

Automotive Linux, Cybersecurity and Transparency

Alison Chaiken

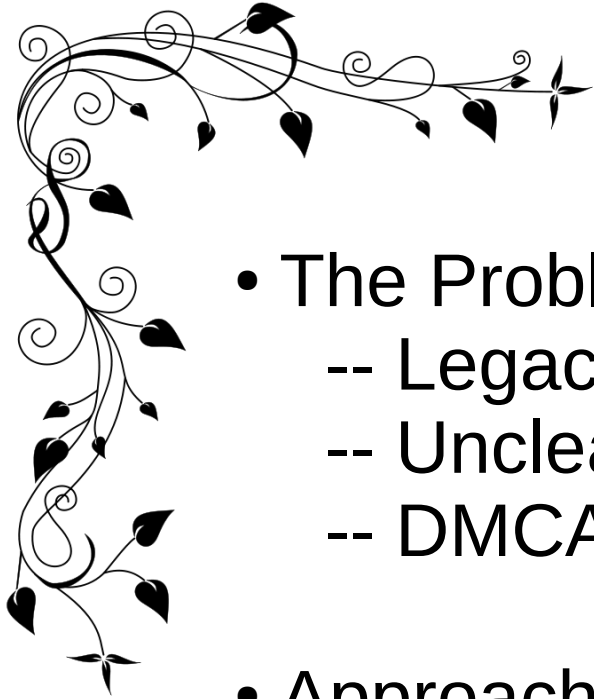



SCALE 14x

alison@she-devel.com

Jan 22, 2016

http://she-devel.com/Chaiken_automotive_cybersecurity.pdf



- 
- 
- 
- 
- The Problem(s)
 - Legacy designs
 - Unclear privacy situation
 - DMCA
 - Approaches to a Solution
 - PKE
 - Virtualization
 - Architecture-based security
 - Open Source

Ready or not, here come new regulations

[Caltrans source link](#)

Department of Motor Vehicles

Invitation to Public Workshops on Draft Regulations for Autonomous Vehicles

The department is seeking public discussion in the following areas:

- Feedback on specific provisions of the draft regulations
- How the state can best require compliance with transparent and technical safety standards
- Manufacturer certification requirements and how the department can best determine the validity of those certifications

Workshop Schedules

Northern California

10:00 a.m.

Thursday, January 28, 2016

Harper Alumni Center,

California State University, Sacramento

6000 J Street, Sacramento, CA 95819

Southern California

10:00 a.m.

Tuesday, February 2, 2016

Junipero Serra Building, Carmel Room

320 West 4th Street, Los Angeles, CA 90013

July 2015: Miller and Valasek “state-sponsored” takedown of Jeep

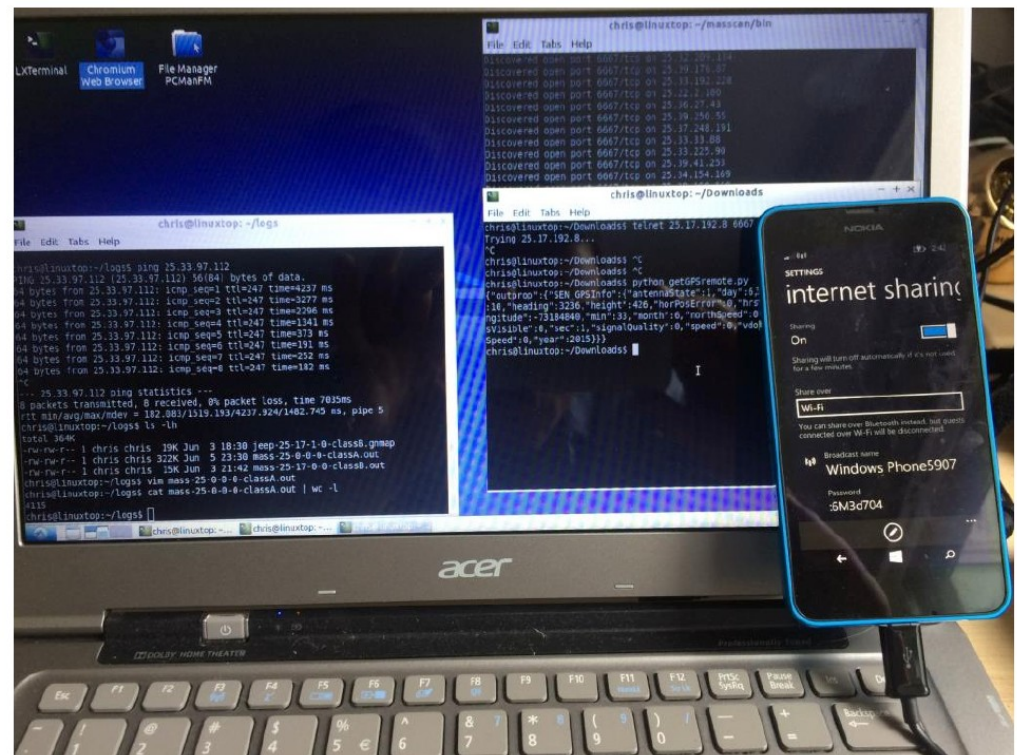


source: <http://illmatics.com/Remote%20Car%20Hacking.pdf>

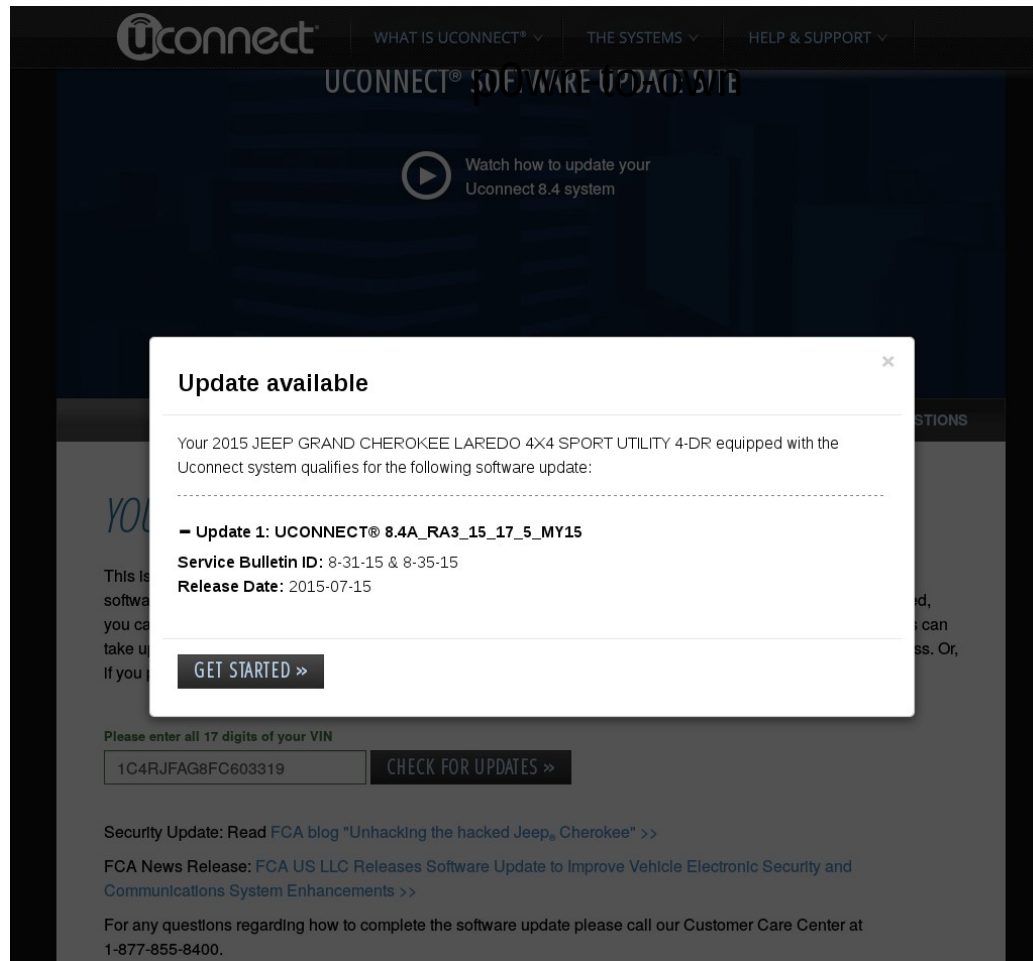
Miller-Valasek: D-Bus service responding to an open 3G port

