SECURITY FOR SELF-DRIVING CARS
Session 2: Security – impact on connected systems

Timo van Roermund, Director Automotive Security
TNO-ESI symposium 2017, Eindhoven

NXP
SECURE CONNECTIONS FOR A SMATER WORLD
NXP – #1 GLOBAL AUTO SEMI POWERHOUSE

#1 AUTO SEMI SUPPLIER GLOBALLY

>30 AUTO SITES IN ALL REGIONS

2400+ AUTO ENGINEERS

~40% OF NXP’S REVENUE IS FROM AUTO

+60 YEARS OF AUTOMOTIVE EXPERIENCE
Agenda

Trends
Self-Driving, Vehicle Architectures

The Need for Security
What is at stake?

Way Forward
Is security-by-design enough?
INDUSTRY MEGA TRENDS

Autonomy  Electrification  Connectivity

SAFE AND SECURE MOBILITY
ENABLED BY ELECTRONICS AND SOFTWARE
VEHICLE ELECTRONICS & CONNECTIVITY

**System Type**
- **Single Service Component Equipment**
- **Composed Services Composed Systems Super Systems**
- **Systems of Systems up to Eco-system (Co-Existence)**

**Interaction**
- Collaborating
- Interacting
- Sharing
- Multi customer

**Interconnected**
- Integrated

**Standalone**
- Autonomous

- Engine control ECU (~1980)
- Telematics, Bluetooth, WiFi, V2X (2000 - now)
Cars are becoming self-driving robots

The potential benefits are huge:
- Drivers spend 200-300 hours in their car (annually)
- Cars are parked (unused) 95% of the time
- > 90% of road accidents caused by human mistakes

Source: SAE J3016
Vehicle networks evolve, to accommodate the ever increasing amount of electronics:

**Today: Flat networks**
- Direct connection between all ECUs
- Cost-effective for low # of ECUs

**Tomorrow: Domain-based**
- Upgradeability and Scalability
- Separation of Concerns (a.o. Safety and Security)

**Future: Centralized**
- Fewer ECUs
- Flexible use of compute power
NEXT: DOMAIN BASED VEHICLE ARCHITECTURES

Connectivity

Driver Replacement

Powertrain & Vehicle Dynamics

Body & Comfort

Driver Experience

Secure Networks & Gateways

More than a brain on four wheels. The core of safe and secure mobility.
NXP LEADS DOMAIN BASED VEHICLE ARCHITECTURES

COMPLETE SOLUTIONS
FASTER TIME TO MARKET
FULL SCALABILITY

SENSE
V2X
Broadcast Radio
Cellular
WIFI, BT, GNSS, NFC
Smart Car Access

THINK
Connectivity Domain Controller

ACT
Fusion

Connectivity
Driver Replacement
Powertrain & Vehicle Dynamics
Body & Comfort
Driver Experience

1
2
3
4
5

Motion & Pressure
Speed
Ultrasonic

Powertrain & Vehicle Dynamics

Motion & Pressure

Powertrain Domain Controller

Powertrain & Vehicle Dynamics

TPMS

Body Domain Controller

Body & Comfort

Smart Light
Access, Door Ctrl
eCockpit
Amplifiers

Infotainment
Agenda

Trends
Self-Driving, Architectures

The Need for Security
What is at stake? Is it real?

Way Forward
Is security-by-design enough?
DID YOU KNOW?

- >25 Vehicle hacks published since 2015
- 1.4M Vehicle recalled in the largest incident to date

Why hacking?
- Valuable Data attracts hackers
  - Car-generated data may become a USD 750B market by 2030

Why is it possible?
- High System Complexity implies high vulnerability
  - Up to 150 ECUs per car, up to 200M lines of software code

Why now?
- Wireless Interfaces enable scalable attacks
  - 250M connected vehicles on the road in 2020

SECURITY IS A MUST-HAVE FOR CONNECTED & AUTONOMOUS VEHICLES
Security is often ignored, or applied as an after-thought!

No (or weak) security countermeasures, no (domain) isolation, etc.
## WHAT IS AT RISK, AND WHOM IS AFFECTED?

### STAKEHOLDERS

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>Car User</th>
<th>Car Owner</th>
<th>Insurers</th>
<th>OEM &amp; Suppliers</th>
<th>Service Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety</td>
<td>Injuries</td>
<td>Damage</td>
<td></td>
<td>Claims, Brand Damage</td>
<td></td>
</tr>
<tr>
<td>Financial</td>
<td>Vehicle Theft</td>
<td>Insurance Claims</td>
<td>IP Theft</td>
<td>Loss of Income (Fraud, DoS, …)</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Loss of Personal Data (PII)</td>
<td></td>
<td>Claims, Brand Damage</td>
<td>Claims, Brand Damage</td>
<td></td>
</tr>
</tbody>
</table>

**Privacy**
- Loss of Personal Data (PII)
- Claims, Brand Damage
- Claims, Brand Damage
Way Forward
Is security-by-design enough?

The Need for Security
What is at stake?

