IETF Mobile IP Working Group
INTERNET-DRAFT

Charles E. Perkins
Nokia Research Center
5 Apr 2003

Preconfigured Binding Management Keys for Mobile IPv6
<draft-perkins-mobileip-precfg-kbm-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.

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. 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.

3. IANA Considerations

No new protocol numbers are required.

4. Acknowledgement

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

References

[1] D. Johnson and C. Perkins. Mobility support in IPv6 (work in progress). Internet Draft, Internet Engineering Task Force, November 2002.

[2] Tuomas Aura and Jari Arkko. MIPv6 BU Attacks and Defenses (work in progress). Internet Draft, Internet Engineering Task Force, February 2002.

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: charliep@iprg.nokia.com