Kaspersky
Automotive
Security
Services

Driving Automotive Cybersecurity

Transportation
System Security

kaspersky

Learn more on
kaspersky.com

Kaspersky Automotive Security Services

Role of security tests in the automotive industry

Threat landscape

Modern vehicles are complex computerized systems with a variety of features to assist the driver, enhance safety and provide entertainment. The rapidly increasing number of user interfaces and cloud connections is enlarging the attack surface of vehicles, while any sort of connection – from a cellular modem on a telematics unit to infotainment – can be targeted to compromise a vehicle or its infrastructure. Computer-based attacks also impact transport safety as has been demonstrated by publicly available security research. The growing body of research into security issues[1] in the automotive industry shows we are facing the threat of numerous data breaches[2] from auto insurance value-added services, fleet management, etc.

One of the most challenging problems in the automotive industry is supply-chain security. Most vehicle components are developed by a variety of vendors with no uniform security requirements or acceptance testing. While security regulations are evolving, control of security compliance for each vehicle ECU remains a time-consuming process that requires considerable expertise. It becomes even more expensive when a new untested solution appears on the market, as security issues in the architecture can force significant changes. The process of addressing these issues starts with an understanding of the current security posture and vulnerabilities in ECUs, the vehicle network and vehicle backend infrastructure. This knowledge is used as a baseline for later investments to harden security aligned with industry practices.

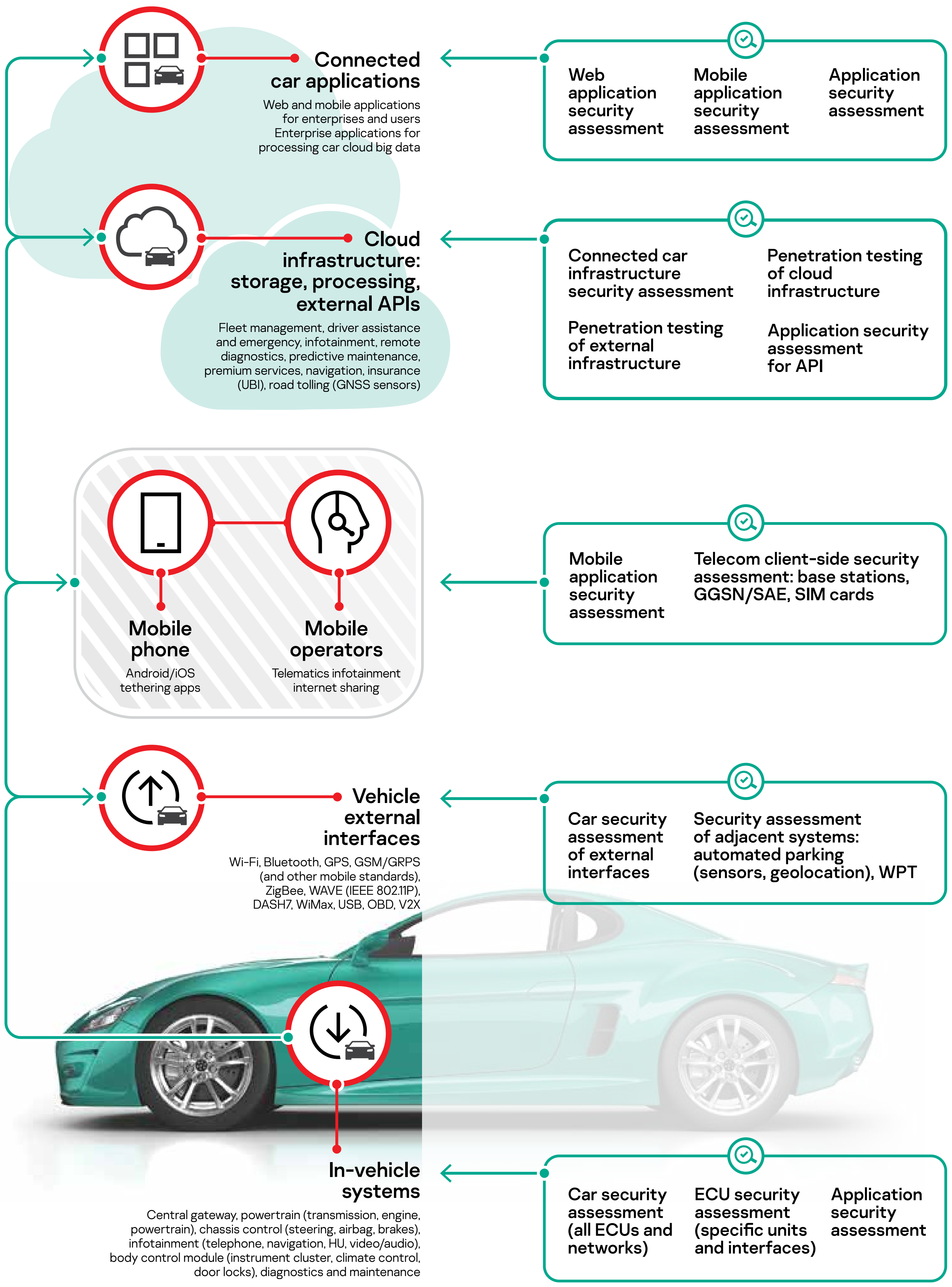
Managing risks and threats

Kaspersky offers a set of services to identify threats for all automotive ecosystem components as well as recommendations on how to enhance security posture, including:

