802.1aa 인증과 802.11i 키교환을 지원하는 라디우스 클라이언트의 구현

함영환, 정병호, 정교일
한국전자통신연구원 정보보호연구본부
{yhham^{O}, cbh, kyoil}@etri.re.kr

The Implementation of Radius Client for 802.1aa Authentication and 802.11i Key Exchange

Young-Hwan Ham, Byung-Ho Chung, Kyo-Il Chung
Information Security Research Division,
Electronics and Telecommunications Research Institute

요 약

최근에 공공장소에서의 보다 안정적이고 고속의 무선 인터넷 접속에 대한 욕구가 커지면서 무선랜에 대한 수요가 많아지고 있고, 유무선 사업자들은 무선랜 시장을 선점하기 위해서 서비스를 서두르고 있다. 이와 같은 무선랜환경에서 안전하게 사용자를 인증하고 서비스를 제공하기 위한 표준으로 802.1aa 와 802.11i 가 있다. 이와 같은 802.1aa 와 802.11i 를 지원하는 액세스포인트를 위해서는 두 표준을 지원할 수 있는 라디우스 클라이언트가 필요하다. 본 논문에서는 위의 액세스포인트가 라디우스 프로토콜을 사용하여 무선단말 사용자를 인증시켜 주고 WEP(Wired Equivalent Privacy)을 위한 키를 교환할 수 있는 라디우스 클라이언트를 설계하고 구현하였다.

1. 서론

최근에 공공장소에서의 보다 안정적이고 고속의 무선 인터넷 접속에 대한 욕구가 커지면서 무선랜에 대한 수요가 많아지고 있고, 유무선 사업자들은 무선랜 시장을 선점하기 위해서 서비스를 서두르고 있다. 그리고 액세스포인트(Access Point) 장비와 무선랜 단말사이의 안전한 인증과 서비스를 위하여 802.1aa 표준이 정의되었다[1]. 802.1aa 는 무선랜 단말이 액세스포인트 장비에 접속하여 서비스를 받고자 할 때 필요한 인증에 대한 방법을 제공한다.

802.1aa 는 PAP, CHAP 을 지원하지 않고 EAP(Extensible Authentication Protocol)만을 지원한다. EAP 프로토콜은 사용자의 인증을 위해서 MD5, TLS, SRP(Secure Remote Protocol)와 같은 다양한 인증메카니즘을 사용할 수 있게 한다[2][3][4][5][6]. 또한 인증서버(authentication server)를 EAP 서버와 분리시킬 수 있도록 함으로써, 보다 유연하고 확장가능한 시스템을 구축할 수 있다. 여기에서는 EAP 서버 즉 인증서버의 역할을 하는 서버를 라디우스 서버로 가정한다. 본 논문에서는 위의 액세스포인트가 라디우스 프로토콜을 사용하여 무선단말 사용자를 인증시켜 주고 WEP(Wired Equivalent Privacy)을 위한 키를 교환할 수 있는 라디우스 클라이언트를 설계하고 구현하였다.

2. 라디우스 클라이언트의 설계

2.1 시스템의 구성요소

무선랜환경에서는 IEEE 802.1aa 표준을 이용하여 인증을 받기 위해서는 Supplicant(wireless terminal), 액세스포인트 그리고 Authentication Server 가 필요하다. Authentication 서버로는 Radius 서버나 보다 확장되고 개선된 표준인 Diameter[7]를 따르는 서버를 이용할 수 있는데 여기서는 Radius Server 를 Authentication Server 로 이용하는 것으로 가정한다[8].

802.1aa 를 지원하는 액세스포인트는 EAP 를 이용하여 authentication server 에게 인증을 요청하는데, 이때 액세스포인트는 *Supplicant* 의 EAP 패킷을 받아 이것을 Radius 패킷으로 Encapsulaton 한 다음 Radius 서버에게 전달하는 역할을 한다. 반대로 Radius server 의 응답메시지를 *Decapsulation* 한 다음 EAP 패킷을 Supplicant 에게 전달하는 역할을 수행한다. 위와 같은 Radius

Encapsulation/Decapsulation 의 역할을 라디우스 인증 클라이언트 모듈에서 수행한다.

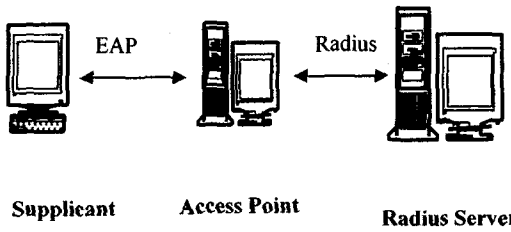

그림 1. 시스템의 구성요소

위와 같은 EAP 에 의한 인증이 성공하고 나면 사용자의 무선랜 서비스 세션(Session)이 시작된다. EAP-TLS 와 같은 인증방식을 쓰는 경우에는 마지막 인증 성공메시지에 TLS 에 의해 생성된 키를 추가함으로써 Supplicant 와 Access Point 사이에 공통된 Shared Key 를 공유하게 한다. Shared Key 를 가지고 802.11i 표준에 의해서 키교환을 할 수 있고 교환된 키는 무선구간의 WEP 암호화에 이용된다.

