CYBERSECURITY OF THE CONNECTED VEHICLES

Antoine Boulanger

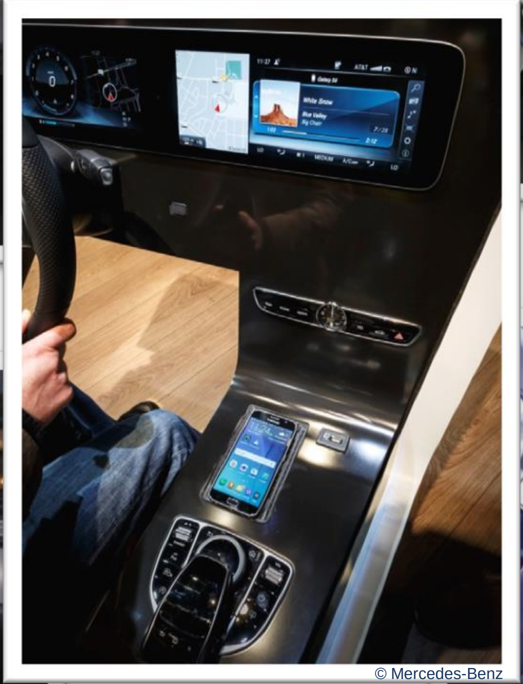
PSA GROUPE

RESEARCH & DEVELOPMENT

FUTURE CARS : CONNECTED !

- CES Las Vegas: the new Auto Show !

