Securing the future of mobility

www.kaspersky.com
#truecybersecurity

KASPERSKY lab

AVL

Securing the future of mobility

The need for built-in security

Modern cars are not just electromechanical vehicles anymore. With each generation, they become more and more connected, incorporating new progressive intelligent technologies, making vehicles more efficient, comfortable and safe. At the same time, new technologies like remote diagnostics, telematics and infotainment bring new challenges to the industry, turning connected vehicles into cyberattack targets. The growing risk of a vehicle being infiltrated, or having its safety, privacy and financial features violated, requires methodical, organizational and technical measures to ensure protection.

This raises the demand for secure solutions, which should be capable of

- Making the vehicle resilient to remote attacks
- Detecting emerging attacks and reacting safely
- Assuring the connected vehicle is secure

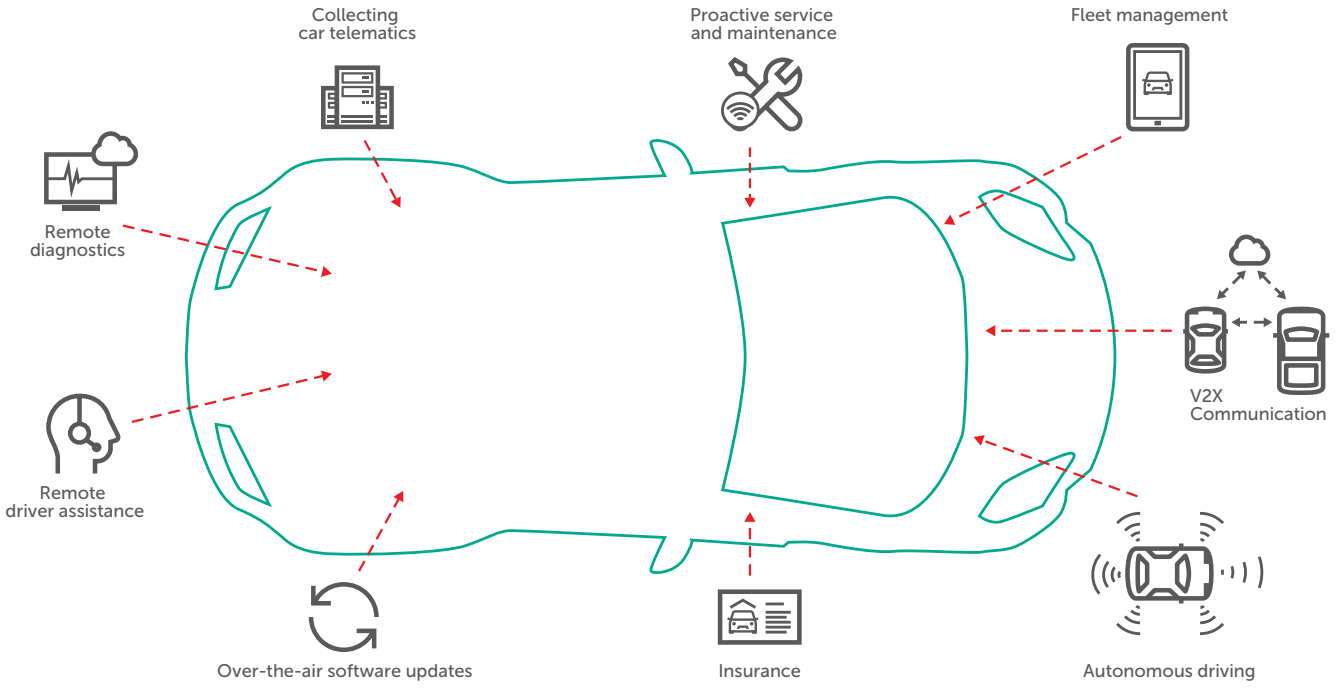
Strategic partnership

To meet the cybersecurity challenges of next generation automotive system development, Kaspersky Lab and AVL Software and Functions GmbH have developed a reliable and flexible software platform that allows car manufacturers to develop and implement a Secure Communication Unit (SCU) into their cars, using hardware and additional software components that are aligned with their manufacturing plans. The platform exploits KasperskyOS, that is designed for, and meets the requirements of, embedded devices used in car manufacturing – connected cars in particular.

