Access Control of Visiting Mobile Node on the Foreign Domain Network in Mobile IPv6

Sugil Choi[1], Masayuki Abe[2] and Kwangjo Kim[1]

[1] International Research center for Information Security (IRIS)

ICU, Korea

[2] NTT Information Sharing Platform Laboratories, Japan

Abstract

The need for network protection, accounting and resource management in foreign administrative domain requires appropriate security services. In this paper, we propose an access control protocol to support the authentication between mobile node and visiting subnet. Our hybrid way of approach aims to reduce computational overhead and minimize the use of network bandwidth. We also propose non-certificate based public-key cryptography to provide non-repudiation, which does not require CRL retrieval and certificate validation.

I.Introduction

Using Mobile IP, mobile nodes need to visit foreign domain network and use resources in the network. For the purposes of network protection, accounting and resource management, the identity of a mobile node must be verified before being allowed to complete its access and establish an attachment point on the visiting subnets. Some proposals on the authentication between mobile node and visiting network in MIPv4 include the role of foreign agent, but foreign agent is not required anymore in MIPv6. Here, we realized that a protocol for access control of visiting mobile nodes in foreign administrative domain is required and the protocol should be compatible with MIPv6.

The organization of this paper is as follows: In Section 2, we need to define an entity to function like access control agent in foreign subnets. In MIPv4, foreign agent might be the candidate for doing this role, but it does not exist any more in MIPv6. In this paper, only the scenario that DHCP Server serves as access control agent will be described, as stateful address autoconfiguration provides better characteristics for control. In Section 3, after defining the concerned entities, we need to make the exchange of messages secure. In Section 4, we conclude by mentioning a few directions about the following research.

II.Mobile IP Protocol

Internet Protocol routes packets to their destination according to IP addresses which are associated with a fixed network. So, when the packet's destination is a mobile node, this means that each new point of access made by the node is associated with a new network number, hence, new IP address must be set to maintain connections as mobile node moves from place to

place. This makes transparent mobility impossible.

In mobile IP, mobile nodes use two IP addresses: home address and care-of address. The home address is static and used to identify TCP connections. The care-of address changes at each new point of attachment. Mobile IP requires the existence of a network node known as the home agent and foreign agent. Whenever the mobile node moves, it registers its new care-of address with its home agent and the home agent redirects all the packets destined for the mobile node to the mobile node's care-of address. In MIPv4, home agent and foreign agent broadcast agent advertisement at regular intervals and mobile node gets network configuration information from the advertisement. But, in MIPv6, foreign agent does not exist anymore. In MIPv6, a care-of address can be derived from the receipt of router advertisement (stateless address autoconfiguration), or be assigned by DHCP server (stateful address autoconfiguration).

III.Proposed Access Control Protocol

1. Design Principles

Some design principles and assumptions in our new protocol are:

· he main goal in designing this protocol is to support secure and efficient roaming between different subnets. While achieving fast roaming, we also try to provide mutual message and origin authentication, integrity, replay attack protection, and non-repudiation. While the protocol offers the benefit of scalability and non-repudiation from its use of public key cryptography, its public key operations are kept to minimal. Thus our protocol exercises a hybrid approach.

· or the practical use, we do not use WPKI in our protocol Instead, non-certificate based public-key cryptography is applied, so mobile nodes can be free from the requirements to perform CRL retrieval and certificate validation. Also, it consumes less computing resources and less network bandwidth compared to certificate-based public-key cryptography authentication.

· his protocol is only compatible with IPv6 as new feature of IPv6 is employed. DHCP server functions as access control agent, as foreign agent does not exist in MIPv6.

· his protocol employs the role of AAA server to check the current status of mobile node, besides verifying the identity of it.

· ll network entities except mobile node are assumed to reside on wired network and have strong computational power.

2.The Protocol

In our paper, we use the following notations in the network shown in figure 1.

