 인터넷 사용을 매개하는 AP 및 인증서버와 상호인증을 수행하도록 한다 또한 기밀성 및 무결성의 관점에서 동적인 키 분배를 제공하여 하나의 키를 장기간 사용하는 기존 WEP의 취약성을 보완한다. 이를 위해 본 논문에서 제안하는 무선랜 보안 시스템은 다음과 같은 환경에서 보안 서비스를 제공한다.

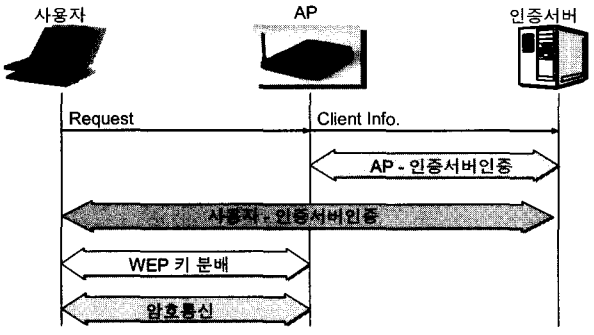
- 인터넷 연결 시점, 즉 AP를 통해 유선랜과의 통신을 시작하는 시점에서의 사용자 인증을 제공한다. 즉, 클라이언트 입장에서는 인증서버와 인터넷과의 연결에 있어서 매개 역할을 하는 AP에 대해서만 인증을 수행하면 된다. 이 후, 클라이언트가 인터넷을 이용하는 과정에서 발생하는 웹 서버를 비롯한 서버 혹은 다른 클라이언트와의 인증은 본 논문에서는 다루지 않는다.
- 클라이언트와 AP 사이의 구간에서는 기본적으로 WEP을 이용한 암호통신이 가능하다.
- 인터넷과 같은 개방형 네트워크에서 운영된다.

3.1.2 제안 시스템 구조

제안하고자 하는 무선랜 보안 시스템은 (그림 3)과 같이 IEEE802.1x 기반의 프레임워크에서 보안 서비스를 제공한다.

(그림 3)에서 보는 바와 같이 제안 시스템은 크게 인증단계와 암호통신 단계로 구분되어 동작하는데, 이 때 사용자 인증은 AP 인증과 클라이언트 인증 등 2단계 인증이 이루어진다. AP 인증은 클라이언트로부터의 연결 요청을 AP가 인증서버에게 전송했을 때, 정당한 AP인지 여부를 인증서버가 판단하고 AP 역시 정당한 인증서버인지 여부를 판단하는 과정이다. 그리고 클라이언트 인증은 무선랜카드 사용자가 정당한 사용자인지 여부를 인증서버가 판단하고 또한 정당한 인증서버인지 여부를 무선랜카드 사용자가 판단하는 상호인증 과정이다. 이와 같은 2단계 인증과정을 통해서 무선랜 통신에 참여하는 모든 구성요소들 간의 상호인증이 이루어진다. 이 때, IEEE802.1x에서는 구체적인 인증 메커니즘으로는 다양한 방법이 사용될 수 있도록 하고있는데, 제안 프레임워크에서도 역시 AP와 인증서버 사이의 인증, 사용자와 인증서버 사이의 인증에 있어서 여러 가지 방법이 사용될 수 있다. 또한 인증 과정에서 교환되는 모든 메시지는 IEEE802.1x EAP 규격을 따르기 때문에 제안하는 메커니즘은 기존 표준기술에 쉽게 적용이 가능하다. 이 때 본 논문에서 WEP 키의 동적인 분배를 위해서 사용자와 인증서버 간의 인증에 EAP-TLS를 이용하며, 분배된 키를 이용해서 암호통신을 제공한다. 이와 같은 사용자 인증 및 암호 통신을 위해서 제안 시스템은 다음과 같은 4가지 요소로 구성된다.

- 클라이언트(무선랜 사용자)
- AP
- 인증 서버
- CA

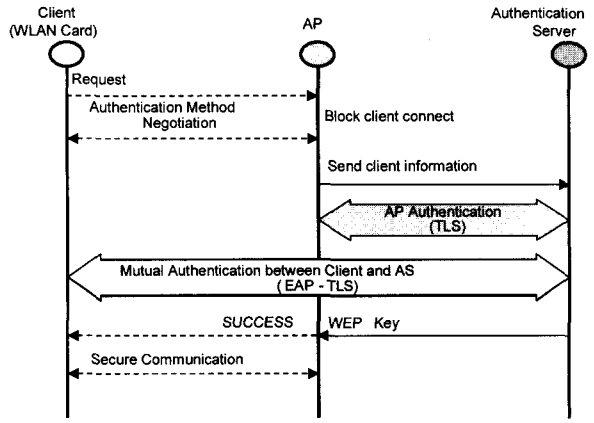


(그림 3) 안전한 무선랜 통신 시스템 프레임워크

3.2 제안 시스템에서의 인증 절차

우선 무선랜 보안 시스템의 사용자 인증 메커니즘((그림 4) 참조)에 대해서 살펴보면, 다음과 같은 4단계로 구분할 수 있다.

① 클라이언트 접속 요청 단계
② AP 인증 단계
③ 클라이언트 인증 단계
④ 키 교환 단계



(그림 4) 제안 메커니즘에서의 인증 절차

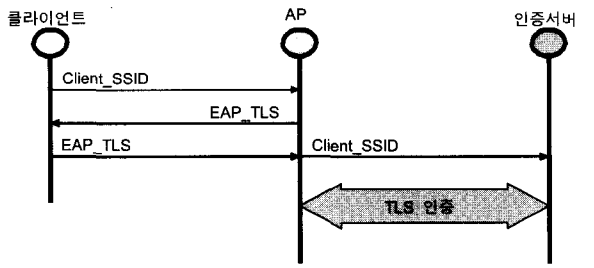
각 단계에 대해서 살펴보면 다음과 같다.

