A SIMPLE PRIVACY EXTENSION FOR MOBILE IPV6

Claude Castelluccia,[1] Francis Dupont,[2] and Gabriel Montenegro[3]

[1]*INRIA Rhone-Alpes*
655 Avenue de l'Europe
38334 Saint Ismier Cedex, France
Claude.Castelluccia@inria.fr

[2]*GET/ENST Bretagne*
CS 17607, 35576 Cesson-Sevigne Cedex, France
Francis.Dupont@enst-bretagne.fr

[3]*Sun Labs, Europe*
180 Avenue de l'Europe
38334 Saint Ismier Cedex, France
gab@sun.com

Abstract In Mobile IPv6, each packet sent and received by a mobile node contains its home address. As a result, it is very easy for an eavesdropper or for a correspondent node to track the movement and usage of a mobile node. This paper proposes a simple and practical solution to this problem. The main idea is to replace the home address in the packets by a temporary mobile identifier (TMI), that is cryptographically generated and therefore random. As a result, packets cannot be linked to a mobile node anymore and traffic analysis is more difficult. With our solution, an eavesdropper can still identify the IP addresses of two communicating nodes but is not able to identify their identities (i.e., their home addresses). Furthermore since a mobile node uses a new identifier for each communication, an eavesdropper cannot link the different communications of a given mobile node together. We show that HMIPv6 can also benefit from the proposed privacy extension.

Keywords: Mobile IPv6, CGA, Privacy.

1. Introduction

Mobile IPv6 specifies a protocol which allows nodes to remain reachable while moving around in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet.

In Mobile IPv6, a mobile node has two IP addresses: (1) A home address that is an address in the network the mobile node belongs to (i.e., the address in its home network). (2) A care-of address that is a temporary address in the visited network. The home address is constant but the care-of address changes as the mobile node changes links.

One privacy problem of Mobile IPv6 is that the home address of a mobile node is included in all the packets (data and signaling) that it sends and receives. As a result any eavesdropper in the network can identify packets that belong to a particular mobile node (and use them to perform some kind of traffic analysis) and track its movements (i.e., its successive care-of addresses) and usage.

The main security threat against Mobile IPv6 is the remote redirection attack, i.e., binding updates using a fake care-of address. Therefore it is critical to verify that signaling messages are properly authenticated and authorized.

In this paper, we propose a solution to prevent such tracking while still enabling route optimization. In particular, with our proposal, a mobile node can hide its identity, i.e., its home address, from any eavesdropper in the network while still being able to move. Furthermore if a mobile node initiates a communication, it can also hide its identity from its correspondent node. We only look at privacy issues in Mobile IPv6 and assume that a mobile node's identity is not revealed by other mechanisms such as network access control, IPsec setup [Kaufman, 2004], or by the applications (i.e., applications must not use any IP address in their payloads.)

Our solution is practical. It requires only few simple modifications of the Mobile IPv6 specification, it is easily deployable and it does not compromise security or affect performance.

The paper is structured as follows: Section 2 defines the problem we are addressing in this paper. Section 3 presents and analyzes some existing solutions. Section 4 details our proposal. Section 5 explains how our scheme can be combined with HMIPv6 to further improve privacy. Finally, Section 6 concludes our paper.

2. Problem Statement

Mobile IPv6 [Johnson et al., 2004] allows nodes to move within the Internet topology while maintaining reachability and on-going connections between mobile and correspondent nodes. In Mobile IPv6, a mobile node has two IP addresses: (1) A home address that is an address in the network the mobile node belongs to (i.e. the address in its home network). (2) A care-of address that is a temporary address in the visited network. The home address is constant but the care-of address changes as the mobile node moves. The Mobile IPv6 protocol works as follows: When a mobile node moves into a new network it gets a new

care-of address. It then registers the binding between its home address and its current care-of address with its home agent. A home agent is a router in the home network that is used as a redirection point. When a node wants to communicate with a mobile node, it sends the packets to the mobile node's home address. The home agent then intercepts the packets and forwards them to the mobile node current care-of address. At this point, the mobile node may decide to use the route optimization procedure. In this case, the mobile node sends a signaling message (Binding Update) to its correspondent node that contains its current care-of address. The correspondent node can then send the packets directly to the mobile node.

