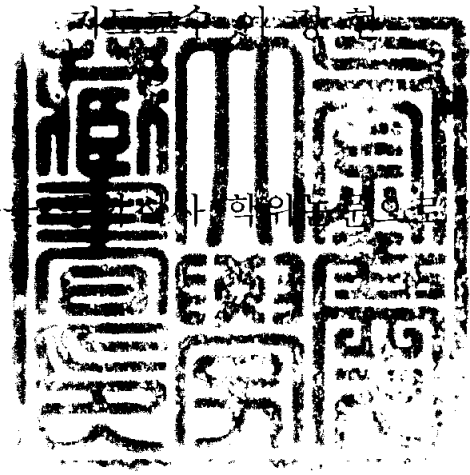
공학석사 학위논문

802.11 보안 서비스를 위한 새로운 키 관리 구조

지도교수 안 광 현



이 논문을 공학석사 학위논문으로 제출함

2004년 2월

부경대학교 대학원

정보보호학과

장 성 렬

장성렬의 공학석사 학위논문을 인준함

2003년 12월 26일

주 심 공학박사 김 창 수 

위 원 공학박사 정 연 호 

위 원 이학박사 이 경 현 

<제목차례>

<표차례>

<그림차례>

New Key Management Structure for 802.11 Security Service

Sung-Ryul Chang

Dept. of Information Security, Graduate School.
Pukyong National University

Abstract

The IEEE 802.11 WLANs(Wireless Local Area Networks) are fast growing due to the advantages of mobility, flexibility, extension and efficiency. The 802.11 standard includes the WEP(Wired Equivalent Privacy) protocol to provide security services for WLANs such as confidentiality, integrity and user authentication to link-layer communications. However the WEP has not been known to provide any avaliable security services.

So the IEEE 802.1X Task Group and the IEEE 802.11i Task Group proposed methods to improve the drawbacks of the WEP. One of the methods is to use the EAP-TLS which provides strong mutual authentication for establishing the RSN(Robust Security Network). But the EAP-TLS is attacked Man-in-the-Middle Attack and Session Hijacking successfully by using the tool being developed as a part of the ***Open1x***.

This paper proposes a new key management structure for the IEEE 802.11 security services on single ESS(Extended Service Set). This key management structure presents the IEEE 802.11 security services, which has not been provided by the WEP and solves the problems, such as Man-in-the-Middle Attack and Session Hijacking on the IEEE 802.1X and the IEEE 802.11i.

1. 서론

서비스가 지원되는 지역 내에서 위치에 상관없이 어디서든 접속할 수 있는 무선 통신 기술의 발전과 함께 컴퓨터 환경에서도 무선 네트워크를 이용하여 유선 환경과 동일한 서비스(Service)를 제공하고자하는 것이 무선랜(WLAN: Wireless Local Area Network)이 등장하게 된 배경이다. 국내에서도 여러 통신 서비스 사업자들이 공중 무선랜(Public WLAN) 서비스를 전개해 나가고 있어 무선랜에 대한 인지도와 무선랜의 사용이 늘어나고 있다. 무선랜 기술이 갖는 장점을 살펴보면 다음과 같다.

- 이동성(Mobility) : 무선 사용자는 기본 스테이션(Station)이 서비스 범위 내에만 있다면, 자유롭게 이동하면서 네트워크에 접속, 이용할 수 있다.

- 유연성(Flexibility) : 네트워크 사용이 어려운 장소에서도 액세스 포인트(Access Point)가 구축되었다면 네트워크의 사용이 가능하다.

- 확장성(Extension) : 여러 개의 액세스 포인트만 설치한다면 새로운 공사를 하지 않고 서비스 범위(Range)를 쉽게 확장할 수 있다.

- 효율성(Efficiency) : 무선랜 제품의 가격 하락에 의해 네트워크 구축에 필요한 비용과 시간이 적게 소요된다.

이러한 무선랜의 많은 장점에도 불구하고, 안전한 무선랜 사용을 보장할 만한 무선랜 보안 솔루션(Solution)은 상대적으로 취약하다. 무선랜은 무선 매체(Wireless Medium)를 사용한다는 특성상 일정한 장비만 갖춰지면, 언제든 도청(Eavesdropping)이 가능하다. 그래서 무선랜 환경을 위한 기본적인

보안 서비스를 크게 세 가지 측면에서 지적할 수 있다. 첫 번째는 승인된 사용자에게만 네트워크 접속을 허용하는 인증(Authentication)에 관한 보안이며, 두 번째는 스니퍼(sniffer)등을 이용해 무선랜을 통해서 전송되는 데이터에 대한 도청 행위를 방어할 수 있는 데이터 기밀성(Confidentiality)에 관한 보안이다. 마지막으로 데이터가 악의적인 스테이션에 의해 훼손되지 않았음을 보장하는 무결성(Integrity)에 관한 보안이다.

IEEE 802.11[1] 무선랜 표준 중 IEEE 802.11b[2]는 무선 구간의 보안을 위해 WEP(Wired Equivalent Privacy)을 사용하고 있으나, 24 비트의 짧은 초기화 벡터(IV : Initialization Vector)에 의한 키 스트림(Stream)의 단순성으로 인한 도청과 실시간 공격으로 평문 노출과 DOS(Denial Of Service) 공격의 가능성, 동적인 WEP 키 분배의 부재와 같은 보안상 취약점으로 위에서 지적한 세 가지 보안 서비스를 하나도 만족시키지 못하고 있다.

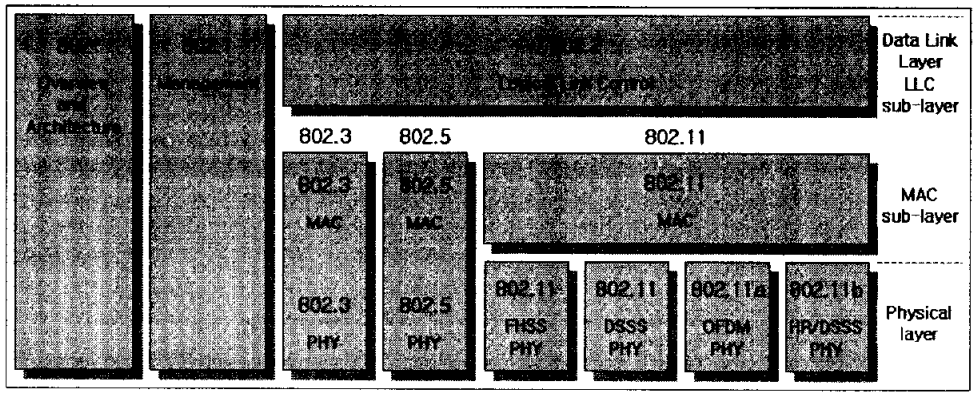
현재 가장 많이 상용화된 장비인 IEEE 802.11b의 알려진 취약성을 보완하기 위한 방안으로 IEEE 802.1X[3]에서는 포트(Port) 기반의 인증을 제안하고 있고, IEEE 802.11i[4]에서는 데이터 기밀성과 무결성을 보완하기 위해 AES(Advanced Encryption Standard) 기반의 CCM 프로토콜(Counter mode with CBC-MAC Protocol)을 제공하여, 무선랜에서의 보안 수준을 강화하는 표준화 작업을 진행 중이다.

무선랜의 사용이 급격히 증가하고 있으나, 아직까지 대부분의 무선랜은 유선 네트워크(Wired Network) 커버리지(Coverage)를 보완하기 위한 작은 규모의 네트워크에 많이 쓰이고 있으며, 기존의 802.11b를 보안하기 위한 기술인 IEEE 802.1X도 보안상 취약점이 발견되었고, IEEE 802.11i이 아직 표준화 단계에 있기 때문에 현재 무선랜 서비스를 제공하고 있는 벤더(Vendor)들도 IEEE 802.11i를 IEEE 802.11 보안 서비스에 접목시키지 못하고 있다.

본 논문은 이러한 무선랜의 사용 현황을 고려하여 단일 확장 서비스 셋과 같은 작은 규모의 무선랜을 사용하는 사용자들에게 기존의 IEEE 802.11 무선랜 보안이 제공하지 못하는 보안 서비스(기밀성, 무결성, 인증)와 IEEE 802.1X, IEEE 802.11i의 보안상 문제점을 개선하기 위한 방안을 키 컨트롤러(Key Controller)를 통한 새로운 키 관리 구조를 이용하여 제공하려고 한다.

2. 802.11 무선랜 개요

802.11은 근거리 네트워크(Local Area Network) 기술 표준인 IEEE 802 계열의 한 구성원이다.[5] 802.11은 아래 [그림 1]과 같이 기존의 유선랜에 기반한 표준들과는 다른 MAC(Medium Access Control) Layer와 Physical Layer를 사용한다.



[그림 1] IEEE 802 계열과 OSI 모델과의 관계

최초의 802.11 스펙(Spec)에는 802.11 MAC과 두 개의 물리 계층인 주파수 도약 확산 스펙트럼(FHSS : Frequency Hopping Spread Spectrum)과 직접 시퀀스 확산 스펙트럼(DSSS : Direct Sequency Spread Spectrum)으로 이루어져 있었다. 이후 802.11을 개정하면서 새로운 물리 계층인 고속 직접 시퀀스 계층(HR/DSSS : High Rate DSSS)이 추가되었다. 현재 시장에는 물리 계층으로 HR/DSSS를 사용하는 802.11b에 기반한 제품이 주류를 이루고 있으며, 2002년 초반부터 직교 주파수 분할 다중화(OFDM : Orthogonal Frequency Division Multiplexing)에 기반한 802.11a 제품이 출시되고 있다. [표 1]은 802.11 RF(Radio Frequency) 표준 기술들을 비교한 것이다.

[표 1] 802.11 표준 비교

IEEE 표준	속도	주파수 대역	변조 방법	참고
802.11	1Mbps 2Mbps	2.4GHz	FHSS DSSS	첫 번째 표준 (1997)
802.11a	최대 54Mbps	5GHz	OFDM	두 번째 표준 (1999)
802.11b	5.5Mbps 11Mbps	2.4GHz	HR/DSSS	개정 후
802.11g	최대 54Mbps	2.4GHz	OFDM	표준화 작업 중

2.1. 802.11 무선랜 구성요소

802.11 네트워크는 다음과 같이 네 개의 물리적인 구성 요소로 구성되어 있으며, 이는 [그림 2]에 요약되어 있다.

- 분산 시스템(Distribution System)

액세스 포인트에 프레임(Frame)을 전달하는데 사용되는 802.11의 논리적인 구성 요소이다. 802.11은 분산 시스템을 위하여 어떤 특정한 기술로 한정하고 있지 않으며, 액세스 포인트와 연결된 백본 네트워크를 의미한다.

- 액세스 포인트(Access Point)

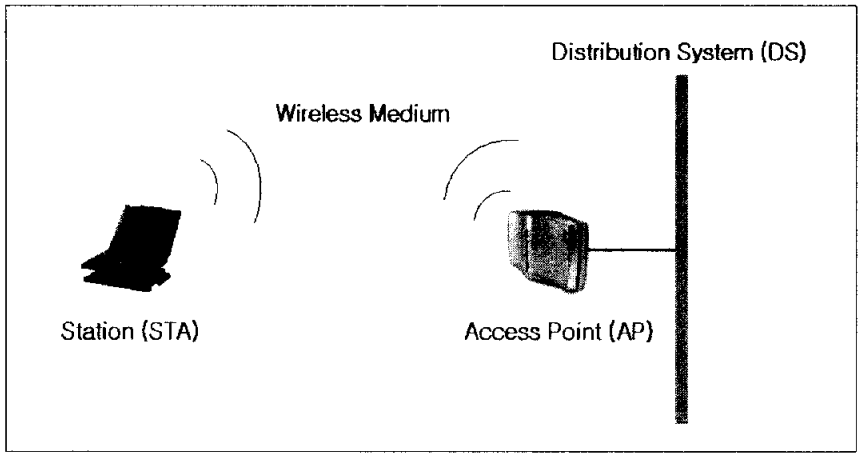
802.11 네트워크의 프레임을 다른 네트워크로의 전달을 위하여 다른 형태의 프레임으로 변환해주는 무선-유선 브리징(Bridging) 기능을 수행한다.

- 무선 매체(Wireless Medium)

한 스테이션에서 다른 스테이션으로 프레임을 전송하기 위하여 표준은 무선 매체를 사용하는데, 여기에는 여러 다른 물리 계층이 정의되어 있다.

● 스테이션(Station)

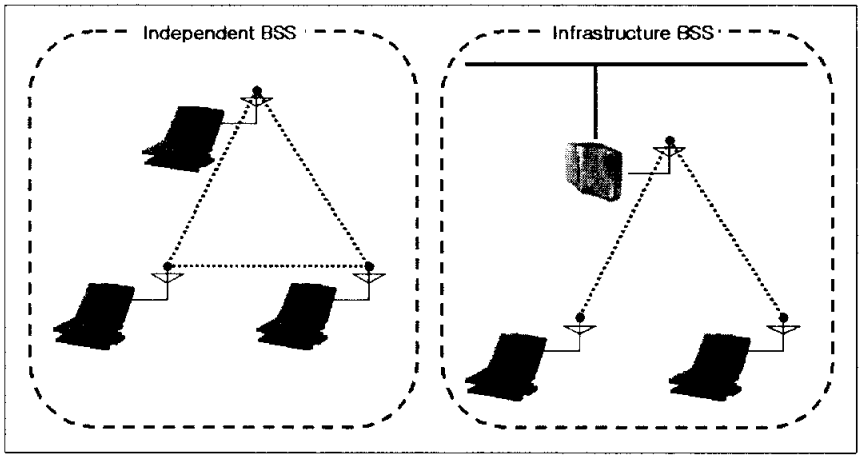
무선 네트워크는 스테이션끼리 데이터를 전송하기 위해 만들어졌다. 일반적으로 스테이션은 배터리에 의해서 동작하는 노트북(Notebook)이나 PDA(Personal Digital Assistant)를 의미하지만 반드시 휴대 가능한 기기에 한정된 것은 아니므로 무선랜 카드를 장착한 데스크탑(Desktop)도 스테이션이 될 수 있다.



