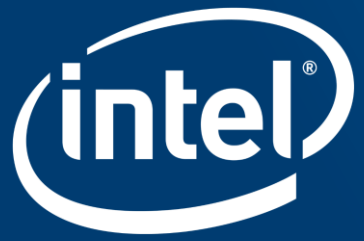


AUTOMOTIVE LINUX SUMMIT

Common Attacks Against Car Infotainment Systems

Lin, Tong; Chen, Luhai

July 2019

Agenda

- Background information
- Attack surfaces and related hacking incidents
- Possible mitigations
- Practices for automotive security testing
- Conclusion

What is IVI?

- In-vehicle infotainment.
- A combination of in-vehicle systems that include both hardware and software.
- Deliver information and entertainment to the driver and the passengers.
- Usually isolated from vehicle safety critical components through gateway.

IVI is becoming more and more important with the growing demand for smart vehicles.

IVI systems owned by automakers

Top key players

Key features of IVI system

- Multimedia play (audio and video)
- Hands-free phone call
- Satellite navigation and traffic condition update
- Social networking
- Interactive voice recognition services
- ...

Most hacked cars are the ones with most features!!!

Back to the topic

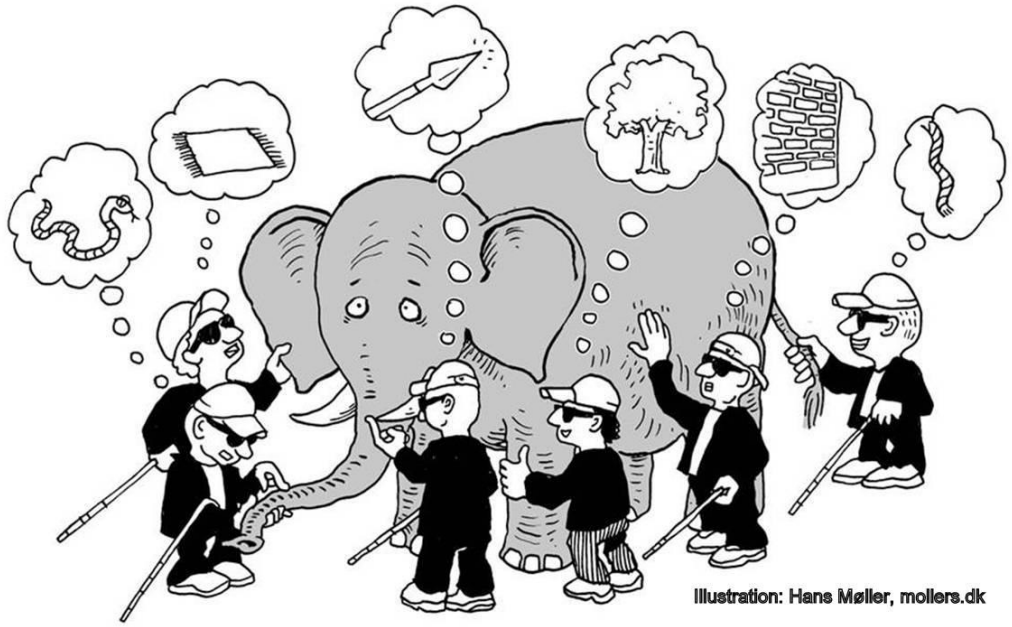
- Scope
  - Focus on attacks against the IVI system.
    - External diagnostic interface (OBD-II) is also included.
  - No CAN bus hacking.
- The hacking incidents mentioned in the slides have already been mitigated, although some of the details are not disclosed.

