Network Working Group   C. Castelluccia
Internet-Draft   INRIA
Expires: December 30, 2005   F. Dupont
                                                             Point6
                                                      G. Montenegro
                                                          Microsoft
                                                      June 28, 2005

A Simple Privacy Extension for Mobile IPv6
draft-dupont-mip6-privacyext-01.txt

Status of this Memo

   By submitting this Internet-Draft, each author represents that any
   applicable patent or other IPR claims of which he or she is aware
   have been or will be disclosed, and any of which he or she becomes
   aware will be disclosed, in accordance with Section 6 of BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF), its areas, and its working groups. Note that
   other groups may also distribute working documents as Internet-
   Drafts.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt.

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html.

   This Internet-Draft will expire on December 30, 2005.

Copyright Notice

Abstract

   This draft presents a simple privacy extension for Mobile IPv6 that
   prevents eavesdroppers from identifying the packets sent or received
   from a particular mobile node. This extension also allows a mobile
   node to hide its identity from correspondent nodes when the mobile
   node initiates the communication.

1. Introduction

   In Mobile IPv6 [RFC3775], the home address of a mobile node is
   included in the packets that it sends and receives.

   As a result any node 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 care-of address)
   and usage. We propose a solution to prevent such tracking while
   still using route optimization.

   In particular our proposal solves the two following problems:

   - Privacy of mobile client from its correspondent node and from any
      eavesdroppers in the network: the mobile node connects to a remote
      node (a server for example) and wants to hide it identity (i.e.,
      its home address) from this node and from any eavesdropper in the
      network while still being able to move.

   - Privacy of mobile server from eavesdroppers: the remote node
      initiates the communication and the mobile node is able to hide
      its identity (and therefore its locations) from any eavesdropper
      in the network (but not from the remote node).

   We do not solve the problem of privacy of a mobile server from its
   correspondent nodes. In this case a mobile node still needs to
   reveal its care-of address to its correspondent nodes to ensure
   optimal routing. If this level of privacy is desired, one possible
   solution is bi-directional encrypted tunneling via the home agent.
   Full privacy is then provided at the cost of routing performance. It
   should be noted that [HMIPv6] in revealing the regional care-of
   address (RCoA) instead of the care-of address might be an other
   alternative.

   In this draft we only look at privacy issues in Mobile IPv6 and
   assume that a mobile node's identity is not revealed by other
   protocols such as AAA, IKE,...and by the applications (i.e.
   applications must not include any IP address in their payloads.)

2. Problem statement

   In Mobile IPv6, the home address of a mobile node is included in
   clear text in the 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 home
   address. As a result, any eavesdropper within the network can easily
   identify packets that belong to a particular mobile node (and use

them to perform some kind of traffic analysis) and track mobile
movements and usage.

3. Possible solutions

Several solutions are possible, all with their limitations:

- IPv6 privacy extension: a solution could be to used the privacy
   extension described in [RFC3041] to configure the home address and
   the care-of addresses. While this solution represents a marked
   improvement over the default address configuration methods
   [RFC2462], and should be used for the home and care-of addresses,
   we contend that this is not sufficient. [RFC3041] 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 if [RFC3041] is used to
   generate the home address, this address will change periodically
   but the network prefix (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 [RFC3041] 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.

- Home address option encryption: an other solution could be to
   encrypt the home address option. This solution is not
   satisfactory because
       (1) it would require to modify IPsec implementation (security
       associations should then be indexed with the care-of address
       and therefore would need to be updated at each movement of the
       mobile node) and
       (2) it would make the usage of firewalls difficult (currently
       firewalls look at the home address option to perform some
       filtering).
   Furthermore this solution does not solve the problem of incoming
   packets that contain a routing header which reveals the home
   address.

- 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 [RFC3024]. This solution has the following
   disadvantages:
       (1) addition of extra bandwidth (packets need to be
       encapsulated) and processing overhead,
       (2) the routing is suboptimal.

4. **Our Proposal**

   In our scheme a mobile node uses the privacy extension described in
   [RFC3041] 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 identify a mobile node's identity and track its
   movement.

   We also propose to 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 identify
   the mobile node. This TMI might be used by the correspondent node to
   index the correspondent IPsec security association to the mobile and
   might be used by firewalls to do filtering.

4.1 **Protocol description**

   Two cases must be considered:

   - Mobile Client (The mobile node initiates the communication).

   - Mobile Server (the correspondent node initiates the
      communication).

4.1.1 **Mobile client**

   The mobile then uses standard Mobile IPv6 with the TMI as its 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 the correspondent node and from potential eavesdroppers
   in the network.

   Note that in this case the correspondent node must never use the home
   address, i.e., the TMI that is not routable, but must use the care-of
   address (Mobile IPv6 should be modified to provide such
   functionality.)

4.1.2 **Mobile Server**

   In this case, the correspondent node knows the mobile identity by
   definition. If a mobile node wants to hide its mobility, i.e., its
   care-of address, to a particular correspondent node, it must not send
   any binding update to this correspondent node and use bi-directional
   tunneling. As a result the packets that are 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 draft. Any eavesdroppers between the home
agent and the mobile node is able to identify and track the mobile
movement by looking at the inner packet. Therefore we suggest to
encrypt the packets that are sent between the mobile node and its
home agent.

If the mobile node decides to use route optimization, it then sends 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.

