백서

# 802.11 무선 LAN 보안에 대한 포괄적 검토 및 Cisco Wireless Security Suite


## 작성자

Pejman Roshan은 무선 네트워킹 제품 담당자로서 본 백서의 작성자입니다.


## 1. 개요

1999년 IEEE 802.11b 표준으로 승인된 이후 무선 LAN은 더욱 널리 사용되기 시작했습니다. 오늘날 무선 LAN은 기업의 회의실, 산업용 창고, 인터넷 이용이 가능한 강의실을 비롯하여 심지어 커피숍에 이르기까지 광범위하게 설치되어 있습니다.

이와 같은 IEEE 802.11 기반 무선 LAN의 사용이 증가하자 네트워크 관리자와 정보 보안 관리자에게는 모두 새로운 과제가 대두되었습니다. 유선 이더넷 설치가 비교적 단순한 것과 달리 802.11 기반의 무선 LAN은 클라이언트 스테이션에서 수신할 수 있도록 무선 주파수(RF) 데이터를 송출합니다. 이로 인해 802.11 표준을 확장하는 것과 관련된 복잡한 보안 문제가 새롭게 제기되었습니다.

IEEE 802.11 사양 중에서 802.11b, 802.11a 및 802.11g에 적용되는 보안 문제에 대해 집중적인 검토가 이루어졌습니다. 검토 결과 IEEE 802.11 사양에서 규정한 인증, 데이터 프라이버시 및 메시지 무결성 메커니즘에 대해 여러 가지 취약성이 있음이 알려졌습니다. 이 백서에서 다룰 내용은 다음과 같습니다.

- IEEE 802.11 사양의 8절에 명시된 인증 및 데이터 프라이버시 기능에 대한 검토
- 이와 같은 기능이 갖고 있는 보안상의 취약성과 관리 문제
- 802.11 보안 표준을 확장하는 것만으로도 보안 문제를 효과적으로 해결할 수 있는 방법
- Cisco Wireless Security Suite를 비롯한 무선 LAN의 보안 기능을 향상하기 위해 Cisco Systems 아키텍처 검토
- 장기적인 보안 기능 향상 방법 모색

## 2. 802.11 인증 및 인증상의 단점

무선 LAN에서는 브로드캐스트 특성 때문에 다음을 추가해야 합니다.

- 네트워크 리소스에 대한 무단 액세스를 방지하기 위한 사용자 인증
- 전송된 데이터의 무결성 및 프라이버시를 보호하기 위한 데이터 프라이버시

802.11 사양에서는 무선 LAN 클라이언트 인증을 위해 개방형 인증과 공유 키 인증이라는 두 가지 메커니즘을 규정하고 있습니다. 그 밖에 SSID(Service Set Identifier)와 클라이언트 MAC(Media Access Control) 주소에 의한 인증이라는 메커니즘도 널리 사용됩니다. 이 단원에서는 각각의 인증 방법과 그에 대한 단점을 설명합니다.

정확한 WEP(Wired Equivalent Privacy) 키가 없는 클라이언트는 액세스 포인트와 데이터를 주고 받을 수 없기 때문에 WEP 키를 사용하면 일종의 액세스를 컨트롤하는 기능을 얻을 수 있습니다. IEEE 802.11 위원회가 채택한 암호화 체계인 WEP는 40비트 또는 104비트 키 강도의 암호화를 제공합니다. 이어지는 단원에서는 WEP와 WEP의 단점에 대해 자세히 설명합니다.

### 2.1. SSID(Service Set Identifier)

SSID는 무선 LAN을 논리적으로 분할할 수 있는 구조를 가지고 있습니다. 일반적으로 적절한 SSID로 클라이언트를 구성해야 무선 LAN에 액세스할 수 있습니다. SSID는 데이터 프라이버시 기능을 제공하지 않으며 실제로 클라이언트를 액세스 포인트에 인증하지도 않습니다.

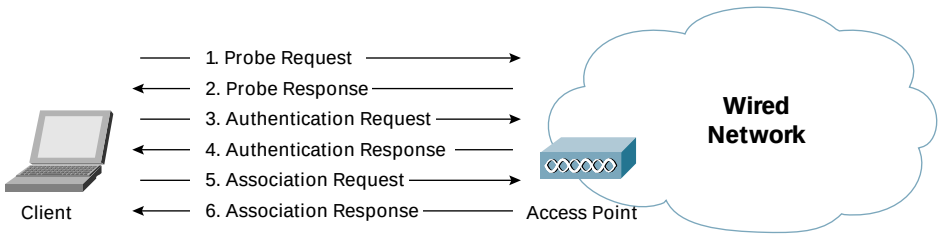
### 2.2. 802.11 스테이션 인증

802.11 사양에서 인증은 사용자를 인증하는 대신 무선 기지국 또는 무선 장치를 인증하는 방식을 사용합니다. 802.11 사양에서는 개방형 인증과 공유 키 인증이라는 두 가지 인증 모드를 제공합니다.

802.11 클라이언트 인증 프로세스는 다음과 같은 트랜잭션으로 구성됩니다(그림 1).

1. 클라이언트가 모든 채널에서 프로브 요청 프레임을 송출합니다.
2. 범위 내에 있는 액세스 포인트가 프로브 응답 프레임을 통해 응답합니다.
3. 클라이언트가 액세스에 가장 적합한 액세스 포인트(AP)를 결정한 후 인증 요청을 전송합니다.
4. 액세스 포인트가 인증 응답을 전송합니다.
5. 인증이 성공하면 클라이언트가 액세스 포인트에 연결 요청 프레임을 전송합니다.
6. 액세스 포인트가 연결 응답을 통해 응답합니다.
7. 클라이언트가 액세스 포인트로 트래픽을 보낼 수 있게 됩니다.

**그림 1: 802.11 클라이언트 인증 프로세스**



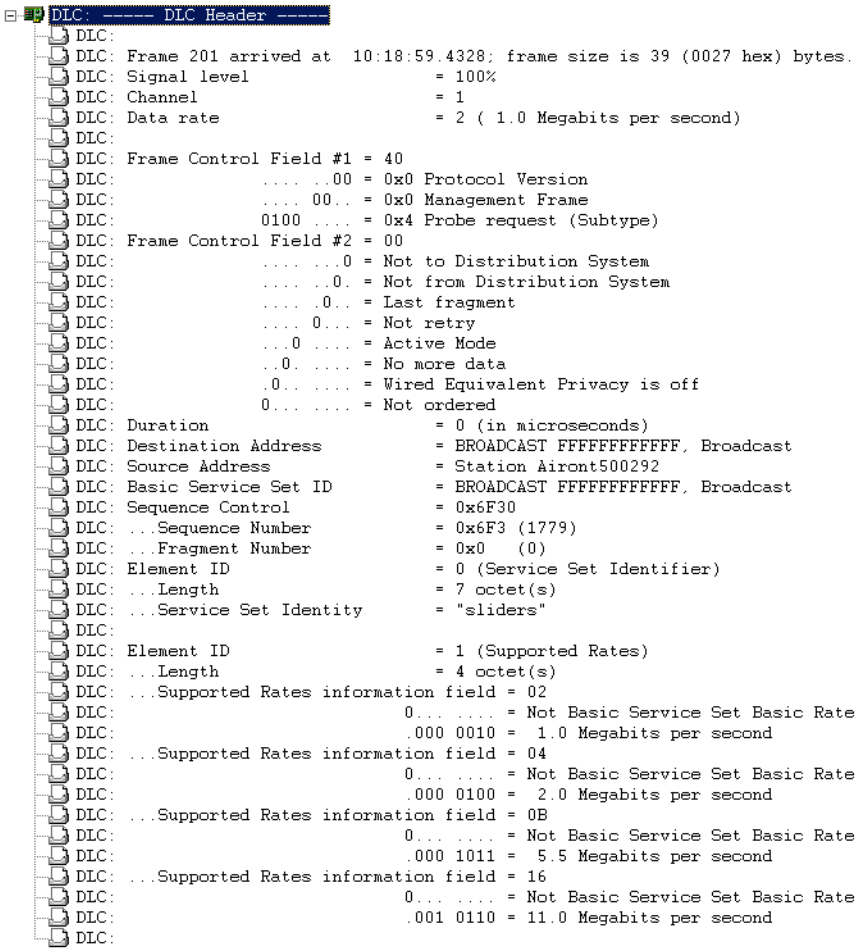

이후의 네 단원에서는 클라이언트 인증의 개별적인 프로세스에 대해 자세히 설명합니다.

### 2.2.1. 프로브 요청 및 응답

클라이언트가 매체에서 활성화되면 프로브 요청 프레임으로 알려진 802.11 관리 프레임을 사용하여 무선 전파 범위에서 액세스 포인트를 검색합니다. 프로브 요청 프레임을 클라이언트가 지원하는 모든 채널로 전송하여 SSID 및 클라이언트 요청 데이터 속도와 일치하는 범위 내에 있는 모든 액세스 포인트를 찾아냅니다(그림 2).

범위 내에 있고 프로브 요청 기준도 만족하는 모든 액세스 포인트는 동기화 정보 및 액세스 포인트 로드를 포함하는 프로브 응답 프레임을 통해 응답합니다. 클라이언트는 지원되는 데이터 속도와 액세스 포인트 로드를 검토하여 어떤 액세스 포인트를 연결할 것인지 결정할 수 있습니다. 클라이언트가 연결할 최적의 액세스 포인트를 결정하면 802.11 네트워크 액세스의 인증 단계로 넘어갑니다.

**그림 2: 프로브 요청 프레임**



### 2.2.2. 개방형 인증

개방형 인증은 Null 인증 알고리즘을 사용합니다. 액세스 포인트는 모든 인증 요청을 승인합니다. 이와 같은 알고리즘을 사용하는 것이 무의미해 보일 수도 있지만 개방형 인증은 802.11 네트워크 인증에 엄연히 포함됩니다. 1997 802.11 사양에서 인증은 연결 중심으로 이루어집니다. 인증을 위한 요구 사항을 두는 것은 장치가 신속하게 네트워크에 액세스할 수 있도록 하기 위한 것입니다. 뿐만 아니라 802.11 사양을 준수하는 장치들은 대개 바코드 판독기와 같은 휴대용 데이터 수집 장치이며 복잡한 인증 알고리즘에 필요한 CPU 기능을 가지고 있지 않습니다.

개방형 인증은 다음과 같이 두 개의 메시지로 구성됩니다.

- 인증 요청(그림 3)
- 인증 응답(그림 4)

**그림 3: 개방형 인증 요청**

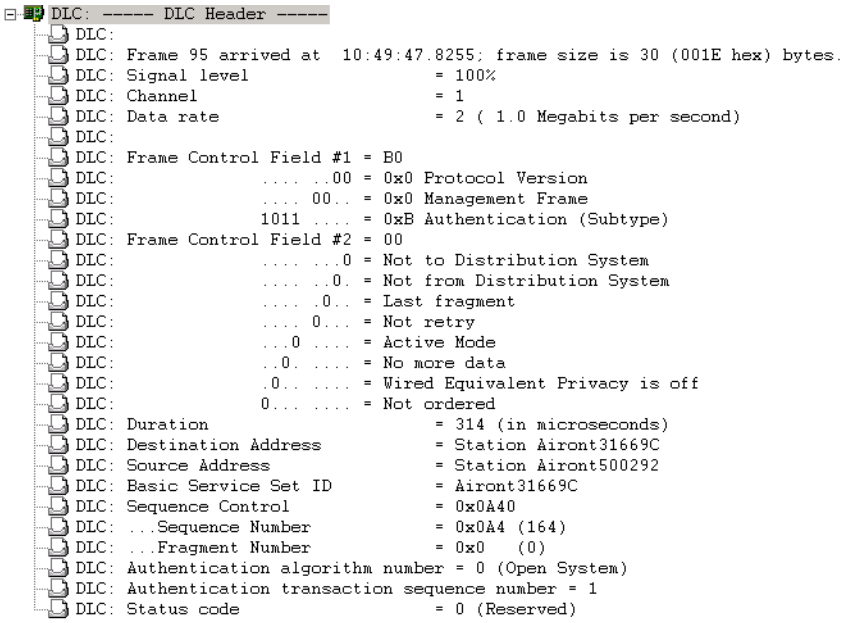
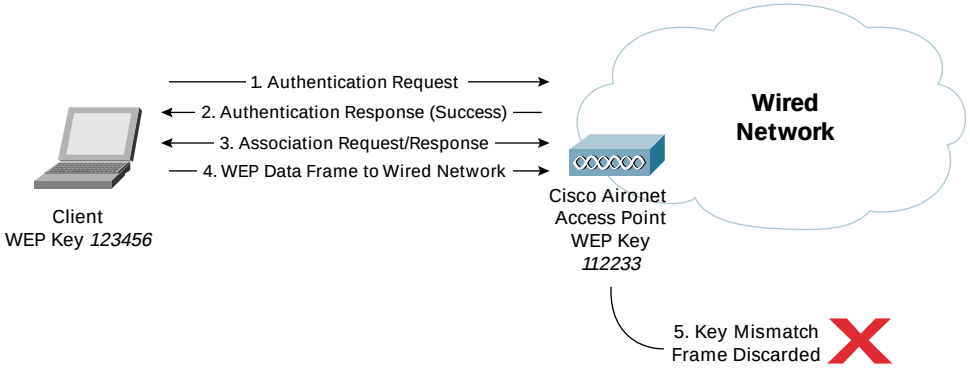


그림 4: 개방형 인증 응답

```
DLC: ----- DLC Header -----
DLC:
DLC: Frame 97 arrived at  10:49:47.8279; frame size is 30 (001E hex) bytes.
DLC: Signal level                  = 81 %
DLC: Channel                       = 1
DLC: Data rate                     = 22 (11.0 Megabits per second)
DLC:
DLC: Frame Control Field #1 = B0
DLC:              .... ..00 = 0x0 Protocol Version
DLC:              .... 00.. = 0x0 Management Frame
DLC:              1011 .... = 0xB Authentication (Subtype)
DLC: Frame Control Field #2 = 00
DLC:              .... ...0 = Not to Distribution System
DLC:              .... ..0. = Not from Distribution System
DLC:              .... .0.. = Last fragment
DLC:              .... 0... = Not retry
DLC:              ...0 .... = Active Mode
DLC:              ..0. .... = No more data
DLC:              .0.. .... = Wired Equivalent Privacy is off
DLC:              0... .... = Not ordered
DLC: Duration                      = 258 (in microseconds)
DLC: Destination Address           = Station Aironf500292
DLC: Source Address                = Station Aironf31669C
DLC: Basic Service Set ID          = Aironf31669C
DLC: Sequence Control              = 0xED50
DLC: ...Sequence Number            = 0xED5 (3797)
DLC: ...Fragment Number            = 0x0   (0)
DLC: Authentication algorithm number = 0 (Open System)
DLC: Authentication transaction sequence number = 2
DLC: Status code                   = 0 (Successful)
```

개방형 인증을 통해 모든 장치의 네트워크 액세스를 얻을 수 있습니다. 네트워크에서 암호화가 이루어지지 않는 경우에는 액세스 포인트의 SSID를 알고 있는 장치가 네트워크 액세스 권한을 갖게 됩니다. 액세스 포인트에서 WEP 암호화가 이루어지는 경우에는 WEP 키 자체가 액세스를 컨트롤하는 방법으로 사용됩니다. 장치가 올바른 WEP 키를 갖고 있지 않으면 인증이 성공했더라도 장치는 액세스 포인트를 통해 데이터를 전송할 수 없습니다. 또한 액세스 포인트에서 수신한 데이터를 암호 해독할 수도 없습니다(그림 5).