3.2.1 클라이언트 접속 요청

클라이언트가 인터넷 사용을 위해 AP에게 접속요청을 하는 단계로 (그림 5)와 같이 AP에게 클라이언트의 SSID가 전송된다.

클라이언트로부터 접속 요청을 수신한 AP는 클라이언트의 SSID가 유효한 것인지를 확인한다. 유효한 SSID를 수신한 경우, AP는 우선 클라이언트의 유선랜 접속을 차단한다. 이때, 유효하지 않은 SSID를 수신한 경우에는 응답하지 않는다. 이때, 클라이언트에 대한 인증은 뒤에 EAP-TLS 등을 통해서 이루어지기 때문에, SSID에 대한 클라이언트 인증은 생략해도 무방하다. 즉, SSID를 "NULL"이나 "ANY"로 설정하고 사용해도 된다.

클라이언트의 SSID를 확인함과 동시에 AP는 클라이언트로 수신한 클라이언트의 SSID를 인증서버에게 전송하여 클라이언트의 접속요청이 있음을 알린다.



(그림 5) 클라이언트 접속 요청 및 AP 인증 단계

3.2.2 AP 인증

기존 무선랜의 사용자 인증 메커니즘의 가장 큰 문제점은 AP에 대한 인증이 없다는 것이다. 따라서 공격자가 AP의 IP 주소나 MAC 주소를 위장하여 클라이언트와 인증서버 사이에서 man-in-the-middle 공격을 수행할 수 있다. 제안하는 메커니즘에서는 AP에 대한 인증 과정을 추가하였다.

클라이언트와 인증서버가 인증을 수행하기 앞에서 AP는 인증서버와 상호인증을 수행한다. 제안 메커니즘에서는 인증 방법으로 TLS를 사용한다. 따라서 AP와 인증서버는 인증서를 반드시 소지하고 있어야 한다.

3.2.3 클라이언트 인증

AP와 인증서버 간에 인증이 완료되면 클라이언트와 인증서버 간의 상호인증이 수행된다. 이는 기존 IEEE8021.x에서와 마찬가지로 AP를 통해서 EAP-TLS를 이용해서 인증서버와 상호인증을 수행한다. 단, 클라이언트와 인증서버와 사이의 인증과정 가운데, AP와 인증서버 사이의 구간은 AP와 인증서버 사이에 수립된 TLS 채널을 이용한다.

3.2.4 SUCCESS 메시지

EAP-TLS를 통한 클라이언트와 인증서버의 상호인증이 완료되면, 인증서버는 AP에게 성공을 알리는 SUCCESS 메시지를 전송한다. SUCCESS 메시지는 클라이언트와의 인증과정에서 생성된 FINISHED 메시지에 인증서버의 전자서명을 첨부한 메시지이다. AP는 서버로부터 수신한 서버의 전자서명이 첨부된 FINISHED 메시지와 자신이 생성한 성공 메시지를 서버로부터 수신한 암호키로 암호화하여 전송한다. SUCCESS 메시지는 다음과 같이 구성된다.

$$EKU_{AP}[EKR_{server}[H(FINISHED \,||\, WEP\_Key)] \,||\, FINISHED \,||\, WEP\_Key] \quad (1)$$

이 때, WEP 키는 AP만 알아야 하는 정보이므로 AP의 공개키로 암호화되며, FINISHED는 인증서버와 클라이언트의 인증 과정에서 인증서버가 클라이언트에게 전송한 메시지이다. WEP_Key는 클라이언트와 서버가 인증 과정을 통해 공유한 키이다.

식 (1)의 전달 목적은 AP에게는 클라이언트 인증이 성공하였음을 알리고 AP에게 클라이언트와의 암호통신에 사용될 WEP 키를 전달하는 것이다. 즉, WEP 키는 클라이언트와 인증서버만 알고있는 정보인데, WEP 암호통신을 이용하기 위해서는 AP도 WEP 키를 알아야 하기 때문에 인증서버가 AP에게 WEP 키를 전달하는 것이다. 클라이언트 입장에서는 AP가 소지하고 있는 WEP 키가 자신이 인증서버와 인증 과정에서 생성한 WEP 키와 동일하지 않으면, AP 인증이 실패한 것으로 간주한다. 이때, WEP 키는 클라이언트, AP, 인증서버를 제외한 외부로는 노출되어서는 안되는 정보이기 때문에 AP의 공개키로 암호화되어 저장된다.

식 (1)을 수신한 AP는 클라이언트에게 EAP SUCCESS 메시지를 전송하는데 이 메시지의 구성은 다음과 같다.

$$EAP_{WEP\_Key}[EKR_{server}[H(FINISHED \,||\, WEP\_Key)] \,||\, FINISHED \,||\, WEP\_Key \,||\, EAP\_SUCCESS] \quad (2)$$

즉, AP는 서버로부터 수신한 메시지를 복호화한 결과와

자신이 생성한 EAP_SUCCESS를 메시지를 합친 뒤 이를 다시 WEP_Key로 암호화하여 클라이언트에게 전송한다. 이 때, WEP_Key는 서버로부터 수신한 식 (1)을 복호화하여 얻은 값이다. 이 메시지는 클라이언트에 AP가 인증된 AP임을 알리는 목적으로 사용된다. 즉, 인증서버와 인증을 수행하지 못한 AP라면 AP의 비밀키를 알지 못하기 때문에 식 (1) 메시지 전체를 복호화할 수 없다. 따라서 WEP 키를 얻지 못하기 때문에 클라이언트에게 WEP 키로 암호화된 메시지를 전송할 수 없다. 클라이언트는 자신이 가지고 있는 WEP 키로 이 메시지를 복호화하지 못하면 자신과 통신하고 있는 AP를 인증되지 못한 AP로 간주하고 통신으로 종료한다. 또한 좀 더 안전성을 강화하기 위해 서버의 전자서명 메시지가 포함되어 있다. 즉 공격자가 WEP 키를 알아냈다 하더라도 서버의 개인키를 알 수 없기 때문에 서버의 전자서명 메시지를 생성하지 못하여 식 (2)를 생성할 수 없다.

