

Tampere University of Technology
8306500 Security protocols
Security in Mobile IPv6
18.4.2002
Timo Koskiahde

Security in Mobile IPv6

Table of Contents:

1. Introduction	1
2. Mobile IPv6 Basic Operation	1
3. Mobile IPv6 Security Objectives and Threats	3
4. Proposed Authentication Methods	5
4.1 IPSec	5
4.2 Return Routability	6
4.3 Cryptographically Generated Addresses	9
4.4 Method Comparison	11
5. Conclusions	13
References	14

1. Introduction

Internet has traditionally been a network of quite static nodes. Today, the situation is changing: new types of mobile devices, like mobile phones, are connected to the Internet. Concurrently of course, the total number of devices connected to the Internet is increasing rapidly, which makes the address shortage problems of the IPv4 even worse. That is why the new version of the Internet Protocol, called IPv6, has been developed.

Mobile IPv6, which is a mandatory feature of the IPv6, has been developed to enable mobility in IP networks for mobile terminals. Mobile IPv6 specification is still unfinished, so the protocol will most probably undergo some changes and the functionality described in this document will develop further. Data security is a fundamental part of the Mobile IPv6; it will be discussed in detail in this document, without going into other specifics of the protocol.

IPSec is also a mandatory feature of the IPv6. It provides data security services for the transportation and application layer protocols of the TCP/IP stack. It is possible to use it to provide security also for the Mobile IPv6, but there are some problems and unsolved issues that prevent that in most of the cases and that is why some new methods have been developed to secure Mobile IPv6.

2. Mobile IPv6 Basic Operation

Mobile IPv6 is needed to enable mobility in IP networks. The problem with mobility in IP networks is that the both ends of a TCP connection need to keep the same IP address for the life of the connection and on the other hand the IP address need to be changed when a network node moves to a new place in the network. Mobile IPv6 changes this problem into a routing problem by using different addresses for routing and for connection identification. Mobile IPv6 provides also reachability with one IP address for a moving node despite its location in the network.

Mobile IPv6 introduces three new types of network entities [Figure 1]: Mobile Node (MN), Home Agent (HA) and Correspondent Node (CN). MNs are capable of moving in the network and they use HAs for maintaining their reachability. All other Mobile IPv6 aware nodes are considered as CNs. Mobile IPv6 introduces also two new type of addresses for the MN: Home Address (HoA) and Care-of-Address (CoA). HoA is used for connection identification and CoA is used for routing, i.e.

HoA remains the same during movements and CoA changes every time when the MN's point of attachment in the network changes. HoA is allocated from the MN's home network, where also the MN's HA resides. CoA is configured separately for the MN in every foreign network, i.e. network different than home network. Mobile IPv6 binding messages are used for binding a MN's HoA and CoA, i.e. the MN's identity and location together.

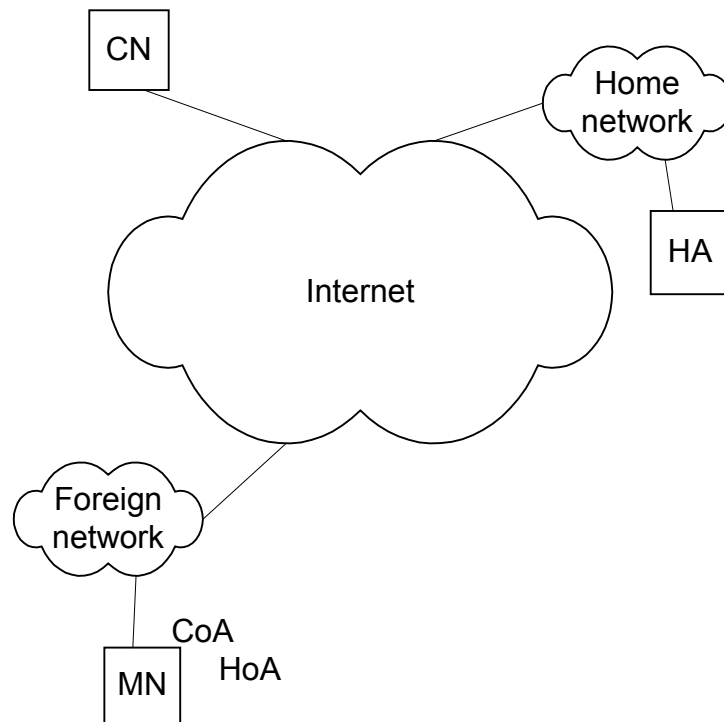


Figure 1. Mobile IPv6 Network Picture

There exist three binding messages that are used for actual binding management: Binding Update (BU), Binding Acknowledgement (BA) and Binding Request (BR). BU is used by MN to reveal its current CoA to HA and CN, BA is used by HA and CN to acknowledge BU and BR is used by HA and CN to request MN to refresh its current binding.

