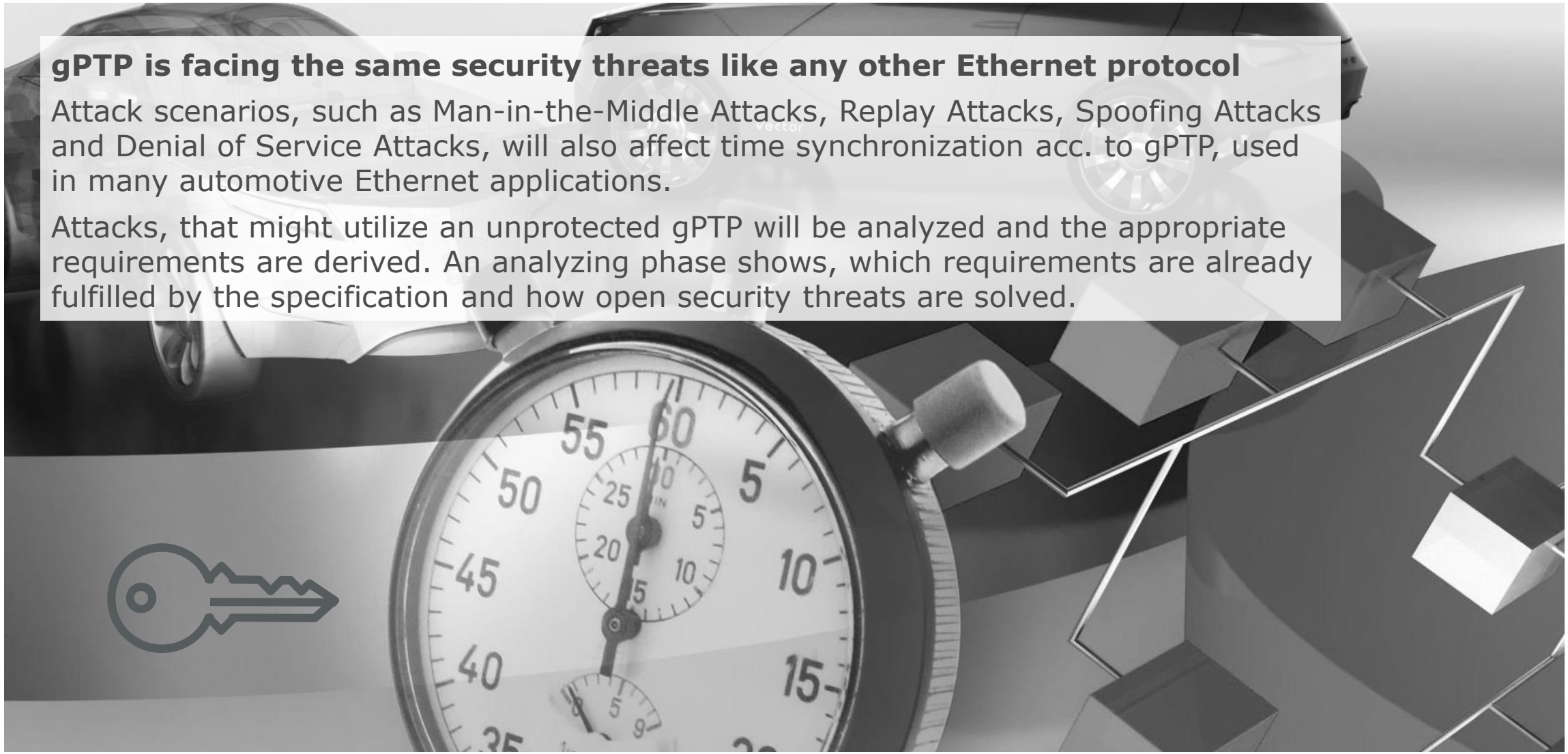
VECTOR

Making gPTP Capable for Secure Time Synchronization

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

V1.00.02 | 2018-10-09

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.

