Submitted by UL-Netherlands

Document No. ITS/AD-09-15
(9th ITS/AD, 22 June 2016, agenda item 4)

Security of In-Vehicle Software

A Vision on Security for Road Safety

Geneva, 22 June 2016
UNECE Informal Group on ITS/ Automated Driving

Arjan Geluk, arjan.geluk@ul.com

CLASSIFICATION: PUBLIC

Agenda

The Challenge of Vehicle Security

Target Situation: Secure Vehicles for Safe Roads

Bridging the Gaps

The Challenge of Vehicle Security

The Trends

- Transition of the automobile into the information age
  - Vehicle connectivity, vehicle automation, data collection
- Growing complexity
  - 20-100 connected embedded devices
  - Tens of millions of lines of code
  - Wireless capability: keyless entry, tire-pressure monitoring, infotainment, telematics systems

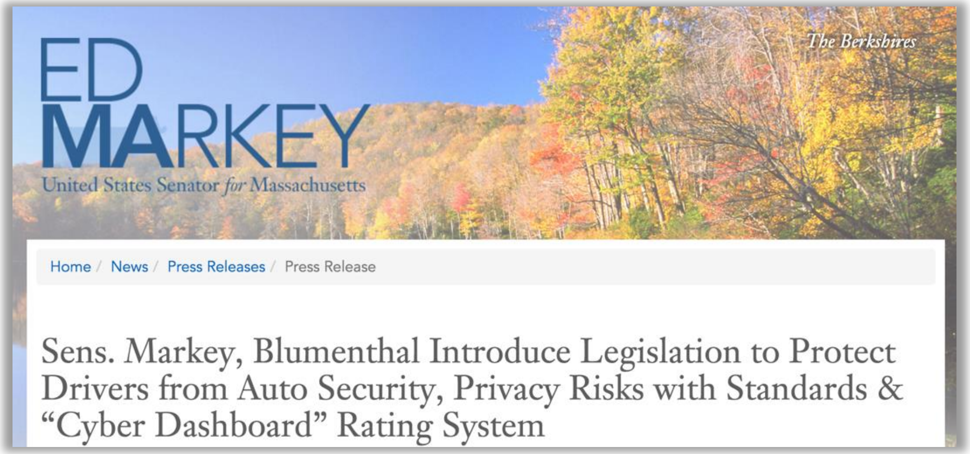
In Security Terms:

- **Increasing probability of exploitable software flaws**
- **Larger attack surface**
- **Greater risk of privacy violations**

The Challenge of Vehicle Security

The Trends

- Increased attention and accessibility for car hacking

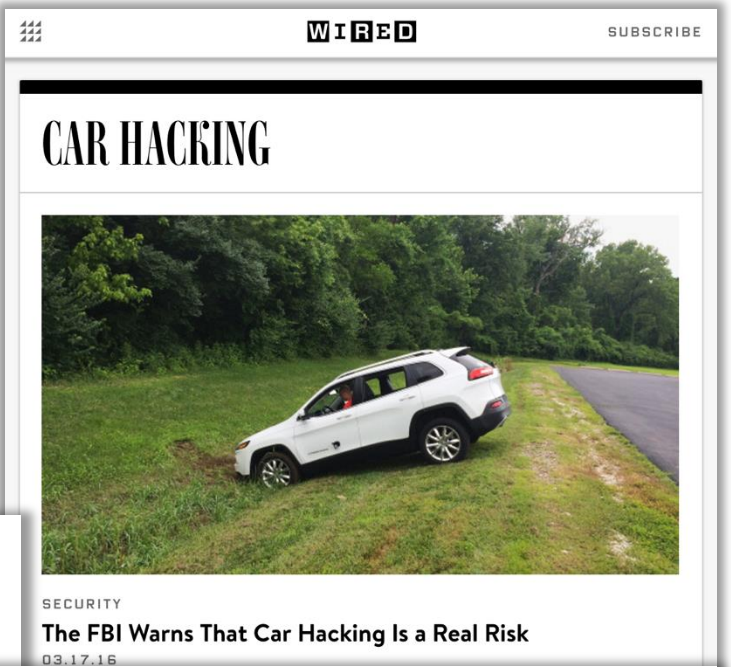


ED MARKEY

United States Senator *for* Massachusetts

Home / News / Press Releases / Press Release

Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & "Cyber Dashboard" Rating System