When a MN moves to a foreign network it reveals its location to its HA, i.e. creates a binding with its current CoA and HoA. If a CN sends a packet to the MN (to HoA), the packet is routed to the MN's home network, where the HA intercepts the packet and tunnels it to the MN. After receiving the tunneled packet, the MN reveals its current location also to the CN. After the CN has established the binding between the HoA and the CoA, the CN sends packets destined to the MN directly to the MN's CoA and vice versa. IPv6 routing header is used by the CN to send the

packet directly to the MN; the destination address is set to CoA and the HoA is located into routing header. When a MN receives the packet, it replaces the destination address with the HoA before passing the packet to the upper layer protocol. When sending a packet directly to the CN, the MN uses a home address destination option to indicate the real sender of the packet, i.e. the HoA, to the CN and uses CoA as source address of the packet. After receiving the packet, the CN replaces the source address with the HoA before passing the packet to the upper protocol layer. Thus the Mobile IPv6 operation and CoA are invisible from the perspective of the upper protocol layers and HoA is used for all communication.

Mobile IPv6 is independent of access technology. That means that it can be used with any link layer technology, e.g. WLAN, Ethernet, GPRS and Bluetooth. That is why any link layer issues, e.g. how a node connects to a specific network or security issues in the link layer, are not discussed in this document.

3. Mobile IPv6 Security Objectives and Threats

Mobile IPv6 can be considered as a mobility extension for the basic IPv6 functionality. From the data security perspective, the basic objective during the development of Mobile IPv6 has been that it must be at least as secure as basic IPv6 or IPv4 from the MN perspective and it should not introduce any new security threats to IPv6 from the network and other nodes' perspective. Mobile IPv6 security threats can be divided into several categories [1]:

1. Threats against binding messages to home agent.
2. Threats against route optimization with correspondent nodes.
3. Threats where Mobile IPv6 correspondent node functionality can be used to launch reflection attacks against other parties.
4. Threats where the tunnels between the mobile node and the home agent are attacked to make it appear like the mobile node is sending traffic while it is not.
5. Threats where IPv6 Routing Header, which is employed in Mobile IPv6, is used to circumvent IP-address based rules in firewalls or to reflect traffic from other nodes.

6. The security mechanisms may also be attacked, e.g. by forcing the execution of expensive cryptographic algorithms unnecessarily.

Most of the above threats are concerned as denial of service. Some of the threats also open up possibilities for man-in-the-middle, connection hijacking, and impersonation attacks. All the threats are caused by the modified routing used to enable mobility in the network, so the security objective is to make the routing changes securely.

Threats 1 and 2 both concern binding message authentication, but they are different from the security perspective, because the authentication is needed between different entities. The first case concerns trust and authentication between a MN and a HA. The MN uses services of the HA, so they must have some relationship and trust in advance, because the MN must have somehow agreed to use the service. That is why they can exchange some secret beforehand, which can be then used in authentication of the binding messages. It is also possible to exploit some private authentication infrastructure easily in this case.

In the second case, a CN can be any node in the network, so the MN and the CN will most probably have no relationship in advance. Several methods can be used to authenticate the binding messages between the MN and the CN. One alternative is to use some public key authentication method, but the problem is that the needed global public key infrastructure does not exist at the moment. Another alternative to ensure binding messages validity is to utilize the Mobile IPv6 specific network architecture. One example of this alternative is discussed in section 4.2. Some other methods can be used to binding message authentication; one of them is described in section 4.3.