“To find vulnerable vehicles you just need to scan on port 6667 from a Sprint device. . . ”

```
# netstat
Active Internet connections
Proto Recv-Q Send-Q Local Address Foreign Address
tcp 0 0 144-103-28-21.po.65531 68.28
tcp 0 27 144-103-28-21.po.65532 68.28
tcp 0 0 *.6010 *.
tcp 0 0 *.2011 *.
tcp 0 0 *.6020 *.
tcp 0 0 *.2021 *.
tcp 0 0 localhost.3128 *.
tcp 0 0 *.51500 *.
tcp 0 0 *.65200 *.
tcp 0 0 localhost.4400 localhost.65533
ESTABLISHED
tcp 0 0 localhost.65533 localhost.4400
ESTABLISHED
tcp 0 0 *.4400 *.
tcp 0 0 *.irc *.
LISTEN
LISTEN
```



Without Over-the-Air Updates, Jeep is stuck



Dec. 2015 view of Uconnect update

The Jeep was running QNX

- QNX is outshipping Linux 6:1 say analysts.
- Many automakers plan cars that run Linux:
 - **GENIVI** members: BMW, FAW, CMC, Great Wall, Honda, Hyundai, JLR, Daimler, Nissan, Peugeot-Citroen, Renault, SAIC, Volvo
 - **AGL** members: Toyota, JLR, Mitsubishi, Nissan, Honda, Ford, Mazda, Subaru
- So everything's fine, right?

What about . . .

- attaching your phone via USB to a rental car?
- leaving your car at a repair shop overnight?

How do we . . .

- opt out of automakers' data collection?
- reset a car for sale to factory defaults?

Should . . .

- an unpatched car fail its safety inspection?
- law enforcement routinely monitor speed data?



We need societal values to inform
transportation technological decisions
. . . *not* the other way around!



Safety vs. Security Tradeoffs?



- 2-seconds-to-rear-view-camera NHTSA rule enforces minimum boot time.
- Ill-considered regulations can lead to *less* safety when increased attack surface is factored in.

Event Data Recorders: NHTSA decision pending



Driving Safety

Vehicle Safety

Research

Data

Laws & Regulations

About NHTSA

About NHTSA
Home

About the
Administrator

Congressional
Testimony

Jobs at NHTSA

Speeches, Press
Events &
Testimony

CHAT HELP

t

f

You

✉

🖨

U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety

NHTSA 46-10

Friday, December 7, 2012

Contact: Karen Aldana, 202-366-9550

Requirement aims to capture valuable safety-related information in seconds before and during a motor vehicle crash



ELECTRONIC FRONTIER FOUNDATION eff.org

What is being collected?

- 14 mandatory points + 28 optional
- But that's a floor, not a ceiling
- What else?
 - Location
 - Audio or Video

courtesy
Nate Cardozo,
EFF



The surest approach to security:
avoid being an attractive target



The ONLY way that payment credentials should
be stored in a car



Connectivity to car systems: double-stick tape

HOME / CONNECTED VEHICLES, AUTOMOTIVE SECURITY, CONNECTED DRIVER, CONNECTED VEHICLES / [DOCUSIGN MAKES SECURE DIGITAL TRANSACTIONS FOR VISA'S CONNECTED CAR INITIATIVE](#)

DocuSign makes secure digital transactions for Visa's connected car initiative

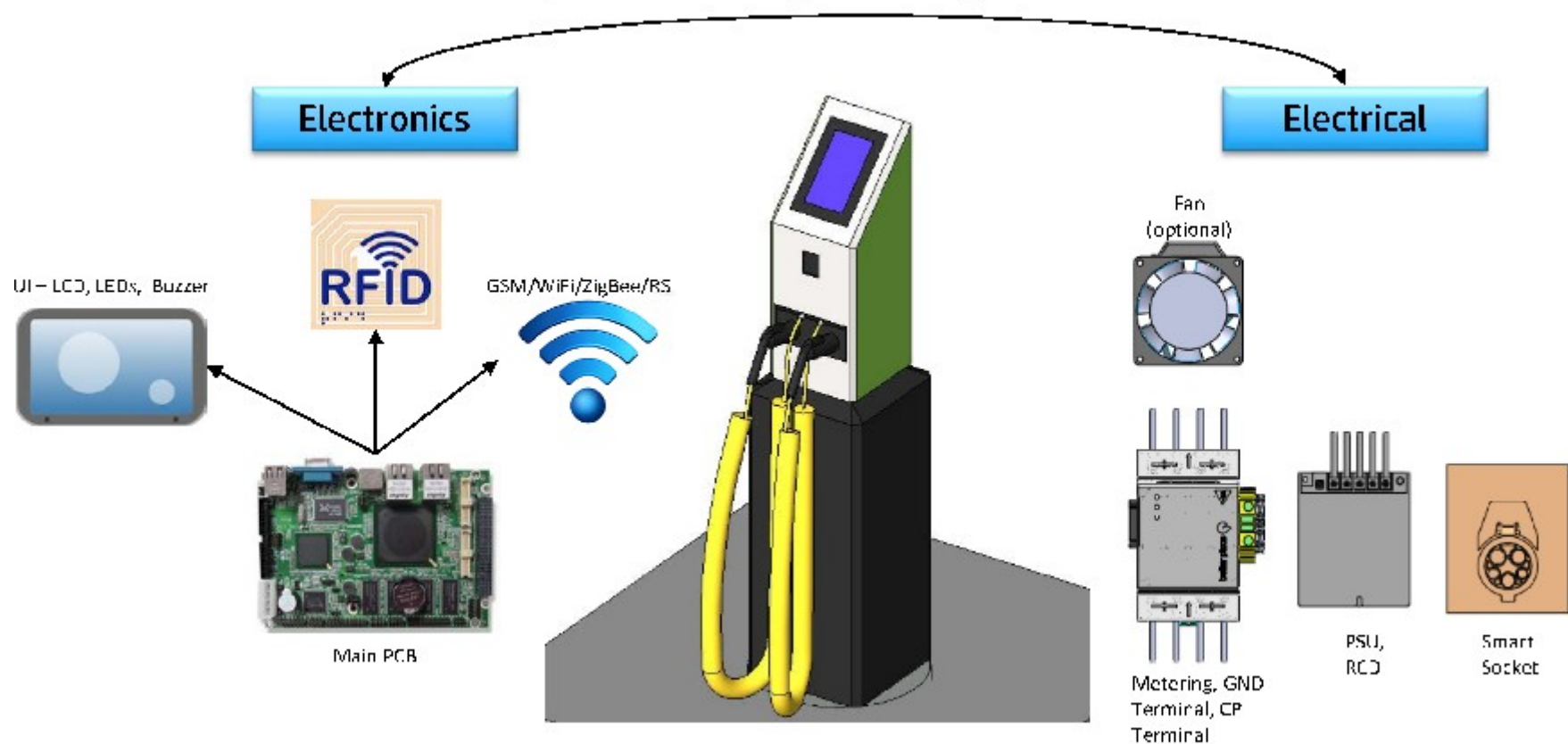
Published: November 03, 2015 | Las Vegas, NV

Associating *broad* payment credentials
with *embedded* car systems
puts lives in danger.

Payment credentials + High Voltage + Connectivity

What could possibly go wrong?

