Mobile IP AAA에서의 등록과 세션키 분배 프로토콜

정회원 황 재 훈*, 송 홍 엽*

Public-Key Based Registration/Session-Key Distribution Protocol in AAA for Mobile IP

Jae Hoon Whang*, Hong-Yeop Song* *Regular Members*

요 약

본 논문은 Mobile IP의 보안적인 측면에 대해 다룬다. 인증 기법과 재생공격 방지 기법을 사용함에도 불구하고 재생공격이 여전히 일어남을 보여주고 이를 해결하기 위해 공개키를 이용한 AAA에서의 새로운 등록방법과 세션키 분배 방법을 제안한다. 제안된 프로토콜은 이동노드의 인증이 완료됨과 동시에 session-key의 분배가 이루어지도록 설계하였다. 또한 공개키 시스템을 최소한으로 사용하여 재생공격의 문제점을 해결하였고 이동노드에서 최소의 계산량을 요구하도록 설계하였다. AAA에서의 정확한 accounting이 가능하도록 부인방지 기능도 추가하였다.

ABSTRACT

Mobile IP aims to support mobility within the Internet. This paper concerned with the security aspect of Mobile IP. We show that current registration protocol has a possible replay attack, despite the use of authenticated registration message and replay protection. We propose a public-key based registration protocol that also distributes a session-key distribution protocol in AAA. Proposed protocol provides authentication of mobile node and session-key distribution simultaneously. It also provides non-repudiation of service request.

I. Introduction

The need for service from foreign network requires AAA service [1]. An FA (Foreign Agent) is likely to request or require the customer to provide credentials which can be authenticated before accessing to resources. Once authentication is done, an MN (Mobile Node) may be authorized to access services within foreign domain. An accounting of actual used resources can be assembled. The registration part is crucial and must be protected from any malicious attack that might try to take illegitimate advantages.

Currently the Mobile IP protocol still relies on the use of secret key with manual distribution for authentication of its control messages. But this approach leads to scalability problem in key management and inappropriate the global network. A recently proposed solution by Jacobs [2] can provide scalable authentication based on public key cryptography. But drawback of this solution is heavy requirements on MN to perform demanding certificate-based public-key cryptography operations.

In this paper, we propose a new registration and session-key distribution protocol in AAA for Mobile IP, intented to get rid of these drawbacks by employing minimal use of public-key cryptography.

* 연세대학교 전기·전자공학과 부호및정보이론 연구실(jh.whang@coding.yonsei.ac.kr)
논문번호 : 010245-0908, 접수일자 : 2001년 9월 8일
※ 본 논문은 2000년도 연세대학교 교내학술연구과제지원에 의하여 수행되었습니다.

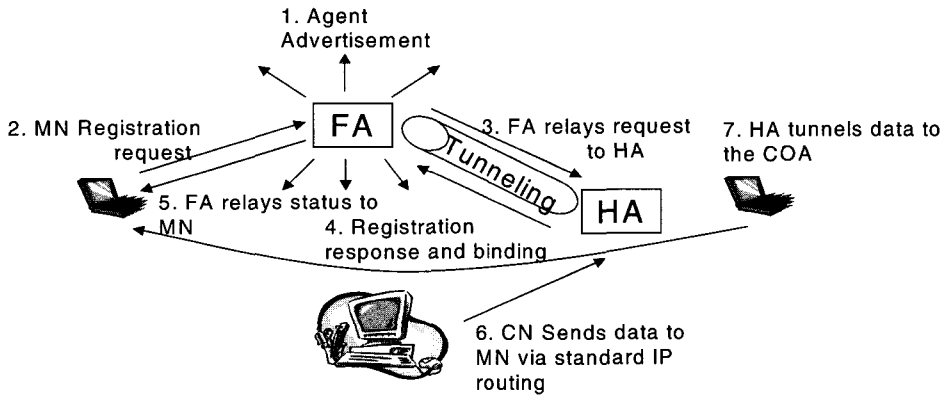

Figure 1. Mobile IP Protocol

Ⅱ. Mobile IP and AAA

2.1. Mobile IP

Mobile IP Protocol is an on-going effort under IETF (Internet Engineering Task Force) towards an Internet Standard that aims to support node mobility within the Internet.

