IETF Mobile IP Working Group
INTERNET-DRAFT

Charles E. Perkins
Nokia Research Center

5 April 2004

Preconfigured Binding Management Keys for Mobile IPv6

<draft-ietf-mip6-precfgKbm-00.txt>

Status of This Memo

Abstract

A mobile node and a correspondent node may preconfigure a Binding Management Key for authorizing Binding Updates.

1. Preconfiguring a Binding Management Key (Kbm)

A mobile node and a correspondent node may preconfigure a Binding Management Key (Kbm) for authorizing binding management messages, especially Binding Update and Binding Acknowledgement messages. The key MUST be the same length as that configured using inputs from Mobile IPv6 [1] return routability. The key is associated to the mobile node's home address.

Replay protection for Binding Update messages using the preconfigured Kbm depends upon the value of the sequence number field in the Binding Update. If the correspondent node does not maintain information about the recently used values of that field, then there may be an opportunity for a malicious node to replay old Binding Update messages and fool the correspondent node into routing towards an old care-of address. For this reason, a correspondent node that uses a preconfigured Kbm also MUST keep track of the most recent value of the Sequence Number field of Binding Update messages using the preconfigured Kbm value.

When a Binding Update is to be authenticated using such a preconfigured binding key (Kbm), the Binding Authorization Data suboption MUST be present. The Nonce Indices option SHOULD NOT be present. If it is present, the nonce indices supplied MAY be ignored and are not included as part of the calculation for the authentication data, which is to be carried exactly as specified in [1].

2. Applicability Statement

Preconfigured keys between a mobile node and a correspondent node are useful in several specific scenarios:

- mobile node and correspondent node are administered within the same domain, and the correspondent node has good reason to trust the actions of the mobile node

- the correspondent node has some guarantee that the mobile node will behave properly (perhaps by contractual agreement)

- the method of assignment for keys between the correspondent node and mobile node results in a stronger security association than what can be provided by the Return Routability procedure.

- diagnostic procedures

- software development and testing

Generally speaking, the required level of trust that the correspondent node needs for enabling a preconfigured Kbm with a mobile node is more often found within relatively small, closed groups of users who are personally familiar with each other, or who have some external basis for establishing trustworthy interactions.

3. Security Considerations

A correspondent node and a mobile node MAY use a preconfigured binding management key (Kbm) to manage the authentication requirements for binding cache management messages. Such keys must be handled carefully to avoid inadvertent exposure to the threats outlined in [2].

A mobile node MUST use a different binding management key (Kbm) for each node in its Binding Update List. This ensures that the sender of a Binding Update can always be uniquely determined. This is necessary, as this authorization method does not provide any guarantee that the given care-of address is legitimate. For the same reason, this method SHOULD only be applied between nodes that are under the same administration. The return routability procedure is RECOMMENDED for all general use and MUST be the default, unless the user explicitly overrides this by entering a key for a particular peer.

Replay protection for the Binding Authorization Data option authentication mechanism is provided by the Sequence Number field of the Binding Update. This method of providing replay protection fails when the Binding Update sequence numbers cycle through the 16 bit counter (i.e., not more than 65,536 distinct uses of Kbm), or if the sequence numbers are not protected against reboots. If the mobile node were to move every hour, 24 hours a day, every day of the year, this would require changing keys every 7 years. Even if the mobile node were to move every minute, this would provide protection for over a month. Given typical mobility patterns, there is little danger of replay problems; nodes for which problems might arise are expected to use methods other than manual configuration for Kbm anyway. When the sequence number field rolls over, the parties SHOULD configure another value for Kbm.

If a correspondent node does NOT keep track of the Sequence Number for Binding Update messages from a particular mobile node, then the correspondent node could be fooled into accepting an old value for the mobile node's care-of address. In the unlikely event that this address was reallocated to another IPv6 node in the meantime, that IPv6 node would then be vulnerable to unwanted traffic emanating from the correspondent node. In order to circumvent this possibility, correspondent nodes are mandated to keep track of the most recent Sequence Number value in a Binding Update message from the mobile node.

There is no upper bound on the lifetime defined for the preconfigured Kbm. As noted, the key is very, very likely to be quite secure over the lifetime of the security association and usefulness of applications between a mobile node and correspondent node that fit the terms specified in section 2.

4. IANA Considerations

No new protocol numbers are required.

5. Acknowledgement

Thanks are due to everyone who reviewed the discussion of issue #146.

References

[1] D. Johnson, C. Perkins, and J. Arkko. Mobility support in IPv6 (work in progress). Internet Draft, Internet Engineering Task Force, May 2003.

[2] P. Nikander, T. Aura, J. Arkko, G. Montenegro, and E. Nordmark. Mobile IP version 6 Route Optimization Security Design Background. Internet Draft, Internet Engineering Task Force, June 2003.

The first citation is normative, and the second citation is informative only.

Intellectual Property Statement

Full Copyright Statement

Author's Address

Questions about this document can also be directed to the author:

Charles E. Perkins
Nokia Research Center
313 Fairchild Drive
Mountain View, CA 94043
USA

Phone: +1 650 625-2986
Fax: +1 650 625-2502
E-mail: charles.perkins@nokia.com