Mobile IPv6 응용을 지원하는 RADIUS 서버 설계

이해동*, 최두호*
*한국전자통신연구원 정보보호연구단
e-mail : haenamu@etri.re.kr

A Design on Radius-based AAAv6 System Supporting Mobile IPv6

HaeDong Lee *, DooHo Choi *
* Information Security Research Division, Electronics and Telecommunications Research Institute

요 약

RADIUS 프로토콜은 AAA 시스템의 역할을 수행하기 위해서 사용되는 프로토콜로서 널리 사용되어 왔다. RADIUS 는 원래 전화망 사용자의 PPP 서비스를 지원하기 위해 초기에 개발되었고, Mobile IP 버전 4 응용 서비스를 지원하는 범위까지 확장되어 왔다. 본 논문은 RADIUS 시스템이 Mobile IP 버전 6 응용 서비스를 지원하도록 하기 위해서 추가적으로 지원되어야 하는 표준 사항들을 설계하고자 한다. 본 설계는 Mobile IPv6 프로토콜과 RADIUS 프로토콜 정합 구조 및 Mobile IP 세션키 분배 방법을 포함한다.

1. 서론

무선 인터페이스를 장착한 이동 단말 사용자는 언제, 어디서나 네트워크에 접속할 수 있기를 요구하며, 다양한 종류의 단말 장치(PDA, 휴대폰, 스마트폰, 노트북 등등)와 다양한 기술(PSTN, ADSL, PCS, IMT2000, WLAN LAN 등등)을 적용한 네크워크가 존재한다. 위의 네크워크 서비스 제공자는 네크워크를 설계 및 구성하여 사용자들이 자신의 망에 접속하게 하고, 접속 댓가로서 사용자들에게 비용을 부과하는 사업모델을 가진다. 이때 사용자에게 어디서나 망에 접속할 수 있도록 하기 위해서 이동성을 지원하는 프로토콜이 필요하며, 인터넷 망에서 개발되고 있는 프로토콜은 Mobile IP 이다. Mobile IP 는 네트워크 구성을 변경하지 않고, 다른 네트워크 서브넷으로 이동할 수 있게 한다. 또한 네트워크 서비스 사업자는 사용자의 네트워크 엑세스 연결유지 기능의 제공뿐만 아니라 합법적인 사용자의 인증(authentication) 수단, 정책기반의 네트워크 서비스 인가 수단(authorization) 및 사용자의 네트워크 자원사용에 대한 과금(accounting) 수단이 필요하다. 위의 세가지 기능을 통합적으로 제공하는 시스템(AAA)은 서비스 사업자에게 사용자 관리를 효율적으로 수행하도록 지원한다.

Back-end 로 운용되는 AAA 시스템을 구현하기 위해서 다양한 프로토콜이 제안 개발되어 왔다. RADIUS 프로토콜은 전화망 사용자의 PPP 접속의 인증 기능을 제공하기 위해서 설계되었다. 이후 TACAS+, COPS 등이 개발적으로 개발되었다. 이후 RADIUS 프로토콜을 계승하고, 다양한 응용 서비스(Mobile IPv4, SIP 등등)을 지원하는 Diameter 프로토콜이 인터넷 표준 국제기관인 IETF 에서 제정되게 되었다. 그러나 기존의 RADIUS 프로토콜의 확장 및 지원에 대한 요구가 존재한다. 그리고 Mobile IPv4 응용 서비스를 지원하기 위한 AAA 프로토콜로는 Diameter Mobile IPv4 응용이 제안되었으나, Mobile IPv6 를 지원하는 RADIUS 표준의 제안은 현재 이루어 지고 있지 않다. 그 이유로는 IPv4 와는 달리 IPv6 의 대중화는 초기단계이기 때문으로 판단된다. 그러나 국가기관의 IPv6 의 적극적 보급 노력를 감안할 때, Mobile IPv6 를 지원하는 RADIUS 표준의 개발을 서둘러야 하겠다.

본 논문에서는 Mobile IPv6 응용 서비스에 AAA 기능을 제공하는 RADIUS 표준을 확장하고자 한다. 이를 위해서 이동 단말에 대한 인증 방법 및 Mobile IP 세션키 분배 방법, 인증 메시지 구성을 정의한다.