[그림 2] 802.11 무선랜 구성요소

2.2. 802.11 무선 네트워크 유형

802.11 네트워크의 기본 구성 블록은 기본 서비스 셋(BSS : Basic Service Set)이다. 이는 서로 통신하는 스테이션의 그룹을 일컫는다. BSS는 [그림 3]과 같이 두 가지 구성을 가지며, [그림 4]와 같이 ESS로 확장 가능하다.



[그림 3] 독립 BSS와 인프라스트럭처 BSS

2.2.1. 독립 기본 서비스 셋

[그림 3]의 왼쪽 부분이 독립 기본 서비스 셋(IBSS : Independent Service Set)이다. IBSS에 있는 스테이션은 통신 영역 내에 있는 다른 기기와 직접 통신한다. 두 개의 스테이션만으로 구성된 IBSS는 가장 작은 802.11 네트워크를 구성한다. 일반적으로 IBSS는 특정한 목적을 가지고, 특정 기간동안 구성되는 몇 개의 스테이션들로 이루어지기 때문에 때때로 ad-hoc BSS 또는 ad-hoc 네트워크라고도 한다.

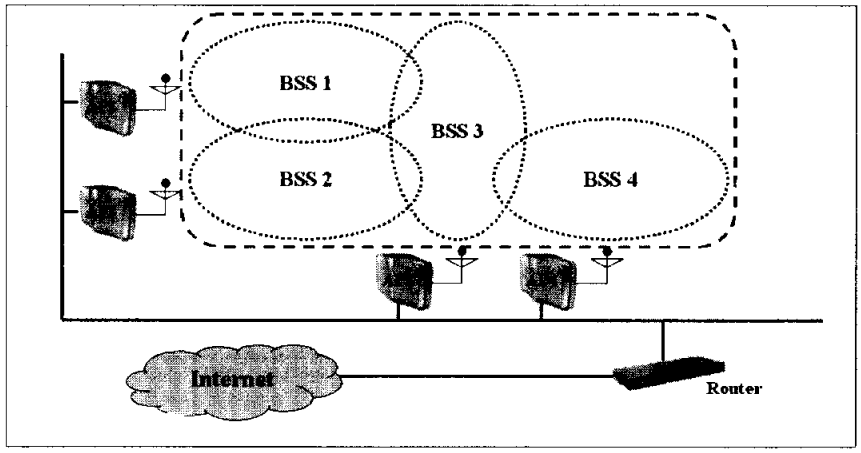
2.2.2. 인프라스트럭처 기본 서비스 셋

[그림 3]의 오른쪽 부분은 인프라스트럭처 기본 서비스 셋(Infrastructure BSS)을 보여주고 있다. 보통 무선랜은 인프라스트럭처 BSS를 가리키며, 편의상 BSS라고 한다. BSS는 액세스 포인트의 사용으로 IBSS와 구별될 수 있다. BSS 영역에서 스테이션의 통신을 포함한 모든 통신 과정에서는 액세

스 포인트가 사용된다. BSS에서 기본 서비스 영역은 액세스 포인트로부터 신호를 받을 수 있는 영역으로 정의된다.

2.2.3. 확장 서비스 셋

BSS는 조그만 사무실이나 가정에서도 커버리지를 구성할 수 있지만, 더 큰 영역에서의 커버리지는 제공할 수 없다. 그래서 802.11은 여러 BSS를 연결함으로써 구성되는 임의적인 규모의 무선 네트워크를 확장 서비스 셋(ESS : Extended Service Set)을 허용하고 있다. ESS는 백본 네트워크와 함께 BSS를 연결함으로써 이루어진다. [그림 3]의 ESS는 네 개의 BSS로 구성되어 있다.



[그림 4] 확장 서비스 셋

2.3. 802.11 무선 네트워크 동작

설계 초기부터 802.11은 상위 계층 프로토콜의 또 하나의 링크 계층이 되

도록 고안되었다. 그래서 802.11을 때때로 "무선 이더넷(Wireless Ethernet)" 이라고 부르기도 한다. 그래서 이더넷에 존재하는 핵심 요소는 802.11에도 존재한다. 스테이션은 48 비트 802.11 MAC Address로 인식되며, 개념적으로 프레임은 MAC Address에 기반하여 전달된다.[6]

2.3.1. 802.11 네트워크 서비스

802.11은 분산(Distribution), 통합(Integration), 결합(Association), 재결합(Reassociation), 결합 해제(Disassociation), 인증(Authentication), 인증 해제(Deauthentication), 프라이버시(Privacy), MAC 서비스 데이터 유닛(MSDU : MAC Service Data Unit) 전달이라는 아홉 가지의 네트워크 서비스를 제공한다. 참고로 아홉 가지 서비스 중 Privacy 서비스는 이번 802.11i에서 Confidentiality라는 용어로 개정되었다. 이후 본 논문에서는 Privacy라는 용어를 Confidentiality라는 용어로 대체하여 사용한다.

아래 [표 2]와 같이 서비스의 사용 주체에 따라 아홉 가지 서비스는 다시 네 개의 스테이션 서비스와 다섯 개의 분산 서비스로 나누어진다.

[표 2] 802.11 네트워크 서비스

서비스	스테이션 서비스 or 분산 서비스
분산(Distribution)	분산 서비스
통합(Integration)	분산 서비스
결합(Association)	분산 서비스
재결합(Reassociation)	분산 서비스
결합 해제(Disassociation)	분산 서비스
인증(Authentication)	스테이션 서비스
인증 해제(Deauthentication)	스테이션 서비스
Confidentiality	스테이션 서비스
MSDU 전달	스테이션 서비스

- 분산(Distribution)

분산 서비스는 인프라스트럭처 네트워크에 있는 스테이션이 데이터를 보낼 때마다 사용된다.

- 통합(Integration)

통합은 분산 시스템을 802.11이 아닌 네트워크에 접속하도록 한다.

- 결합(Association)

결합은 스테이션이 서비스를 받을 수 있는 상태를 의미하며, 결합되지 않은 스테이션은 케이블(Cable)이 접속되어 있지 않은 이더넷 개체(Entity)처럼 네트워크에 존재하지 않는다.

- 재결합(Reassociation)

재결합은 단일 확장 서비스 영역에 있는 기본 서비스 영역 사이를 스테이션이 움직이고 있을 때 신호의 강도를 측정하고, 신호 조건에서 다른 결합이 필요하다고 요구될 때, 스테이션에 의해 초기화된다.

- 결합 해제(Disassociation)

스테이션이 결합 해제 서비스를 불러내면, 분산 시스템에 저장되어 있는 이동 데이터는 삭제된다. 결합 해제란 접속하고 있던 스테이션이 더 이상 네트워크에 접속되어 있지 않다는 의미다.

- 인증(Authentication)

무선 네트워크는 원천적으로 유선에 대응하는 물리적인 보안을 제공할 수 없으므로, 네트워크에 접근하는 사용자는 접근 권한(Access Authorization)을 가지고 있음을 확인하는 추가적인 인증 루틴(Routine)이 필요하다. 인증은

인증 받은 사용자만이 네트워크를 사용할 수 있으므로 결합의 필요조건이다.

- 인증 해제(Deauthentication)

인증 해제는 인증 관계를 종료시킨다. 인증은 네트워크 사용 권한을 얻기 전에 필요하므로 인증 해제의 부효과는 현재 결합의 종료이다.

- Confidentiality

무선 네트워크로의 물리적인 접근은 속성상 정확한 안테나(Antenna)와 변조 방법을 이용하기만 하면 가능하다. 유사한 수준의 기밀성을 제공하기 위하여 802.11은 WEP이라고 부르는 기밀성 서비스를 제공한다. WEP의 목적은 802.11 매체를 이동하는 프레임을 암호화함으로써 유선 네트워크와 대략적으로 유사한 정도의 기밀성을 제공하는 데 있다.

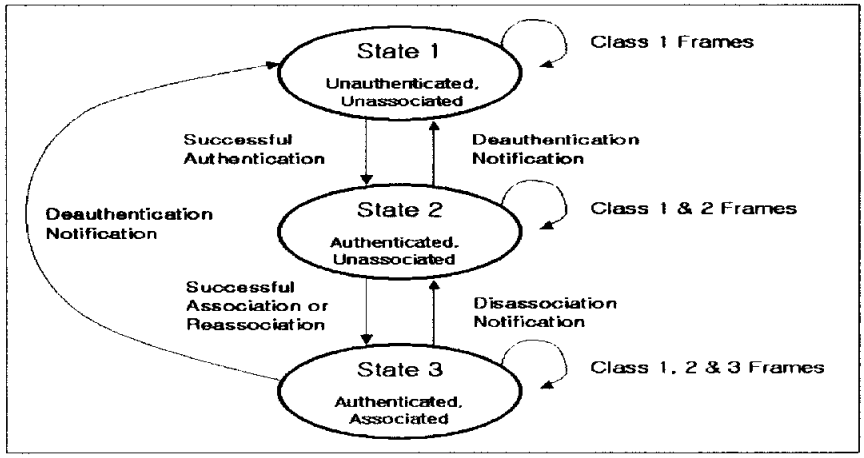
- MSDU 전달

스테이션은 MAC 서비스 데이터 유닛 전달 서비슬 제공하는데, 이는 실제 목적지로의 데이터 전달 책임을 지며, 하나의 MAC에서 다른 곳으로 데이터가 전송되었다는 것을 책임진다.

2.3.2. 802.11 상태 머신

802.11에서 허용되는 프레임 유형은 인증 및 결합 상태(State)에 따라 달라진다.[7] 스테이션은 인증(Authentication) / 비인증(Unauthentication), 결합(Association) / 비결합(Unassociation)의 상태가 될 수 있다. 이러한 두 값은 서로 연결되어 세 가지 허용되는 상태를 구성할 수 있으며, 다음과 같은 802.11 상태 단계를 구성한다. [그림 5]는 802.11에서 프레임 전송을 위한 전체 상태 머신이다.

- State 1 - Unauthenticated / Unassociated (초기 상태)
- State 2 - Authenticated / Unassociated
- State 3 - Authenticated / Associated



[그림 5] 802.11 상태 머신

3. 802.11 무선랜 보안

서론에서 잠깐 언급하였듯이 802.11 표준은 무선 환경에서의 안전한 운영을 제공하기 위해 몇 가지 보안 서비스를 정의하고 있다. 이 보안 서비스들은 주로 WEP 프로토콜에 의해 제공되는데, WEP의 가장 핵심적인 역할은 스테이션과 액세스 포인트간의 무선 전송 시 Link Layer의 데이터를 보호한다. 즉, WEP은 End to End(단 대 단) 보안을 제공하는 것이 아니라 연결 중 무선 부분에 대한 보안만을 제공한다.

802.11에서 정의한 무선랜 환경을 위한 세 가지 기본적인 보안 서비스는 인증, 기밀성, 무결성이다. 이 장에서는 WEP을 기반으로 한 보안 서비스와 그 취약점에 대해 살펴보고, 이를 개선하기 위한 표준화 단체의 방안에 대해 살펴보도록 한다.

3.1. 802.11 보안 서비스

무선랜은 물리적인 특성상 액세스 포인터의 주파수 범위 내에서는 수신 가능한 디바이스(Device)만 있으면 정당한 사용자이건 아니건 상관없이 무선상의 데이터에 접근할 수 있다. 이러한 취약성을 보안하기 위해 802.11에서는 WEP을 기반으로 데이터 기밀성, 데이터 무결성, 사용자 인증 서비스를 제공하고 있다.

3.1.1. WEP 프로토콜

WEP 프로토콜은 무선을 사용하는 네트워크 트래픽(Traffic)에 기밀성과 무결성을 제공하기 위해 설계(Design) 되었다. WEP은 무선 환경을 고려하여 대칭

알고리즘(Symmetric Algorithm)보다 약 10배 빠른 RC4 스트림 암호(Stream Cipher)를 사용하고 있다. WEP 프로토콜은 공유 비밀키(Shared Secret Key)를 사용하여 암호화・복호화를 수행한다. 암호화・복호화 과정은 아래와 같이 수행되며, [그림 6], [그림 7]은 각각 암호화 과정과 복호화 과정을 보여준다.

- WEP 암호화 과정

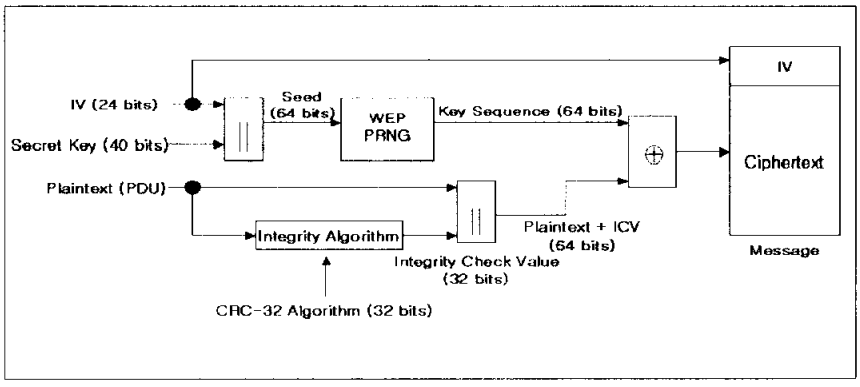
① 40 비트의 공유한 비밀키를 24 비트의 초기화 벡터(IV : Initialization Vector)와 연접하여 총 64 비트인 Seed를 생성한다.