식 (1)과 식 (2)를 통해 클라이언트는 AP로부터 수신한 성공 메시지가 인증서버와의 인증과정에서 교환된 암호키로 복호화되지 않거나, 복호화된 내용 가운데 인증서버의 전자서명이 없는 경우, 또는 전자서명 확인에 실패한 경우 통신을 종료한다. 인증에 성공한 경우에는 AP와의 암호통신을 수행한다.

또한 클라이언트가 AP로부터 수신한 메시지가 클라이언트가 가지고 있는 WEP 키로 복호화되지 않는다면, AP가 인증서버로부터 정당한 WEP 키를 분배받는데 실패하였는 것을 뜻하며 이는 AP 인증이 이루어지지 않았다는 의미임으로 통신을 종료해야 한다. 복호화에 성공하였다 하더라도 복호화된 내용 가운데 인증서버의 전자서명이 없거나 전자서명 확인에 실패하였다면 AP가 인증서버로부터 인증을 받는데 실패하여 인증서버의 전자서명을 획득하지 못하였다는 것을 의미한다.

3.2.5 인증서버 인증

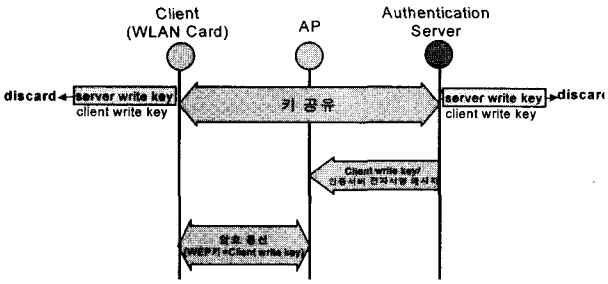
인증서버는 먼저 AP와 제안 메커니즘에 의해 인증서 기반의 상호인증을 수행하고, 다시 클라이언트와 EAP-TLS를 이용해 상호인증을 수행한다. 이때, 인증서버는 동일한 인증서를 이용한다. 인증서버가 AP로부터 키를 제대로 수신했음을 확인하는 메시지를 수신하고 나면 모든 인증 완료되고, 클라이언트와 AP가 암호통신을 수행하게 된다. 클라이언트와의 인증이 성공적으로 종료되면, 인증서버는 클라이언트와 교환환 WEP 키를 AP에게 전달한다.

3.3 암호통신

IEEE802.1x에서는 EAP_START나 EAP_Logoff와 같은 관리 데이터에 대한 무결성을 제공하고 있지 않으나, 앞에서 살펴본 바와 같이 이로 인해 여러 가지 데이터 위장 및 사용자 위장 공격이 가능하다. 따라서 이와 같은 관리 데이터의 보호를 위해서는 반드시 암호통신이 필요하다.

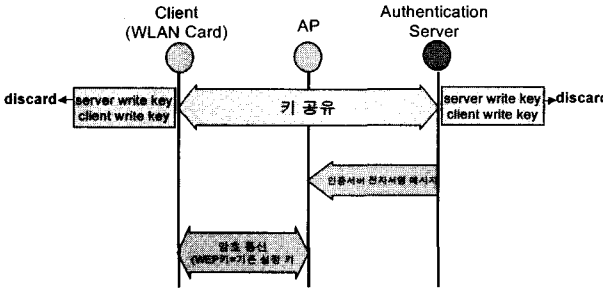
이에 따라 제안하는 무선랜 보안 시스템에서는 사용자 인증과 키 교환이 모두 성공적으로 종료되면, 클라이언트와 AP 사이의 구간은 WEP으로 암호화된다. 이 때 WEP 암호화는 3가지 모드 가운데 하나로 동작할 수 있다.

첫 번째는 기존의 WEP과 동일한 방식으로 암호화가 이루어지되, 인증서버와 클라이언트가 TLS를 통해서 공유하게 된 키를 WEP 키로 사용하는 방법이다((그림 6) 참조). 이 때는 클라이언트에서 AP로 전송하는 데이터를 암호화할 때 사용하는 키와 AP에서 클라이언트로 전송하는 데이터를 암호화할 때 사용되는 키가 동일하다. 따라서 인증서버로부터 AP에게 전송되는 WEP 키의 내용은 'client write key'로 구성된다. 즉, TLS를 통해서는 2가지 종류의 세션키('client write key', 'server write key')가 생성되지만, 기존의 WEP은 방향에 관계없이 동일한 키를 사용하기 때문에 'client write key'만을 이용해서 암호화가 이루어진다.



(그림 6) 암호통신 모드 1

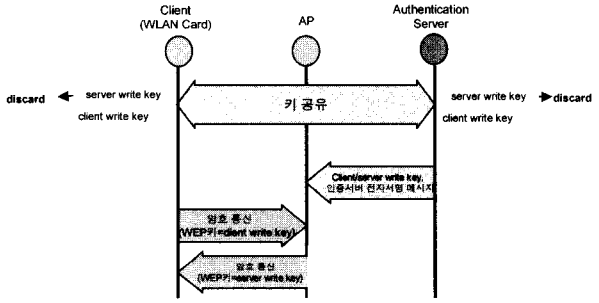
두 번째 모드는 (그림 7)과 같이 기존의 WEP을 그대로 사용하는 동일한 방식이다. 이 경우에는 클라이언트와 인증서버가 공유하는 키를 WEP 키로 새롭게 설정하지 않고, 기존에 클라이언트와 AP에 설정되어 있는 WEP 키를 그대로 사용한다. 즉, 제안 메커니즘은 사용자 인증의 기능만 수행하고 WEP 키 교환의 기능은 수행하지 않는다. 그러나 이 경우에도 AP와 인증서버는 상호인증을 수행한다.