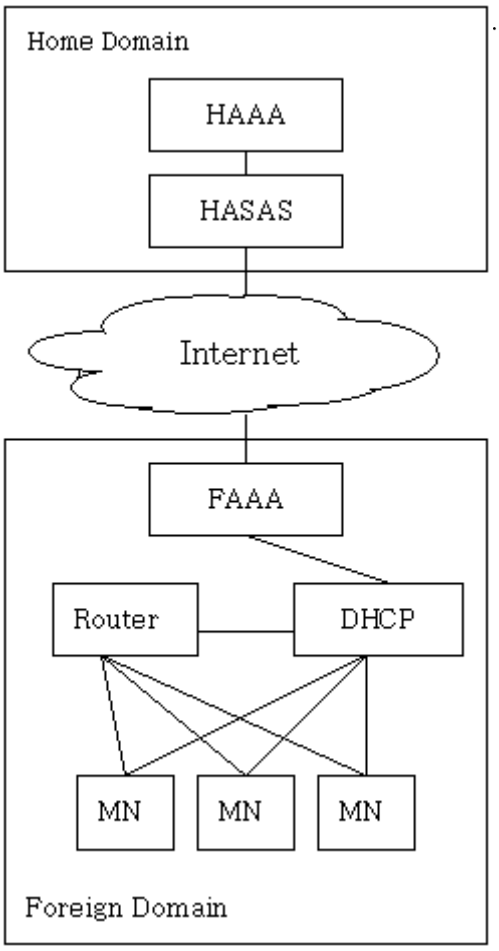
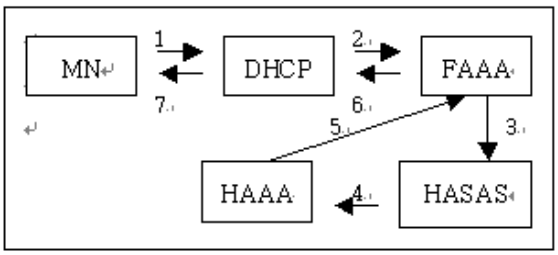


Figure 1.Network Architecture
Figure 2 Message Flow



AAA Authentication, Authorization, Accounting

Ha Home AAA server

Fa Foreign AAA server

HASAS Home AAA Server Allocation Server

S_{MN-Ha} shared secret between mobile node and HAAA

NAI Network Access Identifier, each MN is identified with NAI. (e.g. : fred@3com.com)

La link local address, formed by appending token to the architecturally defined Link-Local prefix. In this protocol, sub-network prefix + 64 bit (combination of leading 62 bit of hashed value of public key and "u" and "g" bits).

N_{MN-Ha} Nonce between MN and HAAA

R_{Ha-MN} Reply from HAAA to MN

PK_{DHCP} Public key of DHCP server

K^{-1}_{DHCP} Private key of DHCP server

NCI Network configuration information

$DHCP_{id}$ Address of DHCP server

Here, we present message exchanges only between MN and DHCP.:

1) MN → DHCP

· ompute S_{MN-Ha}

· I1 : NAI, MN La, N_{MN-Ha}, $N_{MN-DHCP}$, $DHCP_{id}$, { H(NAI, MN La, N_{MN-Ha}, $N_{MN-DHCP}$, $DHCP_{id}$) }S_{MN-Ha}

2) DHCP → MN

· etrieve MN authentication information from $R_{Fa-DHCP}$ and record the authentication result

· I2 : M3, NCI, MN La, $DHCP_{id}$, PK_{DHCP}, $N_{DHCP-MN}$, {H(M3, NCI, MN La, $DHCP_{id}$, $N_{DHCP-MN}$)}K^{-1}_{DHCP}

where M3 = R_{Ha-MN}, N_{Ha-MN}, { H(R_{Ha-MN}, N_{Ha-MN}) }S_{MN-Ha}

3. Security Analysis of the Protocol

In our protocol, AAA servers have pre-defined security associations with other entities in the same administrative domain network. MN has shared secret with HAAA and this shared secret is used to generate onetime secret key. Secret key is the hashed value of shared secret and $Nonce_{MN-HAAA}$. The use of one time secret key makes it more difficult to compromise shared secret.

