대학 무선 랜에 적용되는 새로운 확장 가능 인증 프로토콜

지성배*, 이현록*, 김광조*

*국제정보보호기술연구소, 한국정보통신대학교

A New EAP Method suitable for University WLAN

Sungbae Ji*, Hyunrok Lee*, Kwangjo Kim*

*International Research center for Information Security (IRIS),

Information and Communication University (ICU)

요 약

최근 노트북과 PDA 와 같은 휴대용 정보화 기기의 사용이 증가하면서, 더 많은 무선 랜 기반 시설들이 공항과 대학, 심지어 커피숍 까지 설치되고 있다. 그러나 무선 통신은 보안의 수준이 낮게 설정되어 있다면 근처에 있는 누구라도 모든 무선 트래픽을 가로채어 볼 수 있어 유선 통신에 비해 취약하며, 더 나아가 내부 네트워크 자원에 인가되지 않은 접근과 불법적인 행동을 하는 것이 가능하다.

본 논문은 무선 랜 환경에서 발생할 수 있는 많은 보안 문제점들 가운데 인증 메커니즘에 초점을 맞춘다. 대학교 무선망을 대상 모델로 보안 위협과 그에 상응하는 보안 요구사항을 정의하고 이를 바탕으로 새로운 EAP 인증 방식을 제안한다. 제안 인증 방식은 비인가자의 접근으로부터 무선 랜을 보호하는 효율적인 인증서 기반의 상호 인증 접근법을 택하여 기존의 EAP-MD5 나 LEAP 과 같은 단방향 인증 방식에서 제기된 사전 공격 문제를 해결하였고 대표적인 인증서 기반의 상호 인증 방식인 EAP-TLS 과 비교해 암호화 알고리즘 협상과 인증서 교환이 필요 없다는 장점을 가진다. 또한 빠른 재연결 (Re-association)을 이용하여 자원이 제한된 기기나 실시간 멀티미디어 어플리케이션을 사용한다고 하더라도 서비스 품질을 보장할 수 있도록 기기와 응용프로그램에 따라 다른 보안 수준을 제공한다.

I. 서론

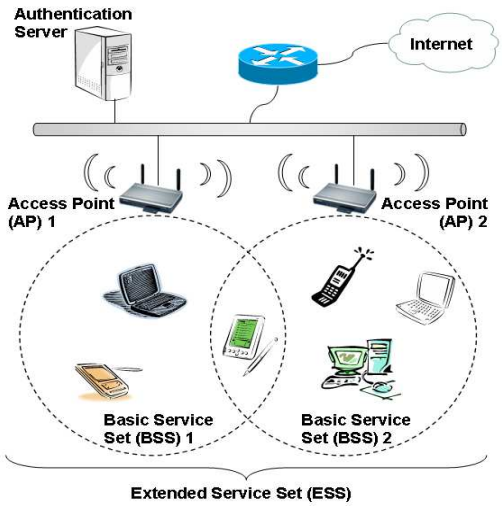
무선 랜은 둘 이상의 컴퓨터를 선을 사용하지 않고 라디오 신호를 이용하여 연결하는 무선 근거리 통신망 [3]으로 (그림 1)은 세 가지 개체들로 구성된 무선 랜의 전형적인 구조이다. 그림에서 노트북, PDA 와 같은 모바일 기기는 Supplicant, Station 혹은 Mobile Node (MN)라고 부른다. Access Point (AP)는 Authenticator 나 Network Access Server (NAS)라고도 불린다. Authentication server (AS)는 인증, 인가, 과금 (AAA: Authentication, Authorization and Accounting)을 담당한다. AS 의 예로 RADIUS [18]와 Diameter [19]가 있다.

해당 구조에서 보듯이, 모바일 노드들이 엑세스 포인트를 통해 서로 통신할 수 있는 기본 서비스 세트 (BSS: Basic Service Set)가 있다. BSS 에 있는 MN 와 AP 사이의 패킷들을 암호화하지 않으면, 누구라도 패킷을 가로채어 기밀 정보를 빼낼 수 있다. 적절한 인증 메커니즘 또한 비인가 사용자가 네트워크에 접근하는 것을 막기 위해 필요하다.

무선 랜에서 사용하는 대표적인 인증 메커니즘은 EAP (확장 가능 인증 프로토콜: Extensible Authentication Protocol) [1][2]이다. EAP 는 무선 랜에서 다수의 인증 방식을 지원하는 보편적인 인증 프레임워크로서 IETF RFC 는 약 40 여개의 EAP 인증 방식을 정의하고 있다.