In Mobile IPv6, the home address of a mobile node is included in cleartext in packets it sends and receives. In fact, packets sent by a mobile node includes a home address option that contains its home address. Packets sent by a correspondent node to a given mobile node contains a routing header that includes the mobile node's home address. Furthermore when a mobile node moves to a new subnet, it sends a binding update to its correspondent nodes that contains its home address and its new Care-of Address.

As a result, any eavesdropper within the network can easily identify packets that belong to a particular home address. The eavesdropper can then identify the network the mobile node belongs to and often infer its identity. The home address can be used to perform traffic analysis and track the mobile node's movements and usage.

The goal of our work is propose a practical solution to this problem i.e. a solution that does not require to significantly modify the Mobile IPv6 specification, that is easily deployable and that does not affect performance.

Home Address Option

The home address destination option is used in a packet sent by a mobile node while away from home, to inform the recipient of that packet of the mobile node's home address. For packets sent by a mobile node while away from home, the mobile node generally uses one of its care-of addresses as the source address in the packet's IPv6 header. By including a home address option in the packet, the correspondent node receiving the packet is able to substitute the mobile node's home address for this care-of address when processing the packet, thus making the use of the care-of address transparent to the correspondent node.

The home address option must be placed as follows:

- After the routing header, if that header is present

- Before the fragment header, if that header is present

- Before the AH Header or ESP Header, if either one of those headers is present

Routing header

Before sending any packet, the sending node should examine its binding cache for an entry for the destination address to which the packet is being sent. If the sending node has a binding cache entry for this address, the sending node should use a routing header to route the packet to this mobile node (the destination node) by way of the care-of address in the binding recorded in that binding cache entry. The destination address in the packet's IPv6 header is set to the mobile node's care-of address copied from the binding cache entry.

3. Some possible solutions

Several existing solutions are available, all with their limitations:

1 *IPv6 Privacy Extension*: a solution could be to use the privacy extension described in [Narten and Draves, 2001] to configure the home address and the care-of addresses. While this solution represents a marked improvement over the standard address configuration methods [Thomson and Narten, 1998], and should be used for the home and care-of addresses, we contend that this is not sufficient.

[Narten and Draves, 2001] causes nodes to generate global-scope addresses from interface identifiers that change over time, even in cases where the interface contains an embedded IEEE identifier. As a result when [Narten and Draves, 2001] is used to generate the home address, this address will change periodically but the network prefix (the 64 highest bits) will remain unchanged. This network prefix can still reveal much information about the mobile node's identity to an eavesdropper. This mechanism described in [Narten and Draves, 2001] must be used for the home address and care-of addresses in Mobile IPv6 but one should not rely on it to get full privacy protection.

2 *Home Address option encryption*: another solution could be to encrypt the home address option. This solution is not satisfactory because (1) it would require to modify IPsec implementation (the care-of address should then be used as traffic selector and therefore would need to be updated at each movement of the mobile node) and (2) it would make filtering difficult (currently some firewall implementations may examine the home address option for filtering purposes). Furthermore, this solution does not solve the problem of incoming packets that contain a routing header revealing the home address.

3 *IPsec bi-directional Tunnel (mobile VPN)*: a solution could be to open a bi-directional IPsec tunnel between the mobile node and its home agent [Montenegro, 2001, Arkko et al., 2004]. This solution has the following disadvantages: (1) Addition of extra bandwidth (packets need to be encapsulated) and processing overhead, (2) the routing is suboptimal: to keep Mobile IPv6 efficiency the routing optimization must remain possible.

4. Our Proposal

In our scheme a mobile node uses the privacy extension described in [Narten and Draves, 2001] to configure its home address and care-of addresses. A mobile node must use an interface identifier for its home address that is different from the one used for its care-of addresses. It should also use a new interface identifier when configuring a new care-of address. As a result, it would be more difficult for an eavesdropper to infer the mobile node's identity and track its movement.

We also assign to each mobile node a TMI (Temporary Mobile Identifier) that is a 128-bit long random number. This TMI is used by the mobile node's home agent and correspondent nodes to securely identify the mobile node.

This TMI might be used by the correspondent node as the mobile address in the traffic selectors of the IPsec security association and might also be used by firewalls to perform filtering.