In Mobile IP, a MN is given a long-term address on home domain and it retains this home address regardless of its location. While MN is visiting foreign domain, a Care-of-Address (COA) is also temporarily assigned to it. A network layer agent on home network called Home Agent (HA) should be available to maintain an association between MN's home address and its COA, that is commonly called binding. Under a valid binding of MN that it serves, HA is responsible for intercepting any datagrams destined to MN's home address that reach home domain and then redirect these datagrams to MN's COA. The binding is created and updated through the registration part, in which MN informs HA of its current COA through an FA on foreign domain [3].

2.2. Authentication, Authorization, and Accounting Service (AAA)

A client often needs access to resources provided by an administrative foreign domain than home domain. Service providers in a foreign domain commonly require authorization to ensure a good business relationship with the client. This leads to authentication, and of course accounting ; these three AAA functions are interdependent.

Let's take a closer look at the individual AAA functions to understand the services provided by AAA framework. Authentication is involved validating the end users' identities prior to permitting them network access. This process keys on the notion that the end-user possesses a unique piece of information-a username/password, a secret key, etc.-that serves as unambiguous identification credentials.

Authorization defines what rights and services are allowed to the end user, once network access is granted. Authentication and Authorization are usually perform together in AAA framework.

Accounting provides the methodology for collecting information about end user's resource consumption, which then will be processed for billing, auditing, and capacity planning [4].

For AAA environment, IETF suggested RADIUS (Remote Authentication Dial-In User Service) and DIAMETER protocol. Now, DIAMETER is selected as the standard AAA protocol. DIAMETER is lightweight and peer-based AAA protocol. Designed to offer a scalable foundation for introducing a new policy, AAA services over existing(PPP), and emerging (Roaming, Mobile IP). It employs many same mechanism as RADIUS, such as attribute/value pairs, proxy server support. DIAMETER is much

better than RADIUS in support of reliability, Fail-over and Fail-back, Routing procedures, etc. It also provides public-key infrastructure (PKI) between AAA node [5].

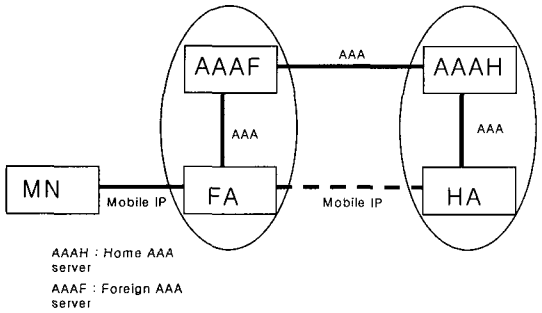

Figure 2. Basic AAA Model

Figure 2. illustrates the basic AAA model. We will assume security association between FA and AAAF, and HA and AAAH. Then propose a protocol, based on this model.

In addition to authentication service, AAA may also serve as a Key Distribution Center (KDC) that generates and distributes session-keys. These session- keys are used to establish a security association between MN and FA, MN and HA, and FA and HA for immediate and future use [1]. We then propose a protocol, that AAA server authenticates a MN and generates a session key.

Ⅲ. Current Registration Protocol and Replay Attack

This section presents current registration protocol of Mobile IP and a possible weakness on it. This protocol doesn't include the AAA server.

3.1. Current Registration Protocol

The following notations are used to represent messages in protocol.

M,N concatenation of two messages, M and N, in the order of specified;
MN_{HM} MN's home address;
MN_{COA} MN's care-of-address;
HA_{id} HA's IP address as its ID;
FA_{id} FA's IP address as its ID;
N_{MN}, N_{HA} nonces issued by MN and HA;
{M}K encryption of message M under key K;
<M>K MAC value of message M under key K;
S_{MN-HA} shared secret key between MN and HA;
Req bit pattern of a request;
Rep bit pattern of a reply;
Result a value of result of the request;

Registration Protocol using nonce

⓪ HA->MN : N_{HA} (previously given)
: HA delivers nonce of HA to MN.
① MN->FA : M_1, $<M_1>S_{MN-HA}$
where M_1 = Req, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{HA}, N_{MN}
: MN relays MAC value of M_1 under key S_{MN-HA}.
② FA->HA : M_1, $<M_1>S_{MN-HA}$
: FA relays the messages to HA.
③ HA->FA : M_2, $<M_2>S_{MN-HA}$
where M_2 = Rep, Result, FA_{id}, HA_{id}, MN_{HM}, N_{HA}, N_{MN}
: HA relays MAC value of M_2 under key S_{MN-HA}.
④ FA->MN : M_2, $<M_2>S_{MN-HA}$
: FA relays the messages to MN.