② 이 Seed를 RC4 기반의 WEP PRNG(Pseudo Random Number Generator)를 이용하여 의사난수 키 시퀀스(Key Sequence)를 생성한다.

③ 데이터 무결성을 위해 평문에 무결성 알고리즘(Cyclic Redundancy Check-32 Checksum)을 사용하여 ICV(Integrity Check Value)를 생성하고, 이를 평문과 연접한다.

④ 평문과 ③에서 만들어진 ICV를 연접한 값에 ②에서 출력된 키 시퀀스를 XOR하여 암호문을 생성한다.

⑤ 암호문과 함께 4 바이트의 확장된 데이터를 추가하여 전송된다.



[그림 6] WEP 암호화 과정

● WEP 복호화 과정

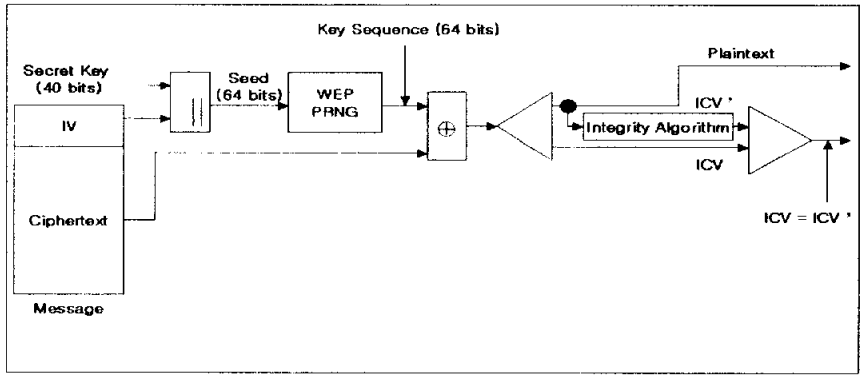
① 전송 받은 메시지에서 3 바이트의 초기화 벡터는 암호화와 마찬가지로 수신자의 RC4 비밀키와 연접하여 WEP PRNG에 입력할 Seed를 생성한다.

② WEP PRNG는 조합된 키와 초기화 벡터가 연접된 Seed를 이용하여 RC4 키 시퀀스를 생성한다.

③ 전송 받은 메시지에서 암호문을 ②에서 생성한 키 시퀀스와 XOR 연산을 수행한다.

④ 전송된 데이터의 무결성 검사를 위해, 생성된 평문을 암호화 시 사용하였던 CRC-32 Checksum 알고리즘을 사용하여 ICV'을 생성한다.

⑤ 메시지에 대한 무결성 체크는 ③에서 출력된 ICV와 ④에서 생성된 ICV'을 비교하여 수행할 수 있다.



[그림 7] WEP 복호화 과정

위의 암호화·복호화 과정에서는 40 비트의 비밀키(WEP 키)를 사용하고 있으나, 현재에는 WEP 프로토콜의 보안성을 강화하기 위해 104 비트, 128 비트의 비밀키를 지원하고 있다. 그래서 104 비트의 WEP 키의 경우 24 비트의 초기화 벡터를 포함해서 128 비트의 RC4 키가 된다.

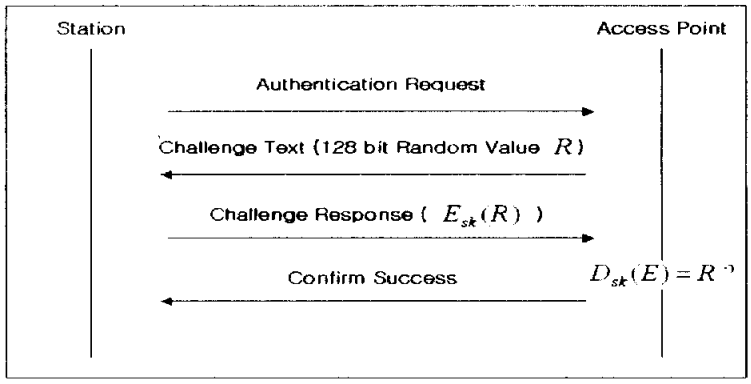
데이터의 무결성 검사는 WEP 암호화·복호화 과정 속에 CRC-32 Checksum 알고리즘을 이용하여 암호화·복호화와 함께 수행한다. [그림 6]에서처럼 전송되기 전에 각 페이로드(Payload)에 대해 CRC가 계산된다. 무결성이 부여된 패킷(Packet)은 RC4 키 스트림을 사용해서 암호화된다. 그리고 나서 [그림 7]에서처럼 수신측에서는 패킷을 복호화하고 수신된 메시지에 대해 CRC를 재계산한다. 재계산된 CRC는 전송 측에서 보낸 CRC와 비교되어서, 무결성의 손상 여부를 판단하게 된다. 무결성이 손상되었을 경우 그 패킷은 버려지게 된다. 결국 IEEE 802.11 표준에서는 WEP 프로토콜을 이용하여 트래픽에 대한 기밀성과 무결성을 같이 제공하고 있다.

3.1.2. 802.11 인증 메커니즘

IEEE 802.11 스펙은 유선 네트워크에 접근하려는 무선 사용자를 검증하기 위해 비 암호학적 접근 방법, 암호학적 접근 방법이라는 두 가지 방법을 정의하고 있다.

비 암호학적 접근 방법에는 단순히 SSID(Service Set ID)를 Empty String으로 해서 인증을 받는 Open System 인증 방법과 무선 네트워크의 실제 SSID를 전송하여 인증을 받는 Closed System 인증 방법이 있다.

암호학적 접근 방법인 공유키 방법은 인증을 위해 암호화 기술을 사용한다. 이것은 스테이션이 공유 비밀키를 알고 있는지에 기반한 Challenge-Response 메커니즘을 사용한다. 이 방법에서 액세스 포인트는 [그림 8]에서와 같이 128 비트 Challenge를 생성해서 스테이션에게 보낸다. 그러면 스테이션은 액세스 포인트와 공유하고 있는 비밀키(WEP 키)를 사용해서 Challenge를 암호화시키고, 그 결과를 액세스 포인트에게 보낸다. 액세스 포인트는 돌려 받은 값을 복호화해서 그 값이 처음에 전송한 Challenge와 같은 경우에만 접근을 허용한다.



[그림 8] 802.11 공유키 인증

3.2. 802.11 보안 서비스 취약점

802.11 보안 서비스는 대부분 WEP 프로토콜을 사용하여 제공한다. 그래서 WEP 프로토콜의 취약점이 802.11 보안 서비스 전체의 취약점이 된다. 이와 함께 WEP 키를 관리하는 메커니즘의 부재가 802.11 보안 서비스의 가장 큰 취약점이다. 802.11 보안 서비스와 관련된 몇 가지 문제점은 다음과 같다.

① RC4 알고리즘 취약점

스트림 암호의 보안은 전적으로 키 스트림의 랜덤성에 의존하므로, 키 스트림의 재사용은 스트림 암호 기반의 시스템에서 큰 약점이다. 만약 동일한 RC4 키 스트림으로 암호화되었다면, 두 암호화된 패킷의 XOR 연산은 두 평문 패킷의 XOR과 동일하다. 프레임 몸체의 구조와 함께 [표 3]과 같이 두 스트림의 차이를 분석함으로써 공격자는 평문 프레임 자체의 내용도 알 수 있다. 그래서 키 스트림의 재사용 방지를 돕기 위하여 WEP은 다른 RC4 키로 다른 패킷을 암호화할 수 있도록 초기화 벡터를 사용한다. 그러나 초기화 벡터는 패킷 헤더의 부분이므로 암호화되지 않으며, 도청자는 동일한 RC4

키로 암호화된 패킷에서 분리해 낼 수 있으므로 초기화 벡터도 알 수 있게 된다.[8]

[표 3] RC4 알고리즘 취약점

$$Cipher_1 \oplus Cipher_2$$
$$= \{ Plain_1 \oplus (IV, k) \} \oplus \{ Plain_2 \oplus (IV, k) \}$$
$$= Plain_1 \oplus Plain_2$$

② 초기화 벡터 취약점

WEP에서 초기화 벡터는 메시지 중 암호화되지 않고 전송되는 24 비트 필드(Field)이다. 이 24 비트 스트링은 RC4 알고리즘에 의해 생성되는 키 스트림을 초기화하는데 사용되는 것으로 암호 목적으로 사용되기에는 상대적으로 필드가 작다. 이와 같이 초기화 벡터 공간은 매우 작으므로, 분주한 네트워크에서는 재사용될 가능성이 매우 높다.

③ WEP 키 취약점

표준화된 WEP 구현은 40 비트의 공유 비밀키를 사용한다. 보안 전문가는 이러한 40 비트 비밀키 길이의 적합성에 의문을 제기하였고, 그래서 업계에서는 104 비트, 128 비트 WEP 키로 128 비트, 152 비트 RC4 키를 만들어 사용하고 있으나, 이런 긴 비트 키에 대한 표준은 만들어지지 않았다. 또한 잘 설계된 암호화 시스템은 더 긴 길이의 키를 사용하면 추가된 키 길이만큼 키를 해독해내는 시간이 늘어나는 추가적인 보안을 얻을 수 있으나, WEP 프로토콜은 잘 설계된 암호화 시스템이 아니므로, WEP 공격으로 잘 알려진 방법(AirSnort)을 사용하면 WEP 키의 길이에 상관없이 몇 초안에 비밀키를 찾아낼 수 있다.[9]

④ CRC-32 Checksum 알고리즘 취약점

WEP 프로토콜은 트래픽의 무결성을 위해 CRC-32 Checksum 알고리즘을 사용하고 있으나, 이 알고리즘은 암호학적으로 안전하지 않다. CRC-32 Checksum 알고리즘의 선형적인 성질을 이용하여, 공격자는 자신이 변조한 트래픽을 액세스 포인트가 아무런 의심 없이 받아들이게 할 수 있다. [표 4]은 이런 CRC-32 Checksum 알고리즘의 취약점을 보여주고 있다.

[표 4] CRC-32 Checksum 알고리즘 취약점

$Ciper = \{ Plain \oplus (IV, k)\} \Rightarrow \{< Message, c(Message) > \oplus (IV, k)$
$Ciper' = \{ Cipher \oplus (Delta, c(Delta)\}$
$(IV, k) \oplus < Message, c(Message) > \oplus < (Delta, c(Delta) >$
$(IV, k) \oplus < Message, Delta >, < c(Message, c(Delta) >$
$(IV, k) \oplus < Message', c(Message') >$
• *Cipher* : *Original Ciphertext* • *Cipher'* : *Modified Ciphertext by Attacker* • *linear temper* : $c(a \oplus b) = c(a) \oplus c(b)$

⑤ WEP 키를 사용한 인증 메커니즘 취약점

동일한 공유 비밀키인 WEP 키를 가지고 인증하는 것은 진정한 의미의 인증이라 볼 수 없다. 단방향 Challenge-Response 인증 메커니즘은 상호 인증을 지원하지 않아 스테이션은 액세스 포인트를 인증할 수 없어, 올바른 액세스 포인트와 통신을 하는지 확신할 수 없게 된다.[10]

⑥ 키 관리(Key Management) 메커니즘 부재

WEP은 키 분배에 아킬레스건(Achilles's Tendon)을 가지고 있다. WEP 키의 비밀 비트는 802.11 서비스 셋에 참여하는 모든 스테이션에 분배되어야

만 한다. 그러나 802.11은 키 분배 메커니즘에 대한 스펙을 정하고 있지 않다. WEP 키를 분배하는 문제뿐만 아니라, 한 번 설정한 키를 드물게 재설정하는 것 또한 공격자가 동일한 키 스트림으로 암호화된 많은 수의 프레임을 가지고 스트림을 조립할 수 있게 한다. 이러한 키의 설정, 분배, 갱신에 관한 키 관리 메커니즘의 부재가 전체적으로 802.11 보안 서비스를 취약하게 만든다.

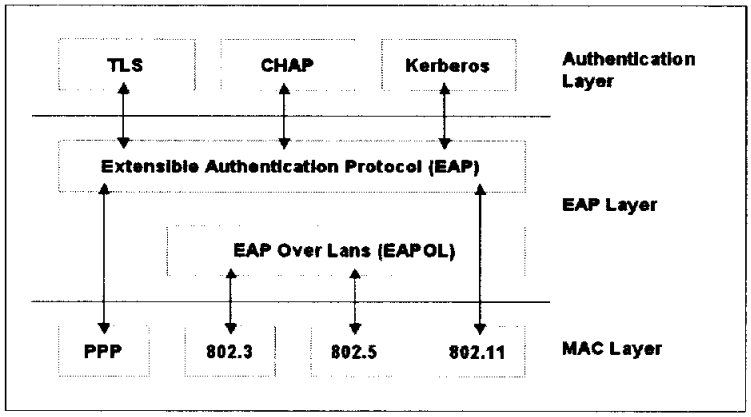
3.3. 802.11 보안 서비스 개선을 위한 표준화 기관의 연구

표준화 기관에서는 이런 802.11 무선랜의 보안과 관련하여 여러 Task Group을 만들어 기존 무선랜에서의 취약점을 개선하려는 연구를 진행중이다. 무선랜 보안요소 중 사용자 인증에 대한 표준화 활동을 펼치고 있는 곳은 IEEE 802.1X, IEEE 802.11i Task Group이고, 트래픽의 기밀성과 무결성에 대한 표준화 활동은 IEEE 802.11i Task Group에서 진행중이다.

