Car hacks 101

- An overview of noticed automotive (in)security cases 2010-2016

Image source: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

>whoami

- M.Sc. Computer Science & Engineering Chalmers
- In the IT industry since 2001
  - Ericsson, Accenture, **Volvo Cars**
- IT Security @ Volvo Cars
- Security enthusiast
- OWASP Göteborg leader
- Speaker

OWASP
Gothenburg Göteborg

https://www.linkedin.com/in/andersrosdahl/

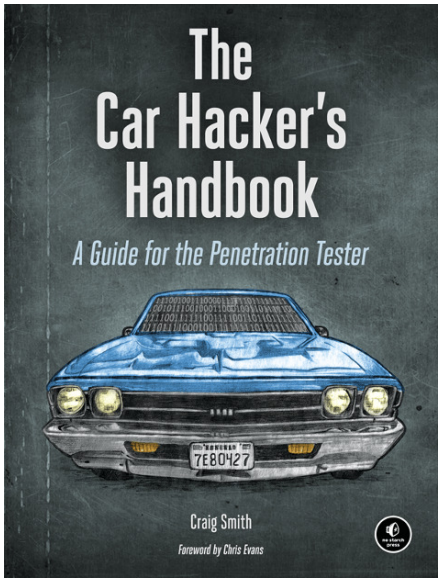
twitter: @rosdahl

mail: anders.rosdahl@volvocars.com

Car hacking – buzz?

“No need for panic…”

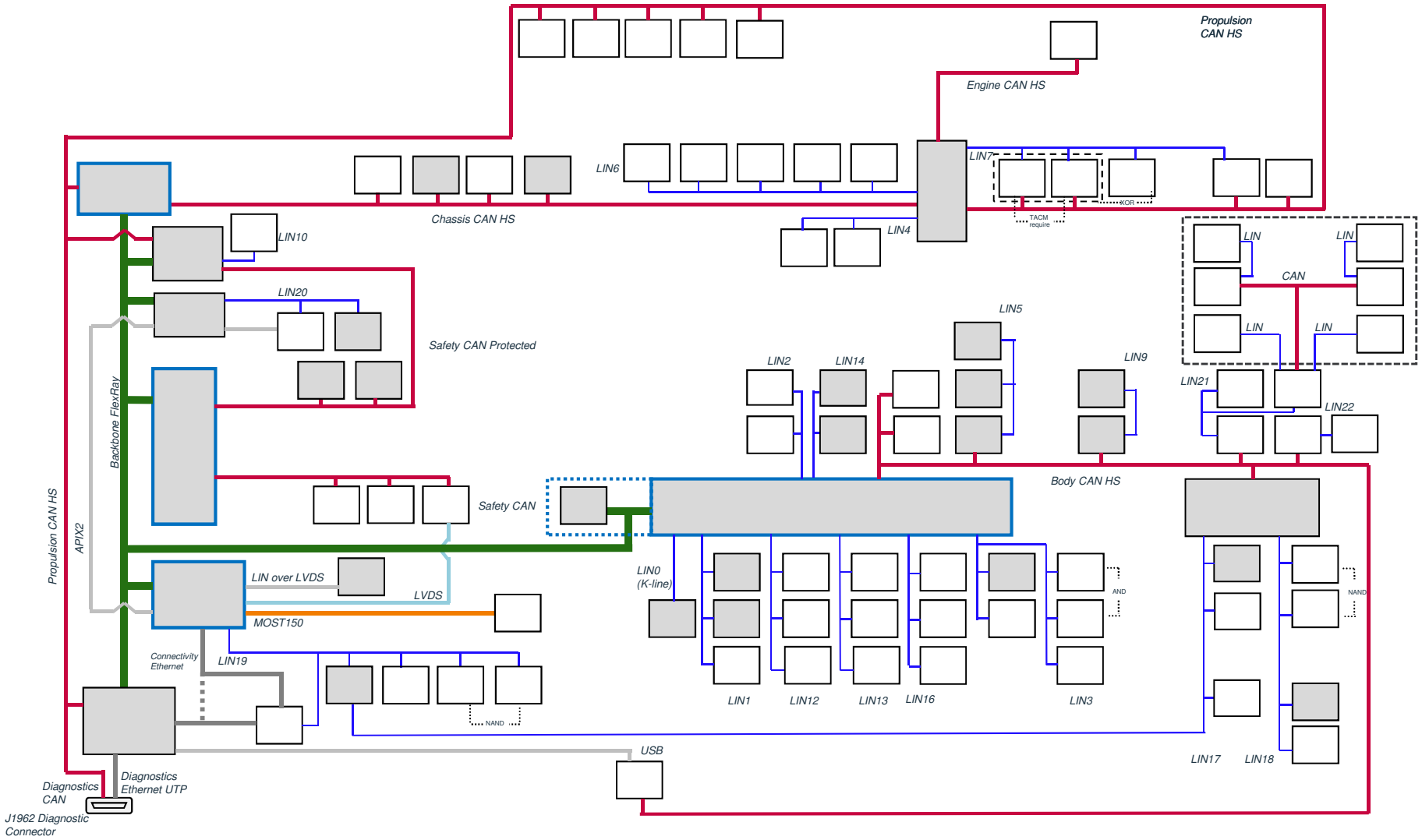
“it’s unlikely, but with the strong caveat that it’s not impossible”



