A Secure Protocol for Mobile IP Using Smartcards

Chu-Hsing Lin*, Chien-Liang Tsai*, Chen-Yu Lee**
**Department of Computer Science and Information Engineering*
Tunghai University, Taiwan
E-mail: {chlin, g922907}@thu.edu.tw

***Department of Computer Science and Information Engineering*
National Chiao-Tung University, Taiwan
E-mail: chenyu@csie.nctu.edu.tw

ABSTRACT

In this paper, we discuss the security weakness in the registration method for mobile IP protocols. We point out that there are some probable attacks such as malicious foreign agent attack and the other malicious attacks in existing schemes. We also propose a new secure mobile IP protocol using smart card to solve the problems.

Keywords: *Mobile IP, smart card, home agent, home address, foreign agent, care of address.*

1: INTRODUCTIONS

With the rapid progress of the Internet and wireless technologies, more and more commercial applications are developed on mobile devices. The research issues on wired environment such as security, authentication and integrity are shifted to mobile communication and become increasingly important. TCP/IP protocol shall be modified to support mobility for mobile devices roaming from one network to another. In general, IP address has two parts, one is the prefix bits (defining the address of network), and the other is the rear bits (defining ID of the host computer). The prefix bits is related to the network to make access control of routing paths. The solution for Mobile IP [3] is available with two addresses, home address and care of address. The Home address is a long-lasting address and the care of address changes with the foreign network when mobile node is moved to another network. As illustrated in Figure 1, when the mobile node moves to a foreign network, it can obtain a care of address through the registration procedure. A mobile node communicates with a correspondent in the following three phases:

Phase 1: Agent Discovery

The mobile node leaves from the home network to a foreign network and find out a foreign agent. Then it changes the address to the care of address and foreign address.

Phase 2: Registration

When the mobile node sends the request of registration to a foreign agent for registering a care of address, the foreign agent shall register it and then transfer the message to home agent.

Phase 3: Data Transfer

After the completion of registration, the mobile node starts to communicate with the correspondent.

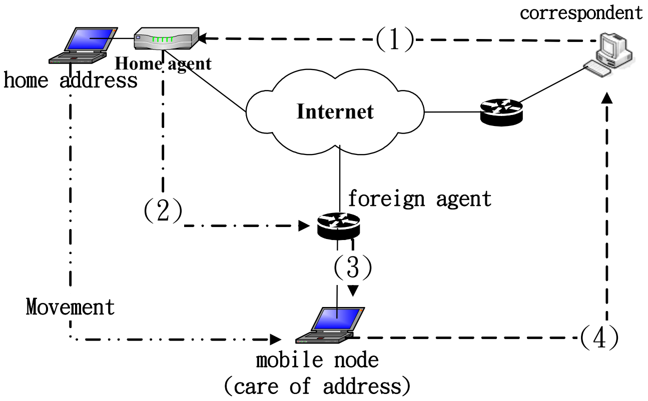

Figure 1. Mobile node communicates with the correspondent

Figure 1 shows the communication between the mobile node and the correspondent, described briefly as follows.

Step 1: The correspondent sends the packets to the home agent.

Step 2: The home agent transfers the packets to the foreign agent.

Step 3: The foreign agent transfers packets to the mobile node.

Step 4: The mobile node feeds back messages to the correspondent.

2: RELATED WORKS

Mobile IP is vulnerable to some attacks such as eavesdropping during the registration and data transfer. Thus, IPSec [5] is recommended to protect the mobile IP communication. In 2004, Mufti and Khanum [1] developed a method to preventing the mobile communication from "Denial of Service Attack" by using the public key technique. In 2005, Lee et al. [2] advised to use authentication method to ensure the security of mobile communication.

