Transportation Systems Security. Modern Threats

Transportation is expanding from its origin – transport – to encompass more than just moving vehicles. Transportation can feature systems with feedback for power generation (smart cities), providers of commonly used location services (GPS/GLONASS), smartphone managed vehicles (automotive), value added entertainment platforms (IFE, IFPL), connected cars, and, in the not too distant future, it will also encompass driverless cars.

Kaspersky Lab and AVL Software and Functions offer a set of proactive threat intelligence services for the automotive industry that is going to enhance security operations and take a proactive approach against advanced threats:
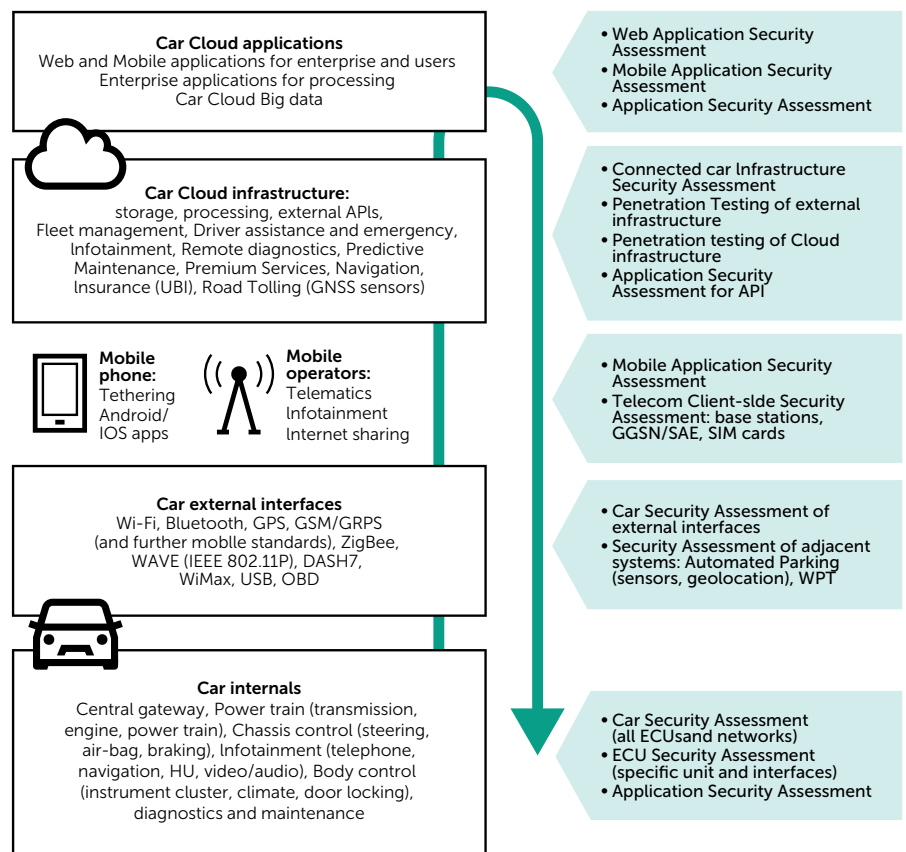
- **Car Security Assessment and ECU Security Assessment**
  In-depth security analysis of vehicle internals (ECU, TCU, TPMS, RKE, PATS, etc.) and corresponding internal and external interfaces (wired and wireless).

- **Application Security Assessment**
  Detailed security analysis of applications, including static and dynamic analysis of the application's source code and architecture. Kaspersky Lab experts are able to discover any vulnerabilities that might enable an intruder to bypass authentication and authorization procedures, raise privileges, or bypass security controls or fraud detection.

- **Connected Cars Security Assessment**
  A complex approach for the security analysis of cloud-based and datacenter systems with telematics (remote control parking, real-time traffic updates, tele services, online entertainment, smartphone integration, etc.).

- **Penetration Testing**
  Analysis of network and system infrastructure from the point of view of external and internal intruders. Our experts will attempt to bypass security controls on behalf of various types of intruders in order to obtain maximum possible privileges in important systems.