“Hacking a car: a real threat or yet another shocker?”

THE FBI WARNS THAT CAR HACKING IS A REAL RISK

“We're seeing car thefts in the wild accomplished through hacking”


Propulsion CAN HS
Engine CAN HS
LIN6
LIN7
KOR
TACM require
Chassis CAN HS
LIN4
LIN10
LIN20
Safety CAN Protected
LIN
LIN
CAN
LIN
LIN
LIN5
LIN2
LIN14
LIN9
LIN21
LIN22
Backbone FlexRay
APIX2
Propulsion CAN HS
Safety CAN
Body CAN HS
LIN over LVDS
LVDS
MOST150
LIN0
(K-line)
AND
NAND
Connectivity
Ethernet
LIN19
NAND
LIN1
LIN12
LIN13
LIN16
LIN3
USB
LIN17
LIN18
Diagnostics
CAN
Diagnostics
Ethernet UTP
J1962 Diagnostic
Connector

Agenda

- Academic vehicle security research 2010-2011
- BMW
- Jeep Cherokee
- Mitsubishi Outlander
- Tesla Model S
- GM OnStar
- Audi TT (Workshop systems)
- Wireless Unlock/Remote Keyless Entry

Academic research (CAESS)

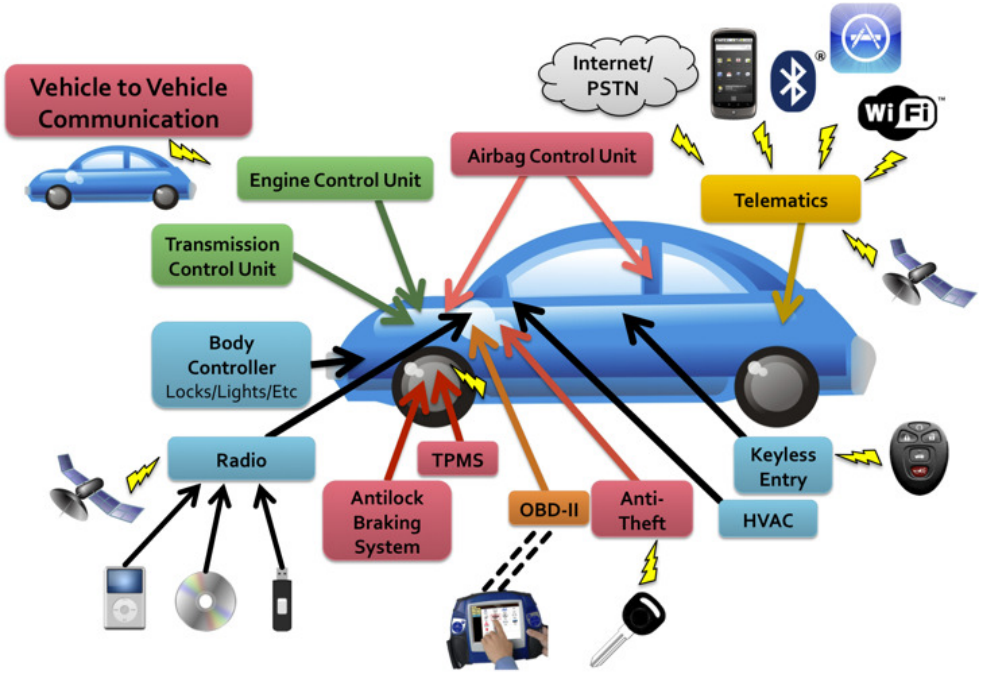
"The Center for Automotive Embedded Systems Security (CAESS) is a collaboration between researchers at the University of California San Diego and the University of Washington."