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

Approach

Analysis

AUTOSAR SWS 676

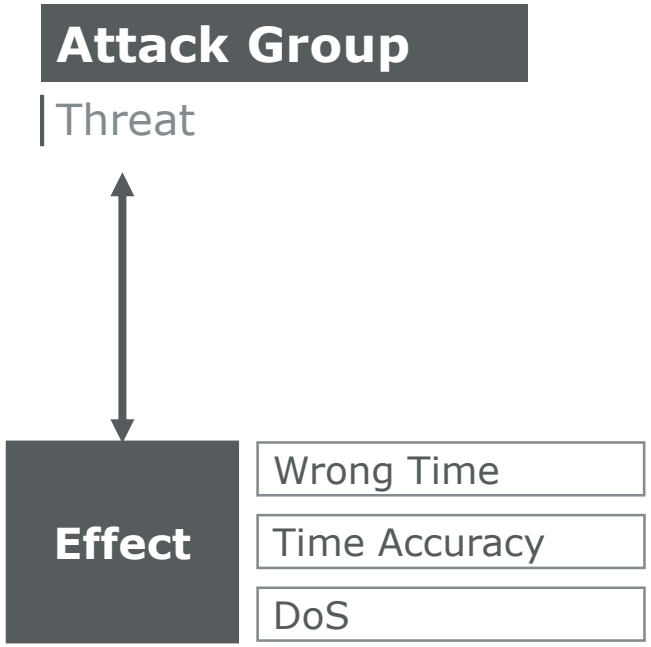
- "Time Synchronization over Ethernet"

IEEE 802.1AS-2011

- "Timing and Synchronization for Time-Sensitive Applications"

IETF RFC 7384

- "Time Protocol Security Requirements"



- Automotive time synchronization is realized acc. to AUTOSAR which references gPTP acc. to IEEE.
- This analysis focusses on AUTOSAR SWS 676 (ETHTSYN), 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

Analyze which specification item is vulnerable by which attack scenario

- Man In The Middle Attack
- Denial of Service (DoS) Attack
- Time Source Attack
- …

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

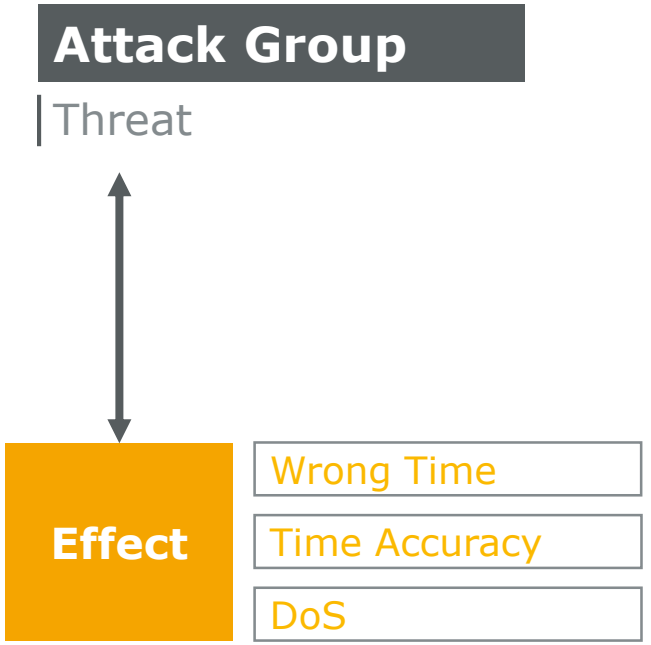
- By using Timesync messages to identify addresses / latencies to figure out the topology

Approach

Coverage

Analyze which threats are covered by existing countermeasures

- Protocol Integrity checks
- CRC
- …



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

… Regarding Already Supported Protection Against Vulnerability

Coverage

- Threat coverage by existing specification

Man in the Middle Attack

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

Time Source Attack

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

Master Selection Attack

- X | Let nodes believe a time from the wrong Time Master

Denial of Service Attack

- X | By overloading the cryptographic components
- X | On network at layer 2, e.g. message flooding
- X | By overloading of Timesync messages

Spoofing Attack

- X | By Masquerading as a legitimate participant in the Timesync protocol

Vulnerability Attack

- X | By attacking exploits of Timesync protocol design and implementation vulnerabilities