그림 5: 서로 다른 WEP 키를 사용한 개방형 인증

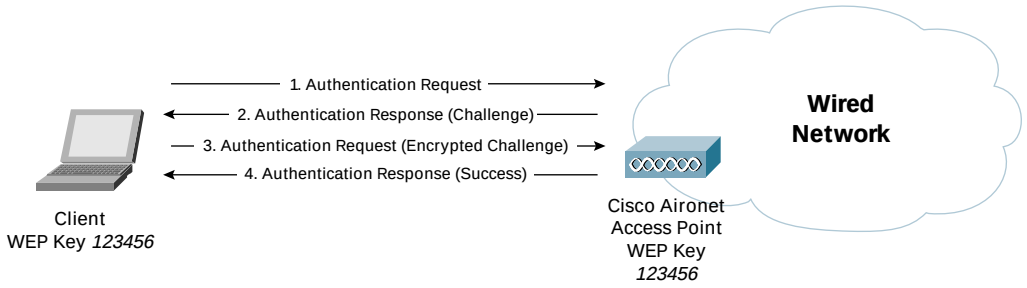


### 2.2.3. 공유 키 인증

공유 키 인증은 802.11 표준에서 규정한 두 번째 인증 모드입니다. 공유 키 인증을 위해서는 클라이언트가 정적 WEP 키를 구성해야 합니다. 그림 6은 공유 키 인증 프로세스를 보여줍니다.

1. 클라이언트가 공유 키 인증을 요청하는 액세스 포인트로 인증 요청을 전송합니다.
2. 액세스 포인트가 해당 텍스트를 포함하는 인증 응답을 통해 응답합니다.
3. 클라이언트가 로컬로 구성된 WEP 키를 사용하여 해당 텍스트를 암호화하고 후속 인증 요청을 통해 응답합니다.
4. 액세스 포인트가 인증 요청의 암호를 해독하고 원래의 해당 텍스트를 검색할 수 있는 경우, 액세스 포인트가 클라이언트 액세스를 승인하는 인증 응답을 통해 응답합니다.

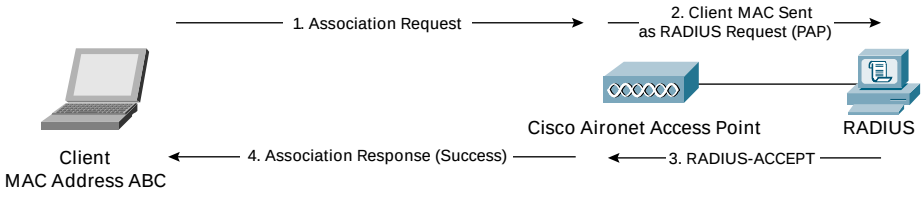
**그림 6: 공유 키 인증 프로세스**




### 2.2.4. MAC 주소 인증

MAC 주소 인증은 802.11 표준에서 규정되지 않았지만 시스코를 비롯한 많은 공급업체가 이 방식을 지원합니다. MAC 주소 인증은 로컬로 구성된 허용 주소 목록 또는 외부 인증 서버를 기준으로 클라이언트의 MAC 주소를 확인합니다(그림 7). MAC 인증은 802.11에서 규정한 개방형 인증 및 공유 키 인증을 확장함으로써 장치가 네트워크에 무단으로 액세스할 수 있는 가능성을 줄이는 데 사용됩니다.

**그림 7: MAC 주소 인증 프로세스**



## 2.3. 인증상의 취약성

### 2.3.1. SSID 사용

SSID는 액세스 포인트 비콘(beacon) 메시지에서 일반 텍스트 형식으로 통지됩니다(그림 8). 사용자가 비콘 메시지를 볼 수 있긴 하지만 도청자는 Sniffer Pro와 같은 802.11 무선 LAN 패킷 분석기를 사용하여 SSID를 쉽게 확인할 수 있습니다. 시스코를 비롯한 액세스 포인트 제공업체들은 비콘 메시지에서 SSID 브로드캐스트가 불가능하도록 설정할 수 있는 옵션을 제공합니다. 그렇다 하더라도 액세스 포인트에서 프로브 응답 프레임을 찾아내어 SSID를 확인할 수 있습니다(그림 9).

SSID는 보안 메커니즘으로 고안된 것도 아니고 그러한 목적으로 사용하는 것도 아닙니다. 또한 SSID 브로드캐스트를 사용할 수 없도록 설정하면 복합 클라이언트 설치 시 Wi-Fi 상호 운영성에 악영향을 미칠 수도 있습니다. 따라서 SSID를 보안 모드로 사용하지 않는 것이 좋습니다.

그림 8: 액세스 포인트 비콘(beacon) 프레임의 SSID

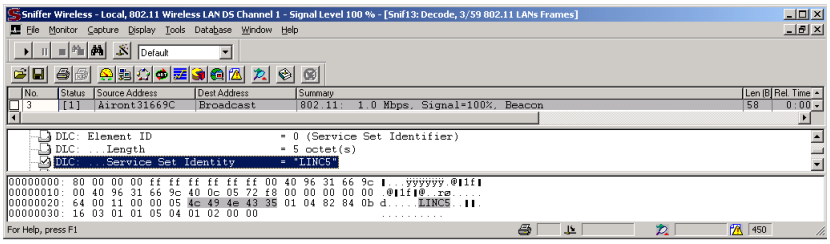
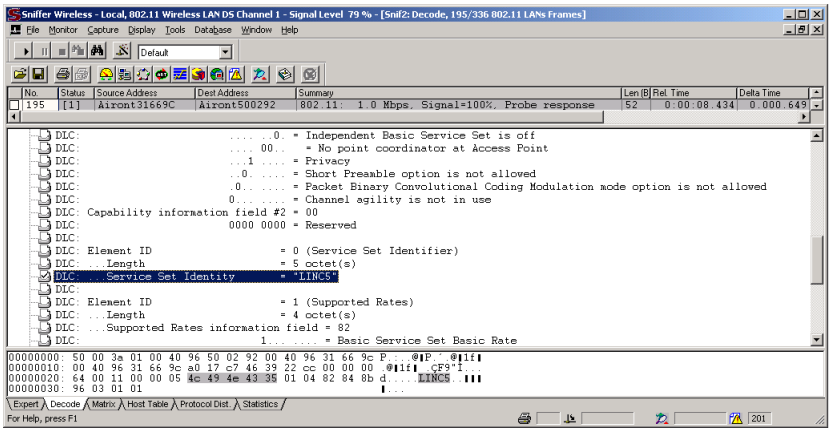



그림 9: 액세스 포인트 프로브 응답 프레임의 SSID




### 2.3.2. 개방형 인증의 취약성

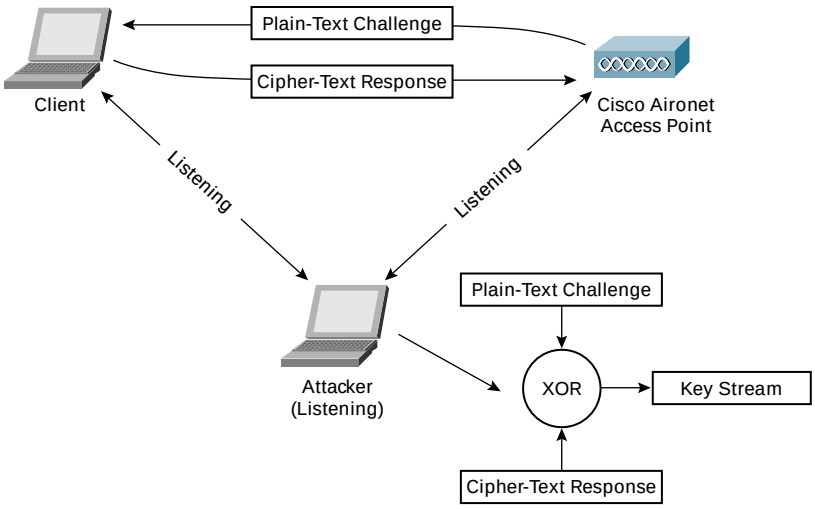
개방형 인증은 액세스 포인트에서 클라이언트가 유효한지를 확인할 수 있는 어떤 방법도 제공하지 않습니다. 이러한 특성은 무선 LAN에서 WEP 암호화가 구현되지 않는 경우에는 중대한 보안상의 취약성입니다. 따라서 WEP 암호화 기능이 없는 무선 LAN은 설치하지 않는 것이 좋습니다. 공중 무선 LAN을 설치하는 경우처럼 WEP 암호화가 필요하지 않거나 구현하기에 적절하지 않은 경우에는 SSG(Service Selection Gateway)를 구현하여 강력한 상위 계층 인증을 제공할 수 있습니다.

### 2.3.3. 공유 키 인증의 취약성

공유 키 인증을 사용하려면 클라이언트가 미리 공유한 WEP 키를 사용하여 액세스 포인트에서 전송된 해당 텍스트를 암호화해야 합니다. 액세스 포인트는 공유 키 응답을 암호 해독하고 해당 텍스트가 동일한지 확인하여 클라이언트를 인증합니다.

해당 텍스트를 교환하는 프로세스는 무선 링크 상에서 이루어지며 중간자(man-in-the-middle) 공격에 대한 취약성을 갖고 있습니다. 도청자는 일반 텍스트 형식의 해당 텍스트와 암호문의 응답을 모두 캡처할 수 있습니다. WEP 암호화에서는 키 스트림을 포함한 일반 텍스트에 대해 배타적 논리합(XOR) 함수를 실행하여 암호문을 생성합니다. XOR 함수가 일반 텍스트에서 실행되고 암호문에 대해 XOR 연산이 실행되면 결과는 키 스트림이 된다는 사실을 염두에 두어야 합니다. 따라서 도청자는 프로토콜 분석기를 사용하여 공유 키 인증 프로세스를 찾아내는 것만으로도 키 스트림을 쉽게 추론할 수 있습니다(그림 10).

**그림 10: 공유 키 인증의 취약성**




### 2.3.4. MAC 주소 인증의 취약성

MAC 주소는 802.11 사양의 규정에 따라 보안 되지 않은 상태로 전송됩니다. 따라서 MAC 인증을 사용하는 무선 LAN에서 네트워크 침입자는 올바른 MAC 주소를 "속이는" 것으로 MAC 인증 프로세스를 중단시킬 수도 있습니다.

UAA(universally administered address)를 LAA(locally administered address)로 덮어쓸 수 있는 802.11 네트워크 인터페이스 카드(NIC)에서는 MAC 주소를 속일 수 있습니다. 네트워크 침입자는 프로토콜 분석기를 사용하여 BSS(business support system)의 유효 MAC 주소와 유효 MAC 주소를 속이기 위한 LAA 호환 NIC를 찾아낼 수 있습니다.

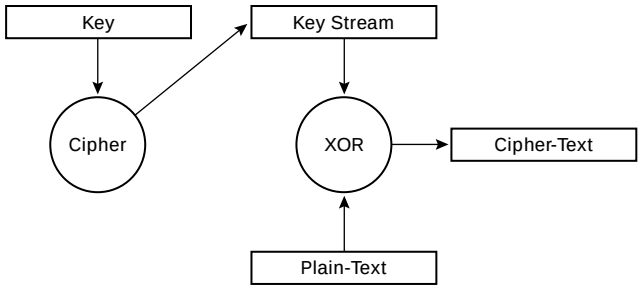
## 3. WEP 암호화 및 단점

WEP는 대칭 키 스트림 암호인 RC4 알고리즘을 사용합니다. 앞에서도 설명했듯이 프레임 교환이 성공적으로 이루어지려면 암호화 키가 클라이언트와 액세스 포인트에서 모두 일치해야 합니다. 다음 단원에서는 스트림 암호에 대해 살펴보고 암호의 작동 원리 및 블록 암호와의 비교에 대해 설명합니다.

### 3.1. 스트림 암호 및 블록 암호

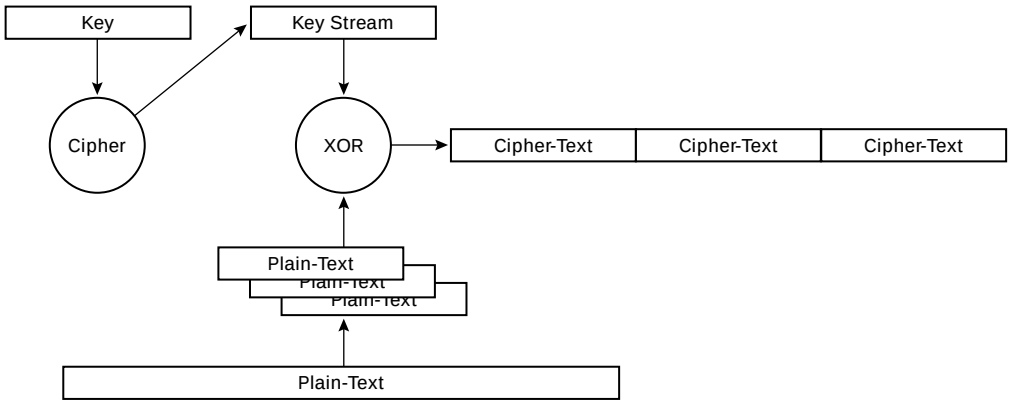
스트림 암호는 키에서 키 스트림을 생성하고 일반 텍스트 데이터를 포함한 키 스트림에서 XOR 함수를 실행함으로써 데이터를 암호화합니다. 키 스트림의 크기는 암호화할 일반 텍스트 프레임의 크기와 일치하기만 한다면 어떤 크기라도 상관 없습니다(그림 11).

**그림 11: 스트림 암호 실행**



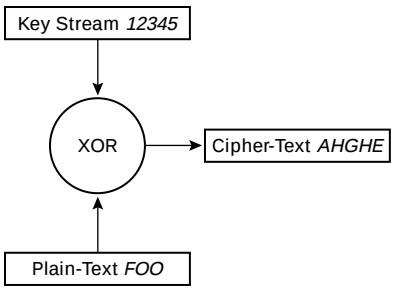

블록 암호는 다양한 크기의 프레임보다는 정해진 블록의 데이터를 처리합니다. 블록 암호는 프레임을 미리 정해진 크기의 여러 블록으로 나누고 각각의 블록에 대해 XOR 함수를 실행합니다. 각 블록은 크기가 미리 정해져 있어야 하며 나머지 프레임 조각은 적절한 크기의 블록으로 채워집니다(그림 12). 예를 들어 블록 암호가 프레임을 16바이트 블록으로 나누어 38바이트 프레임을 암호화한다면 블록 암호는 프레임을 16바이트 블록 두 개와 6바이트 블록 하나로 나눕니다. 6바이트 블록에는 10바이트의 패딩이 채워져 16바이트 크기의 블록이 됩니다.

**그림 12: 블록 암호 실행**



앞에서 설명한 스트림 암호와 블록 암호에 대한 암호화 프로세스를 ECB(Electronic Code Book) 모드 암호화라고 합니다. ECB 모드 암호화를 사용하면 동일한 일반 텍스트 입력은 항상 동일한 암호문 출력을 생성합니다. 그림 13에서 보듯이 "FOO"라는 입력 텍스트는 항상 동일한 암호문을 생성합니다. 도청자는 암호문의 패턴을 익혀서 원래의 일반 텍스트가 어떤 것이었는지 추측해 낼 수 있기 때문에 이러한 방법은 보안상의 위협이 될 수 있습니다.

**그림 13: ECB(Electronic Code Book) 암호화**



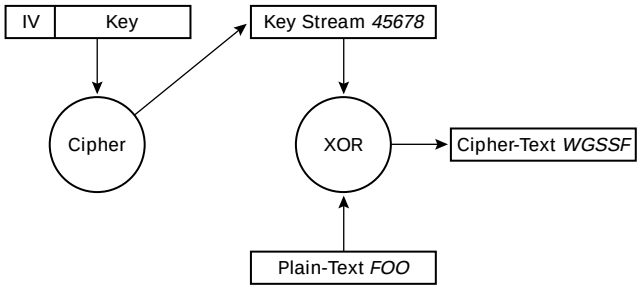

이와 같은 문제를 해결하기 위한 암호화 방법은 다음 두 가지입니다.

- 초기화 벡터
- 피드백 모드

### 3.1.1. 초기화 벡터

초기화 벡터(IV)는 키 스트림을 변경하는 데 사용됩니다. IV는 키 스트림이 생성되기 전에 기본 키에 연결되는 숫자 값입니다. IV가 변경될 때마다 키 스트림도 변경됩니다. 그림 14에서는 다른 암호문을 생성하기 위해 IV가 키 스트림을 확장한 상태에서 XOR 함수를 실행한 동일한 일반 텍스트 "FOO"를 보여줍니다. 802.11 표준에 따르면 IV가 프레임 단위로 변경되는 방식이 더욱 좋습니다. 이러한 방식으로 동일한 패킷이 두 번 전송되면 결과적으로 암호문은 각각의 전송마다 달라집니다.