4.1 Temporary Mobile Identifier (TMI)

The TMI of a mobile node must be globally unique. The consequences of two mobile nodes using the same TMI is similar than the consequences of two mobile nodes using the same home address with standard mobile IPv6.

A dedicated prefix (we assume a 16 bit prefix, previously known as a Top-Level Aggregation (TLA) identifier [Hinden et al., 1998]) would be allocated for exclusive use as the TMI space. As a result, the first 16 bits are fixed, but 112 bits are enough to keep the TMI collision probability very close to zero. Defining a specific TLA has several benefits. For example, (1) Any mobile node can be automatically authorized to use any address in this TLA, and, (2) the allocated TLA can be marked as unroutable (i.e., a wrong packet to a TMI destination will be dropped by the first router, not the first default free router). In general, misuses of TMIs become very easy to detect.

A TMI has a role similar to that of a home address in standard MIPv6. As a result, it is also subject to the redirection attack of Mobile IPv6. In Mobile IPv6, a node that communicates with a mobile node keeps a record that binds the mobile node's home address and its current care-of address. When the mobile node moves to another subnet, it sends a binding update that specifies its

new care-of address. Upon receiving this signaling message, the correspondent node updates the mobile node's record with the new care-of address. However to avoid traffic redirection attacks, the mobile node has to prove ownership of the home address contained in the binding update. Otherwise any malicious host could redirect a target home address to one of its addresses and hijack the communication.

To solve this problem, IPv6 Cryptographically Generated Addresses (CGA) have been designed [Montenegro and Castelluccia, 2004, O'Shea and Roe, 2001, Aura, 2003]. CGA are IPv6 addresses where the interface identifier is generated by hashing the address owner's public key. The address owner can then use the corresponding private key to assert authority over its address by signing messages sent. This uses public key cryptography but does not require any additional security infrastructure.

For the same reason, we propose to use TMI that are Crypto-based Identifiers (CBID) [Montenegro and Castelluccia, 2004]. CBIDs have a strong cryptographic binding with their public components (of their private-public key pairs). Because of this, once a correspondent node obtains information about one of these identifiers, it has a strong cryptographic assurance about which entity created it. Not only that, it knows that this identifier is owned and used exclusively by one node: its peer in the current exchange. Hence it can safely heed its redirects when it says that the mobile node is now available at some different care-of address (and later at another). A mobile node generates its CBID as follows:

- It generates a temporary RSA key pair (PK, SK), where PK is the public key and SK the secret key.
- It computes $TMI = SHA1_{112}(PK|imprint)$, where $imprint$ is a 128-bit random value and $SHA1_{112}$ is the $SHA1$ hash function whose output is truncated to 112 bits.

A mobile node can use its CBID for the inline protection of binding updates as follow: it includes in its binding update its public key, PK, the $imprint$ value and signs the whole message with SK. Upon reception of the binding update, the correspondent node can verify that the binding update was issued by the owner of the TMI (and not by an impersonator) by verifying that (1) the TMI was generated from PK and $imprint$ and (2) the signature is valid (i.e., the sender knows SK).

There are essentially two ways an adversary can impersonate a mobile node: (1) He can try to find a RSA key pair and $imprint$ that result to the same TMI than the target node. Since the size of a TMI is 112 bits, the adversary has to try, on average, 2^{111} parameters sets. If the attacker can perform 1 billion hashes per second this would take him $8 * 10^{25}$ years. Note that our scheme is more secure than current Mobile IPv6 schemes that rely on CGA addresses

generated from a 59-bit long hash function [Aura, 2003]. (2) He can try to retrieve the private key SK associated with the mobile node's public key PK. A size of the modulus n of at least 1024 bits is commonly assumed to provide a good security level.

The TMI of a mobile user must be changed periodically (every few minutes, hours or days) in order to avoid TMI leakage as explained in [Narten and Draves, 2001]. This can easily be performed with the CBIDs by keeping the same PK/SK pair but changing the random value $imprint$ periodically.

4.2 Protocol description

Two scenarios have to be considered:

1 *Mobile Client: the mobile node initiates the communication*

When the mobile node initiates the communication and it is moving, we argue that the mobile node does not need to reveal its home address at all. In this case, neither the correspondent node nor any eavesdropper should be able to identify the mobile node home address and thereof its identity.