2. 관련 프로토콜 개요

(1) Mobile IP 및 IPsec 의 기능 및 한계점

Mobile IP 는 두 개의 IP 주소(home address, care of address)를 조합하여 네트워크간의 이동중에 네트워크 구성 파라미터를 수정하지 않으면서 네트워크 참조 모델에서의 상위 계층의 끊김없는 연결성을 제공한다. IP 버전에 따라 각각 Mobile IPv4, Mobile IPv6 로 불리며, 서로 다른 표준 문서로 정의되어 있지만 핵심적인 프로토콜의 목적과 두 개의 주소 조합 기법은 동일하다. 본 논문에서는 IP 버전 4 에 따른 Mobile IPv6 를 대상으로 한다.

Mobile IPv6 는 이동성으로 발생하는 문제점을 극복하기 위해 홈에이전트와 이동 노드사이의 보안프로토콜로써 IPsec 프로토콜을 사용하도록 규정하고 있다. 보안 측면의 안전성을 획득하기 위하여 IPsec 프로토콜을 사용하도록 규정하고 있다. IPsec 은 이동 노도와 홈 도메인의 홈에이전트간의 보안 연계(SA)를 설정하고 두 노드사이에서 교환되는 메시지의 인증 기능을 수행한다. 한편, 이동 노드가 다른 사업자의 관리하에 있는 망으로 로밍을 하는 경우, 이동 단말은 타 사업자 망에서 네트워크에 접속할 수 있는 권한을 인증받아야 한다. 그러나 IPsec 에서는 이동 노드가 타 사업자의 관리망으로 이동할 경우, 그 망에서는 이동 노드가 정상적으로 등록된 노드인지를 인증할 수 없다. 우리는 서로 다른 사업자 망간에 인증, 인가, 과금등의 정보를 글로벌하고 안전한 채널을 통해 주고 받을 수 있는 AAA 인프라 구조가 필요하다. 본 논문에서는 AAA 인프라 구조를 구현할 프로토콜로서 RADIUS 를 선택한다.

(2) 보안 및 인증 기법의 개요 및 문제점

AAA 인프라를 통하여 인증, 인가, 과금 기능을 제공받는다하더라도, 전술한 바와 같이 Mobile IPv6 는 이동 노드와 홈 에이전트간에는 IPsec 를 통하여 보안 기능을 사용하도록 규정한다. 또한 IPsec 이 정상적으로 운용되기 위해서는 사전에 위의 두 노드사이에 보안 키가 안전하게 공유되어 있어야 한다. IKE 프로토콜은 두 노드가 공유하는 보안 연계를 협상하고 설정하는 기능을 제공한다. 그러나 IKE 는 다양한 키 교환 방식, 여러 가지 표준, 다양한 협상 방법의 허용 등의 복잡성, 상호 연동성 문제, 서비스 거부 공격에 취약, 무선 단말기에는 무거운 프로토콜로서 무선 응용 적용에 제약점을 가진다. 본 논문에서는 AAA 인프라 구조를 이용하여 IKE 의 문제점을 보안하고자 한다.

이동 노드가 타사업자가 관리하는 망으로 로밍할 경우 Mobile IPv6 프로토콜상의 등록 과정 이전에 RADIUS 서버로부터 인증 및 인가를 받고, 과금 작업을 위한 파라미터 교환을 받아야 한다. 즉 이동 노드와 RADIUS 서버 사이에 필요한 인증방법이 정의 되어야 한다. 본 논문에서는 EAP 인증 방법을 적용하여 다양한 인증 기법의 수용을 가능케 하고자 한다.

3. AAA 네트워크 기반 구조 및 메시지 교환

그림 1 은 Mobile IPv6 프로토콜을 사용하는 이동 단말에 글로벌 로밍을 지원하는 AAA 네크워크 기반 구조를 나타내었다.

