Network Working Group	J. Laganier
Internet-Draft	Qualcomm Inc.
Intended status: Experimental	October 26, 2010
Expires: April 29, 2011	

TOC

Authorizing Mobile IPv6 Binding Update with Cryptographically Generated Addresses
draft-laganier-mext-cga-01

Abstract

The standard RFC 3775 mechanism to secure Mobile IPv6 Binding Updates sent by a Mobile Node to its Home Agent relies on the use of a pair of unidirectional IPsec security associations between these two nodes. The standard mechanism to secure Mobile IPv6 Binding Updates sent by a Mobile Node to one of its Correspondent Nodes relies on the use of a return routability test that involves the Correspondent Node verifying reachability of the Mobile Node at both its Home Address and its Care-of Address. The mechanism also requires the correspondent node to send keying material to both of these addresses.
RFC 4866 specifies a standard track mecanism that allows a Mobile Node that has configured a Cryptographically Generated Address (RFC 3972) as its Home Address to secure Mobile IPv6 Binding Updates sent its Correspondent Nodes based on the properties of its Cryptographically Generated Addresses. Note that Cryptographically Generated Addresses have also been used to counter similar security issues in the context of SHIM6 (RFC 5533) and Secure Neighbor Discovery (RFC 3971.)
This memo proposes a mechanism that would let a Mobile Node use a similar mechanism to secure Mobile IPv6 Binding Updates its sent to its Home Agent with a similar technique based on the use of Cryptographically Generated Addresses.

Status of this Memo

Table of Contents

1. Introduction
2. Disclaimer
3. Requirement Levels Key Words
4. Terminology
5. Usage Scenario
6. Mobile Node Operation
7. Home Agent Operation
8. IPv4 Support
9. IANA Considerations
10. Security Considerations
11. Acknowledgment
12. References
    12.1. Normative References
    12.2. Informative References
§ Author's Address

---

1. Introduction

TOC

The standard RFC 3775 (Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.) [RFC3775] mechanism to secure Mobile IPv6 Binding Updates sent by a Mobile Node to its Home Agent relies on the use of a pair of unidirectional IPsec security associations between these two nodes [RFC4877] (Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture," April 2007.). The standard mechanism to secure Mobile IPv6 Binding Updates sent by a Mobile Node to one of its Correspondent Nodes relies on the use of a return routability test that involves the Correspondent Node verifying reachability of the Mobile Node at both its Home Address and its Care-of Address. The mechanism also requires

the correspondent node to send keying material to both of these addresses.
RFC 4866 (Arkko, J., Vogt, C., and W. Haddad, “Enhanced Route Optimization for Mobile IPv6,” May 2007.) [RFC4866] specifies a standard track mecanism that allows a Mobile Node that has configured a Cryptographically Generated Address [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.) as its Home Address to secure Mobile IPv6 Binding Updates sent its Correspondent Nodes based on the properties of its Cryptographically Generated Addresses. Note that Cryptographically Generated Addresses have also been used to counter similar security issues in the context of SHIM6 [RFC5533] (Nordmark, E. and M. Bagnulo, “Shim6: Level 3 Multihoming Shim Protocol for IPv6,” June 2009.) and Secure Neighbor Discovery [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.).
This memo proposes a mechanism that would let a Mobile Node use a similar mechanism to secure Mobile IPv6 Binding Updates its sent to its Home Agent with a similar technique based on the use of Cryptographically Generated Addresses.

---

2. Disclaimer

TOC

This Internet Draft is still Work in Progress.

---

3. Requirement Levels Key Words

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

---

4. Terminology

TOC

Other terms used throughout this document are defined in the relevant documents: [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.), [RFC4866] (Arkko, J., Vogt, C., and W. Haddad, “Enhanced Route Optimization for Mobile IPv6,” May 2007.), [RFC3972] (Aura, T., “Cryptographically Generated Addresses (CGA),” March 2005.).

5. Usage Scenario

TOC

The mechanism described herein is useful in situations where there is a desire not to depend on IPsec for protection of the Mobile IPv6 signaling between the Mobile Node and the Home Agent.

6. Mobile Node Operation

TOC

A Mobile Node sends a Binding Update message to its Home Agent when any of the following applies:

- It is needs to establish a new binding because it is away from the home link and first attaches to a foreign link.
- It attaches to a different foreign link and needs to update the binding with its new care-of address.
- It needs to refresh a binding because it is about to expire.
- It needs to acquire a new permanent home keygen token for the binding, either because it does not have one yet, or because the current permanent home keygen token is going to become unusable due to the sequence number being about to roll over since the token was acquired.
- It needs to deregister an existing binding.