**그림 14: 초기화 벡터(IV)를 사용한 암호화**




IV는 40비트 WEP 키를 64비트로, 104비트 WEP 키를 128비트로 확장하는 24비트 값(그림 15)을 가집니다. IV는 프레임 헤더에서 보안 되지 않은 상태로 전송되므로 수신 스테이션은 IV 값을 알아 내어 프레임을 암호 해독할 수 있습니다(그림 16). 40비트 및 104비트 WEP 키는 64비트 및 128비트 WEP 키로 사용되는 경우가 많지만 IV가 암호화되지 않은 상태로 전송되므로 유효한 키 강도는 각각 40비트와 104비트에 지나지 않습니다.

그림 15: WEP 암호화 프레임의 초기화 벡터

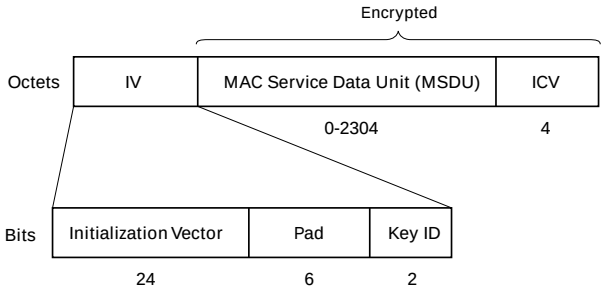
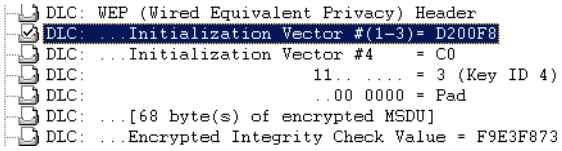



그림 16: 802.11 프로토콜 디코드의 초기화 벡터

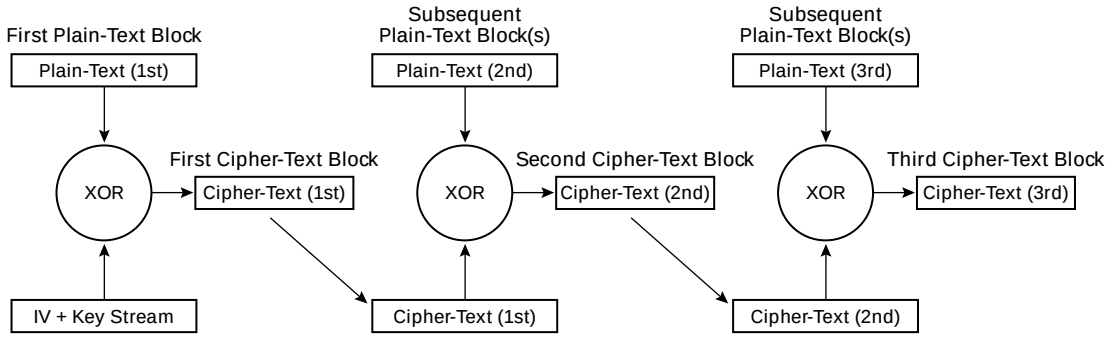



### 3.1.2. 피드백 모드

피드백 모드는 암호화 과정에서 일반 텍스트 메시지가 동일한 암호문을 생성하지 못하도록 암호화 프로세스를 일부 수정한 것입니다. 피드백 모드는 일반적으로 블록 암호와 함께 사용되며, 가장 일반적인 피드백 모드는 CBC(cipher block chaining) 모드로 알려져 있습니다.

CBC 모드의 전제 조건은 이전의 암호문 블록을 통해 일반 텍스트 블록에서 XOR 함수를 실행하여야 한다는 것입니다. 첫번째 블록에는 이전의 암호문 블록이 없기 때문에 키 스트림을 변경하기 위해 IV를 사용합니다. 그림 17은 CBC 모드의 작동을 나타냅니다. 그 밖의 사용 가능한 피드백 모드는 여러 가지가 있으며 그 중 일부에 대해서는 뒷부분에서 설명합니다.

그림 17: CBC 모드 블록 암호



### 3.2. 통계 키 파생 – 소극적인 네트워크 공격

2001년 8월 암호 분석가인 Fluhrer, Mantin, Shamir는 무선 LAN에서 특정 프레임을 소극적으로 수집함으로써 WEP 키를 파생할 수 있다는 사실을 확인했습니다. 취약성은 WEP가 RC4 스트림 암호에서 KSA(key scheduling algorithm)를 구현하는 방식이었습니다. 여러 개의 IV(약한 IV라고도 함)는 통계 분석이 끝나면 키 바이트를 노출할 수 있습니다. AT&T/Rice University의 연구원들과 AirSnort 애플리케이션 개발자들은 이러한 취약성을 구현해 본 결과 40비트 또는 128비트 키 길이를 지닌 WEP 키가 겨우 400만 프레임 이후에 파생될 수 있다는 사실을 확인했습니다. 이것은 사용량이 많은 무선 LAN의 경우에는 대략 네 시간 정도면 128비트 WEP 키가 파생됨을 의미하는 것입니다.

이러한 취약성 때문에 WEP를 사용하는 것은 비효율적입니다. 동적 WEP 키를 사용하면 이러한 취약성을 완화할 수 있지만 그만큼의 노력이 있어야만 알려진 문제를 해결할 수 있습니다. 이와 같은 취약성을 없애려면 WEP 키를 강화하는 메커니즘이 필요합니다.

### 3.3. 귀납적 키 파생 – 적극적인 네트워크 공격

귀납적 키 파생은 무선 LAN에서 정보를 강제로 끌어와 키를 파생시키는 프로세스로서 적극적인 네트워크 공격이라고도 합니다. 스트림 암호에 관한 단원에서도 언급했듯이 암호문을 생성하기 위해 스트림 암호를 통해 XOR 함수를 실행하면 암호화할 수 있습니다. 귀납적 네트워크 공격은 이러한 전제 조건에서 이루어집니다.

귀납적 키 파생 공격의 한 형태인 중간자(Man-in-the-middle) 공격은 효과적인 메시지 무결성이 없기 때문에 802.11 네트워크에 영향을 미칩니다. 프레임 수신자는 전송 과정에서 프레임이 변경되었는지 여부를 확인할 수 없습니다. 뿐만 아니라 메시지 무결성을 제공하는 데 사용하는 ICV(Integrity Check Value)는 CRC32(32-bit cyclic redundancy check) 체크섬 기능을 사용합니다. CRC32 값은 비트 플립핑 공격에 취약하므로 이를 사용하는 것은 효율적이지 않습니다. 메시지 무결성 검사를 위한 효율적인 메커니즘이 없는 무선 LAN은 비트 플립핑 공격 및 IV 재생 공격과 같은 중간자 공격에 취약합니다.

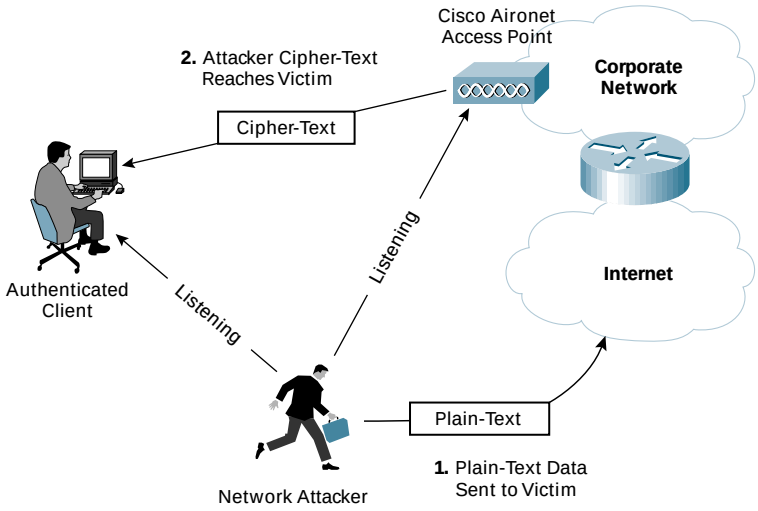
#### 3.3.1. 초기화 벡터 재생 공격

초기화 벡터(IV) 재생 공격은 이론 뿐만 아니라 실제로도 구현되었던 네트워크 공격입니다. 다양한 형태의 네트워크 공격이 있지만 귀납적 성격을 명백히 보여주는 공격은 아래에서 설명합니다(그림 18).

1. 관찰할 수 있는 무선 LAN 클라이언트로 알려진 일반 텍스트 메시지(예: 전자 메일 메시지)가 전송됩니다.
2. 네트워크 침입자가 무선 LAN을 스니핑하여 예상되는 암호문을 찾습니다.
3. 네트워크 침입자가 알려진 프레임을 발견하여 키 스트림을 파생시킵니다.
4. 네트워크 침입자가 관찰했던 프레임과 동일한 IV/WEP 키 쌍을 사용하여 키 스트림을 "확장"시킵니다.

이것은 IV와 기본 WEP 키를 반복적으로 다시 사용하거나 재생함으로써 네트워크를 파괴하기에 충분히 큰 키 스트림을 생성할 수 있다는 원리를 이용한 공격입니다.

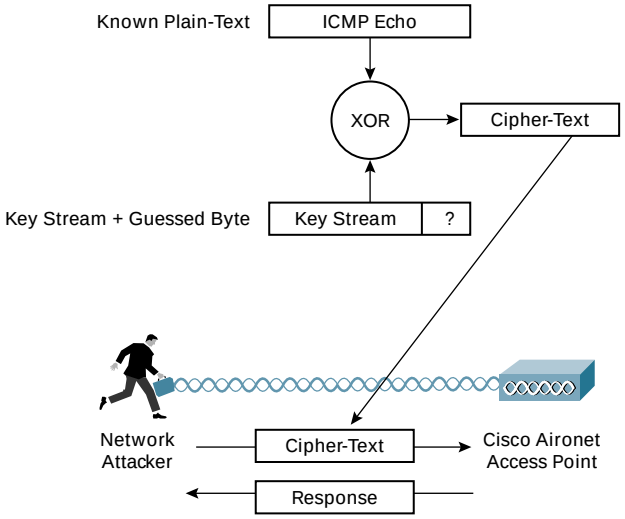
그림 18: 초기화 벡터 재사용으로 인한 취약성




키 스트림이 일정한 크기의 프레임으로 파생되고 나면 필요한 어떤 크기로든 키 스트림을 "확장"할 수 있습니다. 이 프로세스는 아래에서 설명합니다(그림 19).

1. 네트워크 침입자는 알려져 있는 키 스트림의 크기보다 1바이트 큰 프레임을 구성할 수 있습니다. 액세스 포인트에서 응답을 요청하므로 ICMP(Internet Control Message Protocol) 에코 프레임이 이상적입니다.
2. 그런 다음 네트워크 침입자는 키 스트림을 1바이트씩 확장합니다.
3. 256개의 값만 사용하므로 추가 바이트를 추측할 수 있습니다.
4. 네트워크 침입자가 정확한 값을 추측하면 예상되는 응답이 수신됩니다. 이 예제에서는 ICMP 에코 응답 메시지입니다.
5. 원하는 키 스트림 길이에 도달할 때까지 프로세스가 반복됩니다.

그림 19: 키 스트림 "확장"

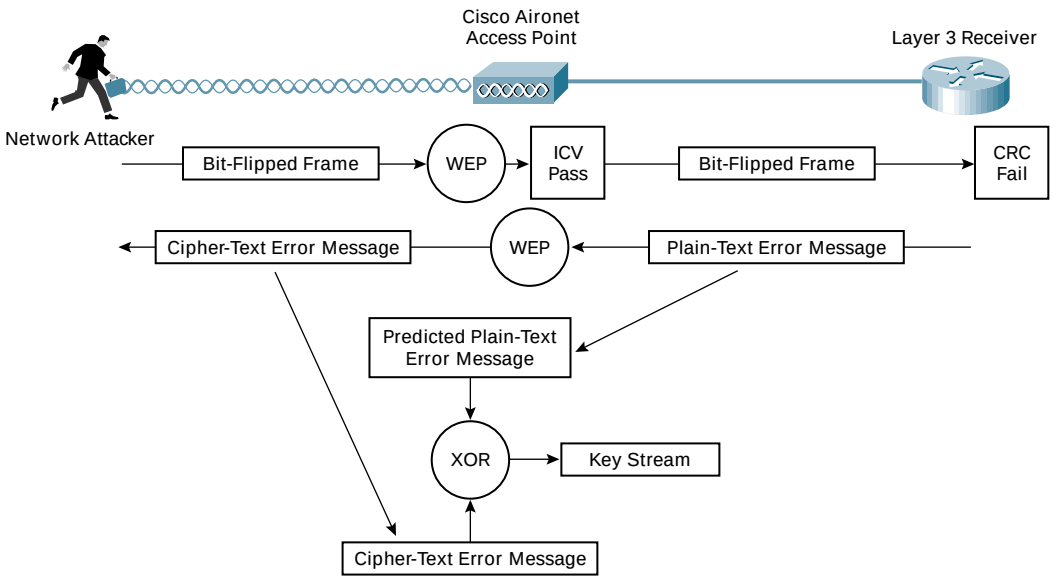


### 3.3.2. 비트 플립핑 공격(Bit-Flipping Attack)

비트 플립핑 공격은 IV 재생 공격과 동일한 목적으로 사용되지만 ICV의 약점을 이용한다는 차이가 있습니다. 데이터 페이로드 크기는 다양할 수 있지만 많은 요소들은 일정하며 동일한 비트 위치를 갖고 있습니다. 침입자는 프레임의 페이로드 부분을 변경하여 상위 계층의 패킷을 수정합니다. 다음은 비트 플립핑 공격의 프로세스에 대한 설명입니다(그림 20).

1. 침입자가 무선 LAN에서 프레임을 스니핑합니다.
2. 침입자가 프레임을 캡처하여 프레임의 데이터 페이로드에서 임의의 비트를 변환합니다.
3. 침입자가 ICV를 수정합니다(세부 사항은 뒤에 설명).
4. 침입자가 수정된 프레임을 전송합니다.
5. 수신자(클라이언트 또는 액세스 포인트)가 프레임을 수신하여 프레임 내용을 기반으로 ICV를 계산합니다.
6. 수신자가 계산한 ICV를 프레임의 ICV 필드 값과 비교합니다.
7. 수신자가 수정된 프레임을 허용합니다.
8. 수신자가 프레임의 캡슐화를 해제하고 Layer 3 패킷을 처리합니다.
9. 레이어 패킷에서 비트가 변환되었으므로 Layer 3 체크섬에 오류가 발생합니다.
10. 수신자 IP 스택에서 예측 가능한 오류를 생성합니다.
11. 침입자가 무선 LAN를 스니핑하여 암호화된 오류 메시지를 찾습니다.
12. 침입자가 오류 메시지를 수신하면 IV 재생 공격의 경우와 마찬가지로 키 스트림을 파생시킵니다.

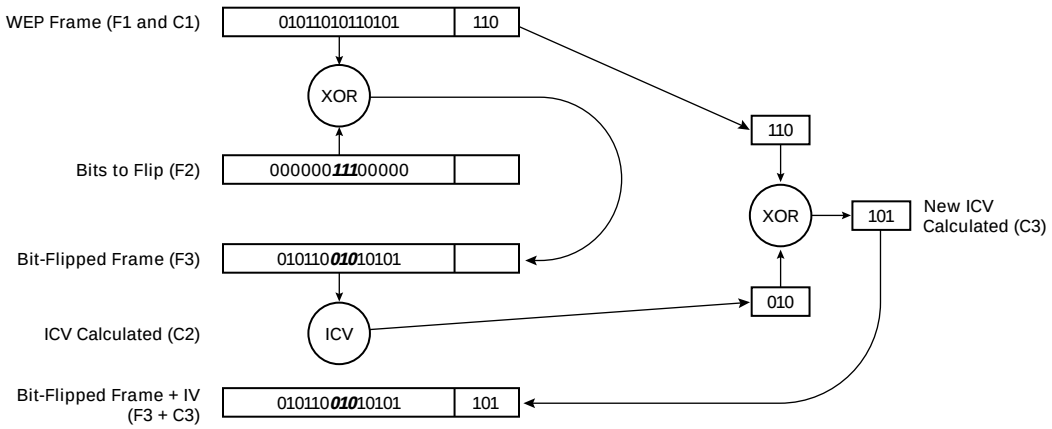
**그림 20: 비트 플립핑 공격**



이 공격은 기본적으로 ICV에 오류가 발생하도록 하는 것입니다. ICV는 프레임의 EWP 암호화 부분에 있으므로 침입자는 비트 플립핑에 의한 프레임 변경 사항과 일치하도록 ICV를 수정할 수 있습니다. 비트 플립핑의 프로세스는 다음과 같습니다.