Replay Attack

- **Time Leap Check**

Network Backtracking

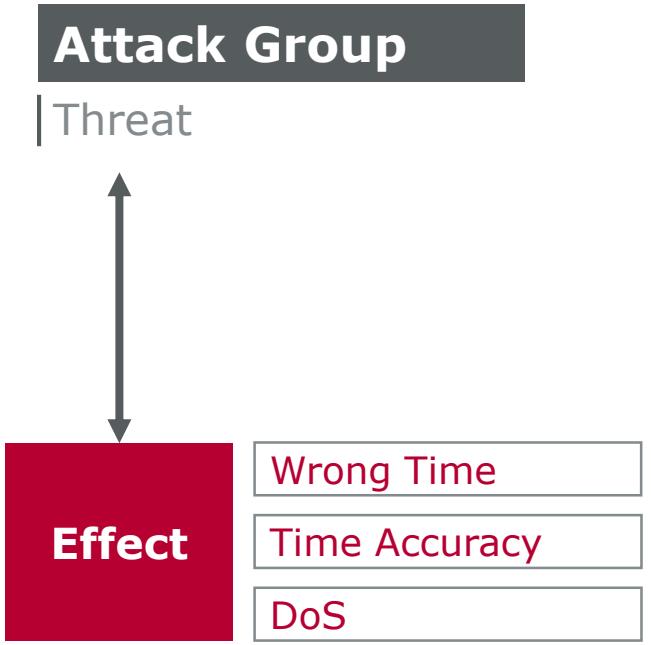
- X | By using Timesync messages to identify addresses / latencies to figure out the topology

Approach

Open Threats

Identify relevant open threats

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



- Certain threats cannot be solved on protocol-level
  - These threats are out of scope of this security concept.
  - Mark them with an **X**.
- Define focus items.

… With Given Focus Points

Open Threats

- Define threats as focus items to prepare the countermeasure phase

Man in the Middle Attack

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

Time Source Attack

- X Corruption of the external clock sources used by the Global Time Master, e.g. GPS fraud
- X 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**
  - X 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

- X By attacking exploits of Timesync protocol design and implementation vulnerabilities

Replay Attack

- **Time Leap Check**

Network Backtracking

- X 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

Threat

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

OR

1=OK
0=NOK

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

… 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**

Denial of Service Attack

- **Message Gap Check**

X On network at layer 2, e.g. message flooding

- **Message Gap Check**

Time Source Attack

X Corruption of the external clock sources used by the Global Time Master, e.g. GPS fraud

X Corruption of the internal global time reference clock

Spoofing Attack

- **Authentication**

Replay Attack

- **Time Leap Check**

Master Selection Attack

- **Authentication**

Vulnerability Attack

X By attacking exploits of Timesync protocol design and implementation vulnerabilities