Component by component



16

Ozer Shezaf, http://xiom.com/2013/04/13/who_can_hack_a_plug_the_presentation



Security and transparency approaches



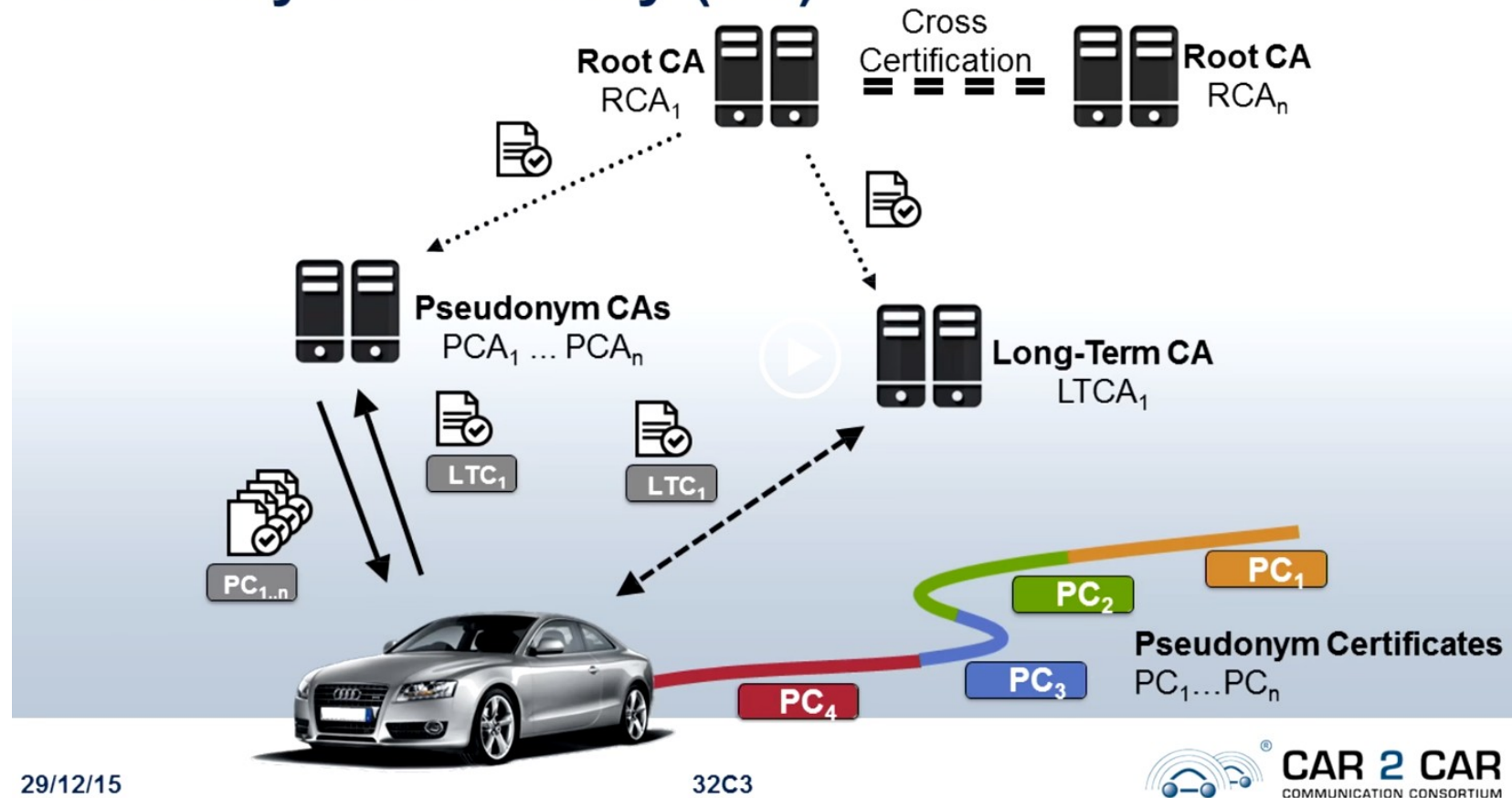
Securing back end communications

- Each device is issued a private key at manufacture, the public key is sent to the back end along with the device ID
- Each message is signed when it is sent, inside of an HTTPS connection with certificate verification



Preserving anonymity with PKE is Challenging

Security and Privacy (EU)



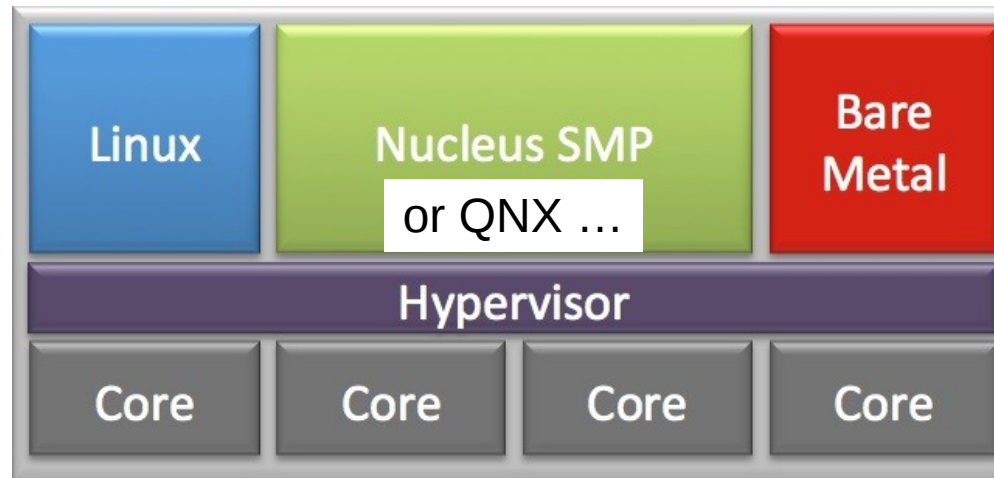
Courtesy B. Lehrmann, 32C3, “Vehicle2Vehicle Communication based on IEEE802.11p”

Multiple processor cores with multiple OSes



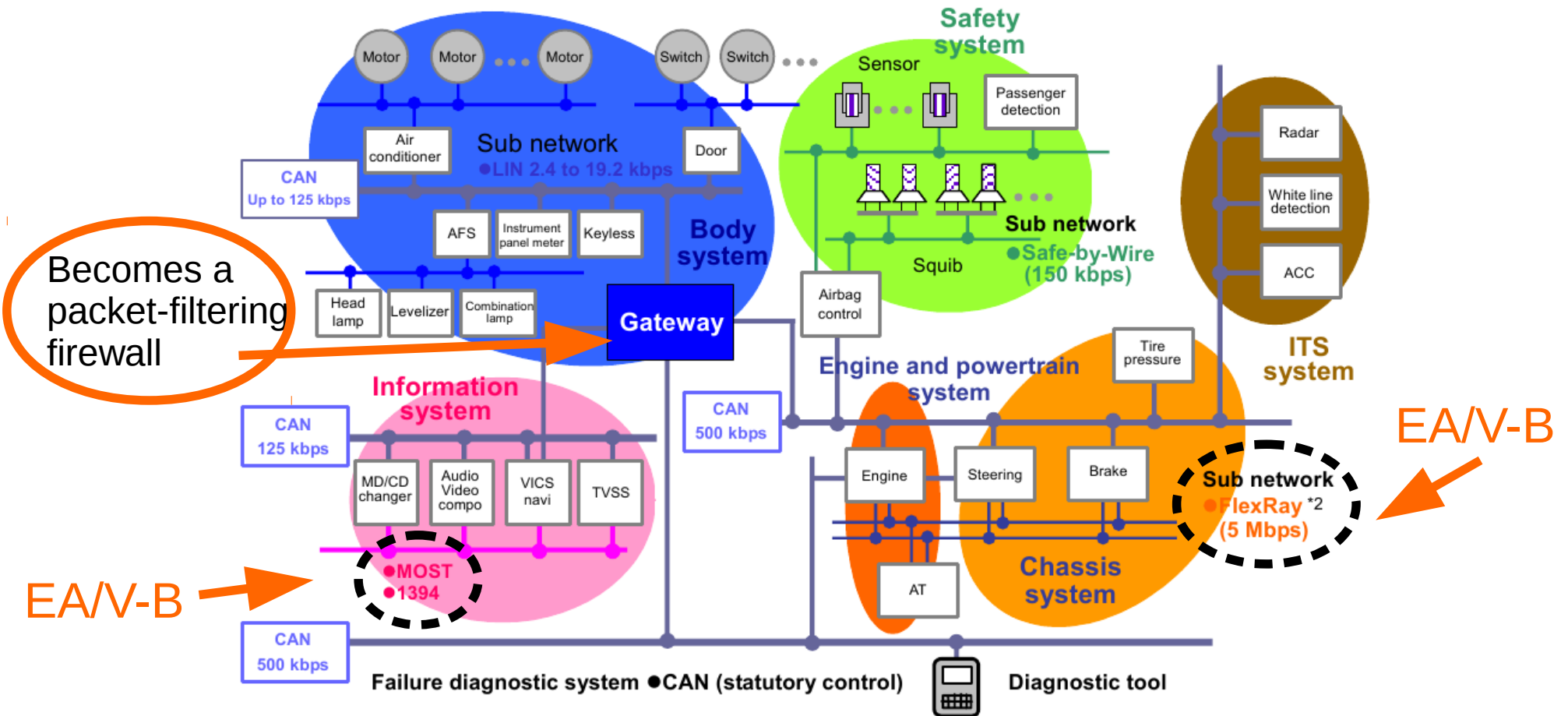
Driver Assistance,
Navigation, Entertainment