3.3.1. 802.1X Task Group

IEEE 802.1X Task Group이 작성하여 2001년 6월에 승인 받은 IEEE 802.1X 규격은 사용자 인증을 위한 다양한 인증 프로토콜을 수용하면서 접속 포트에 기반한 접근제어 기능을 정의하고 있다. 802.1X는 인증을 위한 WEP의 단점을 보완하기 위하여, IETF(Internet Engineering Task Force)의 확장 인증 프로토콜(EAP : Extensible Authentication Protocol)에 기반하고 있다. IEEE 802.1X는 현재 IEEE 802.1aa로 변경되어 추가 표준화 작업이 진행되고 있다. EAP는 다양한 인증 메커니즘을 제공하면서 어떠한 Link

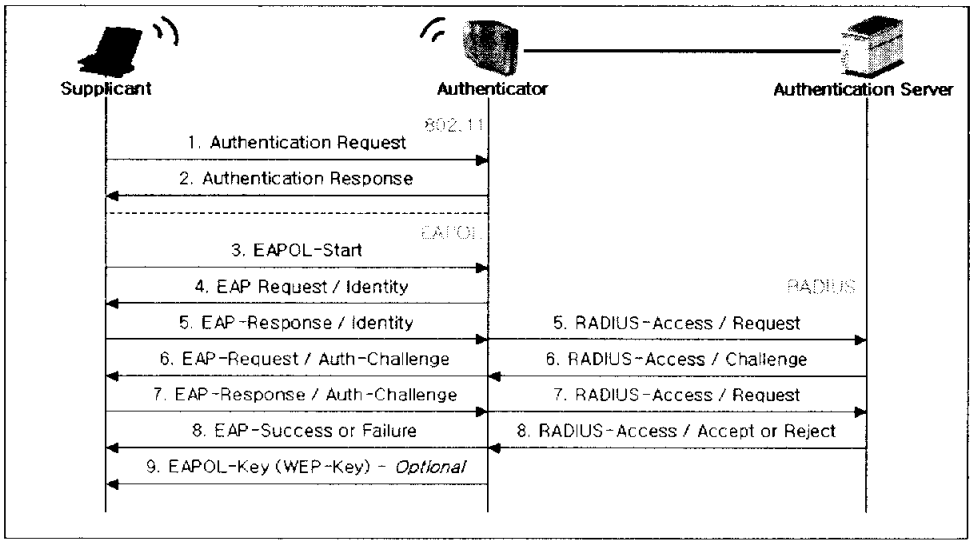
Layer에서도 적용할 수 있는 단순한 Encapsulation이다. [그림 9]은 EAP 기본 구조인데, 이는 모든 Link 계층에 적용될 수 있으며, 다양한 인증 방법을 사용할 수 있도록 설계되어 있다.[11]



[그림 9] EAP 기본 구조

802.1X는 인증 커뮤니케이션(Communication)에 Supplicant, Authenticator, Authentication Server라는 세 가지 구성 요소를 정의하고 있으며, 이러한 802.1X 구성 요소들이 EAP와 RADIUS 메시지를 이용하여 802.11 네트워크에서 EAPOL(EAP Over LAN) 교환 과정을 [그림 10]에서 보여주고 있다. Supplicant는 네트워크 자원에 접근을 구하고 있는 단말 사용자 시스템이다. 네트워크 접근은 Authenticator에 의해서 제어되는데, Authenticator는 전통적인 전화 네트워크에서 접근 서버와 동일한 역할을 수행한다. Supplicant와 Authenticator는 스펙에서 포트 인증 요소(PAE : Port Authentication Entity)라고 부른다. Authenticator는 Link Layer 인증 교환만 종료하고, 사용자 정보는 유지하지 않는다. Authenticator로 들어오는 모든 요청은 처리를 위하여 RADIUS(Remote Authentication Dial In User Service) 서버와

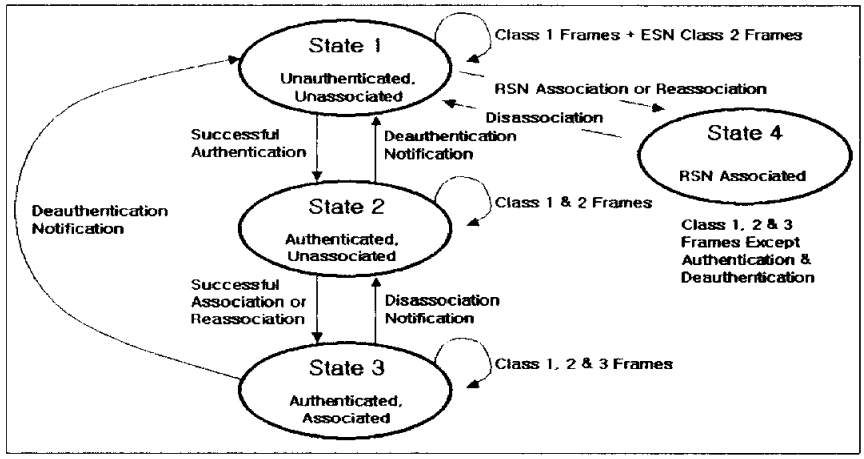
같은 인증 서버(Authentication Server)로 넘겨진다. 802.1X를 수용할 수 있는 디바이스의 포트는 권한이 부여된 상태에 있을 때에만 사용할 수 있다. 교환은 논리적으로 Supplicant와 Authentication Server 사이에서 일어나며, Authenticator는 브리지로서의 역할만 수행한다.



[그림 10] 802.11 네트워크에서의 EAPOL 교환 과정

3.3.2. 802.11i Task Group

IEEE 802.11i Task Group은 기존의 IEEE 802.11 무선랜 시스템이 가지는 무선구간 보안의 취약점을 해결하고자 IEEE 802.1X 기반 접근 제어, 보안 세션 관리, 동적인 키 교환 및 키 관리, 그리고 무선구간 데이터 보호를 위한 새로운 대칭키 암호 알고리즘(AES : Advanced Encryption Standard)의 적용하고 있으며, 강인한 보안 네트워크(RSN : Robust Security Network) 구축이 주된 목표이다. [그림 11]은 802.11i RSN 상태 머신을 보여주고 있다.



[그림 11] 802.11i RSN 상태 머신

3.4. 802.11 보안 서비스 개선 방안의 취약점

IEEE 802.1X의 도입 목적은 강력한 인증 메커니즘이 없는 무선랜에서 강한 인증과 접근 제어 그리고 키 관리를 제공하는 것이다. 그러나 IEEE 802.1X와 IEEE 802.11 무선랜 표준을 결합한 최초의 분석에서는 강한 접근 제어와 인증을 제공하지 못했고, ***openlx project***(IEEE 802.1X 표준의 Open Source 구현으로 만든 Project)의 한 부분으로 개발된 공격 Tool을 이용하여 Man-in-the-Middle Attack과 Session Hijacking이 성공하였다.[12] 이러한 공격이 성공한 이유는 IEEE 802.1X의 EAP와 IEEE 802.11내의 설계상 결함 때문이다.[13] 이러한 문제점은 IEEE 802.1X 인증 방법 중 하나인 EAP-TLS[14]를 사용하고 있는 IEEE 802.11i의 취약점으로까지 확장된다. 설계상의 주요 결함을 살펴보면 아래와 같이 크게 세 가지로 나누어 볼 수 있다.

① 상호 인증(Mutual Authentication)의 결여

EAP-MD5는 Supplicant와 Authenticator간에 비대칭(Asymmetric)적인 인증 방법을 사용하고 있다. Supplicant에서 Authenticator로의 일 방향 인증은 Supplicant가 잠재적으로 Man-in-the-Middle Attack에 노출될 수 있다. 비록 EAP-TLS 같은 강한 상호 인증을 제공하지만 강제적인 사항이 아니어서 EAP-TLS를 사용하려면 내부 구조를 수정해야 한다. 또한 EAP-TLS를 사용한다 하더라도 802.1X의 설계상 결함으로 인해 전체 EAP-TLS 인증을 우회하여 아래와 같이 Man-in-the-Middle Attack이 성공할 수 있다.

② EAP Success 메시지에 대한 Man-in-the-Middle Attack

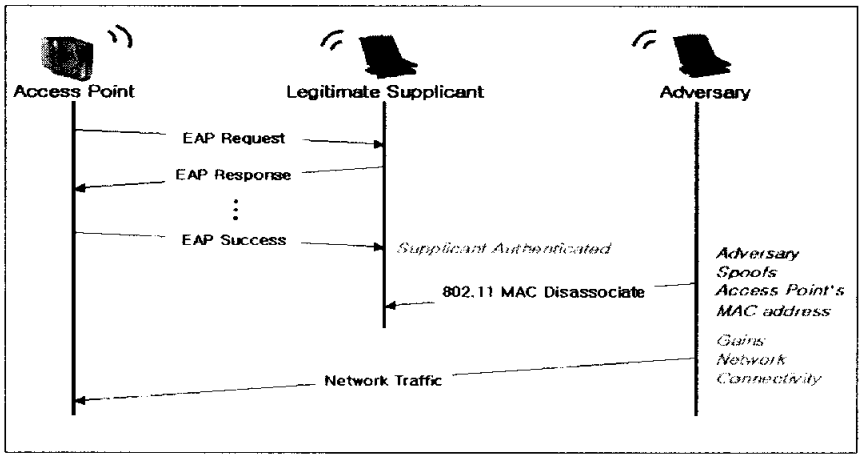
EAP Success 메시지는 Authentication Server로부터 RADIUS Access Accept 메시지의 영수증(Receipt)으로 Authenticator가 Supplicant에게 보낸다. 이것은 상태 머신이 인증을 성공했다는 것을 가리킨다.

High-Layer 인증 방법(EAP-MD5, EAP-TLS)에 상관없이 EAP Success 메시지는 정보를 보호할 만한 어떠한 무결성도 포함하고 있지 않다. 그러므로 공격자가 Authenticator를 대신하여 패킷을 위조할 수 있으며, Man-in-the-Middle Attack을 시작하여 공격자는 Supplicant가 보내는 모든 네트워크 트래픽을 얻을 수 있다. 이것은 어떠한 High-Layer 인증에서도 완벽한 우회가 가능하므로 802.11i Draft 6.0에서 Supplicant와 Authenticator의 상호 인증과 마스터 키(Master Key)를 유도하기 위해 사용하도록 정의한 EAP-TLS에서도 동일한 취약점이 노출되게 된다.

③ Session Hijacking

RSN은 [그림 11]과 같이 기존 802.11 상태 머신에 4번째 상태가 추가되었다. IEEE 802.1X에서의 High-Layer 인증은 RSN Association /

Reassociation 이후에 일어난다. 그러므로 802.1X와 RSN 두 개의 상태 머신이 존재하며, 이 두 머신의 결합된 행동은 인증 상태를 보여준다. 이 두 머신들 사이에서 메시지 확신성(Authenticity)에 대한 명백한 커뮤니케이션의 결여로 Session Hijacking이 수행될 가능성이 있다. [그림 12]는 Session Hijacking이 일어나는 과정을 보여준다.



[그림 12] Session Hijacking 과정

4. 제안하는 802.11 보안 서비스 개선 방안

4.1. 키 컨트롤러를 이용한 802.11 보안 서비스

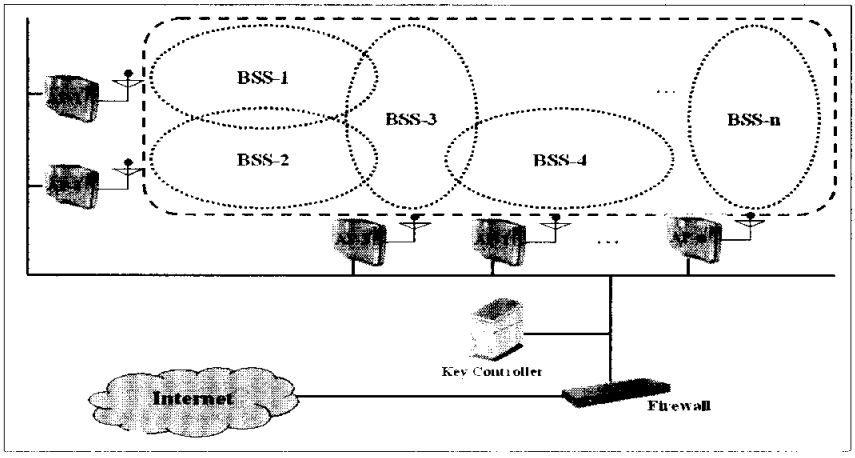
802.11에서 제공하는 보안 서비스 취약점이 발생하는 근본적인 이유는 키 설정, 분배, 갱신과 관련된 키 관리 메커니즘이 존재하지 않기 때문이다. 본 논문에서는 802.11 보안 서비스의 근본적인 취약점을 개선하기 위한 방안으로 키 컨트롤러를 이용한 802.11 보안 서비스를 위한 새로운 키 관리 구조를 제안한다. 제안된 방안을 사용하여 802.11 무선랜에서 안전한 통신을 하는 것이 본 논문의 궁극적인 목적이다.

여러 통신 서비스 사업자들이 공중 무선랜 서비스를 전개해 나가고 있지만, 대부분은 학교나 연구실내의 작은 소규모 그룹 단위로 무선랜을 구축해 사용하고 있다. 기존의 유선랜과 완전 별개의 서비스 형태로 무선랜을 사용하는 것이 아니라, 유선랜의 확장 또는 보완하는 차원으로 많이 사용하고 있는 실정이다. 현재 무선랜 사용의 상황을 고려해 본 논문에서는 단일 확장 서비스 셋에서의 보안 서비스에 초점을 맞추어 진행한다.