(그림 7) 암호통신 모드 2

마지막 방법은 (그림 8)과 같이 기존의 WEP 암호 방식과는 달리 전송 방향에 따라 서로 다른 키를 사용하는 모드이다. 즉 인증서버에서 AP로 전달되는 WEP 키의 내용에는

'client write key'와 'server write key'가 모두 포함된다. AP와 클라이언트의 WEP 암호통신에 있어서 클라이언트가 AP에게 전송하는 메시지는 'client write key'를 이용해서 암호화되며, AP가 클라이언트에게 전송하는 메시지는 'server write key'를 이용해서 암호화된다.



(그림 8) 암호통신 모드 3

4. 제안 시스템 분석

본 장에서는 제안한 무선랜 보안 시스템에 대해서 분석을 위해 제안 시스템의 구현 내용에 대해서 기술하고 이를 분석한다.

4.1 제안 메커니즘 구현

4.1.1 구현 환경

제안 메커니즘은 <표 1>과 같은 환경에서 구현된다.

〈표 1〉 구현 환경

	클라이언트	AP	인증서버
운영체제	Windows2000	Linux	Linux
사용언어	C/C++	C/C++	C/C++
암호 라이브러리	OpenSSL 0.9.5	OpenSSL 0.9.5	OpenSSL 0.9.5
비 고	Cisco3496 무선랜카드 사용	리눅스에서 에뮬레이션	

클라이언트는 open1x 오픈소스를 수정하여 구현하였다[11]. 또한 현재 제안 시스템과 같은 사용자 인증 기능을 제공하는 AP는 없기 때문에, AP의 기능은 무선랜카드와 유선랜카드를 동시에 장착한 리눅스에서 에뮬레이션하였다. 그리고 인증서버는 오픈소스로 공개된 RADIUS 서버에 제안 시스템 지원을 위해 필요한 기능을 추가하여 사용하였다. 모든 구성요소에서 암호 라이브러리는 역시 오픈소스인 OpenSSL을 사용하였다[12, 13]. 이 밖에 인증서 발급을 위해서 CA 시스템이 필요한다. 이 역시 OpenSSL에서 제공하는 CA 시스템을 사용하였다.

또한 제안 시스템이 동작하기 위해서 각 구성요소별로 다음과 같은 정보를 미리 설정 또는 저장되어 있어야 한다.

① 클라이언트

- 클라이언트 인증서 : CA로부터 발급 받은 사용자 인증서를 저장하고 있어야 한다.
- 인증서버 IP 주소, CA IP 주소, 디렉토리 IP 주소 : AP의 정보는 AP가 브로드캐스트하는 정보에 의해서 획득할 수 있지만, 인증을 위해 필요한 정보인 인증서버 IP 주소, CA 및 저장소 IP 주소는 미리 설정되어 있어야 한다.
- 인증체인 : 클라이언트 인증서를 발급한 CA가 최상위 CA (Root CA)가 아닌 경우에는 최상위 CA로부터 클라이언트 인증서를 발급한 CA까지의 모든 인증서를 저장하고 있어야 한다.

② AP

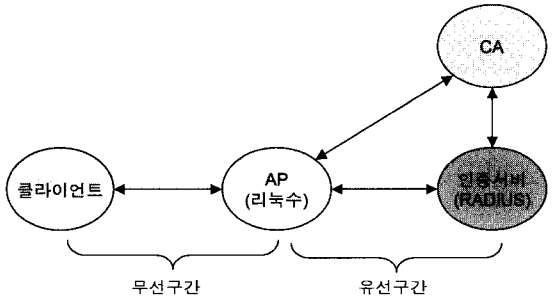
- AP 인증서 : CA로부터 발급 받은 AP 인증서를 저장하고 있어야 한다.
- 인증서버 IP 주소, CA IP 주소, 디렉토리 IP 주소 : 인증을 위해 필요한 정보인 인증서버 IP 주소, CA 및 저장소 IP 주소는 미리 설정되어 있어야 한다.
- 인증체인 : 인증서를 발급한 CA가 최상위 CA (Root CA)가 아닌 경우에는 최상위 CA로부터 AP 인증서를 발급한 CA까지의 모든 인증서를 저장하고 있어야 한다.

③ 인증서버

- 인증서버 인증서 : CA로부터 발급 받은 인증서버 인증서를 저장하고 있어야 한다.
- CA IP 주소, 디렉토리 IP 주소 : CA 및 저장소 IP 주소는 미리 설정되어 있어야 한다.
- 인증체인 : 인증서를 발급한 CA가 최상위 CA (Root CA)가 아닌 경우에는 최상위 CA로부터 인증서버 인증서를 발급한 CA까지의 모든 인증서를 저장하고 있어야 한다.

이 때 인증서를 발급하는 CA는 반드시 동일한 CA일 필요는 없지만, 본 논문에서는 모두 동일한 최상위 CA에서 클라이언트, AP, 인증서버 인증서를 발행하여 사용하였다.

제안 메커니즘이 동작하는 전체 시스템 환경은 (그림 9)와 같다.



(그림 9) 시스템 구성

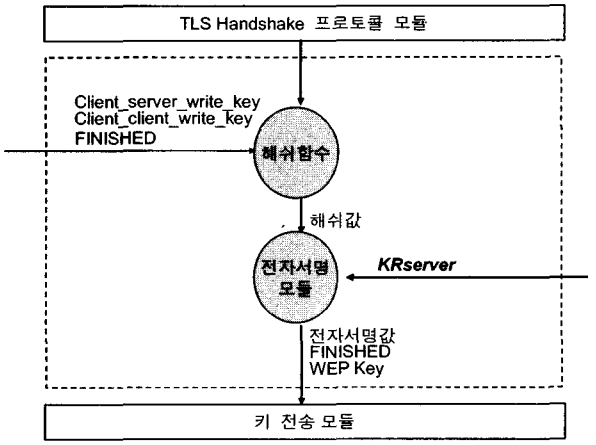
클라이언트는 AP를 통해서 인터넷(유선랜)을 이용하려는 사용자이다. AP는 클라이언트의 인터넷 접속을 중개하는 역할을 한다. 인증서버는 클라이언트와 AP에 대한 인증을 수행하여 정상적인 사용자만이 인터넷을 사용할 수 있도록 한다.