Linux can
be AGL-GENIVI
or Android, or one
core of each



Proprietary
or Xen

Automotive LAN, 2025



Copyright Renesas, "Introduction to CAN", with permission.

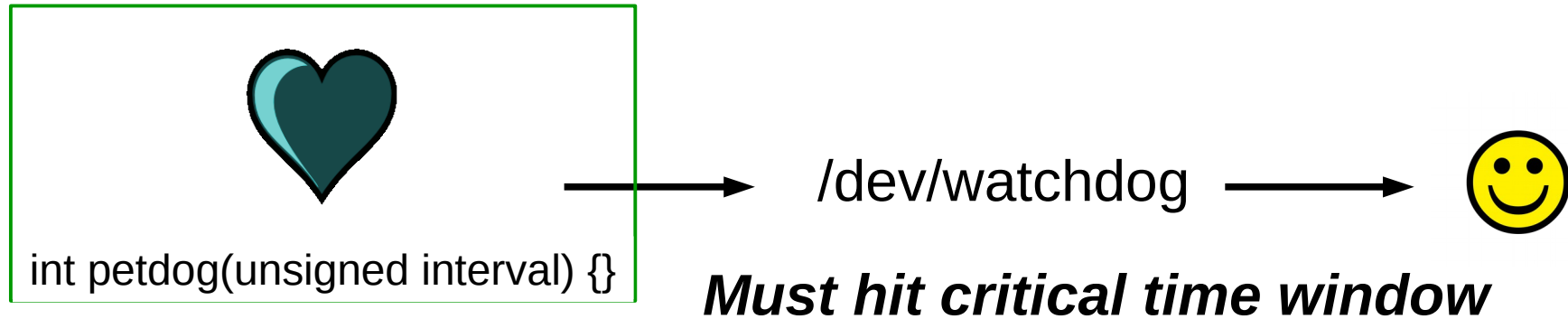
Ethernet A/V-B (audio-video bridging) will displace FlexRay and MOST₂₀

Proposal: scantool connection via DB only

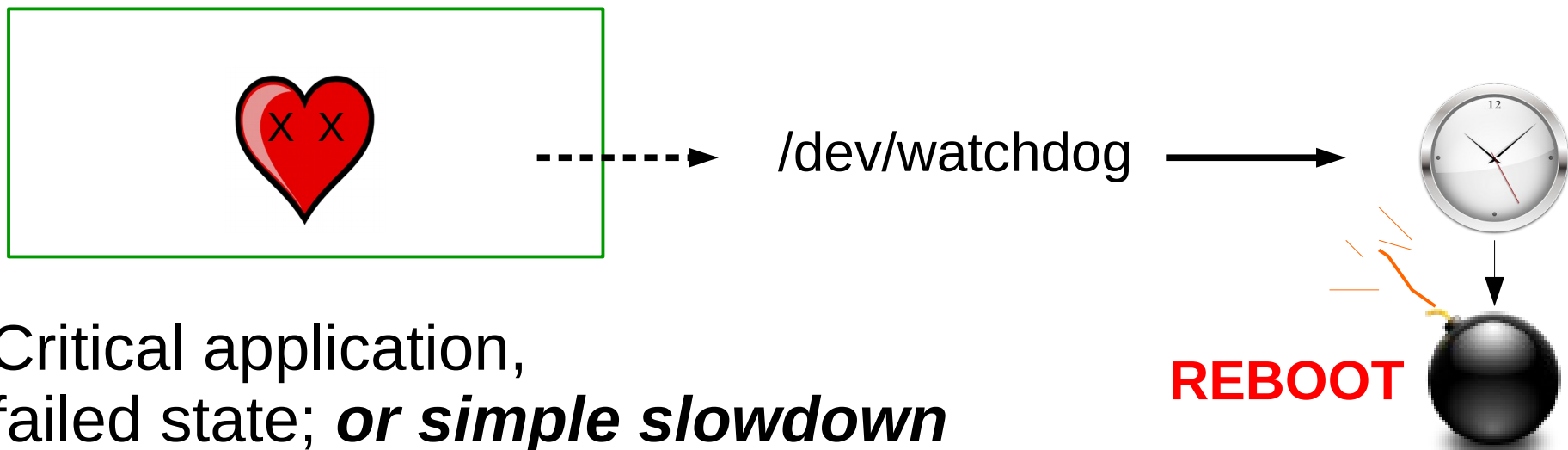


Get rid of *hard* connections to CAN from passenger cabin.

