Making gPTP Capable for Secure Time Synchronization

2018 IEEE Standards Association (IEEE-SA) Ethernet & IP @ Automotive Technology Day
Overview

Making gPTP Capable for Secure Time Synchronization

**gPTP is facing the same security threats like any other Ethernet protocol**

Attack scenarios, such as Man-in-the-Middle Attacks, Replay Attacks, Spoofing Attacks and Denial of Service Attacks, will also affect time synchronization acc. to gPTP, used in many automotive Ethernet applications.

Attacks, that might utilize an unprotected gPTP will be analyzed and the appropriate requirements are derived. An analyzing phase shows, which requirements are already fulfilled by the specification and how open security threats are solved.
Overview

Contents

Analysis
Analyze which specification item is vulnerable by which attack scenario
- Man In The Middle Attack
- Denial of Service (DoS) Attack
- Time Source Attack
- ...

Coverage
Analyze which threats are covered by existing countermeasures
- Protocol Integrity checks
  - CRC
  - ...

Open Threats
Identify relevant open threats
- Authentication of a Time Master [clock identity]
- Protection against Denial of Service (DoS)
- ...

Countermeasures
Specify countermeasures to solve open threats
- Integrated Timesync protocol security check using Message Authentication Codes (MAC)
- Message gap check
Analysis

Approach

- Automotive time synchronization is realized acc. to AUTOSAR which references gPTP acc. to IEEE.
- This analysis focusses on AUTOSAR SWS 676 (ETHETSYN), because automotive extensions and limitations as well as protocol and software interfaces are specified in detail.
- RFC 7384 helps to group the threats and to categorize the effects.
- Each threat leads to at least one out of the given effects.
- Confidentiality is not a focus because the Time Base is a public source.
... of Timesync Specifications Against Time Protocol Security Requirements

**Analysis**

**Man in the Middle Attack**
- By intercepting and removing of valid Timesync messages
- By manipulation of Timesync messages
- By delaying legitimate Timesync messages

**Time Source Attack**
- Corruption of the external clock sources used by the Global Time Master, e.g. GPS fraud
- Corruption of the internal global time reference clock

**Master Selection Attack**
- Let nodes believe a time from the wrong Time Master

**Denial of Service Attack**
- By overloading the cryptographic components
- On network at layer 2, e.g. message flooding
- By overloading of Timesync messages

**Spoofing Attack**
- By Masquerading as a legitimate participant in the Timesync protocol

**Vulnerability Attack**
- By attacking exploits of Timesync protocol design and implementation vulnerabilities

**Replay Attack**
- Of legitimate Timesync messages

**Network Backtracking**
- By using Timesync messages to identify addresses / latencies to figure out the topology
Coverage

Approach

- Check, whether a threat is already covered or not.
- Uncovered threats are marked with an X.

Analyze which threats are covered by existing countermeasures
- Protocol Integrity checks
- CRC
- ...

TCP/UDP

Wrong Time
Time Accuracy
DoS
... Regarding Already Supported Protection Against Vulnerability

**Coverage**

- Threat coverage by existing specification

<table>
<thead>
<tr>
<th>Man in the Middle Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Integrity Checks</td>
</tr>
<tr>
<td>CRC</td>
</tr>
<tr>
<td>Timeout Detection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time Source Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corruption of the external clock sources used by the Global Time Master, e.g. GPS fraud</td>
</tr>
<tr>
<td>Let nodes believe a time from the wrong Time Master</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Denial of Service Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>By overloading the cryptographic components</td>
</tr>
<tr>
<td>On network at layer 2, e.g. message flooding</td>
</tr>
<tr>
<td>By overloading of Timesync messages</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Spoofing Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>By Masquerading as a legitimate participant in the Timesync protocol</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time Source Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corrupted internal global time reference clock</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Master Selection Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>By attacking exploits of Timesync protocol design and implementation vulnerabilities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>By attacking exploits of Timesync protocol design and implementation vulnerabilities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Backtracking</th>
</tr>
</thead>
<tbody>
<tr>
<td>By using Timesync messages to identify addresses / latencies to figure out the topology</td>
</tr>
</tbody>
</table>

**Protocol Integrity Checks**

- CRC

**Timeout Detection**

**Time Leap Check**
Open Threats

Approach

Identify relevant open threats

- Authentication of a Time Master [clock identity]
- Protection against Denial of Service (DoS)
- ...

Attack Group

<table>
<thead>
<tr>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain threats cannot be solved on protocol-level</td>
</tr>
<tr>
<td>These threats are out of scope of this security concept.</td>
</tr>
<tr>
<td>Mark them with an X.</td>
</tr>
<tr>
<td>Define focus items.</td>
</tr>
</tbody>
</table>

Effect

- Wrong Time
- Time Accuracy
- DoS
Open Threats

... With Given Focus Points

- Define threats as focus items to prepare the countermeasure phase

**Open Threats**

**Man in the Middle Attack**
- Protocol Integrity Checks
  - CRC
  - Timeout Detection

**Time Source Attack**
- Corruption of the external clock sources used by the Global Time Master, e.g. GPS fraud
- Corruption of the internal global time reference clock

**Denial of Service Attack**
- By overloading the cryptographic components
- On network at layer 2, e.g. message flooding
- By overloading of Timesync messages

**Spoofing Attack**
- By Masquerading as a legitimate participant in the Timesync protocol

**Replay Attack**
- Time Leap Check

**Master Selection Attack**
- Let nodes believe a time from the wrong Time Master

**Vulnerability Attack**
- By attacking exploits of Timesync protocol design and implementation vulnerabilities

**Network Backtracking**
- By using Timesync messages to identify addresses / latencies to figure out the topology
### Approach