- In-depth security analysis of vehicle internals (ECU, TCU, TPMS, RKE, PATS, etc.) and corresponding internal and external interfaces (wired and wireless)
- Detailed security analysis of applications, including static and dynamic analysis of application source code and architecture to assess their ability to bypass authentication and authorization procedures, raise privileges, or bypass security controls or fraud detection
- Complex security analysis of cloud-based and datacenter systems with telematics (remote control parking, real-time traffic updates, tele services, online entertainment, smartphone integration, etc.)
- Analysis of network and system infrastructure from the point of view of external and internal intruders
- Advanced security analysis of a vehicle's external communications (mobile networks from 2G to 5G) with car clouds, vehicle-to-vehicle and vehicle-to-infrastructure systems

[1] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[2] https://www.forbes.com/sites/daveywinder/2019/09/15/bought-a-car-recently-198m-car-buyer-records-exposed-in-massive-data-leak/#110f65ce7391

Which parts of the ecosystem need testing



Connected car applications

Web and mobile applications for enterprises and users
Enterprise applications for processing car cloud big data

- Web application security assessment
- Mobile application security assessment
- Application security assessment

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 cloud infrastructure
- Penetration testing of external infrastructure
- Application security assessment for API

Mobile phone

Android/iOS tethering apps

Mobile operators

Telematics infotainment internet sharing

- Mobile application security assessment
- Telecom client-side security assessment: base stations, GGSN/SAE, SIM cards

Vehicle external interfaces

Wi-Fi, Bluetooth, GPS, GSM/GRPS (and other mobile standards), ZigBee, WAVE (IEEE 802.11P), DASH7, WiMax, USB, OBD, V2X

- Car security assessment of external interfaces
- Security assessment of adjacent systems: automated parking (sensors, geolocation), WPT

In-vehicle systems

Central gateway, powertrain (transmission, engine, powertrain), chassis control (steering, airbag, brakes), infotainment (telephone, navigation, HU, video/audio), body control module (instrument cluster, climate control, door locks), diagnostics and maintenance

- Car security assessment (all ECUs and networks)
- ECU security assessment (specific units and interfaces)
- Application security assessment

Description of security tests

Security assessment for ECUs

The assessment approach will differ depending on customer needs and may include analysis of various types of ECUs: central gateways, telematic control units (TCU), infotainment systems, remote keyless entry (RKE) systems, tire pressure monitoring systems (TPMS), passive anti-theft systems (PATS). These are standalone components with their respective input/output interfaces.

Assessments include analysis of a vehicle's external and internal communication buses and protocols, including automotive-specific and general-use technologies: CAN, LIN, MOST, FlexRay, Ethernet, UART, USB, etc.

The following types of works can be implemented within this service (depending on the type of system and level of access provided):

- Threat modelling according to business logic and use cases
- Manual and automated identification of vulnerabilities including research aimed to find vulnerabilities
- Analysis of firmware and application source code using static, dynamic and interactive approaches
- Security assessment of underlying communication protocols (CAN, FlexRay, MOST, LIN) and existing security controls
- Security assessment of radio channels, including mobile and various wireless networks (2G/3G/4G, Wi-Fi, Bluetooth, etc.)
- Configuration analysis for operating systems and application components
- Evaluation of implemented security measures
- Exploitation of revealed vulnerabilities and attack demonstration
- Technical report

The technical report contains detailed information on findings, recommendations, as well as conclusions on the likelihood of various threat scenarios affecting processes. The services include an in-depth hardware security assessment to discover potential vulnerabilities in circuit board designs and the implementation and usage of chips in order to prevent unauthorized read or write access to data (for example, cryptographic keys, system configurations and applications).

Penetration testing

Penetration testing is an attempt to bypass security controls using the same tools and techniques as intruders would to obtain maximum possible privileges in important systems. This service provides information on vulnerabilities present in your corporate resources and the potential consequences if exploited. It allows you to assess the effectiveness of existing security measures, and plan work to fix detected flaws and improve security.

- External penetration testing – security assessment of an attack from the internet without any preliminary knowledge of your system
- Internal penetration testing – security assessment of an attack emulating an intruder who has penetrated network defenses, for instance, a visitor with physical access to your office, or a contractor with limited access to certain systems
- Social engineering testing – assessment of your personnel's security awareness by emulating social engineering attacks such as phishing, pseudo-malicious links in emails, suspicious attachments, etc.
- Wireless network security assessment – our experts will visit your site and analyze Wi-Fi security controls

Why Kaspersky?

Kaspersky is a global cybersecurity company founded in 1997. With its deep threat intelligence and cybersecurity expertise gained over 22 years, Kaspersky is constantly developing security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. Protecting over 270,000 corporate clients worldwide, Kaspersky is considered the most trusted cybersecurity brand for business.[3]

With Kaspersky as a cybersecurity partner, automotive enterprises gain visibility into the entire connected vehicle ecosystem and an understanding of how to adjust their cybersecurity strategy. By ensuring a secure drive for clients, we're building a safer tomorrow.

Kaspersky – driving automotive cybersecurity!

[3] According to the results of 2018 report The Boundaries of Trust: Privacy and Protection in Cyberspace

Kaspersky Automotive Security Services: ktss@kaspersky.com
Enterprise Cybersecurity: www.kaspersky.com/enterprise
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

www.kaspersky.com

kaspersky

BRING ON
THE FUTURE