1. 주어진 프레임(그림 21의 F1)에 ICV(C1)가 있습니다.
2. 비트가 설정된 F1과 동일한 길이의 새로운 프레임(F2)이 생성됩니다.
3. XOR 함수 F1 및 F2를 실행하면 프레임 F3이 생성됩니다.
4. F3에 대한 ICV가 계산됩니다(C2).
5. XOR 함수 C1 및 C2를 실행하면 ICV C3가 생성됩니다.

**그림 21: ICV의 단점**




## 3.4. 정적 WEP 키 관리 문제

802.11 표준에서는 키 관리 메커니즘을 지정하지 않습니다. WEP는 미리 공유한 정적 키만 지원하도록 정의되어 있습니다. 802.11 인증에서는 장치 사용자가 아닌 장치를 인증하므로 무선 어댑터 손실이나 도난은 네트워크 보안에 큰 문제를 일으킬 수 있습니다. 어댑터를 손실하거나 기존 키를 손상시키는 문제가 발생하면 네트워크 관리자는 네트워크 상의 모든 무선 장치에 대해 수동으로 키를 다시 생성하는 지루한 작업을 해야 합니다.

소규모 설치인 경우에는 이러한 작업이 가능할 수도 있지만 무선 사용자 수가 수 천에 달하는 중간 규모 이상의 설치에서는 현실적인 방법이 아닙니다. 키를 배포하거나 생성하는 메커니즘이 없다면 관리자는 무선 NIC를 세심하게 관찰해야 합니다.

## 4. Cisco Wireless Security Suite를 사용한 보안 802.11 무선 LAN

시스코는 802.11 인증 및 데이터 프라이버시에 취약성이 있다는 사실을 알고 있습니다. 시스코는 확장할 수 있고 관리할 수 있는 보안 무선 LAN 솔루션을 고객에게 제공하기 위해 Cisco Wireless Security Suite를 개발했습니다. 이 제품군은 802.11 인증 및 암호화에 대한 사전 표준(prestandard)을 개선함으로써 802.11 보안 기능을 향상시킵니다.

WEP가 무선 LAN 보안을 위한 유일한 컴포넌트라고 잘못 알고 있는 경우도 있지만 무선 보안은 사실상 다음과 같이 세 가지 컴포넌트로 이루어져 있습니다.

- 인증 프레임워크
- 인증 알고리즘
- 데이터 프라이버시 또는 암호화 알고리즘

Cisco Wireless Security Suite에는 이와 같은 세 가지 컴포넌트가 모두 포함되어 있습니다.

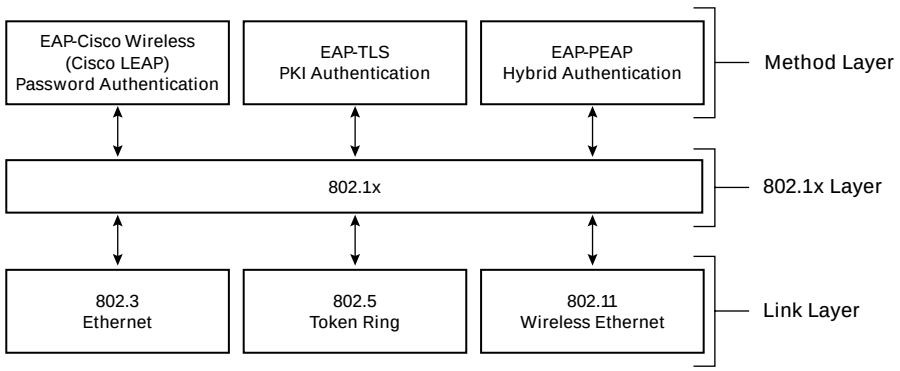
- 802.1X 인증 프레임워크 – IEEE 802.1X 표준은 여러 인증 유형 및 링크 레이어를 위한 프레임워크를 제공합니다.
- EAP(Extensible Authentication Protocol) 시스코 인증 알고리즘 – Cisco LEAP라고도 하는 EAP Cisco Wireless 인증 유형은 동적 WEP 키를 생성할 수 있는 중앙 집중식 사용자 기반 인증을 지원합니다.
- TKIP(Temporal Key Integrity Protocol) – 시스코는 WEP 암호화 기능을 확장하기 위해 두 가지 컴포넌트를 구현했습니다.
  - 메시지 무결성 검사(MIC) – MIC 기능은 중간자 공격으로 인한 취약성을 완화하기 위해 효과적인 프레임 인증 방식을 제공합니다.
  - 패킷별 키 생성(Per-Packet Keying) – 패킷별 키 생성은 모든 프레임에 대해 WEP 키 파생 공격을 완화하는 새롭고 고유한 WEP 키를 제공합니다.
  - 브로드캐스트 키 순환(Broadcast Key Rotation) – 브로드캐스트 및 멀티캐스트 트래픽을 위한 동적 키 순환

### 4.1. Cisco Wireless Security Suite 컴포넌트

#### 4.1.1. 802.1X 인증

802.1X 인증 프레임워크는 현재 IEEE 802.11 TGi(Task Group i)에서 추진 중인 802.11 MAC 레이어 보안 기능 향상을 위한 드래프트에 포함되어 있습니다. 802.1X 프레임워크는 일반적으로 상위 레이어에서 볼 수 있는 확장 가능한 인증을 링크 레이어에 제공합니다(그림 22).

**그림 22: 802.1X 레이어**

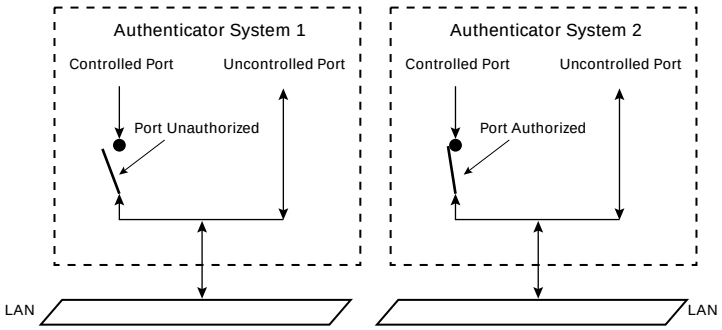


802.1X에는 다음과 같이 세 가지 엔티티가 필요합니다.

- 요청자 – 무선 LAN 클라이언트에 상주
- 인증자 – 액세스 포인트에 상주
- 인증 서버 – RADIUS 서버에 상주

이와 같은 엔티티는 네트워크 장치의 논리적 엔티티입니다. 인증자는 클라이언트의 연결 ID(AID)에 따라 하나의 클라이언트에 하나의 논리적 포트를 생성합니다. 생성한 논리적 포트에는 두 개의 데이터 경로가 있습니다. 제어되지 않은 데이터 경로를 통해 네트워크 트래픽이 네트워크에 전달됩니다. 제어된 데이터 경로는 네트워크 트래픽 전달을 위해 성공적으로 인증을 받아야 합니다(그림 23).

**그림 23: 802.1X 포트**



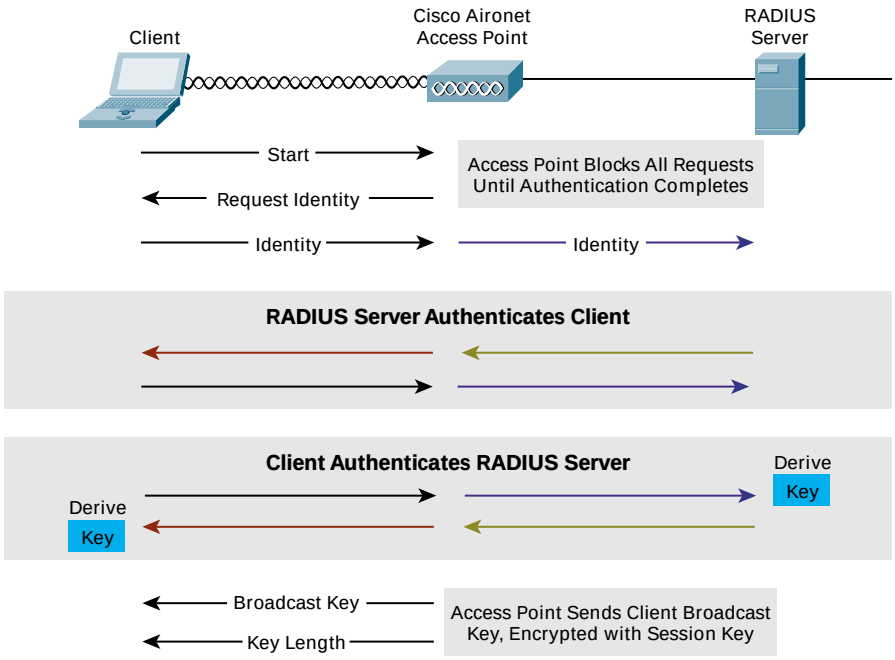

요청자는 매체에서 활성 상태가 되어 액세스 포인트에 연결됩니다. 인증자는 클라이언트 연결을 감지하고 요청자의 포트를 사용할 수 있도록 설정합니다. 그와 같이 설정하면 포트는 권한이 없는 상태가 되므로 802.1X 트래픽만 전달되고 다른 트래픽은 모두 차단됩니다. 클라이언트 초기화는 필요하지 않지만 클라이언트가 EAP Start 메시지를 전송합니다(그림 24).

인증자는 클라이언트 ID를 얻기 위해 EAP Request Identity 메시지를 요청자에게 전송함으로써 응답합니다. 클라이언트 ID가 포함된 요청자의 EAP Response 패킷이 인증 서버로 전달됩니다.

인증 서버는 특정 인증 알고리즘을 사용하여 클라이언트를 인증하도록 구성되어 있습니다. 현재 802.11 LAN에 대한 802.1X 사양에서는 특정 알고리즘을 사용하도록 규정하지 않았습니다. 그러나 본 백서에는 시스코 LEAP 인증에 대해 중점적으로 살펴보고, 시스코 LEAP 자격 증명 확인이 이루어진다고 가정합니다.

최종 결과는 RADIUS 서버에서 액세스 포인트로 전달되는 RADIUS-ACCEPT 또는 RADIUS-REJECT 패킷에 따라 달라집니다. RADIUS ACCEPT 패킷을 수신한 인증자는 클라이언트 포트를 인증된 상태로 전환하며 결과적으로 트래픽을 전달할 수 있습니다.

그림 24: 802.1X 및 EAP 메시지 흐름




802.1X는 무선 LAN 클라이언트가 인증 서버와 통신하면서 클라이언트 자격 증명을 확인할 수 있는 방법을 제공합니다. 802.1X는 확장이 가능하며 다양한 인증 알고리즘을 사용할 수 있습니다.

### 4.1.2. EAP 시스코 인증 알고리즘

시스코는 구현이 간편하고 강력한 인증을 위해 시스코 LEAP 인증 알고리즘을 개발했습니다. 시스코 LEAP는 다른 EAP 인증 방식과 마찬가지로 802.1X 인증 프레임워크에서 작동하도록 설계되어 있습니다. 시스코 LEAP 알고리즘의 강점은 바로 강력한 기능입니다.

#### 4.1.2.1. 상호 인증

필요에 적합한 용도로 사용하기 위한 수 많은 인증 알고리즘이 있습니다. 무선 LAN에서는 클라이언트가 원하는 네트워크 장치와 통신할 수 있어야 합니다. 클라이언트와 네트워크 사이에 물리적 연결이 없다면 클라이언트는 네트워크를 인증해야 할 뿐만 아니리 네트워크에 의해 인증을 받아야 합니다. 따라서 시스코는 상호 인증을 지원하는 시스코 LEAP를 개발했습니다.

#### 4.1.2.2. 사용자 기반 인증

802.11 인증은 장치를 기반으로 이루어집니다. 인증자는 장치 사용자를 볼 수 없으므로 무단 사용자는 인증된 장치에 액세스하는 것만으로도 간단하게 네트워크에 액세스할 수 있습니다. 정적 WEP를 802.11 인증과 함께 사용하는 802.11 NIC가 설치된 랩탑의 경우에는 랩탑을 도난 당하거나 잃어버리면 네트워크 보안에 문제가 발생합니다. 그와 같은 일이 발생하면 네트워크 관리자는 무선 네트워크와 모든 클라이언트에 대한 키를 신속하게 다시 설정해야 합니다.

그와 같은 사례는 흔히 발생하는 일이며 무선 LAN 설치에서 고려해야 하는 주요 장애 요소입니다. 시스코는 무선 LAN 장치가 아닌 사용자를 인증하는 방식을 기반으로 하는 시스코 LEAP를 구현하여 이러한 문제를 해결했습니다.

#### 4.1.2.3. 동적 WEP 키

사용자 기반의 상호 인증은 관리하기 편하고 안전한 인증 방식이지만 WEP 키를 효율적으로 관리하기 위한 메커니즘이 필요합니다. 이를 위해서는 동적 WEP 키에 대한 키 생성 자료를 만들기 위해 인증 알고리즘이 필요하게 됩니다. 시스코 LEAP는 각각의 클라이언트에 대해 고유한 키 생성 자료를 만드는 사용자 기반의 방법을 채택하고 있습니다. 그와 같은 방법을 사용하면 네트워크 관리자가 정적 키를 관리하고 필요할 때마다 수동으로 다시 키를 생성하는 부담을 덜 수 있습니다.

802.1X 세션 시간 초과라는 특성 때문에 클라이언트는 네트워크 연결 유지를 위해 다시 인증을 받아야 합니다. 클라이언트에게는 재인증이 투명하게 이루어지지만 동적 WEP를 지원하는 알고리즘의 재인증 프로세스에서는 다시 인증할 때마다 새로운 WEP 키를 생성합니다. 이것은 통계 키 파생 공격을 줄일 수 있는 중요한 기능으로서 시스코 WEP의 향상된 기능에서 중요한 부분입니다(뒤에서 자세히 설명).

### 4.1.3. TKIP를 통한 데이터 프라이버시

앞 단원에서는 802.11 보안에 대한 네트워크 공격에 관해 중점적으로 설명하였으며 데이터 프라이버시 메커니즘으로서 WEP가 비효율적임을 입증했습니다. 시스코는 기존의 네트워크 공격을 완화하고 그에 대한 결함을 극복할 수 있는 사전 표준(prestandard) 향상 기능을 WEP 프로토콜에 구현했습니다. 이와 같은 WEP에 대한 향상된 기능을 일반적으로 TKIP(Temporal Key Integrity Protocol)라고 합니다. TKIP는 IEEE 802.11 작업 그룹의 Task Group i가 제시한 표준에 관한 드래프트입니다. TKIP는 승인된 표준은 아니지만 시스코는 Cisco Aironet(r) 무선 제품에 대한 기존의 고객 투자를 보호하기 위해 TKIP의 사전 표준(prestandard) 버전을 구현했습니다.

TKIP는 WEP에 다음 두 가지 주요 기능을 새로 추가한 것입니다.

- 모든 WEP 암호화 데이터 프레임에서 메시지 무결성 검사(MIC) 기능
- 모든 WEP 암호화 데이터 프레임에서 패킷별 키 생성

또한 시스코는 IEEE 802.11 Task Group i의 드래프트에서 규정하지 않은 또 다른 기능인 브로드캐스트 키 순환을 추가했습니다.

#### 4.1.3.1. 메시지 무결성 검사(MIC)

MIC는 802.11 표준에서 비효율적이었던 무결성 검사 기능(ICV)을 확장한 것입니다. MIC는 다음의 두 가지 주요 취약성을 해결하도록 설계되었습니다.

- 초기화 벡터/기본 키 재사용 - MIC는 무선 프레임에 시퀀스 번호 필드를 추가합니다. 액세스 포인트는 수신 프레임 중 규칙에 어긋난 프레임은 삭제합니다.
- 프레임 변경/비트 플립핑 - MIC 기능은 무선 프레임에 MIC 필드를 추가합니다. MIC 필드는 ICV와 동일한 수학적 결함을 극복할 수 있는 프레임 무결성 검사 기능을 제공합니다.