© Audi



© Mercedes-Benz

© BMW

© Ford

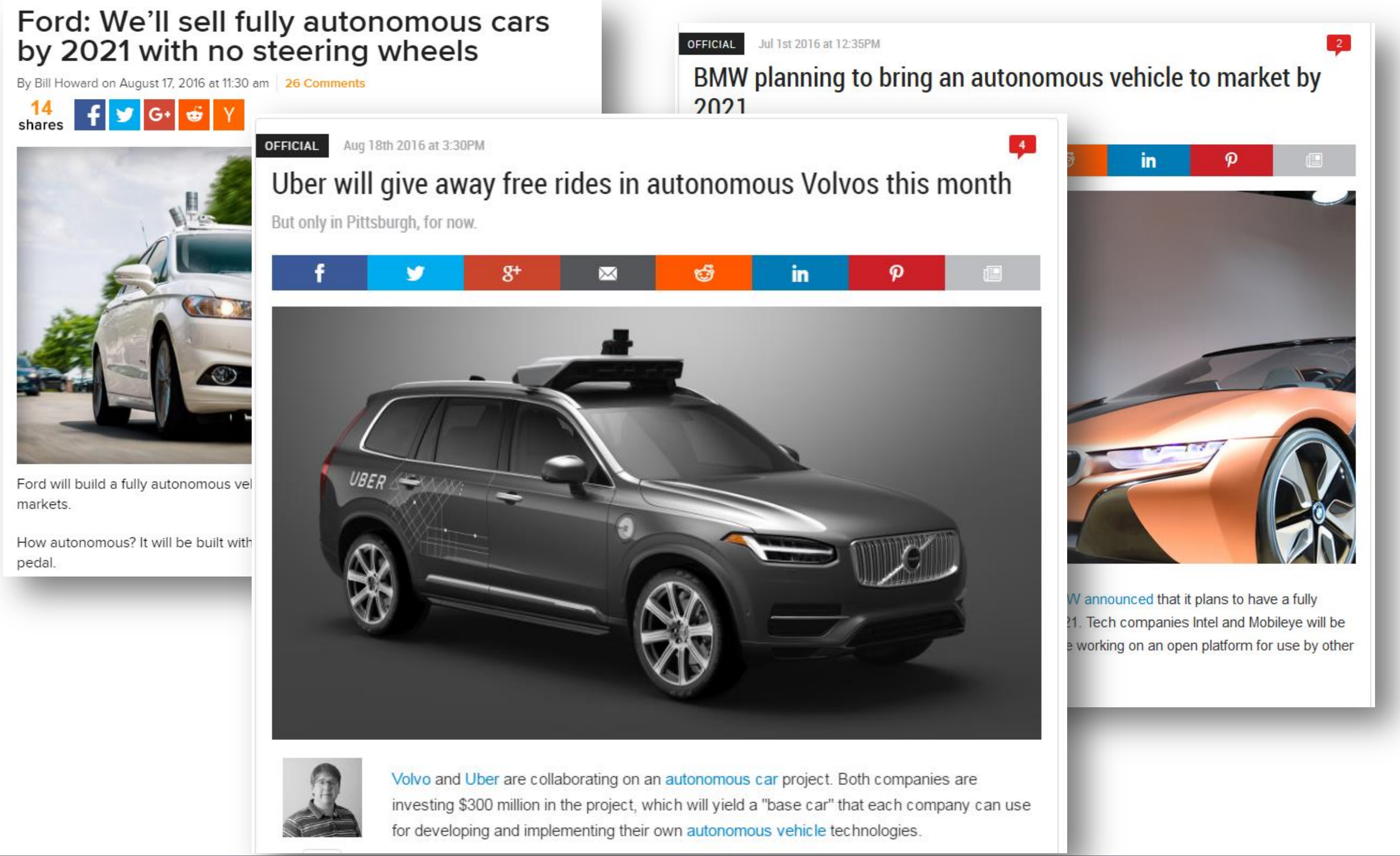
© VW

© Ford

CAR CONNECTED SERVICES

- SOS (e-call) and assistance (b-call)
- Remote diagnostics
- Maintenance monitoring
- Car location (car park) & tracking (theft)
- Car sharing & fleet management
- Connected navigation (traffic, hazards, gas stations with prices, car parks…)
- E-mailing and texting
- Social network
- Weather forecast, news
- Streaming music, audio book
- Software update
- …

FUTURE CARS : AUTONOMOUSLY DRIVING !



Ford: We'll sell fully autonomous cars by 2021 with no steering wheels

By Bill Howard on August 17, 2016 at 11:30 am | 26 Comments

14 shares

Ford will build a fully autonomous vel
markets.

How autonomous? It will be built with
pedal.

OFFICIAL Jul 1st 2016 at 12:35PM

BMW planning to bring an autonomous vehicle to market by 2021

W announced that it plans to have a fully
21. Tech companies Intel and Mobileye will be
e working on an open platform for use by other

OFFICIAL Aug 18th 2016 at 3:30PM

Uber will give away free rides in autonomous Volvos this month

But only in Pittsburgh, for now.

Volvo and Uber are collaborating on an autonomous car project. Both companies are investing $300 million in the project, which will yield a "base car" that each company can use for developing and implementing their own autonomous vehicle technologies.