4.2. 제안하는 키 관리 구조 모델

본 논문은 802.11에서의 보안 서비스를 강화하기 위한 방안으로 새로운 키 관리 구조 모델을 제안하기 위해 몇 가지 가정이 필요하다. 첫 번째로 현재 무선랜 사용 환경을 고려하여 공중 802.11 무선 서비스가 아닌 여러 개의 기본 서비스 셋으로 이루어진 단일 확장 서비스 셋에 국한시킨 802.11 무선랜 환경이다. 그리고, 이 확장 서비스 영역에는 하나의 키 컨트롤러만 존재한다. 두 번째로 본 논문에서 정의하는 스테이션은 PDA를 제외한 무선 NIC을 장

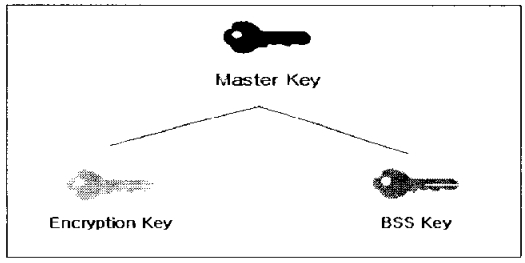
착한 노트북이나 데스크탑을 말한다. 그래서 무선으로 데이터를 전송할 수 있다는 점만 제외하면 스테이션의 계산 능력은 기존 유선 환경에서 스테이션이 가지는 계산 능력과 동일하다. 세 번째로 무선 환경이라는 특성상 무선 NIC과 같이 무선에 접근할 수 있는 장비만 있으면 무선을 통해 전송되는 모든 트래픽을 암호화된 여부에 상관없이 도청할 수 있다. 그래서 본 논문은 항상 무선상의 트랙픽이 도청 가능하다는 점을 고려하여 키 관리를 통한 데이터 기밀성을 보호하는 것에 가장 중점을 둔다. 네 번째로 액세스 포인트와 키 컨트롤러 사이의 유선 구간은 안전하다고 가정한다. 마지막으로 키 컨트롤러와 인증하기 이전의 스테이션과 액세스 포인트가 보내는 모든 트래픽은 키 컨트롤러를 거친다. 키 컨트롤러가 사전에 공유한 마스터 키를 가지고 BSS 키와 암호화 키를 생성하여 각 스테이션에게 분배한 다음 인증 과정을 거치며, 이후 스테이션은 액세스 포인트를 통해 분산 서비스를 이용할 수 있다. 이러한 가정 사항들을 고려하여, 제안하는 키 관리 구조 모델은 [그림 13]과 같다.



[그림 13] 제안하는 키 관리 구조 모델

4.2.1. 구성 요소와 역할

기존의 802.11 표준의 네 가지 구성 요소(분산 시스템, 액세스 포인트, 무선 매체, 스테이션)에 키 컨트롤러라는 개체만 하나 더 추가되었다. 키 컨트롤러는 802.1X 표준이나 802.11i 스펙에 있는 Authentication Server와 비슷한 역할을 담당하지만, 가장 큰 차이점은 EAP 방법을 통해서 키를 생성하는 것이 아니라, 단일 확장 서비스 셋과 같은 작은 규모의 무선랜 서비스라는 점을 이용하여 컨트롤러가 직접 각 개체들(액세스 포인트와 스테이션)의 마스터 키를 사전에 생성하여 인증 과정을 거친 뒤, 오프라인(Off-Line)으로 분배한다는 점이다. 키 컨트롤러와 각 개체들간 사전에 공유한 키는 긴 기간(Long Term)동안 사용되는 마스터 키(Master Key)의 역할을 담당하며, 이 키를 가지고 하나의 BSS에서 사용하는 BSS 키와 하나의 스테이션과 하나의 액세스 포인트만이 공유하는 각각의 공유키를 생성한다. 스테이션과 액세스 포인트의 인증에서뿐만 아니라, 스테이션이 동일한 ESS내의 다른 BSS로 이동 시 사전 인증(Pre-Authentication)에도 사용된다. 그리고 BSS는 서비스를 받기 원하는 스테이션들의 그룹임으로 컨트롤러에 의해 생성된 BSS 키의 안전성은 기존의 그룹 키가 가지는 요구 사항을 만족해야 한다. [그림 14]는 전체적인 키 구조이다.



[그림 14] 전체적인 키 구조

① 키의 종류

- $K_{CA_1}, K_{CA_2}, \cdots, K_{CA_n}$

키 컨트롤러(KC)가 사전에 생성하여 각 $AP_1, AP_2, \cdots, AP_n$에게 오프라인으로 공유하는 각 액세스 포인트의 마스터 키.

- $K_{CS_1}, K_{CS_2}, \cdots, K_{CS_m}$

키 컨트롤러(KC)가 사전에 생성하여 각 $STA_1, STA_2, \cdots, STA_m$에게 오프라인으로 공유하는 각 스테이션의 마스터 키.

- $K_{BSS_1}, K_{BSS_2}, \cdots, K_{BSS_n}$

$BSS_1, BSS_2, \cdots, BSS_n$에게 사용되는 그룹 키. AP_1이 BSS_1를 AP_2이 BSS_2를 담당하는 것과 같이 각 액세스 포인트가 각 BSS를 담당하므로 액세스 포인트의 개수와 BSS의 개수는 동일하다. BSS_1에 있는 스테이션이 AP_1과 AP_2를 모두 감지한다 하더라도 AP_1과 연결이 되어있다면 BSS_2 키로 암호화된 트래픽을 해독할 수 없다.

- $K_{A_1S_1}, K_{A_1S_2}, \cdots, K_{A_nS_m}$

임의의 AP_n과 STA_m간에 전송되는 트래픽을 암호화하기 위해 사용되는 대칭 암호화 키. 본 논문에서 제안하는 BSS 키는 기본 서비스 셋에 존재하는 모든 스테이션에게 멀티캐스팅(Multicasting)하는 키이다. 이런 그룹 키를 이용하여 스테이션이 사적인 내용을 전송한다면 BSS내의 스테이션 모두 그 내용을 볼 수 있다. 본 논문에서는 각 스테이션과 해당 액세스 포인트만 알고 있는 공유키 ($K_{A_nS_m}$)를 이용하여 BSS 키가 가지는 문제점을 해결하고 있다.

② BSS 키의 요구 사항

BSS 키는 하나의 기본 서비스 셋이라는 그룹내의 안전한 통신을 위해 필요하며, 그룹 키와 유사한 성질을 가진다. 그러므로 기존의 그룹 키가 가져야 하는 아래와 같은 네 가지 요구 사항을 만족해야 한다.[15]

- BSS 키의 비밀성(Secrecy)

공격자가 BSS 키를 도출해 내는 것이 계산상으로 불가능하여야 한다.

- 전방 비밀성(Forward Secrecy)

공격자가 이전 세션의 BSS 키에 대한 정보를 알고 있더라도, 이후의 BSS 키를 계산하지 못해야 한다.

- 후방 비밀성(Backward Secrecy)

공격자가 이후에 알려진 BSS 키에 대한 정보를 가지고서 이전 세션의 BSS 키를 계산하지 못해야 한다.

- 키 독립성(Key Independency)

BSS_1 키를 가지고 BSS_2 키를 계산하는 것은 불가능해야 한다.

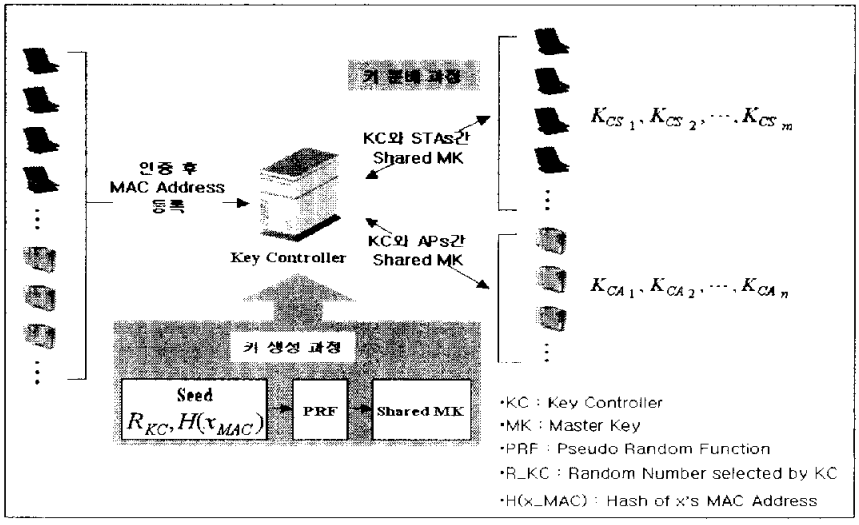
위 네 가지 성질들은 서로 연관성을 가지고 고려되어야 한다. BSS내의 스테이션 탈퇴 시 이후의 데이터에 대한 Forward Secrecy를 제공해야 하며, 새로운 스테이션이 BSS에 참여 시 이전의 데이터에 대한 Backward Secrecy를 제공해야 한다. 그리고 여러 개체들의 공모로 인해 BSS 키가 노출되는 것을 막기 위해 키의 독립성도 제공되어야 한다.

4.2.2. 마스터 키 생성 및 분배

키 컨트롤러가 하나의 확장 서비스 셋에 있는 모든 개체들(액세스 포인트와 스테이션)에 대한 인증을 거친 뒤, MAC Address를 등록시키고, [표 5]와 같이 키 컨트롤러가 선택한 난수와 각 개체들의 MAC Address의 해쉬값을 Seed로 사용하여 의사 난수 함수(PRF : Pseudo Random Function)를 통해 각 개체와 키 컨트롤러가 공유할 마스터 키를 생성하여 [그림 15]와 같이 분배한다.[16]

[표 5] 마스터 키 생성

• $Seed_{K_{CA_1}} = R_{KC}, H(AP_{1\ MAC})$: K_{CA_1}의 Seed
• $Seed_{K_{CS_1}} = R_{KC}, H(STA_{1\ MAC})$: K_{CS_1}의 Seed
• $K_{CA_1} = PRF(Seed_{K_{CA_1}})$: 키 K_{CA_1}의 생성
• $K_{CS_1} = PRF(Seed_{K_{CS_1}})$: 키 K_{CS_1}의 생성



[그림 15] 마스터 키 생성 및 분배 과정

4.2.3. BSS 키와 암호화 키 생성 및 분배

각각의 개체(스테이션과 액세스 포인트)들은 키 컨트롤러로부터 자신들이 사용할 BSS 키와 암호화 키를 전송받기 위해 사전에 키 컨트롤러와 공유한 마스터 키를 사용하여, 아래와 같이 파라메터(Parameter)들을 구성한 후 키 컨트롤러에게 전송한다. BSS 키와 암호화 키를 전송받기 위한 사전 단계와 BSS 키와 암호화 키를 생성하고 분배하는 과정은 아래와 같이 전개된다.

(쉬운 설명을 위해 스테이션 STA_1이 액세스 포인트 AP_1과 연결되었다고 가정한다.)

① 스테이션(STA_1) ⇒ 액세스 포인트(AP_1)

먼저 스테이션(STA_1)은 키 컨트롤러로부터 자신이 속한 서비스 셋의 BSS 키와 암호화 키를 받기 위한 Request 메시지로써 자신의 ID(STA_1)와 자신이 선택한 난수값(N_{S_1})으로 구성된 M_{S_1}을 식 (1)과 같이 구성하고, M_{S_1}에 대한 HMAC, H_{S_1}을 식 (2)와 같이 구성하여 AP_1을 통해 키 컨트롤러로 전송한다. 키 컨트롤러로 전송된 식 (1), (2)는 일단 STA_1과 무선 수신율이 가장 좋은 AP_1에게 전달된다.

(편의상 STA_1, AP_1이라고 정의한 것이며, 스테이션과 액세스 포인트의 구성은 사용자들이 어떻게 구성하느냐에 따라 달라질 수 있다.)

$$M_{S_1} = STA_1, N_{S_1} \quad \cdots\cdots (1)$$

$$H_{S_1} = HMAC(K_{CS_1}, M_{S_1}) \quad \cdots\cdots (2)$$

(2)는 메시지 M_{S_1}을 키 K_{CS_1}로 해쉬한 HMAC

② 액세스 포인트(AP_1) ⇒ 키 컨트롤러(KC)

키 컨트롤러는 각각의 스테이션들과 액세스 포인트들에게 자신과 공유하는

마스터 키를 분배하였지만, 어떤 스테이션이 어떤 액세스 포인트와 결합되었는지 모른다. 즉, 하나의 BSS에 어떤 스테이션들이 연결되어 있는지에 모른다. 키 컨트롤러는 어떤 스테이션이 어떤 액세스 포인트와 연결되어 있는지 알아야만, Request하는 스테이션에게 그들이 속해있는 정확한 BSS 키를 전달할 수 있다. 이 과정에서는 AP_1이 STA_1으로부터 받은 식 (1), (2)에 자신의 ID(AP_1)와 자신이 선택한 난수값(N_{A_1})을 구성된 N_{A_1}과 N_{A_1}의 HMAC (H_{A_1})을 식 (3), (4)와 같이 구성하여 키 컨트롤러에게 보낸다. 식 (3), (4)를 받은 키 컨트롤러는 두 번 해쉬된 값을 풀어봄으로써 키 컨트롤러는 STA_1이 AP_1과 연결되어 있으며, BSS_1에 존재함을 알게 된다.

$$M_{A_1} = M_{S_1}, H_{S_1}, AP_1, N_{A_1} \quad \cdots\cdots(3)$$

$$H_{A_1} = HMAC(K_{CA_1}, M_{A_1}) \quad \cdots\cdots(4)$$

(4)는 메시지 N_{A_1}을 키 K_{CA_1}로 해쉬한 HMAC

식 (3), (4)를 받은 키 컨트롤러는 K_{CA_1}과 K_{CS_1}을 이용하여 차례대로 해쉬값이 풀어진다면 사전에 인증한 정당한 액세스 포인트, 스테이션임을 확인할 수 있다. 그리고, 키 컨트롤러는 어떤 스테이션이 어떤 액세스 포인트와 연결되어 있는지 알게되어 해당 스테이션과 액세스 포인트에 알맞은 BSS 키와 암호화 키를 전달할 수 있다. 여기까지 키 컨트롤러가 각각의 액세스 포인트들과 스테이션들을 인증하는 과정이다.