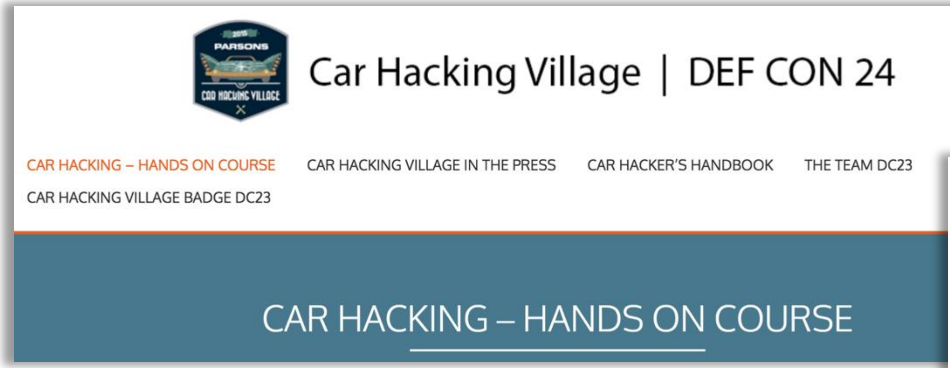


CAR HACKING

SECURITY

The FBI Warns That Car Hacking Is a Real Risk

03.17.16

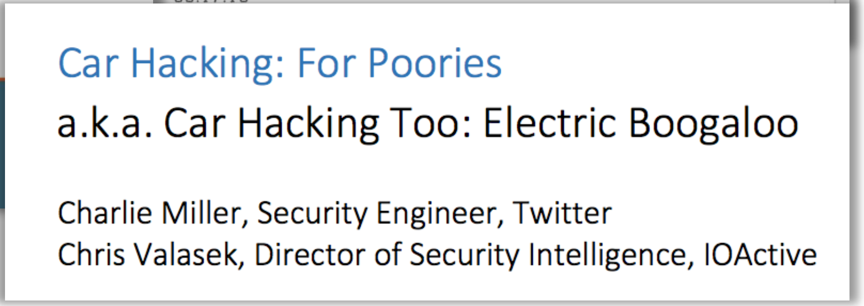


2015
PARSONS
CAR HACKING VILLAGE

Car Hacking Village | DEF CON 24

CAR HACKING – HANDS ON COURSE
CAR HACKING VILLAGE IN THE PRESS
CAR HACKER'S HANDBOOK
THE TEAM DC23
CAR HACKING VILLAGE BADGE DC23

CAR HACKING – HANDS ON COURSE



Car Hacking: For Poories

a.k.a. Car Hacking Too: Electric Boogaloo

Charlie Miller, Security Engineer, Twitter
Chris Valasek, Director of Security Intelligence, IOActive

Target Situation

Secure Vehicles for Safe Roads

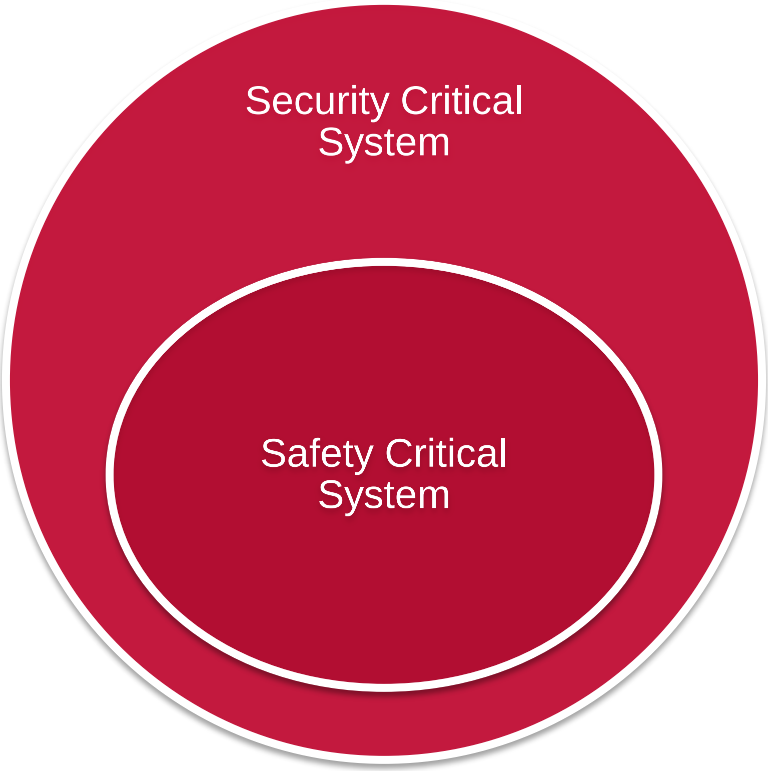
A vision for the future of automotive cybersecurity

