Secure Automotive Telematics Platforms
Challenges & Solutions

Security concerns remain the number one inhibitor to IoT monetization by operators. To leverage the advantages of the first movers, operators have to invest in dedicated security while telematics and vehicle security still mature.
The Security Challenge
Mobile operators have become the natural partner to car manufacturers in offering IoT-based telematics services. Operators monetize vehicle data as collected by telematics platforms in a variety of use cases, such as:
- Over-the-air (OTA) customer services (e.g. software updates)
- Usage-Based Insurance (UBI)
- Fleet Management / Asset tracking

Vehicles are connected via GSM devices placed inside the car. The devices communicate with datacenters controlled by the operator via the mobile GSM network. As more and more frightening hacks become publicly known (for example at security conferences like Blackhat), operators are increasingly concerned with the security of the vehicles and datacenters. These incidents demonstrate that vehicles can be hijacked and that threats to vehicles have escalated from the imaginary realm of possibility to reality. Tech savvy criminals have shown that hacking into both telematics platforms and vehicles seems to be easier than IoT-device manufacturers imagine. This intentional malicious behavior, however, is not the only cause for high-security risk. Accidental misuse is also a cause for concern. The operator of the telematics platform itself, such as an IT administrator, might accidentally send a command to all vehicles that are connected to the telematics service deactivating the GPS positioning and thus unintentionally supporting possible vehicle theft.

Telematics platforms – as all IoT platforms – are most likely proprietary, as standardization of a common IoT platform is still in progress and technical specifications are not yet ready for implementation. This makes it difficult for the operator to assess the quality of the implemented security functions. Security solutions offered by Rohde & Schwarz Cybersecurity can help operators to establish a second line of defense that is totally isolated from the vehicles and the telematics service deactivating the GPS positioning and thus unintentionally supporting possible vehicle theft.

Key Aspects
- Vehicles and telematics platforms become a fruitful target for cyber criminals for fun and profit
- The automotive industry can only slowly react to security problems through multi-year safety certification processes required to meet Federal Motor Vehicle Safety Standards (FMVSS)
- IoT platform security standardization is still in progress, but security is needed right now
- Telematics platform operators have to ensure vehicles are protected from platform compromises and accidental misuse
- A second line of defense is needed to enable security by design

Solutions
Security cannot be achieved just by choosing the right telematics platform. The platform operator has to take care of appropriate security mechanisms to prevent a potential telematics platform compromise from escalating and thereby imposing safety threats on vehicle owners. Rohde & Schwarz Cybersecurity offers a variety of solutions that can be tailored to the specific needs of any telematics platform. The solution portfolio offers:
- Turnkey solutions for platform & datacenter operators
- Software components for IoT device and platform vendors

Embedded Software DPI Engine
R&S®PACE 2 - Protocol and Application Classification Engine - is a software engine that is used by IoT network and security equipment vendors to enhance their products with state-of-the-art IP traffic analytics capabilities, such as:

1. Classification of:
- Protocols like HTTP, SSL, DNP3, AMQP, CoAP, SCADA or BitTorrent
- Applications like Facebook, Skype or Tor
- Application Attributes like a Skype video call or Skype text messaging

2. Extraction of:
- Transferred Commands like OTA software updates, security alerts
- Content & Downloads like URL’s and executable files
- Behavioral Metadata like bandwidth usage, traffic volume, connection duration, attachment types
- QoS / QoE indicators like jitter, throughput and packet loss

This enables manufacturers to implement state-of-the-art security functions in their IoT devices, such as:
- Gateways (both inside and outside the vehicle)
- Firewalls
- Platforms (e.g. for telematics)

Possible use cases are:
- Atomic policy enforcement down to the command level
- Network behavior anomaly detection (NBAD)
- Malware protection

R&S®PACE 2 uses deep packet inspection technology together with a comprehensive toolbox of methodologies, such as:
- Atomic pattern matching
- Heuristics and
- Behavioral analysis

This allows for reliable detection even of encrypted and actively hiding applications and protocols with a low rate of false negatives and virtually no false positives.
Rohde & Schwarz
Secure Automotive Telematics Platforms Challenges & Solutions

**R&S®PACE 2 - Pluggable Semantic Awareness for IoT Security Vendors**

**Specialized Line Firewalls**
*The turnkey solution for platform operator requirements*

The Rohde & Schwarz Specialized Line Firewalls revolutionize the concept of next-generation firewalls by using our unique full-validation whitelisting to ensure maximum network security. Its general operation can be compared to X-ray scanners used at airports. Not a single unknown item is allowed through the security checkpoint, instead each and every item has to be positively identified. Specialized Line uses a novel technology to achieve the same for a company’s network.

**Semantic awareness assures security by design**

Every single network transaction is analyzed down to the application and content level. Only transmissions that are fully understood and validated are allowed to pass through. Everything else is blocked from entering or leaving the network, thereby not only securing the network from outside attacks, but also providing highly effective data loss prevention.

This enables telematics platform operators to define policies based on communication primitives such as the types of OTA functions (e.g. software updates, GPS position tracking) in order to define in an atomic way which kind of actions should be prevented by design.

The Specialized Line firewalls can, for example, enforce that no OTA software updates are sent to any connected vehicle (even if the telematics platform is compromised and criminals have full access to the telematics platform).

Our in-house deep packet inspection (DPI) technology enables us to implement semantic awareness in our firewalls even for proprietary protocols as used frequently in telematics platforms. This in turn allows the platform operator to implement policies based on a full understanding of the transferred communication.

**Key Benefits**

- Available for a variety of platforms – from Android mobiles to cloud-based IoT platforms
- Atomic traffic visibility gives a competitive edge to IoT network equipment vendors
- Market-leading low memory footprint makes R&S®PACE 2 a perfect fit for IoT gateways and firewalls
- 100 % German engineered
- R&S®PACE 2 adds semantic awareness for IoT communication protocols to IoT gateways and firewalls
**Rohde & Schwarz Cybersecurity**

Rohde & Schwarz Cybersecurity is an IT security company that protects companies and public institutions around the world against espionage and cyberattacks. With around 400 employees, the company develops and produces technologically leading solutions for information and network security. Development of the trusted IT solutions is based on the security-by-design approach for proactively preventing cyberattacks.

**Rohde & Schwarz**

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, radiomonitoring and radiolocation. Founded more than 80 years ago, the independent company which is headquartered in Munich, Germany, has an extensive sales and service network with locations in more than 70 countries.

---

**Rohde & Schwarz Cybersecurity GmbH**
Muehldorferstraße 15 | 81671 Munich, Germany
Info: +49 (0) 30 65884-223
Email: cybersecurity@rohde-schwarz.com
www.cybersecurity.rohde-schwarz.com

**Rohde & Schwarz GmbH & Co. KG**
www.rohde-schwarz.com

---