이중 대표적인 단방향 인증 방식인 EAP-MD5 나 LEAP 은 사전 공격이나 중간자 공격에 취약하나 반면에 단방향 인증 방식의 약점을 극복하기 위한 인증서 기반의 접근법들 중에 가장 안전하다고 평가되고 있는 EAP-TLS 의 경우 공개키 연산 부하뿐만 아니라 암호화 알고리즘 협상과 인증서 체인의 교환이라는 부담을 안고 있다. 이러한 기존의 EAP 인증 방식의 문제점을 해결하기 위해 모든 무선 장비들이 WPA2 (Wi-Fi Protected Access 2)를 지원하는 대학교 무선 랜 환경을 모델로 하여 보다 효율적이고 빠른 EAP 인증 방식을 제안한다. 제안 방식은 하나의 MN 가 현재의 BSS 에서 다른 BSS 로 이동할 때 새로운 AP 와의 빠른 재연결을 지원하여 서비스 품질을 보장할 수 있다는 장점도 가진다.

본 논문 II 장에서는 무선 랜에서 발생할 수 있는 기밀성과 인증에 대한 문제를 설명한다. 두 가지 문제 가운데 인증 메커니즘에 초점을 맞추었는데, 제안된 EAP 인증 방식의 적용과 그 목적을 명확히 하기위해 III 장에서 보안 위협과 그와 관련된 보안 요구사항에 근거한 캠퍼스 무선 랜 모델을 제시한다. 다음의 IV 장, V 장에서는 각각 새롭게 제안한 EAP 인증 방식인 EAP-STLS (Simple Transport Layer Security)를 살펴보고 기존의 EAP 인증 방식과 비교를 통해 성능을 분석한다. 마지막으로 앞으로의 연구 과제와 함께 VI 장에서 결론을 내린다.



(그림 1) 무선 랜의 구조 [3]

II. 관련 연구

무선 랜에서는 유선 랜과는 달리 발생 가능한 보안 문제점과 위협이 상대적으로 많이 존재한다 [4]. 공격자는 잡음과 불법적인 트래픽을 가진 2.4 GHz 스펙트럼을 교란시켜서 물리 계층에 대한 서비스 거부 공격을 할 수 있다. 무선 트래픽은 Kismet [13], airodump [14], AiroPeekNX [15]와 같은 도구로 모니터링 할 수 있다. 무선 네트워크가 WEP 을 사용해 보호되어 있다고 하더라도, 공격자는 AirSnort [16]나 WEPCrack [17]을 사용해서 WEP 키를 찾을 수 있다.

AP 는 Service Set IDentifier (SSID)나 MN 의 MAC 주소를 가지고 MN 을 인증한다. 이러한 인증은 스니핑과 스푸핑 공격 앞에서는 인증이 없는 것과 마찬가지로 취약하기 때문에 많은 암호학적인 보안 기능들이 IEEE 802.1X 에 구현되었다. 대표적인 인증 메커니즘으로 EAP 인증이 있는데, 약 40 여개의 방식들이 IETF RFC 로 정의되어 있다. 그렇지만 일부는 사전 공격 (Dictionary Attack)이나 중간자 공격 (MitM: Man-in-the-Middle attack)에 취약하다. 허위 AP (Rogue AP)는 Evil Twin 으로도 알려진 WiPhishing (Wi-Fi 와 Phishing 의 합성어) 위협을 불러온다.

무선 랜 보안을 이해하기 위한 기본 연구로서, 무선 환경에서 기밀성과 인증에 관한 몇 가지 기초 지식을 살펴보겠다.

1. 기밀성

무선 랜에서 기밀성을 위해, 다음 세 가지의 암호화 방법이 사용된다 [5][6].

1) WEP

WEP (Wired Equivalent Privacy)는 IEEE 802.11 표준의 일부로서 40 또는 104 비트의 키를 가진 RC4 스트림 암호화 알고리즘이다. 그렇지만 선형 무결성 검사 (Linear Integrity Check), 정적인 공유키, IV 의 재사용, 24 비트의 짧은 IV 에 기인해, 통계적인 방법을 도입한 전수 검사 공격에 쉽게 깨어진다.

2) WPA

WPA (Wi-Fi Protected Access) 또는 TKIP (Temporal Key Integrity Protocol)은 128 비트의 임시키 (TK)와 48 비트의 IV 를 가진 RC4 암호화 알고리즘이다. 그러나 능동 공격에 대한 메시지 무결성 부호 (MIC: Message Integrity Code)의 보호가 약하기 때문에 IEEE 802.11i 의 단기적인 해결책으로만 쓰이고 있다.

