The Connected Vehicle - Challenges and Opportunities

Christoph G. Nolte
DEKRA Automotive
The connected vehicle ecosystem
Fragmentation in standards

- LTE-V
- DSRC
- WAVE
- 802.11p
- ITS-G5
- 5G
- ITS Connect
Data Usage
The connected vehicle – data usage

- Turn-by-turn navigation
- Web browsing
- VoIP calling
- Music streaming (SD)
- Video streaming (4K)
- Video streaming (HD)
- Video streaming (SD)
- Connected car

Data usage (MB/h)
Mobile network evolution

Speed and latency

- Throughput (Mbps)
- Latency (ms)

LTE
LTE-Adv-Pro
5G

MEC (Mobile Edge Computing)
Cybersecurity
Threats in the connected vehicle

Malicious firmware updates
- Through USB, CD, SD card
- Through OBD port
- Via OTA process

Attack to the vehicle internal bus (injection/capture)

Attack from downloaded applications

Attack from mobile device applications

Man-in-the-middle attack

Compromised actuators controlled by malicious software

Sniffing of user data and passwords through screens and keypads, transmitted to outside world

Malware delivered through encoded music

Open source software vulnerabilities

Any part of the electronic system can be an attack point
Threats in the connected vehicle ecosystem

- Car Manufacturers
- Auto Dealers
- Value added Services
- Application Servers
- DDBB
- Unencrypted Storage
- Insecure Services
- Insecure Configurations
- Unencrypted Data
- Malware
- Fraud
- Insecure Communications
- Third party Servers
- Cloud
- Insecure Services
- Laws
- Third parties
- Traffic infrastructure
- Pedestrian
- Connected vehicle
- Insecure Communications
- Insecure Protocols
- Unsecured setup
- Information Data leak
- Additional services
- Insecure Data leak
- Third party data leak information
- Vulnerabilities in Applications
- Insecure Services
- Laws
- Regulation
- Unencrypted data
- Information Data leak
- Fraud
- Insecure Services
- Unencrypted Storage
- Vulnerabilities in Services
- Insecure Configurations
The connected vehicle – challenges and opportunities

Standards

Data usage

Cybersecurity