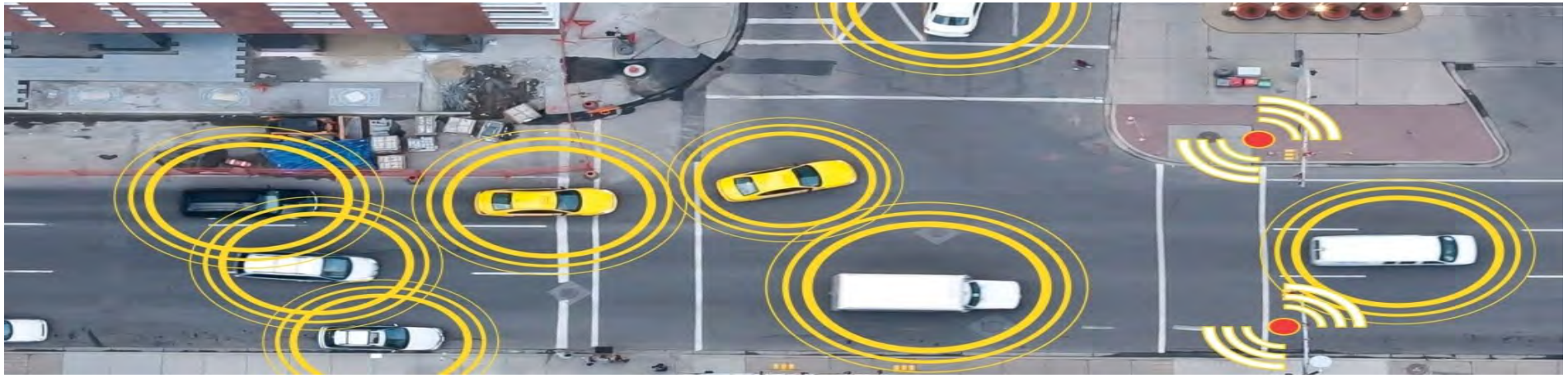
Connected Vehicles
Security, Privacy, and Economics



Alessandro Guarino
StudioAG

Privacy vs. Identity – EEMA 30th Annual Conference -London *5/7/2017*

The Speaker

15+ Years in Information/Cyber Security Consultancy

StudioAG
Consulting & Engineering

Speaker Author

Digital Forensics Alumni — 2011

CyCon International Conference on Cyber Conflict — 2013

ISSE 2016 — 2013-2016

E-PRIVACY XX — 2016

pirate security conference psc
IET Events The Institution of Engineering and Technology
Università di Roma Tor Vergata — 2017

Standards

UNINFO

CS·CG Cyber Security Coordination Group — CEN/CENELEC/ETSI

ETSI

cen CENELEC

2011 →

Introduction

Marketing notwhistanding, having permanently connected vehicles is not a good idea...

Privacy & Data Protection: has anyone given their consent when you bought your car?

(And still, modern cars are impressive (big) data generators)

Cybersecurity: not exactly considered among design parameters...

Figures

- According to an IHS report connected vehicles in 2022 will be 82.6 M, up from 13.8 M in 2013.
- (how long untill **all** vehicles are online?)

- "connected car systems will yield approximately $14.5 billion in revenue from automotive data [...] by 2020."

  IHS Automotive, 2013.

Enjeu

Where all this money is coming from?

"Big Data assets found in the connected car— *diagnostics, location, user experience/feature tracking, and adaptive driver assistance systems/autonomy...”*

- IHS

Data Wars

Winterkorn 2014 (@ VDA Congress):

"We seek connection to Google's data systems, but we still want to be the masters of our own cars,"

Or… data (and revenues) are our property (not Google's, and not the clients' either)

Traditional manufactures are very well aware of the economic value of big datasets.

Under the hood

Modern vehicles carry with them not one but several data networks, a veritable mini-internet on wheels