Threats 3, 4, 5 and 6 can be handled mainly by specifying the conditions for the protocol correctly. The threat 3 is caused by the incorrect use of the home address destination option: if a malicious node sends a packet to a CN with an incorrect address A set to home address destination option the CN sends the upper protocol layer response to the packet to the address A. The real owner of the address A then sees that the CN sends malicious packets to it thus trying to cause e.g. a denial-of-service attack. This can be prevented by requiring the CN to verify that it has a valid binding between the address A and the source address of the received packet.

The threat 4 is caused by the incorrect use of the tunnel between HA and MN: if a malicious node sends a tunneled packet with inner source address set to a MN's address B to a HA of the MN and the HA then forwards the packet, it seems that the MN using the address B has sent the packet. This can be used at least for DoS attacks and it can be prevented by requiring the HA to verify that it has a valid binding between the inner and outer source addresses of the received tunneled packet before it forwards the packet.

The threat 5 is prevented by defining a new routing header type, which can be used only with Mobile IPv6 and only for indicating a Home Address. This prevents the incorrect use of generic routing header to twist the firewall rules and reach some restricted address in a network behind the firewall.

The threat 6 is probably the hardest one to prevent. There is always a risk that security algorithms can be used to launch denial-of-service attacks by bombing a victim with false packets that seem to contain correct information, thus forcing the victim to execute expensive cryptographic algorithms unnecessarily. In the Mobile IPv6 a victim CN may in such case stop processing of all cryptographic algorithms of the Mobile IPv6 and proceed with normal IPv6 operation. The only consequence is that the route optimization of the Mobile IPv6 can't be used anymore, but still the communication with MNs is possible.

4. Proposed Authentication Methods

Initially the plan was to use only IPSec Authentication Header (AH) for binding message authentication, without defining and developing any new authentication protocol. This approach encountered many problems and that is why several other methods have also been developed.

The current specification defines that IPSec ESP should be used for authentication between MN and HA, and Return Routability (RR) should be used for authentication between MN and CN. The specification makes also possible to use some other, more secure methods than RR for authentication between MN and CN. These methods are discussed in the following sections.

4.1 IPSec

IPSec can be used to authenticate and encrypt packets at IP level. That is why it was naturally the first proposed method for authentication of the binding messages.

The biggest problem with the IPsec method is the key distribution. Key distribution of the IPsec, which is called Internet Key Exchange (IKE), uses either preshared secrets or public keys in the key exchange.

When authentication is needed between a MN and a HA, which must have some relationship in advance, because the MN uses services of the HA, the needed secrets might be exchanged beforehand or some private public key distribution can be utilized. After several discussions, IPsec ESP was chosen for binding message authentication between MN and HA instead of IPsec AH.

When considering authentication of the binding messages between a MN and some unknown CN, no preshared secret can be used. There doesn't either exist global public key infrastructure that could be utilized, so at least some other key distribution system than IKE is needed. Because of that and other reasons like threat 6 described in the chapter 3, actually IPsec as a whole isn't very usable for authentication between the MN and the CN.

4.2 Return Routability

Return Routability (RR) [1] method was developed to provide adequate authentication between a MN and a CN. First, it ensures that the MN is able to receive messages with its HoA and CoA, after that it protects the binding messages between the MN and the CN. The MN can receive messages with the HoA only if the MN has created a valid binding to the HA in advance.

A CN has a private secret key, k_{cn} and a random number, N_j , which it renews at regular intervals [Table 1] (e.g. every few minutes). The CN uses the same k_{cn} and N_j with all the mobiles it is in communication with, so it doesn't need to generate and store a new N_j when a new mobile contacts it. Each value of N_j is identified by the subscript j , which is communicated in the protocol, so when N_j is replaced by N_{j+1} , the CN can distinguish messages that should be checked against the old random number from messages that should be checked against the new random number. CNs keeps N_j and a small set of previous values N_{j-1} , N_{j-2} , ... in memory. Older values can be discarded, and messages using them can be rejected as replays.