그림 25에서는 WEP 데이터 프레임 예제를 보여줍니다. MIC는 무선 프레임에 시퀀스 번호 필드와 무결성 검사 필드라는 두 가지 필드를 새로 추가합니다(그림 26).

**그림 25: WEP 프레임 포맷 예제**

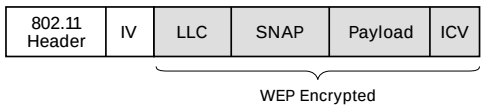
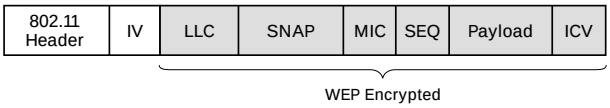
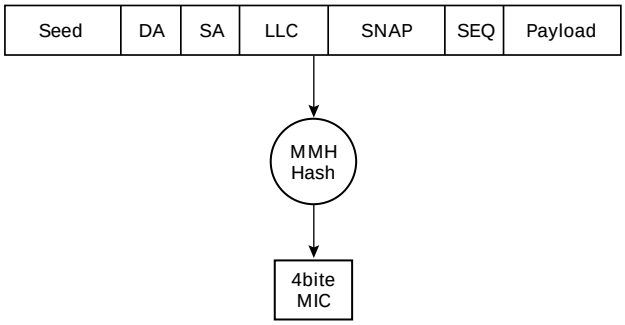


그림 26: MIC를 사용할 수 있는 WEP 프레임 포맷 예제




시퀀스 번호는 프레임별, 연결별로 값이 증가하는 순차적 카운터입니다. 액세스 포인트는 수신 프레임 중 규칙에 어긋난 시퀀스 번호가 있는 프레임은 버립니다. MIC 필드는 그림 27의 필드를 기준으로 계산됩니다.

그림 27: MIC 값 파생




필드를 수정하면 수신 장치의 계산된 MIC에 불일치가 발생합니다. 결과적으로 수신 장치는 프레임을 삭제합니다.
MIC는 현재 사전 표준(prestandard) 구현 사항입니다. MIC는 IEEE 802.11 Task Group i 드래프트에 포함되어 있지만 모든 무선 LAN 공급업체가 이를 채택한 것은 아닙니다. 따라서 MIC에서는 시스코 클라이언트 및 액세스 포인트를 사용해야 합니다.

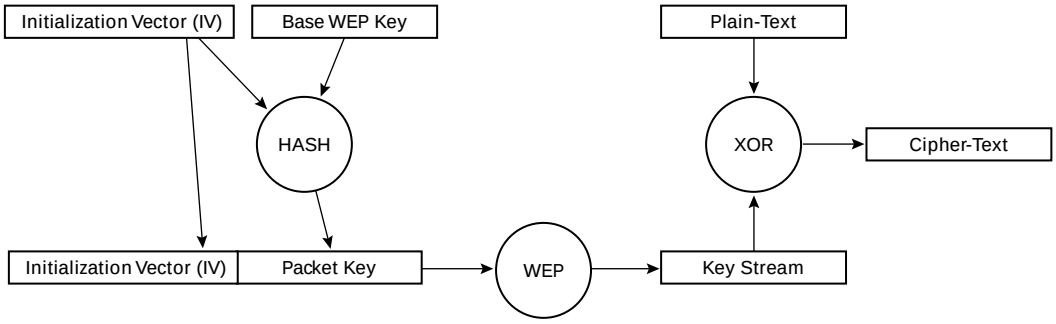
### 4.1.3.2. 패킷별 키 생성(Per-Packet Keying)

공격을 실행할 수 있는 AirSnort 도구에서의 취약성 뿐만 아니라 Fluhrer, Mantin 및 Shamir의 보고서에서 설명한 취약성으로 인해 WEP는 데이터 프라이버시 및 암호화에 비효율적입니다. 802.1X 재인증을 통한 WEP 키 순환 방식을 사용하면 취약성은 완화할 수 있지만 단점을 완전히 해결해 주지는 못합니다.

IEEE는 패킷별로 전송 WEP 키를 변경하는 Task Group I 드래프트의 WEP 성능 개선안을 채택했습니다. 시스코는 이러한 향상된 기능을 고안 및 공동 개발하는 데 적극 참여했으며, 시스코 클라이언트 및 액세스 포인트에서 이 기능을 구현했습니다.

시스코의 802.11 WEP 암호화 구현에서는 IV가 임의로 생성되어 WEP 키와 연결됩니다. 두 개의 값은 WEP 알고리즘으로 처리되어 키 스트림을 생성합니다. 키 스트림은 일반 텍스트와 혼합되어 암호문을 생성합니다.
시스코의 패킷별 키 생성 구현에서는 WEP 키와 IV를 해시하여 새로운 패킷 키를 생성함으로써 프로세스를 확장합니다. 그러면 원래의 IV는 패킷 키와 연결되어 정상적으로 처리됩니다(그림 28).

그림 28: 패킷별 키 생성(Per-Packet Keying)




시스코는 24비트 IV 공간을 효과적으로 이용하기 위해 IV 시퀀싱도 채택했습니다. 시스코 클라이언트와 액세스 포인트는 IV 카운터를 시작하고 IV 값을 매 프레임마다 하나씩 증가시키는 방식으로 IV 시퀀싱을 구현합니다. 클라이언트와 액세스 포인트가 모두 IV 카운터를 0으로 초기화한다면 클라이언트와 액세스 포인트는 해싱 알고리즘을 사용하고 동일한 패킷 키를 생성함으로써 동일한 IV/기준 WEP 키를 전송합니다. 시스코 IV 시퀀싱은 이러한 문제를 해결하는 데 유용합니다. 예를 들어 클라이언트-투-액세스 포인트 프레임은 짝수 번호의 IV를 사용하고 액세스 포인트-투-클라이언트 프레임은 홀수 번호의 IV를 사용할 수 있습니다.

패킷별 키 생성은 고유한 IV/기준 WEP 키 쌍을 사용한다면 동일한 패킷 키를 생성하지 않습니다. 따라서 정적 WEP 키를 사용하는 경우에는 224개의 고유 패킷 키만 허용됩니다. IV 공간은 모두 소모되면 재활용되므로 IV/기준 WEP 키 쌍은 다시 사용됩니다. 이러한 한계점을 극복하려면 IV 공간을 사용하기 전에 기준 WEP 키를 변경해야 합니다. 시스코 LEAP 세션 시간 초과는 이러한 문제 해결을 위한 요구 사항을 충족시킵니다. 기준 WEP 키가 일단 변경되면 새로운 IV/기준 WEP 키 쌍이 사용되고 고유한 패킷 키가 생성됩니다.

#### 4.1.3.3. 브로드캐스트 키 순환(Broadcast Key Rotation)

사용자 기반 WEP 키를 지원하는 802.1X 인증 유형에서는 유니캐스트 트래픽만을 위한 WEP 키를 제공합니다. Cisco Wireless Security Suite에서는 브로드캐스트 및 멀티캐스트 트래픽을 위한 암호화를 제공하기 위해 다음 두 가지 옵션 중 하나를 선택해야 합니다.

- 액세스 포인트에서 구성된 정적 브로드캐스트 키 사용
- 동적 브로드캐스트 키 생성을 위한 브로드캐스트 키 순환 사용

802.1X 클라이언트가 브로드캐스트 및 멀티캐스트 메시지를 수신하도록 하려면 액세스 포인트에서 정적 브로드캐스트 키를 구성해야 합니다. 시스코 TKIP 향상 기능을 구현한 무선 LAN 설치에서 정적 브로드캐스트 키는 패킷별 키 생성 프로세스를 거치게 됩니다. 이로 인해 통계 키 파생 공격을 줄이는 장점은 있지만 기본 브로드캐스트 키가 정적 상태를 유지하므로 IV 공간이 재활용되어 키 스트림도 재사용됩니다. 통계 공격은 실행하는 데 더욱 많은 시간이 걸리지만 충분히 가능한 일입니다.

몇 가지 경우에서 정적 브로드캐스트 키 설치가 필요할 수도 있습니다. 브로드캐스트 키는 클라이언트의 유니캐스트 WEP 키로 암호화되어 액세스 포인트에서 클라이언트로 전송됩니다. 브로드캐스트 키는 인증 후 설치되므로 동일한 브로드캐스트 키로 액세스 포인트를 구성할 필요가 없습니다.

액세스 포인트에서 브로드캐스트 키 순환을 사용하는 것이 좋습니다. 액세스 포인트는 시드된 의사 난수 생성기(PRNG)를 사용하여 브로드캐스트 WEP 키를 생성합니다. 액세스 포인트는 구성된 브로드캐스트 WEP 키 타이머가 종료된 후 브로드캐스트 키를 순환시킵니다. 이 프로세스는 일반적으로 사용자 재인증을 위해 RADIUS 서버에 구성된 시간 초과와 동기화되어 있어야 합니다.

브로드캐스트 키 순환은 802.1X를 사용하는 액세스 포인트를 설치하기 위한 것입니다. 혼합 정적 WEP/802.1X 설치 시 브로드캐스트 키 순환은 정적 WEP 클라이언트에서 연결 문제를 야기할 수 있습니다. 따라서 액세스 포인트에서 802.1X 독점 무선 LAN을 서비스할 때 브로드캐스트 키 순환을 사용하도록 설정하는 것이 좋습니다.

## 5. 시스코 LEAP 아키텍처

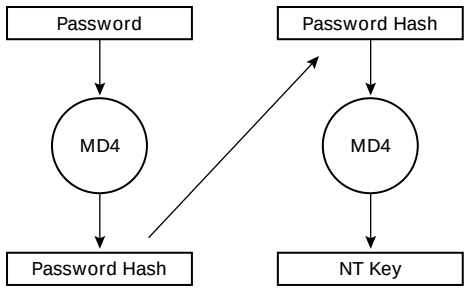
EAP Cisco Wireless 또는 시스코 LEAP 알고리즘은 사용자 기반의 상호 인증을 제공합니다. 또한 WEP 키를 생성하기 위해 클라이언트와 RADIUS 서버에 키 생성 자료를 제공합니다. 이 단원에서는 프로토콜 메시지 교환에서 RADIUS 서버, 액세스 포인트, 클라이언트 장치에서의 알고리즘 구현 방법에 이르기까지 시스코 LEAP에 대해 설명합니다.

### 5.1. 시스코 LEAP 인증 프로세스

시스코 LEAP는 부적절한 무선 LAN 설치에서도 구현할 수 있을 정도로 매우 안전한 사용자 기반의 인증 알고리즘입니다. 시스코는 사용자 요구 사항 및 SSO(single-sign-on) 기능에 대한 요구를 기반으로 하여 MS-CHAP(Microsoft Challenge Handshake Authentication Protocol)을 통한 시스코 LEAP를 구축했습니다.

시스코 LEAP는 암호 기반의 알고리즘으로서 암호를 비밀 키 값으로 변환하여 무선 인증 과정에서 암호의 무결성을 보존하므로 무선 도청자가 시스코 LEAP 인증을 스니핑하여 무선 연결을 통해 전송되는 사용자 암호를 볼 수 없습니다. 비밀 키 값은 해시 함수라는 수학 함수의 연산 결과입니다. 해시 함수는 데이터를 단방향으로 암호화하는 알고리즘입니다. 원래 입력을 파생하도록 데이터를 암호 해독할 수 없습니다. 시스코 LEAP는 Microsoft NT 키 형식의 비밀 키 값을 사용합니다. Windows NT 키는 사용자 암호의 MD4(Message Digest Algorithm 4) 해시입니다(그림 29).

**그림 29: Windows NT 키**




시스코 LEAP는 Windows NT 키를 통해 기존의 Windows NT Domain Services 인증 데이터베이스와 Windows 2000 Active Directory 데이터베이스를 사용할 수 있습니다. 뿐만 아니라 MS-CHAP 암호를 사용하는 모든 ODBC(Open Database Connectivity)도 사용할 수 있습니다.

시스코는 대부분의 Microsoft Windows 버전(Windows 95, 98, Me, 2000, NT 및 XP)을 위한 드라이버를 개발했으며 Windows 로그온을 시스코 LEAP 로그온으로 사용합니다. Windows 로그온의 소프트웨어 심(shim)을 통해 사용자 이름과 암호 정보가 Cisco Aironet 클라이언트 드라이버로 전달됩니다. 드라이버는 암호를 Windows NT 키로 변환하고 사용자 이름과 Windows NT 키를 Cisco NIC로 전달합니다. NIC는 AP와 AAA(authentication, authorization, and accounting) 서버를 사용하여 802.1X 트랜잭션을 실행합니다.

**주** 암호와 암호 해시는 무선 매체를 통해 전송되지 않습니다.

재인증과 후속 WEP 키 파생은 유사한 프로세스에 따라 이루어집니다. 기존 클라이언트 WEP 키 및 액세스 포인트 상의 클라이언트 포트를 사용하여 WEP로 암호화된 트랜잭션은 블로킹 상태로 전환되지 않습니다. 클라이언트가 명시적으로 EAP Logoff 메시지를 전송하거나 재인증에 오류가 발생할 때까지 포워딩 상태를 유지합니다.

### 5.2. 시스코 LEAP 설치

시스코는 강력하고 설치 및 관리가 간편한 무선 보안을 제공하기 위해 시스코 LEAP를 설계했습니다. 시스코는 고객들이 RADIUS 서버 뿐만 아니라 무선 클라이언트에 대한 기존 투자를 활용할 수 있도록 타 업체의 NIC를 지원하며 RADIUS도 지원합니다. 또한 고객들이 Cisco Aironet 제품과 Cisco LEAP 알고리즘을 사용하여 만족스러운 결과를 얻을 수 있도록 설치와 관련된 최상의 작업 방식에 대한 지침을 제공합니다.

#### 5.2.1. 타 업체의 지원

시스코 LEAP RADIUS를 통해 시스코에서 지원하는 제품은 다음과 같습니다.

- Cisco Secure ACS(Access Control Server) 버전 2.6 및 3.0 플랫폼
- Cisco Access Registrar 버전 1.7 이상

시스코는 기존의 RADIUS 서버를 사용하는 고객을 지원하기 위해 Funk Software 및 Interlink Networks와 제휴를 맺었습니다. 시스코 LEAP는 다음 제품에서도 지원됩니다.

- Funk Steel Belted RADIUS v3.0
- Interlink Merit v5.1

뿐만 아니라 Apple Computers의 AirPort 무선 어댑터를 통해서도 타 업체의 클라이언트 지원을 받을 수 있습니다.

#### 5.2.2. 시스코 LEAP 설치를 위한 최상의 작업 방식

시스코는 보안 무선 LAN 설치를 위한 지침으로서 백서 시리즈인 Cisco SAFE Blueprint for enterprise networks(SAFE)를 제공합니다. SAFE: 무선 보안 세부 사항은 다음 웹 페이지를 참조하십시오.

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

무선 LAN 설치에 관한 유용한 정보도 얻을 수 있습니다.

#### 5.2.2.1. LEAP 인증을 위해 강력한 암호 사용

시스코 LEAP는 암호 기반의 알고리즘입니다. 사전 공격의 가능성을 최소화하려면 추측하기 어려운 강력한 암호를 사용해야 합니다. 다음은 그러한 암호의 몇 가지 특성입니다.

- 최소 여섯 글자
- 대소문자 혼합
- 적어도 하나의 숫자 포함
- 사용자 이름이나 사용자 ID는 포함하지 않는 형태
- 국어 사전이나 외국어 사전에 나오지 않는 단어

강력한 암호의 예는 다음과 같습니다.

- cnw84Fri("cannot wait for Friday"를 응용함)
- !crE8vpw("not creative password"를 응용함)
- G8tSm^rt("get smart"를 응용함)

#### 5.2.2.2. 동일한 RADIUS 서버에서 MAC 및 시스코 LEAP 인증을 사용하지 않음

MAC 주소 인증에서 시스코 LEAP와 동일한 ACS를 사용하는 경우 MAC 주소에 별개의 강력한 MS-CHAP 암호를 지정해야 합니다.