Connected cars

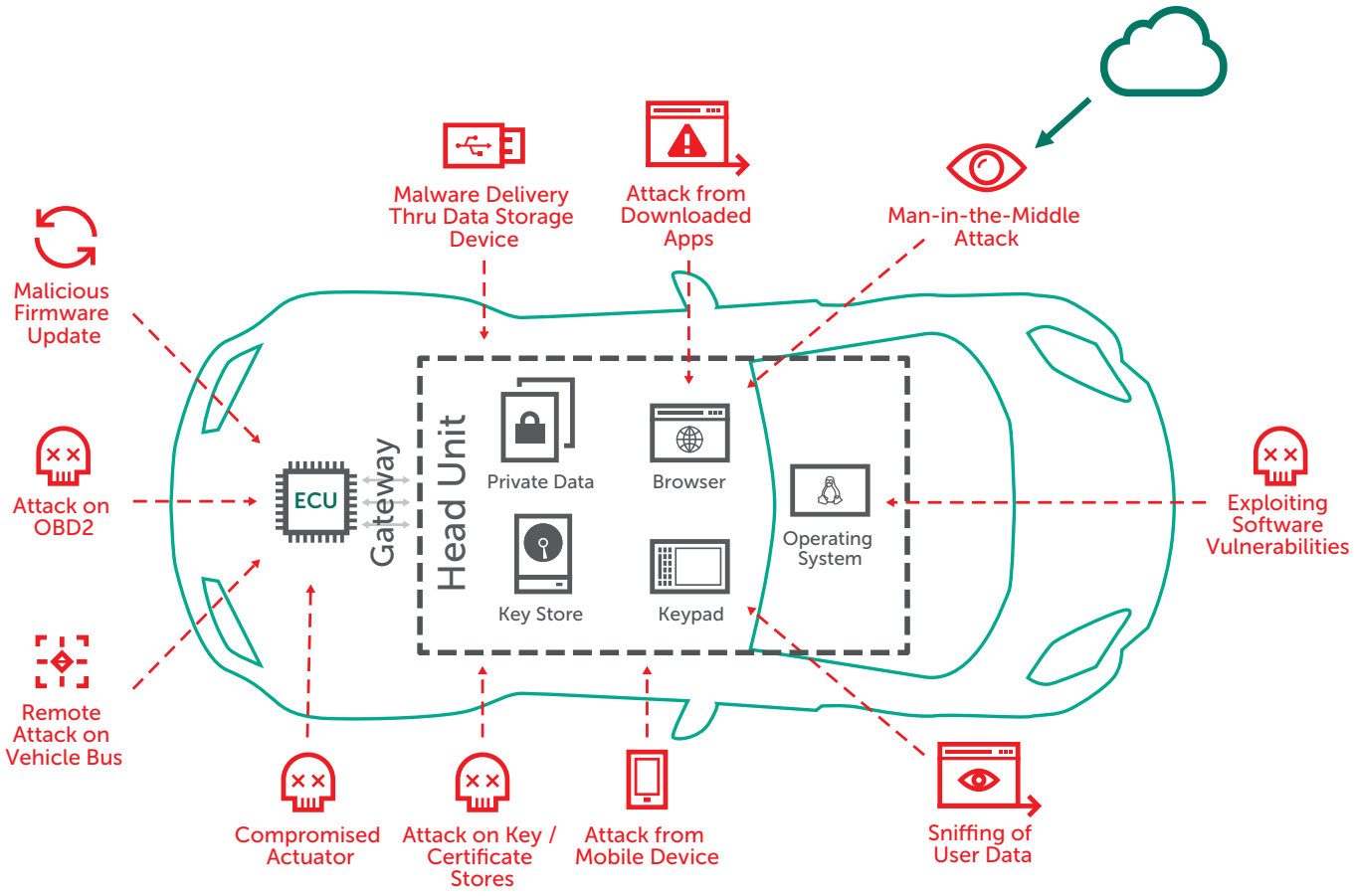
Connected cars with Internet access, sensors, and communication modules can interact with other vehicles and its environment, bringing benefits to many – including drivers, owners, OEMs, workshops, insurance companies, car rental / car sharing / taxis, and logistics companies.

