Mobile IPv6 Session Key Distribution Method At Radius-based AAAv6 System

HaeDong Lee *, DooHo Choi ** and HyunGon Kim ***
AAA Security Information Research Team, Electronics and Telecommunications Research Institute, Daejeon, 305-350, Korea
* Tel : +82-42-860-1560 Fax : +82-42-860-5611 E-mail: haenamu@etri.re.kr
** Tel : +82-42-860-1762 Fax : +82-42-860-5611 E-mail: dhchoi@etri.re.kr
*** Tel : +82-42-860-5428 Fax : +82-42-860-5611 E-mail: hyungon@etri.re.kr

Abstract: Currently, there are many subscriber access networks : PSTN, ADSL, Cellular Network, IMT200 and so on. To these service providers that provide above network service, it is important that they authenticate and authorize legal subscribers and account for their usage. At present, There exist the several protocols that support AAA(Authentication, Authorization and Accounting) service : RADIUS, Diameter, TACACS+. Nowadays, RADIUS has used for AAA service widely. It has been extended to support other access network environment. So, we extend RADIUS to support environment of Mobile IPv6. Mobile IPv6 uses IPsec as a security mechanism, basically. But, IPsec is a heavy security technology for small, portable, mobile device. Especially, it is serious at IKE, the subset of IPsec. IKE is a key distribution protocol that distributes the key to the endpoints of IPsec. In this paper, we extend RADIUS to support environment of Mobile IPv6 and simplify the IKE phase of IPsec by AAA system distributing the keys by using its security communication channel. Namely, we propose the key distribution method for IPsec SA establishment between mobile node and home agent. The suggested method was anticipated to be effective at low-power, low computing device. Finally, end users feel the faster authentication.

About AAA, Mobile IP, IPsec

1. INTRODUCTION

Currently, There are many subscriber access networks : PSTN, ADSL, Cellular Network, IMT200 and so on. These service providers that provide above network service deploy the network infrastructures and they need operating and managing them. And there are more things. The First, they validate the end user's identity prior to permitting them network access. The second, they define what rights and services the end user is allowed once network access is granted. The third, they need to collect information about the end user's resource consumption, which can then be processed for billing, auditing, capacity–planning purposes. AAA system provides the above facilities.

There exist the several protocols that support AAA(Authentication, Authorization and Accounting) service : RADIUS, Diameter, TACACS+ . RADIUS was developed for dial-up PPP user. Diameter, as a new AAA protocol, has inherited the method of the previous protocol, RADIUS and expand the facilities. And Diameter support s the various access applications (Mobile IP, SIP and so on). But, nowadays, RADIUS has used for AAA service widely. It has been extended to support other access network environment.

Mobile IPv6 (MIPv6) specifies routing support to permit an IPv6 host to continue using its permanent home address as it moves around the Internet. Mobile IPv6 supports transparency above the IP layer, including maintenance of active TCP connections and UDP port bindings. MIPv6 defines using IPsec for security between mobile node and home agent, basically. In this paper, we focus IPsec authentication key and encryption key distribution method.

1.1. Combination of Mobile IP and RADIUS AAA

This paper contains the technical issue related to development of RADIUS-based AAAv6 system supporting MIPv6 environment. By RADIUS AAAv6 system combined with MIPv6, MIPv6 will have the various and flexible network deployment scenarios. For example, originally, mobile node demand static home address in Mobile IP protocol, even if it moves another prefix network. But AAA server may dynamically allocate home address for mobile node within any address dynamically. And with help of AAA server, home agent can be allocated to mobile node whether at the home network or at the foreign network. Furthermore, AAA server may be designed to be involved in the key distribution of IPsec security key. In other words, it can be possible that we can simplify the IKE phase by using AAA infrastructure

1.2. EAP Authentication Method

In this paper, we assume that EAP(Extensible Authentication Protocol) method should be used for authentication between mobile node and AAA server. EAP is a general protocol for authentication which supports multiple authentication mechanisms. EAP does not select a specific authentication mechanism at link control phase, but rather postpones this until the authentication phase. This allows the authenticator (for example NAS) to request more information before determining the specific authentication mechanism. This also permits the use of a back-end server(AAA server) which actually implements the various mechanisms while the authenticator merely passes through the authentication exchange. In accordance

with authentication phase, There are several specific methods : EAP-MD5, EAP-TLS, EAP-TTLS, EAP-SRP and PEAP.

1.3. IPsec and IKE

IPsec is designed to provide privacy and authentication services at the IP layer by using cryptography. To protect the contents of an IP datagram, the data is transformed using encryption algorithm. There are two main transformation types that form the basics of IPsec, the Authentication Header(AH) and the Encapsulating Security Payload(ESP). Both AH and ESP are two protocols that provide connectionless integrity, data origin authentication, confidentiality and an anti-replay service.