4.2 Temporary Mobile Identifier (TMI)

4.2.1 TMI generation

The TMI of a mobile node should be globally unique and must be
locally unique. By locally unique we mean that two mobile nodes
communicating with the same correspondent node/or home agent must use
different TMIs but two mobile nodes communicating with different
correspondent nodes can use the same TMI. The consequences of two
mobile nodes using the same TMI with the same correspondent node is
similar than the consequences of two mobile nodes using the same home
address with standard mobile IPv6. The correspondent node might get
confused...

We propose derive the TMI from the SHA-1 message digest of the mobile
node's home address. The mobile node's home address being globally
unique, the TMI collision probability is therefore very small.
Furthermore the probably of two mobile nodes generating the same TMI
and communicating with the same correspondent node is even smaller
and negligible.

SHA-1 was chosen because its particular properties were adequate to
produce the desired level of randomness and uniqueness. IPv6 nodes
are already required to implement SHA-1 as part of IPsec [RFC2401].

4.2.2 TMI management

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
[RFC3041]...

For example, the digest for the new TMI can be generated as follows:
new digest = SHA-112 (home address | old digest), where "|" stands
for concatenation and SHA-112 the 112 first bits of SHA-1.

A dedicated prefix of 16 bits should used and TMI allocated into this
prefix (i.e., an address in this prefix is known to be a TMI). This
has some drawbacks and many advantages:

- the first 16 bits are fixed (but 112 bits should be enough to keep
   the collision probability very close to zero).

- a TMI is very easy to recognize by bad guys.

+ any mobile node can be automatically authorized to use any address
   in this prefix.

+ this prefix 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 TMI become very easy
   to detect.

4.3 Ownership extension

The routing optimization evolves towards more security so we propose
an extension with an integrated ownership proof. Note that some new
protection devices for routing optimization signaling integrate
privacy mechanisms as [ID.privacy-omipv6].

The TMI still begins with a dedicated prefix marked as not routable
but the digest is derived from a public key and a random value. The
new digest generation rule is: digest = SHA-112 (PublicKey | imprint)
where imprint is a 128-bit temporary random value.

The proof of ownership is the same than for CGAs [RFC3972]: the
PublicKey and the imprint are sent to the correspondent and messages
are signed by the PrivateKey.

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.
2. He can try to retrieve the private key associated with the mobile
node's public key. A size of the modulus 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
[RFC3041]. This can easily be performed with the CBIDs by keeping
the same private/public key pair but changing the random value
imprint periodically.

5. Security Considerations

This document address some privacy issues in the mobile IPv6
protocols. Even if privacy does not provide real security (i.e.,
security through obscurity is poor security) then it makes the job of
bad guys (eavesdroppers, rogue correspondents, ...) harder so should
improve the overall security.

The ownership extension is modeled on the CBID/CGA idea. Security of
this idea is already well known [RFC3972] and in this case the proof
of ownership of the TMI can be coupled with a proof of ownership of
the home address, for instance when the home address is a CGA using
the same RSA private/public key pair.

6. Acknowledgments

John Wells (INRIA), Karim El-Malki (Ericsson), Hesham Soliman
(Ericsson), Jean-Michel Combes (France Telecom DR&D), Imad Add
(INRIA), Pars Mutaf (INRIA)...

7. History

This document was directly extracted from an old proposition by the
first two authors. CBID (Crypto-Based IDentifier) and HMIPv6
extensions / improvements were removed to keep the first version of
this draft very small.

The CGA-like extension was added to the second (-01) version, the
original text is from [MWCN04].

The next version should contain more details about the use of this
proposal in the [HMIPv6] context.

8. IANA Considerations

   Allocation of the needed prefix is the subject of [ID.cgpref].

9. References

9.1 Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", RFC 2119, BCP 14, March 1997.

   [RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address
              Autoconfiguration", RFC 2462, December 1998.

   [RFC3041] Narten, T. and R. Draves, "Privacy Extensions for
              Stateless Address Autoconfiguration in IPv6", RFC 3041,
              January 2001.

   [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support
              in IPv6", RFC 3775, June 2004.

9.2 Informative References

   [HMIPv6]   Soliman, H., Castelluccia, C., El Malki, K., and L.
              Bellier, "Hierarchical Mobile IPv6 mobility management
              (HMIPv6)", draft-ietf-mipshop-hmipv6-04.txt (work in
              progress), December 2005.

   [ID.cgpref]
              Dupont, F., Ed., "An IPv6 Prefix for Cryptographically
              Generated IDs", draft-dupont-ipv6-cgpref-01.txt (work in
              progress), June 2005.

   [ID.privacy-omipv6]
              Haddad, W., Ed., "Anonymity and Unlinkability Extension
              for OMIPv6-CGA",
              draft-haddad-privacy-omipv6-anonymity-00.txt (work in
              progress), June 2005.

   [MWCN04]   Castelluccia, C., Dupont, F., and G. Montenegro, "A Simple
              Privacy Extension to Mobile IPv6", IEEE/IFIP International
              Conference on Mobile and Wireless Communication Networks
              (MWCN), October 2004.

   [RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the
              Internet Protocol", RFC 2401, November 1998.

   [RFC3024] Montenegro, G., Ed., "Reverse Tunneling for Mobile IP,

              revised", RFC 3024, December 2001.

   [RFC3972]   Aura, T., "Cryptographically Generated Addresses (CGA)",
               RFC 3972, March 2005.

Authors' Addresses

   Claude Castelluccia
   INRIA

   Email: Claude.Castelluccia@inria.fr

   Francis Dupont
   Point6
   c/o GET/ENST Bretagne

   Email: Francis.Dupont@enst-bretagne.fr

   Gabriel Montenegro
   Microsoft

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment