Empowering Tomorrow’s Automotive Software
www.etas.com

Intrusion detection for vehicles **ESCRYPT CycurIDS**

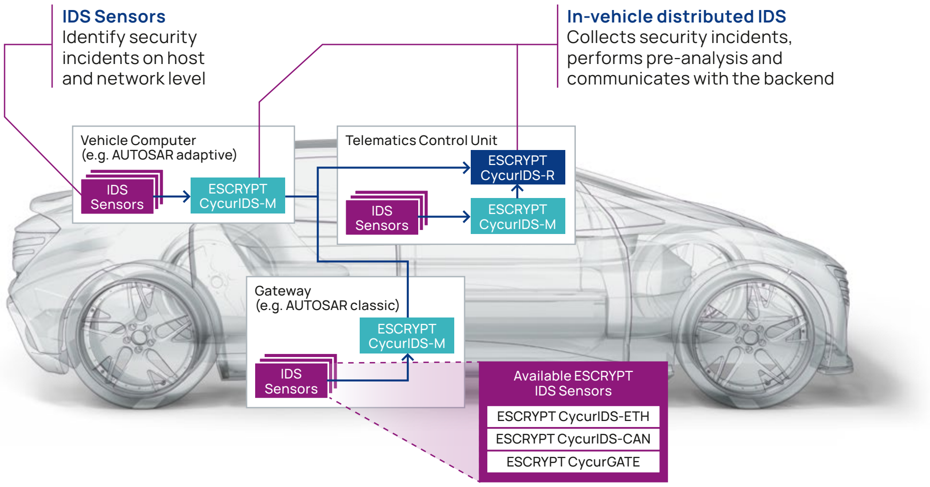
Continuous security monitoring with ESCRYPT intrusion detection solutions

With the increasing connectivity of vehicles, new vectors for cyberattacks are emerging and attackers are constantly perfecting their methods. This erosion of security concerns all building blocks of a connected vehicle fleet: the vehicles themselves as well as the corresponding vehicle backend services.

Ever since the recent enactment of UN R155, cybersecurity monitoring has become a top priority in the automotive industry. OEMs and fleet operators are required to provide effective security risk management for vehicles throughout their entire life cycle.

One of the key elements for achieving this is attack detection via intrusion detection systems (IDS) in the vehicle. But how does a viable IDS solution for the vehicle look like – given the challenges of a distributed E/E architecture with heterogeneous systems and communication protocols, the high performance requirements and the large limits on available computing resources and storage?

ETAS is offering a solution that is tailor-made for current and future vehicles with its ESCRYPT IDS senors CycurIDS-CAN for CAN/CAN-FD networks, CycurIDS-ETH for Ethernet networks, and host-based IDS tailored to automotive ECUs. The IDS manager ESCRYPT CycurIDS-M and the IDS reporter ESCRYPT CycurIDS-R complete the offer.


IDS Sensors
Identify security incidents on host and network level
In-vehicle distributed IDS
Collects security incidents, performs pre-analysis and communicates with the backend
Vehicle Computer (e.g. AUTOSAR adaptive)
IDS Sensors
ESCRYPT CycurIDS-M
Telematics Control Unit
ESCRYPT CycurIDS-R
IDS Sensors
ESCRYPT CycurIDS-M
Gateway (e.g. AUTOSAR classic)
ESCRYPT CycurIDS-M
IDS Sensors
Available ESCRYPT IDS Sensors
ESCRYPT CycurIDS-ETH
ESCRYPT CycurIDS-CAN
ESCRYPT CycurGATE

Distributed vehicle IDS architecture

- CycurIDS-CAN, CycurIDS-ETH and CycurGATE act as smart sensors aggregating and pre-selecting potential security events (SEV) to enable a fast and correct analysis
- Host-based IDS for risk-based monitoring of ECUs
- CycurIDS-M collects, analyses, aggregates, persists, and reports raised security events to the CycurIDS-R
- CycurIDS-R reports the security events from the vehicle to the VSOC

Components of the in-vehicle intrusion detection solution

ETAS offers a modular system of in-vehicle IDS products. The network IDS products ESCRYPT CycurIDS-CAN and ESCRYPT CycurIDS-ETH

- are fully interoperable with the IDS manager concept and can be incorporated as a "smart sensor" to detect intrusions on CAN and Ethernet
- offer graphical user interface based configuration tools providing automatic rule generation and simulation
- support reporting and logging of anomalies, either locally or to the Vehicle Security Operations Center (VSOC)

ESCRYPT CycurIDS-CAN

- Monitors forwarded CAN traffic and detects potential attacks (anomalies)
- Provides heuristic and signature-based detection on ECU

Exemplary detection features

- Allows to observe message frequency to detect message injection
- Makes it possible to compare all messages on the busses with a whitelist to detect unspecified messages
- Allows to detect malicious diagnostic requests while driving, e.g. detect attempts to shutdown certain ECU

ESCRYPT CycurIDS-M

- Acts as security event management for automotive ECUs
- Comes in two product variants:
  - for deeply embedded ECUs
  - for high performance ECUs
- Is an AUTOSAR compliant solution that is designed to be flexibly extended to cover any customer aggregation, persistence or reporting strategy
- Allows selection of relevant security events as early as possible to reduce storage and bandwidth cost
- Ensures an easy vehicle-wide configuration that can be adapted according to generated security events

ESCRYPT CycurIDS-ETH

- Monitors Ethernet traffic and detects potential attacks (anomalies)
- Enables in-vehicle intrusion detection for current and future Ethernet based E/E architectures
- Can run entirely on Ethernet switch as well as μC/μP

Exemplary detection features

- Covers specification, anomaly and signature based intrusion detection
- Allows to detect malicious attacks on application layer protocols like SOME/IP and DoIP, etc.
- Makes it possible to detect pattern of anomalies based on message frequency, sequence and vehicle state, etc.

ESCRYPT CycurIDS-R

- Acts as security event reporting for the vehicle
- Is a customized solution connecting the vehicle to the VSOC
- Ensures encapsulated provison of the IDS communication functionality
- Allows isolated deployments to fulfill security requirements
- Integrates seamlessly with the ESCRYPT CycurIDS components

Your benefits with ESCRYPT CycurIDS

- Timely detection of attacks in the field
- Field-proven ready-to-use solution
- Holistic offering that covers IDS sensors, security event management and reporting for in-vehicle intrusion detection
- In-vehicle IDS components are part of the ESCRYPT Intrusion Detection and Prevention Solution (IDPS), that includes also a VSOC as a managed security service
- Components are compliant to AUTOSAR, fulfill current automotive quality requirements, and are optimized for resource constrained ECUs
- A white-box, transparent security approach that enables you to realize and control your own cybersecurity policy
- Compliance to upcoming legal requirements, e.g. UN R155

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/CycurIDS

ETAS/COM2_AS/12/2022