1. Security will be taken as seriously as safety
2. Security and safety will be addressed in an integrated manner
3. Legal frameworks and type approval requirements enforce high levels of security
4. Vehicle authorities consider the whole vehicular infrastructure
5. Wide adoption of industry standards tailored to automotive cybersecurity
6. Privacy is addressed using general data protection rules applied to the automotive domain

Target Situation

Secure Vehicles for Safe Roads

1. **Security will be taken as seriously as safety**



- Not addressing security means relying on luck
- Any system that must be **SAFE**, must also be **SECURE**
- If a non-safe state can be caused *unintentially*, then what about *maliciously*?

Target Situation

Secure Vehicles for Safe Roads

2. **Security and safety will be addressed in an integrated manner**

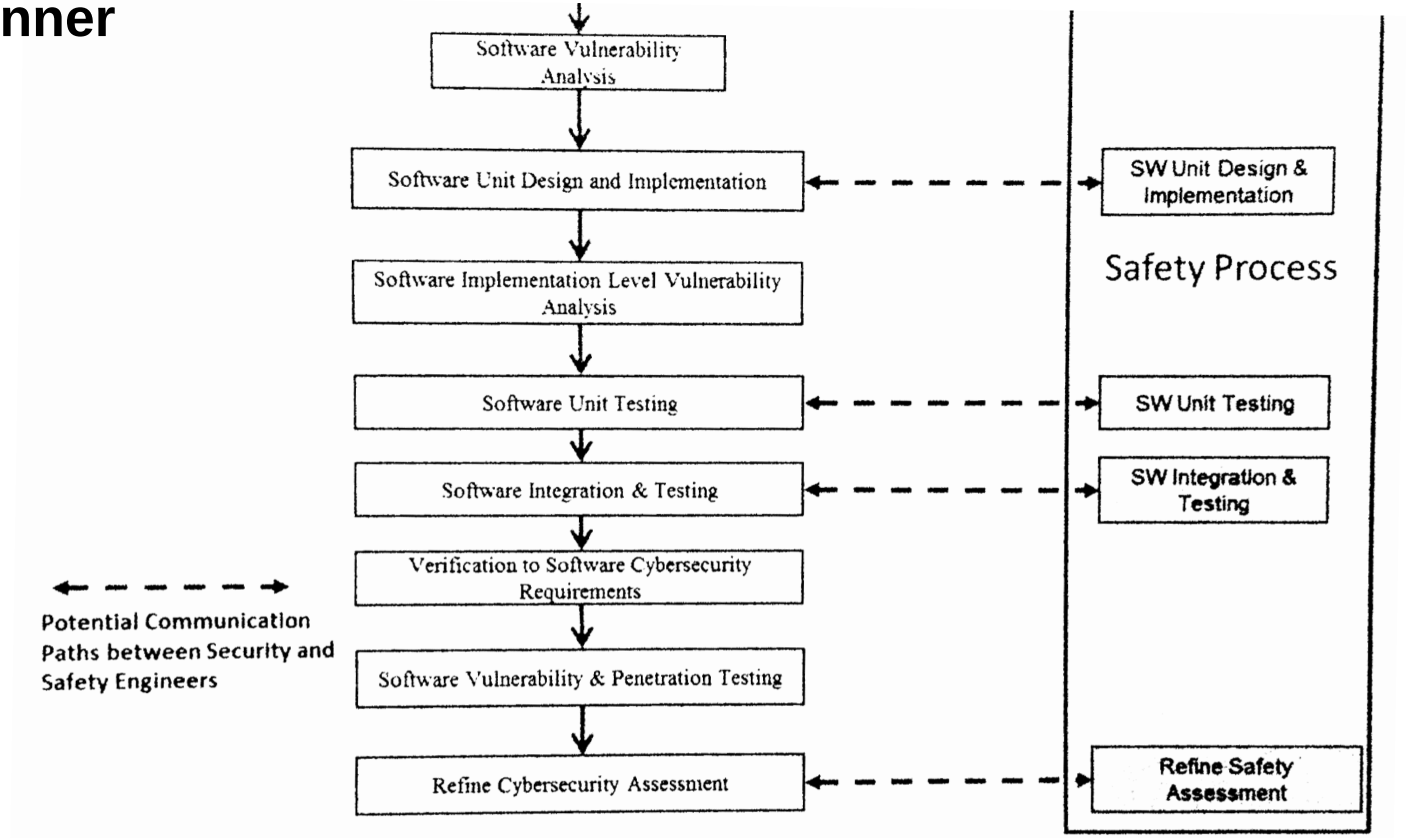

Software Vulnerability Analysis
Software Unit Design and Implementation
Software Implementation Level Vulnerability Analysis
Software Unit Testing
Software Integration & Testing
Verification to Software Cybersecurity Requirements
Software Vulnerability & Penetration Testing
Refine Cybersecurity Assessment
SW Unit Design & Implementation
Safety Process
SW Unit Testing
SW Integration & Testing
Refine Safety Assessment
Potential Communication Paths between Security and Safety Engineers

Figure 17 - Product development at the software level activities with potential communications paths between Cybersecurity and safety activities

Source: SAE J3061

Target Situation

Secure Vehicles for Safe Roads

2. **Security and safety will be addressed in an integrated manner**

Key Advantages:

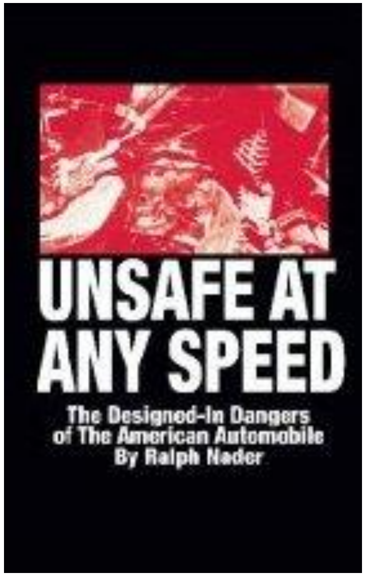
- Same goal: Prevent the vehicle from entering an unsafe state
- Take advantages of already implemented frameworks, processes, *mentalities*
- Efficiency of overlapping safety and security measures
- Consistency and completeness

Target Situation

Secure Vehicles for Safe Roads

3. **Legal frameworks and type approval requirements enforce high levels of security**

- Historically, safety has been driven to a large extent by regulation. Security will be even more so, because
  - Return on investment for security is very long-term
  - We need to act proactively
  - The sector as a whole is not security aware enough (yet!)