3) WPA2

WPA2 (Wi-Fi Protected Access 2)또는 CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)는 기존 방식들의 문제점을 해결하기 위해 암호화 방식으로 IEEE 802.11i 에 기본으로 정의되어 있다. AES 128 비트 블록 암호화 알고리즘을 사용하는데 AES 연산에 필요로 하는 처리 능력을 지원하기 위해서는 새로운 하드웨어 (AP 와 네트워크 카드)가 필요하지만 현재 대부분의 무선 랜 장비들은 802.11i 명세 사항을 기본으로 지원한다.

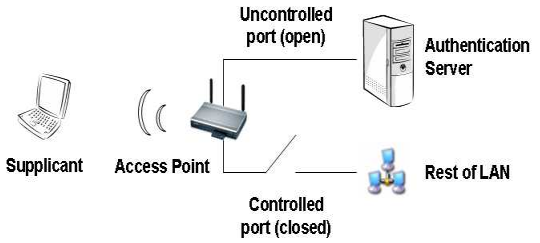
Gin [5]은 WPA2 명세가 적용되었을 때 무선 네트워크의 처리량 (throughput), 지연, 에러 발생률, 다수의 클라이언트와의 상호 작용을 측정하였다. 해당 연구의 실험 결과는 하드웨어 가속 보안 기능을 가진 장비를 사용하면 뚜렷한 성능의 저하 없이도 안전한 무선 네트워크를 설립할 수 있다는 것을 보여준다.

2. 인증

IEEE 802.11i 는 다음과 같은 인증 관련 사항을 정의한다 [5][6].

1) IEEE 802.1X 인증과 키 교환

IEEE 802.1X 는 무선 랜에서 다수의 인증 방식을 지원하는 보편적인 인증 프레임워크인 EAP 를 사용한다. 많은 EAP 인증 방식 중에, EAP-MD5, LEAP (Lightweight EAP), EAP-TLS, EAP-TTLS (EAP-Tunneled TLS), EAP-IKEv2, PEAP (Protected EAP)이 가장 널리 쓰이는 방식이다.



(그림) 포트 기반 인증 [5]

2) 포트 기반 인증 프레임워크 (그림 2)

일반적으로 무선 스테이션은 EAP 인증 방식을 사용해서 RADIUS 인증 서버와 통신한다. 모든 통신은 엑세스 포인트를 통해 보내지고 엑세스 포인트는 단순히 메시지를 중계한다. 일단 인증이 성공적이면, 엑세스 포인트는 인증된 사용자의 접근을 인가한다. 접근의 인가 후, 사용자는 모든 무선 랜 자원에 대해 접근할 수 있다.

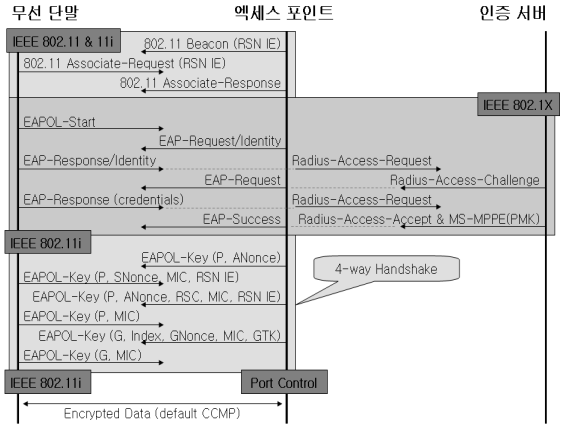
3) 키 교환 및 합의

IEEE 802.1X 인증에서, 각각의 스테이션과 서버는 교환된 키 요소 (Key Material)로부터 하나의 MK (Master Key)를 생성한다. 그리고 각각은 PMK (Pairwise Master Key)를 MK 로부터 유도한다. 서버는 유도된 PMK 를 스테이션에 상응하는 엑세스 포인트로 전달하여 이제 스테이션과 엑세스 포인트는 하나의 PMK 를 공유한다. 인증 후에 이루어지는 Handshake 는 PTK (Pairwise Transient Key), GTK (Group Temporal Key), STAKey (Station to Station Key) 등의 키를 유도한다 [5][6]<표 1>.

<표 1> IEEE 802.11i 키 체계

MK	802.11 정책 결정 토큰
PMK	802.11 정책 집행 토큰
PTK	PMK 와 4-way handshake 로부터 유도 PTK 의 일부를 KCK (Key Confirmation Key), KEK (Key Encryption Key), TK (Temporal Key)로 사용
GTK	브로드캐스트 트래픽 암호화를 위해 사용
STAKey	같은 BSS 에 속한 두 스테이션 사이의 키 (AP 의 암/복호화 부하를 줄임)

(그림 3)은 무선 랩 접근을 위한 IEEE 802.11i 표준의 메시지 흐름을 보여준다. 요약하면, 이 표준의 모든 요소들, 즉, 인증을 위한 IEEE 802.1X, 4-Way Handshake, 키 계층 체계, 암호화 알고리즘 모음이 서로 하나로 연관되어 사용자를 보호하기 위한 강력한 보안 네트워크 (RSN: Robust Security Network)를 만든다고 할 수 있다.



