A Study on Mobile IPv4 Authentication Mechanisms

Jung-Muk Lim*, Hyung-Jin Lim*, and Tai-Myoung Chung*
*School of Information Communication Engineering
Sungkyunkwan University, {izeye, hjlim}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Abstract - With the proliferation of mobile terminals, use of the Internet in mobile environments is becoming more common. To support mobility in these terminals, Mobile IPv4 is proposed and represents the standard in IPv4 environments. Authentication should be mandatory, because mobile terminals can utilize Internet services in any foreign domain. Mobile IPv4 provides symmetric key based authentication using the default HMAC-MD5. However, symmetric key based authentication creates a key distribution problem. To solve this problem, public key based authentication mechanisms have been proposed. In this paper, the performance of each of these mechanisms is evaluated. The results present that, among these mechanisms, partial certificate based authentication has superior performance, and certificate based authentication has the worst performance. Although current public key based authentication mechanisms have lower performance than symmetric key based authentication, this paper presents the possibility that public key based authentication mechanisms may be used for future mobile terminal authentication.

Keywords: Mobile IPv4, Authentication.

1 Introduction

Semiconductor and telecommunications technology has been evolved steadily, the size of computers is continuously being reduced, and communications is progressing from wired environments to the wireless environments. These trends represent the foundation of mobile computers and new forms of communication. Therefore, it is natural for mobile terminals to utilize Internet services continuously, while in motion, and at any location.

The current Internet network protocol standard, IPv4, doesn't support mobility for mobile terminals. Thus, Mobile IPv4 as an IPv4 extension must be implemented to support mobility.

Within a mobile terminal, a user may request Internet services from a foreign do-main instead of a home domain of which the user is registered. Therefore, authentication of terminals is required, unlike wired networks in which a user is only connected to his/her domain. Authentication is classified into terminal authentication, granted by a service agent and service agent authentication granted by a terminal. The former represents the preprocess for authorization and accounting, and the latter represents the process for preventing attackers from masquerading to be a service agent.

This mechanism for mobile terminals to interact with any other domain is required because the terminals can request Internet services in any foreign domain. This is Authentication, Authorization, and Accounting (AAA). a framework to manage authentication, authorization, and accounting comprehensively. Consequently, Mobility of mobile terminals requires an AAA infrastructure.

Mobile IPv4 provides authentication, using HMAC-MD5 by default. However, this method suffers from the key distribution problem in which secret keys must be distributed in advance, due to the requirements of symmetric cryptography. Although a key may be distributed between a Mobile Node (MN) and a corresponding Home agent (HA), it is almost impossible for a key to be distributed between Foreign Agents (FAs) and the MN, or between FAs and the HA. Furthermore, performance is reduced between domains. To solve the key distribution problem, certificated based authentication was proposed [2].

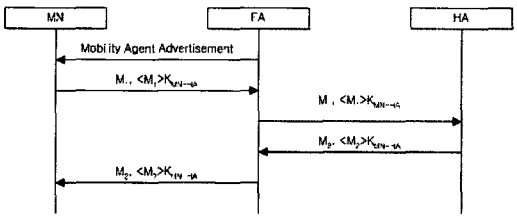
However, public key based mechanisms cannot be applied directly to mobile environments because it is noticeably slower than symmetric key based mechanisms. In addition, it suffers from the problem that mobile terminals don't have enough memory for certificates. To solve this public key based mechanism problem, a partial certificate based authentication mechanism was proposed [3]. The public key is used only between a FA and the HA, as both have high computation power. An identity based authentication mechanism was also proposed [4]. This mechanism does not require a certificate based infrastructure.

2 Mobile IPv4 Authentication

2.1 Default Authentication

The Mobile IPv4 default authentication mechanism requires that a Security Association (SA) between a MN and a HA must be established in advance, in order to use HMAC-MD5 [1].

The registration process using default authentication is presented in [Figure 1].



[Figure 1] Registration Process using Default Authentication

The RRQ consists of M_1 and $<M_1>K_{MN-HA}$. The M_1 is the RRQ's body including the MN's nonce and the HA's previous nonce within the identification field. The $<M_1>K_{MN-HA}$ is the Message Authentication Code (MAC) of the M_1 using HMAC-MD5 and a previously shared 128 bit secret key. The RRQ is forwarded to the HA through the FA. The HA confirms whether its nonce in the RRQ is identical to the nonce previously sent to the MN. If they are not identical, the HA returns an error code in the RRP. If they are identical, the HA verifies the MAC. If the MAC is incorrect, the HA transmits an error code in the RRP to the MN, through the FA. If the MAC is correct, the HA updates its own binding information and transmits a success code in the RRP to the MN, through the FA.

The RRP consists of M_2 and $<M_2>K_{MN-HA}$. The M_2 is the RRP's body including the MN's nonce and the HA's nonce within the identification field. The MN's nonce was in the RRQ and the HA's nonce will be used for the next registration by the MN. The $<M_2>K_{MN-HA}$ is the MAC of the M_2 using HMAC-MD5 and the previously shared 128 bit secret key.