Publications 2010-2011 (www.autosec.org)

- ***Experimental Security Analysis of a Modern Automobile***
  - IEEE Symposium on Security and Privacy, May 2010
- ***Comprehensive Experimental Analyses of Automotive Attack Surfaces***
  - USENIX Security Symposium, August 2011

Usenix 2011 presentation:
https://www.youtube.com/watch?v=bHfOzilwXic

Also reported on SVT Vetenskapens Värld 2013:
https://www.youtube.com/watch?v=c3p-Wy6sGug
(https://www.youtube.com/watch?v=elPb_OfIpgU)



Academic research (CAESS)

CAESS researchers demonstrated full control of a car via compromise of various attack vectors.

OEM and model not disclosed.

Vulnerability Class	Channel	Implemented Capability	Visible to User	Scale	Full Control	Cost	Section
Direct physical	OBD-II port	Plug attack hardware directly into car OBD-II port	Yes	Small	Yes	Low	Prior work [14]
Indirect physical	CD	CD-based firmware update	Yes	Small	Yes	Medium	Section 4.2
	CD	Special song (WMA)	Yes*	Medium	Yes	Medium-High	Section 4.2
	PassThru	WiFi or wired control connection to advertised PassThru devices	No	Small	Yes	Low	Section 4.2
	PassThru	WiFi or wired shell injection	No	Viral	Yes	Low	Section 4.2
Short-range wireless	Bluetooth	Buffer overflow with paired Android phone and Trojan app	No	Large	Yes	Low-Medium	Section 4.3
	Bluetooth	Sniff MAC address, brute force PIN, buffer overflow	No	Small	Yes	Low-Medium	Section 4.3
Long-range wireless	Cellular	Call car, authentication exploit, buffer overflow (using laptop)	No	Large	Yes	Medium-High	Section 4.4
	Cellular	Call car, authentication exploit, buffer overflow (using iPod with exploit audio file, earphones, and a telephone)	No	Large	Yes	Medium-High	Section 4.4

Academic research (CAESS)

One spectacular attack was to get buffer overflow-based remote code execution by dialing the telematics unit and playing maliciously crafted audio.

```
* wwsxfsj (oa@185.sub                .com) has joined

<wwsxfsj> boot time = 2e3a3402, pin = 8544
<KarlInTheOffice> CANPKT E 0004 02 01
<KarlInTheOffice> CANPKT E L 000f 87 20 04 ff 88
<KarlInTheOffice> CANPKT E L 0004 02 01
* UCSDCar (oa@1.sub                 .com) has joined

<UCSDCar> boot time = ab7608c7, pin = 6831
* Steve|laptop (                   ) has joined #oscc
<KarlInTheOffice> CANPKT 000f E L 87 20 04 ff 88
```

The researchers managed to get their own software onto the telematics unit. They installed an IRC client which acted as a bot, receiving commands from a C&C server.

Agenda

- Academic vehicle security research 2010-2011
- BMW
- Jeep Cherokee
- Mitsubishi Outlander
- Tesla Model S
- GM OnStar
- Audi TT (Workshop systems)
- Wireless Unlock/Remote Keyless Entry

BMW Connected drive

ADAC - Allgemeiner Deutscher Automobil-Club, investigated BMW Connected Drive and published their findings early 2015.