TODAY CARS: AUTOMATED FEATURES

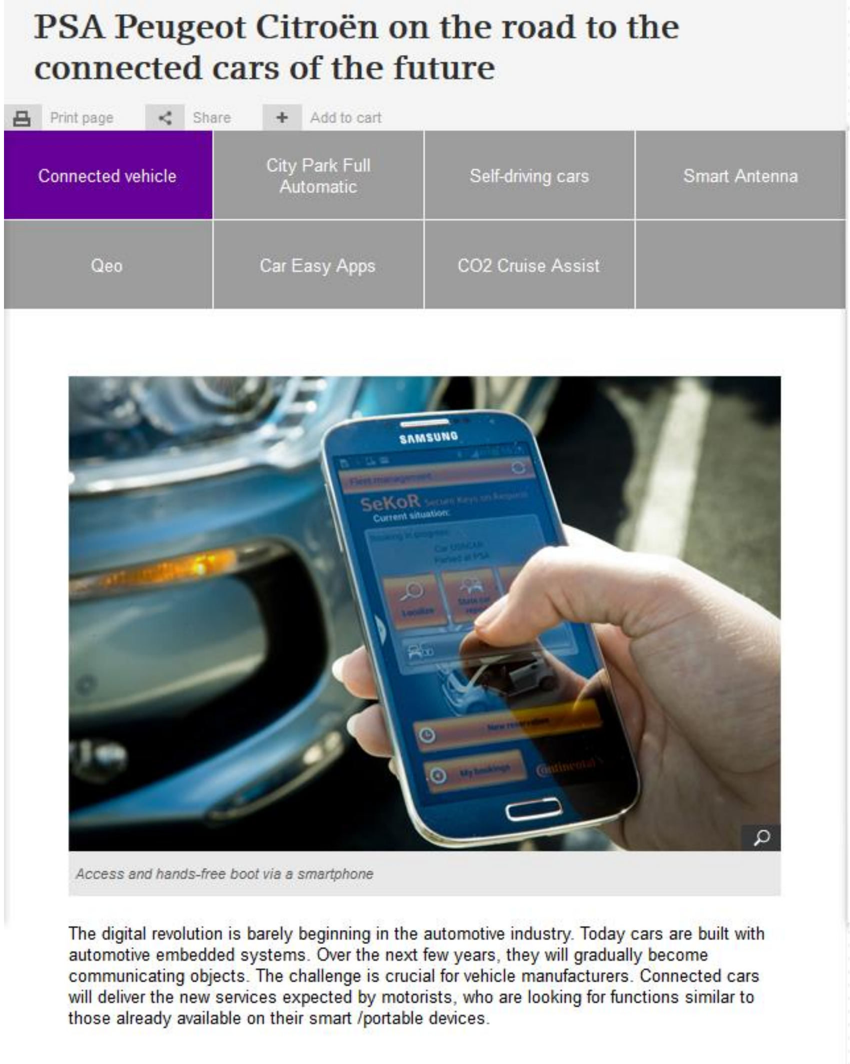
© Audi

© Citroën

© Audi

© Volvo

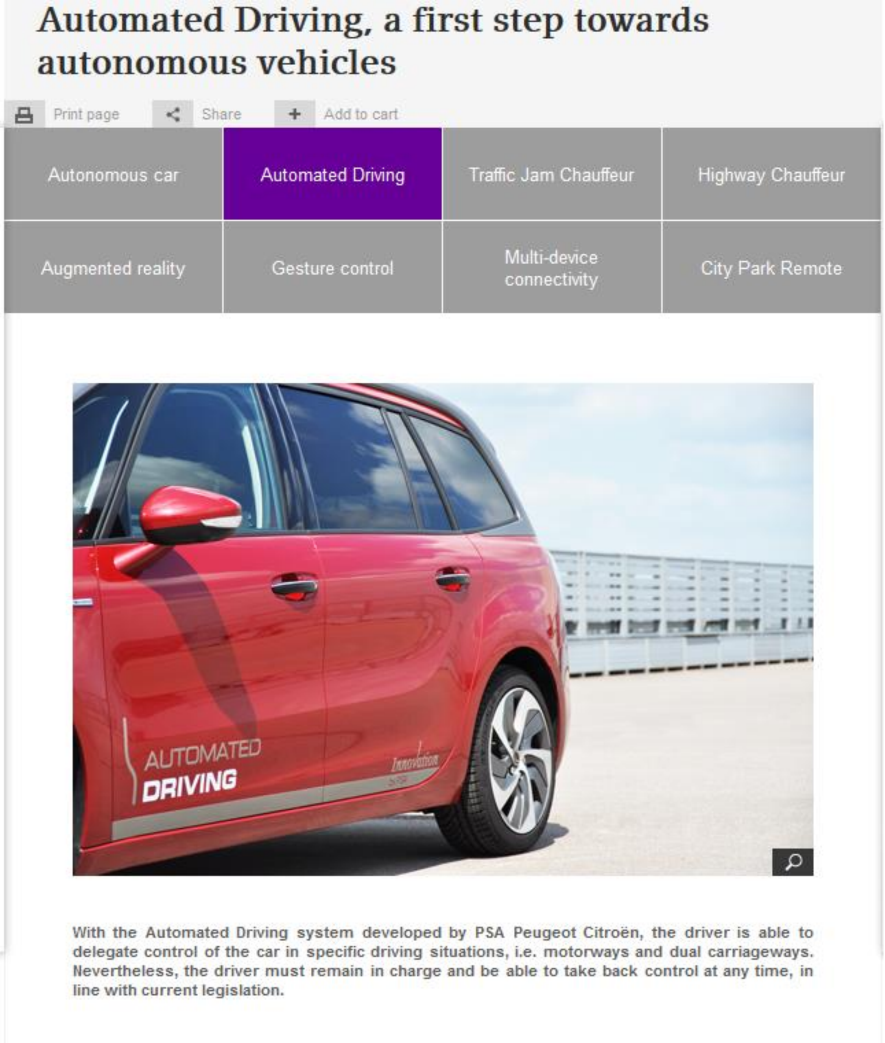
PEUGEOT, CITROËN ,DS CARS TOO



PSA Peugeot Citroën on the road to the connected cars of the future

Access and hands-free boot via a smartphone

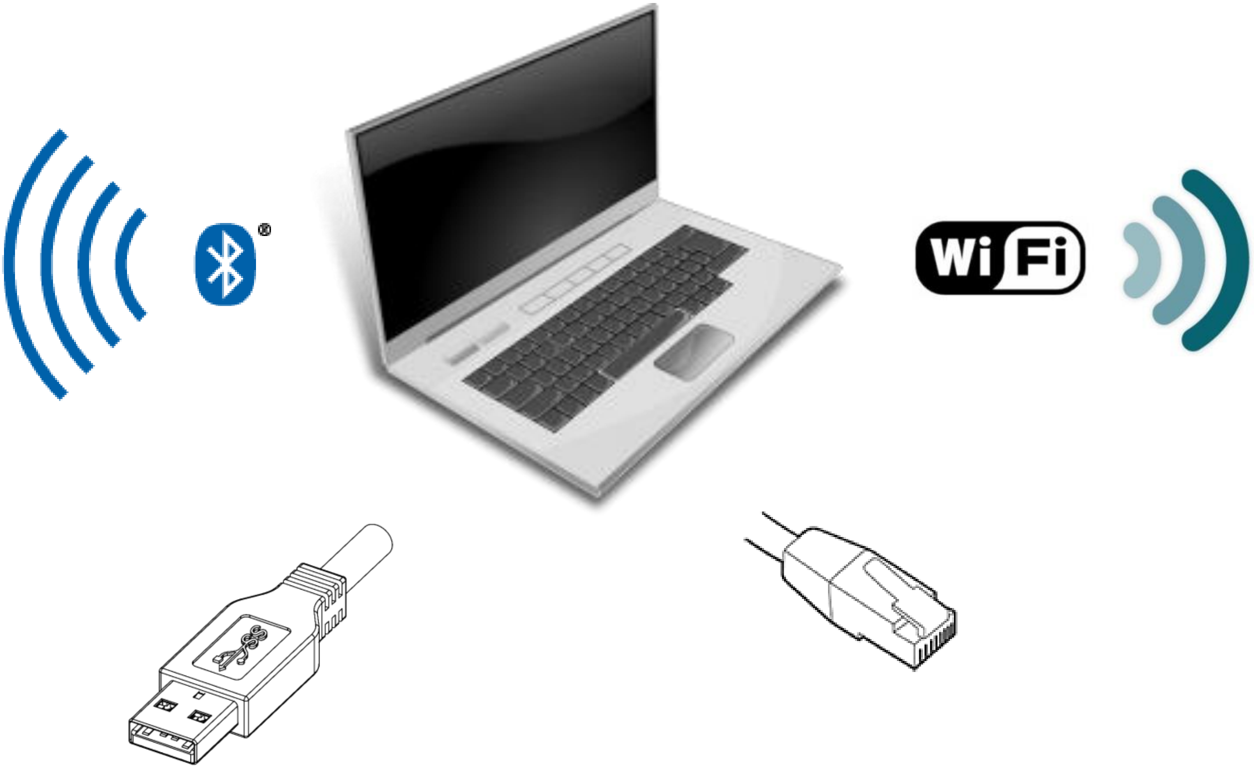
The digital revolution is barely beginning in the automotive industry. Today cars are built with automotive embedded systems. Over the next few years, they will gradually become communicating objects. The challenge is crucial for vehicle manufacturers. Connected cars will deliver the new services expected by motorists, who are looking for functions similar to those already available on their smart /portable devices.