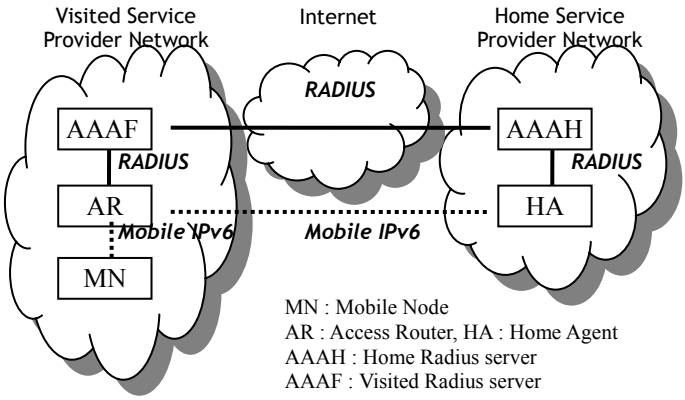

그림 1. Mobile IPv6 서비스를 지원하는 AAA 기반구조

AAA 인프라를 구성하기 위해서 RADIUS 프로토콜을 적용한 AAA 서버를 각각의 관리망에 배치한다. 각각의 서버는 이동 단말의 소속에 따라 AAAF, AAAH 의 역할을 수행한다. AAAH 는 이동 단말의 홈 네트워크에 존재하는 AAA 서버로서 인증, 인가, 과금 정보에 대한 사용자 프로파일 정보를 관리한다. AAAF 는 이동 단말이 현재 위치한 방문 네트워크에 존재하는 서버로서 인증 메시지의 라우팅을 담당한다. 이때의 라우팅은 이동 단말을 식별하는 NAI 의 도메인 영역정보 기반의 라우팅을 의미한다. 홈에이전트(HA)는 Mobile IPv6 프로토콜에서 정의하는 시스템으로서, 이동 단말에 설정된 두 IP 주소에 대한 바인딩 정보를 관리한다. 홈에이전트와 엑세스라우터(AR)는 원래의 기능이외에 AAA 인프라와 통합되기 위해서, RADIUS 클라이언트로 동작하여야 하며, 이동 단말로부터 수신한 인증정보를 RADIUS 메시지로 변환하는 기능을 수행한다.

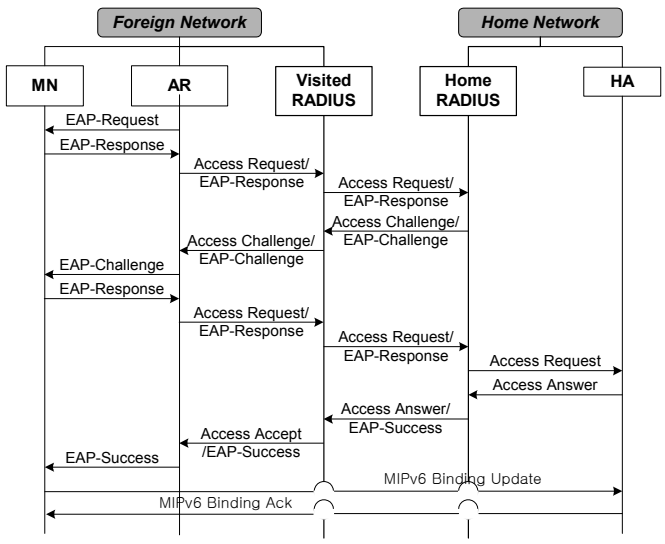

그림 2. RADIUS 메시지 교환

RADIUS 포로토콜의 동작은 그림 2 와 같다. 사용자가 먼저 접속을 시도하는 경우, EAP-Start 메시지를 AR 에게 전송한다. AR 은 EAP-Start 메시지를 받으면 이동 노드에게 인증에 필요한 신원(Identity) 정보를 요청하는 메시지를 보낸다. 이어 Challenge-Response 를 통해 인증이 완료된 후, 그 결과에 따라 인증 성공/실패 메시지가 AR 에 전송되면 인증 과정이 완료된다.

4. 세션키 분배 기법

Mobile IPv6 는 이동 노드와 홈 에이전트사이에 IPsec 를 사용하여 바인딩 메시지, Return Routability 메시지의 안전한 전송을 요구한다. 두 종단 노드사이에 IPsec 를 사용하기 위해서, 먼저 두 종단 노드는 서로 보안 키를 공유해야 한다. 이러한 키들은 특정 세션의 활성 시간 동안 유효해야 한다. 본 논문에서는 상기 키를 세션키라고 호칭한다. IPsec 표준은 키의 협상, 교환, 설정을 수행하는 키 분배 프로토콜인 IKE 를 정의한다. 그러나 이동 노드로 사용되는 셀룰라폰, 스마트폰, PDA 등의 휴대 장비는 저전력, 저용량, 저컴퓨팅파워를 가지고, 무선망 특성상 저대역폭을 가진다. 다양한 키 교환 방식을 포함한 IKE 의 복잡성, 무선 단말기에는 무거운 처리 요구 등으로 인하여, 이동 노드에서 수용하기에 적합하지 않다.

