Network Working Group
Request for Comments: 4449
Category: Standards Track

C. Perkins
Nokia Research Center

June 2006

Securing Mobile IPv6 Route Optimization Using a Static Shared Key

Status of This Memo

Copyright Notice

Abstract

A mobile node and a correspondent node may preconfigure data useful for precomputing a Binding Management Key that can subsequently be used for authorizing Binding Updates.

Table of Contents

1. Introduction

This specification introduces an alternative, low-latency security mechanism for protecting signaling related to the route optimization in Mobile IPv6. The default mechanism specified in [1] uses a periodic return routability test to verify both the "right" of the mobile node to use a specific home address, as well as the validity of the claimed care-of address. That mechanism requires no configuration and no trusted entities beyond the mobile node’s home agent.

The mechanism specified in this document, however, requires the configuration of a shared secret between mobile node and its correspondent node. As a result, messages relating to the routability tests can be omitted, leading to significantly smaller latency. In addition, the right to use a specific home address is ensured in a stronger manner than in [1]. On the other hand, the applicability of this mechanisms is limited due to the need for preconfiguration. This mechanism is also limited to use only in scenarios where mobile nodes can be trusted not to misbehave, as the validity of the claimed care-of addresses is not verified.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [2]. Other terminology is used as already defined in [1].

2. Applicability Statement

This mechanism is useful in scenarios where the following conditions are all met:

- Mobile node and correspondent node are administered within the same domain.

- The correspondent node has good reason to trust the actions of the mobile node. In particular, the correspondent node needs to be certain that the mobile node will not launch flooding attacks against a third party as described in [5].

- The configuration effort related to this mechanism is acceptable. Users MUST be able to generate/select a sufficiently good value for Kcn (see [3])

- There is a desire to take advantage of higher efficiency or greater assurance with regards to the correctness of the home address offered via this mechanism.

- This mechanism is used only for authenticating Binding Update messages (and not, e.g., data), so the total volume of traffic is low (see RFC 4107 [4], and the discussion in section 4).

This mechanism can also be useful in software development, testing, and diagnostics related to mobility signaling.

Generally speaking, the required level of trust that the correspondent node needs for enabling a precomputable 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. A typical example scenario where this mechanism is applicable is within a corporation, or between specific users. Application in the general Internet is typically not possible due to the effort that is required to manually configure the correspondent nodes. Application at a public network operator is typically not possible due to requirements placed on the trustworthiness of mobile nodes.

3. Precomputing a Binding Management Key (Kbm)

A mobile node and a correspondent node may preconfigure data useful for creating a Binding Management Key (Kbm), which can then be used for authorizing binding management messages, especially Binding Update and Binding Acknowledgement messages. This data is as follows:

- A shared key (Kcn) used to generate keygen tokens, at least 20 octets long

- A nonce for use when generating the care-of keygen token

- A nonce for use when generating the home keygen token

The keygen tokens MUST be generated from Kcn and the nonces as specified in Mobile IPv6 [1] return routability. Likewise, the binding management key Kbm must subsequently be generated from the keygen tokens in the same way as specified in Mobile IPv6 [1]. The preconfigured data is associated to the mobile node’s home address. Kcn MUST be generated with sufficient randomness (see RFC 4086 [3]).

Replay protection for Binding Update messages using Kbm computed from the preconfigured data 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 toward an old care-of address. For this reason, a correspondent node that uses a precomputable Kbm also MUST keep track of the most recent value of the Sequence Number field of Binding Update messages using the precomputable Kbm value (for example, by committing it to stable storage).

When a Binding Update is to be authenticated using such a precomputable 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 SHOULD be ignored and are not included as part of the calculation for the authentication data, which is to be performed exactly as specified in [1].

4. Security Considerations

A correspondent node and a mobile node may use a precomputable 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 [5]. Many requirements listed in this document are intended to ensure the safety of the manual configuration. In particular, Kcn MUST be generated with sufficient randomness (see RFC 4086 [3]), as noted in Section 3.

Manually configured keys MUST be used in conformance with RFC 4107 [4]. Used according to the applicability statement, and with the other security measures mandated in this specification, the keys will satisfy the properties in that document. In order to ensure protection against dictionary attacks, the configured security information is intended to be used ONLY for authenticating Binding Update messages.

A mobile node MUST use a different value for Kcn for each node in its Binding Update List, and a correspondent node MUST ensure that every mobile node uses a different value of Kcn. 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 the aforementioned preconfigured data 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 send a fresh Binding Update to its correspondent node 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 do so

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 Kcn and the associated nonces. When the Sequence Number field rolls over, the parties SHOULD configure a new value for Kcn, so that new Kbm values will be computed.

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.

Note that where a node has been configured to use the mechanism specified in this document with a particular peer, it SHOULD NOT attempt to use another mechanism, even if the peer requests this or claims not to support the mechanism in this document. This is necessary in order to prevent bidding down attacks.

There is no upper bound on the lifetime defined for the precomputable Kbm. As noted, the key is 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.

5. Acknowledgement

Thanks are due to everyone who reviewed the discussion of issue #146. Thanks to Jari Arkko for supplying text for the Introduction.

6. References

6.1. Normative References

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

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

[3] Eastlake, D., 3rd, Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[4] Bellovin, S. and R. Housley, "Guidelines for Cryptographic Key Management", BCP 107, RFC 4107, June 2005.

6.2. Informative References

[5] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", RFC 4226, December 2005.

Author's Address

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

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

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).