Automated Driving, a first step towards autonomous vehicles

With the Automated Driving system developed by PSA Peugeot Citroën, the driver is able to delegate control of the car in specific driving situations, i.e. motorways and dual carriageways. Nevertheless, the driver must remain in charge and be able to take back control at any time, in line with current legislation.

HOW MUCH IS THE CAR CONNECTED ?



HOW MUCH IS THE CAR CONNECTED ?

GSM
3G
Lte
Wi Fi
NFC

HOW MUCH IS THE CAR CONNECTED ?

802.11p - ITS G5
V2x communications

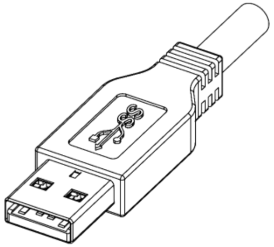
GSM 3G

Lte

Bluetooth

Wi Fi

NFC



On-Board Diagnostics

THE USER CAN IMPROVE THE CAR CONNECTIVITY (USB & BT)

MirrorLink

Apple CarPlay

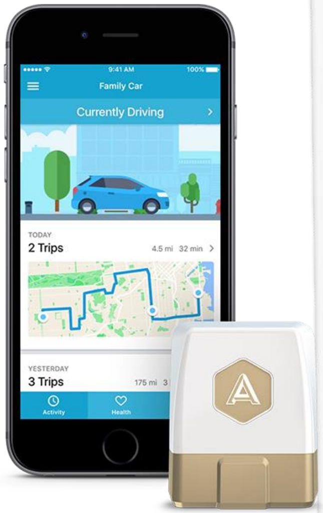
android auto

Considered as secured

THE USER CAN IMPROVE THE CAR CONNECTIVITY (OBD2)

Self diagnostics

And much more apps !



9:41 AM 100%

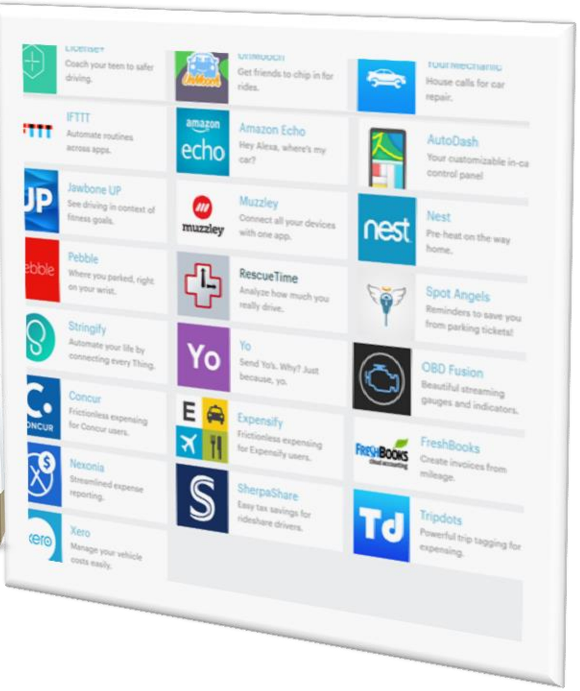
Family Car

Currently Driving >

TODAY
2 Trips 4.5 mi 32 min >

YESTERDAY
3 Trips 175 mi 3

Activity Health



License+
Coach your teen to safer driving.