앞에서 설명한 바와 같이 클라이언트와 AP, 인증서버는 각각 CA에게 인증서 발급요청을 수행하여 인증서를 발급받아야 한다. 이 때, AP와 인증서버는 유선상에 위치하기 때문에 인증서 발급에 어려움이 없으나, 클라이언트는 무선상에 위치하기 때문에 인증서 발급에 어려움이 있다. 이를 유선상에서 사용자에게 발급된 인증서를 그대로 무선환경에서 사용한다는 가정을 하였다. 제안 시스템은 기존의 사용자 인증 메커니즘과 달리 디바이스 인증이 아닌 사용자 인증이기 때문에 이와 같은 가정이 가능하다.

4.1.2 인증서버 시스템

인증서버 시스템은 오픈소스로 공개된 Free RADIUS 서버를 수정하여 사용하였다[12]. 현재 RADIUS 서버는 TLS 및 EAP-TLS를 모두 지원하고 있다. 구현 시스템에서는 제안 메커니즘을 처리하기 위한 인증 모듈을 추가하였다.

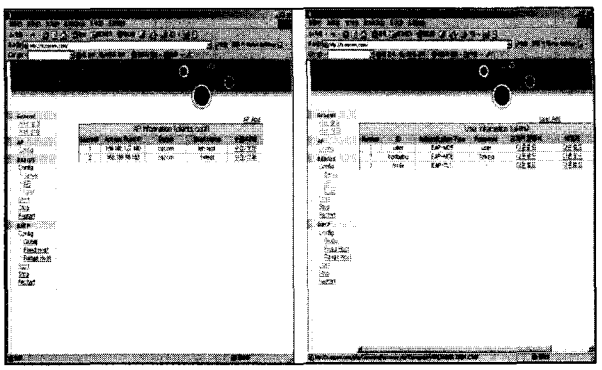
또한 키 전달 모듈의 구조는 (그림 10)과 같이 해쉬함수와 전자서명 모듈로 구성된다. (그림 10)에서 이탤릭체로 표현된 것은 해쉬함수 및 전자서명 연산을 수행하는데 키로 사용되는 파라미터이다. 해쉬함수는 WEP 키 및 FINISHED 메시지의 해쉬값이며, 계산된 해쉬값에는 인증서버의 개인키를 이용해서 인증서버의 전자서명이 첨부된다. 생성된 전자서명값과 FINISHED 메시지, AP의 공개키로 암호화되어 AP에게 전달된다.



(그림 10) 키 전달 모듈

(그림 11)은 인증서버의 관리 페이지이다.

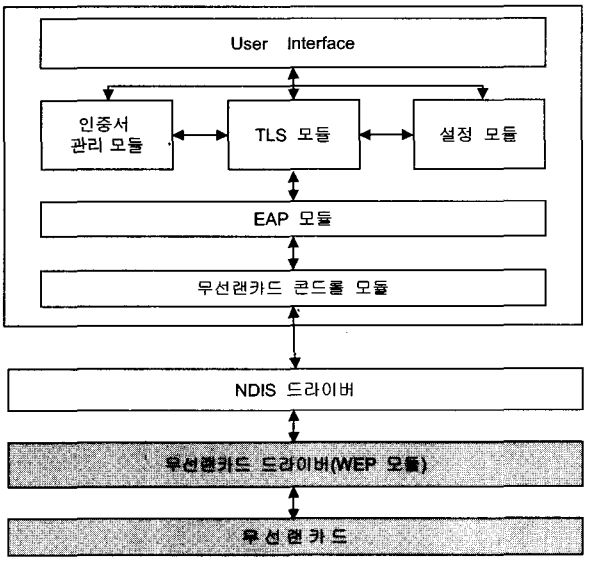
구현된 인증서버는 RADIUS 서버의 기능뿐만 아니라 클라이언트에게 동적으로 IP 주소를 할당하는 DHCP의 기능까지 함께 제공한다. 인증서버는 제안 사용자 인증 메커니즘 뿐만 아니라 기존의 IEEE802.1x의 메커니즘인 EAP-MD5 및 EAP-TLS의 기능도 함께 제공한다.



(그림 11) 인증서버 관리 페이지

4.1.3 클라이언트 모듈

클라이언트 모듈의 구조는 (그림 12)와 같다



(그림 12) 클라이언트 모듈

NDIS 드라이버는 운영체제(Windows)에서 제공하는 것이며, 무선랜카드 드라이버는 무선랜카드 제조업체에서 제공하는 모듈이다. WEP 암호화는 무선랜카드 드라이버에 포함되어 있다.

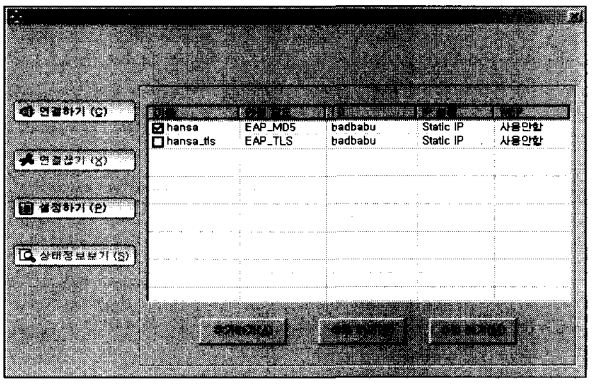
클라이언트 모듈은 크게 사용자 인터페이스와 TLS 모듈, EAP 모듈, 무선랜카드 관리 모듈로 구성된다.

TLS 모듈은 EAP-TLS를 수행한다. 즉, TLS 핸드쉐이크를 통한 인증이 TLS 모듈에서 이루어진다. EAP 모듈은 TLS 모듈에서 생성한 데이터를 EAP 패킷으로 캡슐화하는 부분이며, 무선랜카드 관리 모듈은 NDIS와의 인터페이스를 담당한다.

