MANET Cryptographical Signature TLV Definition
draft-herberg-manet-packetbb-sec-02

Ulrich Herberg
Thomas Clausen

Motivation

- MANET routing protocols such as NHDP/OLSRv2 MAY use such included cryptographic signatures for rejecting messages where signature verification fails.
- This document specifies a common exchange format for cryptographic signatures and timestamps.
- With respect to [RFC5444], this document:
    - is intended to be used in the non-normative but intended mode of use of [RFC5444] as described in its Appendix B.
    - is a specific example of the Security Considerations section of [RFC5444] (the authentication part).

The Draft:

- Uses RFC5444
- Specifies a general and flexible TLV format for associating cryptographic signatures to Messages and Packets
- Makes IANA reservations in the TLV Type registries, for Packet and Message TLVs, for common use by MANET routing protocols, e.g. [DYMO], [NHDP], [OLSRv2]

  (Motivation: code-point-preservation, similar to RFC5497's time TLV registrations, for shared use among multiple protocols)

Signature TLV Structure

- Tlv value:

```
<signature> := <hash-function>
               <cryptographic-algorithm>
               <signature-value>
```

  - Where:

    <hash-function> is an 8-bit unsigned integer field specifying the hash function.

    <cryptographic-algorithm> is an 8-bit unsigned integer field specifying the cryptographic function.

    <signature-value> is an unsigned integer field, whose length is <tlv-length>-2, and which contains the cryptographic signature.

- Can be used as Packet or Message TLV

Timestamp TLV Structure

- Tlv value:

  <timestamp> := <time-value>

  - Where:

    <time-value> is an unsigned integer field, whose length is <tlv-length>, and which contains the timestamp.

- Can be used as Packet or Message TLV

TIMESTAMP TLV Type Registration

Name	Type	Type Extension	Description
TIMESTAMP	TBD2	0	Unsigned **Timestamp of arbitrary** length, given by the tlv-length field. The timestamp is assumed to increase strictly monotonously by steps of 1. The MANET routing protocol has to define how to interpret this timestamp
		1	Unsigned **32-bit timestamp** as specified in [POSIX]
		2	**NTP timestamp** format as defined in [RFC4330]
		3	Signed timestamp with **no constraints** such as monotonicity. In particular, it may represent any random value
		4-223	Expert Review
		224-255	Experimental Use

Questions?