We briefly introduce the method proposed by Mufti and Khanum and point out the weakness of their method. Some notations are defined:

M	mobile node
F	foreign agent
H	home agent of M
K_{MF}	key shared by M and F
IM	IP address of mobile node
IH	IP address of home agent
IF	IP address of foreign agent
n_i	random number
MSG_{AB}	message from A to B
$<..>$	content of message
LT	lifetime
( )X	encrypted message with X as a key
P_A	public key of A
V_A	private key of A
SK_{AB}	session key of A and B

Registration Phase in the Mufti and Khanum's:

Step 1: M → F:

$\mathrm{MSG}_{MF} =< \mathrm{IM,IH,LT},n_1,(K_{MH},n_1,\mathrm{IM})K_{MH} >$

Step 2: F → H:

$\mathrm{MSG}_{FH} =< (\mathrm{MSG}_{MF},\mathrm{IF},n_2,(\mathrm{IF},n_2)V_F)P_H >$

Step 3: H → F:

$\mathrm{MSG}_{HF} =< ((SK_{MF},n_2,\mathrm{MSG}_{HM})V_H)P_F >$

$\mathrm{MSG}_{HM} =< (K_{MH},n_1,SK_{MF})K_{MH} >$

Step 4: F → M:

$\mathrm{MSG}_{FM} =< (\mathrm{MSG}_{HM})V_F >$

After completion of registration, SK_{MF} is taken as the encryption key for data transfer. In their paper, public key is used to protect information exchanged between the mobile node and the foreign agent. However, we found out some weakness in their registration phase, as described below:

1) Key management problem: the authentication of M (mobile node) and H (home agent of M) relies upon the security of K_{MF}.
2) Malicious attacks are probable to succeed:
   A. M (mobile node) sends the following message to F (foreign agent):

      $\mathrm{MSG}_{MF} =< \mathrm{IM,IH,LT},n_1,(K_{MH},n_1,\mathrm{IM})K_{MH} >$
   B. A malicious foreign agent could modify and the horten the LT in MSG_{MF}, and then transfer it to the real foreign agent for registration. The mobile node would fail on functions due to the problem of lifetime even if it registers successfully.
   C. A malicious attacker could intercept the message of M (mobile node) sent to F (foreign agent). However, F (foreign agent) can not identify whether IH or LT is modified or not under the message their authentication scheme. So, the Denial of Service attack could succeed.

In 2005, Lee et al. [2] suggested that an authentication method with one-way hash function and smart card is used. Some notations are used.

U_i	user
ID_i	identification of user
PW_i	password of user
x	private key of server x
$h(\cdot)$	one-way hash function SHA-512[4].
T	timestamp

The scheme needs the smart card registration phase for user Ui:

Step 1: User U_i inputs its ID_i and PW_i to the server for issuing a smart card.

Step 2: Server computes $A_i=h(ID_i||x)$ and $B_i=h(A_i||PW_i)$.

Step 3: Server issues a smart card containing $\{ID_i, A_i, B_i, h(\cdot)\}$ for user U_i under a secure channel.

Lee's login phase is described as belows:

Step 1: (User side)

1) User inserts the smart card into card reader and inputs his/her ID_i and PW^*_i.
2) Smart card computes $B^*_i=h(A_i||h(PW^*_i))$, $C_2=_{.} B^*_i \oplus A_i$, and $C_1=h(T\oplus B_i)$.
3) User sends message $\{ID_i, C_1, C_2, T\}$ to the server.

Step 2: (Server side)

1) Server verifies if the timestamp T is within the lifetime.
2) Server computes $A_i=h(ID_i||x)$ and obtains $B^*_i=C_2\oplus A_i$ and $C_1=h(T\oplus B_i)$.

Server verifies if $C_i^* \overset{?}{=} C_i$. If equal, the authentication is successful; otherwise, it is rejected.

3: PROPOSED METHOD

To make the registration procedure of Mobile IP more secure, we apply Lee's scheme with HMAC. Below, we proposed our scheme.

Smart card registration phase:

Step 1: User U_i inputs his/her ID_i and PW_i to the home agent for requesting a smart card.

Step 2: The home agent issues a smart card by:

1) Compute $A_i=h(ID_i \| h(V_H))$, where V_H is the private key of the home agent.
2) Compute $B_i=h(A_i \| h(PW_i))$.
3) Compute $D_i=(ID_i \oplus n_{ID})V_H$, where n_{ID} is a random number.

The smart card for user U_i contains message of $\{ID_i, A_i, B_i, h(\cdot), D_i\}$.