시스코 LEAP와 MAC 인증을 지원하는 ACS에서 MAC 주소가 구성된 경우 MAC 주소에서는 필수 MS-CHAP/CHAP 필드에 대한 다른 강력한 암호를 사용해야 합니다. 그렇지 않으면 도청자는 올바른 MAC 주소를 속이고 이를 사용자 이름 및 암호 조합으로 사용해 시스코 LEAP 인증을 받을 수 있습니다.

Cisco Wireless Security Suite 구성에 대한 자세한 내용은 http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wrsec_an.htm을 참조하십시오.

#### 5.2.2.3. RADIUS 세션 시간 초과를 사용하여 WEP 키 순환

시스코 LEAP 및 EAP TLS(Transport Layer Security)는 RADIUS 세션 시간 초과 옵션(RADIUS Internet Engineering Task Force 옵션 27)을 사용하여 세션 만료 및 802.1X 재인증을 지원합니다. IV 재사용(IV 충돌)을 방지하려면 IV 공간 모두 소모되기 전에 기본 WEP 키를 순환시켜야 합니다.

예를 들어 재인증 시 최악의 사태가 발생할 수 있는 경우는 최대 패킷 속도(802.11 스테이션에서는 초당 1000프레임)로 실행하도록 설정된 서비스의 스테이션일 것입니다.

- 2^24 프레임(16,777,216) / 초당 1000프레임 ~= 16,777초 또는 4시간 40분

정상 프레임 속도는 구현 내용에 따라 다르지만 이 예제는 세션 시간 초과 값을 결정하기 위한 지침으로 활용할 수 있습니다.

#### 5.2.2.4. 별도의 가상 LAN(VLAN)에 시스코 LEAP 구축

시스코 LEAP 무선 LAN 사용자가 별도의 VLAN에 위치하면 유선 클라이언트에 영향을 미치지 않고도 Layer 3 액세스 목록을 필요에 따라 무선 LAN VLAN에 적용할 수 있습니다. 또한 침입 감지 시스템을 무선 LAN VLAN에 설치하여 무선 LAN 트래픽을 모니터링할 수 있습니다.

## 6. 개선 사항

WEP 암호화 및 802.11 인증에는 약점이 있는 것으로 알려져 있습니다. IEEE는 TKIP를 통해 WEP의 성능을 향상시키며 802.1X를 통해 강력한 인증 옵션을 제공함으로써 802.11 기반 무선 LAN의 안전성을 보장합니다. 이와 동시에 IEEE는 보다 강력한 암호화 메커니즘을 모색하고 있습니다. IEEE는 제안된 802.11i 표준의 데이터 프라이버시 단원에서 소개한 AES(Advanced Encryption Standard)를 사용하기로 채택했습니다.

### 6.1. AES 개요

AES(Advanced Encryption Standard)는 NIST(National Institute of Standards and Technology: 미국 국립 표준 기술 연구소)가 승인한 차세대 암호화 기능입니다. NIST는 새로운 암호화 알고리즘을 개발하도록 암호 해독 관련 커뮤니티에 요청했습니다. 알고리즘은 완전히 밝혀져야 하고 로열티 없이 사용할 수 있어야 합니다. NIST는 암호 해독 뿐만 아니라 실제 구현에도 능력이 있는 후보를 선정했습니다. 이렇게 해서 최종 채택된 방법이 Rijndael 알고리즘입니다.

AES는 대부분의 암호와 마찬가지로 ECB 모드와 관련된 위험 요소를 방지하기 위해 피드백 모드를 사용해야 합니다. IEEE는 AES 암호화에 사용할 피드백 모드를 결정할 것입니다. 다음은 그 두 가지 모드입니다.

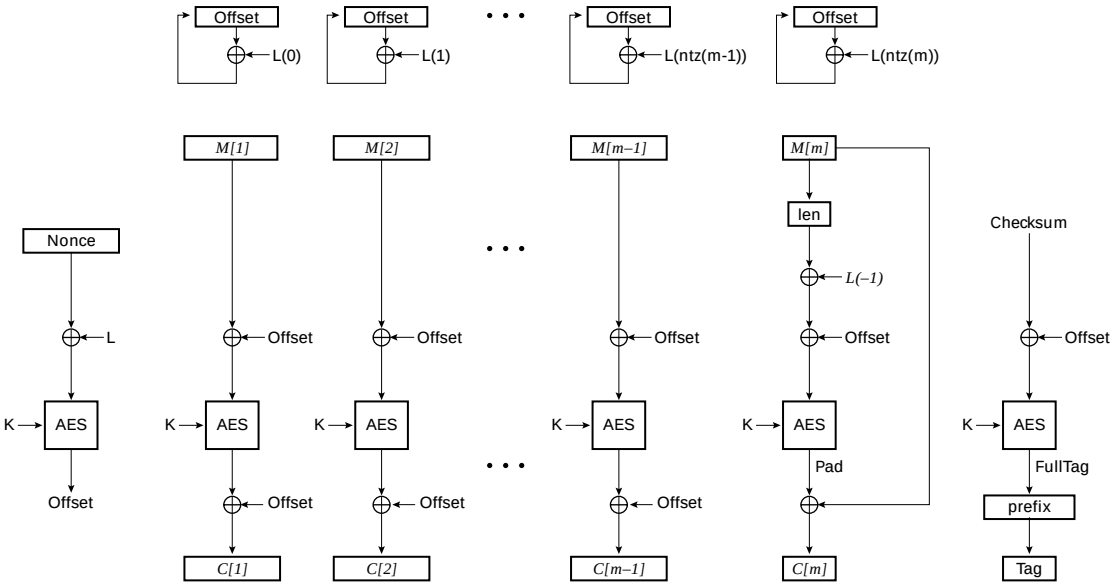
- OCB(Offset code book)
- 암호 블록 연결 메시지 인증 검사(CBC-MAC)를 포함한 암호 블록 연결 카운터 모드(CBC-CTR)로서 일반적으로 CBC-CCM이라고 함

위의 두 가지 모드는 유사하지만 구현 방법 및 성능에는 차이가 있습니다.

#### 6.1.1. AES-OCB 모드

AES-OCB는 오프셋 값을 결합하여 정상적인 암호화 프로세스를 확장함으로써 작동하는 모드입니다. 루틴은 초기 오프셋 값을 생성하는 데 사용되는 고유 넌스(넌스(nonce)는 128비트 숫자)로 초기화됩니다. 넌스는 128비트 문자열(L 값)로 수행되는 XOR 함수를 포함합니다. XOR의 출력은 AES 키로 암호화된 AES이며 결과는 오프셋 값입니다. 일반 텍스트 데이터는 오프셋으로 수행되는 XOR 함수를 포함하므로 동일한 AES 키로 암호화된 AES입니다. 해당 출력은 다시 한 번 오프셋으로 수행되는 XOR 함수를 포함합니다. 결과는 전송될 암호문 블록입니다. 오프셋 값은 새로운 L 값으로 오프셋에서 XOR 함수를 실행함으로써 각각의 블록을 처리한 후 변경됩니다(그림 30).

그림 30: AES-OCB 암호화



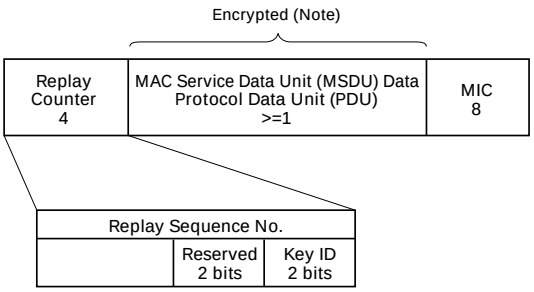

AES OCB 모드에 대한 자세한 내용은 OCB 모드를 참조하십시오.

OCB 모드에는 MIC 기능도 포함됩니다. 다음 값에서 XOR 함수를 실행하여 MIC를 계산합니다.

- 최종 블록을 제외한 모든 일반 텍스트 블록
- 적절한 오프셋 값으로 XOR 함수를 실행한 최종 일반 텍스트 블록
- 최종 암호문 블록
- 최종 오프셋 값

XOR 함수의 연산 결과는 AES 키를 사용하여 암호화된 AES입니다. 128비트 결과 출력 중 처음 64비트는 AES 암호화 프레임에 삽입된 MIC 값입니다(그림 31). MIC는 프레임의 암호화된 부분에 포함되지 않습니다. MIC 자체는 AES 암호화의 결과이므로 MIC 암호화는 필요하지 않습니다.

그림 31: AES 암호화 프레임



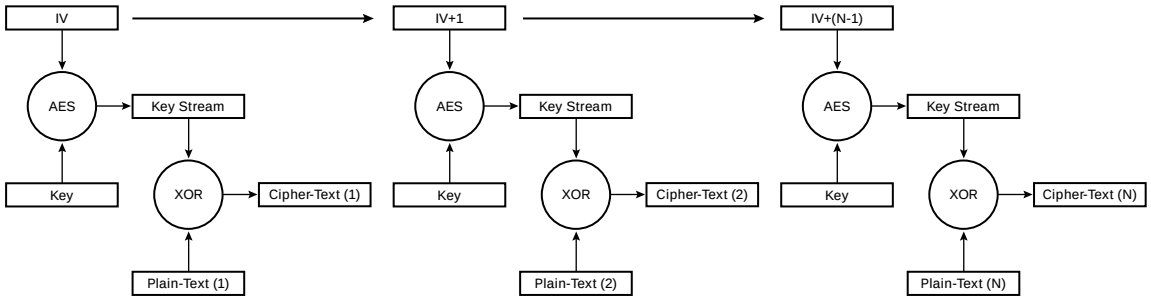
AES-OCB는 암호 해독 커뮤니티에서 볼 때는 처음부터 약점이 있는 새로운 모드입니다. 그러나 이 모드의 작성자인 Phil Rogaway는 암호 해독을 통해 해당 모드의 강점을 입증했으며 암호 해독 커뮤니티의 존경 받는 회원이기도 합니다. OCB 모드는 효율적이며 빠른 것으로 알려져 있습니다. 주요 장점 중 하나는 암호화와 동일한 처리 기능으로 MIC를 계산할 수 있으므로 암호화 관련 경비를 최소화하고 데이터 처리량을 극대화할 수 있다는 점입니다.

### 6.1.2. AES-CCM 모드

AES-CCM 모드는 OCB 모드를 대신할 수 있는 AES 암호화 모드입니다. CCM 모드는 암호 블록 연결 카운터(CBC-CTR) 모드와 암호 블록 연결 메시지 인증 검사(CBC-MAC) 모드를 조합한 것입니다. 두 모드의 기능이 결합되어 하나의 솔루션에서 암호화 및 메시지 무결성을 제공합니다.

CBC-CTR 암호화는 키 스트림을 확장하는 IV를 사용하여 작동합니다. IV는 각 블록을 암호화할 때마다 하나씩 증가합니다. 이로써 각 블록에 고유한 키 스트림을 제공합니다(그림 32).

**그림 32: CBC-CTR 암호화**




CBC-MAC는 프레임 길이, 대상 주소, 소스 주소 및 데이터에 대한 CBC 암호화 결과를 사용하여 작동합니다. 128비트 결과 출력은 전송된 프레임에 사용할 수 있도록 64비트로 잘립니다.
AES-CCM은 암호 해독에 의해 알려진 기능을 사용하지만 암호화 및 메시지 무결성을 위해 두 가지 작업이 필요하다는 약점을 갖고 있습니다. 따라서 컴퓨팅 비용이 많이 들고 암호화 프로세스에 상당히 많은 비용이 소요됩니다.

## 7. 요약

무선 LAN은 최대한 안전하게 구축해야 합니다. 표준 802.11 보안은 수많은 네트워크 공격에 취약한 특성을 갖고 있습니다. 이 백서에서는 이러한 취약 요소들을 집중적으로 살펴보고 Cisco Wireless Security Suite가 802.11 보안을 확장하여 안전한 무선 LAN을 생성하는 방법에 대해 설명했습니다.

시스코의 몇 가지 향상된 보안 기능은 애플리케이션별 장치(정적 WEP만 가능한 802.11 전화기와 같은 ASD) 또는 혼합 벤더 환경과 같은 장치 제한 요인으로 인해 일부 상황에서는 구축하기가 어려울 수도 있습니다. 이런 경우에는 네트워크 관리자가 잠재적인 WLAN 보안 취약 요소를 이해하고 있어야 합니다.

시스코는 고객과 클라이언트에게 시스코 무선 LAN 솔루션에 관한 교육을 실시하고 정보를 제공하기 위해 노력하고 있으며, 자신의 요구에 맞는 최선의 결정의 내릴 수 있도록 설계 및 구축에 관한 지침을 제공합니다.

시스코는 무선 LAN 사용자에게 최대한 가장 안전한 환경을 제공하기 위해 Cisco Wireless Security Suite를 사용하여 기존 인증 및 암호화를 지양하고 가능하면 항상 강력한 인증 및 암호화 방법을 이용할 것을 권장합니다.

시스코는 호환 가능한 무선 LAN 솔루션을 고객들에게 제공할 것을 약속합니다. Cisco Wireless Security Suite는 표준이 재가된 후 호환 가능한 버전으로 업그레이드할 수 있는 여러 가지 사전 표준(prestandard) 기능을 제공합니다. 따라서 오늘날의 안전한 무선 LAN 구현에 대해 향후에 호환 가능한 무선 LAN을 약속할 수 있습니다.

# 8. 부록 A - EAP 인증 유형

## 8.1. EAP 전송 레이어 보안

EAP 전송 레이어 보안(TLS)(RFC2716)은 Microsoft가 TLS 프로토콜(RFC2246)을 기반으로 지원하는 EAP 인증 알고리즘입니다. TLS는 안전한 웹 애플리케이션 트랜잭션을 위해 대부분의 웹 브라우저에서 사용하는 SSL(Secure Socket Layer)의 최신 버전입니다. TLS는 안전한 인증 방식임이 입증되어 현재 802.1X EAP 인증 유형으로 사용 가능한 상태입니다. EAP-TLS는 Microsoft XP 플랫폼에서 지원되며 기존의 Microsoft 운영체제에서도 지원될 예정입니다. 클라이언트 운영체제에 요청자가 포함되므로 손쉽게 구축할 수 있고 단일 벤더 제한 조건이 완화됩니다.

### 8.1.1. TLS 개요

EAP-TLS는 SSL v3.0을 기반으로 합니다. EAP-TLS 동작에 대한 이해를 돕기 위해 이 단원에서는 SSL과 관련된 TLS 동작에 관해 설명합니다. TLS는 TCP/IP 연결을 위해 안전한 인증 및 암호화를 제공하도록 설계었습니다. TLS는 이 기능을 제공하기 위해 다음과 같은 세 가지 프로토콜로 이루어져 있습니다.

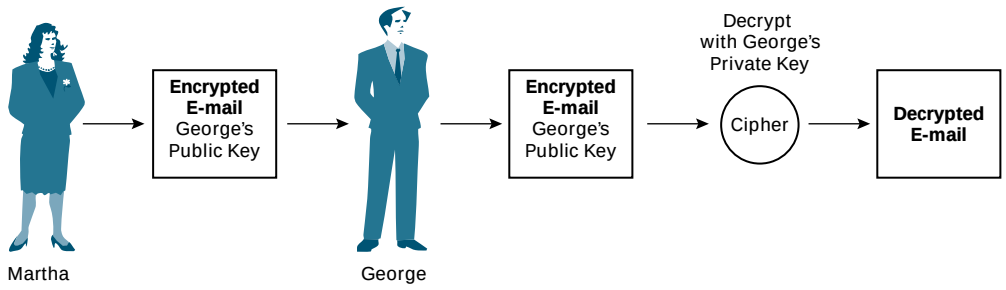
- 핸드쉐이크 프로토콜 - 핸드쉐이크 프로토콜은 SSL 세션을 위한 파라미터를 설정합니다. SSL 클라이언트와 서버는 프로토콜 버전 설정, 알고리즘 암호화, 쌍방 인증, 암호화 키 파생 등의 작업을 수행합니다.
- 레코드 프로토콜 - 레코드 프로토콜은 SSL 클라이언트와 서버 간의 암호 교환을 원활하게 합니다. 설정된 암호화 방식 및 암호화 키는 SSL 엔드포인트 간의 애플리케이션 데이터를 위한 안전한 터널을 제공합니다.
- 경고 프로토콜 - 경고 프로토콜은 세션 종료뿐 아니라 SSL 클라이언트 또는 서버에 오류를 통보하는 데 사용되는 메커니즘입니다.