The authentication of MN is delegated to HAAA and the authentication of foreign domain network, especially DHCP server, is delegated to FAAA. Otherwise, authentication requires WPKI which is not fully deployed globally, because it is infeasible to keep security association with every entity in other administrative domain. The delegated authentication model also provides quite reasonable security, as each AAA servers are authenticated using certificate-based public key cryptography.

But, the path through which authentication reply goes, from DHCP server to MN, has some security weakness. The reply message from HAAA to MN is protected by the use of shared secret, but network configuration information from DHCP server to MN can be modified because no authentication mechanism is employed here. As DHCP server and MN do not share security association and WPKI is not deployed, we need another way to secure the message. Non-certificate based public-key cryptography can be the solution to this problem. Non-certificate based cryptography proceeds as follows:

· HCP server forms its address by appending the hashed value of its public-key to the architecturally defined Link-Local prefix and broadcasts it through DHCP advertisement.

· IN receives the advertisement and sends network configuration information request with MN authentication token.

· HCP server asks the authentication of MN

to FAAA.

· nce DHCP server receives a successful reply from FAAA server, it sends network configuration information, R_{Ha-MN} and the public key of DHCP server to MN.

· /hen MN receives a reply from DHCP server, MN authenticates the R_{Ha-MN} with shared secret between HAAA and MN. Then, MN trust DHCP server with the $DHCP_{id}$ in R_{Ha-MN} and compares the leading 62 bit of hashed value of public key with the last 64 bit of authenticated $DHCP_{id}$ (excluding "u" and "g" bits). If those are equal, MN can be sure that the claimed public key is bound to the authenticated DHCPid, which is the same as the function of certificate that binds public key to certain entity.

· IN validate digital signature with public key and, the authentication procedure completes.

AAA server can serve as KDC, but in this case, AAA server need to perform additional operation to generate random key and has the responsibility of managing the keys securely. Non-certificate based public key authentication explained above does not impose extra overhead on AAA server and is freed from key distribution problem. In addition to those benefit, it provides non-repudiation.

4. Other Considerations

The use of nonce or time stamp in every message provides replay attack protection. Public keys of DHCP server and mobile node are not included in the authentication token sent to AAA servers and, instead, public key is sent to corresponding node directly. In this case, DHCP server and mobile node have to validate the public key, but this requires just one hash operation while reducing the size of message along the way to AAA server. The hashed value of public key can be a part of IPv6 address or sent separately. We chose to form address by appending the hashed value of public-key to the architecturally defined Link-Local prefix, because this does not require any change in DHCP server binding information table. Otherwise, one column for hashed value of public key must be added.

IV.Conclusion and Future Work

We proposed access control protocol designed to support secure and fast roaming between different subnets in MIPv6. Security measures in proposed protocol aims at providing message and origin authentication, integrity, replay protection and non-repudiation. In our protocol, we take into account limited computational power of mobile node and low network bandwidth. Non-certificate based public-key cryptography was proposed to provide non-repudiation, which do not require CRL retrieval and certificate validation. We would stress that this non-certificate based public-key cryptography made mutual authentication between DHCP server and MN possible without any help of KDC and Certificate.

As a further research, we will measure the efficiency of this protocol, examine how these protocol messages can fit into control message packet formats, and design undisputed packet based billing system, etc.

References

[1] Charles E. Perkins, Mobile Networking through Mobile IP, http://www.computer.org /internet/v2n1/perkins.htm

[2] Vipul Gupta and Gabriel Montenegro, Secure and mobile networking, Mobile Networks and Applications 3 (381-390), 1998

[3] Sufatrio, Kwok Yan Lam, National University of Singapore, Mobile IP Registration Protocol: A Security Attack and New Secure Minimal Public-Key Based Authentication,

[4] Charles E. Perkins and Pat R. Calhoun, AAA Registration Keys for Mobile IP, draft-ietf-mobileip-aaa-key-09.txt, February 2002.

[5] Greg O'Shea and Michael Roe, Child-proof Authentication for MIPv6(CAM), 2000

[6] David B. Johnson, Charles E. Perkins and Jari Arkko, Mobility Support in IPv6, draft-ietf-mobileip-ipv6-18.txt, June 2002.