Through reverse engineering (including desoldering of hardware and disassembly of firmware), the researcher found some important flaws:

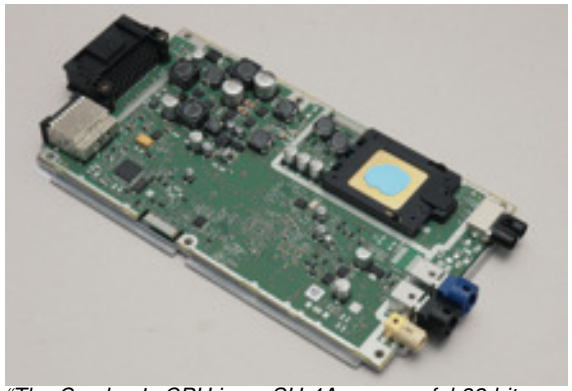
- BMW used the same symmetric keys in all vehicles.
- Some services did not encrypt messages in transit between the car and the BMW backend.
- The ConnectedDrive configuration data wasn't tamper-proof.
- The Combox disclosed the VIN via NGTP error messages.
- NGTP data sent via text messages was encrypted with DES.
- The Combox did not implement any protection against replay attacks.

BMW fixed the flaws via an over the air update!

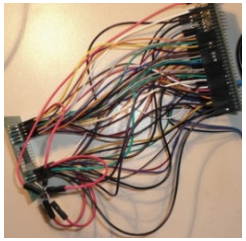
http://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html

BMW Connected Drive (2015)

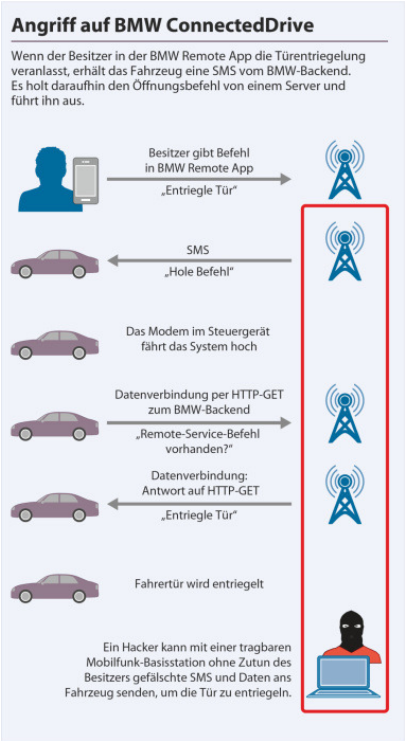
BMW Connected Drive “Combobox”



“The Combox's CPU is an SH-4A, a powerful 32-bit RISC processor from Renesas. Mobile communication is facilitated by a GSM/GPRS/EDGE modem from Cinterion (formerly Siemens). The device also uses a V850ES micro controller, also manufactured by Renesas.”



BMW Connected Drive Protocol



When the user triggers an unlock in the BMW Remote App, the vehicle receives a text message from the BMW backend servers. The car proceeds to fetch the unlock command from the server and executes it.

1. Owner triggers unlock in the BMW Remote App: "Unlock the door”
2. Text message: "Fetch command”
3. The modem in the control unit boots the system
4. Data connection via HTTP GET to the BMW backend: "Remote Service Command available?”
5. Server answering the HTTP GET: "Unlock the door”
6. Driver-side door is unlocked

An attacker with a portable cellular base station can open the car door by forging text messages and data connections and sending them to a car without its owner's knowledge.

http://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html

Agenda

- Academic vehicle security research 2010-2011
- BMW
- Jeep Cherokee
- Mitsubishi Outlander
- Tesla Model S
- GM OnStar
- Audi TT (Workshop systems)
- Wireless Unlock/Remote Keyless Entry

Jeep Cherokee (2015)

In July 2015, Wired featured an article describing how researchers Charlie Miller and Chris Valasek could take remote control of a Jeep Cherokee. They presented their work at Defcon August 2015.

Img source: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

The story got a global attention in the press and resulted in FCA recalling 1.4M vehicles.

http://illmatics.com/Remote%20Car%20Hacking.pdf
https://www.youtube.com/watch?v=MK0SrxBC1xs

Jeep Cherokee (2015)

Miller and Valasek found out that the connectivity ECU in many FCA cars **exposed the D-Bus*** service on port 6667 on all network interfaces including wifi access point **and cellular WAN.**

One of the reachable D-Bus “sub-services” contained an “execute” method. Handy for remote command execution!