Target Situation

Secure Vehicles for Safe Roads

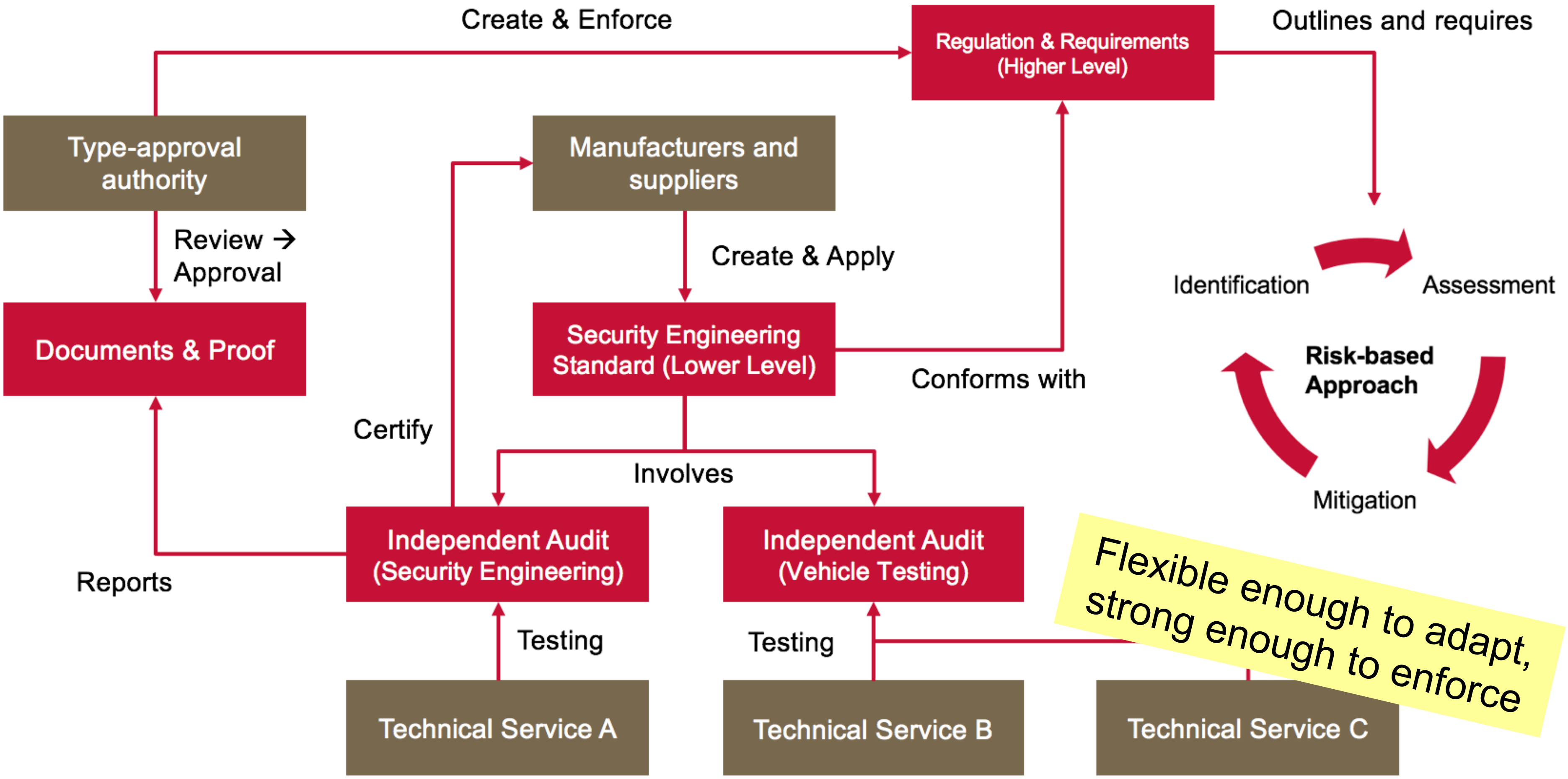
3. **Legal frameworks and type approval requirements enforce high levels of security**

- Security regulation should be integrated in the existing systems for
  - Creating the standards and regulation
  - Enforcing the regulation through national type approval authorities
  - Incident Response

Target Situation

Secure Vehicles for Safe Roads

3. **Legal frameworks and type approval requirements enforce high levels of security**