본 논문에서는 IKE 를 사용하지 않고 IPsec SA 설정을 수행하는 방법을 제안하고 있다. AAA 인프라 구조에서는 사용자가 인증을 받기 전에 홈망과 방문망 사이의 보안 채널이 사전에 설정되어 있다.

IKE 는 IKE SA, IPsec SA 으로 구성된 두 phase 와 SA 를 정의한다. Phase 1 은 IKE SA 를 만들고, Phase 2 는 IPsec SA 를 만든다. 그러나 우리는 IKE Phase 1 를 수행하지 않는다. 즉 IKE SA 가 설정되지 않는다. AAA 서버는 IPsec, TLS 를 사용하여 AAA 서버간의 채널을 보호하고 있다. 비록 사전에 설정된 AAA 보안 채널이 있더라도, IPsec 를 위한 보안 파라미터는 이동 노도와 홈 에이전트에 전달되어야 한다.

Table 1 SPI Table Example

SPI	AH	ESP	Proposal
450	HMAC-MD5	3DES with HMAC-MD5	Transform1
451	HMAC-SHA1	3DES with HMAC-SHA1	Transform2
452	HMAC-MD5	3DES with HMAC- SHA1	Transform3

RADIUS 서버는 이동 노드와 홈 에이전트사이의 IPsec SA 를 결정한다. 이동노드와 홈에이전트는 IP 주소에 의해 식별된다. AAA 서버는 SA 식별자로 IP 주소, SPI 값, 키 material, NAI 의 묶음을 사용한다. Radius 서버는 인증 과정이 끝나면, 키 분배를 위한 과정을 수행하는데 이때 SPI value 와 key material 를 결정한다. 그림 1 과 같이, RADIUS 서버는 인증 결과와 키 정보를 Access-Answer 에 포함시켜서 RADIUS 클라이언트에게 전송한다. RADIUS 클라이언트는 NAS, AP, 혹은 AR 에 구현할 수 있다. 위의 Access Answer 메시지를 수신한 클라이언트는 MN 과 정의한 프로토콜을 통해서 위 정보를 전달한다. 서버는 홈에이전트에게 SPI value, AH 세션키, ESP 세션키를 전송한다. 세션키는 Key material 로부터 유도된다. 그리고나서 MN 과 HA 는 IPsec SA 를 설정할 수 있다.

전송되는 key material 와 세션 key 는 기밀성이 보장되어야 한다. 이동 노드와 AAA 서버사이에서는 Shared secret 를 이용하여 key material 의 기밀성을 보장할수 있다.

세션 키는 shared-secret 없이 key material 로부터 유도될 수 없다. 홈 에이전트는 shared-secret 를 알수 없기 때문에 key material 를 알고 있다하더라도 세컨키를 도출해 낼 수 없다. 그래서 홈에이전트의 경우에는 다른 방법이 적용되어야 한다. AAAH 와 홈 에이전트사이에는 IPsec 혹은 TLS 에 의한 보안 채널이 설정되어 있다. 이 채널에 의해서 AAAH 와 홈에이전트 사이의 세션키의 전송은 안전함을 보장할 수 있다..

Shared secret 은 EAP 인증 과정에서 생성되거나, long-term password 로 가지고 있게 된다. EAP 인증 과정에서 생성될 때, shared secred 은 EAP 인증 알고리즘에 따라 다른 방법으로 만들어진다. 다음은 인증 방법에 따라 달리 생성되는 shared secret 를 정리하였다.

➢ 이동단말과 AAA 서버사이의 shared secret

- EAP-MD5: long term shared secret 로 사용되는 패스워드.
- EAP-SRP: K = SHA_Interleave(S), EAP-SRP 인증 과정중에 공유.
- EAP-TLS, EAP-TTLS, EAP-PEAP: HMAC_MD5(client MAC, server MAC), TLS 핸드쉐이킹 과정에서 클라이언트 MAC 값과 서버 MAC 값을 획득(단 EAP-TTLS, EAP-PEAP 의 경우 단계(phase) 1 에서 획득).

RADIUS 서버는 이동단말과 홈에이전트사이의 안전한 통신을 위해서 IPsec SA 를 설정하고, SAD(Security Association Database)를 관리한다.

➢ 서버의 키 정보 전달 동작 순서

(1) 먼저, 서버는 이동 단말, 홈에이전트, AAA 서버사이에서 공유 하는 SPI 테이블에서 SPI value 를 선택한다. 각각의 SPI value 는 AH 프로토콜 및 ESP 프로토콜에서 사용된다..