Firewall open...

After reverse engineering the ECU and its’ CAN microcontroller (Renesas V850), were able to remotely reprogram the ECU and the CAN microcontroller and thereafter send arbitrary CAN messages to the car from anywhere in the world.

By scanning the correct IP range, they were able to identify other cars of with the same vulnerable connectivity solution.

*D-Bus or DBus is an inter-process communication (IPC) and remote procedure call (RPC) mechanism that allows communication between multiple computer programs (processes) concurrently running on the same machine.

Miller and Vlasek’s automotive security research history:

Black Hat & Defcon 2014: A Survey of Remote Automotive Attack Surfaces
http://illmatics.com/remote%20attack%20surfaces.pdf

Syscan 2014: Car hacking for poories
http://illmatics.com/car_hacking_poories.pdf

Defcon 2013: "Adventures in Automotive Networks and Control Units”
http://illmatics.com/car_hacking.pdf

Agenda

- Academic vehicle security research 2010-2011
- BMW
- Jeep Cherokee
- Mitsubishi Outlander
- Tesla Model S
- GM OnStar
- Audi TT (Workshop systems)
- Wireless Unlock/Remote Keyless Entry

Mitsubish outlander

- PenTest Partners security review 2016
- Control connectivity based on wifi AP in car
- Wifi password cracking (4 x GPU cracking rig at less than 4 days) and then...

Finally, we disabled the theft alarm. Yes, seriously

This took a bit of proving, as we didn't want to have to break a window to make the point.

```
...
>>> def sendit(payload):
...   c=crc(payload)
...   s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
...   s.connect(("192.168.8.46",8080))
...   s.send(payload+c)
...   s.close()
...   time.sleep(10)
...
>>>
>>> alarmoff()
```

Source: https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/

Agenda

- Academic vehicle security research 2010-2011
- BMW
- Jeep Cherokee
- Mitsubishi Outlander
- Tesla Model S
- GM OnStar
- Audi TT (Workshop systems)
- Wireless Unlock/Remote Keyless Entry

Tesla Model S (defcon 2015)

Source: autoexpress.co.uk

- Security review by Marc Rogers and Kevin Mahaffey
- After reverse engineering large parts of the car, the researchers "*gained full control of the entertainment system. They could open and close windows, lock and unlock doors, raise and lower the suspension and cut power to the car*"
- Lot's of dead ends for the researchers, e.g.:
  - signed software
  - patched QtWebKit browser
  - OTA servers only accessible through VPN
- Overall, Tesla came out very well and could patch over OTA