또한 설정 모듈을 통해 WEP의 사용 여부를 결정할 수 있으며, 암호통신의 모드를 선택할 수 있다. 암호모드 1과

암호모드 2의 경우에는 TLS 모듈에서 WEP 키를 NDIS로 넘겨주며, 암호모드 2의 경우에는 무선랜카드 드라이버 내에 저장되어 있는 WEP 키를 그대로 사용한다. 그리고 인증서 관리 모듈은 사용자 인증서, AP 인증서, CA 및 인증서버의 인증서를 저장/검증 및 관리하는 역할을 한다.

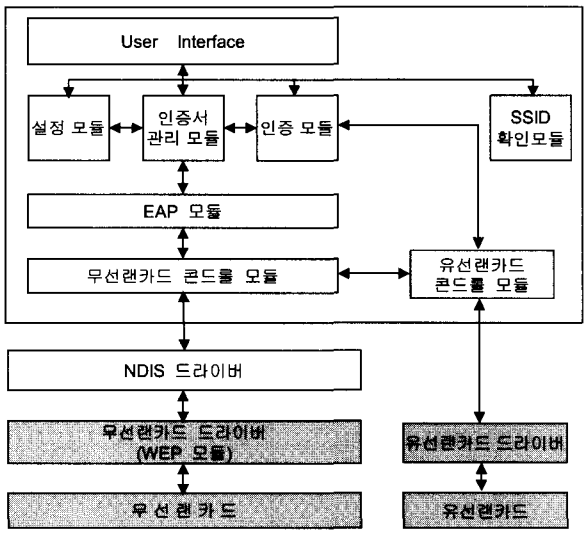
(그림 13)은 클라이언트 프로그램이다.



(그림 13) 클라이언트 프로그램

4.1.4 AP 모듈

AP 모듈의 구조는 (그림 14)와 같다.



(그림 14) AP 모듈

AP에는 무선랜카드와 유선랜카드를 각각 1개씩 필요로 한다. 무선랜카드는 클라이언트와의 통신을 담당하며, 유선랜카드는 인증서버를 비롯한 유선랜과의 통신을 담당한다.

SSID 확인 모듈은 제안 메커니즘에 의한 인증에 앞서 클라이언트의 SSID를 확인하는 부분이다. 설정모듈, 인증서 관리 모듈, TLS 모듈, EAP 모듈, 무선랜카드 콘트롤 모듈은 클라이언트 모듈에서의 해당 모듈들이 수행하는 역할과 동일한 역할을 한다. 다만 무선랜카드 콘트롤 모듈은 클라이언트에서 수신한 데이터를 유선랜카드 콘트롤 모듈로 넘겨준다. 유선랜카드 콘트롤 모듈은 유선랜카드 드라이버를 제어하여 유선랜과의 통신을 수행한다. 유선랜으로부터 수신한 데이터는 무선랜카드 콘트롤 모듈로 전송된다.

4.2 제안 시스템의 안전성 분석

본 절에서는 본 논문에서 제안한 무선랜 보안 시스템을 분석한다. 먼저 앞서 2장에서 살펴본 IEEE802.1x의 취약성에 대한 본 논문의 사용자 인증 메커니즘의 대응 방안에 대해서 분석한다. 다음으로 본 논문의 사용자 인증 메커니즘을 구성하고 있는 각각의 구성요소로 위장 공격이 수행될 경우, 이에 대한 대응 방안에 대해서 분석한다. 그리고 마지막으로 제안 무선랜 보안 시스템의 암호통신의 안전성에 대해서 분석한다.

4.2.1 EAP 메시지 스푸핑 공격

2장에서 살펴본 EAP 메시지 스푸핑 공격은 EAP Success 메시지에 대한 보호가 이루어지지 않기 때문에 가능하다. 그러나 본 논문에서 제안한 무선랜 보안 시스템에서 AP가 클라이언트에게 전송하는 EAP Success 메시지는 다음과 같이 구성된다.

$$EK_{WEP\_Key}[EKR_{server}[H(FINISHED + WEP\_Key)] \,||\, FINISHED \,||\, WEP\_Key \,||\, SUCCESS]$$

이 메시지에서 암호화에 사용된 WEP 키는 인증서버와 클라이언트의 EAP_TLS를 통한 인증과정에서 생성된 것이다. 즉, 클라이언트는 이미 WEP 키를 소지하고 있으며, AP에게는 인증서버가 전송해준다. 따라서 AP가 인증서버와의 인증에 실패하였다면, 클라이언트와 인증서버가 공유하고 있는 키인 WEP 키를 알아낼 수 없어 이 메시지를 생성하지 못한다.

2장에서 살펴본 EAP 메시지 스푸핑 공격에서 공격자는 AP로 위장하여 위장된 EAP SUCCESS 메시지를 생성하여 클라이언트와의 통신에 성공하였는데, 제안된 메커니즘에서는 EAP SUCCESS 메시지 생성 자체가 불가능하기 때문에 제안 메커니즘은 EAP 메시지 스푸핑 공격으로부터 안전하다.

그러나 제안 메커니즘의 암호통신 모드 2의 경우에는 WEP 키를 새롭게 공유된 키로 설정하지 않고 AP와 클라이언트에 미리 설정된 WEP 키를 그대로 사용하기 때문에 WEP 키가 노출 및 유출될 위험이 다른 2가지 방식에 비해 크다. WEP 키가 노출 또는 유출되거나 공격자가 WEP 키 크랙에 성공한 경우, 공격자는 노출 또는 유출된 WEP 키를 이용해서 EAP SUCCESS 메시지를 재구성할 수 있기 때문에 AP로 위장한 뒤 EAP 메시지 스푸핑 공격을 시도할 수 있다. 즉 EAP SUCCESS 메시지의 내용 가운데 FINISHED는 도청이 가능한 정보이고, WEP 키는 공격자

가 알아낸 정보이며, SUCCESS는 쉽게 생성이 가능한 정보이다. 그러나 이 경우에도 EKRserver[H(FINISHED + WEP_Key)]는 인증서버의 개인키를 모르면 생성할 수 없는 정보이다. 즉, AP는 인증서버의 전자서명을 생성할 수 없기 때문에 공격자가 정당한 AP로 위장하는 것은 불가능하다.

