CONNECTED CAR EVOLUTION

Non connected car
PAST

Connected devices, GPS, Internet
YESTERDAY

Cloud Services, Remote assistance
TODAY

Autonomous car, complete remote control
FUTURE
CONNECTED CAR EVOLUTION. Benefits

- Non connected car
  - Past

- Connected devices, GPS, Internet
  - Yesterday

- Cloud Services, Remote assistance
  - Today

- Autonomous car, complete remote control
  - Future
CONNECTED CAR EVOLUTION. Benefits and **Cyber Risks**

- **PAST**: Non-connected car
- **YESTERDAY**: Connected devices, GPS, Internet
- **TODAY**: Cloud Services, Remote assistance
- **FUTURE**: Autonomous car, complete remote control
Mobile apps and stealing a connected car

By Mikhail Kuzin, Victor Chebyshev on February 16, 2017. 10:27 pm

The concept of a connected car, or a car equipped with Internet access, has been gaining popularity for the last several years. The case in point is not only multimedia systems (music, maps, and films are available on-board in modern luxury cars) but also car key systems in both literal and figurative senses. By using proprietary mobile apps, it is possible to get the GPS coordinates of a car, trace its route, open its doors, start its engine, and turn on its auxiliary devices. On the one hand, these are absolutely useful features used by millions of people, but on the other hand, if a car thief were to gain access to the mobile device that belongs to a victim that has the app installed, then would car theft not become a mere trifle?

In pursuing the answer to this question, we decided to figure out what an evildoer can do and how car owners can avoid possible predicaments related to this issue.
CONNECTED CAR MAIN SECURITY OBJECTIVES

- Protect Each Module
  All ECU, Sensors, BCU

- Protect Communications
  Physical and remote connections

- Protect Cloud Services
  OTA updates and Management

- Persist Advanced Threats
  Analytics and Analysis
CONNECTED CAR MAIN INTERNAL VULNERABLE POINTS
POTENTIAL THREAT VECTORS

- Attack from Mobile Device
- Attack on Key / Certificate Stores
- Malware Delivery Thru Data Storage Device
- Operating System
- Remote Attack on Vehicle Bus
- Exploiting Software Vulnerabilities
- Malicious Firmware Update
- Attack from Downloaded Apps
- Man-in-the-Middle Attack
- Compromised Actuator
- Sniffing of User Data
## CONNECTED CAR SECURITY LAYERS

<table>
<thead>
<tr>
<th>Layers</th>
<th>Threat vectors</th>
</tr>
</thead>
</table>
| Car Cloud Services      | • Man in-The-Middle-Attack  
                          • Attack From Downloaded Apps                                              |
| NW Access               | • Sniffing of User Data  
                          • Attack From Downloaded Apps  
                          • Exploiting Software Vulnerabilities                                       |
| Car Gateway             | • Attack from Apps in Mobile Device  
                          • Exploiting SW Vulnerabilities  
                          • Malicious Firmware Update  
                          • Malware Delivery Thru Data Storage Devices                               |
| Car Network             | • Compromised Engine Actuator  
                          • Attack on Vehicle Bus                                                     |
| Car ECU, IVI, OBD2      | • Attack on Key,  
                          • Malicious Firmware Update  
                          • Attack on Vehicle Bus                                                    |
CONNECTED CAR SAFETY THRU SECURITY

Cloud Services
- Security for Data Centers
- Kaspersky Security Network
- Fraud Prevention
- DDoS Protection
- Anti Targeted Attack

Mobile
- Mobile Security SDK
- Mobile Device Management
- Mobile App Management
- Mobile Security

Internet

In Car Security
- KasperskyOS
- Kaspersky Secure Hypervisor
- Kaspersky Security System
- Security Expertise

Vehicle-to-Vehicle

Vehicle-to-Infrastructure
HOW WE WORK

Threat model
- Define security objectives
- Create detailed description of scenarios, with results of misuse/abuse cases identification
- Threat modelling
- Define high-level security requirements
- Create a security-focused system architectural concept
- Refine threat model and security requirements

Architecture
- Specify system requirements for the security features
- Create test plans and test cases for the security features
- Design architecture
- Create low-level design

Development & testing
- Development and testing
- Residual risks assessment
- Integration with HW and testing
- Creation of instrumentation
- Final testing and residual risk assessment
- Penetration testing (separate dedicated team)
Security vs Safety
Security for Safety
KASPERSKY LAB
AUTOMOTIVE SECURITY TECHNOLOGIES

Andrey Nikishin @andreynikishin
Special Projects Director, Future Technologies