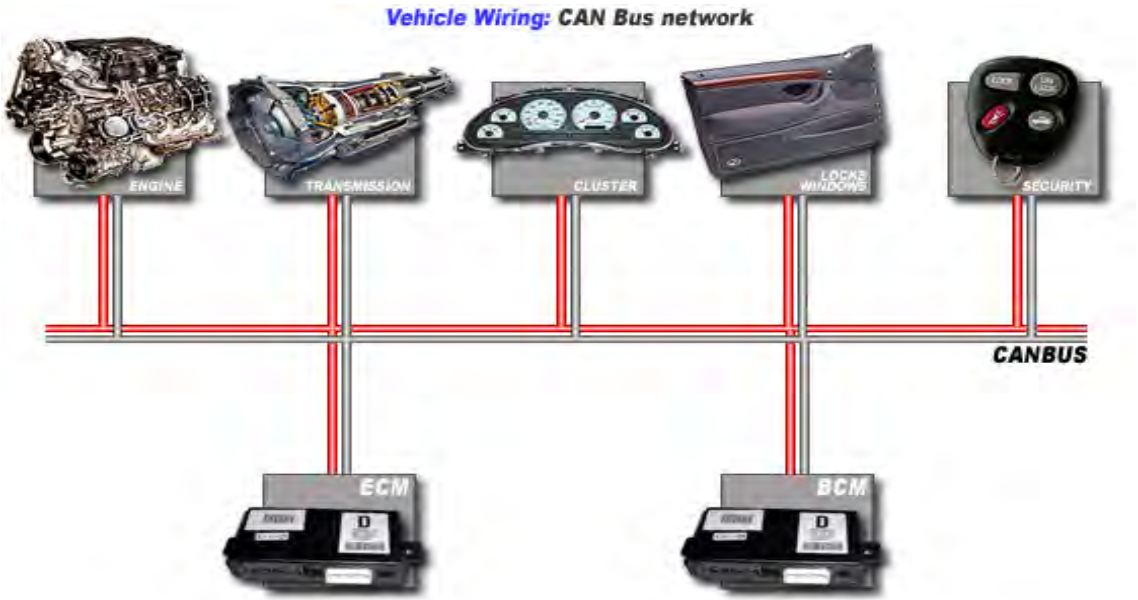
Connected vs. Autonomous – Autonomous vehicles do not need a permanent connection to work, but they will be as well.

Aside: much of what we are discussing applies to lorries, agriculturar machines, etc. even if those domains present some peculiar stakeholders and characteristics

Under the hood

CAN bus (controller area network)

Specialized bus for automotive applications CAN-C e CAN-IHS)

