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:
  
  \[ \text{<signature>} := \text{<hash-function>} \]
  \[ \text{<cryptographic-algorithm>} \]
  \[ \text{<signature-value>} \]

  - Where:
    
    \[ \text{<hash-function>} \] is an 8-bit unsigned integer field specifying the hash function.

    \[ \text{<cryptographic-algorithm>} \] is an 8-bit unsigned integer field specifying the cryptographic function.

    \[ \text{<signature-value>} \] is an unsigned integer field, whose length is \(<\text{tlv-length}>-2\), and which contains the cryptographic signature.

- Can be used as Packet or Message TLV
Timestamp TLV Structure

- Tlv value:

\[ \text{<timestamp>} := \text{<time-value>} \]

  - Where:

    \[ \text{<time-value>} \] is an unsigned integer field, whose length is \( <\text{tlv-length}> \), and which contains the timestamp.

- Can be used as Packet or Message TLV
## TIMESTAMP TLV Type Registration

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Type Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIMESTAMP</td>
<td>TBD2</td>
<td>0</td>
<td>Unsigned <em>Timestamp of arbitrary length</em>, 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>32-bit timestamp as specified in [POSIX]</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
<td>NTP timestamp format as defined in [RFC4330]</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td>NTP timestamp</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td></td>
<td>Signed timestamp with no constraints such as monotonicity. In particular, it may represent any random value</td>
</tr>
<tr>
<td></td>
<td>4-223</td>
<td></td>
<td>Expert Review</td>
</tr>
<tr>
<td></td>
<td>224-255</td>
<td></td>
<td>Experimental Use</td>
</tr>
</tbody>
</table>
Questions?