Network Orchestration for Automotive Communication Lockdown

Dionis Teshler
CTO & Co-Founder
GuardKnox
Hottest new features in cars of 2018

- Noise Level Adjustment
- Semi-Autonomous Driving
- Finding Parking
- Advanced Safety
- Smarter Smart Keys
- Augmented Reality
- Rich Video/Audio Streaming
- Feature Rich Bluetooth
- In-Vehicle Wellness
- Advanced Rear-seat Infotainment

May 13-16, 2019 Santa Clara Convention Center, CA • tmt.knect365.com/iot-world • #IOTWORLD
Future connectivity will integrate shopping, monitoring, insurance and the dealership.
“Cars in the future will run on **DATA** and not **Gasoline**”
MODERN CAR
Approx. 150 ECUs
Approx. 7 networks
145,000 lines of code
40,000,000 lines of code
100,000,000 lines of code
300,000,000 lines of code
Car Electronics Architecture

- Gateway
- Drivetrain CAN
- Infotainment Ethernet
- Convenience LIN
- Body CAN
**IT CYBERSECURITY**

*Heuristic Security is Best*
Better be safe than sorry
Multiple solutions with overlap to leave no holes

*Homogenous Computing Environment*
~1-2 Types of OSes
Uniform hardware (e.g. Intel)

*Open and flexible software environment*
Software is very dynamic
Flexible communication protocols (may not be well defined or defined on the go)

*Functional segmentation only*
Network is separated by functional sub-sections

**AUTOMOTIVE CYBERSECURITY**

*Safety is most important*
Can’t make any mistakes
Less is more

*Heterogenous Computing Environment*
Many OSes and baremetal
Each ECU with different hardware

*Closed Environment*
Main software components are predefined and certified/tested/certified
Communication protocols are fixed

*Safety critical segmentation*
Network is segmented by data and not only function
Prevent Data Theft
Business Continuity
99% with 3% false positive

Passenger Safety
Vehicle Reliability
99.999%
OPTIMAL AUTOMOTIVE CYBER SOLUTION

Standalone Operation
No human interaction
No constant Communication needed
Built as Cyber Solution
Lockdown Methodology™ – Safe Security

COMMUNICATION SPECIFICATIONS
FUNCTIONAL SPECIFICATIONS

OEM Spec

SNO Check Message

CERTIFIABLE

DETERMINISTIC

Verified Message

Allowed | Not Allowed

Drop

Reporting the Attacks

Backend Data Center

May 13-16, 2019 Santa Clara Convention Center, CA • tmt.knect365.com/iot-world • #IOTWORLD
Communication Lockdown in Hardware – GuardKnox Secure Network Orchestrator™ (SNO)

Full Validity Check

Lockdown Security Core

Host CPU

HW Validity Check

FPGA

CAN

Ethernet

Network 1

Network N

May 13-16, 2019 Santa Clara Convention Center, CA • tmt.knect365.com/iot-world • #IOTWORLD
Autonomous vehicle provide additional cyber security challenges which require dedicated solutions

More complex recovery – no human in the loop

Complexity of Safety Critical Systems (e.g. ADAS)

Dependence on a multitude of complex, connected sensors (especially V2V/X)
Where do we go from here?

Security as
A Safety Mechanism

Defence in Depth

Certifiable and
Standardized Security
(ISO 21434)

Incorporate security
into sensors (incl. V2V)

May 13-16, 2019 Santa Clara Convention Center, CA • tmt.knect365.com/iot-world • #IOTWORLD
**Summary**

- Cyber Security is a Safety mechanism in modern vehicles
- Automotive cyber security needs to be reliable and verifiable
- **Lockdown** provides security methodology which is integrates well into existing vehicle development processes
- Can be implemented in hardware to increase security and performance
- Fits the growing need in future autonomous vehicles
- Complies with safety and security standards
THANK YOU

Dionis Teshler, CTO
dionis@guardknox.com
+972-54-6588052