In order to use IPsec between two endpoints, at first two endpoints exchange the security key with each other. The purpose of IKE is to negotiate, and provide authenticated keying material for, security associations in a protected manner. IKE defines two separated phases and SA(security associations) ; IKE SA, IPsec SA. Phase 1 make IKE SA. After phase 2, IPsec SA will be established. But IKE needs many round trip at network and computing power to operate. Finally it causes time delay. Especially, small, portable device with low battery and low computing power has limitation.

In the paper, we suggest a method of IPsec SA establishment without IKE, by exchanging SA parameter through AAA secure channel. Section 2 contains a look at the message flow when RADIUS AAAv6 server supports Mobile IPv6 Application. In Section 3, we describe key distribution method for IPsec SA Establishment, which is made by AAA server's assistance. Also Section 3 shows the behavior of individual nodes; mobile node, home agent, AAA server. Finally, Section 4 contains conclusions.

2. COMBINED RADIUS & MOBILE IPV6

Center the title on the top of page so as it runs across the both columns. Paper title in bold letters followed by the author's names and their addresses. EAP PDU is conveyed between mobile node and authenticator. RADIUS PDU is exchanged between authenticator and RADIUS proxy, between proxy and RADIUS server, between server and home agent. Namely, at first, mobile node send EAP message to authenticator. And then authenticator translate RADIUS message from EAP message and send RADIUS message to RADIUS infrastructure. Radius server receives RADIUS Access-Request message and processes the message. If authentication will be success, the server send Access-Request message including SA information to home agent. If home agent was not specified, the server can allocate home agent dynamically for mobile node.

After authentication process ends at AAA message flow, binding process starts. Mobile node sends binding-update message, home agent responds by binding-acknowledge message.

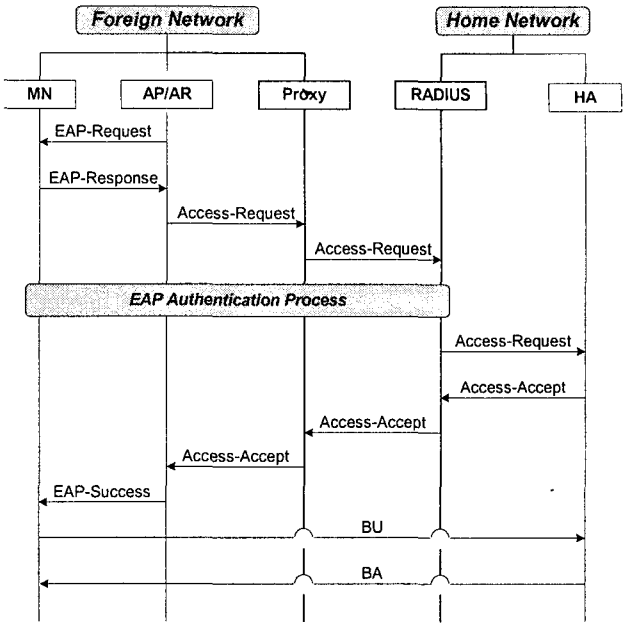

Fig. 1. Message Flow for Radius AAA.

3. KEY DISTRIBUTION METHOD FOR IPSEC SA ESTABLISHMENT

Mobile IPv6 requires secure exchange of binding message by using IPsec between mobile node and home agent. In order to use IPsec between two endpoints, at first two endpoints share the security keys with each other. These keys must be valid for time duration of a specific session. So in this paper, we call these keys session keys. IPsec defines key distribution protocol, IKE, that exchanges these session keys securely. But as portable device(cellular phone, smart phone, PDA, Notebook), used as mobile node has limited battery power, and computing capacity and key exchange flow causes time delay, it can not be afford to end user.

In the paper, we suggest a method of IPsec SA establishment without IKE, by exchanging SA parameter through AAA secure channel. IKE defines two separated phases and SA(security associations) ; IKE SA, IPsec SA. Phase 1 make IKE SA. After phase 2, IPsec SA will be established. But we do not IKE phase 1, namely IKE SA will not be established. AAA servers made secure channel by IPsec and TLS. Through the previous established AAA secure channel, security parameters for IPsec SA should be designed to be exchanged.

In order to perform the key distribution between mobile node and home agent, the three nodes, RADIUS server, mobile node and home agent previously share the SPI table that contains SPI(arbitrary 32 bit value above 256) and AH Proposal-Transform, ESP Proposal-Transform.

