Network Working Group
Internet-Draft
Expires: December 25, 2005

F. Dupont
Point6
J-M. Combes
France Telecom DR&D
June 23, 2005

Care-of Address Test for MIPv6 using a State Cookie
draft-dupont-mipv6-rrcookie-01.txt

Status of this Memo

This Internet-Draft will expire on December 25, 2005.

Copyright Notice

Abstract

This document defines a procedure which performs a "care-of address test" using a state cookie for routing optimization in Mobile IPv6 not protected by the routing routability procedure, i.e., protected by some alternative mechanisms like pre-shared secret or pre-established IPsec security associations.

1. Introduction

The Mobile IPv6 specifications [RFC3775] defines a default protection for routing optimization, the routing routability procedure, which includes an explicit "care-of address test". Alternative protection mechanisms like pre-shared secret [pcfgkbm] or pre-established IPsec security associations [CNIPsec] are more efficient and secure but require in some cases a care-of address test to avoid a "3rd party bombing" vulnerability.

This document proposes a care-of address test procedure at the initiative of the correspondent node using a state cookie as in SCTP [RFC2960] or IKEv2 [IKEv2].

2. Keywords

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 BCP 14, RFC 2119 [RFC2119].

3. A signaling extension for a care-of address test using a state cookie

3.1 Applicability

The care-of address test procedure defined by this document MAY be used in order to check whether the mobile node can really receive packets sent to the care-of address of a new binding update. It SHOULD NOT be used for entry deletion, i.e., when the care-of address is the home address. It MUST be used for real alternate care-of address, i.e., when the address carried by an alternate care-of address option is not the source address of the IP header nor the home address of the mobile node (following the recommendation of [bombing]).

3.2 Protocol

The procedure is based on the state cookie idea of SCTP [RFC2960] which can be found again in IKEv2 proposal [IKEv2]. The binding update is in a first time (1) rejected by a binding acknowledgment with a new dedicated status and a cookie option sent to the tested care-of address. Upon the reception (2) of this binding

acknowledgment, the mobile node retransmits (3) the binding update with the exact received cookie placed in a cookie option. When the correspondent node receives (4) the augmented binding update, it can check by recomputing the cookie and comparing it to the cookie option data that the binding update is from the same mobile node and for the

same care-of address (so it can infer the mobile node is reachable at this care-of address, i.e., a "care-of address test" has been successfully performed).

The cookie MUST reflect the mobile node identity or the binding cache entry or an equivalent, and MUST reflect the tested care-of address. It MUST NOT be easy to infer by the mobile node, including with the knowledge of previous cookies from the same node.

The last point is what to do waiting the retransmitted and augmented binding update. Possibilities are:

- apply the binding update with the new care-of address. It defeats the purpose of the care-of address test so it SHOULD NOT be done, and it MUST NOT be done for a real alternate care-of address.
- keep the previous care-of address. As it is not possible to know whether the previous care-of address is still usable, i.e., whether the mobile node is still reachable at this previous care-of address, the default policy SHOULD NOT be to keep the previous care-of address. The correspondent node MAY keep the previous care-of address in special cases where this is known to be the best solution.
- temporarily disable the binding cache entry, i.e., by using the home address for communication to the mobile node until another binding update is received. This SHOULD be the default policy.

3.3 Cookie Generation Example

This method assumes a global secret key is available and uses in sequence:

- a 16 bit timestamp of when the cookie is created
- the tested care-of address
- the truncated HMAC [RFC2104], keyed by a secret key, of the preceding two fields, the home address and the correspondent address.

The secret key SHOULD be random or pseudo-random and SHOULD be changed reasonably frequently. The timestamp MAY be used to

determine which key was used. The HMAC has to be truncated in order to keep the cookie option length less than the maximum, the higher 96 bits of the HMAC should be enough.

4. Acknowledgments

This document was extracted from [CNIPsec] because what it provides is needed by any alternative to the return routability procedure which has no built-in care-of address test.

5. Security Considerations

Without a test of the care-of address or an other way to trust it, the care-of address presented by the mobile node can be a fake one and offers a 3rd party bombing attack.

Binding updates and acknowledgments are validated using an alternative protection mechanisms so they can't be injected by third parties. The cookie sub-option is small enough to make this procedure a poor candidate for a third party bombing mechanism.

6. IANA Considerations

This document requires:
- a new status for binding acknowledgment.
- a new option for mobility messages used in binding update and acknowledgment messages.

7. References

7.1 Normative References

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, March 1997.

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

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support

in IPv6", RFC 3775, June 2004.

7.2 Informative References

[CNIPsec] Dupont, F. and J-M. Combes, "Using IPsec between Mobile and Correspondent IPv6 Nodes", draft-ietf-mip6-cn-ipsec-01.txt (work in progress), June 2005.

[IKEv2] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-17.txt (work in progress), September 2004.

[RFC2960] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L., and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

[bombing] Dupont, F., "A note about 3rd party bombing in Mobile IPv6", draft-dupont-mipv6-3bombing-02.txt (work in progress), June 2005.

[pcfgkbm] Perkins, C., "Preconfigured Binding Management Keys for Mobile IPv6", draft-ietf-mip6-precfgkbm-02.txt (work in progress), May 2005.

Authors' Addresses

Francis Dupont
Point6
c/o GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30
Email: Francis.Dupont@enst-bretagne.fr

Jean-Michel Combes
France Telecom DR&D
38/40 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Fax: +33 1 45 29 65 19
Email: jeanmichel.combes@francetelecom.com

Intellectual Property Statement

specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

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