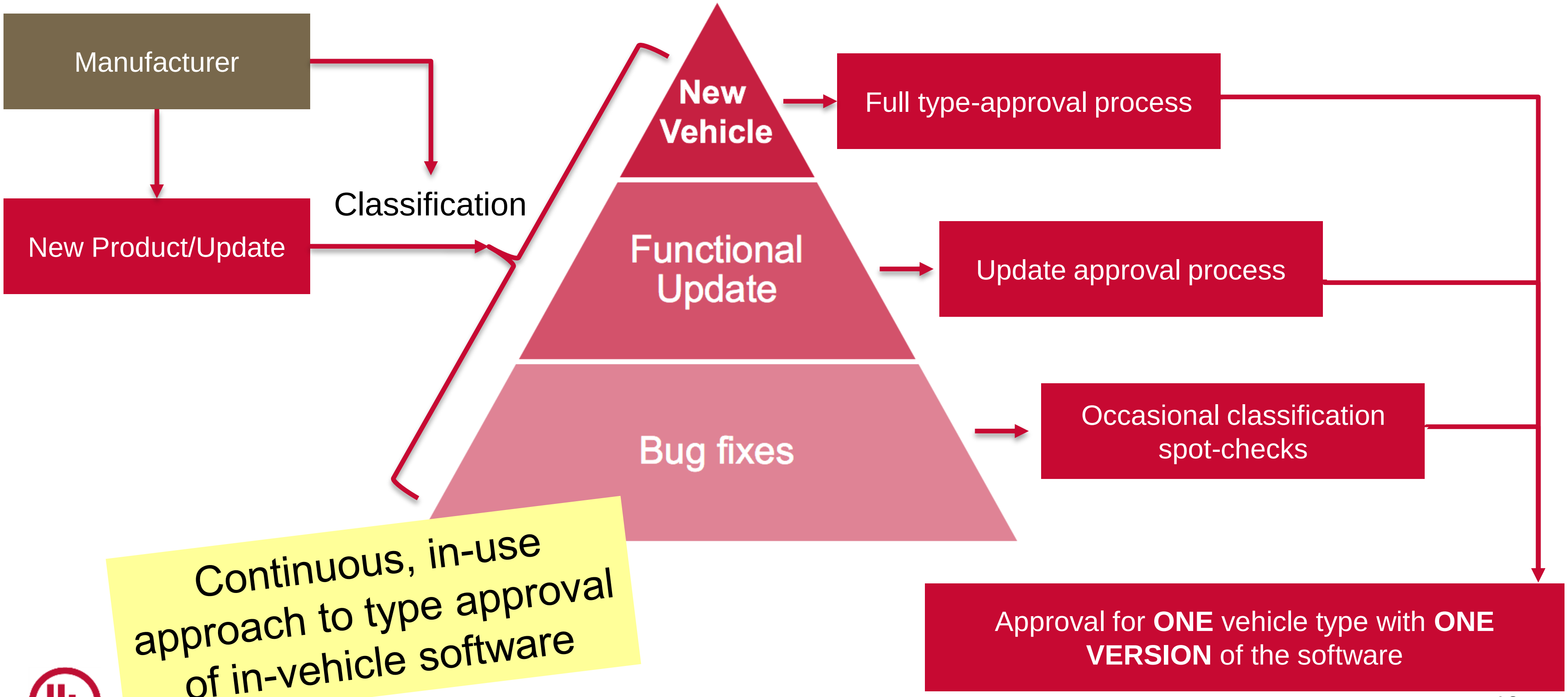


Flexible enough to adapt, strong enough to enforce

Target Situation

Secure Vehicles for Safe Roads

3. **Legal frameworks and type approval requirements enforce high levels of security**