IFTTT
Automate routines across apps.

Jawbone UP
See driving in context of fitness goals.

Pebble
Where you parked, right on your wrist.

Stringify
Automate your life by connecting every Thing.

Concur
Frictionless expensing for Concur users.

Nexonia
Streamlined expense reporting.

Xero
Manage your vehicle costs easily.

Urbmooch
Get friends to chip in for rides.

Amazon Echo
Hey Alexa, where's my car?

Muzzley
Connect all your devices with one app.

RescueTime
Analyze how much you really drive.

Yo
Send Yo's. Why? Just because, yo.

Expensify
Frictionless expensing for Expensify users.

SherpaShare
Easy tax savings for rideshare drivers.

YourMechanic
House calls for car repair.

AutoDash
Your customizable in-ca control panel

Nest
Pre-heat on the way home.

Spot Angels
Reminders to save you from parking tickets!

OBD Fusion
Beautiful streaming gauges and indicators.

FreshBooks
Create invoices from mileage.

Tripdots
Powerful trip tagging for expensing.

« Pay-how-you-drive » insurance

Much less secured !

HACKING CARS

[2013] Miller & Valasek managed to take control of the steering and brakes by connecting directly to the on-board network (Toyota Prius & Ford Escape).

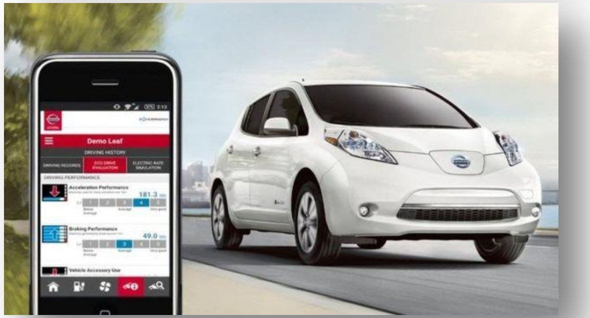
[2014] Students hack Tesla Model S, make all its doors pop open in motion.

[2015] ADAC found out that the communication link was not secure (http~~s~~) and was able to send remote door unlocking instructions.

[2015] Miller & Valasek managed to remotely take control of some features (A/C, infotainment, engine, brakes, steering) of the Jeep Cherokee.

[2015] UCSD researchers managed to take control of the brakes of a Corvette, through an insurance OBD2 dongle.

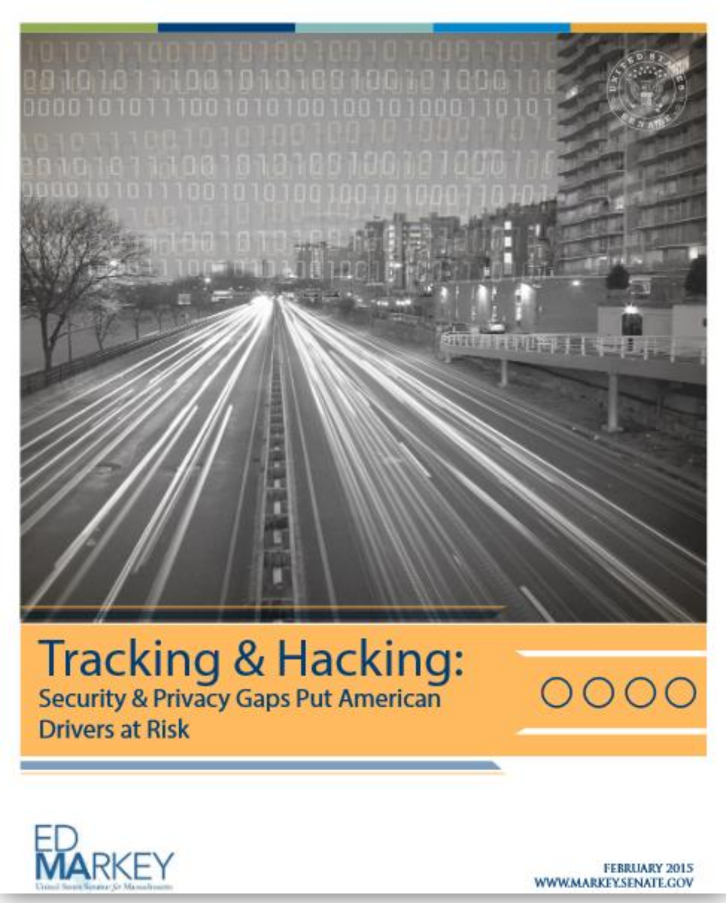
[2016] Hunt discovered that it was possible to remotely control the AC/heating of any Nissan Leaf used with NissanConnect EV app.