Mobile node registration phase:

Step 1: Mobile node (M) → foreign agent (F):

1) User inserts the smart card into card reader and inputs the corresponding ID_i and PW_i^*.
2) Smart card computes $B_i^*=h(A_i \| h(PW_i^*))$, $C_2=B_i^* \oplus A_i$, $C_1=h(T \oplus B_i)$, and $SK_{MH}=h(B_i \| n_1)$.
3) Let MSG_{reg}=<IM, IH, n_1, ID_i, C_1, C_2, T>, and computes $MD_{MF}=h(MSG_{reg})$ and $MSG_{HMAC} = HMAC_{SK_{MH}}(MSG_{reg})$.
4) Let MSG_{MH} = < IM, IH, n_1, ID_i, C_1, C_2, T,MSG_{HMAC} >, MS_{GMF}=<MSG_{MH}, $(MD_{MF}, D_i, n_{ID})P_F$>.
5) Send the message MSG_{MF} to F.

Step 2: F → H:

After receiving the request for registration, the foreign agent verifies the integrity of the message and then transfers the message to the home agent.

1) Foreign agent verifies if timestamp T is within the lifetime.
2) Retrieves MD_{MF}, D_i, n_{ID} using its private key V_F.
3) Computes $ID_i^*=(D_i \oplus n_{ID})P_H$, where P_H is the public key of the home agent and verifies if $ID_i^* \overset{?}{=} ID_i$. If not equal, the registration is rejected, indicating that the mobile node has not been accepted by the home agent.
4) Computes $MD_{FH}=h(MSG_{MH}, IF, n_2)$, MSG_{FH} = <(MSG_{MH}, IF, n_2, $(MD_{FH})V_F)P_H$>.
5) Foreign agent sends the message MSG_{FH} to the home agent (H).

Step 3: H→ F:

Home agent verifies the message of M (mobile node) after receiving the request for registration, and then sends back a registration replay to the foreign agent.

1) Home agent verifies if timestamp T is within the lifetime.
2) After receiving the message, H decrypts the message using V_H.
3) After decrypting MD_{FH} using P_F, H verifies the integrity of MSG_{FH}.
4) Home agent computes $A_i=h(ID_i \| h(V_H))$ based on the data of user U_i, and obtain $B_i^*=C_2 \oplus A_i$.
5) Verifies MSG_{HMAC} using SK_{MH} and MSG_{reg}.
6) Computes $C_1^*=h(T \oplus B_i^*)$ and verifies $C_i^* \overset{?}{=} C_i$. If equal, the authentication is successful.
7) Let MSG_{HM}= <n_1, ID_i, C_1^{**}, C_2, T^*> and MSG_{HF}= <((n_2, $MSG_{HM})V_H)P_F$>, where $C_1^{**}=h(T^* \oplus B_i)$, T^* is a new timestamp.
8) Home agent sends the message MSG_{HF} to the foreign agent.

Step 4: Foreign agent → mobile node:

Foreign agent transfers back the message to M (mobile node).

1) After receiving the message, foreign agent decrypts MSG_{HF} using V_F and P_H to retrieve MSG_{HM} and n_2.
2) Computes MSG_{FM} = <$(MSG_{HM})V_F$> and sends it to mobile node.
3) Mobile node retrieves MSG_{FM} using P_F.
4) M verifies if timestamp T^* is within the lifetime.
5) Computes $C_1^{***}=h(T^* \oplus B_i)$ and verifies $C_i^{***} \overset{?}{=} C_i^{**}$. If equal, the registration is successful.

4: ALANYSIS

In this section, we analyze that the proposed method can solve the problems in the Mufti and Khanum's [1].

1) Against the attacks from a malicious mobile node: when M (mobile node) sends a message to F (foreign agent), F firstly uses the public key P_H and D_i of the home agent to verify whether M (mobile node) is a right node. Further, it resists against the replay attack using random number n_1 when a malicious mobile node uses the former registration messages.

