Security with CANoe.Ethernet and Security Manager

Agenda VectorAcademy

Delivery Format:	This Course is offered in Remote Format
Duration:	5 hours
Target Group:	Experienced users of CANoe.Ethernet
Prerequisites:	Good knowledge of CANoe and CANoe.Ethernet including communication protocols (OSI layers 1-4) and application protocols (DoIP, SOME/IP, AUTOSAR PDU)
Goal:	Overviw and classification of commonly used Security Mechanisms and Protocols for TLS/DTLS and IPsec. Knowledge of phases during a secure communication and used sub-protocols. Procedure of Measurement, Simulation and Trouble-Shooting with CANoe (Implementation of Security in AUTOSAR is not content of this workshop).

1. Introduction

- General Goals of Security
- Automotive Cyber Security within the OSI Layers
- Overview of Security Tasks, Methods, Algorithms and Protocols

2. Basics of Security

- Symmetrical and Asymmetrical Cryptography
- Hashing , Message Authentication Code and Signatures
- Certificates, Key Exchange and Cipher Suite

3. Security by CANoe.Ethernet and the Security Manager

- Vector Security Manager and its CANoe Client
- Public Key Infrastructure
- Typical use cases at measurement, simulation and offline analysis

4. Transport Layer Security (TLS) and Datagram TSL (DTLS)

- TLS/DTLS Phases and Sub-Protocols
- TLS/DTLS in practice with CANoe and the Security Manager
- Authentication by certificates
- Exercises for several use cases
- Examples for different realization options

5. IPsec in Transport Mode with Authentication Header

- Establihment of an Security Association with IKEv2 Protocol
- Secure data transmission with Authentication Header in Transport Mode
- Exercise: Imported Security Profile and Simulation with CANoe