#### Countermeasures

**Specify countermeasures to solve open threats**
- Integrated Timesync protocol security check using Message Authentication Codes (MAC)
- Message gap check

#### Attack Group

<table>
<thead>
<tr>
<th>Threat</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Authentication of a Time Master [clock identity]</td>
</tr>
<tr>
<td></td>
<td>Ensure integrity of Timesync messages</td>
</tr>
<tr>
<td></td>
<td>Prevention of Spoofing Attacks</td>
</tr>
<tr>
<td></td>
<td>Protection against Denial of Service (DoS)</td>
</tr>
<tr>
<td></td>
<td>Protection against Replay Attacks</td>
</tr>
<tr>
<td></td>
<td>State- and time-based refresh of cryptographic keys</td>
</tr>
<tr>
<td></td>
<td>Ensure high performance of Timesync protocol and SW</td>
</tr>
<tr>
<td></td>
<td>Protection against Timesync message delay and interception</td>
</tr>
<tr>
<td></td>
<td>Allow operation in a mixed secure and non-secure environment</td>
</tr>
<tr>
<td></td>
<td>Confidentiality of time synchronization message data</td>
</tr>
</tbody>
</table>

- At least one of the given countermeasures solves the threat.
- Reminder: Confidentiality is not a focus because the Time Base is a public source.

OR

1=OK
0=NOK
Countermeasures

... to Increase the Protection Against Vulnerability

**Countermeasures**

Specify countermeasures to solve open threats

- Integrated Timesync protocol security check using Message Authentication Codes (MAC)
- Message gap check

**Man in the Middle Attack**

- Protocol Integrity Checks
- **CRC Authentication**
- Timeout Detection

**Time Source Attack**

- Corruption of the external clock sources used by the Global Time Master, e.g. GPS fraud
- Corruption of the internal global time reference clock

**Denial of Service Attack**

- Message Gap Check
- On network at layer 2, e.g. message flooding

- Message Gap Check

**Master Selection Attack**

- **Authentication**

**Replay Attack**

- Time Leap Check

**Spoofing Attack**

- Authentication

**Vulnerability Attack**

- By attacking exploits of Timesync protocol design and implementation vulnerabilities

**Network Backtracking**

- By using Timesync messages to identify addresses / latencies to figure out the topology

**Countermeasures to Increase the Protection Against Vulnerability**

- Specify countermeasures to solve open threats
- Integrated Timesync protocol security check using Message Authentication Codes (MAC)
- Message gap check

**Countermeasures**

**CRC Authentication**

**Timeout Detection**

**Protocol Integrity Checks**

**Time Source Attack**

- Corruption of the external clock sources used by the Global Time Master, e.g. GPS fraud
- Corruption of the internal global time reference clock

**Denial of Service Attack**

- Message Gap Check
- On network at layer 2, e.g. message flooding

**Master Selection Attack**

- **Authentication**

**Replay Attack**

- Time Leap Check

**Spoofing Attack**

- Authentication

**Vulnerability Attack**

- By attacking exploits of Timesync protocol design and implementation vulnerabilities

**Network Backtracking**

- By using Timesync messages to identify addresses / latencies to figure out the topology

© 2018. Vector Informatik GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.00.02 | 2018-10-09
Countermeasures

Authentication

Specify countermeasures to solve open threats

- Integrated Timesync protocol security check using Message Authentication Codes (MAC)
- Message gap check

(T)\*MAC will be placed at the end of an AUTOSAR TLV**, which is a part of the Follow_Up message.

*truncated **Type Length Value

Follow_Up Message Header

preciseOriginTimestamp

Follow_Up Message Fields

IEEE TLV with organizationId 0x0080C2

AUTOSAR TLV Header with organizationId 0x1A75FB

Sub-TLV [Time]
Sub-TLV [Status]
Sub-TLV [UserData]
Sub-TLV [OFS]
Sub-TLV [..]
Sub-TLV [TMAC]

Type = 0x30
Length = 16
TmacByte_0
TmacByte_[..]
TmacByte_15
Countermeasures

... Denial of Service Protection

Time Master and Time Slave are checking whether a gPTP message has been received earlier than a minimum allowed time span.

- If so, the message will be dropped.

Specify countermeasures to solve open threats

- Integrated Timesync protocol security check using Message Authentication Codes (MAC)
- Message gap check
Use Case:
1. Initial Secure Global Time

- The DCM triggers the modification of secured Time Bases by the diagnostic tester via SWC.
- The updated time will be distributed to the network.
Use Case:
2. Authentic Global Time

- **ETHTSYN** implements gPTP with TMAC support.
- The **STBM** calculates/verifies the TMAC by using the keys given by the **KEYM** and the methods provided by the **CSM**.
- The **SECOC** generates freshness values for secure on-board communication by using the synchronized monotonously increasing time value.
Use Case:
3. Secure Time Services

- The STBM logs TMAC calculation/verification events to the SEM.
- The SEM logs events along to a secure Time Base.
Use Case:
4. Global Certificate Expiration Time

The KEYM verifies the certificate expiration time against the secure Time Base.

Implementation in Software on Example of AUTOSAR
Summary

Making gPTP Capable for Secure Time Synchronization

gPTP is facing the same security threats like any other Ethernet protocol. Some of those threats are already caught by the current specification. Especially the usage of an authenticated Time Base increases robustness of the gPTP. Nevertheless, making gPTP secure is an ongoing process. A Layer 2 Firewall helps to increase the protection level.
Making gPTP Capable for Secure Time Synchronization