Linux kernel's watchdog timer guards against intrusion-caused slowdown

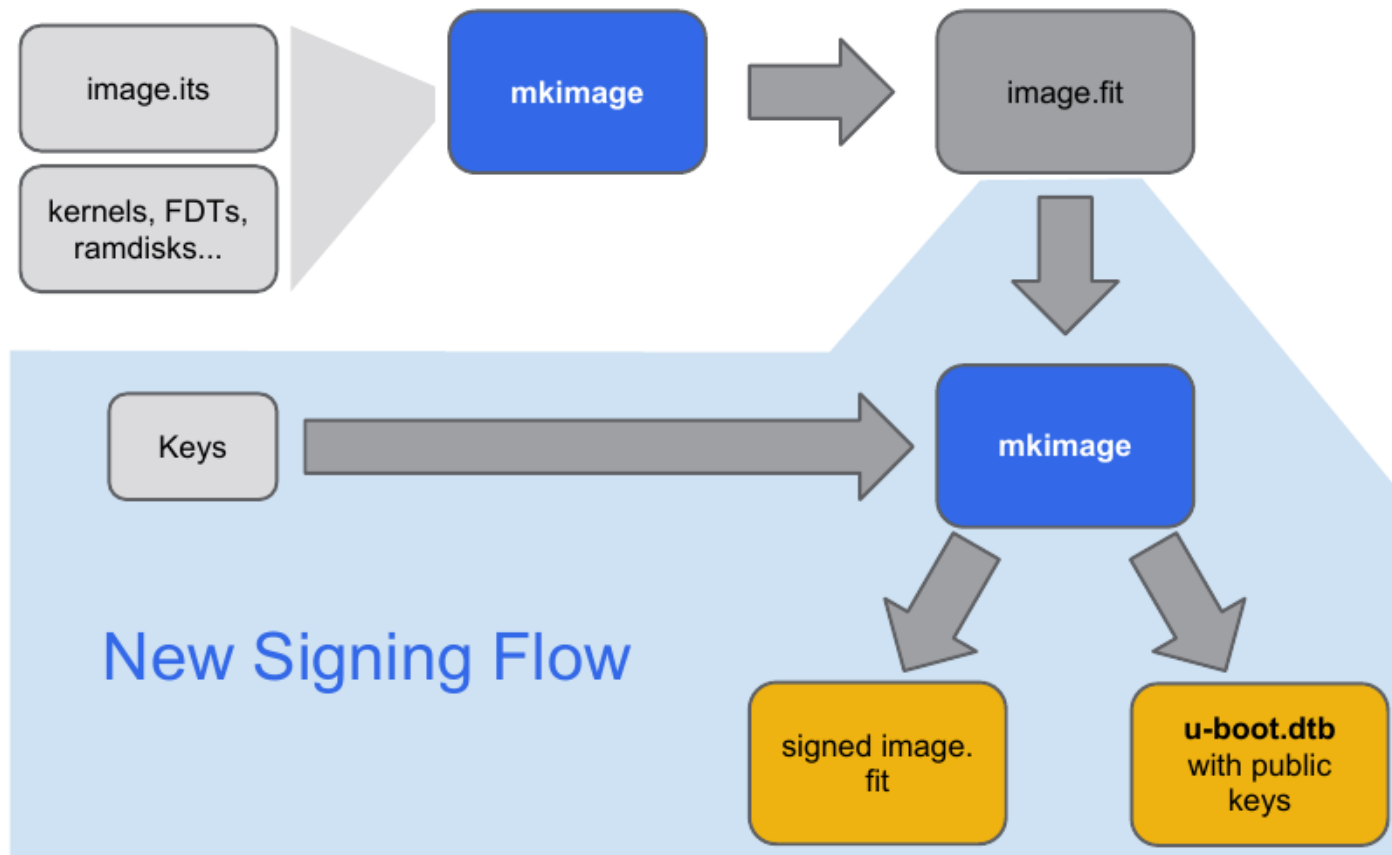


Critical application,
normal state

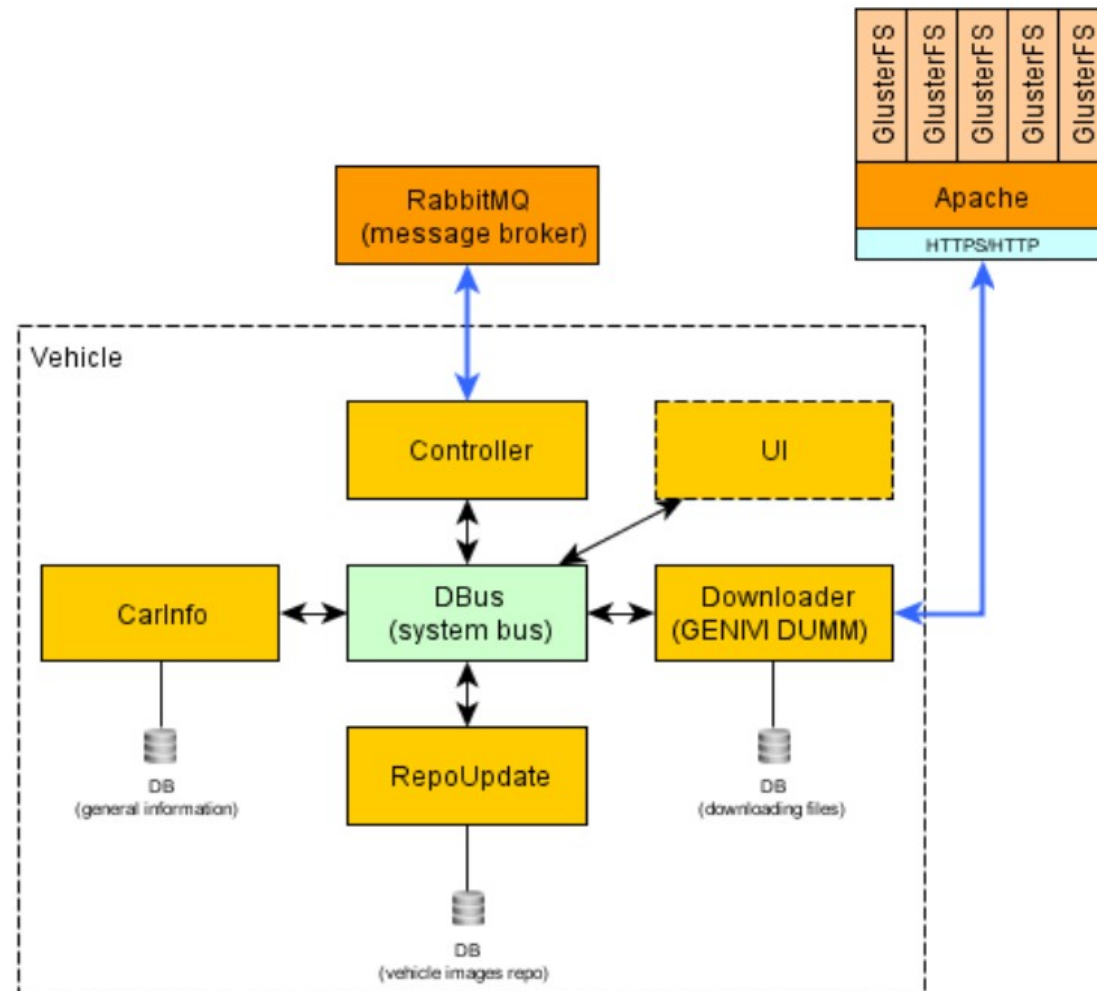


Industry Best Practice: ChromiumOS's [Verified Boot](#)

How signing works



Balances security with [software freedom](#).



Courtesy
GENIVI
and
Arynga

OCTOBER 27, 2015 | BY PARKER HIGGINS AND MITCH STOLTZ AND KIT WALSH AND CORYNNE MCSHERRY      

Victory for Users: Librarian of Congress Renews and Expands Protections for Fair Uses



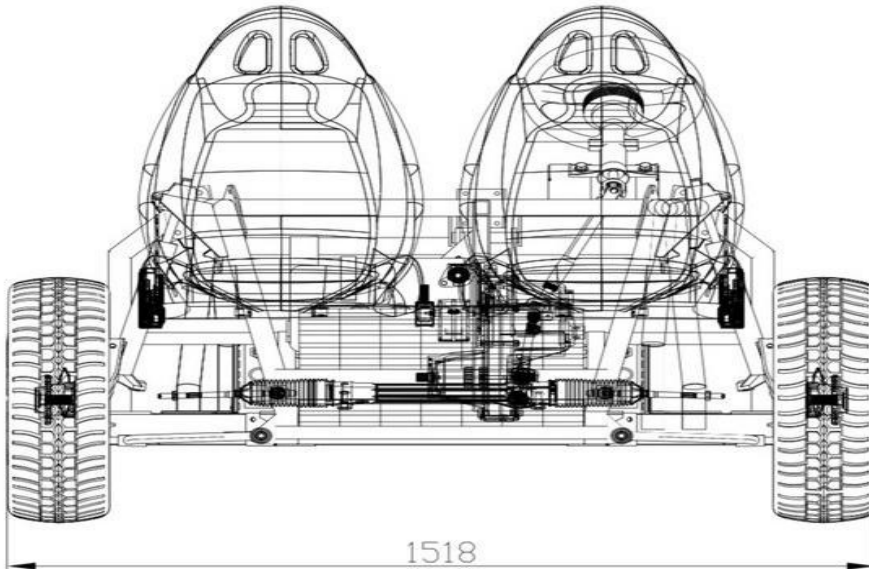
EFF wins automotive DMCA Section 1201 exemption

32c3 2015: F. Domcke reverse-engineers the VW-diesel cheat

Most exciting development of 2015: OSVehicle

TABBY EVO released in Open Source

Open Source: download for free
CC-Share-alike
Community can improve it



Summary

- Adding capability and automation inevitably increases 'attack surface.'
- The FCA-Harman-Sprint installation did not follow best practices.
- The industry as a whole is moving to OTA.
- Considerable open-source activity is underway.
- Traditional Linux security considerations apply equally to cars.