2.2 라디우스 인증 클라이언트의 설계

라디우스 인증 클라이언트는 크게 라디우스 Encapsulation 모듈과 라디우스 Decapsulation 모듈로 이루어진다. 802.1aa EAP 인증에서 라디우스 클라이언트가 동작하는 방식을 살펴보면 아래의 그림과 같다.

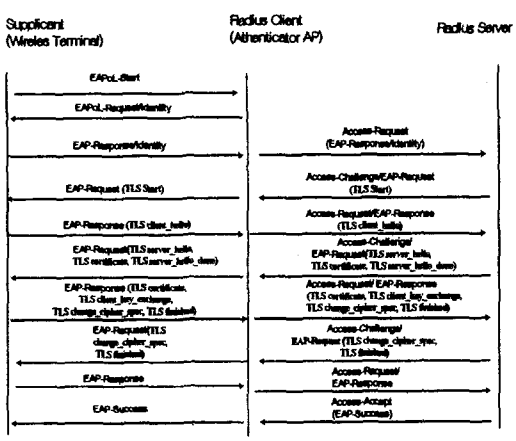

그림 2. EAP-TLS 를 이용한 인증과정

그림에서 보듯이 EAP 를 이용한 인증과정은 비교적 간단하다. Supplicant 가 먼저 접속을 시도하는 경우, EAP-start 메시지를 라디우스 인증 클라이언트에게 보낸고 EAP-Request(Identity)패킷을 Supplicant 에게 보낸다. 인증 클라이언트는 EAP-Request(Identity)메시지를 받으면 메시지안의 ID 정보를 라디우스 메시지안의 User-Name attribute 필드에 넣어서 Access-Request 메시지를 만들어서 라디우스 서버에게 보낸다. 이 때 라디우스 서버는 Access-Challenge 메시지로 응답하고 인증 클라이언트는 메시지를 decapsulation 하여 EAP 메시지를 Supplicant 에게 전달한다. Supplicant 가 인증에 성공하면 라디우스 서버는 Access-Accept 메시지를 인증 클라이언트에게 보내고 클라이언트는 Supplicant 에게 EAP-Success 메시지를 보냄으로써 인증이 완성된다. EAP-TLS 방식의 인증이 사용될 경우에는 EAP-Success 메시지에 TLS 에 의해 생성된 키를 추가해서 보낼 수 있고, 이 키는 Supplicant 에도 존재하게 되므로 Supplicant 와 Access Point 사이에 공통된 키를 갖게되고 이 키는 802.11i 키교환을 위한 PMK(Pairwise Master Key)로 사용된다.

3. 라디우스 클라이언트의 구현

3.1 라디우스에 의한 키전달

라디우스메시지(Access-Accept)에 PMK 을 위한 키값을 넣어서 보내기 위해서는 이것을 위한 AVP 가 필요하고 또한 키값이기 때문에 서버에서는 암호화가 필요하고 클라이언트에서는 복호화가 필요하다. 키의 전달을 위한 라디우스 AVP 로는 RFC2548 (Microsoft Vendor-specific RADIUS Attributes) 에 정의된 MS-MPPE-Recv-Key 를 사용한다.

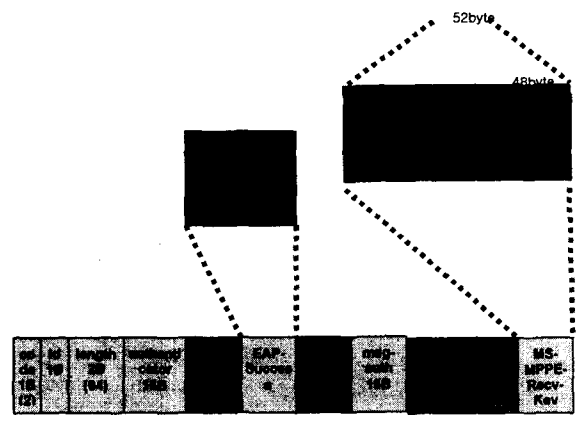

그림 3. MS-MPPE-Recv-Key in Radius Frame

MS-MPPE-Recv 키는 라디우스 클라이언트와 서버사이에 라디우스 보안을 위하여 공유하고 있는 Shared Secret 에 의해서 다음과 같은 방식에 의해서 암호화 된다.