3.2. A Replay Attack on Current Registration

It is obvious that the security protection using nonce provided in registration protocol is intended to ensure that registration legitimately originated from MN or HA, that it has not been altered in transit , and an old registration is not being replayed. But it is less clear in the security requirement, from the point of view of FA, since FA seems to just play a passive role. And it brings about a possible weakness [3].

We can notice that after a successful registration, FA also starts serving MN and thus allow MN to use resources in its network.

Unfortunately, the assumption above is not safe, and it introduces a potential security loophole that

we use in attack. Figure 3. shows a possible attack by spoofing.

The Attacker first needs to record a valid request message (round 1) and its corresponding reply message (round 3) from some previous run of successful registration. Some time later, the Attacker spoofs MN and replays recorded request message to FA to process and relay the request as specified in round 2, the Attacker spoofs HA and sends the corresponding reply message to FA in round 3. As the round 4 then executed, the attack above will end successfully [3].

The result of this attack is that FA still believes that the registration is a valid and fresh one generated by the legitimate HA and FA. And then the attacker's bogus MN can get a connection through FA and freely enjoy resources on foreign domain.

This attack works because no replay protection involving FA is employed in the protocol. This attack can be avoided, simply by additional replay protection.

Ⅳ. Proposed Public Key Based Registration and Session Key Distribution

4.1. Design Principles

By using public key cryptography except MN's digital signature on service request message, that still uses secret key cryptography, we minimize the computing power requirement as well as adminstration cost imposed on MN. We also use a mechanism for certificate retrieval and validation. These factors also provide a secure session-key distribution and non-repudiation of MN's service request for accounting.

We design the registration protocol to operate in AAA environment.

4.2. Proposed Protocol

The following new notations are related to public-key operations and session-keys.

$\mathbf{K_{AAAH}}$, $\mathbf{K_{AAAF}}$ public key of AAAH and AAAF, respectively;

$\mathbf{K^{-1}_{AAAH}}$, $\mathbf{K^{-1}_{AAAF}}$ private key of AAAH and AAAF, respectively;

$\mathbf{<<M>>K^{-1}_{A}}$ digital signature of message M generated using private key of A;

$\mathbf{Cert_{AAAH}}$, $\mathbf{Cert_{AAAF}}$ certificate of AAAH and AAAF, respectively;

AD a bit pattern indicating an advertisement;

Key-Req, Key-Rep bit patterns of session-key request and reply, respectively;

$\mathbf{S_{MN\text{-}AAAH}}$ shared secret key between MN and AAAH;

$\mathbf{S_{MN\text{-}FA}}$,$\mathbf{S_{MN\text{-}HA}}$,$\mathbf{S_{HA\text{-}FA}}$ session-keys generated by AAAH, shared by MN & FA, MN & HA, and HA & FA, respectively;