In any of these cases, the Mobile Node sends a Binding Update message to the home agent. The Binding Update message is authenticated by one of the following two authentication methods:

- If the Mobile Node does not have a usable permanent home keygen token in its Binding Update List entry for the home agent, the mobile node MUST authenticate the Binding Update message based on the CGA property of its home address. The Binding Update message MUST omit the Binding Authorization Data option and MUST include the following options:
  - a CGA Parameters option for the Cryptographically Generated Home Address of the Mobile Node as per [RFC4866] (Arkko, J., Vogt, C., and W. Haddad, “Enhanced Route Optimization for Mobile IPv6,” May 2007.).

-a Timestamp option as per [RFC5213] (Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, “Proxy Mobile IPv6,” August 2008.).

-a Signature option as per [RFC4866] (Arkko, J., Vogt, C., and W. Haddad, “Enhanced Route Optimization for Mobile IPv6,” May 2007.).

*If the Mobile Node has a usable permanent home keygen token in its Binding Update List entry for the home agent, the mobile node MUST authenticate the Binding Update message by a proof of its knowledge of the permanent home keygen token. The Binding Update message MUST omit the CGA Parameters, Timestamp, and Signature options and MUST include the following option:

-a Binding Authorization Data option whose authenticator for the Binding Update message is calculated based on the permanent home keygen token alone. The care-of keygen token is set to zero while calculating the authenticator.

---

7. Home Agent Operation

TOC

A Home Agent MUST accept a Binding Update message from a Mobile Node and maintain accordingly the corresponding Binding Cache Entry if the Binding Update message can be authenticated as follows:

*If the Binding Update message does not contain a Binding Authorization Data option, the Mobile Node does not have a usable permanent home keygen token in its Binding Update List entry for the home agent, and the Home AGent MUST authenticate the Binding Update message based on the CGA property of the Mobile Node home address. The Binding Update message MUST include the following options:

-a CGA Parameters option for the Cryptographically Generated Home Address of the Mobile Node as per [RFC4866] (Arkko, J., Vogt, C., and W. Haddad, “Enhanced Route Optimization for Mobile IPv6,” May 2007.).

-a valid Timestamp option as per [RFC5213] (Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, “Proxy Mobile IPv6,” August 2008.). That is, if there is no existing Binding Cache Entry, the time offset between the Timestamp and local Home Agent clock is recorded in the Binding Cache Entry. If there exists a Binding Cache Entry, the Timestamp MUST not differ from the local Home Agent clock

for more than 1.5 times the time offset recorded in the Binding Cache Entry.

-a valid Signature option as per [RFC4866] (Arkko, J., Vogt, C., and W. Haddad, "Enhanced Route Optimization for Mobile IPv6," May 2007.).

*If the Binding Update message contains a Binding Authorization Data option, the Mobile Node has a usable permanent home keygen token in its Binding Update List entry for the home agent, and the Home Agend MUST authenticate the Binding Update message by proof of the Mobile Node's knowledge of the permanent home keygen token by verifying that the authenticator in the Binding Authorization Data option is calculated based on the permanent home keygen token with the care-of keygen token set to zero.

If the Binding Update message has been authenticated based on the CGA property of the Mobile Node home address, the Home Agent MUST include a new permanent Home Keygen Token in the Binding Acknowledgment.

---

8. IPv4 Support

TOC

This mechanism can be used when the Mobile Node is attached to an IPv4-only foreign link by leveraging on [I-D.ebalard-mext-m6t] (Ebalard, A., "MIPv6 from IPv4-only networks," September 2010.). IPv4 applications can be supported via assigning an IPv4 Home Address as described in [RFC5555] (Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers," June 2009.).

---

9. IANA Considerations

TOC

There are no IANA considerations yet for this specification.

---

10. Security Considerations

TOC

There are no security considerations yet for this document.

TOC

11. Acknowledgment

The author acknowledge prior work in the area of Mobile IPv6 security based on Cryptographically Generated Addresses, Statistically Unique and Crypgraphically Verifiable Identifiers, and more.

---

12. References

TOC

12.1. Normative References

TOC

[I-D.ebalard-mext-m6t]	Ebalard, A., "MIPv6 from IPv4-only networks," draft-ebalard-mext-m6t-02 (work in progress), September 2010 (TXT).
[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3775]	Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004 (TXT).
[RFC3972]	Aura, T., "Cryptographically Generated Addresses (CGA)," RFC 3972, March 2005 (TXT).
[RFC4866]	Arkko, J., Vogt, C., and W. Haddad, "Enhanced Route Optimization for Mobile IPv6," RFC 4866, May 2007 (TXT).
[RFC5213]	Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," RFC 5213, August 2008 (TXT).
[RFC5555]	Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers," RFC 5555, June 2009 (TXT).

12.2. Informative References

TOC

[RFC3971]	Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," RFC 3971, March 2005 (TXT).
[RFC4877]	Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture," RFC 4877, April 2007 (TXT).
[RFC5533]	Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6," RFC 5533, June 2009 (TXT).

Author's Address

TOC

	Julien Laganier
	Qualcomm Incorporated
	5775 Morehouse Drive
	San Diego, CA 92121
	USA
Phone:	+1 858 658 3538
Email:	julienl@qualcomm.com