The key k_{cn} can be either a fixed value or regularly updated. An update of k_{cn} can be done at the same time as an update of N_j , so that j identifies both the random

number and the key. A correspondent node can generate a fresh k_{cn} each time that it boots to avoid the need for secure persistent storage for k_{cn} . The RR signaling happens as follows [Figure 2]:

1. MN(HoA) -> CN: "HoA"
2. MN(CoA) -> CN: "CoA"
3. CN -> MN(HoA): $K0, j$
4. CN -> MN(CoA): $K1, i$
5. MN(CoA) -> CN: BU, K_{bu}, j, i
6. CN -> MN(CoA): BA, K_{ba}
7. CN -> MN(HoA): BR, K_{br}

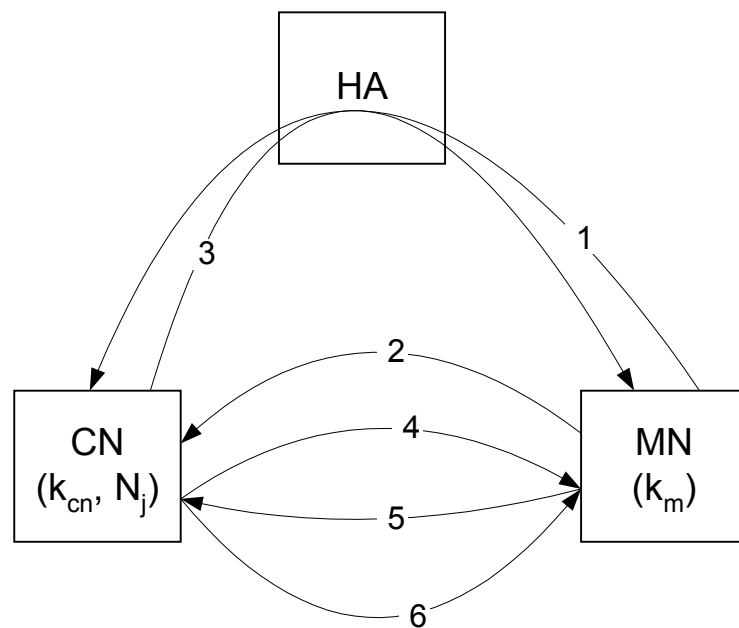


Figure 2. RR Message Flow

The first and the second message are sent concurrently by the MN to the CN to initiate the RR method and they contain only the MN's HoA and CoA respectively. The first message is sent from the HoA and it is sent via a HA by reverse tunneling the packet first to the HA and then forwarding it to the CN. The second message is sent from the CoA to the CN directly.

The third and the fourth messages are sent as responses to the first and the second address respectively. They contain the keys K0 and K1, which are used for authentication of the binding messages, and also the indexes of the used random numbers and private keys. The keys K0 and K1 are calculated as follows:

$$K0 = H_{k_{cn}}(\text{HoA}, N_j, 0)$$

$$K1 = H_{k_{cn}}(\text{CoA}, N_i, 1)$$

HMAC SHA1 function is used to calculate the keys by using the CN's private key k_{cn} from the addresses and the current random number. The final '0' or '1' is used to distinguish keys that are calculated from HoA and CoA.

The fifth message is the binding update message that is sent by the MN to the CN. It is authenticated by using a secret K_{bu} , which is calculated with the HMAC SHA1 function by using k_m as a key from the binding message content. The key k_m is calculated with SHA1 function from the keys K0 and K1. The indexes i and j are used to identify the used random numbers and keys.

$$k_m = H(K0, K1)$$

$$K_{bu} = H_{k_m}(\text{CoA}, \text{CN}, \text{BU}, s)$$

The BU contains HoA, sequence number, which is used to prevent replay attacks, and lifetime, which indicates the preferred lifetime for the binding. The lifetime indicates the preferred time before the binding must be refreshed and thus authenticated again. The last number s is a sequence number that is 0 for the first BU using the key k_m and it is incremented in every subsequent BU messages using the same key. It is used to prevent other nodes from learning the CN's private key k_{cn} from the BUs sent by a MN.

The sixth and the seventh messages are optional and they are authenticated basically in the same way as the fifth message. The BA contains status of the BU processing, sequence number, which is again used to prevent replay attacks, lifetime and refresh time. Lifetime indicates the granted binding lifetime and the refresh time the recommended time to refresh the binding. BR contains the home address to which the request is issued.

$$K_{ba} = H_{K_m}(\text{CoA}, \text{CN}, \text{BA}, s)$$

$$K_{br} = H_{K_m}(CoA, BR, s)$$

The binding lifetime should be adjusted with the renewal period of the CN's random number N_j and the RR authentication period to prevent other nodes from finding out the private key k_{cn} of the CN. The RR authentication period means the interval in which the CN requires MN to perform RR authentication again.

