Time Synchronization Security using IPsec and MACsec

Appeared in ISPCS 2011

Tal Mizrahi
Israel Networking Seminar
May 2012
Time Synchronization Security

• Time synchronization is used for various applications.
• Securing the time protocol is a must for securing the applications that use it.

• IEEE 1588 standard: Precision Time Protocol (PTP).
• IEEE 1588 is challenging to secure:
  – A large number of nodes involved in the protocol.
  – Hop-by-hop data modification.

• IEEE 1588 - Annex K: experimental security appendix.
Agenda

• Brief overview of IPsec, MACsec, and Annex K.
• The IPsec and MACsec scenarios.
• Attacker types.
• Effectiveness of each attacker in the IPsec and MACsec scenarios, Annex K.
• Summary and comparison.
• Conclusion.
IPsec

- A suite of security protocols defined by the IETF (RFC 4301 – architecture).

- Two main functions:
  - Integrity protection using Authentication Header (AH).
  - Confidentiality using Encapsulating Security Payload (ESP).

- Both functions support:
  - Integrity protection using Integrity Check Value (ICV).
  - Replay protection using Sequence Number.

- Both functions support:
  - Tunnel mode.
  - Transport mode.

- IPsec AH encapsulation.
MACsec

- IEEE 802.1AE – MAC security protocol.
- IEEE 802.1X – authentication, key exchange.

- Supports both encrypted and non-encrypted mode.
- Integrity protection using Integrity Check Value (ICV).
  - L2 header protected by ICV.
- Replay protection using Sequence Number.

- MACsec encrypted packet.
IEEE 1588 Annex K

• Experimental annex in IEEE 1588-2008 (v2).

• Provides data integrity using symmetric key scheme.

• Authentication TLV includes:
  – Integrity Check Value (ICV).
  – Replay protection using replayCounter.

• Annex K authenticated packet.
PTP Security – the IPsec Scenario

- Can be used when PTP is transported over an IP network.
- Network-to-network configuration.
- IPsec can be used in encrypted (ESP) or authenticated (AH) mode.
- Either dedicated tunnel for time sync, or single tunnel for all traffic.
- Typical example: Femtocells in 3GPP.
PTP Security – the MACsec Scenario

- Can be used in L2 networks.
- Either with/without encryption.
- All data is secured on a hop-by-hop basis.
- Typical example: Audio and Video Bridging (AVB).
Typical Attackers

- Mary – internal man-in-the-middle (MITM).
- Jeanie – internal injector.
- Emma – external MITM.
- Enya – external injector.
Enya – WHAT can Enya do?

- Cryptographic Performance Attack.
- L2/L3 DoS attacks.
Emma – WHAT can Emma do?

- Packet Interception and Removal.
- Packet Delay Manipulation.
- Cryptographic Performance Attack.
- L2/L3 DoS attacks.
Jeanie – WHAT can Jeanie do?

- Spoofing.
- Replay.
- Rogue Master Attack.
- L2/L3 DoS attacks.
Jeanie (1) – WHERE can Jeanie be found?

IPsec scenario.

- Jeanie 1 is relevant specifically in the IPsec scenario.
- Network-to-network scheme.

MACsec scenario / Annex K

Time Synchronization Security using IPsec and MACsec
Mary – WHAT can Mary do?

- Packet Interception and Manipulation.
- Packet Delay Manipulation.
- Packet Interception and Removal.
- Spoofing.
- Replay.
- Rogue Master Attack.
- L2/L3 DoS attacks.

Time Synchronization Security using IPsec and MACsec
Mary – WHERE can Mary be found?

**IPsec scenario.**

- Mary 1 is relevant specifically in the **IPsec** scenario.
- Network-to-network scheme.

**MACsec scenario / Annex K**

- Mary 2 is relevant specifically in the **MACsec** scenario.
- Hop-by-hop scheme.

**Annex K**

Time Synchronization Security using IPsec and MACsec

15
## Analysis Summary

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>MACsec Scenario</th>
<th>IPsec Scenario</th>
<th>IEEE 1588 Annex K</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>L2 typically LAN</td>
<td>L3 typically public network</td>
<td>Any</td>
</tr>
<tr>
<td>Security approach</td>
<td>Hop-by-hop</td>
<td>Network-to-network</td>
<td>Hop-by-hop</td>
</tr>
<tr>
<td>Accuracy</td>
<td>+ (TCs/BCs)</td>
<td>~ (no TCs/BCs)</td>
<td>+ (TCs/BCs)</td>
</tr>
<tr>
<td>L2/L3 DoS Attack Prevention</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Internal attackers in the “trusted network” (Jeanie 1, Mary 1)</td>
<td>+</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Internal MITM attacks in intermediate nodes (Mary 2)</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
</tbody>
</table>
Conclusion

• IPsec and MACsec are used in different topologies and scenarios.
• Two **complementary** building blocks for securing time synchronization.
• **Intermediate** solutions in the absence of a standard security solution for PTP.
• **Hybrid** solutions can be used in certain topologies.
Thanks!