escrypt
SECURITY. TRUST. SUCCESS.

Vehicle Security Operations Center

Overview

The threat landscape for connected vehicles is constantly evolving. Consequently, vehicle security levels degrade over time as security measurements become ineffective and attackers learn to circumvent them. This erosion of the security level concerns all building blocks of a connected vehicle fleet: the vehicles themselves as well as the corresponding vehicle backend services. As a result, maintaining the appropriate security level for a connected fleet is a holistic and ongoing activity. Detailed knowledge on the security status and potential attacks is paramount and required by upcoming regulations and standards. Two activities establish this knowledge and keep it up to date:

Threat detection: The timely detection and competent analysis of ongoing attacks is a key activity. Acquiring actionable information permits informed decisions and establishes the appropriate measures with which to restore the security level.

Threat intelligence: The acquisition and collection of knowledge on new emerging attack patterns.

ESCRYPT develops and operates a Vehicle Security Operations Center (V-SOC) for connected fleets that enables fleet operators to establish a life cycle of permanent monitoring and continuous security adjustments.

Customer challenges

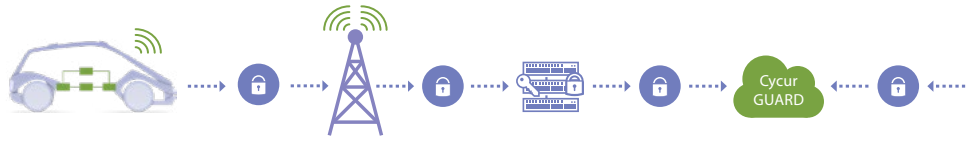
- Continuously evolving threat landscape for vehicles
- Need to constantly maintain the security level
- Scaling to vehicle fleets spread around the globe
- Fulfillment of upcoming worldwide regulations, such as UNECE WP.29 and ISO/SAE 21434

Our value proposition

- Holistic offering that covers in-vehicle intrusion detection (IDS) as well as vehicle backend and dedicated SOC services
- Continuous monitoring of attacks in the field
- Timely detection of attacks
- Security analytics by forensic experts
- Rollout of countermeasures via updates for the entire fleet

ESCRYPT 2020/07

escrypt
SECURITY. TRUST. SUCCESS.



Connected car with in-car IDS frontend | Mobile network provider | Vehicle backend | Hosting in cloud | Security analysis, security incident response, and threat intelligence

Vehicle IDS architecture

- Vehicle intrusion detection components in automotive quality (CycurIDS, CycurGATE)
- Understanding of automotive networks and attack vectors
- Integration components for distributed IDS
- IDS configuration services

Delivery end-to-end solution

- CycurGUARD – automotive IDS building blocks
- Contextualization of detection reports
- Integration with OEM backend systems
- Pseudonymization for data privacy

Security Operations Center services

- Security analytics service with automotive security forensic experts
- Threat detection & intelligence: 10 established Security Operations Center worldwide, 24/7 operation
- Covering vehicle fleets as well as Enterprise IT

Benefits

Holistic end-to-end data privacy solution

ESCRYPT delivers the Vehicle Security Operations Center as a managed security service tailored to the needs of the vehicle fleet. This includes integration of event sources from the vehicle fleets and vehicle backend systems.

Vehicle IDS architecture

ESCRYPT's Vehicle Security Operations Center follows an open architecture approach and integrates all sensors in the vehicle that provide information relevant for cybersecurity monitoring. This includes:

- Network-based intrusion detection for the CAN bus with ESCRYPT's CycurIDS
- Automotive Ethernet firewalls with ESCRYPT's CycurGATE
- Host-based intrusion detection for Linux, QNX, and Android ECUs
- Support for the complex distributed IDS architectures of modern E/E architectures

Security Operations Center services

ESCRYPT cooperates with NTT Security, a company that provides leading Security Operations Center services to numerous customers worldwide. This cooperation unites NTT's operational excellence and expertise in the area of Security Operations Center (SOC) as a service with ESCRYPT's automotive security know-how and provides customers with a highly professional and truly holistic solution that covers in-vehicle and backend security. The benefits:

- Worldwide availability: 10 SOCs with 24/7 operation
- Multi-regional rollout: one solution to cover all regions with 600+ security experts
- Battle-proven SOC tooling and infrastructure

Threat detection

- Advanced analytic capabilities, including machine learning and threat behavior modeling
- Automatic alert validation based on artificial intelligence to identify known attack patterns
- Manual alert validation by teams of security analysts to identify emerging threats
- Event-based threat hunting
- Actionable incident notification with recommendations
- Incident support until resolution is achieved
- Proactive response with network threat containment

Threat intelligence

- Comprehensive honeypot infrastructure
- NTT SOCs and backend cover 40% of worldwide web traffic
- 10+ threat intelligence sources

Data privacy and compliance

ESCRYPT's Vehicle Security Operations Center backend correlates security event information on the basis of pseudonyms instead of personal data such as the vehicle identification number (VIN). Pseudonymization is an integral part of the solution.

ESCRYPT is a pioneer and leading provider of IT security solutions in the automotive sector. By developing software applications and providing extensive consulting services, it has been protecting vehicles for over 15 years. Today, ESCRYPT solutions are an integral part of large-scale automotive production in many places and are used in millions of vehicles worldwide.