| | |
|---|---|
| Mobile Ad hoc Networking (MANET) | U. Herberg |
| Internet-Draft | T. Clausen |
| Intended status: Experimental Protocol | LIX, Ecole Polytechnique |
| Expires: January 12, 2012 | July 11, 2011 |

Cryptographical Signatures in NHDP
draft-herberg-manet-nhdp-sec-02

## 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



## Copyright Notice



## Table of Contents

## 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 [RFC6130]) to the HELLO message processing in [RFC6130].

## 2. Terminology

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]*.
Additionally, this document uses the terminology of [RFC5444], [packetbb-sec], [RFC6130] and [NHDP-sec-threats].

## 3. Applicability Statement

* [RFC6130] enables extensions to recognize additional reasons for rejecting a message as malformed, and mentions security as an explicit example.

* This document, therefore, elaborates on how this in details can be done, providing a framework for signing and validating messages in NHDP.

* 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.

* This document does not specify how to distribute cryptographic keys, shared secrets, parameters for signature algorithms, etc.

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

* This document assumes that the TLV type extension of the SIGNATURE Message TLV, as defined in [packetbb-sec] is 1, i.e. that a signature is composed of a cryptographic function over a hash value of the message.

Therefore:

* This document is generally applicable when [RFC6130] 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:

* Signing a HELLO message, and

* Checking whether a signed incoming HELLO message is valid.

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

- Specifies to calculate a digital signature of the message, and

- 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.
[RFC6130] 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 [RFC6130]. 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:

- The originator address of the message MUST be included.

- The sequence number of the message MUST be included.

Optionally:

- 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 and type extension 1 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

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

* The message does not include the <msg-orig-addr> or the <msg-seq-num> field.

* The message contains more than one TIMESTAMP TLV.

* Any signature of the message is invalid as specified in Section 9.

* 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 TLV type extension is not 1, or if the hash function and the cryptographic function defined in that TLV 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. All SIGNATURE TLVs are restored.

    b. The message size is restored.

7. The message can now be processed according to [RFC6130].

## 10. Parameters and Constants

This document specifies the following parameters and constants:

*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:

*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 mechanism as specified in this document is used, the following MUST be observed:

* NHDP must generate HELLO messages as usual.

* 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 [RFC6130].

* 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.

* An incoming HELLO message MUST be processed according to this specification prior to processing by [RFC6130] as allowed in Section 16 in [RFC6130].

* 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 valid cryptographic keys are able to correctly sig HELLO messages, identity spoofing is counteracted. If a router does not have access to valid keys 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 document, with the same argument as in Section 13.2. A router without access to valid cryptographic keys 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 of the TIMESTAMP TLV (since it does not possess the valid cryptographic keys), 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 keys 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. References


| | |
|---|---|
| **[packetbb-sec]** | Herberg, U and T Clausen, "MANET Cryptographical Signature TLV Definition", work in progress draft-ietf-manet-packetbb-sec-04.txt, July 2011. |
| **[RFC2119]** | Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. |
| **[RFC6130]** | Clausen, T., Dearlove, C. and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, March 2011. |
| **[NHDP-sec-threats]** | Herberg, U. and T.H. Clausen, "Security Threats for NHDP", work in progress draft-herberg-manet-nhdp-sec-threats-00.txt, November 2009. |
| **[RFC5444]** | Clausen, T.H., Dearlove, C.M., Dean, J.W. and C. Adjih, "Generalized MANET Packet/Message Format", RFC 5444, February 2009. |


## Authors' Addresses


Ulrich Herberg Herberg LIX, Ecole Polytechnique 91128 Palaiseau Cedex, France EMail: ulrich@herberg.name URI: http://www.herberg.name/

Thomas Heide Clausen Clausen LIX, Ecole Polytechnique 91128 Palaiseau Cedex, France Phone: +33 6 6058 9349 EMail: T.Clausen@computer.org URI: http://www.thomasclausen.org/