Connected car benefits



Along with obvious benefits, there are plenty of cybersecurity threats, including sensitive data theft, unauthorized access to the car, vehicle software modification, telematics data spoofing, and even accident provocation.

Connected car threats



One of the main sources of these threats are vulnerabilities in the software, including bugs, backdoors and architectural issues.

The connected car functionality is complex and sophisticated, and currently it is impossible to ensure that vehicle software is free from vulnerabilities, especially when it runs third party applications.

Secure platform for connected cars

The unique nature of our solutions lies in the fact that we protect platforms through a secure operating system, and a development approach based on secure methodology and unique patented technologies. This makes the entire solution trusted and reliable.

That is what KasperskyOS was designed for – make complex solutions secure.

We follow a holistic approach to ensure the security of vehicles

- Threat-modelling and risk-analysis
- Methodological approach that allows us to create secure-by-design solutions
- Microkernel secure operating system - KasperskyOS
- Natively implemented Separation Kernel Architecture
- Patented security policy enforcement engine
- Trusted channel framework with state of the art encryption functionality
- Implementation of intrusion detection and prevention systems (IDPS)
- Security evidence by software assurance according to enhanced automotive V-cycle

The more complex system and code you have, the more chances to miss bugs.

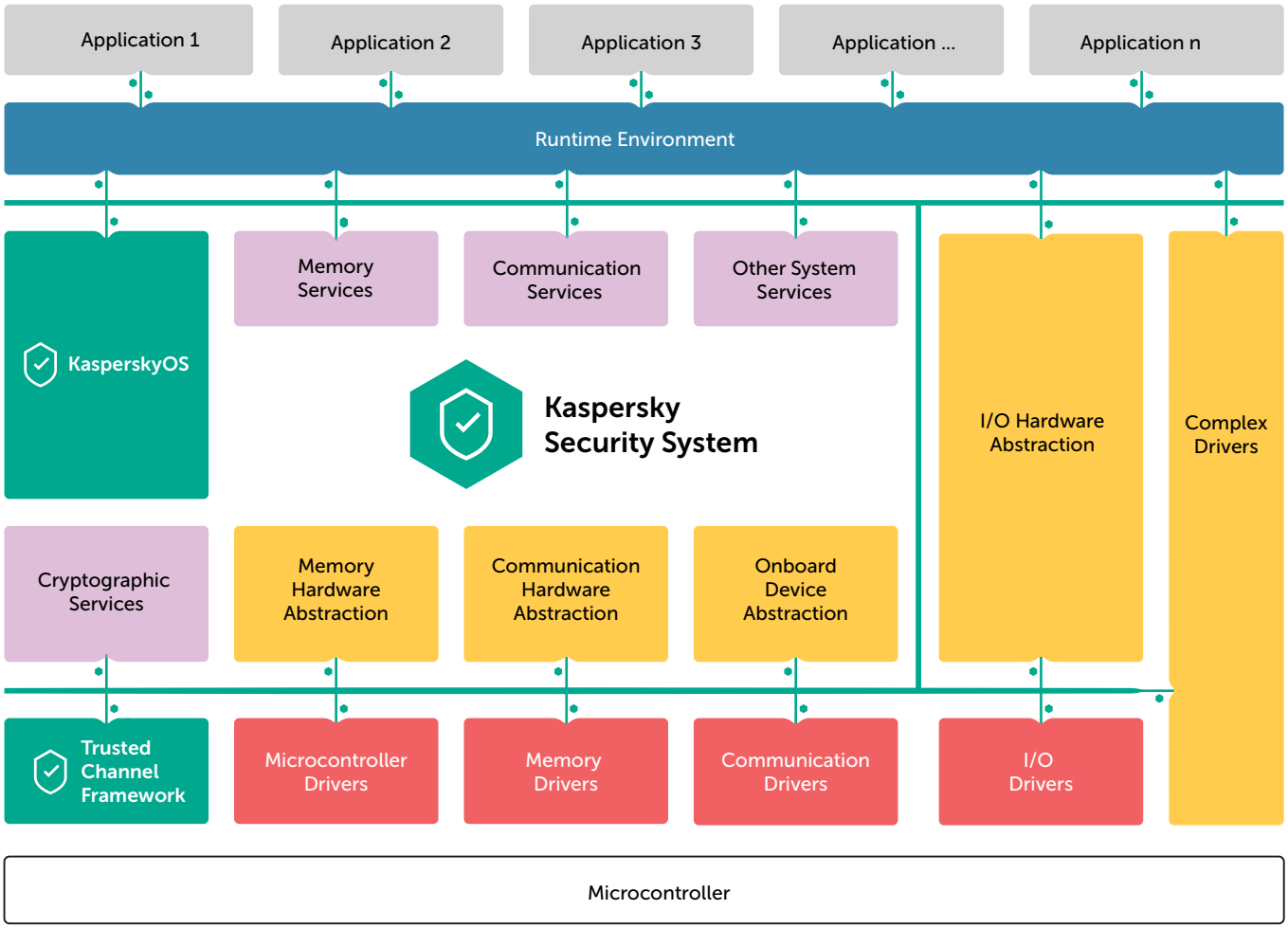
Complexity and security

Complexity and security are conflicting features. The more complex system and code you have, the more chances to miss bugs even after very thorough testing procedures.

That is what KasperskyOS was designed for – make complex solutions secure.

Two main principles are necessary to form a trusted platform – even when the components themselves are not trusted.

1. Strong separation – preventing unwanted interference with components
2. Security Policy Enforcement – allowing valid communications between different components.



Only a minimum number of components are considered trust-worthy

