AGENDA.

Why are automated driving vehicles so interesting for adversaries compared to vehicles without automation?

What are the impacts of attacks? Why do we need extra effort in developing countermeasures?

Are there helpful best practices for developing countermeasures? How to apply them now?
NEW MOTIVATION AND ENABLERS FOR ADVERSARIES.

Remote Car Control

Connectivity

Sensors

Integration platforms
INCREASED USAGE OF SENSORS AND EXTERNAL INFORMATION AS ATTACK VECTOR.
HIGHER IMPACTS IN CASE OF INCIDENTS.
Challenges of Automotive Cybersecurity for Automated Driving | M. Gruber | Vector Automotive Cyber Security Symposium 2019

BEST PRACTICES.
SECURITY-BY-DESIGN. ALLOY WITH SAFETY.

Security Engineering

Security risk analysis
Security architecture
Secure implementation

Pen-test & Release approval
Security review & testing
Security monitoring & Incident management

Safety
Life and limb of customers, public sphere and road users are protected against manipulation.
BEST PRACTICES.
DEFENSE-IN-DEPTH. LAYERED ARCHITECTURE.

Vehicle

- Protection layer vehicle interfaces
- Protection layer vehicle network
- Protection layer ECU level

- Car2Backend Connectivity
- BMW IT Backend

- Connected Mobility Backend
- ADAS Backend
- IT-Backend
- Extended Vehicle ISO 20078

- Neutral Server
- Mobile Apps
- External partners

Vehicle interfaces:
- Various interfaces
- OBDII for Repair & Maintenance
- Charging, Smart Home
- Driver assistance & diagonal — longitudinal dynamics
- Infotainment & Body / Comfort

BMW IT Backend interfaces:
- Mobile Apps
- Neutral Server
- External partners
BEST PRACTICES.
PLATFORM AND SOFTWARE SECURITY.
BEST PRACTICES. ADAPTION OF IT-SECURITY MEASURES. SECURE UPDATES.

Security monitoring:
Active monitoring of worldwide threats and all segments of the internet. Participation in security research networks, Security- and hacking-conferences, and information exchange in ISACs and CERTs.

Incident management:
Established Incident Response Team covers analysis, implementation, test, release and rollout of technical measures.

Security Updates:
Validated software updates are applied to the vehicle in multiple ways: Existing update path via dealership & expansion of OTA updates to the entire vehicle architecture.
SUMMARY.

Why are automated driving vehicles so interesting for adversaries compared to vehicles without automation?
Full vehicle control as main goal, connectivity and sensors as attack vectors, concentrate attack on complex integration platforms.

What are the impacts of attacks? Why do we need extra effort in developing countermeasures?
Driver out of loop, higher safety impacts, Protect safety! Attacks can be expanded to fleets.

Are there helpful best practices for developing countermeasures?
How to apply them now?
SDL to ensure security by design, defense-in-depth approach, hardware and software security incl. secure coding, secure updates.
THANK YOU FOR YOUR ATTENTION.
QUESTIONS?

Miriam Gruber
Automated Driving, Driver Assistance
Automotive Cybersecurity
miriam.gruber@bmw.de