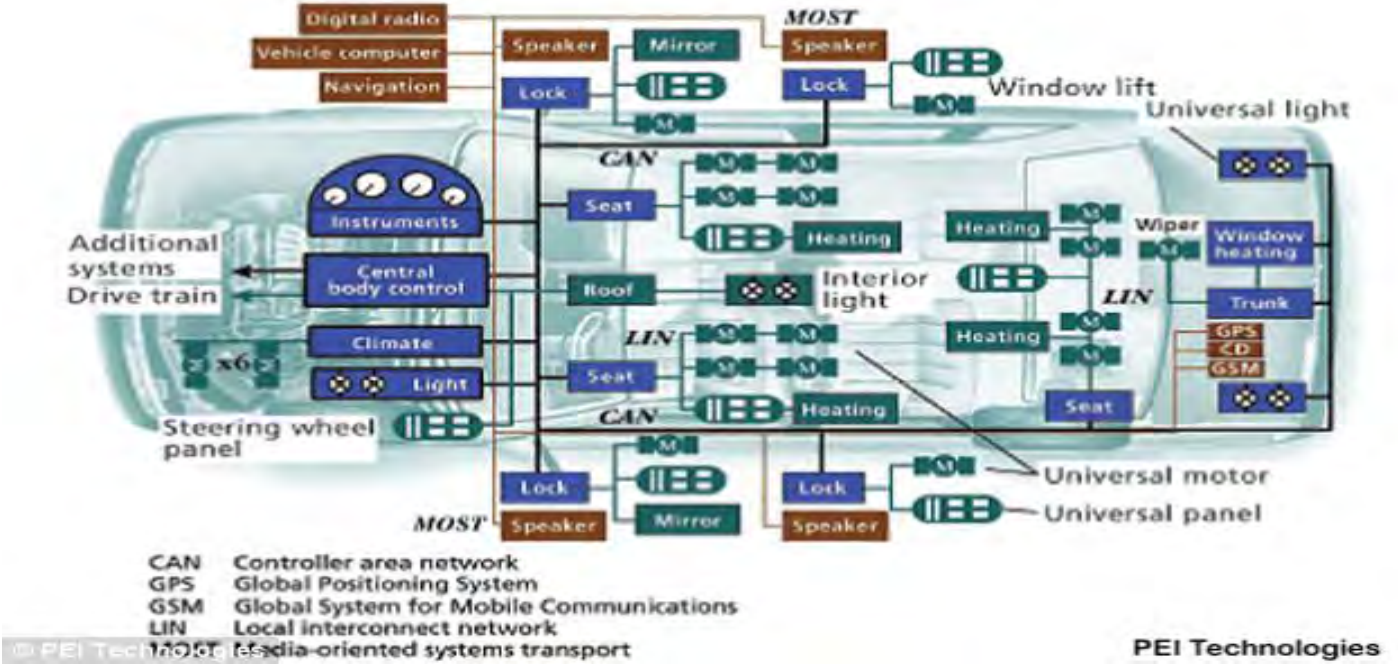


- Sensors and actuators
- Engine Control Module
- Body Control Module
- Interfaces and gateways

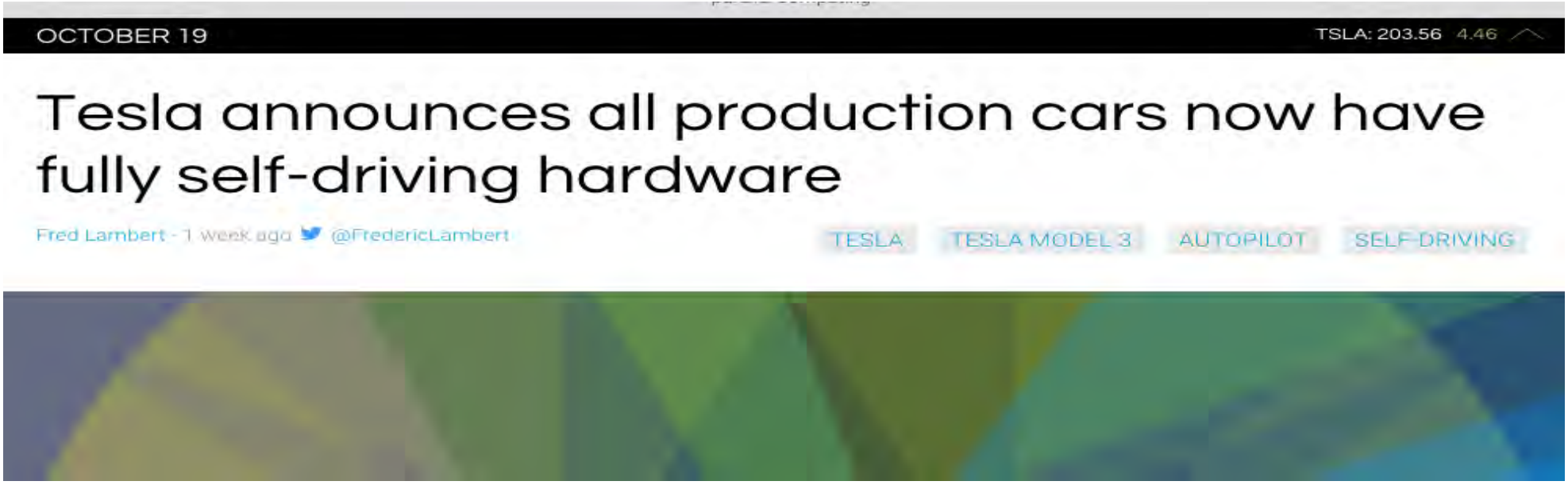
Credit: canbuskit.com

Under the hood

CANbus is the leading networking technology sensors, actuators, computing. Actuators can now control totally the vehicle and the gap with true autonomy is closing fast



Under the hood – Closing the Gap



Ways in...

- Infosec in vehicles relied traditionally on lack of physical access: OBD interfaces were the only access way (OBD is mandatory in Europe since 2001-2003, as EOBD).
- Now cheap OBD wireless dongles are easy to come by and can be accessed via app...
- USB ports.
- Short distance wireless:
  - Bluetooth / Wifi / Radio / Infrared
- Long range wireless:
  - LTE 4G Modem → 5G

Cyber Safety

Huge attack surface

No more need for access to the OBD port, being in the vicinity is enough, and not even that if the car is connected to the Internet...

Some critical points beside access:

- Hard / Impossible to update or patch software
- Lack of awareness – both of the user but from the designers as well (see infotainment systems connected to essewntial systems).

