

Mobile Ad hoc Networking (MANET)
Internet-Draft
Intended status: Experimental
Expires: May 16, 2010

U. Herberg
T. Clausen
LIX, Ecole Polytechnique
November 12, 2009

Cryptographical Signatures in NHDP
draft-herberg-manet-nhdp-sec-00

Abstract

This document specifies an extension to the Neighbor Discovery Protocol (NHDP) which uses cryptographic signatures in HELLO messages to encounter a selection of security threats to NHDP.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on May 16, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction	3
2. Terminology	3
3. Applicability Statement	3
4. Protocol Overview and Functioning	4
5. Transmitting a message in NHDP	4
6. Signing a Message	5
7. Processing a Message in NHDP	5
8. Validating a Timestamp	6
9. Validating a Signature	6
10. Parameters and Constants	7
11. Preconditions	7
12. Summary of NHDP Interaction	7
13. Security Threats Alleviation Analysis	8
13.1. Jamming	8
13.2. Identity Spoofing	8
13.3. Link Spoofing	8
13.4. Replay Attack	8
14. IANA Considerations	9
15. Security Considerations	9
16. Normative References	9
Authors' Addresses	10

1. Introduction

This document describes how to use cryptographic signatures for countering a selection of the security threats analyzed in [NHDP-sec-threats]. It specifies the use of such signatures for validating the identity of the originator of a HELLO message, the validity of the content (i.e. links being advertised) of a HELLO message, and the message integrity. The protection so offered against the threats in [NHDP-sec-threats] is evaluated.

This document specifies TLVs for carrying cryptographic signatures in HELLO messages using [RFC5444], and specifies extensions (as enabled by [NHDP]) to the HELLO message processing in [NHDP].

2. Terminology

This document uses the terminology of [RFC5444], [packetbb-sec], [NHDP] and [NHDP-sec-threats].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Applicability Statement

- o [NHDP] enables extensions to recognize additional reasons for rejecting a message as malformed, and mentions security as an explicit example.
- o This document, therefore, elaborates on how this in details can be done, providing a framework for signing and validating messages in NHDP.
- o Note that there is no "no one-size-fits-all", therefore this document uses the containers for carrying signatures and registries for cryptographic code-points as specified in [packetbb-sec]. The specification should therefore be generally be applicable where cryptographic signatures are thought an appropriate security solution. Note that the the choice of the cryptographic algorithm are to be made for each given deployment and that the choice of such is out of scope for this document.
- o This document does not specify how to distribute cryptographic keys, shared secrets, parameters for signature algorithms, etc.

- o Note also that this document assumes that a router which is able to sign messages correctly (e.g. having a valid cryptographic key), is considered trusted. This document does not handle compromised routers with a valid key (e.g. a router that is compromised by a computer virus).

Therefore:

- o This document is generally applicable when [NHDP] is used, and uses the [RFC5444] extension specified in [packetbb-sec].

4. Protocol Overview and Functioning

The framework presented in this document provides two functionalities:

- o Signing a HELLO message
- o Checking whether a signed incoming HELLO message is valid

When NHDP is about to transmit a HELLO message on an interface, this extension:

- o specifies to calculate a digital signature of the message, and
- o specifies how to add that signature to a message for transmission, by way of a SIGNATURE TLV/

The framework allows to add several signatures with different hash and cryptographic functions.

[NHDP] allows to reject incoming HELLO messages prior to processing by NHDP for reasons such as invalid signatures. This extension specifies that for each SIGNATURE TLV in the Message TLV Block of that incoming message, the value of that TLV (i.e. the contained signature) is verified.

5. Transmitting a message in NHDP

HELLO messages are generated as specified in [NHDP]. In addition, each HELLO message MUST set the <msg-orig-addr> as well as the <msg-seq-num> field as specified in [RFC5444]. Before transmission of a message, it is signed as described in Section 6.

6. Signing a Message

This section specifies how to sign a message. Note that a message may be signed several times using different signature algorithms. The following constraints **MUST** be respected when signing a message:

- o The originator address of the message **MUST** be included.
- o The sequence number of the message **MUST** be included.

Optionally:

- o A **TIMESTAMP** TLV (as defined in [packetbb-sec]) **MAY** be added to the message if no such TLV is already included in the message TLV block of that message. The value of the **TIMESTAMP** TLV is the current **POSIX** timestamp (32-bit) of the router, and the type extension is 1 (one).

For each signature algorithm that is used to sign the message:

1. All TLVs of type **SIGNATURE** are temporarily removed from the message and stored in temporary variables. The message size is recalculated accordingly, i.e. to the size of the message without the **SIGNATURE** TLVs.
2. The signature value is calculated over the whole message (as resulting after step 1) according to the chosen signature algorithm.
3. A TLV of type **SIGNATURE** is added in the message TLV block. The TLV value is set to the signature calculated in step 2 as well as the chosen hash and cryptographic algorithms.
4. All other **SIGNATURE** TLVs that have been temporary removed, are restored.
5. The message size is recalculated.

7. Processing a Message in NHDP

NHDP specifies that

"On receiving a **HELLO** message, a router **MUST** first check if the message is invalid for processing by this router"

and gives a number of conditions that will lead to a rejection of the **HELLO** message if any of these conditions is true. The extension

specified in this document adds the following conditions for rejecting a message:

- o The message does not include the <msg-orig-addr> or the <msg-seq-num> field.
- o The message contains more than one TIMESTAMP TLV.
- o Any signature of the message is invalid as specified in Section 9.
- o The timestamp of the message is invalid as specified in Section 8.

8. Validating a Timestamp

This section specifies how to validate a message timestamp.

1. If the message includes a TIMESTAMP Message TLV, and the value of the TIMESTAMP TLV differs from the current POSIX time of more than MAX_TIMESTAMP_DIFF, the message MUST be discarded.

