Efficient testing of ECUs despite Security

Vector Cyber Security Symposium 2017
Security makes testing harder

- **Security is a must have**
  Todays features in vehicles require security

- **Test Tools must support security**
  Access is restricted by OEM-specific security mechanisms

- **Vector Security Manager**
  How does Vector make efficient testing possible
Vehicle network architecture in the past

No external interfaces

Isolated from the outside-world

Classical automotive networks (CAN, Flexray,...)
Vehicle network architecture today

Many important external interfaces

Connected to the outside-world

Ethernet as new network technology
Vehicle network architecture today

Efficient testing of ECUs despite Security

Many important external interfaces

Security is required!

Connected to the outside-world

Ethernet as new network technology
Efficient testing of ECUs despite Security

Testing vehicles
Efficient testing of ECUs despite Security

Testing vehicles in the past

Any test tool could communicate with the ECU networks

Security:
✓ Data Integrity
✓ Seed & Key

Testing network communication
✓ Reading network data
✓ Stimulating
✓ Replay recorded data
Efficient testing of ECUs despite Security

Testing vehicles today

Security:
- Integrity
- Authentication
- Encryption
- TLS
- SecOC

Any test tool could communicate with the ECU networks.

Testing network communication
- ✔ Reading network data
- ✗ Stimulating
- ✗ Replay recorded data
Efficient testing of ECUs despite Security

Testing vehicles today

Test tools must support security

Security:
- Integrity
- Authentication
- Encryption
- TLS
- SecOC

Testing network communication
- Reading network data
- Stimulating
- Replay recorded data
Efficient testing of ECUs despite Security

Diversity of security implementation

Secured Onboard Communication

**Sender**
- Secret key $k$
- PDU-ID
- DLC
- Data
- Authentic-1-PDU
- Freshness
- MAC

**MAC calculation**
- Authentic-1-PDU
- FV
- MAC
- Secured I-PDU

**Receiver**
- Secret key $k$
- PDU-ID
- DLC
- Data
- Authentic-1-PDU
- Freshness
- MAC

**MAC verification**
- Authentic-1-PDU
- FV
- MAC
- Secured I-PDU

**OEM 1**
- Time-based freshness
- CMAC
- Keys on server

**OEM 2**
- Trip-based freshness
- SipHash
- Keys in secured container

**OEM 3**
- Time-based freshness
- Challenge-Response
- CMAC
- Default key in development
**Effect on test tools**

**Test tools have to manage a huge diversity of security implementations**

- Accessing OEMs security data
  - Keys
  - Certificates

- Managing different security algorithms
  - CMAC
  - Sip Hash

- Different freshness models
  - Time-based
  - Trip-based
  - OEM specific variants

- Security on different layers
  - SecOC
  - TLS
Security in a vehicle's life cycle

Test tools have to manage security depending on the vehicle's life cycle.

- **Security**
  - Active / Inactive
- **Key**
  - Default key
  - Flexible
- **Freshness**
  - Development
- **Backend**
  - Development
- **Certificates**
  - Full Access

- **Development**
  - Active
  - Key generation
  - Fixed, Initial value
  - Productive
  - Restricted

- **Production**
  - Active
  - Defined vehicle key
  - Fixed, Any value
  - Productive
  - Restricted

- **After Sales**
  - Active
Vector Security Manager concept

Efficient testing of ECUs despite Security

Vector Security Manager

Crypto Backend

Security Sources

Vector Tools

CANoe  CANape  ...

Device Under Test

Interface

Network
Efficient testing of ECUs despite Security

Vector Security Manager concept – Security Profiles

- OEM specific Security Source
  - Implements specific security algorithms
  - Provides access to keys and certificates on OEM specific infrastructure
  - Provides Security Profiles

- Security Manager
  - Central secret management for all Vector tools
  - Encapsulation of secrets (do not forward them)
  - Provides functional interface to tools
Efficient testing of ECUs despite Security

Summary

- Vehicles today with many external interfaces require security mechanisms

- Efficient testing is only possible if the test tool supports the OEM specific security
  - Security restricts access and does not distinguish between tester and hacker
  - High diversity of security data and implementations

- Vector Security Manager is Vectors’ solution to efficiently test secured vehicle networks and ECUs
  - Management of security data (Keys, Certificates)
  - Implementation of OEM specific security, freshness models
  - Unique secret management for all Vector tools
I wish you efficient testing of secured vehicles!
For more information about Vector and our products please visit

www.vector.com

Author:
Brenner, Matthias
Vector Germany