Symbol	Usage
j, i	Indices used to identify random numbers
K_0	First part of the RR authentication key
K_1	Second part of the RR authentication key
K_{ba}	BA authentication data
K_{br}	BR authentication data
K_{bu}	BU authentication data
k_{cn}	CN's private key
k_m	MN's private key, calculated from K_0 and K_1
N_j, N_i	CN's periodically updated random number

Table 1. Symbols used in RR authentication

4.3 Cryptographically Generated Addresses

Cryptographically Generated Addresses (CGA) method is based on the idea that a part of the IPv6 address is derived somehow from the public key of the node. The advantage of this method is, that no certificate is needed to convince another node in the network that the address is used by the owner of the public key that is e.g. included in the packet. This means that no public key infrastructure or such is either needed or used, and the key owner publishes the public key when using it.

As a matter of fact, CGA is not just one proposed method. Several different ways for generating the IPv6 address based on a public key have been proposed [4][2]. This document tries to describe the idea behind all these methods without going into their special characteristics.

The length of the IPv6 address is 128 bits. It consists of a 64-bit network prefix and a 64-bit interface identifier. The network prefix is used for routing in the network and a specific node in a link is identified with the interface identifier, which must be of

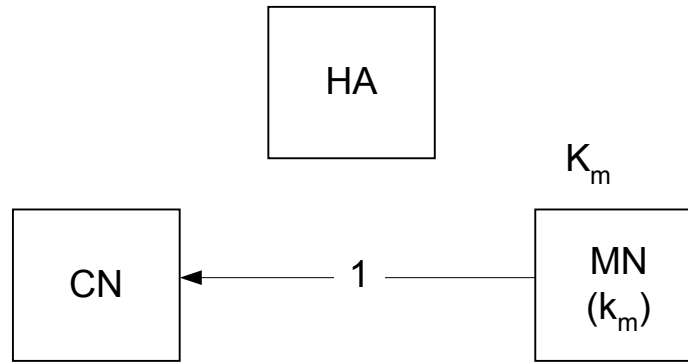


Figure 4. Binding Update Authentication with CGA

The Binding Acknowledgement and Binding Request messages can be authenticated also with this method, but then CN must also use a Cryptographically Generated Address.

Symbol	Usage
K_m	MN's public key
k_m	MN's private key

Table 2. Symbols used in CGA authentication

4.4 Method Comparison

One of the design principles of Mobile IPv6 from the security perspective was that it should not introduce any new threats and vulnerabilities for the IPv6. The problem is that an attacker in the route between two communicating nodes can use binding messages, which are authenticated with using the RR method, to break the connection easily.

This is possible, because any node between a CN and a HA gets both the keys K_0 and K_1 and can use them to convince the CN to believe the impersonated attacker's binding messages. This happens as follows: the attacker M eavesdrops two communicating nodes A and B that are located in their home networks and learns their IP addresses. They can be any type of nodes, i.e. CNs, MNs or even Mobile IPv6 unaware nodes. After that M initiates the RR method by sending messages 1 and 2 directly to B with using its own address as CoA and A's address as HoA. B sends messages 3 and 4 as response to the received messages and M gets the keys K_0 and K_1 . After that M sends a BU to B where it claims that A has moved to its own address and B accepts the message, because it is authenticated correctly with using the RR method.

M has now hijacked the A's connection with B. Because B doesn't know if A is really a Mobile Node or not, this can be used even to hijack a connection where A is a popular WWW-server. One proposed solution for this problem is the bit-method [3]: one bit in the interface ID part of the IPv6 address is used to indicate that the address can be used as HoA, i.e. it can be redirected by using the RR authentication. This partially solves the problem by preventing the redirection of addresses of non-mobile nodes, thus not introducing any new problems for the basic IPv6.