③ 컨트롤러에 의한 BSS 키의 생성

키 컨트롤러가 AP_1가 담당하는 영역인 BSS_1내에서 사용될 BSS 키의 Seed를 식 (5)와 같이 구성하여 식 (6)의 K_{BSS_1}를 생성한다.

$$Seed_{K_{BSS}} = R_{KC}, K_{CA_1}, H(AP_{1_{MAC}} \| BSS_{1_{ID}}) \quad \cdots\cdots(5)$$

$$K_{BSS_1} = PRF(R_{KC}, K_{CA_1}, H(AP_{1_{MAC}})) \quad \cdots\cdots(6)$$

(5)는 AP_1의 영역에서 사용될 BSS 키(K_{BSS_1})의 Seed

(6)의 $K_X = PRF(B)$: B를 Seed로 사용하여 PRF를 통해서 생성된 X의 키

식 (6)에 의해서 생성된 K_{BSS_1}는 BSS_1내의 모든 스테이션이 사용할 그룹 키가 된다. 기존의 802.11 보안 서비스에서 WEP 키의 사용이 선택적(Optional)이었던 반면, 본 논문에서는 보안성 강화를 위해 무선상으로 전송하는 모든 메시지는 최소한 BSS 키를 사용하여야 한다.

④ 컨트롤러에 의한 STA_1과 AP_1간의 암호화 키($K_{A_1S_1}$)의 생성

암호화 키의 생성 방법은 PRF에 들어갈 초기 Seed만 다르고, 방법은 BSS 키의 생성과 동일하다. Seed는 식 (7)과 같고, 암호화키는 식 (8)과 같다.

$$Seed_{K_{AS}} = R_{KC}, K_{CS_1}, H(AP_{1_{MAC}} \| STA_{1_{MAC}}) \quad \cdots\cdots(7)$$

$$K_{A_1S_1} = PRF(R_{KC}, K_{CS_1}, H(AP_{1_{MAC}} \| STA_{1_{MAC}})) \quad \cdots\cdots(8)$$

(7)은 STA_1과 AP_1가 공유할 STA_1 암호화 키($K_{A_1S_1}$)의 Seed

⑤ 키 컨트롤러(KC) ⇒ 액세스 포인트(AP_1)

키 컨트롤러는 AP_1으로부터 받은 STA_1의 Request에 대한 Response로써 메시지 M_C를 식 (11)과 같이 구성하여 AP_1를 통해 STA_1에게 전송한다. 식 식 (11)을 받은 AP_1은 자신이 복호할 수 있는 메시지($resM_{A_1}$)만 가지고, 복호할 수 없는 메시지($resM_{S_1}$)는 STA_1으로 보낸다. AP_1은 $resM_{A_1}$을 복호하여 키 컨트롤러를 인증하고, 자신이 전송한 난수값(N_{A_1})을 확인하여 메시지의

무결성을 체크한다.

$$resM_{A_1} = K_{CA_1}(K_{BSS_1}, K_{A_1S_1}, N_{A_1}) \quad \cdots\cdots(9)$$

$$resM_{S_1} = K_{CS_1}(K_{BSS_1}, K_{A_1S_1}, N_{S_1}, AP_{1_{MAC}}) \quad \cdots\cdots(10)$$

$$M_C = resM_{A_1}, resM_{S_1} \quad \cdots\cdots(11)$$

(9)의 $resM_{A_1}$는 (3)의 M_{A_1}에 대한 Response

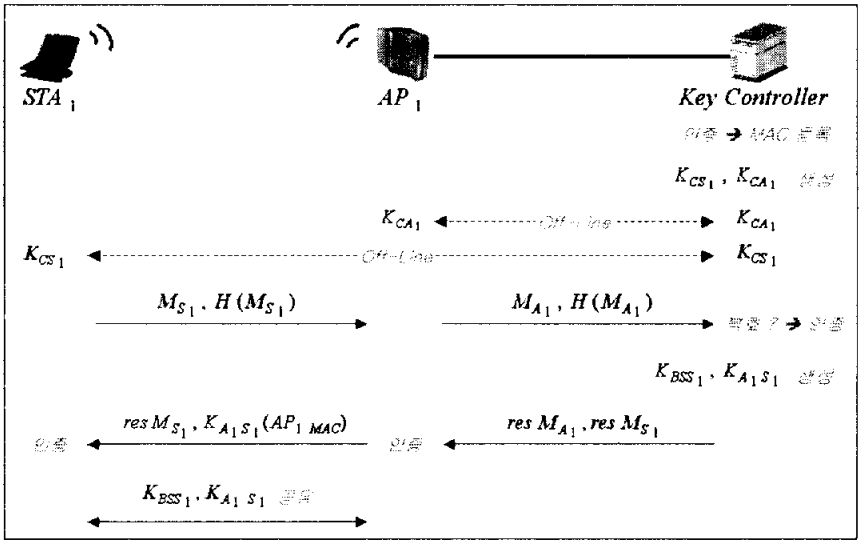
(10)의 $resM_{S_1}$는 (1)의 M_{S_1}에 대한 Response

⑥ 액세스 포인트(AP_1) ⇒ 스테이션(STA_1)

AP_1은 자신이 복호할 수 없었던 메시지($resM_{S_1}$)와 자신의 MAC Address를 식 (9)내의 $K_{A_1S_1}$로 암호화한 후, 식 (12)와 같이 구성하여 STA_1에게 전달한다.

$$resM_{S_1}, K_{A_1S_1}(AP_{1_{MAC}}) \quad \cdots\cdots(12)$$

이를 전달받은 STA_1은 먼저 $resM_{S_1}$를 복호하여 키 컨트롤러를 인증하고, $resM_{S_1}$내의 $AP_{1_{MAC}}$과 키 $K_{A_1S_1}$로 복호하여 나온 $AP_{1_{MAC}}$을 비교해봄으로써 AP_1이 정당한 개체임을 인증한다. 그리고 $resM_{S_1}$내의 난수값(N_{S_1})을 확인하여 메시지의 무결성을 체크한다. 그리하여 STA_1과 AP_1은 K_{BSS_1}와 $K_{A_1S_1}$을 공유하게 되어 STA_1은 K_{BSS_1} 또는 $K_{A_1S_1}$을 이용하여 트래픽을 암호화하여 목적지로 전송한다. 전체적인 키 생성과 분배과정은 [그림 16]과 같다.



[그림 16] 전체적인 키 생성 및 분배 과정

[표 6] 약어 표기법

- K_{CS_1} : 키 컨트롤러와 공유한 STA_1의 마스터 키
- K_{CA_1} : 키 컨트롤러와 공유한 AP_1의 마스터 키
- K_{BSS_1} : AP_1이 담당하는 영역에서 사용되는 BSS 키
- $K_{A_1S_1}$: AP_1과 공유한 STA_1의 암호화 키
- $M_{S_1} = STA_1, N_{S_1}$
- $H_{S_1} = H(K_{CS_1}, M_{S_1})$: M_{S_1}의 해쉬값
- $M_{A_1} = M_{S_1}, H_{S_1}, AP_1, N_{A_1}$
- $H_{A_1} = H(K_{CA_1}, M_{A_1})$: M_{A_1}의 해쉬값
- $M_C = resM_{A_1}, resM_{S_1}$: 키 컨트롤러의 전체적인 Response
- $resM_{A_1} = K_{CA_1}(K_{BSS_1}, K_{A_1S_1}, N_{A_1})$: AP_1에게 전달하는 Response
- $resM_{S_1} = K_{CS_1}(K_{BSS_1}, K_{A_1S_1}, N_{S_1}, AP_{1_{MAC}})$: STA_1에게 전달하는 Response

4.2.4. BSS 키와 암호화 키 갱신

본 논문에서 BSS 키와 암호화 키의 갱신은 크게 키 컨트롤러에 의한 주기적인 키 갱신과 스테이션의 이동으로 인한 키 갱신 두 가지로 나뉜다.

① 주기적인 BSS 키와 암호화 키 갱신

BSS 키는 BSS내의 정당한 개체들 모두가 공유하는 키이다. 그래서 BSS 내에서 각 스테이션의 암호화 키로 암호화된 트래픽보다 BSS 키로 암호화된 트래픽이 더 많이 발견되어 악의적인 공격자가 지속적으로 트래픽을 도청하여 그 패턴(Pattern)을 분석함으로써 BSS 키를 알아낼 가능성이 있다. 이러한 이유로 본 논문에서는 키 컨트롤러가 주기적으로 BSS 키를 갱신한다. BSS 키의 갱신 방법은 Seed로 타임 스탬프(Time Stamp)만 추가되는 것을 제외하면 식 (5)의 BSS 키 생성하는 과정과 동일하다. 암호화 키는 해당 스테이션만 알고 있는 비밀키이기에 BSS 키와 같이 빈번하게 암호화 키를 갱신하는 것은 네트워크에 과부하를 줄 수 있다. 그래서 스테이션의 암호화 키 갱신은 스테이션이 요구할 시 식 (7)에 Seed로 타임 스탬프만 추가하여 해당 스테이션의 갱신된 암호화 키를 생성하고 전송한다. 갱신될 BSS 키와 암호화 키의 Seed는 식 (13), (14)와 같다.

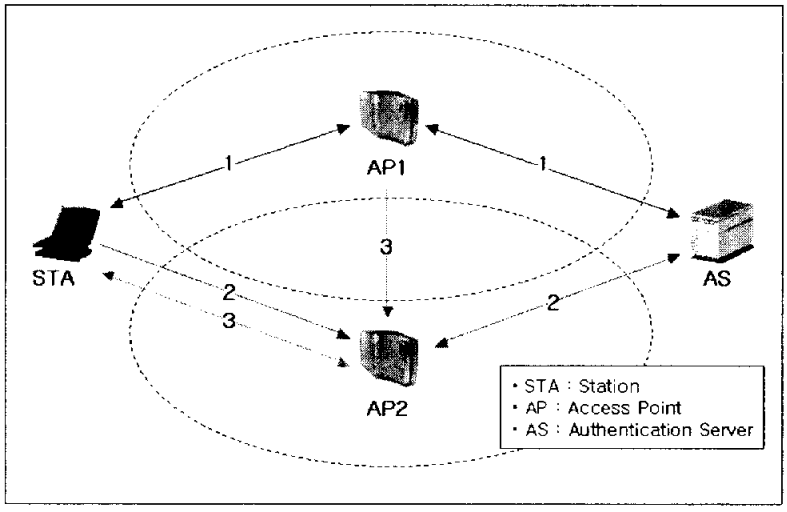
$$Seed_{K_{BSS}} = R_{KC}, K_{CA_1}, H(AP_{1\,MAC} \| BSS_{1\,ID}), Time\ Stamp \quad \cdots\cdots\cdots\cdots\cdots\cdots (13)$$

$$Seed_{K_{AS}} = R_{KC}, K_{CS_1}, H(AP_{1\,MAC} \| STA_{1\,MAC}), Time\ Stamp \quad \cdots\cdots\cdots\cdots\cdots\cdots (14)$$

② 스테이션의 전이(Transition) 시 BSS 키와 암호화 키 갱신

단일 ESS내에 있는 스테이션은 [그림 13]과 같이 하나의 BSS에서 다른 BSS로 전이가 가능하다. 이런 스테이션의 전이에서도 Forward Secrecy와

Backward Secrecy를 제공하기 위해 키의 갱신이 필요하다. 주기적인 키의 갱신과 가장 큰 차이점은 BSS 키의 갱신과 함께 스테이션의 암호화 키의 갱신과 같이 일어난다는 점이다. 그러나 이런 스테이션의 전이로 인한 키 갱신은 본 논문에서 가정하고 있는 작은 규모의 네트워크에서는 매우 드물게 일어난다. 동일한 ESS내의 다른 BSS로 전이 시 [그림 17]과 같은 사전 인증(Pre-Authentication)이라는 과정이 발생하는데, 이는 이동한 BSS 영역을 담당하는 액세스 포인트와 빠른 연결(Association)을 제공하기 위한 목적으로 사용된다.



[그림 17] Pre-Authentication 과정

여기서는 전이 시 사전 인증의 과정이 포함된 키 갱신에 대해 설명한다. 이 때의 키 갱신은 스테이션의 암호화 키와 BSS 키의 갱신, 스테이션이 이동한 영역의 BSS 키의 갱신, 이전 스테이션이 있었던 BSS의 BSS 키의 갱신과 같이 세 가지 키 갱신이 일어나게 된다. 그 과정은 아래와 같이 전개된다.