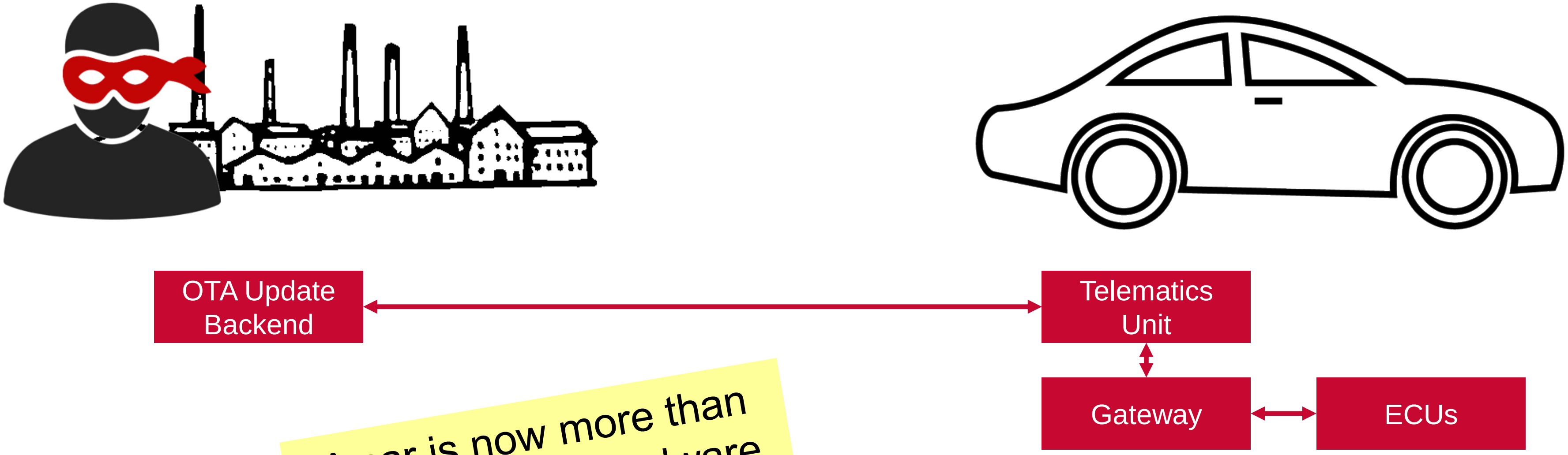

Manufacturer
New Product/Update
Classification
New Vehicle
Functional Update
Bug fixes
Full type-approval process
Update approval process
Occasional classification spot-checks
Approval for **ONE** vehicle type with **ONE VERSION** of the software

