Network Working Group
INTERNET-DRAFT
Expires: September 6, 2005
Network Working Group

Feng BAO
Robert DENG
James KEMPF
Ying QIU
Jianying ZHOU

March 7, 2005

Protocol for Protecting Movement of Mobile Nodes in Mobile IPv6
<draft-qiu-mip6-mnprivacy-00.txt>

Status of this Memo

Abstract

When a mobile node roams, its location information can be revealed by monitoring the IP addresses in its IP packets. This document proposes a technique for hiding a mobile node's care-of adress from its correspondent node and its home address from an eavesdropper using reverse tunelling. It also proposes another technique for preventing movement tracing of a mobile node by an eavesdropper during route optimization.

Table of Contents

1. INTRODUCTION

A mobile node (MN) can be uniquely identified by its Home Address (HoA). According to the current Mobile IPv6 specifications RFC3775 [1], a MN will be assigned a care-of address (CoA) when it roams to a foreign network and the MN will inform its Home Agent(HA) and Correspondent Node (CN) about its new CoA through a binding update process. Since the CoA includes location information of its current foreign network (prefix of the subnet) and the binding message as well as the subsequent IP packets contains both HoA and CoA, it is easy to find out the location of a mobile node (and its user) by keeping track of messages containing its HoA. In many circumstances, the users of mobile nodes desire to hide their geographical locations from their correspondent nodes as well as from eavesdroppers.

This document proposes a technique for hiding a mobile node's care-of adress from its correspondent node and its home address from an eavesdropper using reverse tunelling mode. It also proposes another technique for preventing movement tracing of a MN by an eavesdropper during route optimization.

2. ASSUMPTIONS

As in Mobile IPv6 RFC3775 [1], we assume that communications between a Mobile Node (MN) and its Home Agent (HA) are protected via IPSec Security Associations (SAs) (RFC3776 [2]).

In particular, we assume that the MN and the HA shares a secret key Kph. This Kph could be derived from the secret key pre-established manually between the MN and HA or derived from the secret key set up during IKE phase 1 between the MN and the HA.

In addition, the MN and its HA shares a "Pseudo HoA" which is a 128 bits random number. This Pseudo HoA and/or the real HoA will be used as selectors/indexes for the IPSec Security Associations (SAs) between the MN and HA.

3. HIDING CoA FROM CORRESPONDENT NODE AND HoA FROM AN EAVESDROPPER VIA REVERSE TUNNELING

To hide its CoA from the CN and its HoA from an eavesdropper, the MN communicates Mobile IP signaling and IP data packets with its HA via reverse tunneling.

When the MN sends a Home Binding Update from a visited network to its HA, it uses the following packet form to hide its HoA from being monitored on the access network:

```
    IPv6 header (source = CoA, destination = HA)
    Destination option header
       Home Address option (Pseudo HoA)
    ESP header in transport mode
    Mobility header
       Binding Update
         Alternative CoA option (CoA)
```

The HA uses the following packet form to reply a Binding Acknowledgement to the MN that is not on the home link:

```
    IPv6 header (source = HA, destination = CoA)
    Routing header (type 2)
        Pseudo HoA
    ESP header in transport mode
    Mobility header
       Binding Acknowledgement
```

In case the MN fails to receive the Binding Acknowledgement, the MN will retranismit the Binding Update but with a new sequence number in order to detect replay attack.

The MN and HA each computes a new Pseudo HoA as follows:

```
    Pseudo HoA = HMAC_SHA1(Kph, Old Pseudo HoA))
```

The MN and HA then each replaces the old Pseudo HoA with the new one in their respective databases. This updating of Pseudo HoA is only performed once right after the successful home binding update and acknowledgement.

4. HIDING HoA FROM AN EAVESDROPPER VIA ROUTE OPTIMIZATION

The application of pseudo HoAs as described in Section 3 can be used to hide HoA of the MN from an eavesdropper during route optimization.