Agenda
Trends
Self-Driving, Architectures
AUTOMOTIVE SECURITY – WAY FORWARD

Essential element: Defense-in-Depth approach

- Multiple layers of protection, at different levels in the system
- To mitigate the risk of one component of the defense being compromised or circumvented

APPLY BEST PRACTICES:

- Security-by-design & Privacy-by-Design (as opposed to being an afterthought)
- Lifecycle Management (incl. FOTA)

TODAY

FUTURE
CORE SECURITY PRINCIPLES

Secure External Interfaces
Secure Domain Isolation
Secure Internal Communication
Secure Software Execution

They need to be in place in any E&E network

- Regardless of the actual architecture and implementation
## APPLYING THE CORE SECURITY PRINCIPLES

Securing the Vehicle’s E&E Architecture using a Defense in Depth approach

<table>
<thead>
<tr>
<th>Prevent access</th>
<th>Detect attacks</th>
<th>Reduce impact</th>
<th>Fix vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>M2M authentication</td>
<td>Intrusion detection systems (IDS)</td>
<td>Separate functional domains</td>
<td>Secure OTA updates (firmware, policies, …)</td>
</tr>
<tr>
<td>Firewalls (isolate access points)</td>
<td>Firewalls (context-aware message filtering)</td>
<td>Isolated TCU &amp; OBD-II</td>
<td></td>
</tr>
<tr>
<td>Secure Messaging (e.g. SecOC)</td>
<td>Run-Time Integrity Protection</td>
<td>Message Filtering, Rate Limitation</td>
<td></td>
</tr>
<tr>
<td>Code Authentication (secure boot)</td>
<td>Resource control (virtualization)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**secure**
- external interfaces
- domain isolation
- internal communication
- software execution

---

**vehicle architecture axis**

**time axis**
4 LAYERS TO SECURING A CAR

Layer 1: Secure Interface
Secure M2M authentication, secure key storage

Layer 2: Secure Gateway
Domain isolation, firewall/filter, centralized intrusion detection (IDS)

Layer 3: Secure Network
Message authentication, filtering, distributed intrusion detection (IDS)

Layer 4: Secure Processing
Secure boot, run time integrity, OTA updates
4 LAYERS TO SECURING A CAR (VIDEO)

Available online: https://www.youtube.com/watch?v=cclydY87a1E
SECURITY TOOLBOX
MIX OF TECHNOLOGIES AND BEST PRACTICES

**Cryptography** – an important basis, but not a substitution for security
- Crypto algorithms like AES, RSA, SHA2 are ‘basic building blocks’
  (Please don’t invent your own crypto algorithm…)

**Restricting Access** – e.g. using:
- Physical Isolation (e.g. separate networks and “air gaps”)
- Logical Isolation (e.g. firewalls between networks)
- Access Control (e.g. identification, authentication & authorization)

**Other tools:**
- Monitoring (e.g. intrusion detection systems)
- Software updates (e.g. SOTA / FOTA)
- Design, code and protocol reviews
- Defensive, secure and clean programming
- Security assessment (Pen Test, …)
- Formal proof systems, …

Most security vulnerabilities are caused by design & implementation weaknesses(!)
Vehicle security requires a tight integration of **hardware**, **software** and **services**

**Complementary strengths:**

- Threat Monitoring & Response – e.g. Cloud Analytics
- Device & Identity Management – e.g. Trust Provisioning
- Flexibility / Updateability – e.g. FOTA/SOTA For Fixing Bugs, Vulnerabilities
- Performance – e.g. Crypto Accelerators
- Immutability – e.g. Hardware Enforced Isolation (HSM)
- Tamper Resistance – e.g. Sensors, Glue Logic, Shields
SECURITY REQUIRES A HOLISTIC APPROACH (& ONGOING EFFORT)

Security must be an integral part of the lifecycle
- In product design, implementation *and* maintenance
- So from its initial conception, until its end-of-life

But also in associated processes; e.g.:
- Secure Development and Manufacturing Processes
- Risk Assessment and Management
- Security Awareness Trainings for Employees
- Threat Intelligence Feed
- Product Security Incident Response Team
- External Audits for Product / Site Security

NXP was amongst the first suppliers to join the Auto-ISAC (Aug. ‘16)

Goals of the Auto-ISAC:
- Intel Sharing & Analysis
- Best Practice Sharing
- Partnerships & Community Development
KEY TAKEAWAYS

1. What does it take to come to security-by-design?
   • Holistic approach, covering a.o.:
     • Mindset – *e.g.* pro-active vs. reactive (i.e. not an afterthought) → ‘security culture’
     • Solutions – *e.g.* changes in architectures, security & privacy by design, …
     • Lifecycle management – *e.g.* maintenance after product release
     • Way of working – *e.g.* secure engineering/manufacturing/… processes
     • Business case – *e.g.* willingness to pay an ‘insurance premium’
     • Education – *e.g.* awareness trainings

2. How do I become aware of system security issues?
   • Use collective intelligence – *e.g.* sharing information & best practices in industry

3. How can I survive without being a security expert?
   • Rely on experts (internal/external) – while understanding the basics yourself
CONCLUSION

• Automotive Innovation is changing towards developing self-driving robots

• Security is essential – people must be able to trust their cars

• It requires a holistic approach:
  − secure technical solutions (products and architectures)
  − the application of best practices
  − maintenance (continuous effort!)
  − security policies and processes

www.nxp.com/automotivesecurity