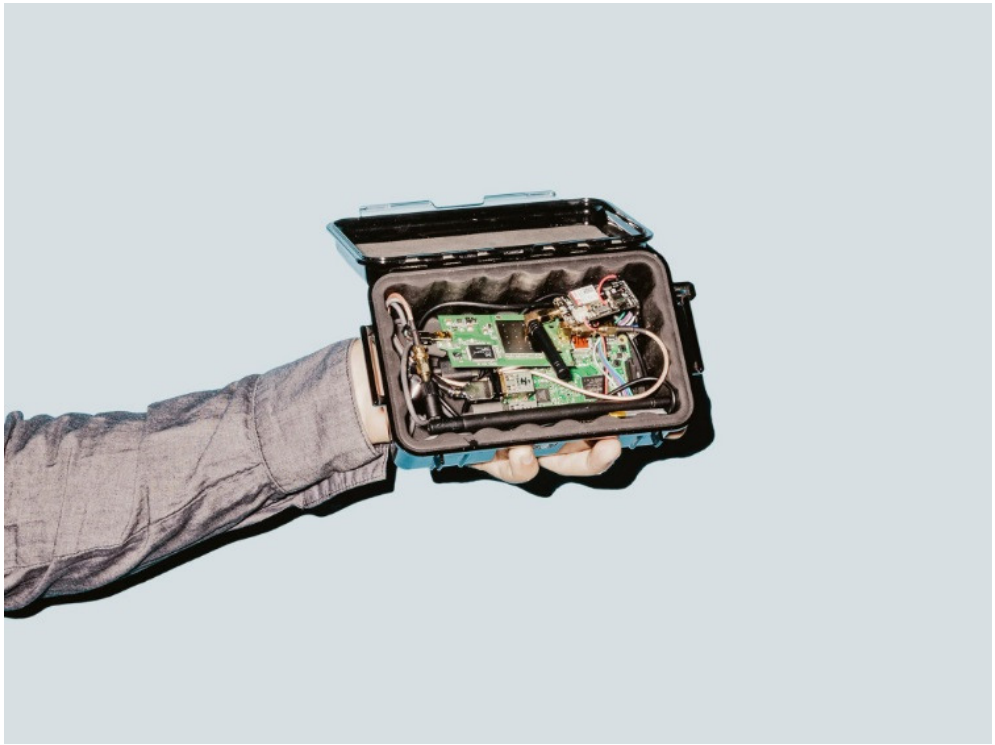
Agenda

- Academic vehicle security research 2010-2011
- BMW
- Jeep Cherokee
- Mitsubishi Outlander
- Tesla Model S
- GM OnStar
- Audi TT (Workshop systems)
- Wireless Unlock/Remote Keyless Entry

OWASP
Open Web Application Security Project

GM onstar

- Sammy Kamkar created **OwnStar**
- Attack based on rogue AP and credential stealing
- With the credentials, an attacker can do anything the owner can...



Source: https://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/

Source: http://media.gm.com

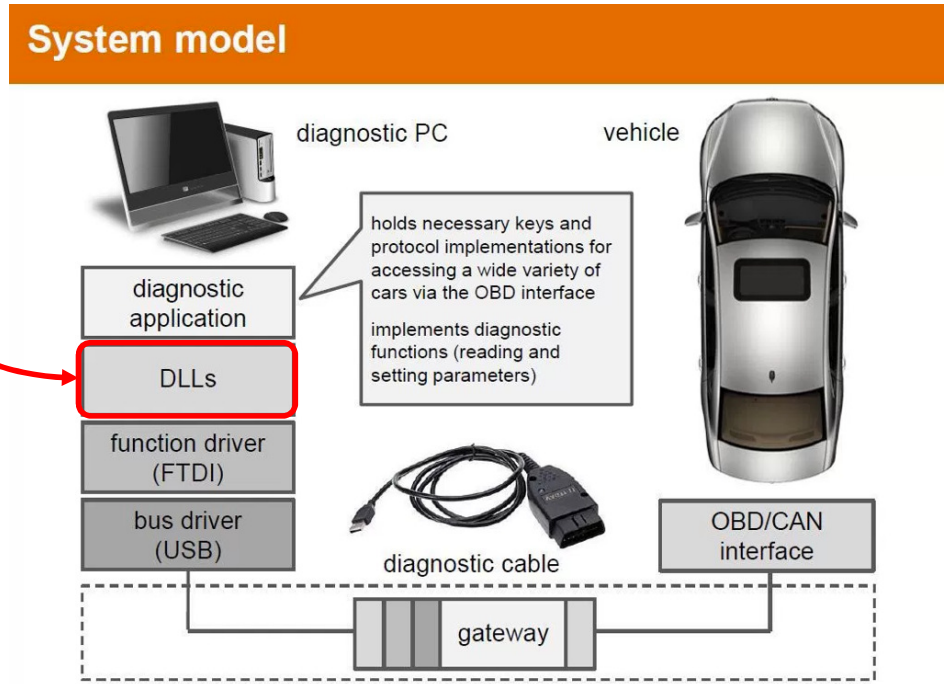
Agenda

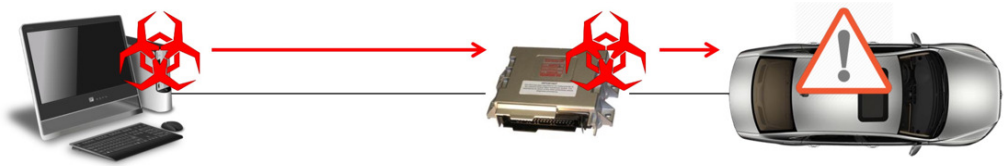
- Academic vehicle security research 2010-2011
- BMW
- Jeep Cherokee
- Mitsubishi Outlander
- Tesla Model S
- GM OnStar
- Audi TT (Workshop systems)
- Wireless Unlock/Remote Keyless Entry

