Are we ready for the connected car?
A look into automotive security from a microchip perspective

Shawn Slusser
Vice President Infineon Automotive
## Agenda

- Connected Car Will Change Our Industry
- A Look Into Automotive Security – Some Basics
- What’s Needed For Automotive Security
Connected Car Will Allow

Apps

Content from Cloud

Software Updates

V2I for Convenience

V2V for Safety
Connect Car Will Allow Autonomous Driving
Convergence of Automotive & Consumer Worlds
Similar to the PC Market
History Repeats Itself – Changing Value Stream

November 6, 2013

MORGAN STANLEY BLUE PAPER

Autonomous Cars
Self-Driving the New Auto Industry Paradigm

Exhibit 59
Value of the Car – Today vs. Tomorrow

Today

- Hardware 90%
- Software 10%

Tomorrow

- Hardware 40%
- Content 20%
- Software 40%

Source: Morgan Stanley Research
What does this mean?

New Requirements are Necessary to Support the Connected Car
New Requirements for Connected Cars

Safety
- Protection against \textit{unintentional} errors, malfunctions and anomalies

Security
- Protection against \textit{intentional} errors, tampering, theft and data privacy

Functional Safety
- ISO 26262 Ahead

Dark-Side Scenarios
- Theft of IP/Content
- Hacking of System
- False Data Communicated
- Data Privacy
The Center for Automotive Embedded Systems Security (CAESS) is a collaboration between researchers at the University of California, San Diego and the University of Washington.

Our research mission is to help ensure the security, privacy, and safety of future automotive embedded systems.

www.autosec.org

2011  Comprehensive Experimental Analyses of Automotive Attack Surfaces

2010  Experimental Security Analysis of a Modern Automobile
“...should be read as a wake-up call...”

today's car owners should not be alarmed, ...it is time to focus squarely on addressing...automotive security issues...”

“potential analogy with desktop personal computers... pervasive broadband connectivity exposed... latent flaws... to attackers...”

“...will require a concerted effort from all relevant stakeholders...”
February 2015 Examples

**BMW Security Patch**

BMW Update Kills Bug In 2.2 Million Cars That Left Doors Wide Open To Hackers


**Senator Markey Report with 8 Key Findings**

Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk
Basic Security Elements/Functions

Secure Memory
For
Passwords & Certificates

Cryptography
For
Encryption & Decryption

Authentication
For
Genuine Confirmation

Root of Trust
Designed As & Always
Assumed As Genuine

Revocation
Is the ability to Cancel
Security Clearance
Security Technology Already Exists

Smart Card Security Technology
Will Be Needed For the Connected Car

Smart Card Security Technology = Dedicated Security Microcontroller
Smart Card’s Since 1980’s

Applications

- Prepaid Phone Cards
- Health Insurance
- Debit Cards
- Pay-TV
- Debit / Credit cards
- ID cards
- Patient cards
- Ticketing
- 3G Phones
- e-Passports
- Computers

Technologies

- Secure Memory Card
- Contactless Chip Cards
- Secure Controller Cards
- Contactless Label/ID/Tags
- Trusted Platform Modules

1980’s 1994 2000 2006 ...
Automotive Security Questions

With Up to 70 ECUs in a Modern Car

What Security Technology Adaptions are Needed?
Which ECUs Need Security and to What Security Level?

ACC – Adaptive Cruise Cntl
BCM – Body Cntl Module
BSD – Blind Spot Detection
ECU – Engine Cntl
EPS – Steering
ESC – Braking / Stability
GATE – Gateway
IMM – Immobilizer / Ignition
IC – Instrument Cluster
RES – Restraint / DCU
RKE – Remote Entry
TCU – Transmission Cntl
Tele – Telematic / Radio Ent.
Automotive Security Architecture

Car Makers will have to Consider Security in Future Electrical Architectures

ECUs Will Need Specialized Security Hardware

Specialized Security Software
Stand Alone Security IC Example

Considerations:
- Security Level
- Performance Needs
- Automotive Qual?

Be Aware: Non-Automotive Security ICs May Work
But, Most Are Not Designed for Automotive Applications!
Automotive Security Project

EU Funded Project:
Security architecture for automotive on-board networks

www.evita-project.org
Embedded Automotive Security Example

HSM

Hardware Security Module (HSM)

- Secure Memory
- Encryption & Decryption
- Authentication
- Root of Trust

HSM Trusted Execution Environment

Infineon Aurix

Flash, TriCore™ 0, TriCore™ 1, SRAM, Bridge, Peripherals, 32-bit CPU, SRAM, Boot ROM, AES 128, TRNG, Timer, Security Software

Copyright © Infineon Technologies AG 2015. All rights reserved.
Automotive Development Process Will Need to Consider Security

- Threat and attack scenario analysis
- Security objectives and measures

- Security hardware architectures expertise

- Security-certified design and development process

- Security Lab for hardware security penetration testing

- Security certified production
- Secure personalization

- Large portfolio of Security certified products

- Security objectives and measures

- Security hardware architectures expertise

- Security-certified design and development process

- Security Lab for hardware security penetration testing

- Security certified production
- Secure personalization

- Large portfolio of Security certified products
Automotive Security Will Need a Coordinated Ecosystem

V2V for Safety

Content from Cloud

Service Garages

IT Security Infrastructure

Automotive Supply Chain

Si Supplier

Tier 1

OEM
New Roles & Expertise Needed

- For Car Development
  - Security Architects
  - Engineers with Security Expertise

- For Manufacturing:
  - Security Officers (Key Management)
  - IT & Operations Security Experts

- For IT:
  - Security Architects
  - IT Key System Developers
  - Security Life Cycle Managers (for EOL)
Automotive Security Summary

- Smart Card Technology Will Be Adapted for Automotive

- Connected Cars will Need:
  - Security Defined into Vehicle Architectures
  - New Security HW & SW for ECUs
  - Security Included in Development Process

- Security Eco-System will Require New Expertise

- It’s Not Simple; We All Need to Build Our Security Expertise Now!
ENERGY EFFICIENCY
MOBILITY
SECURITY

Innovative semiconductor solutions for energy efficiency, mobility and security.