(그림 3) IEEE 802.11i Flow [7]

III. 적용 모델

이번 장에서는 본 논문에서 제안된 새로운 EAP 인증 방식의 실례를 살펴보기 위해 작은 네트워크 사이즈를 가진 무선 랜을 위한 모델을 만들 것이다. 설명의 편의를 위해서 우리가 대학의 학생, 교수, 또는 직원이라고 가정하자.

1. 보안 위협

우선 캠퍼스 무선 랜에서 발생 가능한 보안 위협과 기술적인 문제들을 나열하면 다음과 같다.

- 비인가자가 무선 랜에 접근할 수 있고 이를 이용해 공격을 시도할 수 있다.
- 적법한 사용자라고 하더라도 자신의 신원을 숨기거나 위장하여 학내 자원을 공격할 수 있다.
- 확장 서비스 세트 (ESS: Extended Service Set) 내에 전송되는 패킷을 도청할 수 있다.
- 허위 AP 는 WiPhishing 위협을 불러온다.
- 중간자 공격으로 키가 노출되거나 패킷을 임의로 삽입, 버리거나 재전송 할 수 있다.
- 인증 지연은 특히 실시간 서비스에 심각한 서비스 품질 저하를 초래할 수 있다.

2. 보안 요구사항

위에서 살펴본 보안 위협과 문제을 해결하기 위해서는 다음과 같은 보안 요구사항을 고려해야 한다 [8].

- 상호 인증
- 무결성 보호
- 재전송 보호
- 기밀성
- 키 유도
- 사전 공격에 대한 저지
- 빠른 재연결
- 암호적 바인딩 (Cryptographic Binding)
- 허위 AP 감지

3. 보안 모델을 위한 가정

위에 제시된 보안 요구사항을 만족시키기 위한 모델에서 필요한 가정은 다음과 같다.

- 대학교 무선 랜은 어디서나 네트워크에 접근할 수 있도록 캠퍼스 전체를 대상으로 한다.
- 모든 장치는 WPA2 를 사용해 기밀성을 보장할 수 있도록 하드웨어 가속 보안 기능을 가지고 있다.
- 오직 인가된 사용자만 무선 랜에 접근할 수 있도록 해야 한다.
- 모든 구성원은 학교에 입학할 때 인증서를 발급받는다.
- 모든 인증서는 학사 정책과 규정에 근거해 인증 기관 (CA: certificate authority)에 의해 발급, 폐기, 재발급 된다.
- AS 는 단일 도메인 인증 기관 (SDCA: Single-Domain CA)의 역할을 한다. 따라서 AS 의 인증서를 스스로 서명한다.
- AS 와 AP 는 절대로 공격에 의해 무력화되지 않는다.
- AS 와 AP 는 유선으로 직접 연결되어 있기 때문에 서로를 전적으로 신뢰한다.

일반적으로 대학의 구성원, 특히 학생들은 매 학기 입학하고, 졸업하고, 휴학을 했다가 복학을 한다. 네트워크의 사이즈가 작고 구성원의 수가 적은 경우를 고려하면서도 인증서 기반의 인증 방식을 선택한 이유는 오랜 기간을 놓고 보았을 때 현 구성원 수에 비해 상당히 많은 수의 사용자에 대한 인가 여부를 처리해야 하고 따라서 키 관리 문제가 상당히 복잡해지기 때문이다. 학사 행정과 맞물려 인증서의 발행, 폐기, 만료에 따른 키 관리를 수행한다면 보다 간단하고 명료한 관리가 가능하다.

AS 와 AP 가 직접 유선으로 연결되어야 전적으로 신뢰가 가능하기 때문에 작은 규모의 무선 네트워크 모델을 설정하였다. 또한 무선 네트워크에 AS 나 AP 이외에 다른 호스트가 유선으로 연결되어도 안 된다. 네트워크 주소 체계 중 C 클래스의 네트워크를 고려한다면 연결 가능한 유무선 호스트의 개수는 AS 와 AP 를 포함하여 254 개이다. 네트워크의 사이즈를 크게 만들기 위해 CIDR (Classless Inter-Domain Routing)을 고려하지 않는다면 이 모델은 작은 사이즈의 네트워크에 적합한 모델이다.