OWASP
Open Web Application Security Project

Workshop system attack

- By attacking the pc running the diagnostics application, researchers were able to turn off the airbags in an Audi TT
- Done by replacing an original DLL with an attacker controlled version. This made it possible to manipulate traffic between the diagnostics application and the car, man-in-the-middle style.



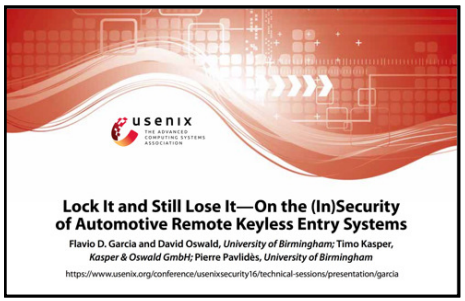


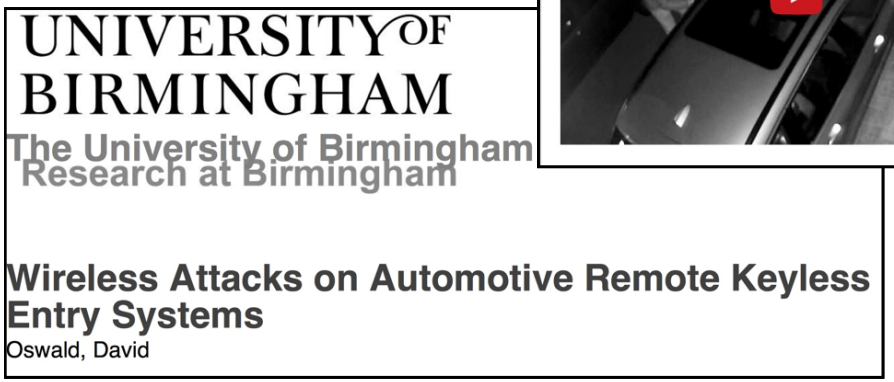
Agenda

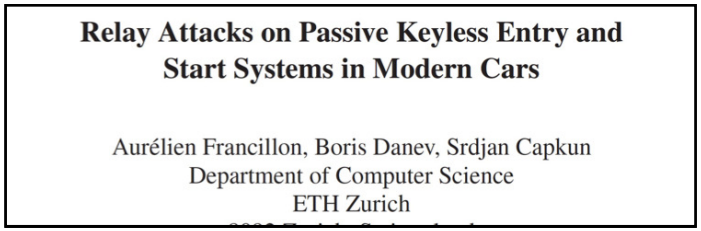
- Academic vehicle security research 2010-2011
- BMW
- Jeep Cherokee
- Mitsubishi Outlander
- Tesla Model S
- GM OnStar
- Audi TT (Workshop systems)
- Wireless Unlock/Remote Keyless Entry

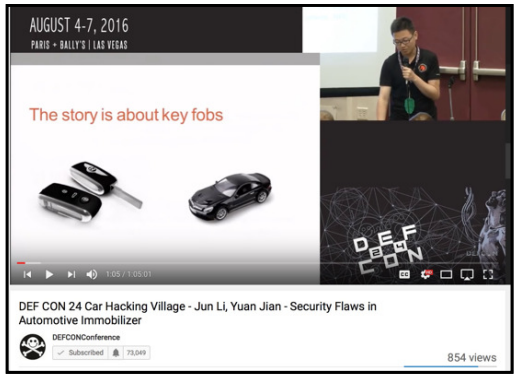
OWASP
Open Web Application Security Project

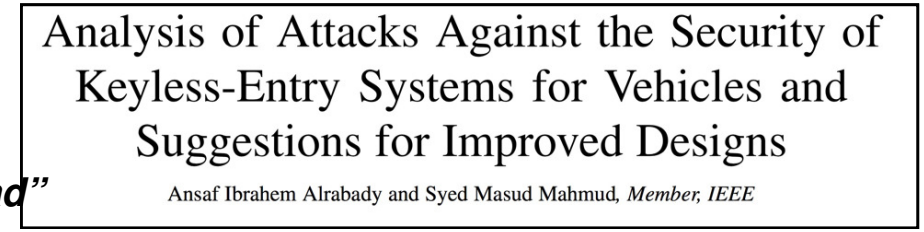
A lot of research on the insecurity of electronic car lock techno











Seen in the wild...