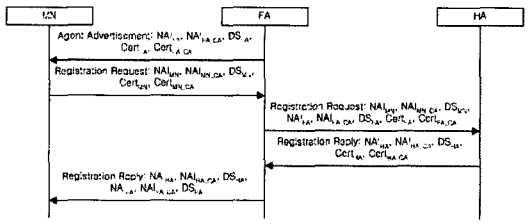
Herein, the authentication between the FA and the HA is omitted but authentication between the FA and the HA must be achieved if accounting is considered.

Default authentication assumes that previously shared secret keys exist between MN and HA, between MN and FA, and between FA and HA. It is a bit cumbersome that a MN and a HA share a secret key between them in advance. Furthermore, it is almost impossible for a MN and a FA or a FA and a HA to share a secret key between them in advance. To solve this problem, another mechanism is required. In one way, the requirement that secret key must be distributed in advance, can be solved by distributing keys dynamically. However, this solution is not suitable because of excessive overhead. Alternatively, this problem can be solved using public key cryptography.

2.2 Certificate based Authentication

To solve the problem of the Mobile IPv4 default authentication mechanism being based on symmetric key, a public key based authentication mechanism was proposed [2]. This mechanism, which has different basis to the Mobile IP default authentication mechanism, solves the key distribution problem by transmitting certificates, which include the public key, in the registration process.

A registration process, using certificate based authentication, is presented in [Figure 2].



[Figure 2] Registration Process using Certificate based Authentication

The FA sends an Agent Advertisement message including its NAI, CA's NAI, signature, certificate, and CA's certificate to the MN. The MN authenticates the Agent Advertisement message by verifying the FA's signature using the FA's certificate and the CA's certificate of the FA.

The MN transmits a RRQ, including its NAI, CA's NAI, signature, certificate, and CA's certificate to the FA. The FA authenticates the MN by verifying the MN's signature using the MN's certificate and the CA's certificate of the MN.

The FA transmits the RRQ including the MN's NAI, MN's CA's NAI, MN's signature, its NAI, CA's NAI, certificate, and CA's certificate to the HA. The HA authenticates the MN by verifying the MN's signature using the MN's certificate and the CA's certificate of the MN, which are shared in advance. It also authenticates the FA by verifying the FA's signature using the FA's certificate and CA's certificate of the FA, in the RRQ received from the FA.

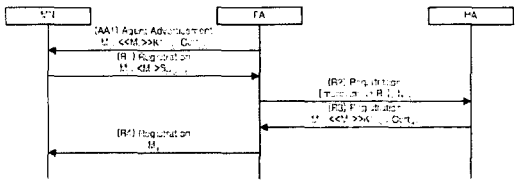
RRP procedure is similar with RRQ procedure. In these flows, mutual authentication between the MN and the FA, between the MN and the HA, and between the FA and the HA are achieved. However, public key based authentication requires much more computation than

symmetric key based authentication. Thus, it is not suitable to use in devices having low computation power such as mobile terminals. Furthermore, it has another problem where a MN must store certificates, despite the limited memory space of the MN.

2.3 Partial Certificate based Authentication

Instead of protecting the whole registration process, a mechanism was proposed where certificate based authentication is used only in places where the MN does not require processing of the public key algorithm and does not require storing the certificate [3].

The registration process using partial certificate based authentication is shown in [Figure 3].



[Figure 3] Registration Process using Partial Certificate based Authentication

The FA transmits an Agent Advertisement including M_1 and signature of the M_1, its certificate to the MN. The M_1 includes its id and the MN's CoA. Without any authentication process to the FA, the MN transmits a RRQ including the FA's id, HA's id, its home address, its CoA, previous HA's nonce, its nonce, M_2, and the MAC of the M_2 using the secret key shared with the HA to the FA. M_2 represents the Agent Advertisement message received from the FA. The FA appends its nonce to the RRQ received from the MN and transmits it to the HA. The HA prevents a malicious person from deploying a replay attack, by confirming its previous nonce. It authenticates the FA by verifying the FA's signature using the FA's certificate, and authenticates the MN by verifying the MN's MAC, using the previously shared secret key. Thus, the FA and the MN are authenticated by the HA.

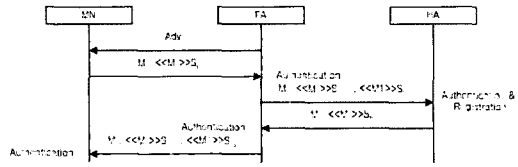
The HA transmits a RRP, which includes M_3, signature of the M_3, and its certificate to the FA. The M_3 includes M_4, MAC of the M_4 using the secret key, which is shared with the MN, and FA's nonce. The M_4 includes the FA's id, its id, the MN's home address, its next nonce, and the MN's nonce. The FA prevents malicious individuals from deploying a replay attack by confirming its nonce in the RRP received from the HA. It authenticates the HA by verifying the HA's signature using the HA's certificate and authenticates the MN by confirming the registration result in the RRP received from the HA. The FA transmits the M_4 to the MN. The MN authenticates the HA by verifying the HA's MAC using the secret key which is shared with the HA, and authenticates the FA by confirming the registration result in the RRP received from the FA. Thus, the MN and the HA are authenticated by the FA and the FA and the HA are authenticated by the MN.