TLS 인증은 일반적으로 서버측 인증과 클라이언트측 인증으로 이루어집니다. 서버측 인증은 PKI 인증서라고도 하는 공개 키 인프라(PKI)를 사용합니다. 클라이언트측 인증 역시 PKI 인증서를 사용할 수 있지만 여기서는 옵션입니다. EAP-TLS는 클라이언트측 인증서를 사용합니다.

### 8.1.2. PKI 및 전자 인증서

PKI 암호화는 비동기 암호화 키를 기반으로 합니다. PKI 사용자는 공개 키와 개인 키 두 가지를 갖고 있습니다. 공개 키로 암호화된 데이터는 개인 키로만 해독할 수 있고 그 반대의 경우도 마찬가지입니다. 예를 들면 다음과 같습니다. George가 Martha에게 공개 키를 제공합니다. Martha는 George의 공개 키로 암호화된 전자 메일을 그에게 전송합니다. George가 이 메시지를 읽으려면 자신의 개인 키로 메시지를 해독해야 합니다. George는 자신의 개인 키에 액세스할 수 있는 유일한 사람이므로 그만이 메시지를 해독할 수 있습니다(그림 33).

**그림 33: 공개 키 암호화**

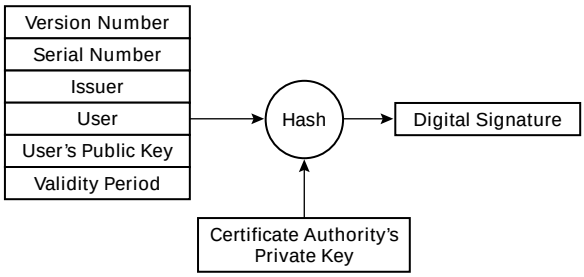


전자 인증서는 공개 키를 사용자에게 조인(join)하는 인증 기관에서 배포하는 데이터 구조입니다. 전자 인증서는 일반적으로 다음과 같은 정보들로 이루어집니다.

- 인증서 버전
- 일련번호
- 인증서 발행자
- 사용자
- 사용자의 공개 키
- 유효 기간
- 옵션 확장명
- 서명 알고리즘
- 서명

전자 서명은 인증서 버전, 일련번호, 발행자, 사용자, 사용자 공개 키, 유효 기간 등을 조합하여 파생되며 키 해시 함수를 통해 값을 실행합니다. 인증 기관은 자체 개인 키로 키 해시 작업을 수행합니다(그림 34).

**그림 34: 전자 서명**




### 8.1.3. TLS 인증 프로세스

TLS 프로세스는 핸드쉐이크 프로세스로 시작됩니다.

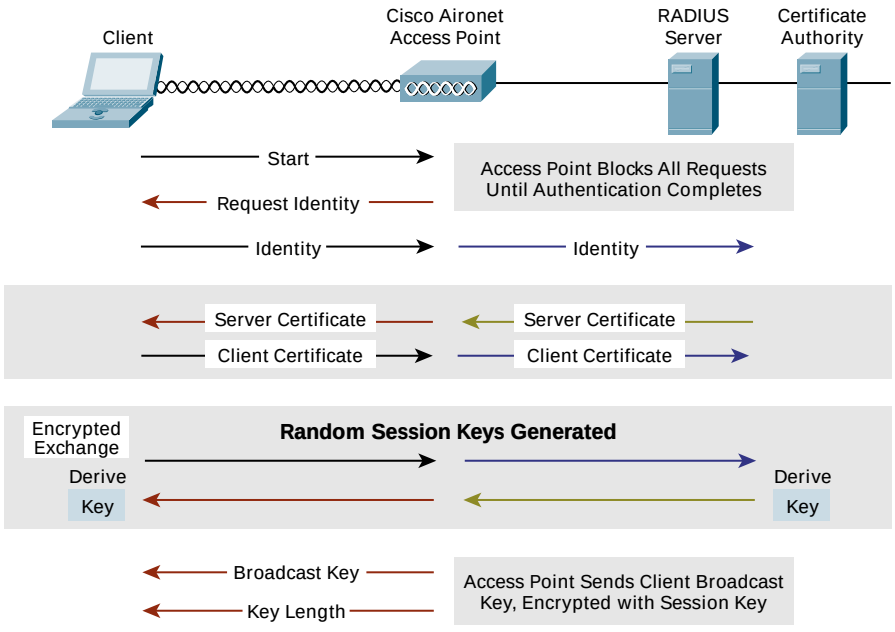
1. SSL 클라이언트가 서버에 연결하여 인증 요청을 수행합니다.
2. 서버가 클라이언트로 전자 인증서를 전송합니다.
3. 클라이언트가 인증서의 유효성 및 전자 서명을 검사합니다.
4. 서버가 클라이언트측 인증을 요청합니다.
5. 클라이언트가 서버로 전자 인증서를 전송합니다.
6. 서버가 인증서의 유효성 및 전자 서명을 검사합니다.
7. 암호화 및 메시지 무결성 방식이 설정됩니다.
8. 애플리케이션 데이터가 레코드 프로토콜을 통해 암호화된 터널로 전송됩니다.

### 8.1.4. EAP-TLS 인증 프로세스

EAP-TLS 인증 프로세스는 다음과 같습니다(그림 35).

1. 클라이언트가 액세스 포인트에 EAP Start 메시지를 전송합니다.
2. 액세스 포인트가 EAP Request Identity 메시지로 응답합니다.
3. 클라이언트가 사용자 이름에 해당하는 네트워크 액세스 식별자(NAI)를 EAP Response 메시지의 액세스 포인트로 전송합니다.
4. 액세스 포인트가 RADIUS Access Request 메시지에 포함된 RADIUS 서버로 NAI를 전달합니다.
5. RADIUS 서버가 전자 인증서를 클라이언트로 전송합니다.
6. 클라이언트가 RADIUS 서버의 전자 인증서 유효성을 검사합니다.
7. 클라이언트가 전자 인증서를 RADIUS 서버로 전송합니다.
8. RADIUS 서버가 클라이언트 전자 인증서를 기준으로 클라이언트의 자격 증명 유효성을 검사합니다.
9. 클라이언트 및 RADIUS 서버가 암호화 키를 파생합니다.
10. RADIUS 서버가 클라이언트의 WEP 키를 포함한 RADIUS ACCEPT 메시지를 액세스 포인트로 전송하여 인증에 성공했음을 알립니다.
11. 액세스 포인트가 EAP Success 메시지를 클라이언트로 전송합니다.
12. 액세스 포인트가 브로드캐스트 키와 키 길이를 클라이언트의 WEP 키로 암호화하여 클라이언트로 전송합니다.

그림 35: EAP-TLS 인증 프로세스



## 8.2. EAP SIM 아키텍처

EAP 가입자 식별 모듈(SIM) 인증 알고리즘은 무선 LAN(WLAN) 클라이언트와 AAA 서버 간의 사용자/세션별 상호 인증을 제공하도록 설계되었습니다. 또한 클라이언트와 AAA 서버가 WEP 키 파생을 위해 사용하는 마스터 키의 생성 방법도 정의합니다. 시스코의 EAP SIM 인증 구현은 최신 IEEE 초안 프로토콜을 기반으로 합니다. 이 단원에서는 프로토콜 메시지 교환에서부터 AAA 서버, 액세스 포인트 및 클라이언트 장치에서의 EAP SIM 구현 방법에 이르기까지 EAP SIM에 대해 자세히 설명합니다.

### 8.2.1. GSM(Global System for Mobile Communications)

EAP SIM 인증은 GSM 표준에 명시된 구체적인 요건에 따라 설계된 스마트카드(Smartcard)인 GSM(Global System for Mobile Communications) SIM에 저장된 인증 및 암호화 알고리즘을 기반으로 합니다. GSM 인증은 과제-응답(challenge-response) 메커니즘을 기반으로 하며, SIM에 저장되어 있거나 그렇지 않은 경우에는 GSM 운영자의 인증 센터(AuC)만 알고 있는 공유 보안 키 Ki를 사용합니다. GSM SIM이 128비트의 난수(RAND)를 과제로 수신하면 운영자 고유의 비밀 알고리즘을 사용하여 32비트 응답(SRES) 및 64비트 암호화 키(Kc)를 계산합니다. GSM 시스템의 Kc는 에어 인터페이스를 통한 휴대 전화 내용을 암호화하는 데 사용됩니다. GSM 인증에 대한 자세한 내용은 http://www.etsi.org/getastandard/home.htm을 참조하십시오.

### 8.2.2. EAP SIM 인증 프로세스

EAP SIM 인증은 불안할 수도 있는 공용 무선 LAN 설치에서 안전하게 구현할 수 있는 하드웨어 기반의 인증 방법을 제공합니다. 이 인증 방법을 사용하는 GSM 모바일 운영자는 기존의 인증 인프라를 재사용하여 주로 공용 액세스가 많은 지점에서 무선 네트워크에 대한 액세스를 제공할 수 있습니다. EAP SIM은 AuC에서 입수한 여러 GSM(RAND, SRES, Kc)의 데이터를 조합하여 더욱 안전한 세션 암호화 키를 생성합니다. 또한 EAP SIM은 클라이언트와 AAA 서버 간의 상호 인증을 제공함으로써 기본 GSM 인증 메커니즘의 성능을 개선합니다.

클라이언트 측에서는 스마트카드 판독기(Smartcard reader) 및 SIM과의 연동에 필요한 코드와 EAP SIM 프로토콜이 EAP SIM 요청자에서 구현됩니다. 요청자 코드는 운영체제가 제공하는 EAP 프레임워크로 연결됩니다. 현재 Microsoft Windows XP 및 2000에서 요청자 코드를 사용할 수 있습니다. EAP 프레임워크는 EAP 프로토콜 메시지와 요청자 및 AAA 서버 간의 통신을 처리합니다. 또한 클라이언트의 WLAN 라디오 카드에서 요청자가 제공하는 암호화 키를 설치합니다.

네트워크 측에서는 EAP SIM 인증자 코드가 서비스 제공자의 AAA 서버에 상주합니다. 이 코드는 EAP SIM 프로토콜의 서버측을 처리할 뿐만 아니라 서비스 제공자의 AuC와 통신하는 일을 담당합니다. 시스코의 EAP SIM 구현에서 AAA 서버는 IP와 시그널링 시스템 7(SS7) 네트워크 사이의 게이트웨이 역할을 하는 Cisco ITP(IP Transfer Point)와 통신합니다. Cisco ITP는 AAA 서버의 메시지를 표준 GSM 프로토콜 메시지로 변환한 다음 AuC로 전송합니다.

시스코의 EAP SIM 구현을 사용한 802.1X 인증 순서는 다음과 같습니다(그림 36).

1. 클라이언트의 EAPOL(EAP-over-LAN) Start 메시지가 인증 프로토콜을 시작하며, 클라이언트가 EAP를 사용하여 인증하고자 함을 액세스 포인트에 알립니다.

2. 이에 대한 응답으로 액세스 포인트가 EAP Identity Request 메시지를 클라이언트로 전송합니다. 이 시점에서 클라이언트가 아직 IP 주소를 할당 받지 못한 상태이면 액세스 포인트는 인증에 필요한 메시지(EAP 및 EAP SIM 프로토콜 메시지)를 제외한 모든 메시지를 클라이언트가 보지 못하도록 차단합니다.

3. 클라이언트가 액세스 포인트의 요청에 대해 사용자의 네트워크 ID를 포함한 EAP Identity Response 메시지를 전송합니다. 이 ID는 클라이언트에 첨부되거나 통합된 카드 판독기를 사용하여 SIM 카드에서 판독됩니다. ID 형식은 0〈IMSI〉@〈realm〉입니다. 여기서 〈IMSI〉는 GSM 네트워크에서 사용되는 국제 이동 가입자 ID이며 〈realm〉은 운영자의 도메인 이름 문자열(예: voicestream.com)입니다. 네트워크 ID는 SIM에 저장되어 서비스 제공업체가 확인합니다. 이것은 사용자의 로그인 자격 증명과 다를 수도 있으며 주로 WLAN에 대한 액세스를 인증하는 데 사용됩니다.

4. 액세스 포인트가 시스코 벤더 고유의 속성을 가진 RADIUS 프로토콜 메시지를 사용하여 EAP Identity Response 메시지를 AAA 서버로 전달합니다.

5. AAA 서버가 사용자가 구성 파라미터를 기준으로 EAP SIM 인증을 사용할 것인지 아니면 전달된 ID를 기준으로 할 것인지를 확인한 다음 EAP SIM 확장 코드를 호출합니다. 이 코드는 EAP SIM Start 요청을 다시 클라이언트에게 전송하여 EAP SIM 확장 프로토콜을 시작합니다. 또한 GSM triplet의 (구성 가능한) 수를 요청하는 AuC에 GetAuthInfo 메시지를 생성할 수도 있습니다. 이 단계는 EAP SIM Start 메시지가 수신되어 클라이언트가 실제로 EAP SIM 프로토콜을 지원하게 될 때까지 지연될 수 있습니다.

**주**: ID 문자열에 포함된 도메인에 따라 AAA 요청이 로컬 AAA 서버에서 서비스 제공자의 AAA 서버로 위임되어야 할 경우도 있습니다.

6. GetAuthInfo 메시지가 서비스 제공업체의 SS7 네트워크에 대한 게이트웨이 역할을 하는 ITP MAP(Internet Transfer Point Mobile Application Part) 프록시로 라우팅됩니다. ITP는 요청을 AuC로 전송하기 전에 표준 GSM MAP GetAuth 요청으로 변환합니다.

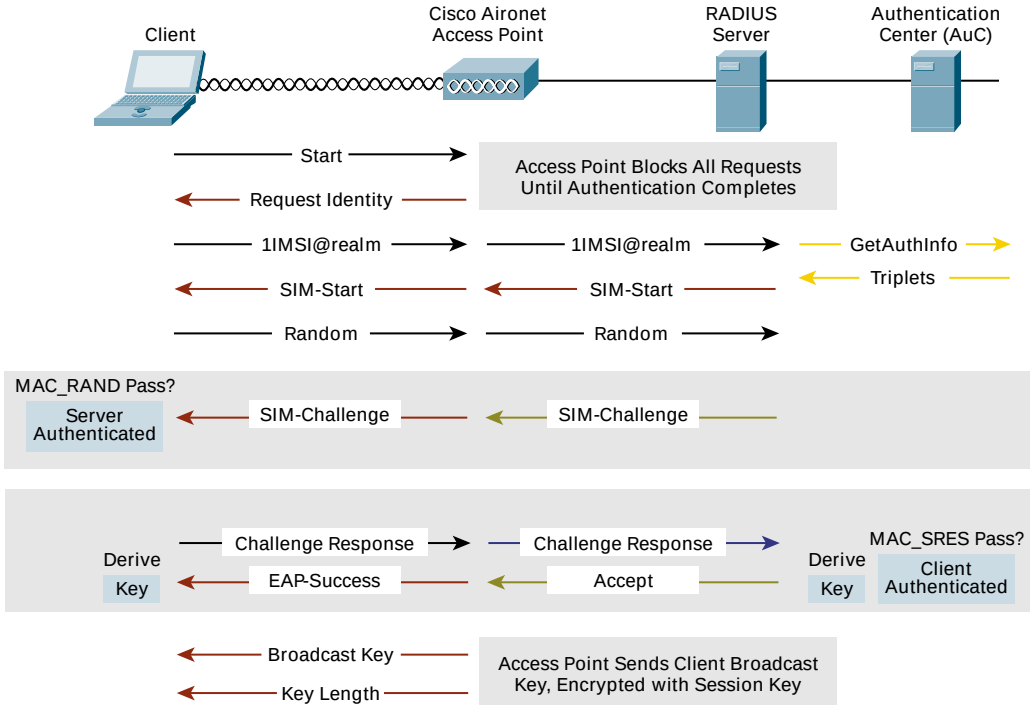
7. EAP SIM Start 요청을 수신한 클라이언트가 SIM에서 생성된 128비트(16바이트)의 난수를 읽고 EAP SIM Start 응답에서 AAA 서버로 다시 전달합니다.