● 이동한 스테이션의 암호화 키와 BSS 키의 갱신

예를 들어, STA_1이 AP_1에서 AP_2로 이동하였다고 가정하자. STA_1은 AP_1을 통해 키 컨트롤러에게 보내었던 초기 메시지와 동일한 식 (1), (2)를 AP_2에게 보낸다.

$$M'_{S_1} = STA_1, N'_{S_1} \quad \cdots\cdots(15)$$

$$H'_{S_1} = H(K_{CS_1}, M_S'_1) \quad \cdots\cdots(16)$$

(16)은 메시지 M'_{S_1}을 키 K_{CS_1}로 해쉬한 HMAC

식 (15), (16)을 받은 AP_2는 아래와 같은 식 (17), (18)을 구성하여 키 컨트롤러에게 전송한다.

$$M'_{A_2} = M'_{S_1}, H'_{S_1}, AP_2, N'_{A_2} \quad \cdots\cdots(17)$$

$$H'_{A_2} = H(K_{CA_2}, M'_{A_2}) \quad \cdots\cdots(18)$$

(4)는 메시지 N'_{A_2}을 키 K_{CA_2}로 해쉬한 HMAC

식 (17), (18)을 받은 키 컨트롤러는 인증 과정을 거치는데, 이 때의 인증을 사전 인증이라 한다. 즉, 연결은 AP_1과 되어있지만, 이후 빠른 연결을 위해 AP_2와 연결되기 전에 키 컨트롤러를 통해서 AP_2에게 사전에 인증을 받아두는 것이다. 이 후 STA_1이 BSS_2로 완전히 이동하면, 키 컨트롤러는 BSS_2에서 사용될 새로운 BSS 키(K_{BSS_2})를 생성하여 BSS_2내의 모든 스테이션들이게 전송하고, STA_1의 새로운 암호화 키($K_{A_2S_1}$)를 생성하여 STA_1에게 전송한다. 갱신될 BSS 키(K_{BSS_2})와 암호화 키(K_{BSS_2})는 식 (13), (14)와 동일한 방법으로 Seed를 사용하여, PRF를 거쳐 생성된다.

● 스테이션이 참가하고, 떠난 BSS에서 BSS 키 갱신

[그림 17]에서 STA_1이 완전히 AP_2의 영역으로 이동하면 기존 AP_1과의 연결을 끊고, AP_2와 연결을 하게 된다. 그러면 AP_1은 이런 정보를 키 컨트롤러에게 전달함으로써 키 컨트롤러는 STA_1이 AP_1에서 AP_2로 이동했다는 것을 알게 된다. BSS 키의 Forward Secrecy와 Backward Secrecy의 요구사항을 만족시키기 위해 키 컨트롤러는 STA_1이 새로이 참가한 BSS_2 키(K_{BSS_2})와 STA_1이 떠난 BSS_1 키(K_{BSS_1})을 모두 갱신시킨다. 갱신시키는 방법과 전송하는 방법은 위에서 설명한 키 생성 및 전송 방법과 동일하다.

4.3. 제안하는 키 관리 구조 모델의 안전성 분석

IEEE 802.11 보안 서비스의 WEP 프로토콜은 무선으로 전송되는 트래픽에 대한 기밀성, 무결성 그리고 사용자 인증이라는 기본적인 세 가지 보안 서비스를 충족시키지 못하였다. 이를 개선하기 위한 IEEE 802.1X와 IEEE 802.11i Task Group의 제안 방안 또한 Man-in-the-Middle Attack과 Session Hijacking의 가능성 있음을 살펴보았다. 본 논문에서 제안하는 새로운 키 관리 구조 모델과 기존의 모델과의 가장 큰 차이점은 키 컨트롤러에 의해 생성된 마스터 키가 사전 분배되고, 이 마스터 키를 이용하여 BSS 키와 각각의 스테이션마다 무선상에서 사용하는 자신들만의 고유한 암호화 키를 유도해 낸다는 점과 키 컨트롤러에 의해 지속적으로 키가 갱신된다는 점이다. 또한 무선상으로 데이터를 전송할 시에는 BSS 키를 선택적으로 사용하는 것이 아니라, 보안을 위해 강제적으로 사용하여야 한다는 점이다. 이 장에서는 제안하는 새로운 키 관리 구조는 아래와 같은 보안 서비스를 제공한다.

① 기밀성 제공

단일 ESS내의 모든 스테이션은 키 컨트롤러가 제공한 각각의 BSS 키와 암호화 키를 가진다. 무선상으로 전송되는 모든 메시지들은 최소한 BSS 키로 암호화되어 있어서, 오프라인으로 키 컨트롤러에 등록하지 않은 악의적인 스테이션 또는 BSS에 우연히 나타나는 스테이션은 정당한 개체가 아니기에 트래픽을 복호화할 수 없다. 또한 스테이션만의 비밀스런 데이터는 각 스테이션만의 암호화 키로 암호화함으로써 무선 구간에서의 데이터 기밀성을 제공하고 있다.

② 무결성 제공

본 논문에서는 HMAC을 사용하여 전송되는 데이터에 대한 무결성도 함께 제공한다. 키 컨트롤러의 키 관리 부담을 줄이기 위해 HMAC을 위한 별도의 키를 사용하지 않고, BSS 키나 각 스테이션이 소유한 암호화 키는 HMAC을 위한 키로 사용한다. 그리고 난수를 사용하여 해당 세션에 대한 무결성도 제공한다.

③ 사용자 인증

키 컨트롤러에게 마스터 키를 제공받기 전에 오프라인으로 인증 과정을 거친다. [그림 16]과 같이 스테이션과 액세스 포인트는 키 컨트롤러로부터 BSS 키와 암호화 키를 제공받기 위해 사전에 분배된 마스터 키를 사용하여 모든 메시지를 암호화하여 키 컨트롤러로 전송한다. 메시지를 받은 키 컨트롤러는 해당 개체의 마스터 키로 해당 메시지를 복호함으로써 액세스 포인트와 스테이션은 정당한 개체임이 인증한다. 이후 BSS 키와 암호화 키의 분배 시 키 컨트롤러는 해당 개체의 마스터 키로 암호화하고, 이를 분배함으로써 이를 받은 액세스 포인트와 스테이션은 정당한 키 컨트롤러임을 인증한

다. 그리고 스테이션은 정당한 액세스 포인트임을 인증하기 위해 해당 액세스 포인트로부터 MAC Address를 암호화 키로 암호화한 메시지를 하나 더 받게 된다. 스테이션은 이 메시지를 복호화 함으로써 정당한 액세스 포인트임을 인증하게 된다.

④ Man-in-the-Middle Attack으로부터 보호

IEEE 802.1X와 IEEE 802.11i에서 초기 인증을 위해 사용하는 EAP-TLS는 Man-in-the-Middle Attack의 가능성이 존재함을 살펴보았다.

본 논문에서 제안하는 키 관리 구조 모델에서는 만약 정당한 스테이션 또는 정당한 액세스 포인트라면 무선상으로 전송되는 모든 트래픽은 최소한 BSS 키로 암호화하여 보낸다고 정의하였기에, BSS 키는 가지고 있어야 한다. 이런 BSS 키를 가지려면 사전에 키 컨트롤러와 공유한 마스터 키가 있어야 하고, 마스터 키를 분배받으려면 오프라인으로 키 컨트롤러에게 인증을 받아야 한다. 그러므로 이러한 인증을 받지 못한 악의적인 공격자가 정당한 스테이션과 정당한 액세스 포인트 사이에서 자신이 만든 키로 Man-in-the-Middle Attack을 한다는 것은 불가능하다.

⑤ Session Hijacking으로부터 보호

악의적인 공격자가 [그림 12]와 같이 액세스 포인트의 MAC Address로 위장한다 하더라도, 정당한 개체가 아니므로 모든 트래픽에 사용되는 최소한의 키인 BSS 키를 알지 못한다. 그러므로 악의적인 사용자가 액세스 포인트의 MAC Address를 위장하여 Disassociation 메시지를 스테이션에게 보낸다하여도 BSS 키로 암호화되어 있지 않으므로, 스테이션은 그 Disassociation 메시지를 버린다. 그래서 공격자에 의한 Session Hijacking으로부터 보호된다.

5. 제안 방안의 키 생성 시뮬레이션

5.1. 시뮬레이션 환경

- 사용 언어
  - Visual C++

- 시스템 환경
  - CPU : Pentium Ⅳ 1.5GHz
  - Memory : 256M
  - OS : Windows 2000

5.2. 키 생성 시뮬레이션

이 장에서는 본 논문에서 제안하는 가장 중요한 핵심인 키 생성을 시뮬레이션 결과로 제시한다. 키의 생성에는 마스터 키, BSS 키, 암호화 키의 생성으로 구분할 수 있지만, 이 키들은 Seed만 제외하고 같은 PRF를 사용하기 때문에 마스터 키 생성에 대한 시뮬레이션만 수행하였고, 그 결과를 제시한다. 그리고 스테이션과 액세스 포인트의 마스터 키 생성은 MAC Address만 다르기 때문에 스테이션의 마스터 키 생성에 대해 살펴보겠다.

5.2.1. 스테이션(STA_1)의 마스터 키 생성

STA_1의 마스터 키 생성은 아래의 식 (19)와 같다.

$$K_{STA_1} = PRF(R_{KC}, H(STA_{1\,MAC})) \quad \cdots\cdots(19)$$

PRF의 Seed로 키 컨트롤러가 선택한 랜덤값에 STA_1의 MAC Address를 MD5로 해쉬한 값을 사용한다.

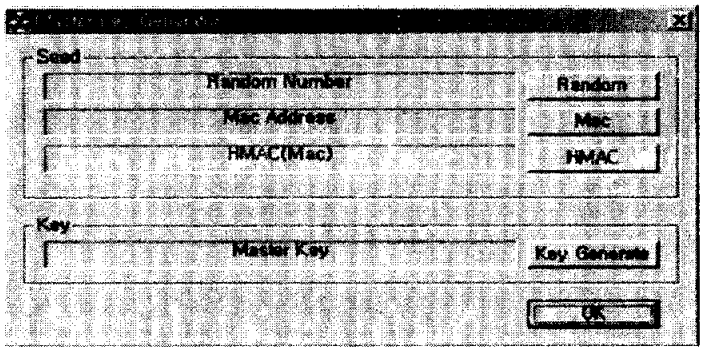
5.2.2. PRF 내부 구성

키 컨트롤러가 선택하는 랜덤값(R_{KC})은 Visual C++의 srand()함수를 사용하였다. 이 함수는 starting point random 함수로 랜덤 넘버를 생성하는 또 다른 함수인 rand()함수가 0의 값을 출력할 수도 있기 때문에 이를 방지하기 위해 srand()함수를 사용하였다. 이 함수가 무작위로 선택하는 값으로 시스템에 세팅(Setting)된 연도와 날짜의 곱을 사용하였으며, 이를 128 비트의 integer형으로 출력하게 하였다. 그래서 rand()함수와 같이 출력으로 0이 출력되는 일이 없도록 하였다. 스테이션의 MAC Address도 MD5를 통해 128 비트의 출력으로 나오게 하였으며, Seed를 모두 입력하지 않고 Key Generator를 눌렀을 경우 정확한 키 값이 생성되지 않도록 하였다.[16]

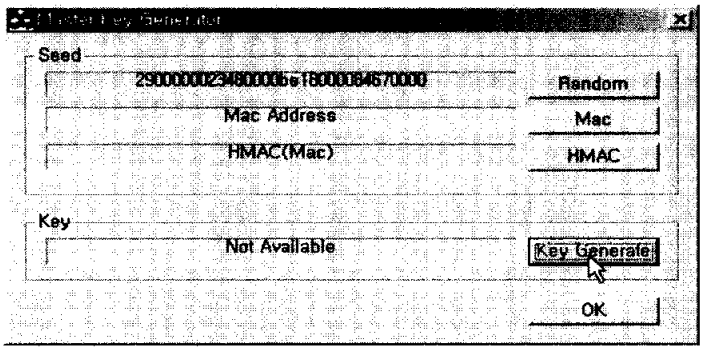
PRF도 MD5를 사용하며 구현하였으며, 두 개의 Seed, R_{KC}와 $H(STA_{1\ MAC})$를 XOR한 값을 PRF의 Seed로 입력하였다.

5.3. 키 생성 시뮬레이션 결과

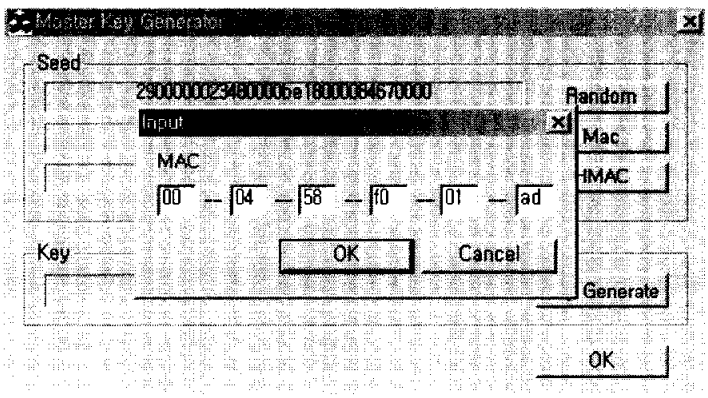
스테이션의 마스터 키 생성 시뮬레이션 결과는 다음 페이지의 [그림 18]과 같다. 액세스 포인트의 마스터 키도 Seed로 MAC Address만 다르게 입력하면 생성이 가능하며, BSS 키와 암호화 키의 경우에도 Seed로 키 컨트롤러가 선택한 랜덤값(R_{KC})에 각 개체의 마스터 키와 추가적인 파라메터만 입력받아 동일한 PRF를 사용하여 생성할 수 있다.