References

- [Smart Automotive](#) special issue of Telematics Wire
- Nate Willis, [“Linux and the Automotive Security Lab”](#)
- [“Dieselgate” and V2V communication](#) talks at 32c3 2015
- EPIC [“Internet of Cars” Congressional testimony](#), 11/18/2015
- [“Vehicle Forensics”](#) SchmooCon 2014
- [“Remote Vehicle Interaction,”](#) AGL meeting, 9/2015
- Ethernet A/V-B: [Junko Yoshida](#), EE Times
- [Automotive Grade Linux](#) and [GENIVI](#)
- General Motors' [kernel source](#)
- Freenode [#automotive](#) IRC
- I Am the Cavalry [Five Star Automotive Cyber Safety Framework](#)

Acknowledgements

Thanks to the following people for comments on, contributions to or support of (but not endorsement of) this presentation:

Dan Bartz, Mike Linksvayer, Roni Michaels, Linda Campbell, Charlie Vogelheim, Nate Cardozo, Andre Nakkurth, Julian Palau, Vinli, IBM Enterprise Security



extra slides



Hardware-level security on a device

- x86: **TPM**, IMA . . .
- ARM: Cortex-R, **TrustZone**
- Both ARM and x86 solutions have some Linux driver support

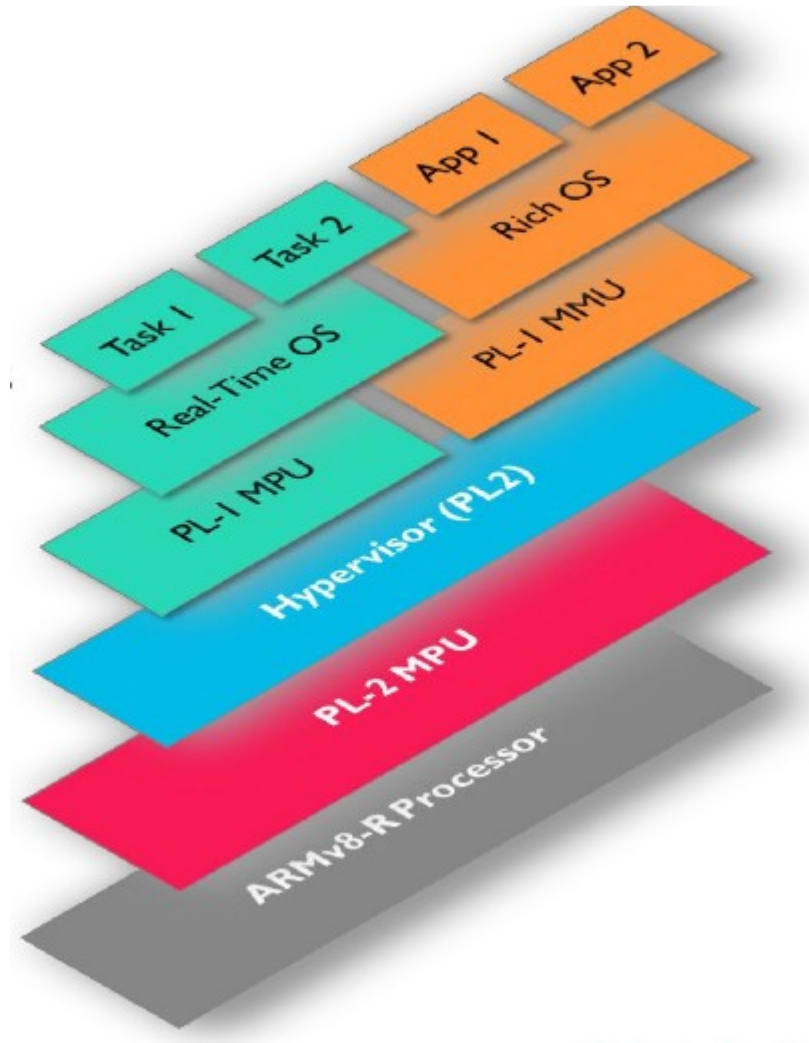
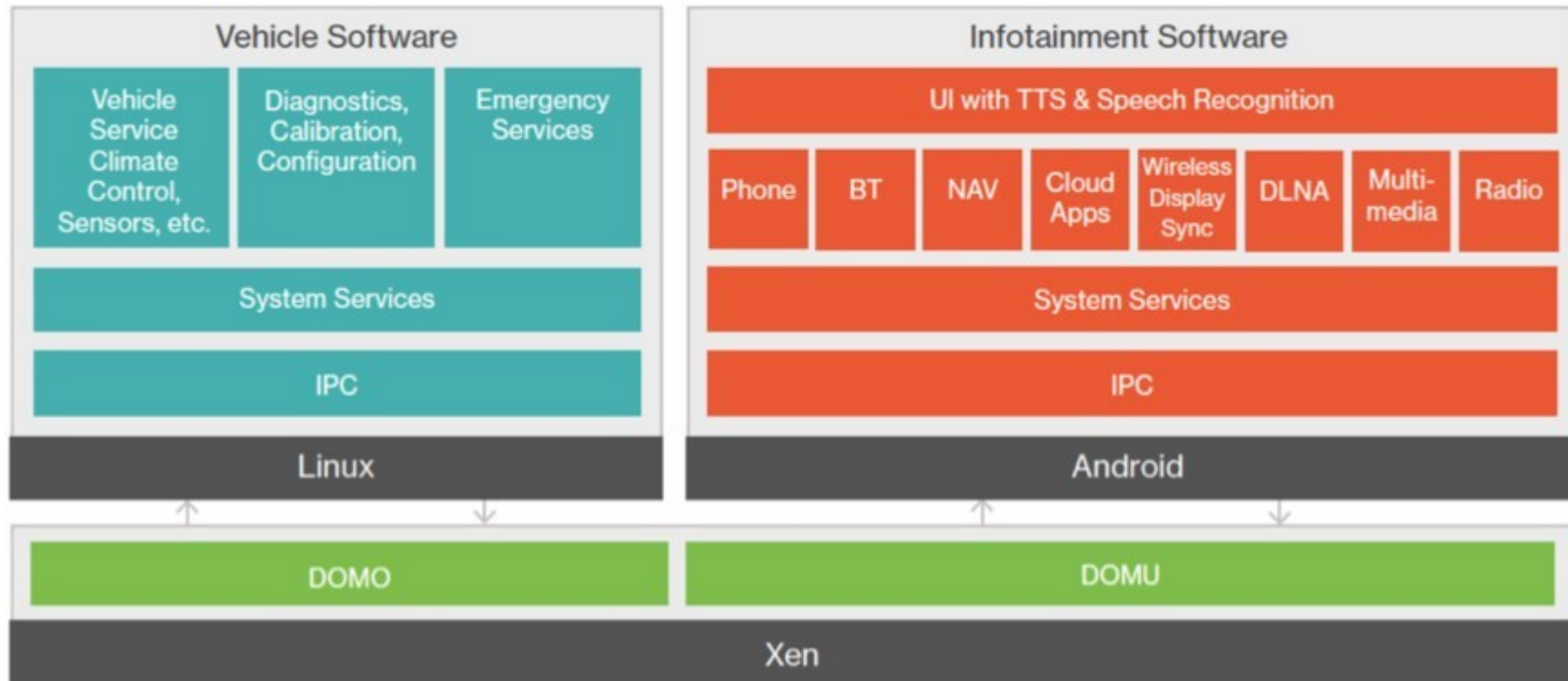


Image courtesy Chris Turner, ARM

Familiar problems, familiar solutions



DOM0 and DOMU run on different cores of a processor.

Global Logic: <http://tinyurl.com/ojnrbr2>

Driver drowsiness detection has great potential, but . . .

INTERIOR MONITORING WITH ACTIVE PERSONALIZATION

Interior Monitoring:

Monitor the driver's gaze direction, attention, drowsiness and emotion using a 2.3 mp camera module with IR illumination connected to FPGA processing FC.