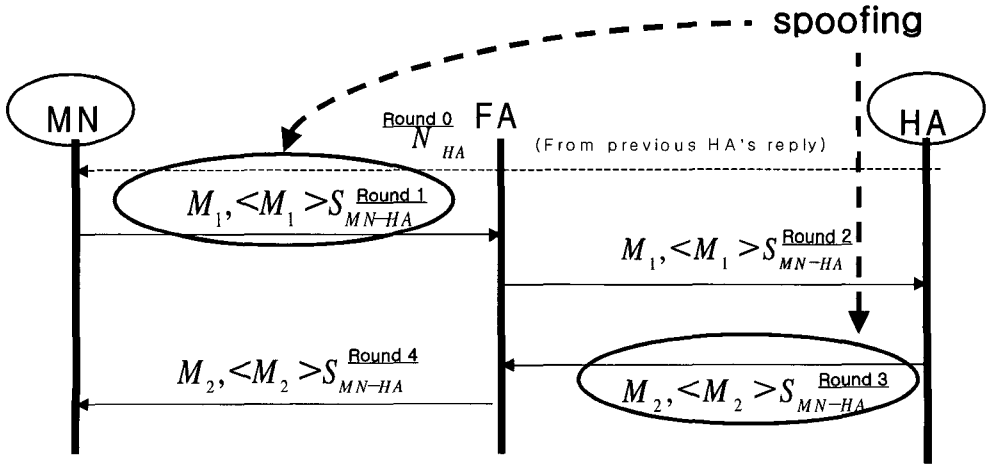

Figure 3. Replay Attack on Current Registration Protocol

MN_{COA} MN's care of address

⓪ AAAH->MN : N_{AAAH} (Previously given)

: AAAH gives a nonce to MN previously

① AAAF->FA->MN : A, $<<A>>K^{-1}_{AAAF}$, $Cert_{AAAF}$

where A = AD, FA_{id}, $AAAF_{info}$

: AAAF generates a digital signature of message A and sends to MN through FA. Message A contains advertisement, ID of FA, and information of AAAF. And we assumed the secure association between AAAF and FA.

② MN->FA : C, $<C>S_{MN-AAAH}$

where C = Req, $<<Req>>K^{-1}_{MN}$, $Cert_{MN}$, N_{MN}, N_{AAAH}, MN_{HM}, HA_{id}, FA_{id}, $AAAF_{info}$, Key-Req, B

B = A, $<<A>>K^{-1}_{AAAF}$, $Cert_{AAAF}$

: MN receives the advertisement message from FA then, sends digital signature of message C and original message C which contains registration and session-key requests, certification of MN, and nonce of AAAH and MN, MNs home address etc.

③ FA->AAAF : D

where D = C, $<C>S_{MN-AAAH}$

: FA relays the message to AAAF.

④ AAAF->AAAH : D, N_{AAAF}

: AAAF generates its nonce and sends with message.

(upon receipt of ④)

AAAH : validate $<C>S_{MN-AAAH}$ using $S_{MN-AAAH}$,

check whether FA_{id} in B = FA_{id} in C,

validate $Cert_{AAAF}$ based on existing PKI at AAAH,

validate $<<A>>K^{-1}_{AAAF}$ using authenticated K_{AAAF}.

⑤ AAAH->HA : Req, MN_{HM}

: AAAH sends MNs request message and home address to HA for registration

⑥ HA->AAAH : Rep, Result

: HA sends reply and result message to AAAH.

⑦ AAAH->HA : S_{MN-HA}, S_{HA-FA}

AAAH->AAAF : F,$<<F>>K^{-1}_{AAAH}$, $Cert_{AAAH}$

where F = E ,$<E>S_{MN-AAAH}$,N_{AAAF}, $\{S_{MN-FA}, S_{HA-FA}\}K_{AAAF}$

E = Rep, Result, N_{MN}, N'_{AAAH}, HA_{id}, FA_{id}, $AAAF_{info}$, S_{MN-FA}, S_{MN-HA}, Key-Rep

: AAAH also performs key distribution center, so it generates session-keys and distributes to HA ,FA, and MN. AAAH sends digital signed message and original message which contains reply, result, new AAAH's nonce, session-key, etc.

(upon receipt of ⑦)

AAAF : validate N_{AAAF},

validate $Cert_{AAAH}$ based on existing PKI at AAAF,

validate $<<F>>K^{-1}_{AAAH}$ using authenticated K_{AAAH}

⑧ AAAF->FA : E, $<E>S_{MN-AAAH}$, S_{MN-FA}, S_{HA-FA}

: AAAF sends message E and session-keys

⑨ FA->MN : E, $<E>S_{MN-AAAH}$

: FA gets its session-key and sends message with MN's new care-of-address.

(upon receipt of ⑨)

MN : validate $<E>S_{MN-AAAH}$ using $S_{MN-AAAH}$

⑩ MN->HA : $<MN_{COA}>S_{MN-HA}$

: MN informs HA of the new care-of-address.