Cyber Safety

FCA Jeep Cherokee (1.4 Millon vehicles recalled in 2015)

- Radio connected to (both) CAN buses

- Uconnect (SO QNX) – connected both to critical systems and wifi/bluetooth interfaces


ANDY GREENBERG SECURITY 07.24.15 12:30 PM

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

Miller attempts to rescue the Jeep after its brakes were remotely disabled, sending it into a ditch. ANDY GREENBERG/WIRED

Beyond Safety

Mitsubishi Outlander PHEV Hybrid

- AP Wifi. Same password for all cars, and conveniently available in the manual...

- sssid simple formats allowed attacker to **geolocalize** every car (through "*crowdsourced wardriving*" services)

- Once inside the internal network it was possible to reverse engineering the message protocol used by the app and… turn off the alarm, among other things...

Beyond Safety

Nissan Leaf

– App “Nissan Connect”

- VIN Number was enough for authentication

- And you can find it…

(Big) Data

Raw Data: rpm, distribution, fuel level, instant speed, acceleration, GPS position, water temp, engine power, fuel pressure, oil pressure, oil level, tire pressures, throttle position, temperatures, instant torque, steering angle, turbo position…

Calculated Values: fuel consumption, mean speed, mean acceleration, code violations (speed + GPS), “driving style”

Others: phone cells, dash cam videos, music preferences...

Control & Controllers

Who controls the use of these data?

A whole lot of stakeholders...

VDA Principles (2014):

- Vehicle-related data: the manufacturer.

- Personal Data (address, usage, infotainment): the user.

- Infotainment and maintenaince data should be subject to deletion by the user.

Control & Controllers

Consent mechanism is clearly inadequate for cars and almost always services are not available if consent is not given.

Blurred lines between personal data and simple technical data.

Stakeholder 1/6

Not so brief list of actors involved

- Owner, driver (may bot be the same person)
- Manufacturer
- Insurance companies and experts
  - Fees based on driving style
  - Damages evaluation and incident reconstruction

Stakeholder 2/6

- Leasing companies
- Governments, government agencies, and the EU
  - Tax agencies – Interested in the owner, the vehicle and its use (personal or work)
  - Other administrations
  - eCall. Data actually used and transmitted, another connection not accessible to the user

Stakeholder 3/6

- The Police
  - Accident Reconstruction
  - The car as a witness (against the driver in some cases). Data are seen by the Courts as “objective”, more realiable than human witnesses. e.g. GPS, accelerometers, speed, seat and belts sensors...
  - Can you refuse access?

Stakeholder 4/6

- Fire Brigade, EMTs, rescuers, hospitals and health
  - Interesested to number of people involved (seats) and gravity (belts on or off)
- Legal system
  - Lawyers, Courts, Expert Witnesses
- All suppliers of services connected to cars.

Stakeholder 5/6

- Employers and fleet managers
- Road assistance
  - raw data useful in order to make repairs on the road
  - trasmission to other subjects
- Rental companies
- Car sharing

Stakeholder 6/6

- Taxi companies
- Repair shops
  - Independent and in-house
  - Integration with personal data in possess of the manufacturers...
  - Body shops

The Economics

- The automotive sector is undergoing a deep trasnformation
- Entry barriers are lower, the boundaries are blurred: spaces and opportunities for new actors
- High innovation rate, shorter development cycles, new technologie
- Moblity itself is changing
  - New models of ownership
  - Integrated systems (ITSs)
- Laws and regulations

Open Issues...

...for privacy and data protection

- Classification, consent
- Necessity and Proportionality
- Seemingly irrelevant or non-personal data con be used for individual profiling
- Personal data (places, journeys, phone calls etc)
- Hard to individuate the controller and processors
- Retention and disposal
- Different jurisdictions fracture the market (EU GDPR Vs. Non-EU)

Open Issues...

...for safety and security

- Convenience over security, when it comes to vehicles it's dangerous for your physical well-being.
- Economic mechanisms that operate against information security. Hard to solve (security & safety by design)
- Standards and regulations

Security – Possible Solutions

- Design software with fail modes from the ground up, incorporate hardware failsafe systems
- Manual override (it should be always possible to ovverride the automation)
- Authentication! (at least for driving systems)
- Air-gapping critical systems

And Privacy?

- Simpler privacy policies
- Better control of the data, functions to delete / manage data, even for technical telemetry
- Vertical regulations for data protection
- Actually, very little to do when the main stakeholder is the state (or the Union)

Thanks for Your Time.
Questions?

Contacts:

a.guarino@studioag.eu

 **@alexsib17**

Slides online on:
www.studioag.pro

StudioAG – Consulting & Engineering
www.studioag.eu