일반적인 인증서 기반 인증의 경우에는 인증서 체인의 단편화 (Fragmentation)에 때문에 훨씬 더 많은 수의 Round Trip (RT)이 추가로 필요할 수도 있다. 그러므로 이 모델에서는 AS 가 대학 도메인의 유일한 최상위 인증 기관 (Root CA)의 역할을 동시에 담당한다.

4. 시나리오

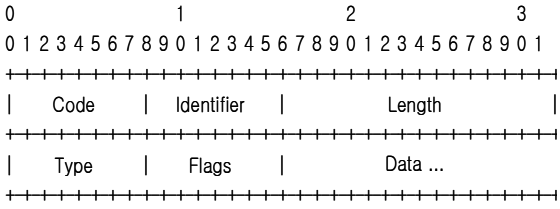
본 논문에서 사용되는 모델에서는 사용자를 크게 두 그룹으로 나누어 생각해 볼 수 있다. 우선 노트북 사용자의 입장에서 생각해보자. 노트북은 이동하면서 사용하기에는 아직 무겁다. 일단 사용자가 도서관과 같은 곳에 자리를 잡으면, 보통은 작업을 끝내기 전까지 그 자리에 머무르는 경향이 있다. 반면에 PDA 를 사용하고 있다고 가정한다면, VOD 사이트에서 놓친 강의를 시청하면서 동시에 캠퍼스 무선 랜 범위(ESS) 어느 곳이라도 갈 수 있다. 일반적으로 PDA 는 노트북에 비해 가용 자원이 제한적이다. 이로부터 다음의 가정을 덧붙인다.

- 노트북은 빈번한 로밍이나 재연결이 필요하지 않다.
- PDA 는 끊기지 않는 로밍을 위한 인증 상한 시간을 고려한 재연결이 이루어져야 한다.

IV. EAP-STLS

본 장에서는 위에 제시된 대학교 무선 랜 모델을 위한 새로운 EAP 인증 방식인 EAP-STLS (EAP-Simple Transport Layer Security)를 제안한다. 제안 프로토콜은 인증 서버와 스테이션의 공개키 암호화 방식을 사용한 상호 인증 방식이라는 점에서 EAP-TLS 와 비슷하다. 그러나 이 방식은 암호화 알고리즘 협상과 인증서 교환이 필요 없다는 점이 제안 프로토콜의 장점이다.

1. 프레임 구성



(그림 4) EAP-STLS 프레임 구성

(그림 4)는 EAP-STLS 에 사용되는 프레임의 포맷을 보여준다 [9]. Code 필드는 1 옥텟(Octet)으로 EAP 패킷의 타입을 식별하게 한다. EAP Code 는 다음과 같이 값이 주어진다.

1 = Request 2 = Response

3 = Success 4 = Failure

한 옥텟의 Identifier 필드는 응답이 요청과 일치가 되는지 알 수 있게 한다. 즉, 응답의 Identifier 필드는 반드시 현재의 미해결된 요청의 Identifier 필드와 일치해야 한다.

Length 필드는 두 옥텟이고 Code, Identifier, Length, Data 필드들을 포함한 EAP 패킷의 길이를 옥텟으로 나타낸다. Length 필드 범위 밖의 옥텟들은 데이터 링크 계층의 패딩으로 취급되어 수신시 반드시 버려진다. 수신한 옥텟 수 보다 큰 값으로 설정된 Length 필드를 가진 메시지는 필히 무시되어야 한다.

Data 필드는 0 또는 그 이상의 옥텟으로 채워진다. Data 필드의 포맷은 Code 필드에 의해 결정된다.

Type 필드는 EAP-STLS 타입이라는 것을 알려주기 위한 필드이다. 현재 값이 할당되지 않은 어떠한 예비 값으로도 지정할 수 있지만 사용을 위해서는 도메인의 모든 멤버에게 사전에 알려줘야 한다.

Flags 필드는 다음과 같은 여덟 비트의 플래그를 가지고 있다.[S F H R R R R R]S = EAP-STLS StartF = EAP-STLS FinishedH = EAP-STLS HandoffR = Reserved.