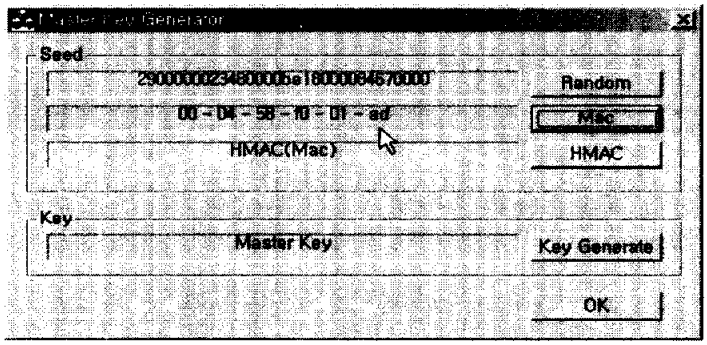
마스터 키 생성 초기 화면



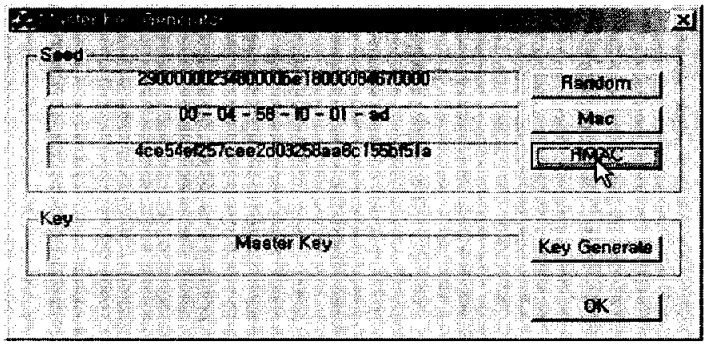
Seed가 완전하지 않을 경우의 에러 화면



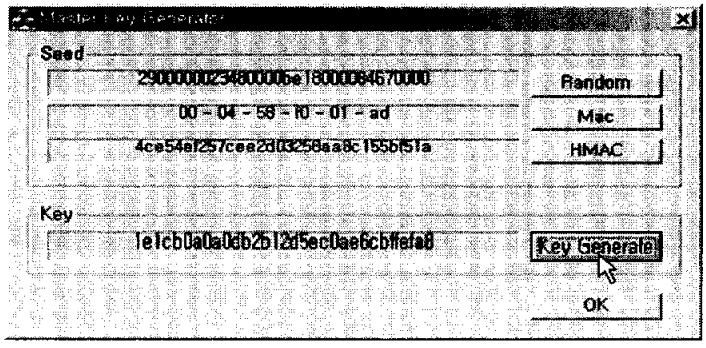
스테이션의 MAC Address 입력 화면



스테이션의 MAC Address를 입력받은 후 화면



스테이션의 MAC Address를 해쉬한 화면



스테이션 마스터 키 생성 화면

[그림 18] 스테이션 마스터 키 생성 과정

6. 결론 및 향후 연구

IEEE 802.11 무선랜 서비스는 이동성, 유연성, 효율성, 확장성 등의 이점으로 그 사용이 급격히 증가되고 있다. 그러나, 무선랜 서비스에 대한 보안은 상대적으로 취약하다. IEEE 802.11 표준에서는 무선 환경에서의 안전한 운영을 제공하기 위해 기밀성, 무결성, 인증과 같은 보안 서비스를 정의하고 있다. 이런 무선 환경에서의 보안 서비스들은 주로 WEP 프로토콜에 의해 제공되는데, WEP 프로토콜에 대한 많은 취약점이 알려지면서, WEP은 더 이상 무선 환경에서 보안 서비스를 제공하기 위한 방안이 될 수 없다.

WEP 프로토콜을 개선하기 위한 방안으로 IEEE 802.1X에서는 포트 기반의 사용자 인증과 IEEE 802.11i에서는 RSN을 통한 데이터 기밀성, 무결성을 제공하기 위한 연구를 진행 중이다. 그러나, 본론에서 살펴본 것과 같이 이런 방안들도 Man-in-the-Middle Attack이나 Session Hijacking에 노출될 가능성이 있다.

따라서 본 논문에서 이런 문제점을 해결하기 위한 방안으로 키 컨트롤러를 통한 새로운 키 관리 구조 모델을 이용하여 세 가지 기본적인 보안 서비스(기밀성, 무결성, 인증)의 제공과 표준 기관들이 제안한 개선 방안의 취약점인 Man-in-the-Middle Attack이나 Session Hijacking에 대한 안전성도 함께 제공하고 있다.

이러한 안전성과 함께 마스터 키를 사전에 분배하기에 무선상에서 마스터 키를 안전하게 유도하기 위한 방안(802.11i에서 마스터 키를 설정하는 과정과 세션 키를 유도하는 과정)보다 트래픽의 양도 줄어들어 단일 확장 서비스 셋으로 이루어진 작은 규모의 무선랜에서는 효율적이다.

그러나, 새로운 디바이스(액세스 포인트나 무선 NIC을 장착한 노트북 또는

데스크탑) 추가 시에는 항상 키 컨트롤러에 등록시켜야 하는 번거로움이 있다. 오랜 기간동안 사용하기 위한 디바이스가 아니라, 무선랜을 잠시 동안 사용할 경우에도 새로운 디바이스를 키 컨트롤러에 등록시켜야 하기에 사용자들이 무선랜을 사용하는데 번거롭다. 사용자 측에서의 효율성은 공중 무선랜의 사용에 비해 떨어진다.

그리고 본 논문에서의 제안 방안은 공중 무선랜에서의 보안 서비스가 아니라, 단일 확장 서비스 셋에서의 보안 서비스로 범위를 제한하고 있다. 차츰 공중 무선랜으로 서비스가 확장되고 있는 상황을 고려하여 제안하는 키 관리 구조 모델을 공중 무선랜으로 확장했을 시, 이에 대한 고려사항 및 보안에 대한 향후 연구가 필요하다.

참고문헌

[1] Tutorial of draft Standard IEEE 802.11/D3.0, March 1996. "http://grouper.ieee.org/groups/802/11/main.html"

[2] Sultan Weatherspoon, Network Communications Group, Intel Corporation. "Overview of IEEE 802.11b Security", Intel Technology Journal Q2, 2000.

[3] IEEE 802.1X - Port Based Network Access Control MIB, 1998. "http://www.ieee802.org/1/pages/802.1x.html"

[4] IEEE, LAN/MAN Specific Requirement - Part 11 : Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specfication : Medium Access Control(MAC) Security Enhancements, IEEE Std 802.11i/D6.0, Septemper 2003.

[5] Mattbew S. Gast "802.11 Wireless Networks - The Definitive Guide", p.7-p.22 O'REILLY, April 2002.

[6] Bruce Potter and Bob Fleck "802.11 Security", O'REILLY, December 2002.

[7] W. A. Arbaugh, N. Shankar, and J. Wang. "Your 802.11 Network has no clothes", In Proceeding of the First IEEE International Conference on Wireless LANs and Home Network, December 2001.

[8] S. Fluhrer, I. Martin, and A. Shamir. "Weakness in the key scheduling algorithm of RC4" Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

[9] A. Stubblefield, J. Ioannidis, and A. D. Rubin. "Using the fluhrer, martin, and shamir attack to break wep", ATT Labs Technical Report, TD4ZCPZZ, August 2001.

[10] N. Borisov, I. Goldberg, and D. Wagner. "Intercepting Mobile Communications : The Insecurity of 802.11", In Procceeding of the Seventh Annual International Conference on Mobile Computing and Networking, p.180-p.188, 2001.

[11] L. Blunk and J. Vollbrecht. "PPP extensible authentication protocol(eap)", RFC 2284, March 1998.

[12] Open1X - Open Source Implementation of IEEE 802.11, "http://open1x.sourceforge.net".

[13] Arunesh Mishra, William A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard", Tech. Rep. CS-TR-4328, University of Maryland, College Park, February 2002.

[14] B. Aboba and D. Simon. "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

[15] D. Bruschi and E. Rosti, "Secure Multicast in Wireless Networks of Mobile Host : Protocols and Issues", ACM Balzer MONET Journal, Special Issue on Multipoint Communication in Wireless Mobile Networks, 2000.

[16] C. Rigney, W. Willats and P. Calhoun. "RADIUS Extensions", RFC 2869, June 2000.

[17] R. Rivest. "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

감사의 글

2004년 1월 2일, 감사의 글을 쓰는 오늘이 연구실에 들어온 지 꼭 만 2년이 되는 날이군요! 졸업을 한다 생각하니 시원하고, 교수님과 선·후배님들과 함께 할 시간이 얼마 남지 않았다고 생각하니 서운하네요!

처음 접해본 학문을 좀더 깊이, 좀더 많이 배우고가지 못하는 아쉬움은 있지만, 정말 좋은 연구실에서 교수님을 비롯한 많은 선·후배들을 만나고, 함께 생활했다는 것만으로도 2년이라는 시간이 저에게 정말로 소중하고 보람되었습니다.

제가 이 자리에 오기까지 힘이 되어주신 모든 분들께 '감사하다'는 말만으로 제 맘을 다 표현할 수 있겠냐만은 이 보다 더 좋은 말은 없을 것 같습니다.

우선 저의 훌륭하신 스승이자, 지도 교수님인 이경현 교수님께 감사 드립니다. 제가 교수님의 정보보호학 석사 과정의 첫 졸업생이라는 것에 제 나름대로 의미를 부여하며, 이 영광을 교수님께 돌립니다.

제 논문을 보고 조언을 아끼지 않으신 김창수 교수님, 정연호 교수님, 정보보호학 주임 교수님인 박지환 교수님, 저에게 범접하지 못할 학문같이 느껴졌던 수학에 조금이라도 관심을 갖게 해주신 조성진 교수님, 정보보호학 여러 분야에서 활동중이신 정목동 교수님, 최명구 교수님, 조경연 교수님! 감사 드립니다.

연구실 생활 2년 동안 연구실 짱이었던 준석선배(한 아이에서 두 아이의 아버지가 된 것 축하드려요!), 연구실 大母 정화선배(선배만 보면 ○○가 생각나요! → 정답 : 국수), 연구실에선 실세(實勢)지만 미선이 앞에선 실세(失勢)가 되어버리는 종필선배(살은 언제 빼실런지...), 나의 영원한 사수 영호선배(과묵함을 너무 사수하지 마세요. 선밴 웃는 얼굴이 직이는데...), 밤샘의 제왕 철이선배(박사 땐 매일매일 일찍 오실꺼죠?), 앞으로 연구실을 웃음바다(?)로 이끌고 가실 현호선배(그러다 Edda 당하지 않길...), 연구실 귀염둥이 원조 희연씨, 2년 동안 동고동락한 영원한 동기 영경이(그 동안 수고 많았다!)에게 감사 드립니다. 그리고 내 사랑스런 후배들. 한 남자의 여인이자 앞으로 우리 연구실의 석사 왕고(Wow~) 지원이(항상 건강해라!), 언제나 부지런한 우리 연구실의 산 증인 미선이(널 보면 "세상을 지배하는 것은 남자지만, 그 남자를 지배하는 것은 여자"라는 격언이 정답임을 느낀다.), 술 잘 마신다

고 해놓고 그런 모습 한 번도 안 보여준 채 서울로 도망친 종찬이, 연구실 새 식구가 된 민현이(술은 좀 하나?), 마운드에서 마구(魔球)를 마구 던진다는 소문이 있는 봉기, 술 못한다고 해놓고 술 잘 마신다고 해놓고 도망친 Nom보다 더 술 잘 마시는 내숭의 달인 주영이. 모든 분께 감사 드립니다.

마지막에 제 논문을 꼼꼼히 봐주신 상욱선배(교수님보다 선배가 낫죠?) 그리고 제가 2%로 부족할 때마다 일용할 양식으로 배를 채워주던 성훈선배, 내 중학교 동기이자 논문의 마지막에 신경 써준 명국이, 연구실은 다르지만 한 건물에서 2년 동안 생활한 정보보호학 동기 진호, 2학기에 토익을 같이 공부한 남진이, 모두 모두 감사 드립니다.

영경이 말고, 또 다른 나의 동기들. 우리 연구실에서 가장 나이가 많으신 큰 형님 주한식 샘, 약주를 무척 좋아하시는 조선제 샘, 불의를 보면 참지 못하는 justice 맨 정경훈 샘, 옆 집 아저씨처럼 정다운 새 신랑 전준수 샘, 곧 한 아이의 아버지가 될 위성균 샘(형 닮은 딸이 아니라니 천만다행이네요! 후후~), 청춘사업을 끝내지 못하고 아직까지 방황중인 정순이(너무 고르는 거 아니가?)께 감사 드립니다. 동기는 아니지만 잉꼬부부란 이런 것이다라는 것을 몸소 보여주시는 김우경·서선희 샘께도 감사 드립니다.

동병상련이라고 나와 처지가 비슷해 2년 동안 죽이 잘 맞은 경일이(너도 졸업 축하해!), 지금 이 시각에도 열심히 기차 배치에 구슬땀을 흘리고 있을 찬빈이, 일한다고 정신 없을 연정이, 밀양에서 對民 서비스를 하고 있을 정국이, 몇 개월 얼굴을 보지 못한 태헌이와 짝지 윤희, SK맨이라고 자부심이 대단한 성남이, 멀리 떨어져 있는 상미·종훈 커플과 서울로 유학 가서 열심히 공부하는 악바리 종성(열심히 하리라 믿는다.) 좀 늦게 만났지만 토익이란 명분으로 만나 (술로) 친해진 동생 성록이, 자칭 전·컴 학부 여학생들에게 인기 절정이라고 하는 동문 후배 락기(빨리 회사도!)에게도 감사의 말을 전합니다.

마지막으로 날 여기까지 있게 해주신 내가 가장 존경하는 어머니와 최전방에서 나라를 지키고 있을 동생 범렬이, 그리고 2년 동안 물심양면으로 도와주며 말없이 나를 지켜봐 준 은지(넌! 내가 책임진다!)에게 이 글을 바칩니다.

모두 새해에서는 福 많이 받으시고, 하시는 일마다 운수대통 하시길 기원합니다.

2004년 1월 2일 동 틀녘에