Network Backtracking

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

Authentication

Countermeasures

Specify countermeasures to solve open threats

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

Calc

- 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

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

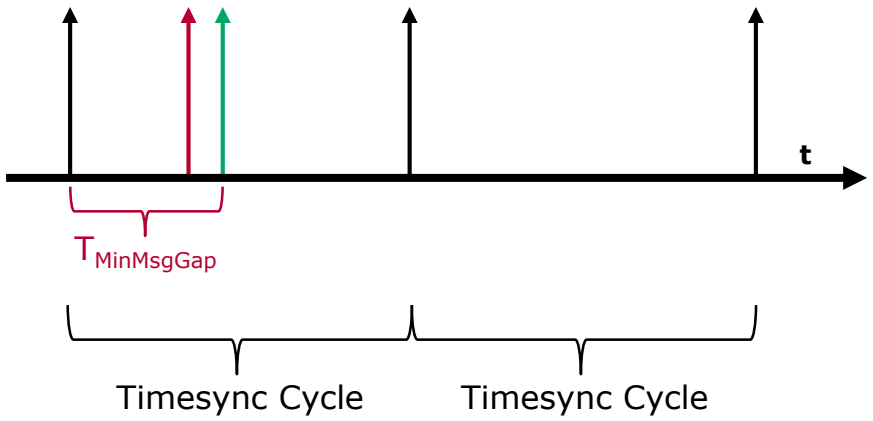
*truncated **Type Length Value

… Denial of Service Protection

Countermeasures

Specify countermeasures to solve open threats

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



Cyclic Timesync Message

Asynchronous Timesync Message

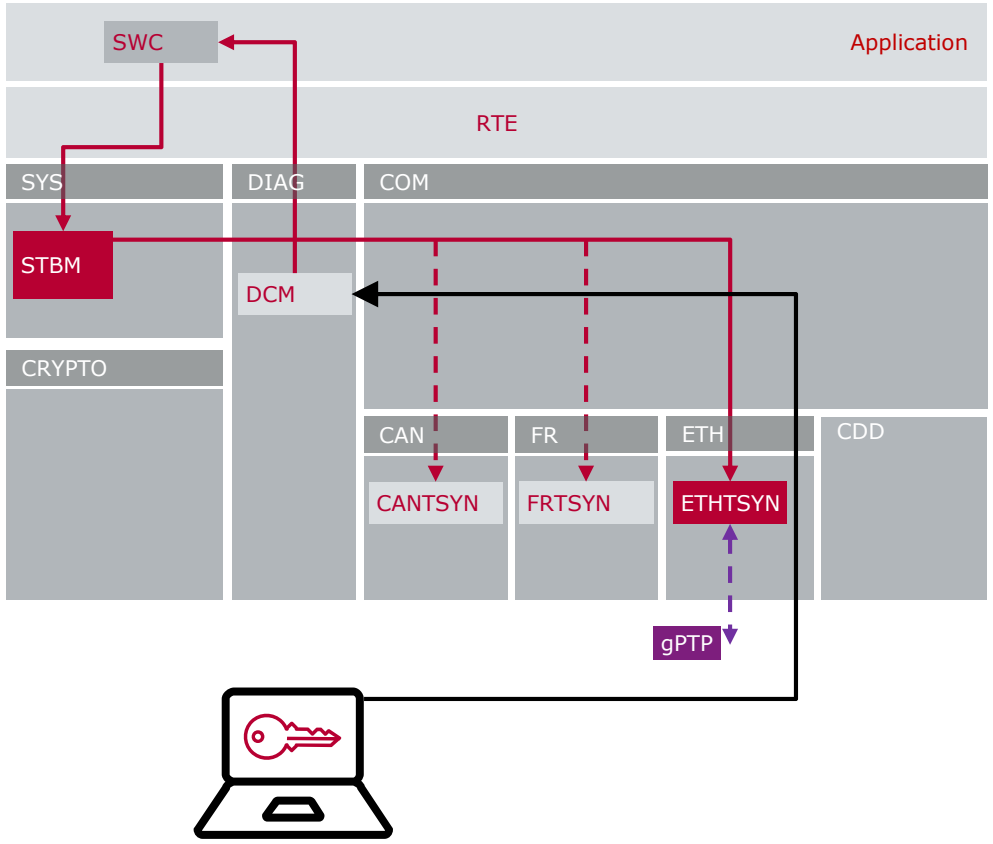
Unexpected Timesync Message

- 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.

Implementation in Software on Example of AUTOSAR

Use Case:

1. Initial Secure Global Time

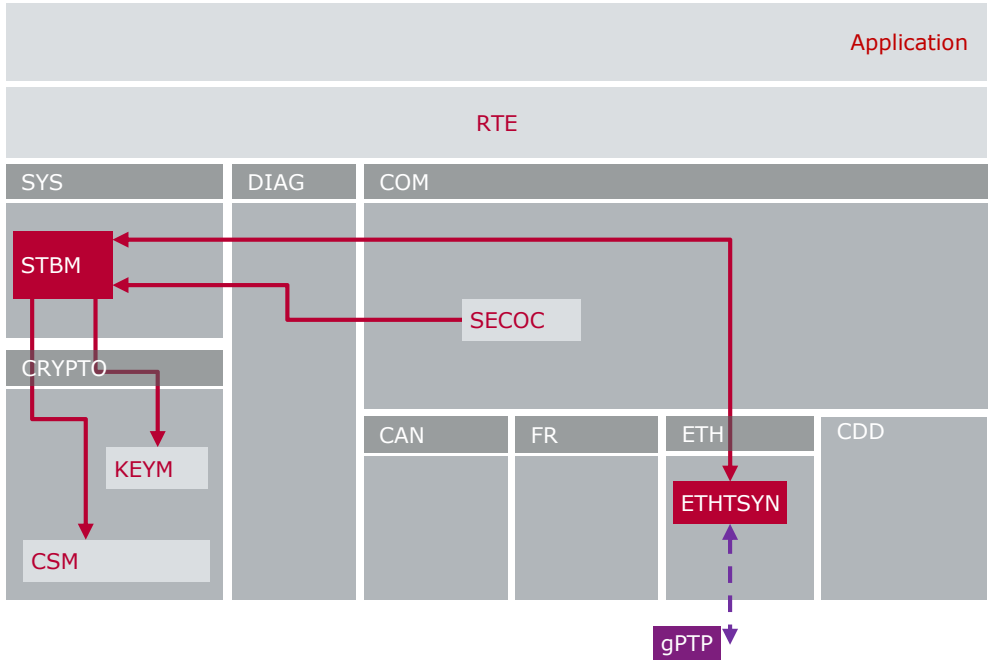


- The DCM triggers the modification of secured Time Bases by the diagnostic tester via SWC.
- The updated time will be distributed to the network.