(2) 서버는 세션키 생성 입력값으로 사용될 key material 를 만든다. Key material 은 의사 랜덤 넘버 생성기(pseudo-random number generator)에 의해 만들어지고, 128 bit pseudo-random value 이다. Pseudo-random number generator 는 cryptographic 랜던값 생성기에 의해 만들어 져야 한다..

(3) Radius 서버는 AAA 인증 과정이 끝나면 SPI value, AH Security Key, ESP Security Key 를 HA 에게 전송한다. Access-Request 메시지를 이용함
(4) Radius 서버는 마지막 전송 메시지인 Access-Accept 에 SPI value, key material 를 attribute 형태로 MN 에게 전달한다.
(5) 서버는 해킹에의한 키의 노출을 막기위해서 계산된 세션키를 삭제한다.

➢ 키 유도 방법 (Session Key Calculation)

세션키는 해쉬함수의 출력값으로 만들어 진다. 이때, 해쉬 함수의 입력값은 생성된 key material, 이동 단말과 AAA 서버사이에서 공유되는 shared secret, 사용자를 식별하는 NAI 가 된다. AH security key and ESP security key 는 해쉬 함수의 출력값인 MAC 이다. 사용될 수 있는 해쉬 알고리즘으로는 HMAC_MD5, HMAC_SHA1 등이 있다.

- *AH Security Key*
  = HMAC_MD5(shared secret, key material|NAI|1)

- *ESP Security Key(Authentication)*
  = HMAC_MD5(shared secret, key material|NAI|2)

- *ESP Security Key(Encryption)*
  = HMAC_MD5(shared secret, key material|NAI|3)

5. 결론

본 논문에서는 인증 프로토콜로 널리 사용되는 RADIUS 를 차세대 인터넷 프로토콜로 사용될 IP 버전 6 기반의 Mobile IP 버전 6 서비스를 지원하기 위하여 필요한 제반 사항을 기술하였다. 즉 Mobile IP v6 프로토콜와 RADIUS 프로토콜이 연동하여 이동 사용자에 대한 인증/인가 서비스를 제공하기 위하여 추가적으로 정의되어야 하는 정합 구조를 기술하고 세션 키 분배 기법을 제안하였다. 제안 한 세션 키 분배 기법은 저전력, 저컴퓨팅파워를 가진 단말을 가진 사용자에게 더욱 빠른 인증 속도를 제공할 것이다.

참고문헌

[1] Marie Kim, Hyungon Kim, “The Diameter AAA Mobility Support for MIPv6”, WSEAS Issue2, Vol. 3, April 2004
[2] L. Blunk, and J. Vollbrecht, “PPP Extensible Authentication Protocol (EAP)”, RFC 2284, March 1998.
[3] B. Aboba and D. Simon, “PPP EAP TLS Authentication Protocol”, RFC 2716, October 1996.
[4] Paul Funk. Simon Blake-Wilson, “EAP Tunneled TLS Authentication Protocol (EAP-TTLS)”, draft-ietf-pppext-eap-ttls-01.txt, February 2002.
[5] 송지은, 왕기철, 김태연, 조기환, “무선 LAN 환경에서 요구되는 보안기술”, 7`정보처리학회지 제 10 권 제 2 호
[6] HaeDong Lee, DooHo Choi, HyunGon Kim, ”Mobile IPv6 Session Key Distribution Method At Radius-based AAAv6 System”
[7] Glen Zorn, Daniel Simon, Ashwin Palekar and Simon Josefsson, “Protected EAP Protocol (PEAP)”, draft-josefsson-pppext-eap-tls-eap-06.txt, March 2003.
[8] G. H. Kildong, “The SRP Authentication and Key Exchange System”, RFC 2945, September 2000.
[9] T. Dierks and C. Allen, “The TLS Protocol Version 1.0”, RFC 2246, January 1999.
[10] C. Rigney, A. Rubens, W. Simpson and S. Willens, “Remote Authentication Dial In User Service (RADIUS)”, RFC 2865, June 2000.
[11] Pat R. Calhoun, and Tony Johansson, “Diameter Mobile IPv4 Application”, draft-ietf-aaa-diameter-mobileip-19.txt, July 2004.
[12] P. Eronen and T. Hiller, “Diameter Extensible Authentication Protocol (EAP) Application”, draft-ietf-aaa-eap-08.txt, June, 2004.
[13] D. Johnson and C. Perkins, “Mobility Support in IPv6”, RFC 3775, June 2004.