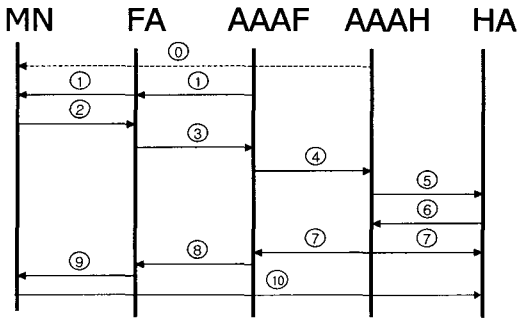

Figure 4. Message Flows in Proposed Protocol

V. Some Remarks on The Proposed Protocol

In this protocol, we assumed SA (security association) between MN and AAAH, FA and AAAF, and HA and AAAH.

Followings are positive aspects of proposed protocol

i) By applying public-key cryptography and certification, AAAH can verify AAAF as legitimate entity and, so can AAAF.

ii) MN still performs all cryptographic operations using secret-key based authentication,

except digital signature on request message. it also free from the requirement to perform CRL(Certificate Revocation List) retrieval and certificate validation.

iii) As MN performs digital signature operation on request message, MN's non-repudiation service is possible.

iv) To avoid the replay attack, early mentioned, AAAF should generate a N_{AAAF} and we can prevent the replay attack.

v) In AAAH, besides authentication, now it also serves as a session-key generation and distribution. So registration and session-key generation are performed at the same time. Once registration and session-key distribution is completed, each entity performs the secure communication by encrypting messages with this session-key.

References

[1] Charlie E. Perkins, "Mobile IP and Security Issue : An Overview," *Internet Technologies and Services, 1999. Proceedings. First IEEE/ Popov Workshop*, pp.131-148, 1999.

[2] Jacobs, S., "Mobile IP Public Key Based Authentication," Internet Draft, <draft-jacobs-mobileip-pki-auth-00.txt>, Aug. 1998. Work in progress

[3] Sufatrio and Kwok Yan Lam, "Mobile IP Registration Protocol: A security Attack and New Secure Minimal Public-Key Based Authentication," *Parallel Architectures, Algorithms, and Networks, 1999. (I-SPAN '99) Proceedings. Fourth International Symposium*, pp.364-369, 1999.

[4] Christopher Metz, "AAA Protocols : Authentication, Authorization, and Accounting for Internet," *IEEE Internet Computing*, Vol.3, No.6 , pp.75-79, Nov.-Dec. 1999.

[5] The official DIAMETER Web Site : http:// www.diameter.org

[6] Charlie E. Perkins, "Mobile IP Joins Forces with AAA," *IEEE Personal Communications*, Vol.7, No.4 , pp.59-61, Aug. 2000.

[7] Charlie E. Perkins, "Mobile Networking Through Mobile IP," *IEEE Internet Computing*, Vol.2, No.1 , pp.58-69, Jan.-Feb. 1998.

[8] Asha Mehrotra and Leonard S. Golding, "Mobility and Security Management in the GSM System and Some Proposed Future Improvements," *Proceedings of The IEEE.* Vol.86, No.7, pp.1480 -1497, July 1998.

[9] J. Solomon, *Mobile IP, The Internet Unplugged*, Prentice-Hall, New Jersey, 1998.

[10] Douglas R. Stinson, *Cryptogaraphy Theory and Practice*, CRC Press, Boca Raton, 1995.

황 재 훈(Jae Hoon Whang) 정회원

2000년 2월 : 연세대학교 기계전자공학부(전기전자전공)학사

2002년 2월 : 연세대학교 전기 · 전자공학과 석사

<주관심 분야> Cryptography, Network Security, Wireless Network

송 홍 엽(Hong-Yeop Song) 정회원

1984년 2월 : 연세대학교 전자공학과 학사

1986년 5월 : USC 전자공학과 석사

1991년 12월 : USC 전자공학과박사

1992년 ~ 1993년 : Post Doc, USC 전자공학과

1994년 ~ 1995년 : Qualcomm Inc., 선임연구원

1995년 9월 ~ 현재 : 연세대학교 전기 · 전자공학과 교수

<주관심 분야> Error Correcting Codes, PN Sequences, CDMA, Spread Spectrum Communication