The problem described above doesn't exist in the CGA method, because it uses public key signatures for binding message authentication. If e.g. RSA with long enough keys is used, authentication can be considered to be strong enough. One way to attack against CGA method is to try to find a public-private key pair of which CGA is the same as the victims HoA. With using these keys an attacker can use binding messages even more easily to redirect the address of the victim, because it doesn't need to authenticate itself to the HA of the victim or eavesdrop the RR messages in the path between HA and CN. Because the real length of the hash used in the CGA method is only 62 bits, with using brute-force attack approximately only $2^{62/2}$ attempts is needed, thanks to birthday paradox, to discover a public-private key pair of which CGA is the same as victim's HoA. However it should be kept in mind that every attempt requires also a generation of new public-private key pair, which requires also some resources, although the prime number tests can be ignored when performing the attack. Still this can be considered to be one of the biggest weaknesses of the CGA method.

In the RR method it is also possible that if an attacker finds out the k_{cn} and the current N_j of a CN, it can impersonate itself as any MN and use binding messages to break or hijack their connections with the CN. This is possible because the attacker can use k_{cn} and N_j to form K_0 and K_1 for any CoA and HoA and create binding between them to CN. An attempt to prevent this is the requirement that the N_j must be renewed quite often, e.g. in every 5 minutes. Because the value of N_j is not specified to be unique for every MN, it might be too easy for an attacker to find out the k_{cn} and N_j of a popular WWW-server that might have hundreds of MN clients creating binding concurrently thus giving a lot of K_0 - K_1 pairs to the attacker.

One way to make the RR method more secure is to use IPsec ESP in tunnel mode between the MN and the HA when sending the messages 1 and 3. If these messages are also encrypted in addition to authentication, anyone in the foreign network of the MN cannot break the security of the protocol. This operation is currently an optional feature, but it might be feasible to make it mandatory. This is extremely important if consider that the foreign network where the MN is located is very insecure in the link layer, as e.g. public WLAN, where any hostile client may hijack connections from the MN. On the other hand, it is also possible to use the IPv6 Neighbor Discovery Protocol (NDP) to hijack a connection from the MN, but in this case the MN will detect the hijacking from NDP messages unlike in the previous attack.

Another concern in the CGA is that if it enables the threat 6 so that any CN can be overloaded with the protocol by sending malicious CGA packets that consume all the processor power and memory. That is why it has been proposed that the CGA method should be used in parallel with the RR to provide better security, but not enabling any new threats. This also prevents the use of the weaknesses of CGA alone in attacks against Mobile IPv6.

One concern has been that the Mobile IPv6 should also provide a way to use some other optional authentication methods with the binding messages than the proposed RR method. The problem is that an attacker may prevent the using of those more secure methods quite easily by grabbing or altering the signaling packets and thus forcing the use of RR method. This is called bidding down attack [3].

5. Conclusions

Mobile IPv6 specification is still unfinished and it needs some research work to get it working and to get it widely accepted. The basic functionality has been there for some time already, but the problems have been in the security of the protocol. The security has been identified to be the most crucial part of the protocol, because without a proper security solution, the protocol has no possibility to be accepted and usable at all.

The specified RR method provides some level of security for the Mobile IPv6, but there have been some discussions if it is enough. CGA might be the solution for the problem, but it has not been fully researched yet to know its possibilities to use.

Writing of this document has been a challenging task because the Mobile IPv6 specification is under development at the moment and a lot of changes and new propositions are introduced all the time. Finding the most important ones of them required a lot of reading of different research papers, Internet drafts and mailing list messages and filtering the issues that should be covered in this document. Actually the specification is under heavy changes right now and most of the security issues of the protocol are just now evolving towards their final destination. This means also that there is a real chance to contribute to the development work of an important protocol.

References

1. Johnson, D., Perkins, C. [Mobility Support in IPv6](#). Internet Engineering Task Force, draft-ietf-mobileip-ipv6-16, March 2002. 152 pages.
2. Montenegro, G., Castelluccia, C. [SUCV Identifiers and Addresses](#). Internet Engineering Task Force, draft-montenegro-sucv-02, November 2001. 28 pages.
3. Montenegro, G., Nikander, P. [Protecting Against Bidding Down Attacks](#). Internet Engineering Task Force, draft-montenegro-mipv6sec-bit-method-00, April 2002. 18 pages.
4. O'Shea, G., Roe, M. [Child-proof Authentication for MIPv6 \(CAM\)](#). Microsoft Research Ltd. 5 pages.