- Microkernel operating system (KasperskyOS) which contains only basic functions that are easy to test and verify
- Security policy engine (Kaspersky Security System) based on formal models like Domain Type Enforcement, Object Capability, Role Based Access, various dialects of Temporal Logics and others
- Trusted channel framework that includes a set of crypto algorithms as well as low level protection services, based upon hardware capabilities

These mechanisms, along with AUTOSAR ,and AUTOSAR adaptive platform aligned features, implement secure onboard communications and protect various E/E architectures including car network topologies with domain controllers or a central gateway.

This enables the implementation of cutting-edge features and services for equipped vehicles

- Over-the-air security updates
- Secure IVN communications
- Remote diagnostics
- Proactive service and maintenance
- Fleet management
- Autonomous driving
- Remote driver assistance
- Driver health, wellness and wellbeing digitization

The added value

Kaspersky Lab and AVL Software and Functions GmbH work together to develop advanced, embedded security technologies through a collaborative and comprehensive partnership approach.

- Providing 20 years of experience in automotive safety as well as in industrial and IT security
- Supporting our customers with a holistic approach from the first asset definition to system maintenance during the product life
- Development of tailored on- and off-board security solutions

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company celebrating its 20 year anniversary in 2017. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

About AVL

AVL is the world's largest independent company for the development, simulation and testing technology of powertrains (hybrid, combustion engines, transmission, electric drive, batteries and software) for passenger cars, trucks and large engines. AVL has more than 8,600 employees all over the world. In 2016, sales revenues reached EUR 1.4 billion.

KASPERSKY lab

Kaspersky Transportation System Security
39A/3 Leningradskoe Shosse, Moscow,
1252121, Russian Federation
www.kaspersky.com
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