4.2.2 Disassociate 메시지 스푸핑

Disassociate 메시지 스푸핑 공격은 공격자가클라이언트에 대해서는 AP로 AP에 대해서는 클라이언트로 위장이 가능하기 때문에 일어날 수 있는 공격이다.

이 공격은 클라이언트와 AP가 암호통신을 수행함으로써 차단이 가능하다. 즉, 인증에 실패하여 인증서버와 클라이언트 사이에 공유되는 키를 얻지 못한 AP는 암호화된 Disassociate 메시지를 생성할 수 없다.

4.2.3 클라이언트 위장

공격자가 클라이언트로 위장하는 경우이다. 이는 EAP-TLS에 의해 인증서버와의 인증을 수행하고, 인증이 완료되면 인증서버가 AP에게 인증 성공을 알리는 메시지를 보내기 때문에 불가능하다. TLS의 사용자 인증 메커니즘은 안전하다고 할 수 있다[14].

4.2.4 AP 위장

AP는 인증서버와 인증서 기반의 상호인증을 수행한다. 이 때, AP 인증에 실패하게 되면 인증서버가 성공 메시지를 전송하지 않기 때문에 통신은 성립되지 않는다.

클라이언트는 직접적으로 AP를 인증하지는 않는다. 하지만 인증서버가 AP 인증에 성공해야만 클라이언트와의 인증을 수행하기 때문에 클라이언트는 인증서버로부터 인증 요청을 받았다면 AP는 신뢰할 수 있는 AP로 간주할 수 있다.

4.2.5 인증서버 위장

인증서버는 AP와 인증서 기반의 상호인증을 수행하고, 클라이언트와는 TLS를 이용해서 상호인증을 수행하기 때문에, 제 3자가 인증서버로 위장하는 것은 불가능하다.

4.2.6 암호통신

사용자 인증이 완료된 후의 암호통신의 안전성은 동적인 키 교환이 이루어지는지와 연관된다. SSID, MAC 주소 필터링, WEP 등은 사용자 인증과정에 키 교환이 포함되어 있지 않기 때문에, 고정된 하나의 키를 장기간 사용할 수밖에 없어 암호통신의 보안성이 떨어진다. 또한 IEEE802.11b에서는 키 분배나 관련된 어떤한 기술도 제시하고 있지 않다.

제안 시스템은 클라이언트와 인증 서버간의 인증 과정에서 세션키를 생성한 후, 이를 WEP 암호통신의 암호키로 이용한다. 따라서 클라이언트와 인증 서버가 인증을 수행할 때마다 새로운 키가 생성되기 때문에 WEP 암호통신의 보안성을 강화시킨다.

4.3 기존 시스템과의 비교/분석

지금까지 살펴본 제안 메커니즘과 기존 메커니즘의 비교/분석 결과를 요약하여 살펴보면 <표 2>와 같다.

〈표 2〉 제안 메커니즘과 기존 기술의 비교

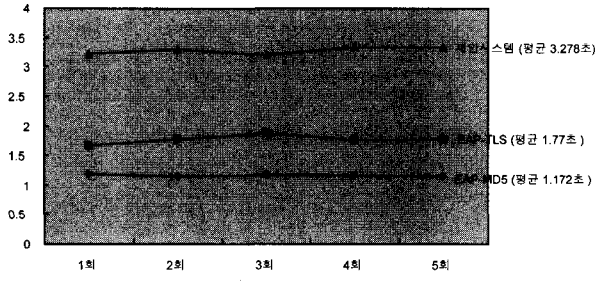
항 목	IEEE802.11b (SSID, MAC 주소 필터링, WEP)	IEEE802.1x (EAP-MD5, EAP-TLS, EPA-Keberos)	LEAP/ PEAP	제안 메커니즘
클라이언트 위장	위장 가능	위장 불가능	위장 불가능	위장 불가능
AP 위장	위장 가능	위장 가능	위장 가능	위장 불가능
인증서버위장	해당사항 없음	위장 불가능	위장 불가능	위장 불가능
인증 메커니즘의 안전성	매우 취약	안 전	안전(PEAP), 취약(LEAP)	안 전
암호통신의 안전성	키 교환 없음	키 교환 제공 가능	키 교환 제공 가능	키 교환 제공 가능
인증주체	디바이스	사 용 자	사용자	사용자
802.11b와의 호환성	해당사항 없음	AP 수정 필요, 인증서버 추가 설치	AP 수정 필요, 인증서버 추가 설치	AP 수정 필요, 인증서버 추가 설치
확 장 성	낮 음	매우 낮음	매우 낮음	높 음
소 요 시 간	적 음	보 통	결과 없음	많 음

<표 2>와 4.2에서 기술한 바와 같이 제안 시스템은 클라이언트, AP, 인증서버로의 위장이 불가능한 매우 안전한 사용자 인증 메커니즘을 제공하며, 사용자 인증 과정을 통해 WEP 키 교환이 가능하다. 즉, 제안 시스템에서는 무선랜 통신에 참여하는 어떤 구성요소로도 위장이 불가능하여 기존 무선랜 시스템에서 가능한 도청에 의한 사용자 위장이나, 키 스트림 재사용 공격, 메시지 스푸핑 등이 불가능하다. 또한 디바이스 인증이 아닌 실질적인 사용자 인증이 이루어지기 때문에 무선 단말기를 도난당하는 경우에도 안전하다. 그리고 기존의 무선랜 시스템에서는 암호화에 사용되는 키를 장기간 사용함으로서 취약점이 제기되었으나, 제안 시스템에서는 통신이 이루어질 때마다 새로운 키를 생성해서 암호화에 사용하기 때

문에 이러한 문제도 해결되었다. 이와 함께 전송 방향에 따라 각기 다른 키를 사용하도록 하여 안전성을 향상시켰다.