4.1 Home Test Init from the Mobile Node

The MN sends HoTI to HA with the following packet form:

```
       IPv6 header (source = CoA, destination = HA)
       ESP header in tunneling mode
       IPv6 header (source = HoA, destination = CN)
       Mobility header
          HoTI
```

The HoTI is then forwarded to the CN in the following form:

```
      IPv6 header (source = HoA, destination = CN)
      Destination option
            Pseudo HoA
      Mobility header
            HoTI
```

4.2 Home Test from Correspondent Node

Upon receiving the HoTI from HA, the CN replies with HoT in the following form:

```
      IPv6 header (source = CN, destination = HoA)
      Mobility header
           HoT = (home init cookie, home keygen token, home nonce
                  index)
```

where

```
           home keygen token =
             First (64, HMAC_SHA1(Kcn, (Pseudo HoA | nonce | 0)))
```

and Kcn is the CN's local secret [1].

4.3 Home Test to the Mobile Node

The HA receives the following HoT packet from the CN:

```
      IPv6 header (source = CN, destination = HoA)
          Mobility header
            HoT
```

The HA then sends HoT to the MN in the following form:

```
IPv6 header (source = HA, destination = CoA)
ESP header in tunneling mode
IPv6 header (source = CN, destination = HoA)
Mobility header
   HoT
```

4.4 Binding Update to the Correspondent Node

The MN sends the CoTI to the CN and the CN replies to the MN with CoT, in exactly the same ways as specified in the RR [1].

After receiving the HoT and CoT, the MN sends the Binding Update to the CN in the following packet form:

```
IPv6 header (source = CoA, destination = CN)
Destination Option
   E(Kbm, HoA)
Mobility header
   Binding Update = (Pseudo HoA, home nonce index, ...)
```

where Kbm is the binding update key given by

```
Kbm = SHA1 (home keygen token | care-of keygen token)

home keygen token =
          First (64, HMAC_SHA1(Kcn, (Pseudo HoA | nonce | 0)))
```

```
    Care-of keygen token =
              First (64, HMAC_SHA1(Kcn, (CoA | nonce | 1)))
```

and E(Kbm, HoA) is a symmetric key encryption of the HoA under the secret binding update key Kbm.

After receiving the BU, the CN first computes home keygen token and care-of keygen token. The CN then computes Kbm and decrypts E(Kbm, HoA) to recover HoA. The CN then keeps both HoA and Pseudo HoA in its binding cache table. The subsequent data traffic between the MN and the CN will follow the same procedure and packet format as specified in [1] except that the Pseudo HoA is used in place of the HoA.

5. SECURITY CONSIDERATIONS

The techniques proposed here assume that the RR procedure is secure. In particular, an eavesdropper is not able to eavesdrop at the HA-CN path [1].

6. CONCLUSION

The proposal presents techniques for providing location privacy for mobile nodes. When using reverse tunneling, the proposal hides a MN's HoA from an eavesdropper and CoA from the CN. When using the route optimization, the proposal hides a MN's CoA from an eavesdropper.

7. ACKNOWLEDGEMENTS

8. REFERENCES

[1] D. B. Johson and C. Perkins, "Mobility Support in IPv6", RFC 3775, June 2004.

[2] J. Arkko, V. Devarapalli and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

9. AUTHORS' ADDRESSES

Feng BAO
Institute for Infocomm Research
21 Heng Mui Keng Terrace
Singapore 119613
Phone: +65-6874-8456
EMail: baofeng@i2r.a-star.edu.sg

Robert H. DENG
Singapore Management University
469 Bukit Timah Road
Singapore 259756
Phone: +65-6822-0920
EMail: robertdeng@smu.edu.sg

James KEMPF
DoCoMo USA Labs
181 Metro Drive, Suite 300
San Jose California 95110
USA
Email: kempf@docomolabs-usa.com

Ying QIU
Institute for Infocomm Research
21 Heng Mui Keng Terrace
Singapore 119613
Phone: +65-6874-6742
EMail: qiuying@i2r.a-star.edu.sg

Jianying ZHOU
Institute for Infocomm Research
21 Heng Mui Keng Terrace
Singapore 119613
Phone: +65-6874-6668
EMail: jyzhou@i2r.a-star.edu.sg

INTELLECTUAL PROPERTY STATEMENT

DISCLAIMER OF VALIDITY

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

COPYRIGHT STATEMENT

ACKNOWLEDGMENT

Funding for the RFC Editor function is currently provided by the Internet Society.