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 server determines IPsec SA between specific mobile node and specific home agent. Mobile node and home agent is identified by its IP address. RADIUS server linkes IP address, SPI, key material, NAI(Network Authentication Identifier) as one SA identifier. And RADIUS server sends SPI value and key material to mobile node finally. Like the figure 1, RADIUS server sends Access-Answer message including attributes that be encapsulated by above SA parameters to RADIUS client. RADIUS client may be NAS, AP or AR. And then parameters are exchanged between mobile node and AAA client. But we do not specify any particular mechanism to convey information between the mobile node and the AAA Client: in a different suitable manner outside the scope of this document (e.g. ICMP, the protocol defined by the PANA WG, etc.). And the server sends SPI values, AH session key and ESP session key to home agent. Session key will be derived from Key material. And then both of mobile node and home agent can establish IPsec SA.

Transmitted key material and session key can be guaranteed. Shared secret will be needed to be shared between mobile node and AAA server. Session key can not be derived from key material without shared-secret. But home agent does not have the shared-secret, so home agent can not calculate session key even if it knows key material. Thus, different method has to be. But there exists AAA secure communication. Session key between AAA server and home agent will not be disclosed.

Shared secret that is shared between mobile node and RADIUS server may be determined in accordance to EAP authentication algorithm. The following table shows shared secret per individual EAP algorithm.

Table 2 Shared Secret

Authentication Method	Shared secret
EAP-MD5	long term shared secret(password) between MN and RADIUS Server
EAP-SRP	K=SHA_Interleave(S), which is shared during EAP-SRP authentication process
EAP-TLS, EAP-TTLS, EAP-PEAP	HMAC_MD5(client MAC, server MAC), where client MAC and server MAC is obtained by the TLS handshaking process(In the case of EAP-TTLS, EAP-PEAP, phase 1).

4. INDIVIDUAL NODE BEHAVIOR

4.1. Behavior of Radius-based AAAv6 Server

RADIUS server manages SAD(Security Association Database) establishing IPsec SA for secure communication between mobile node and home agent. At first, server selects SPI values from the SPI table that mobile node, home agent and AAA server share. Each SPI value is for AH protocol and ESP protocol.
The Second, server makes key materials for session keys. Key material is made by pseudo-random number generator and is 128 bit pseudo-random values. Pseudo-random number generator should be cryptographic random number generator.

Generated key material, shared secret shared between mobile node and AAA server, NAI(Network Authentication Identifier) will be input to hash function. AH security key and ESP security key is hash function output, MAC value There are 2 hash algorithms for use; HMAC_MD5, HMAC_SHA1.

Table 3 Session Key Calculation

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)

The second, RADIUS server send SPI values AH Security Key, ESP Security Key to HA after AAA authentication phase. Finally, the server sends selected SPI values and key material to mobile node by using last Access-Accept message. And then the server deletes calculated session keys against key disclosure by hacking.

4.2. Behavior of Mobile IPv6 Home Agent

When the authentication of mobile node will success, AAA server sends IPsec SA information to home agent. Home agent establishes IPsec SA with mobile node from received SPI, AH session key ESP session key, and then exchange binding messages with mobile node securely.

4.3. Behavior of Mobile IPv6 Mobile Node

When the authentication of mobile node will success, AAA server sends IPsec SA information to mobile node. Mobile node calculates session key from key material like table 3. And then it establishes IPsec SA with home agent received SPI, calculated session keys, and then exchange binding messages with mobile node securely.

5. CONCLUSIONS

There are many subscriber access networks. It is important that service providers need to authenticate and authorize legal subscribers and account for their usage. RADIUS has used for AAA service widely.
We extended RADIUS to support environment of MIPv6 and propose the key distribution method for IPsec SA establishment between mobile node and home agent. The suggested method was anticipated to be effective at low-power, low computing device. Finally, end users feel the faster authentication, especially when the device reboots or IPsec SA lifetime expires.

References

[1] L. Blunk. and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[2] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1996.

[3] Paul Funk. Simon Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS) ", draft-ietf-pppext-eap-ttls-01.txt, February 2002.

[4] Glen Zorn, Daniel Simon, Ashwin Palekar and Simon Josefsson, "Protected EAP Protocol (PEAP) ", draft-josefsson-pppext-eap-tls-eap-06.txt, March 2003.

[5] "PPP EAP SRP-SHA1 Authentication Protocol", draft-ietf-pppext-eap-srp-01.txt, March 2001.

[6] G. H. Kildong, "The SRP Authentication and Key Exchange System", RFC 2945, September 2000.

[7] T. Dierks and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[8] C. Rigney, A. Rubens, W. Simpson and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[9] Pat R. Calhoun, and Tony Johansson, "Diameter Mobile IPv4 Application", draft-ietf-aaa-diameter-mobileip-19.txt, July 2004.

[10] P. Eronen and T. Hiller, "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-08.txt, June, 2004.

[11] D. Johnson and C. Perkins, " Mobility Support in IPv6", RFC 3775, June 2004.