This mechanism requires that a MN and a HA must have a previously shared secret key and a public key infrastructure must exist for the FA and the HA.

2.4 Identity based Authentication

To solve the problem of storing certificates by the MN, and reducing network overhead by transmitting certificates, identity based authentication was proposed [4].

The registration process using identity based authentication is presented in [Figure 4].



[Figure 4] Registration Process using Identity based Authentication

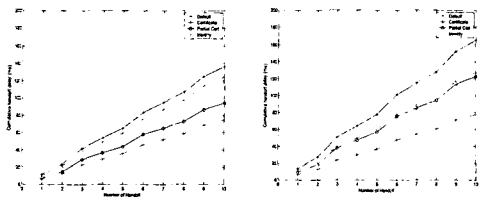
The MN receives an Agent Advertisement message from the FA and then transmits M_1, which is the RRQ's body, and its signature of the M_1 to the FA. The FA authenticates the MN by verifying the MN's signature using the MN's identity, appends its signature to the RRQ, and then transmits it. The HA authenticates the MN by verifying the MN's signature using the MN's identity and authenticates the FA by verifying the FA's signature using the FA's identity.

The HA transmits M_2, which is RRP's body, and its signature of the M_2 to the FA. The FA authenticates the HA by verifying the HA's signature using the HA's identity, appends its signature to the RRP, and then transmits it. The MN authenticates the HA by verifying the HA's signature using the HA's identity and authenticates the FA by verifying the FA's signature using the FA's identity.

3 Performance Evaluation

In this section, we evaluate previously described mechanisms [5].

Relationship between the number of handoffs and cumulative handoff delay is shown in [Figure 5].



[Figure 5] Relationship between the Number of Handoffs and Cumulative Handoff Delay (Left: 100Mbps Wired Environments, Right: 10Mbps Wired Environments)

In 100Mbps wired environments, the relationship between the number of handoffs and cumulative handoff delay is presented in [Figure 5, Left]. The performance rank is ordered as default authentication, partial certificate based authentication, identity based authentication, and certificate based authentication. Partial certificate based authentication reduces authentication processing delay and network delay to transmit certificates using partial symmetric key based authentication. Identity based authentication eliminates network delay when sending certificates by eliminating the requirement for a certificate. The reason partial certificate based authentication is superior over identity based authentication, is that the network delay used to send certificates is mitigated due to the high speed wired environments.

In 10Mbps wired environments, the relationship between the number of handoffs and cumulative handoff delay is presented in [Figure 5, Right]. Similarly, performance rank is ordered as default authentication, partial certificate based authentication, identity based authentication, and certificate based authentication. However, performance difference between partial certificate based authentication and identity based authentication is smaller than that in 100Mbps wired environments, because network delay when sending certificates increases. If the bit rate of a wired environment is much less than 10Mbps, that identity based authentication is expected to provide superior performance over partial certificate based authentication.

4 Conclusions

Symmetric key based authentication, using HMAC-MD5 provided in Mobile IPv4 standard is fast but suffers from the key distribution problem. Key distribution between a MN and a HA is slightly cumbersome, but possible, however, key distribution between a MN and a FA or between a HA and a FA is impossible because a MN can move to any network in any domain. To solve this problem, public key based authentication mechanisms were proposed. The previously proposed pure certificate based authentication is not suitable for a mobile terminal suffering from low network bandwidth and low computation power, because large network overhead is created when sending certificates and a large processing overhead is required when processing the public key algorithm. To solve these problems, partial certificate based authentication and identity based authentication are proposed. However, they still create more overhead over symmetric key based authentication. This paper evaluates these public key based authentication mechanisms, presenting the current direction of public key based authentication mechanisms, providing an indication of future mechanisms.

In the future, advantages from the previously proposed public key based authentication mechanisms will be extracted, and disadvantages will be eliminated, creating a new authentication mechanism.

Acknowledgement

This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment)

References

[1] C. Perkins, "IP Mobility Support for IPv4", RFC 3344, August 2002.

[2] S. Jacobs, S. Belgard, "Mobile IP Public Key Based Authentication", INTERNET DRAFT, draft-jacobs-mobileip-pki-auth-03.txt, July 2001.

[3] Sufatrio, Kwok Yan Lam, "Registration Protocol: A Security Attack and New Secure Minimal Public-Key Based Authentication", ISPAN'99, June 1999.

[4] Byung-Gil Lee, Doo-Ho Choi, Hyun-Gon Kim, Seung-Won Sohn, Kil-Houm Park, "Mobile IP and WLAN with AAA Authentication Protocol using Identity-based Cryptography", ICT 2004, February 2003.

[5] A. Hess, G. Schaefer, "Performance Evaluation of AAA / Mobile IP Authentication", Technical Report TKN-01-012, Telecommunication Networks Group, Technische Universität Berlin, August 2001.