In our proposal, a mobile node that initiates a communication uses standard Mobile IPv6 with the TMI as Home address. Packets sent and received by a mobile node will contain its TMI instead of its home address. As a result, the mobile identity is hidden from correspondent nodes and from potential eavesdroppers in the network.

Note that in this case correspondent nodes must never route directly to the "home address" (because this "home address" is a non-routable TMI), but should use the care-of address instead.

Since the TMI is a random value unrelated to the home address, neither a correspondent node nor any eavesdropper can link a TMI to a mobile node. Furthermore we suggest that the mobile node change its TMI periodically and use a different one per *session* or per *connection* to make linkability more difficult.

Mobile IPv6 uses a procedure called *Return Routability test* to authorize the establishment of the binding between a home address and a care-of address. This procedure enables the correspondent node to verify that the mobile node is really reachable at its claimed care-of address as well as at its home address. This is done by testing whether packets addressed to the two claimed addresses are routed to the mobile node. The mobile node can pass the test only when it is able to supply proof that it received certain data which the correspondent node sends to those addresses. Note that this procedure requires that the correspondent node know the mobile home address. Therefore our scheme is incompatible

with the return routability procedure since a correspondent does not have to know the mobile node's home address.

2 *Mobile server: the correspondent node initiates the communication*

When the correspondent node initiates the communication, it knows by definition the home address of the mobile node. In this case it is meaningless to hide the home address from it.

However the mobile node might still want to hide its mobility, i.e., its care-of address, to a particular correspondent node. In this case, it must not send any binding update to this correspondent node and use bi-directional tunneling. As a result, packets sent to the mobile node are addressed to its home address and encapsulated by the home agent to its current care-of address. The decision to send or not to send a binding update to a correspondent node is a policy issue that is out of the scope of this paper. Any eavesdropper between the home agent and the mobile node is able to identify and track mobile movements by looking at inner packets. Therefore we suggest to encrypt all packets that are sent between the mobile node and its home agent [Arkko et al., 2004].

If the mobile node decides to use route optimization (and therefore reveal its care-of address to its correspondent node), it must then send a binding update to its correspondent node. This binding update contains the TMI in the home address option and the actual home address is encoded in a newly defined binding update sub-option. Of course to preserve privacy the binding update must be encrypted (the security association should be indexed with the TMI and not the home address). The correspondent node uses the binding update to bind the TMI with the home address and the care-of address.

Subsequent packets between the mobile node and the correspondent node will contain the TMI in the home address option and in the routing header extension instead of the actual home address. As a result an eavesdropper won't be able to identify the packets belonging to a particular node.

The mobility signaling (i.e., the binding update/binding acknowledgment exchange) may be protected by IPsec. For instance in the first scenario, the mobile client could establish an IPsec security association pair for mobility messages using its TMI as its address in its traffic selector, its care-of address for running IKE over, its RSA public key for signing and putting the $imprint$ value in the IDi payload of type ID_KEY_ID or in a new type of CERT payload. The local policy on the correspondent node can recognize this special case and apply a specific authorization, for example accepting only ESP protection of mobility signaling messages. As in IKEv2 [Kaufman, 2004] the authentication

and the negotiation of the first IPsec security association are done in the same exchange, the support of this kind of policy could be easily provided.

5. Privacy with Hierarchical Mobile IPv6

Hierarchical Mobile IPv6 (HMIPv6) is an optimization of Mobile IPv6 that is designed to reduce the amount of signaling required and to improve handoff speed for mobile connections [Soliman et al., 2004]. With HMIPv6, a mobile node gets two care-of addresses: a local one, the local care-of address (LCoA), and a global one, the regional care-of address (RCoA). It then registers the binding between its LCoA and its RCoA with a local server, the *Mobility Anchor Point (MAP)* and the binding between its RCoA and Home Address with its Home Agent and its correspondent nodes. As a result, the correspondent nodes or the home agent only know the global address but don't know where the mobile really is within the domain. This is clearly an improvement over Mobile IPv6 in term of privacy. Note that in HMIPv6, the Mobile Anchor Point (MAP) does not know the home address (i.e., the identity) of the mobile node. The MAP only knows the binding between the mobile's node regional and local care-of addresses. One may argue that a MAP could snoop the mobile host's packets to discover its home address. This is true but however this is still an improvement over Mobile IPv6.