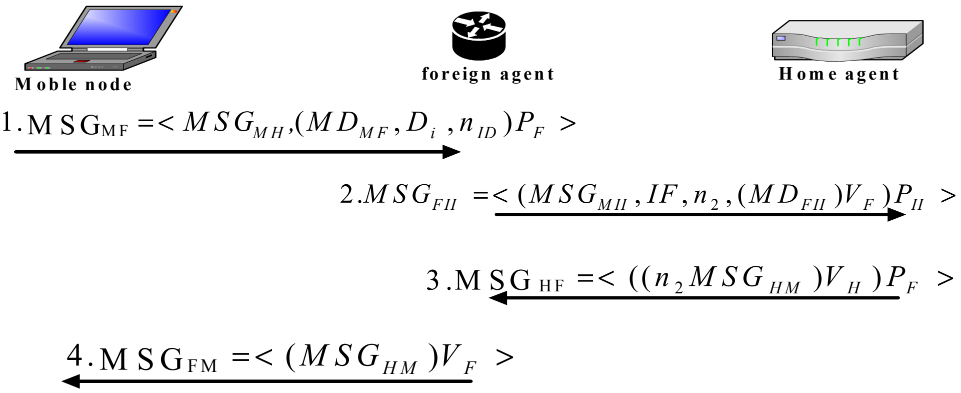
Moble node
foreign agent
Home agent
1. $MSG_{MF} =< MSG_{MH},(MD_{MF}, D_i, n_{ID})P_F >$
2. $MSG_{FH} =< (MSG_{MH}, IF, n_2, (MD_{FH})V_F)P_H >$
3. $MSG_{HF} =< ((n_2 MSG_{HM})V_H)P_F >$
4. $MSG_{FM} =< (MSG_{HM})V_F >$

Figure 2. Mobile node Registration

2) Against the attack from a malicious foreign agent: in our scheme the registration message contains the authentication information of H (home agent) and F (foreign agent) using HMAC, a malicious foreign agent can not modify the messages to forge the home agent H. Further, since M verifies the registration response from H, so the malicious agent can not modify it, too.

5: CONCLUSIONS

With the rapid progress of the Internet and wireless technologies, there are more and more applications developed on the mobile IP environments. However, there also bring many security problems on the mobile IP. In the paper, we propose a new registration scheme for mobile IP. Based on the security property of smart card, our scheme improves the security to resist some attacks such as Denial of Service attack and malicious foreign agent attacks and offers users a convenience to use the ID and password.

Acknowledgement

This research is partially supported by the National Science Council of Taiwan, by contract NSC 95-2221-E-029-020-MY3.

REFERENCES

[1]. Muid Mufti ,Aasia Khanum., “Design and Implementation of a Secure Mobile IP Protocol,” *Proceedings of the International Networking and Communication Conference on Network Security (INCP 2004)*, June 2-13 ,2004, pp. 53-57.

[2]. Chia-Yin Lee ,Chu-Hsing Lin , and Chin-Chen Chang , "An Improved Low Computation Cost User Authentication Scheme for Mobile Communication , " *Proceedings of International Conference on Advanced Information Networking and Applications (AINA 2005)* , Vol. 2, March 25-30, 2005 , pp. 249 – 252.

[3]. Charles E. Perkins, “IP Mobility Support”, *RFC 2002*, Oct 1996.

[4]. NIST, U.S. Department of Commerce, “Secure hash standard,” August 2002, U.S. *Federal Information Processing Standard (FIPS) 180-2*.

[5]. J. Zao, M. Condell, “Use of IPSec in Mobile IP,” *Internet Draft*, draft-ietf-mobileip-ipsec-use-OO. txt, 1997.

[6]. C. C. Chang, C. T. Wang, and Chu-Hsing Lin, “Conference Key Distributions Using Self-Certified Public Keys,” *International Journal of Applied Mathematics*, Volume 2, No. 3, 2000, pp.327-337.

[7]. T. M. Hsieh, Y. S. Yeh, Chu-Hsing Lin, and S. H. Tuan, “One-Way Hash Functions with Changeable Parameters,” *Information Sciences*, Vol. 118, September 1999, pp.223-239.

[8]. Chu-Hsing Lin, C. C. Chang and R. C. T. Lee, "A New Public-Key Cipher System Based on the Diophantine Equations," *IEEE Transactions on Computers*, Vol.44, No.1, January 1995, pp.13-19.

[9]. Chu-Hsing Lin, Wei Lee, and Chien-Sheng Chen, " Dynamic Key Generations for Secret Sharing in Access Structures , " *Proceedings of International Conference on Advanced Information Networking and Applications (AINA 2005)*, Vol. 2, March 25-30, 2005 , pp. 127-130.

[10]. James D. Solomon, “Mobile IP The Internet Unplugged”, Prentice Hall International, Inc.

[11]. Behrouz A. Forouzan, Sophia Chung Fegan,” TCP/IP Protocol Suite”, Second Edition, Mcgraw-Hill Company, Inc.