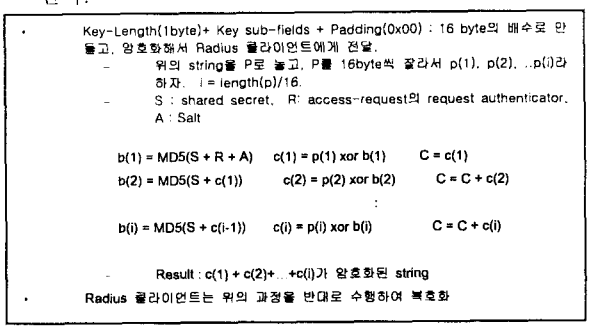

그림 4. MS-MPPE-Recv-Key 의 암호화

3.2 인증 클라이언트의 구현

라디우스 인증 클라이언트는 Supplicant 로부터의 EAP 전송메시지가 있을 때 이를 라디우스 패킷으로 Encapsulation 하여 라디우스 서버에게 전송한다. 이 때 라디우스 헤더안의 Code, Id, Length 가 구성되고 EAP 메시지는 EAP attribute 로 들어가는데 이 attribute 의 데이터 필드 크기가 253 바이트로 제한되었기 때문에 253 바이트를 초과할 경우 몇 개의 attribute 로 나누어서 들어가게 된다. 라디우스 Encapsulation 루틴에서는 UDP 헤더와 라디우스 헤더를 구성하고 EAP attribute 포함된 메시지의 인증을 위하여 전체 메시지에 대한 HMAC-MD5 를 계산하여 "Message-Authenticator" attribute 에 추가한다. . 또 Supplicant 에게 할당된 포트에 적절한 라디우스 Id 를 할당하고 이를 포트번호와 저장해 두었다가 라디우스 서버의 응답이 왔을 경우 응답 메시지안의 Id 와 비교해서 요청한 메시지에 대한 응답인지를 확인한다.

라디우스 Decapsulation 루틴에서는 라디우스 서버의 응답 메시지(Challenge, Accept, Reject)가 왔을 경우 이 메시지를 파싱하고 EAP attribute 안에 들어있는 메시지들을 합하여 하나의 EAP 메시지로 만든 다음 Supplicant 에게 보내는 기능을 수행한다. 이 때 라디우스 헤더안의 Id 를 가지고 Encapsulation 루틴에서 저장한 포트번호를 검색해서 해당하는 포트와 Supplicant 를 식별한다.

```
Void radius_decap()
{
 open socket;
 while()
 {
  listen on opened socket;
  receive the packet;
  parse the Radius_header;
  portnumber = search_radiusID(Id);
  parse radius AVP;
  add_radiusQ();  //radiusQ 에 eap 를 넣어줌
  switch(radius_packet_type) {
      case   Acess_Challenge:
      case   Access_Accept:
      case   Access_Reject :
             call   authentication_related function;

   } //switch end
  } //while end
}
```

그림 5. 라디우스 Decapsulation 모듈 Pseudo Code

4. 결론

AP 장비와 무선랜 단말사이의 안전한 인증과 서비스를 위하여 802.1aa 표준이 정의되었다. 802.1aa 는 무선랜 단말이 액세스포인트 장비에 접속하여 서비스를 받고자 할 때 필요한 인증에 대한 방법을 제공한다. EAP 서버 즉 인증서버의 역할을 하는 서버로서 라디우스 서버가 널리 사용된다. 본 논문에서는 위의 액세스포인트가 라디우스 프로토콜을 사용하여 무선단말 사용자를 인증시켜 주고 802.11i 키교환에 사용될 키를 전달해주는 기능을 수행할 수 있도록 라디우스 클라이언트 시스템을 설계하고 구현하였다. 구현된 클라이언트 시스템은 라디우스 프로토콜 스펙을 준수하였으므로 현재 상용이나 비상용의 라디우스 서버와 함께 802.1aa 및 802.11i 를 준수하는 무선랜 액세스 포인트를 위한 효율적이고 편리한 AAA 시스템을 구축할 수 있다.

참고문헌

[1] IEEE 802.1aa, "IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control", November 2002.
[2] W.Simpson, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.
[3] W.Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.
[4] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP) ", RFC2284, March 1998.
[5] B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.
[6] T.Wu, "The SRP Authentication and Key Exchange System", RFC2945, September 2000.
[7] Pat R. Calhoun, John Loughney, "Diameter Base Protocol", draft-ietf-aaa-diameter-13, October, 2002.
[8] C.Rigney, "Remote Authentication Dial In User Service(RADIUS)" RFC 2865, June 2000.