🔦 Camera Point Tracking Algorithms

- Gaze Direction
- Eye Closure
- Blink Rate
- Head Tracking
- Yawn Detection
- Emotion Recognition

🔦 Holistic HMI



Active Personalization:

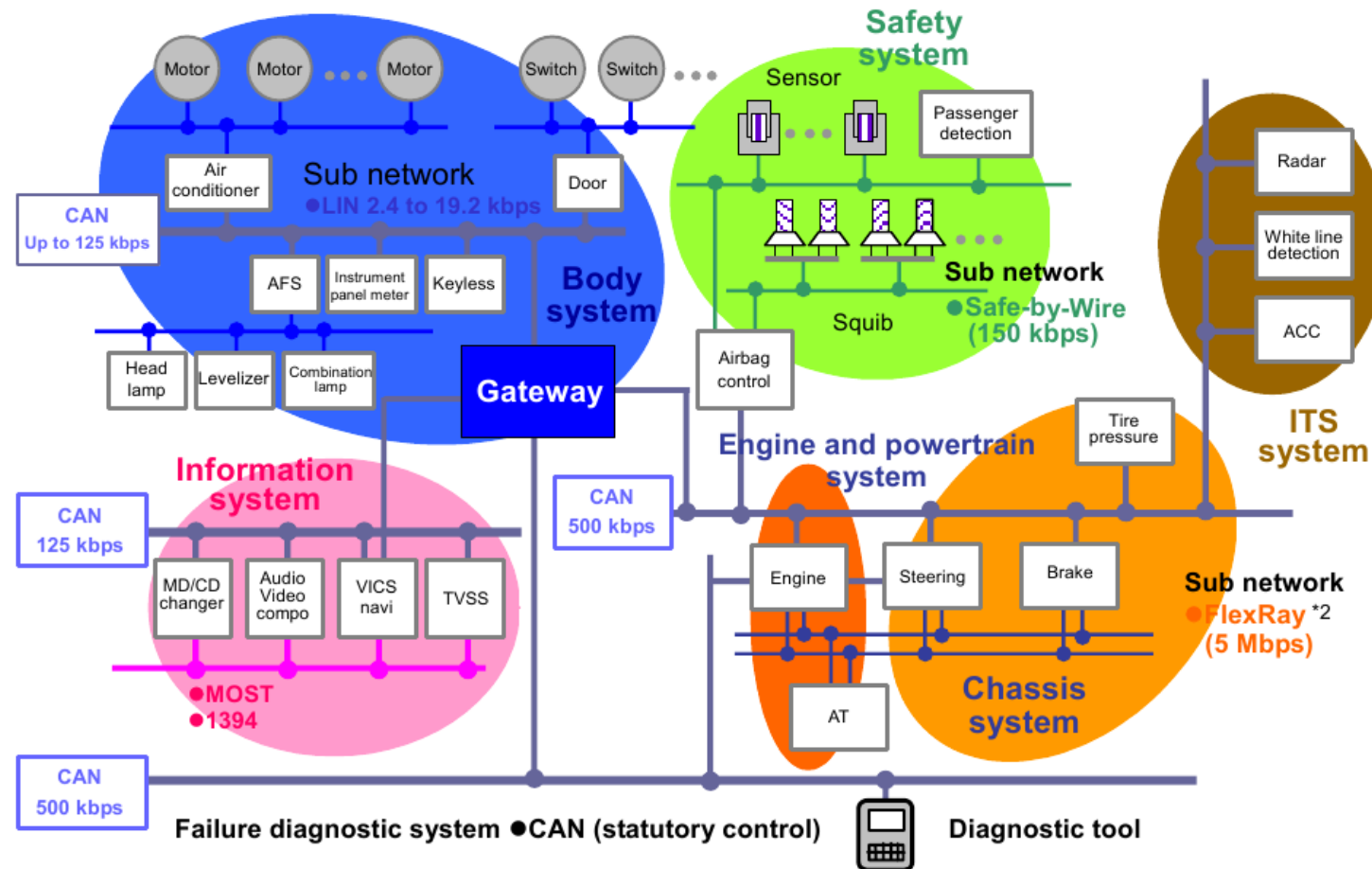
Vehicle preferences and customization is saved and automatically set when system identifies driver.

🔦 For Fun:

- Personal Profile
- Mobile, Infotainment and Comfort Presets
- Seat and Climate Presets
- Recommended Routes
- Better Routing and Incentives
- Text, Email and Social Reader



Automotive LAN, 2015



Copyright Renesas, "Introduction to CAN", with permission.

>100 microprocessors on MOST, CAN-FD, LIN, FlexRay networks

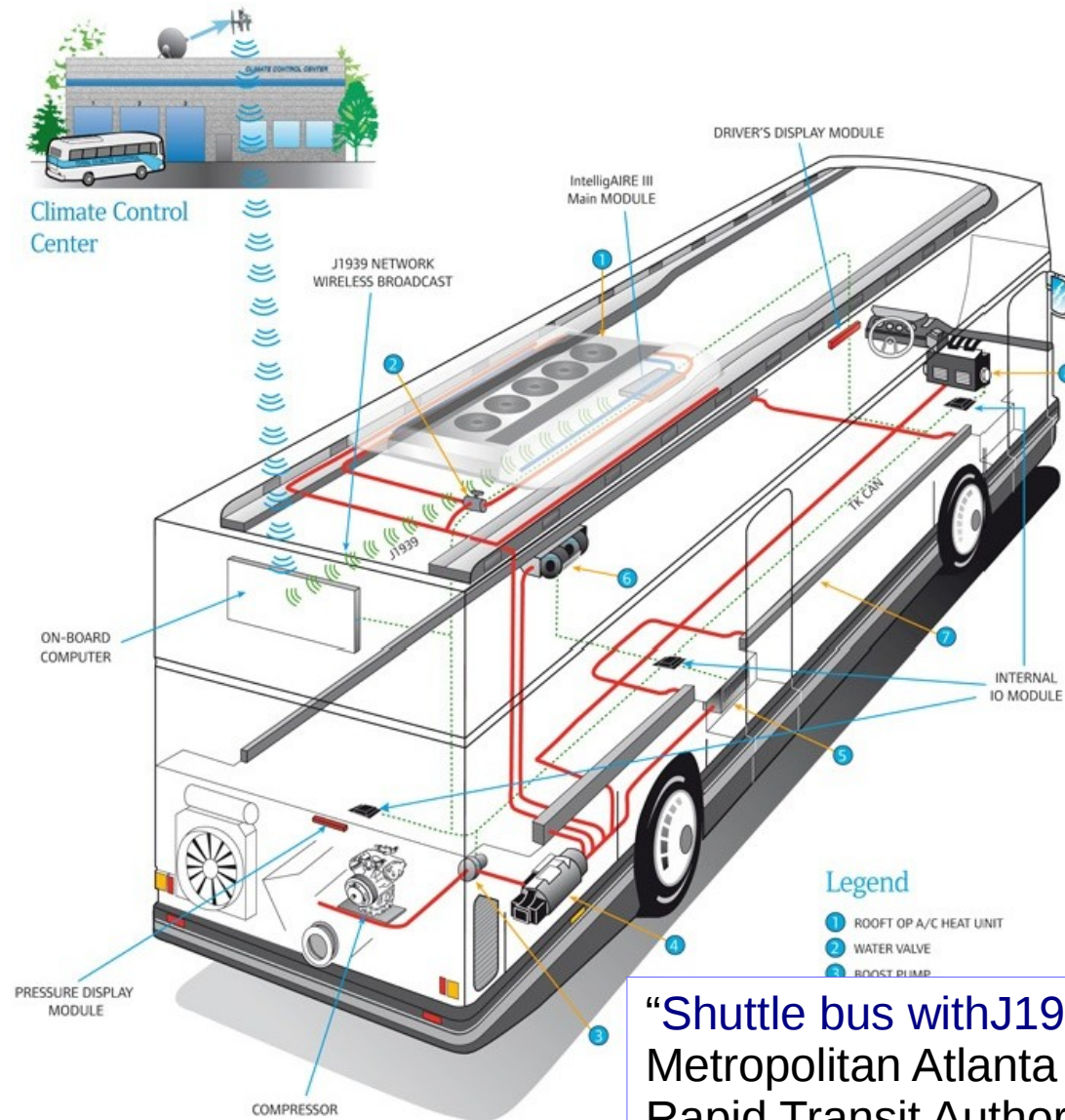
GPS Spoofing: Qihoo at Defcon

Try to spoof cars

- Demo video: The car, BYD Qin, was located in a lake center.