이와 같이 제안 시스템은 기존 시스템에 비해서 안전성이 향상되었을 뿐만 아니라 무선 네트워크의 확장에 있어서도 장점을 갖고 있다. 즉, SSID, MAC 주소 필터링의 경우에는 무선 네트워크의 확장이 필요한 경우에는 추가적인 AP를 설치하고, AP에서 SSID나 MAC 주소를 설정해야하며, WEP의 경우에도 AP를 추가한 뒤에 SSID 및 WEP 키를 설정하는 과정이 필요하기 때문에 많은 수의 무선랜 사용자가 추가될 경우에 어려움이 많다. 또한 EAP-MD5, EAP-Kerberos, LEAP, PEAP와 같은 메커니즘은 기본적으로 사용자의 ID/Password를 필요로 하기 때문에 사용자 등록과정 또한 필요하다. 따라서 이와 같은 기존의 기술들은 AP와 사용자의 추가 또는 제거가 자주 발생하는 대규모 무선 네트워크 서비스에는 적합하지 않다고 할 수 있다. 즉, 사용자나 AP의 추가 또는 제거가 일어날 때마다 인증서버에서 이러한 정보를 관리하는 것은 많은 비용 및 시간을 필요로 한다. 이에 비해 제안 시스템은 인증서 기반의 사용자 인증을 제공하기 때문에 사용자 패스워드의 보관이 필요없으며, 인증서가 설치된 AP를 추가만 하면 쉽게 무선 네트워크의 확장이 이루어진다.

그러나 제안 시스템은 관용 암호기술에 비해 많은 연산 시간을 필요로 하는 공개키 암호기술을 기반으로 하기 때문에 유선랜 연결에 앞선 사용자 인증에 비교적 많은 시간이 소요된다((그림 15) 참조). 이와 관련하여 RSA나 DSA가 아닌 ECC와 같은 공개키 암호기술을 적용할 경우에는 인증에 소요되는 시간을 좀 더 줄일 수 있다.



(그림 15) 제안 시스템과 기존 시스템의 인증 소요 시간 비교

5. 결 론

무선랜 사용자가 증가하고 있음에도 불구하고 현재 무선랜 표준인 IEEE802.11b는 실질적으로는 사용자 인증이 아닌 디바이스 인증을 제공하며, 디바이스 인증에도 많은 취약성이 존재하고 있다. 이에 대한 보완인 IEEE802.1x 역시 AP에 대한 인증을 수행하지 않는 등 강력한 사용자 인증을 제공한다고 할 수 없다. 또한 기밀성 및 무결성 제공을 위한 WEP에서도 여러 가지 취약성이 지적되고 있다.

이에 따라 본 논문에서는 무선랜 환경에 적합한 안전한 무선랜 통신 시스템을 제안하였다. 이는 무선랜의 구성요소인 클라이언트, AP, 인증서버에 대한 사용자 인증을 모두 수행한다. 즉, AP와 인증서버 간의 상호인증 과정을 추가하고, 인증 성공 메시지를 수정하여 클라이언트와 AP, 인증서버 간의 인증이 가능하도록 하였다. 또한 안전한 사용자 인증 메커니즘으로 알려진 TLS를 이용하여 사용자 인증의 강도를 향상시켰다. 그리고 키의 동적인 분배를 통해 암호통신의 안전성 역시 향상시켰다.

그러나 AP가 반드시 인증서를 소지해야 하는 점, PKI 운영에 있어서 인증서 및 인증서폐지목록 검증 등에 대해서는 향후 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] James T. Geier, Jim Geier, "Wireless LANs (2nd Edition)," SAMS, 2001.

[4] 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, July, 2001.

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

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

[7] B. Aboba, D. Simon, 'PPP EAP TLS Authentication Protocol,' IETF RFC2716, Oct., 1999.

[8] Arunesh Mishra, William A. Arbaugh, 'An Initial Security Analysis of the IEEE 802.1X Standard,' Feb., 2002.

[9] S. Fluhrer, I. Martin, A. Shamir, "Weaknesses in the key scheduling algorithm of rc4," *Eighth Annual Workshop on Selected Areas in Cryptography*, Aug., 2001.

[10] Core SDI, "crc32 compensation attack against ssh-1.5 http://www.core-sdi-com/soft/ssh/attacke.txt", 1995.

[11] Arunesh Mishra, Nick L. Petroni, Jr, Bryan D. Payne, "Open Source Implementation of 802.1x," http://www.open1x.org, 2003.

[12] The Free RADIUS Project, http://www.freeradius.org, 2002.

[13] John Viega, Matt Messier, Pravir Chandra, "Network Security with OpenSSL," O"reilly, 2002.

[14] D. Wagner and B. Schneier, "Analysis of the SSL 3.0 protocol," Proceddings of the 2nd USENIX Workshop on Electronic Commerce(EC-96), Nov., 1996.

이 종 후

e-mail : jjongfu@cqcom.com
1997년 충남대학교 컴퓨터과학과(학사)
1999년 충남대학교 대학원 컴퓨터과학과 (이학석사)
2004년 충남대학교 대학원 컴퓨터과학과 (이학박사)
1997년~현재 (주) 시큐컴 대표이사
관심분야 : 네트워크 보안, IC카드, 지불시스템

이 명 선

e-mail : mslee@kisti.re.kr
1982년 아주대학교 전자공학과(학사)
1996년 한남대학교 대학원 컴퓨터공학과 (공학석사)
1983년~현재 한국과학기술정보연구원 슈퍼컴퓨팅센터 책임연구원
2001년~현재 한남대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 컴퓨터시스템, 네트워크, 정보통신보안

류 재 철

e-mail : jcryou@home.cnu.ac.kr
1985년 한양대학교 산업공학과(학사)
1988년 Iowa State Univ.(전산학 석사)
1990년 Northwestern Univ.(전산학 박사)
1991년~현재 충남대학교 정보통신공학부 교수
2003년~현재 충남대학교 인터넷 침해대응기술연구센터장
관심분야 : 인터넷 보안