2. 인증 메시지 흐름

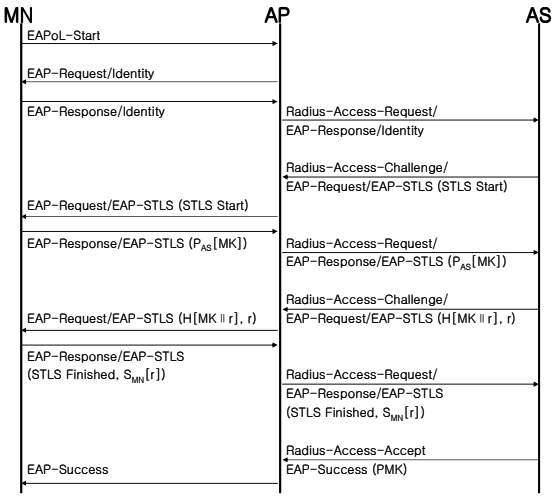
III 장에 제시된 모델을 바탕으로 EAP-STLS 인증을 (그림 5)와 같이 설계하였다. EAP-STLS 에서 STLS 동작은 AS (EAP 인증 서버)와 MN (EAP Peer) 사이에 이루어지고, AP 는 메시지를 전달하는 역할 (Pass-thorough)로 동작한다. 즉, EAP 프레임워크를 따랐기 때문에, AP 를 바꾸지 않고도 구현할 수 있다. MN 와 AS 만 업그레이드하면 되기 때문에 무선 랜 기반 시설의 업그레이드가 쉽고 단순하다.

인증을 시작하기 전에, MN 는 자신의 인증서를 가지고 있어야 한다. 이 발급 절차는 오프라인에서 수행될 수 있다. 예를 들어, 신입생들에게 ID 를 부여하면서 소지자의 인증서가 포함된 스마트 카드를 발급할 수 있다.

IEEE 802.1X 인증은 MN 의 EAPoL-Start 메시지와 함께 시작되어 신원 (Identity)의 요청과 응답으로 이어진다. 실제 EAP 인증 방식은 그 다음에 AS 의 Start 플래그를 설정한 EAP-Request 로 시작한다. MN 은 AS 의 STLS Start 메시지를 받고, 랜덤 Master Key (MK)를 AS 의 공개키로 암호화하여 AS 에게 전달한다. AS 는 MK 를 복호화하고 임의의 수 r 을 생성한다. (MK || r)의 해쉬 값과 r 이 MN 로 다시 보내진다. MN 는 해쉬 값을 검증한 다음에, r 을 개인키로 서명하고 STLS Finish 플래그

비트를 설정하여 보낸다. AS는 MN가 보낸 값이 r 인지 MN 의 공개키로 확인하고, 다음의 의사난수 함수를 이용하여 PMK 를 계산하고 이를 EAP-Success 메시지에 담아 AP 에 전달한다.

PMK = STLS-PRF(MK, "EAP-STLS", r)



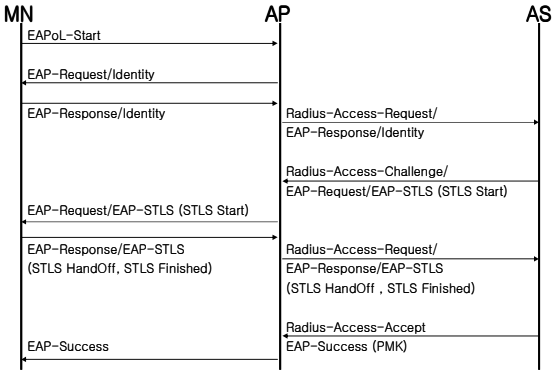
(그림 5) EAP-STLS 인증 흐름

MN 가 EAP-Success 메시지를 받으면 MN 또한 같은 값과 함수를 이용하여 PMK 를 생성한다. 이제 MN 과 AP 는 동일한 PMK 를 공유한다. WPA2 를 지원하는 장치와 SDCA 로서 동작하는 AS 를 가정했기 때문에 프로토콜의 흐름에 어떠한 암호화 알고리즘 협상이나 인증서의 전달이 없어도 가능하다.

한 노드가 현재의 BSS 에서 다른 BSS 로 이동할 때 새로운 AP 와 재연결이 필요하다. 빠른 재연결을 위해 선인증 (Pre-authentication) 방식 및 PMK 관련 정보의 캐시 (cache) 기능의 도입이 제안되었지만 MN 와 재연결하지 않는 AP 에게도 보안 정보 (security context)가 전달되고 AP 는 이를 유지해야 한다는 단점이 있다 [2][10]. 반면에 MN 주도의 재연결은 이러한 문제점을 해결하고 AP 간 프로토콜 (IAPP: Inter-AP Protocol)의 필요 없다 [20].

EAP-STLS 는 MN 주도의 재연결 방식을 EAP 인증 프로토콜에 적용함으로써 빠른 재연결이 가능하도록 하였다. MN 가 Handoff 플래그를 설정하면 (그림 5)의 모든 인증 절차를 밟지 않고도 새로운 AP 와 PMK 를 공유할 수 있다. AS 가 STLS-Handoff/Finished 메시지를 이미 인증된 MN 로부터 기존의 대응되던 AP_a 와는 다른 새로운 AP_b 를 통해 받게 되면, AS 는 MN 의 이전 PMK 를 AP_b 에게 전달한다. 그러면 MN 과 AP_b 는 PMK 를 공유하고 새로운 BSS 를 형성한다 (그림 6).