- **Telecom Client-side Security Assessment**
  Advanced security analysis of vehicle external communications (mobile networks from 2G to 4G) with Connected Cars Service Platforms, and also vehicle-to-vehicle and vehicle-to-infrastructure systems.
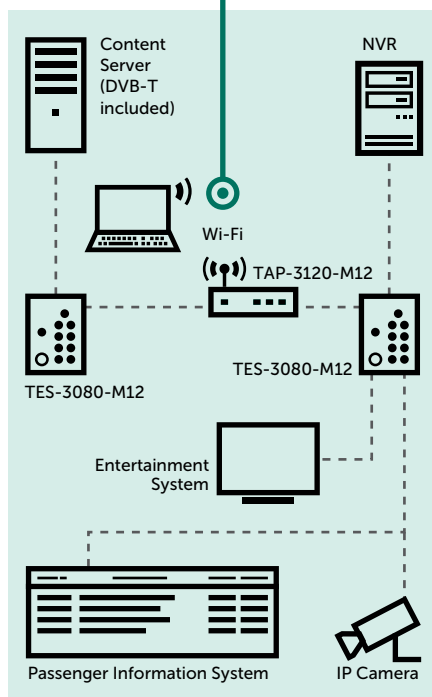
Automotive Industry Security

Vehicles are becoming cluttered with technologies inside and outside of the car. Introduction of more ECUs inside the vehicle or external services in the well known security domain of public networks or clouds increases the threat model (and attackers possibilities). Automotive Industry security is on the verge right now with newspaper headlines covering vulnerabilities and attacks, while fundamental architecture flaws torturing automotive vendors.

Threat Intelligence Services for Automotive Industry

Kaspersky Lab and AVL Software and Functions offer a set of proactive Threat Intelligence services for the Automotive Industry that is going to enhance security operations and take a proactive approach against advanced threats:

Car Cloud applications
Web and Mobile applications for enterprise and users
Enterprise applications for processing
Car Cloud Big data

- Web Application Security Assessment
- Mobile Application Security Assessment
- Application Security Assessment

Car Cloud infrastructure:
storage, processing, external APIs, Fleet management, Driver assistance and emergency, Infotainment, Remote diagnostics, Predictive Maintenance, Premium Services, Navigation, Insurance (UBI), Road Tolling (GNSS sensors)

- Connected car Infrastructure Security Assessment
- Penetration Testing of external infrastructure
- Penetration testing of Cloud infrastructure
- Application Security Assessment for API

Mobile phone: Tethering Android/IOS apps

Mobile operators: Telematics Infotainment Internet sharing

- Mobile Application Security Assessment
- Telecom Client-slde Security Assessment: base stations, GGSN/SAE, SIM cards

Car external interfaces
Wi-Fi, Bluetooth, GPS, GSM/GRPS (and further moblle standards), ZigBee, WAVE (IEEE 802.11P), DASH7, WiMax, USB, OBD

- Car Security Assessment of external interfaces
- Security Assessment of adjacent systems: Automated Parking (sensors, geolocation), WPT

Car internals
Central gateway, Power train (transmission, engine, power train), Chassis control (steering, air-bag, braking), Infotainment (telephone, navigation, HU, video/audio), Body control (instrument cluster, climate, door locking), diagnostics and maintenance

- Car Security Assessment (all ECUsand networks)
- ECU Security Assessment (specific unit and interfaces)
- Application Security Assessment

Railway Systems Security Assessment

One of the most crucial areas of public transportation are Railway Systems. The safety of rapid transit railway transportation is closely connected to the security of train communication networks, wireless communications, signalling systems, station automation systems and many more. Kaspersky Lab role is to provide its information security expertise in building security processes with mechanisms to understand and manage risks, and to detect and prevent security incidents.

Security Assessment of Railways Systems enriches the railway operators and manufacturers with knowledge about modern threats, best practices and remediation approaches tailored specifically for their environment. We have a vast experience in analysis of any Smart Transportation System from railway locomotive powertrain control and vehicle ECUs to Fleet Management Systems and Car Clouds. Kaspersky Lab services are focused on providing prioritised and actionable recommendations based on threat model developed covering safety of transportation.

Kaspersky Transportation Security Services Customers

Our list of customers includes, but is not limited to:

- Ferrari S.p.A.
- LKQ
- Carglass
- Hankook Tire
- Abu Dhabi Racing
- AGC Glass Germany
- TÜV Rheinland

Content Server (DVB-T included)

NVR

Wi-Fi

TAP-3120-M12

TES-3080-M12

TES-3080-M12

Entertainment System

Passenger Information System

IP Camera

KASPERSKY lab

Kaspersky Transportation System Security
39A/3 Leningradskoe Shosse, Moscow,
1252121, Russian Federation
kaspersky.com
kaspersky.com/enterprise-security/cybersecurity-services
transportation.security@kaspersky.com
connectedcars@kaspersky.com
Phone: +7-495-797-8700
Fax: +7-495-797-8709; +7-495-956-7000

AVL

AVL Software and Functions GmbH
Im Gewerbepark B29
D-93059 Regensburg
www.avl.com
info.rgb@avl.com
Phone: + 49 (0)941 630 890
Fax: + 49 (0)941 630 89 111