escrypt
SECURITY. TRUST. SUCCESS.

CycurIDS

Intrusion detection for vehicles

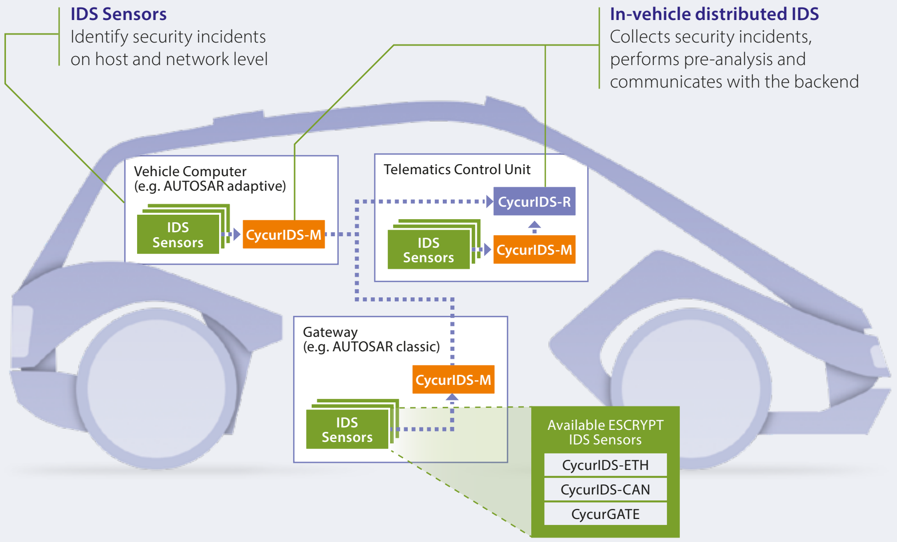
Continuous security monitoring with ESCRYPT's CycurIDS components

With the increasing connectivity of vehicles, new vectors for cyber-attacks 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?

ESCRYPT is offering a solution that is tailor-made for current and future vehicles and the future zonal architecture with its 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 CycurIDS-M and the IDS reporter CycurIDS-R complete the offer towards a distributed in-vehicle intrusion detection system.



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

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

ESCRYPT 2022/05

ESCRYPT's in-vehicle IDS components

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

CycurIDS-CAN

- Monitoring of forwarded CAN traffic and detection of potential attacks (anomalies)
- Heuristic and signature-based detection on ECU

Exemplary detection features

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

CycurIDS-ETH

- Monitoring of Ethernet traffic and detection of 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

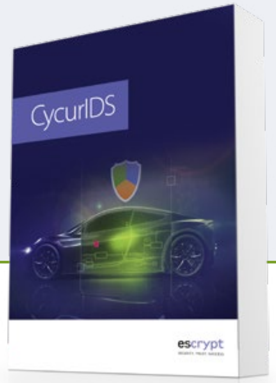
- CycurIDS-ETH covers specification, anomaly and signature based intrusion detection
- CycurIDS-ETH allows to detect malicious attacks on application layer protocols like SOME/IP and DoIP, etc.
- CycurIDS-ETH allows to detect pattern of anomalies based on message frequency, sequence and vehicle state, etc.

CycurIDS-M

- Acts as security event management for automotive ECUs
- Comes in two product variants:
  - for deeply embedded ECUs
  - for high performance ECUs
- 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
- Easy vehicle-wide configuration that can be adapted according to generated security events

CycurIDS-R

- Acts as security event reporting for the vehicle
- Customized solution connecting the vehicle to the VSOC
- Encapsulated provison of the IDS communication functionality
- Allows isolated deployments to fulfill security requirements
- Seamless integration with ESCRYPT's CycurIDS components



Your benefits

- ✓ 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 ESCRYPTs Intrusion Detection and Prevention Solution (IDPS), that includes also a VSOC as a managed security service
- ✓ CycurIDS components are compliant to AUTOSAR, fulfill current automotive quality requirements, and are optimized for resource constrained ECUs
- ✓ CycurIDS is a white-box, transparent security approach that enables you to realize and control your own cybersecurity policy
- ✓ CycurIDS enables compliance to upcoming legal requirements, e.g. UN R155

Any questions?

Please contact us any time.

info@escrypt.com
Phone: +49 234 43870-200
www.escrypt.com

escrypt
SECURITY. TRUST. SUCCESS.