HACKING CARS

[2016-09-20] Chinese researchers were able to wirelessly (over WiFi) attack a Tesla Model S and gain control over some of its internal electronic components including the car’s brakes.

(U.S.) AUTHORITIES ARE TACKLING THE TOPIC

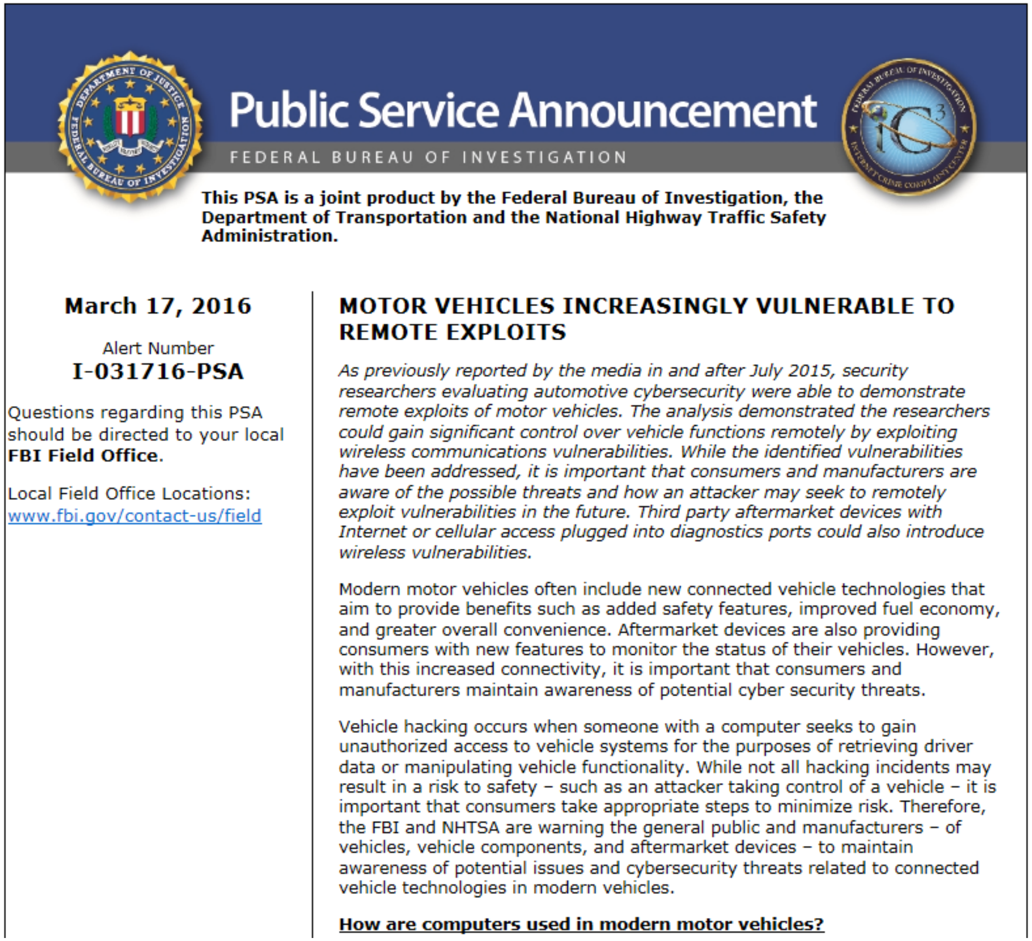


Tracking & Hacking:

Security & Privacy Gaps Put American Drivers at Risk

ED MARKEY

FEBRUARY 2015
WWW.MARKEY.SENATE.GOV



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

This PSA is a joint product by the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration.