Connectivity may be a bad choice



“Shuttle bus with J1939 air conditioning,”
Metropolitan Atlanta
Rapid Transit Authority,
<http://can-newsletter.org>

The “Thermo King Intelligaire III”

Ambient Insecurity: the Internet of Threats


“Alternative Web browser-based user interface allows remote programming and status observation”
([Safetran Cobalt brochure](#))




Background: [Thinking Highways](#)


Open Street Map and [Ubuntu uNav](#)

This is an unofficial app viewer for Ubuntu Touch apps.










uNav GPS Navigation

★★★★☆  77
Marcos Costales
Free

 **INSTALL**

*Install will take you to the official appstore on an Ubuntu Touch device

Description Changelog Info Support

Map viewer & turn-by-turn GPS navigator for car, bike & walking

IMPORTANT:

- * You have to update your phone to OTA8 (released 15th November 2015).

FEATURES:

- * Map viewer and GPS navigator.
- * Powered by OpenStreetMap & Mapzen! You'll have the last map/routes updates on fly!
- * Car, bike or walk modes.
- * Avoid tolls.
- * Nearby POIs.
- * Works online (~10 km/~20 min = 2,5 MB).
- * For any country in the world.
- * 100% GPL and 100% based in libre projects.
- * turn-by-turn indicators with voice.
- * Unit: kilometers or miles.

Automotive pen-testing

Security conference

Save as PDF 

Tesla only partially hacked

Last week's Syscan-360 Security Conference in Beijing (China) posed a challenge: a prize of US\$ 10 000 was announced for anyone who managed to hack a Tesla. The prize money went unclaimed - none of the participants managed to meet all specifications set by the organizers.

ACCORDING TO THE SOUTH CHINA MORNING POST, 10 600 yuan were awarded to a white hat hackers team from Zhejiang University, which managed to exploit a “flow design flaw” of the Tesla model S to access the car's CAN network. They could “unlock the vehicle, sound the horn, and flash the lights, and open the sunroof.” All this was achieved while the car was in motion, but no team managed to hack the engine during the set timeframe.

CAN Industry Association newsletter, July 24, 2014

RISK ASSESSMENT / SECURITY & HACKTIVISM

GM embraces white-hat hackers with public vulnerability disclosure program

First major automaker (aside from Tesla) to issue guidelines promising not to sue researchers.

by **Sean Gallagher** - Jan 8, 2016 7:44am PST



General Motors

www.gm.com

[Profile](#)

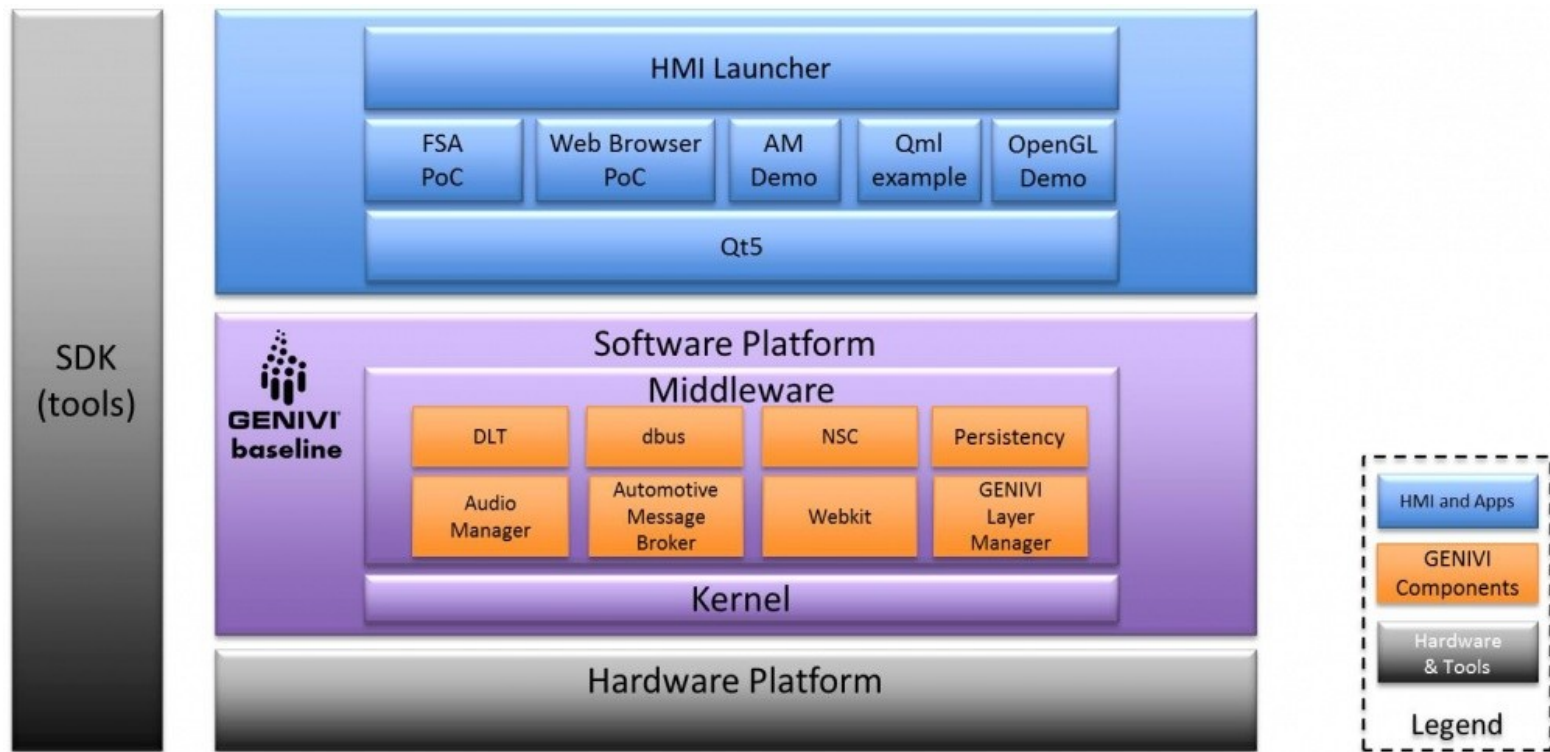
[Thanks](#)

Auto Security Products & Solutions

	Security Function	Company/Product
Cyber-Security Services	<ul style="list-style-type: none"> ▶ Security risk assessment ▶ Penetration testing ▶ Vulnerability assessment 	<ul style="list-style-type: none"> ▶ Cisco OpSec ▶ IOActive ▶ Many others
Hardware Security	<ul style="list-style-type: none"> ▶ Cryptographic processing ▶ Secure microprocessor 	<ul style="list-style-type: none"> ▶ Freescale microcomputers ▶ TI and others
Hypervisor Software	<ul style="list-style-type: none"> ▶ Protect at software boot-up ▶ OS & software isolation 	<ul style="list-style-type: none"> ▶ OpenSynergy, Mentor Graphics ▶ Green Hills & others
Over-the-air SW Update	<ul style="list-style-type: none"> ▶ Remote software update with built-in security 	<ul style="list-style-type: none"> ▶ Arynga ▶ Redbend
Apps Security Framework	<ul style="list-style-type: none"> ▶ Security framework for connected car apps 	<ul style="list-style-type: none"> ▶ Secunet Application Control Unit ▶ Others expected

Courtesy of IHS and E. Juliussen

GENIVI Demo Platform



Qemu image plus BSPs for RPi, Minnowboard, Nvidia Jetson and Renesas R-Car

A typical automotive data center



Source: [RTKL blog](#)

Chaos Computer Club 2012 video

Christie Dudley, Santa Clara University Law School

TALK/ID-5095

2.9-C/3

PRIVACY AND THE CAR OF THE FUTURE

CONSIDERATIONS FOR THE CONNECTED VEHICLE

CHRISTIE DUDLEY

<http://tinyurl.com/crbazg9>