8. AAA 서버가 클라이언트의 EAP SIM Start 응답과 충분한 수의 GSM triplet(대개는 2 또는 3)을 포함한 응답을 AuC로부터의 수신하면 AuC에서 수신한 난수(RAND)와 160비트(20바이트) 메시지 인증 코드(MAC_RAND)를 포함한 EAP SIM Challenge 메시지를 구성합니다.

9. 클라이언트가 EAP SIM Challenge 요청을 SIM 카드로 전달하면 SIM 카드는 자체 MAC_RAND를 먼저 계산합니다. 그 결과가 서버에서 수신된 MAC_RAND와 일치하는지 확인하기 위해 AAA 서버에 대한 유효성 검사가 수행됩니다. 이러한 경우에만 SIM은 수신한 각 RAND에 대한 GSM 결과(SRES) 및 암호화 키(Kc)를 계산하고 그 결과와 사용자 ID를 기준으로 160비트(20바이트) 메시지 인증 코드(MAC_SRES)까지 계산합니다. EAP SIM Challenge 응답에서는 MAC_SRES만 AAA 서버로 반환되어 무선 링크에 노출됩니다. 또한 SIM은 사용자 ID 및 GSM 암호화 키에서 안전한 해시 함수를 사용하여 암호 키 생성 자료를 계산함으로써 세션 암호화 키를 파생시킵니다.

10. AAA 서버가 클라이언트의 EAP SIM Challenge 응답을 수신하면 자체 MAC_SRES를 계산하여 이를 클라이언트로부터 수신한 값과 비교합니다. 두 값이 일치하면 클라이언트가 인증되고 AAA 서버는 세션 암호화 키를 계산합니다. 그런 다음에는 요약된 EAP Success 메시지와 (암호화된) 클라이언트 세션 키를 포함하는 액세스 포인트로 RADIUS ACCEPT 메시지를 전송합니다.
11. 액세스 포인트가 클라이언트의 연결 ID에 대한 세션 키를 설치하고 EAP Success 메시지를 클라이언트로 전달합니다. 그런 다음 클라이언트로 전송하는 EAP Key 메시지에 클라이언트의 세션 키로 암호화된 브로드캐스트 키를 전송합니다. 또한 클라이언트를 위한 데이터 경로 차단을 해제함으로써 IP 트래픽이 클라이언트와 네트워크의 나머지 부분 사이에 전송될 수 있도록 합니다.
12. EAP Success 메시지를 수신한 EAP SIM 요청자가 SIM에서 계산한 세션 암호화 키를 EAP 프레임워크로 반환하여 클라이언트의 WLAN 라디오 카드에 설치되도록 합니다.
13. 이제 클라이언트가 네트워크 트래픽을 안전하게 송수신할 수 있습니다.

**그림 36: EAP SIM 인증**




**주**: 클라이언트의 세션 키는 무선 링크를 통해 전송되지 않으므로 메시지 트래픽에 끼여든 네트워크 침입자가 이를 가로챌 수 없습니다. 마찬가지로 GSM 인증 알고리즘(SRES, Kc) 결과도 무선 링크를 통해 침입자에게 절대 노출되지 않습니다. 따라서 EAP SIM은 무선 전화용 표준 GSM 인증에 비해 네트워크 침입자에게 노출되는 정보가 훨씬 적습니다.

위에서 설명한 모든 메시지 인증 코드는 안전한 키 해싱 알고리즘 HMAC-SHA1(단계 4 및 5)을 사용하여 계산됩니다. 해시 함수는 데이터를 항상 한 쪽 방향으로만 암호화하는 알고리즘이므로 해독하여 원래의 입력 데이터를 파생할 수 없습니다. 이 알고리즘은 사용자 ID, SIM에 의해 생성된 난수, GSM 암호화 키 Kc, 기타 데이터를 사용하여 EAP SIM에 사용되는 인증 코드와 암호화 키를 계산합니다.

시스코의 EAP SIM 구현은 GSM 인증 알고리즘(SRES, Kc) 결과가 SIM을 방치하지 않기 때문에 특히 안전합니다. 따라서 네트워크 침입자가 EAPSIM 요청자 코드를 가로채더라도 액세스가 불가능합니다. 이는 스마트카드(Smartcard) 기술 분야의 선도업체이며 GSM 업계에 SIM 칩을 공급하는 시스코와 Gemplus의 파트너십 덕분에 가능한 것입니다. 표준 GSM SIM 칩 또는 소프트웨어 기반 SIM 에뮬레이터를 사용한 다른 EAP SIM 구현도 가능하지만 시스코 솔루션에 비해서는 안전하지 못합니다.

### 8.3. PEAP(Protected EAP)

PEAP(Protected EAP)는 하이브리드 인증이 가능하도록 설계된 초안 EAP 인증 유형입니다. PEAP는 서버측 PKI 인증을 사용합니다. 클라이언트측 인증의 경우 PEAP는 다른 EAP 인증 유형을 모두 사용할 수 있습니다. PEAP는 서버측 인증을 통해 안전한 터널을 구축하기 때문에 상호 인증 방식이 아닌 EAP 유형은 OTP(one-time password)를 위한 EAP 일반 토큰 카드(GTC)와 암호 기반 인증을 위한 EAP MD5 같은 클라이언트측 인증에 사용할 수 있습니다.

PEAP는 서버측 EAP-TLS를 기반으로 하며 EAP-TLS의 관리 및 확장과 관련된 단점을 해소합니다. 기업은 EAP-TLS의 경우처럼 모든 클라이언트 컴퓨터에 디지털 인증서를 설치할 필요 없이 로그온 암호나 OTP와 같은, 회사의 요구 사항에 가장 적합한 클라이언트 인증 방법을 선택할 수 있습니다.

#### 8.3.1. PEAP 인증 프로세스

PEAP 인증은 EAP-TLS와 같은 방법으로 시작합니다(그림 37).

1 클라이언트가 액세스 포인트에 EAP Start 메시지를 전송합니다.

2. 액세스 포인트가 EAP Request Identity 메시지를 전송합니다.

3. 클라이언트가 EAP Response 메시지에서 사용자 이름에 해당하는 네트워크 액세스 ID(NAI)를 액세스 포인트로 전송합니다.

4. 액세스 포인트가 RADIUS Access Request 메시지에 포함된 NAI를 RADIUS 서버로 전달합니다.

5. 이에 대한 응답으로 RADIUS 서버가 전자 인증서를 클라이언트로 전송합니다.

6. 클라이언트가 RADIUS 서버의 전자 인증서 유효성을 검사합니다.

여기서부터 인증 프로세스는 EAP-TLS의 경우와 달라집니다.

7. 클라이언트와 서버가 암호화된 터널을 결정하여 생성합니다.

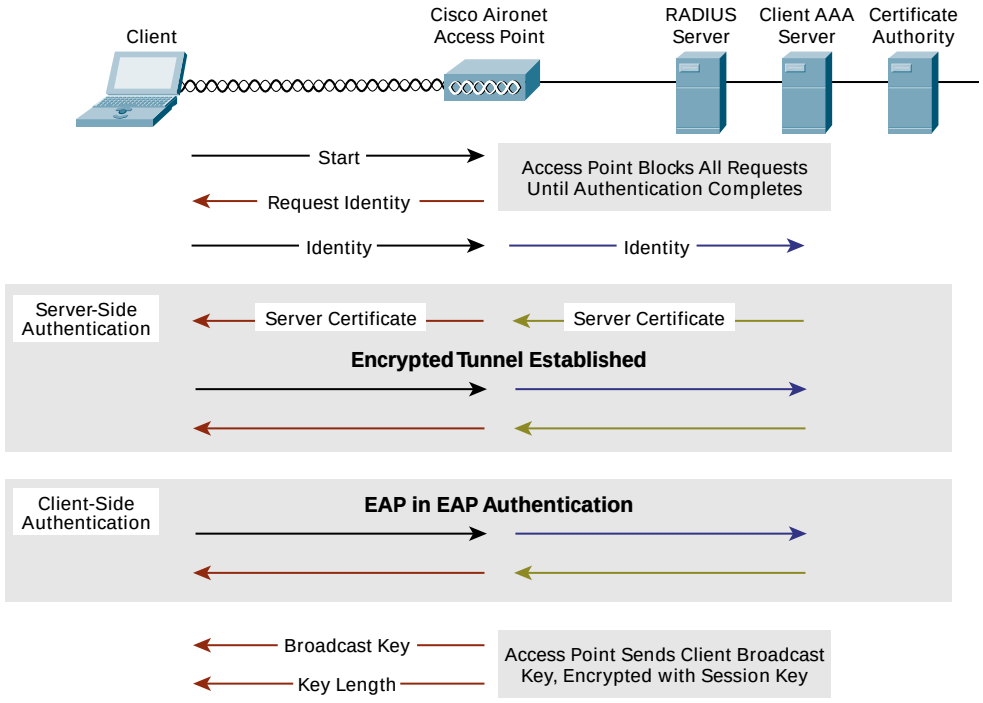
8. 이 터널은 클라이언트 인증을 위해 안전한 경로를 제공합니다.

9. RADIUS 서버가 TLS Record 프로토콜을 사용하여 새 EAP 인증을 초기화합니다.

10. 교환 항목에는 클라이언트 인증에 사용되는 EAP 유형별 트랜잭션이 포함됩니다.

11. RADIUS 서버는 클라이언트의 WEP 키를 포함한 RADIUS ACCEPT 메시지를 액세스 포인트로 전송하여 인증이 성공적으로 이루어졌음을 알립니다.

그림 37: PEAP 인증

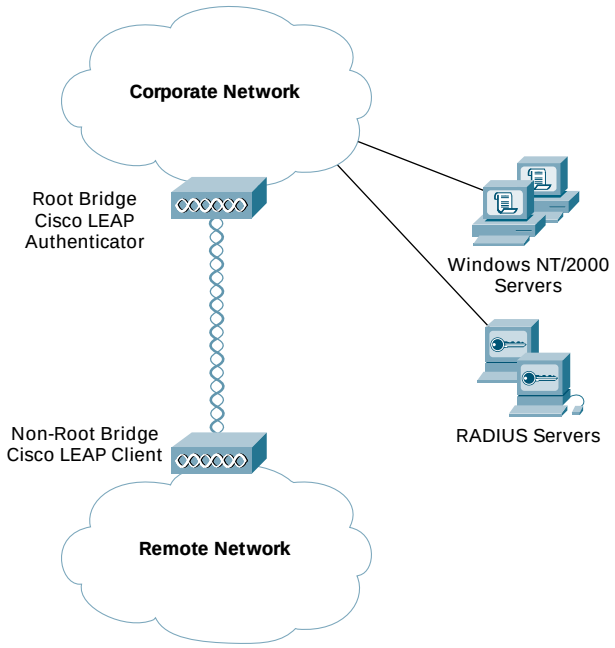

Client
Cisco Aironet Access Point
RADIUS Server
Client AAA Server
Certificate Authority
Start
Access Point Blocks All Requests Until Authentication Completes
Request Identity
Identity
Identity
Server-Side Authentication
Server Certificate
Server Certificate
Encrypted Tunnel Established
Client-Side Authentication
EAP in EAP Authentication
Broadcast Key
Access Point Sends Client Broadcast Key, Encrypted with Session Key
Key Length

## 9. 부록 B – 브리지 구현에서의 Cisco Wireless Security Suite

인증 및 TKIP WEP의 향상된 기능은 인프라의 기본 서비스를 처리하는 데 중점을 두었습니다. 시스코는 포인트-투-포인트 및 포인트-투-멀티포인트 브리지 환경에서 보안 기능을 향상시킬 필요성을 인식하고 있으며, 무선 브리지 링크가 시스코 LEAP 인증 및 TKIP WEP의 향상된 기능을 활용할 수 있도록 브리지 펌웨어에 새로운 기능을 추가했습니다.

그림 38은 전형적인 포인트-투-포인트 브리지 시나리오를 나타낸 것입니다. 루트 브리지는 패킷별 키 생성, MIC, 브로드캐스트 키 순환 등을 비롯하여 802.1X 인증 및 TKIP WEP의 향상된 기능을 지원하도록 구성되어 있습니다.

**그림 38: Cisco LEAP와 TKIP 및 브리지 링크**




비 루트 브리지는 사용자 이름과 암호를 사용하여 정적으로 구성됩니다. 또한 비 루트 브리지는 패킷별 키 생성 및 MIC 기능을 지원하도록 구성되어야 합니다. 브로드캐스트 키는 NIC 기반 클라이언트와 마찬가지로 무선 링크를 통해 비 루트 브리지의 동적 WEP 키로 암호화된 비 루트 브리지로 전송됩니다.

시스코 LEAP 및 TKIP WEP의 향상된 기능을 활용함으로써 무선 브리지 링크는 관리자가 제어하는 재인증(및 WEP 재연결) 간격에 따라 동적 WEP 키를 사용할 수 있습니다.

## 10. 부록 C - 유용한 링크

시스코 무선 LAN 보안 웹 사이트
http://www.cisco.com/go/aironet/security

*Cisco Aironet 무선 LAN 보안 개요*
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

*안전: 무선 LAN 보안 세부 사항*
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

*이동 통신 가로채기: 802.11의 보안 취약 요소*
http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

*802.11 무선 네트워크의 취약 요소*
http://www.cs.umd.edu/%7Ewaa/wireless.pdf

*802.11 무선 네트워크의 취약 요소에 대한 시스코의 응답*
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm

*IEEE 802.1x 표준의 초기 보안 분석*
http://www.cs.umd.edu/~waa/1x.pdf

*IEEE 802.1x 표준의 초기 보안 분석에 대한 시스코의 응답*
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.htm

*WEP 침입을 위한 Fluhrer, Mantin 및 Shamir 공격*
http://www.cs.rice.edu/~astubble/wep/

*시스코 무선 LAN 보안 게시판*
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm

*혼잡한 WAN 링크에서 802.1x 및 EAP를 사용한 인증*
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/authp_an.htm

*Cisco Wireless Security Suite 구성*
http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wrsec_an.htm

*OCB 모드*
http://www.cs.ucdavis.edu/~rogaway/ocb/ocb.htm

*IEEE 802.11 작업 그룹 웹 사이트*
http://grouper.ieee.org/groups/802/11/

CISCO SYSTEMS

www.cisco.com/kr

*2002-12-15*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ■ Gold 파트너 | • ㈜데이콤아이엔 | 02-6747-4700 | • 한국아이비엠㈜ | 02-3781-7800 | • 쌍용정보통신㈜ | 02-2262-8114 |
| | • ㈜데이타크레프트코리아 | 02-6256-7000 | • ㈜콤텍시스템 | 02-3289-0114 | • 에스넷시스템㈜ | 02-3469-2400 |
| | • ㈜인네트 | 02-3451-5300 | • ㈜인성정보 | 02-3400-7000 | • 현대정보기술 | 02-2129-4111 |
| | • ㈜링네트 | 02-6675-1216 | • 한국후지쯔㈜ | 02-3787-6000 | | |
| ■ Silver 파트너 | • 한국휴렛팩커드㈜ | 02-2199-0114 | • 케이디씨정보통신㈜ | 02-3459-0500 | • 대우정보시스템 | 02-3708-8642 |
| | • ㈜시스폴 | 02-6009-6009 | • 한국유니시스㈜ | 02-768-1114, 1432 | • 한국NCR | 02-3279-4423 |
| ■ Local SI 파트너 | • ㈜IG씨엔에스 | 02-6276-2821 | • 포스데이타주식회사 | 031-779-2114 | • 이스텔시스템즈㈜ | 031-467-7079 |
| | • SK씨앤씨㈜ | 02-2196-7114/8114 | | | | |
| ■ Global 파트너 | • 이퀀트코리아 | 02-3782-2600 | | | | |
| ■ Local 디스트리뷰터 | • ㈜소프트뱅크코리아 | 02-2187-0114 | • ㈜인큐브테크 | 02-3497-9303 | • ㈜아이넷뱅크 | 02-3400-7486 |
| ■ IPT 파트너 | • 청호정보통신 | 02-3498-3114 | • IG기공 | 02-2630-5156 | | |
| ■ WLAN 전문 파트너 | • ㈜에어키 | 02-541-1557 | • ㈜텔레트론INC | 02-2105-2300 | | |
| ■ Security 전문 파트너 | • 코코넛 | 02-6007-0133 | • TISS | 051-743-5940 | | |
| ■ NMS 전문 파트너 | • ㈜넷브레인 | 02-573-7799 | | | | |