March 17, 2016

Alert Number
I-031716-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field

MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS

As previously reported by the media in and after July 2015, security researchers evaluating automotive cybersecurity were able to demonstrate remote exploits of motor vehicles. The analysis demonstrated the researchers could gain significant control over vehicle functions remotely by exploiting wireless communications vulnerabilities. While the identified vulnerabilities have been addressed, it is important that consumers and manufacturers are aware of the possible threats and how an attacker may seek to remotely exploit vulnerabilities in the future. Third party aftermarket devices with Internet or cellular access plugged into diagnostics ports could also introduce wireless vulnerabilities.

Modern motor vehicles often include new connected vehicle technologies that aim to provide benefits such as added safety features, improved fuel economy, and greater overall convenience. Aftermarket devices are also providing consumers with new features to monitor the status of their vehicles. However, with this increased connectivity, it is important that consumers and manufacturers maintain awareness of potential cyber security threats.

Vehicle hacking occurs when someone with a computer seeks to gain unauthorized access to vehicle systems for the purposes of retrieving driver data or manipulating vehicle functionality. While not all hacking incidents may result in a risk to safety – such as an attacker taking control of a vehicle – it is important that consumers take appropriate steps to minimize risk. Therefore, the FBI and NHTSA are warning the general public and manufacturers – of vehicles, vehicle components, and aftermarket devices – to maintain awareness of potential issues and cybersecurity threats related to connected vehicle technologies in modern vehicles.

How are computers used in modern motor vehicles?

…and consider a regulation for the cybersecurity in the cars.

GOOD NEWS ! CAR MANUFACTURERS HAVE BEEN TACKLING IT TOO !

- Cybersecurity experts in the development teams
- Cybersecurity training for developers and project managers
- Development methods and processes adapted to cybersecurity
- Cybersecurity risk analysis and requirements from the early phases of development
- Cybersecurity statements in project milestones
- Penetrations tests
- Threat Intelligence
- Bug bounties
- Work to strenghten the current and future in-vehicle electronic architectures/networks

TECHNICAL SOLUTIONS AT DIFFERENT LEVELS

- Security monitoring
  - Security Operational Center
- Telematics & Infotainment
  - Virtualisation (hypervisor)
  - Encryption & authentication of external communications
- In-vehicle electronic architecture
  - Sub-networks isolation
  - Internal and external firewall
  - Authentication of in-vehicle communications
  - Intrusion Detection/Protection Systems
  - SW update Over-the-air
- ECUs
  - ECU hardening (remove or disable unused ports & services)
  - Hardware Security Module, Trusted Execution Environment for secure boot, secure storage, secure execution environment.

COMMON WORKS

Security is not considered as a competitive differentiating feature. Automotive manufacturers and suppliers are working together to improve the security.

- Research partnerships
  - European projects: EVITA, PRESERVE, SEVECOM, …
  - IRT SystemX – France (projects ELA, ISE, CTI)

- Standardisation
  - Development methodology including security activities
  - Security evaluation criteria
  - Security of the V2x communications

ISO/TC 22/SC 32

CONCLUSION

- All the future cars will be connected, most of them will have automated features

- The combination of extended car connectivity and automation makes possbile hacks, which can sometimes be spectacular.

- Authorities are tackling the topic, working on regulation.

- Car manufacturers have been working hard to improve car security, internally and also through partnerships with other manufacturers.

antoine.boulanger@mpsa.com

in Antoine Boulanger

THANK YOU !

PSA
GROUPE