Continuous, in-use approach to type approval of in-vehicle software

Target Situation

Secure Vehicles for Safe Roads

4. **Vehicle authorities consider the whole vehicular infrastructure**

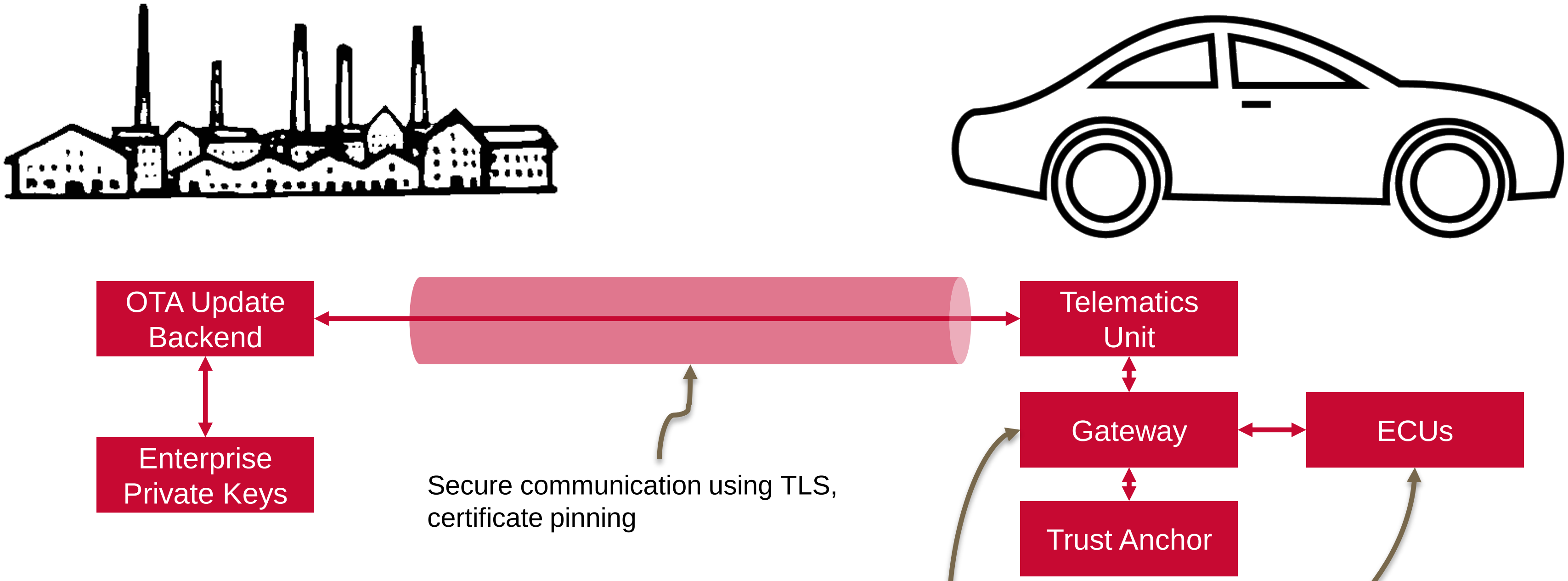


A car is now more than just in-vehicle hardware and software

Target Situation

Secure Vehicles for Safe Roads

4. **Vehicle authorities consider the whole vehicular infrastructure**



OTA Update Backend

Enterprise Private Keys

Telematics Unit

Gateway

ECUs

Trust Anchor

Secure communication using TLS, certificate pinning

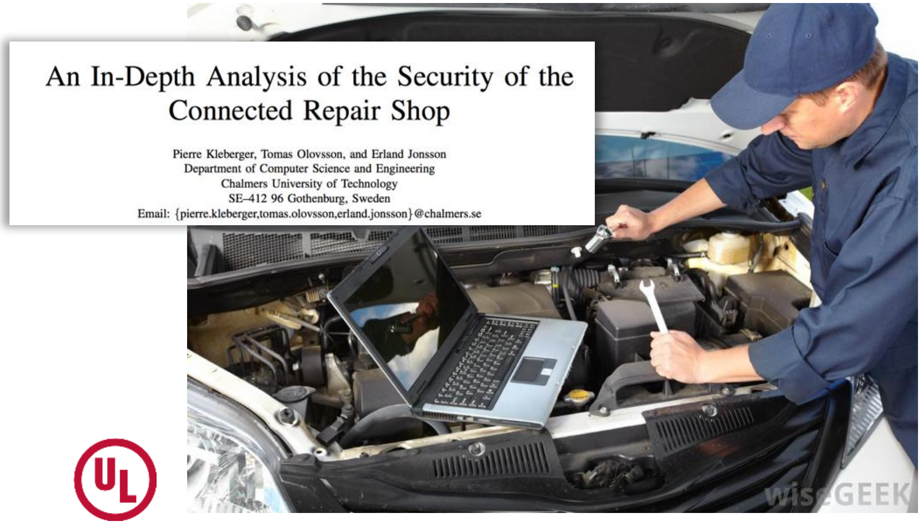
Code signature verification, integrity checks, secure distribution of service pack, secure boot loader, etc. …

Target Situation

Secure Vehicles for Safe Roads

4. **Vehicle authorities consider the whole vehicular infrastructure**

- In-vehicle security measures alone may not be effective
  - Extra-vehicular systems with safety critical functions
  - Vulnerable after-market additions
  - Compromised service stations and vehicle repair shops



An In-Depth Analysis of the Security of the Connected Repair Shop

Pierre Kleberger, Tomas Olovsson, and Erland Jonsson
Department of Computer Science and Engineering
Chalmers University of Technology
SE–412 96 Gothenburg, Sweden
Email: {pierre.kleberger,tomas.olovsson,erland.jonsson}@chalmers.se

Target Situation

Secure Vehicles for Safe Roads

5. **Wide adoption of industry standards tailored to automotive cybersecurity**

- Current situation:
  - Many security standards and best practices for other domains, but not specific to automotive
  - Standards are being developed, but are in early stages