이러한 빠른 재연결 기능의 사용 여부에 대한 결정은 모바일 노드/클라이언트가 결정한다. 새로 만든 PMK 를 사용하는 것이 완전 순방향 비밀성 (Perfect Forward Secrecy) 측면에서 더 안전하겠지만, MN 가 안전하게 보호될 필요가 없는 작업을 수행하거나 시간 지연에 치명적인 실시간 작업을 하고 있다면, STLS Handoff 를 사용하는 것이 합리적이다. 다시 말하면, EAP-STLS 는 자원이 제한된 기기나 실시간 멀티미디어 어플리케이션을 사용한다고 하더라도 서비스 품질을 보장할 수 있도록 기기와 응용프로그램에 따라 다른 보안 수준을 제공할 수 있다.



(그림 6) EAP-STLS Handoff

재사용되는 PMK 가 지금 노출되지 않은 상태라면, 4-Way Handshake 는 통신하고 있는 스테이션의 동작 여부을 확인하고, 새로운 세션키의 생성을 보장하고, 암호화 키를 설치하고 확인하는 역할을 하므로 어느 정도 수준의 완전 순방향 비밀성을 보장한다.

V. EAP-STLS 보안 성능 분석

본 장에서는 EAP-STLS 을 <표 2>에 제시한 바와 같이 다른 EAP 인증 방식과 비교함으로써 분석한다 [2][11][12]. EAP-MD5 는 단방향 인증 방식이기 때문에 EAP-MD5 는 중간자 공격 (인증 스푸핑)에 취약하다. 또한 EAP-MD5 와 LEAP 은 보안을 패스워드 해쉬에 의존하기 때문에 사전공격에 취약하다.

EAP-TLS [9]의 보안은 매우 높은 수준이지만 비교적 많은 RSA 연산과 RT 이 필요하다. 인증서 기반의 인증의 경우, 인증서 체인의 단편화에 기인한 추가적인 RT 이 필요하게 된다. 일반적으로 단편화된 EAP 패킷은 단편의 개수만큼 많은 RT 를 필요하다. 따라서 단편화를 고려하지 않으면 4.5 RTs 가 소요되지만 실제로는 약 8.5 RTs 가 필요하다. 단편화를 고려하지 않았을 때 TTLS/PEAP 이 6.5 RTs 로 TLS 보다 많은데도 불구하고 단편화를

고려하였을 때 오히려 TLS 가 TTLS/PEAP (8 RTs)보다 더 많은 RTs 가 필요한 것은 그 이유 때문이다.

EAP-TTLS 나 PEAP 은 오직 서버 쪽의 인증서만 필요로 한다. 때문에 프로토콜이 조금 더 가벼워진다. 그렇지만 사용자가 단지 인터넷 연결을 위해 공격자의 유효하지 않은 가짜 인증서를 받아들이면 취약해지는 단점이 있다. 또한 MN 는 어떠한 AP 도 인증을 하지 않기 때문에 중간자 공격이 발생할 수 있다. 이러한 문제는 EAP 메커니즘과 터널 사이의 암호적인 바인딩으로 해결될 수 있지만 그 경우에는 두개의 메시지 (1 RT)가 더 필요하게 된다.

<표 2> 기존 EAP 인증 방식과의 비교

	MD5	LEAP	TLS	TTLS PEAP	STLS
인증	단방향	쌍방향	쌍방향	쌍방향	쌍방향
클라이언트 인증서	X	X	O	X	O
서버인증서	X	X	O	O	O
허위 AP 감지	X	O	X	X	X
RT	2.5	2.5 + 1.5	4.5 / 8.5	6.5 / 8(MD5)	3.5
RSA 연산	X	X	1S 2 v1 ε1 D	- 1 v1 ε1 D	1S 1 v1 ε1 D
재연결	X	X	X	X	O
보안 위협/위협	사전/중간자공격, 세션탈취	사전공격	-	중간자공격	-
보안수준	하	하	상	중상	상
제공자	MS	Cisco	MS	Funk MS	ICU

(기호 S: sign, V: verify, ε: encrypt, D: decryptO: 필요/지원, X: 불필요/미지원)

EAP-STLS 공개키 기술에 기반한 시도-응답을 통해 상호 인증을 한다. STLS 는 TTLS/PEAP 보다 한번의 RSA 서명 연산이 더 필요하지만, 반면에 중간자 공격에 안전하고 훨씬 더 작은 RT 로 수행 가능하다. EAP-STLS 는 인증서를 보내지 않기 때문에 추가적인 RT 가 필요 없다는 장점을 가진다. 또한 STLS Handoff 를 적절히 사용하면 RSA 연산의 부하를 줄일 수 있다. EAP-STLS 는 허위 AP 를 감지하지 못하지만 허위 AP 가 있다고 하더라도 PMK 를 알아낼 수 없고, 4-Way Handshake 로 유도된 PTK 로 WPA2 암호화가 이루어지므로 공격자는 허위 AP 를 이용한 공격을 할 수 없다.