9. Validating a Signature

This section specifies how to validate a message signature.

1. For all SIGNATURE Message TLVs:
 - A. If the hash function and the cryptographic function defined in that are known to the router: goto step 2.
 - B. Otherwise goto step 1
2. If no signature algorithm has been recognized in step 1, the message MUST be discarded.
3. All SIGNATURE TLVs are removed from the message, and the message size is recalculated.
4. The signature is recalculated using the same hash function and cryptographic function as indicated in the TLV, and compared with the signature from the SIGNATURE TLV that has been removed in step 3.
5. If the verification fails, the message MUST be discarded.
6. Otherwise:

- A. Restore all SIGNATURE TLVs.
 - B. Restore the message size.
7. The message can now be processed according to [NHDP].

10. Parameters and Constants

This document specifies the following parameters and constants:

- o MAX_TIMESTAMP_DIFF - The maximum age a message that is to be validated may have. If the current POSIX time of the router validating the message minus the timestamp indicated in the TIMESTAMP TLV of the message is greater than MAX_TIMESTAMP_DIFF, the message will be discarded.

The following constraints apply to these parameters:

- o MAX_TIMESTAMP_DIFF > 0

11. Preconditions

Before a router is able to sign or validate messages, it must initially parameterize some security settings. In particular, it MUST acquire the cryptographic key(s) and any parameters of the cryptographic algorithm from all other routers that are to participate in the network. This document does not specify how a router acquires the cryptographic keys and parameters used in the MANET.

12. Summary of NHDP Interaction

When the security mechanisms as specified in this document is used, the following MUST be observed:

- o NHDP must generate HELLO messages as usual.
- o NHDP MUST allow this security mechanism access to the HELLO message after its generation and prior to transmission, in order that a SIGNATURE TLV can be generated and inserted, as allowed by Section 16 in [NHDP].
- o Any other NHDP extension which adds information to a HELLO message and which wishes this added information to be included when calculating the cryptographic signature MUST do so prior to the

HELLO message being handed off for signature generation.

- o An incoming HELLO message MUST be processed according to this specification prior to processing by [NHDP] as allowed in Section 16 in [NHDP].
- o Any other NHDP extension, which has added information to a HELLO message and which wishes that the HELLO message is rejected if a cryptographic signature is not valid, MUST likewise process the HELLO message only after its processing according to this specification.

13. Security Threats Alleviation Analysis

This section analyzes which of the security threats that are detailed in [NHDP-sec-threats] are alleviated by the framework presented in this document.

13.1. Jamming

Since jamming is a physical layer issue, it cannot be alleviated by protocols on the routing layer. This framework does not counteract jamming attacks, therefore.

13.2. Identity Spoofing

As only routers possessing a valid cryptographic keys are able to sign correctly HELLO messages, identity spoofing is counteracted. If a router does not have access to a valid key or does not sign messages at all, it is not able to create HELLOs that are processed by neighbor routers. Such wrongly signed or unsigned messages are rejected by receiving routers as described in Section 9.

13.3. Link Spoofing

Link spoofing is counteracted by the framework specified in this draft, with the same argument as in Section 13.2. A router without access to a valid cryptographic key cannot sign the message correctly, and therefore the message will be rejected by any receiving routers. Hence, all links postulated by an attacker are ignored.

13.4. Replay Attack

Replay attacks are only counteracted if TIMESTAMP TLVs are included in HELLO messages. This is optional, and depends on synchronized clocks of all routers in the MANET. An attacker which records

messages to replay them later can only do so in the time interval between the timestamp that is contained in the `TIMESTAMP` TLV and `MAX_TIMESTAMP_DIFF` seconds later. As an attacker cannot modify the content if the `TIMESTAMP` TLV (since it does not possess the valid cryptographic key), it cannot replay messages after this time interval. Within this time interval, however, it is still possible to replay attacks.

14. IANA Considerations

This document has no actions for IANA.

15. Security Considerations

This document specifies a protocol extension to NHDP which allows to alleviate some of the security threats of NHDP analyzed in [NHDP-sec-threats].

If no synchronized clocks are available in the MANET, replay attacks cannot be counteracted by this framework.

This framework does not avoid or detect security attacks by routers possessing the cryptographic key that is used to sign messages.

This specification depends on the quality of the used signature algorithm and provides as such the same security considerations as the hash function and the cipher algorithm.

This specification relies on an out-of-band protocol to distribute keys and parameters. The security considerations of that protocol apply.

This specification does not provide a key revocation mechanism.

16. Normative References

[NHDP] Clausen, T., Dean, J., and C. Dearlove, "MANET Neighborhood Discovery Protocol (NHDP)", work in progress draft-ietf-manet-nhdp-11.txt, October 2009.

[NHDP-sec-threats] Herberg, U. and T. Clausen, "Security Threats for NHDP", work in progress draft-herberg-manet-nhdp-sec-threats-00.txt, November 2009.

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5444] Clausen, T., Dearlove, C., Dean, J., and C. Adjih, "Generalized MANET Packet/Message Format", RFC 5444, February 2009.
- [packetbb-sec]
Herberg, U. and T. Clausen, "MANET Cryptographical Signature TLV Definition", work in progress draft-herberg-manet-packetbb-sec-02.txt, July 2009.

Authors' Addresses

Ulrich Herberg
LIX, Ecole Polytechnique
91128 Palaiseau Cedex,
France

Email: ulrich@herberg.name
URI: <http://www.herberg.name/>

Thomas Heide Clausen
LIX, Ecole Polytechnique
91128 Palaiseau Cedex,
France

Phone: +33 6 6058 9349
Email: T.Clausen@computer.org
URI: <http://www.thomasclausen.org/>