When combining the privacy extension presented in this paper with HMIPv6, a mobile node uses the privacy extension to register with its home agent, its correspondent nodes and the local MAP. We can achieve full privacy protection because the mobile node's identity is hidden from its correspondent nodes and the local MAP. Its local care-of address is hidden from its home agent and correspondent nodes. No node knows the mobile node's identity (home address) and its care-of address together. Furthermore the MAP cannot find out the mobile node identity by snooping its packets (because the home address is not included in packets anymore). We argue that the combination of HMIPv6 with the privacy extension of this paper provides a level of privacy to a mobile node that is superior to that which a VPN provides (bi-directional tunnel between the mobile node and its home agent) but without the cost of a VPN.

Indeed when using HMIPv6 with the proposed privacy extension, we can:

- Hide the location (care-of address) of a mobile node from its Home Agent (this is not provided by a VPN),

- Hide the location (care-of address) of a mobile node from its correspondent nodes (provided by a VPN),

- Hide the identity of a mobile node from its correspondent nodes when the mobile is the initiator (not provided by a VPN),

- Prevent any eavesdropper in the network from identifying the packets that belong to a particular mobile and to track its location.

6. Conclusions

In Mobile IPv6, each packet sent and received by a mobile node contains its home address. As a result, it is very easy for an eavesdropper or for a correspondent node to track the movement and usage of a mobile node. This paper proposes a new, simple and practical solution to this problem. The main idea is to replace the home address in the packets by temporary crypto-based identifiers (CBIDs). As a result, packets cannot be linked to a mobile node anymore and traffic analysis is more difficult. With our solution, an eavesdropper can still identify the IP addresses of two communicating nodes but is not able to identify their identities (i.e., their home addresses). Furthermore since a mobile node uses a new identifier for each communication, an eavesdropper cannot link the different communications of a given mobile node together. We show that HMIPv6 can also benefit from the proposed privacy extension.

References

[Arkko et al., 2004] Arkko, J., Devarapalli, V., and Dupont, F. (2004). *Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents*. IETF, RFC3676.

[Aura, 2003] Aura, T. (2003). Cryptographically generated addresses (CGA). In *6th Information Security Conference (ISC'03*, volume 2851, pages 29–43, Bristol, UK. LNCS.

[Fasbender et al., 1996] Fasbender, A., Kesdogan, D., and Kubitz, O. (1996). Analysis of security and privacy in mobile ip.

[Hinden et al., 1998] Hinden, R., O'Dell, M., and Deering, S. (1998). *An IPv6 Aggregatable Global Unicast Address Format*. IETF, RFC2364.

[Johnson et al., 2004] Johnson, D., Perkins, C., and Arkko, J. (2004). *Mobile IP for IPv6*. IETF, RFC 3775.

[Kaufman, 2004] Kaufman, C., E. (2004). *Internet Key Exchange IKEv2 Protocol*. IETF, draft-ietf-ipsec-ikev2-14.txt.

[Montenegro, 2001] Montenegro, G. (2001). *Reverse Tunneling for Mobile IP, revised*. IETF, RFC3024.

[Montenegro and Castelluccia, 2004] Montenegro, G. and Castelluccia, C. (2004). Crypto-Based Identifiers (cbids): Concepts and applications. *ACM TISSEC*, 7(1).

[Narten and Draves, 2001] Narten, T. and Draves, R. (2001). *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*. IETF, RFC3041.

[O'Shea and Roe, 2001] O'Shea, G. and Roe, M. (2001). "Child-proof Authentication for MIPv6 (CAM). *ACM Computer Communications Review*.

[Reed et al., 1998] Reed, M. G., Syverson, P. F., and Goldschlag, D. M. (1998). Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications*, 16(4).

[Soliman et al., 2004] Soliman, H., Castelluccia, C., El-Malki, K., and Bellier, L. (2004). *Hierarchical MIPv6 mobility management*. IETF, draft-ietf-mipshop-hmipv6-01.txt, work in progress.

[Thomson and Narten, 1998] Thomson, S. and Narten, T. (1998). *IPv6 Address Autoconfiguration*. IETF, RFC2462.