VI. 결론

본 논문에서는 작은 규모의 대학교 무선 랜 모델에 적용 가능한 새로운 EAP 인증 방식이 제안되었다. EAP-STLS 는 적당한 RSA 연산과 적은 수의 RT 로도 가능한 인증서 기반의 상호 인증 방식이다. 제안 프로토콜은 안전한 인증과 가벼운 로밍 부하를 지원하도록 설계되었다.

또한, 제안 인증 방식은 EAP 프레임워크와 EAP 인증 방식 요구사항을 만족하도록 설계되었다. 따라서 AP 는 인증의 대상이 아니고 오직 Pass-through 에이전트로서 동작한다. 제안 인증 프로토콜은 AP 의 업데이트 없이 구현될 수 있지만 EAP 프레임워크와의 호환성을 고려하지 않고 설계한다면 보다 유연하고 최적화된 인증 메커니즘을 구현할 수 있으리라고 생각한다.

본 논문에서는 인증서 폐기를 아직 고려하지 않았다. 향후 인증서 폐기를 고려한 설계시에 인증 시간을 줄이면서 인증서 폐기 목록(CRL: Certificate Revocation List)을 효과적으로 확인할 수 있는 새로운 방식을 고려할 것이다. 또한 EAP-STLS 를 구현해서 실질적인 조건에서 성능을 검증할 필요가 있다.

참고문헌

[1] Bernard Aboba, Larry J. Blunk, John R. Vollbrecht, James Carlson, Henrik Levkowetz, “Extensible Authentication Protocol (EAP),” RFC 3748, June, 2004.

[2] Wikipedia,http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol.

[3] Wikipedia, http://en.wikipedia.org/wiki/WLAN

[4] Jonathan Hassell, “Wireless Attacks and Penetration Testing,”http://www.securityfocus.com/infocus/1783.

[5] Andrew Gin, “The Performance of the IEEE 802.11i Security Specification on Wireless LANs,”http://www.cosc.canterbury.ac.nz/research/reports/HonsReps/2005/hons_0505.pdf,November, 2005.

[6] Jyh-Cheng Chen, Ming-Chia Jiang, and Yi-Wen Liu, “Wireless LAN Security and IEEE 802.11i,” IEEE Wireless Communications, February, 2005.

[7] 강유성, 오경희, 정병호, 정교일, 정찬형, “무선랜 보안 표준 IEEE 802.11i,” TTA Journal, June, 2005.
[8] Dorothy Stanley, Jesse R. Walker, Bernard Aboba, “EAP method Requirements for Wireless LANs,” RFC 4017, March, 2005.
[9] Bernard Aboba, Dan Simon, “PPP EAP-TLS Authentication Protocol,” RFC 2716, October, 1999.
[10] Mohamad Kassab, Abdelfettah Belghith,Jean-Marie Bonnin, Sahbi Sassi, “Fast Pre-Authentication based on Proactive Key Distribution for 802.11 Infrastructure Networks,” WMuNeP'05, October, 2005.
[11] Mohamad Badra, Pascal Urien, and Ibrahim Hajjeh, “Flexible and fast security solution for wireless LAN,” Pervasive and Mobile Computing, June, 2006.
[12] Intel,http://www.intel.com/support/wireless/wlan/sb/cs-008413.htm.
[13] Kismet, http://www.kismetwireless.net.
[14] airodump,http://www.wirelessdefence.org/Contents/Aircrack_airodump.htm.
[15] AiroPeek NX,http://www.wildpackets.com/products/airopeek/airopeek_nx/overview.
[16] AirSnort, http://airsnort.shmoo.com.
[17] WEPCrack,http://www.wirelessdefence.org/Contents/WEPCrackMain.htm.
[18] Carl Rigney, Allan C. Rubens, William A.Simpson, Steve Willens, “Remote Authentication Dial In User Service (RADIUS),” RFC 2865, June, 2000.
[19] Pat Calhoun, John Loughney, Jari Arkko,Erik Guttman, Glen Zorn, “Diameter Base Protocol,” RFC 3588, September, 2003.
[20] Daniel Faria, David Cheriton, “DoS and Authentication in Wireless Public Access Network,” WiSe'02, September, 2002.