    - e.g. VDA & SAE contributions to ISO
- Target:
  - Standards describing a secure development lifecycle and best practices for securing automotive systems, from in-vehicle software until cloud services

Target Situation

Secure Vehicles for Safe Roads

6. **Privacy is addressed using general data protection rules applied to the automotive domain**

- A lot of sensitive data is being collected by vehicular systems
- Voluntary “Consumer Privacy Protection Principles” have been developed specifically for the automotive industry
- Compliance is required with general data protection rules, applied to the automotive domain

So how do we get there?

Bridging the Gaps?

Key measures

- Security-by-design, a life-cycle approach for designing in-vehicle software
  - How do regulators conduct surveillance? Rating system?
- Software Updates:
  - Secure using code signing and trust anchor
  - Roll-out of security patches
  - Management of type-approval if functional changes are conducted
- Collaboration with the security community
  - Bounty Programs
  - Information sharing of threats, vulnerabilities, best practices among manufacturers. Maturity models
  - Learning from other industries (aeronautical industry? Industrial control systems?)
- Defence-in-depth
  - Layered approach
  - Segmentation and Isolation
  - Logging
  - In-vehicle network security (redesign of protocols, intrusion detection and prevention)
- Initiatives
  - Security workgroup under UNECE
  - ISO standardisation using SAE and VDA input

THANK YOU.

UL Software & Security – Contact Details

Europe
Leiden, the Netherlands
Call +31 71 581 3636
Email ulcyber@ul.com

Visit www.ul.com