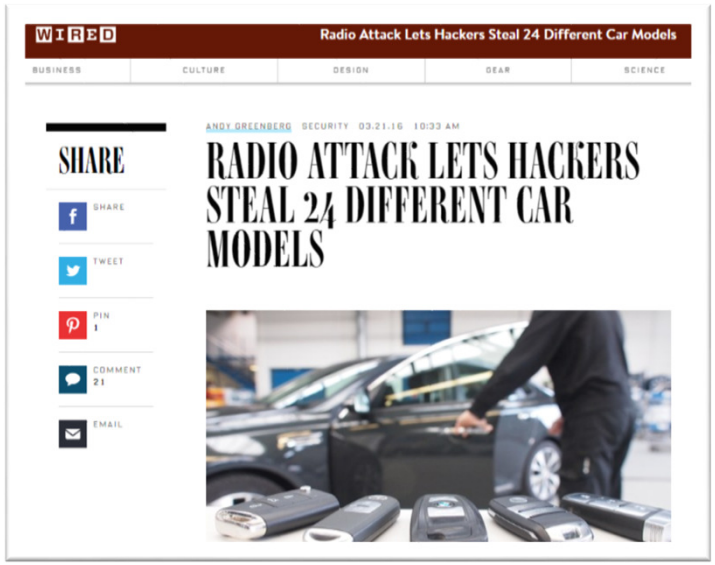
"Three keyless thefts of luxury cars EACH DAY in Hampstead"

Relay Attack on RKE

Idea: Make the car believe that the key fob is close, by:

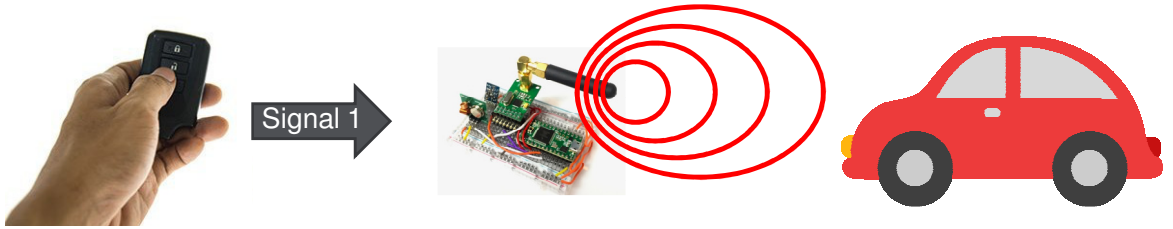
- Place a pair of relaying devices between the keyfob and the car
- Effectively amplifying the signals between the keyfob and the car

- ADAC video: https://www.youtube.com/watch?v=0AHSDy6AiV0



Rolljam

(Sammy Kamkar, again...)



When user presses unlock on key fob – record the unlock signal and jam the car from recieving it

When user presses a second time, release the first unlock signal and record the second

Save second signal for future use

Agenda

- Academic vehicle security research 2010-2011
- BMW
- Jeep Cherokee
- Mitsubishi Outlander
- Tesla Model S
- GM OnStar
- Audi TT (Workshop systems)
- Wireless Unlock/Remote Keyless Entry
- Movie time!

Movie time!

Jeep movie

Source: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

Nissan leaf

Early 2016, a security interested Norwegian Nissan Leaf owner (attending a training session with security researcher Troy Hunt) found out that Nissan provided a web API that allowed unauthenticated traffic to connected Nissan Leaf cars.

By just knowing the VIN, anyone with internet access could read car status and control the heater of any connected Nissan Leaf.


Thanks!