Implementation in Software on Example of AUTOSAR

Use Case:

2. Authentic Global Time

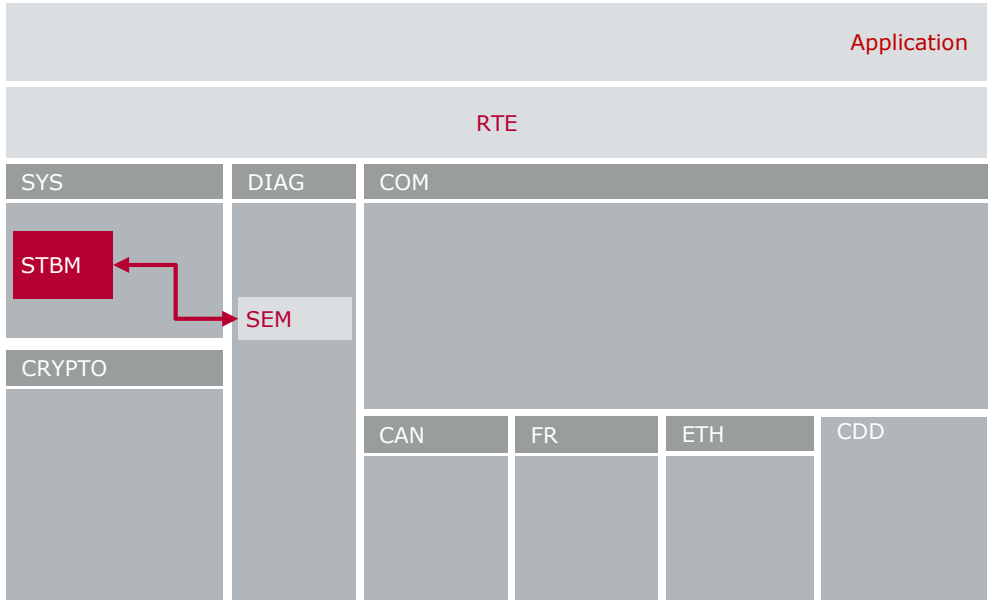


- ETHTSYN implements gPTP with TMAC support.
- The STBM calculates/verifies the TMAC by using the keys given by the KEYM and the methods provided by the CSM.
- The SECOC generates freshness values for secure on-board communication by using the synchronized monotonously increasing time value.

Implementation in Software on Example of AUTOSAR

Use Case:

3. Secure Time Services

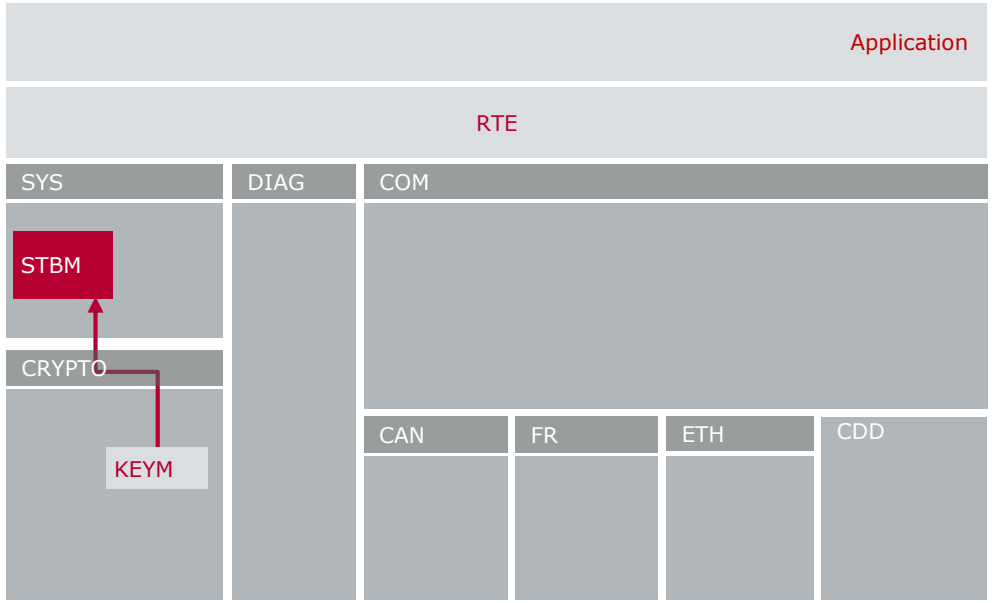


- The STBM logs TMAC calculation/verification events to the SEM.
- The SEM logs events along to a secure Time Base.

Implementation in Software on Example of AUTOSAR

Use Case:

4. Global Certificate Expiration Time



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

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

For more information about Vector
and our products please visit

www.vector.com

Author:
Jesse, Bernd
Vector Germany