Agenda

- Background information
- Attack surfaces and related hacking incidents
- Possible mitigations
- Practices for automotive security testing
- Conclusion

Security without visibility

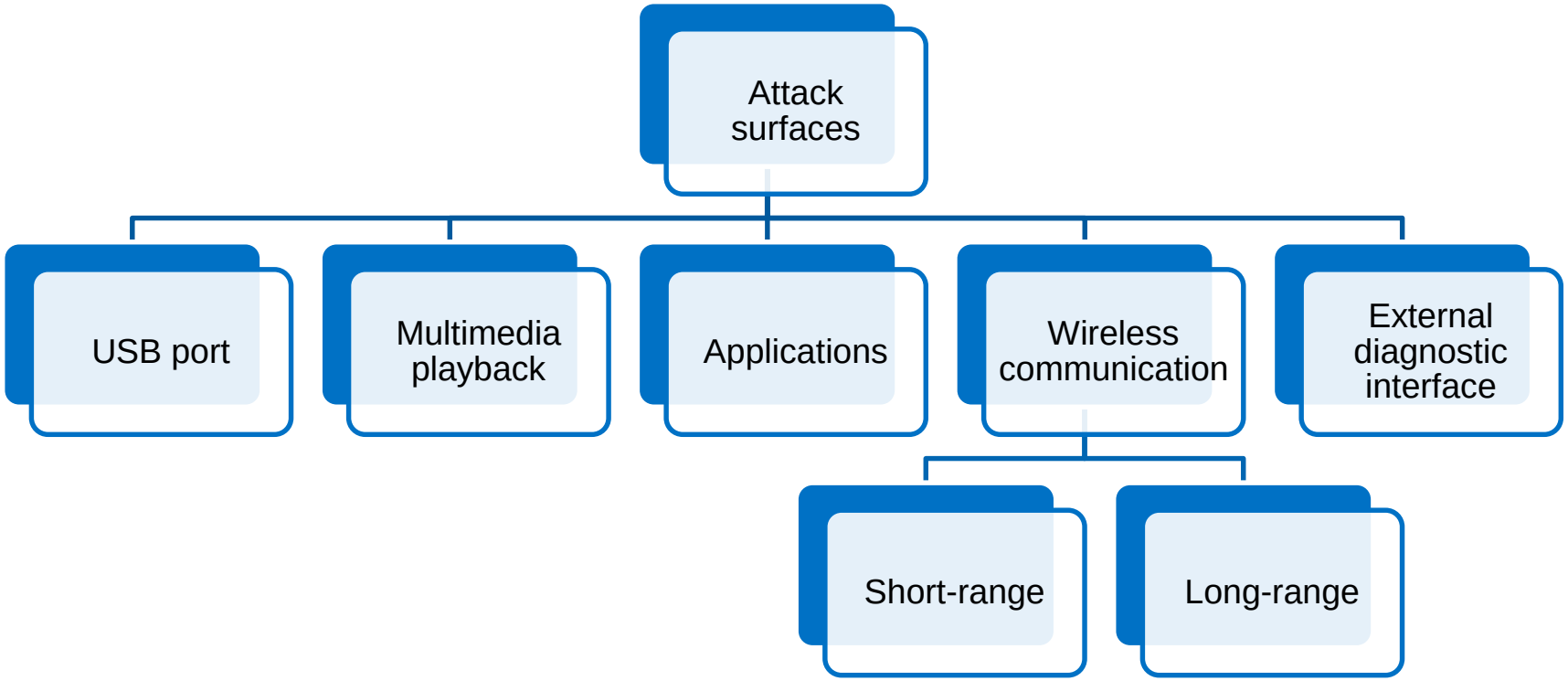
- Poor attack visibility is a major threat to automotive security



You can’t protect what you can’t see!!!

https://cdn-images-1.medium.com/max/1600/1*4UPp3Tc4A32S0WXJ0pWP7g.jpeg

Quick glimpse



USB port

- Media playback via USB
- Firmware/software updates via USB
- USB-to-Ethernet
  - Serve as debug interfaces but also create an extra interface
  - Use port scanning to detect vulnerable internal networking services
- Run shell scripts or install unauthorized software via USB
- DMA attack against USB 3.x

Malware injection via USB

- Researchers from Zingbox found a way to hack into IVI system with a maliciously crafted USB device.
- The attack could be done via social engineering tricks.
- Malware installed in the IVI system can
  - leverage SMS service on the paired driver's phone to access personal information, intercept banking authentication pins, or even block phone calls.
  - be commanded remotely through SMS messages and put the IVI system into an unusable state.

https://www.businesswire.com/news/home/20180809005216/en/Zingbox-Identifies-New-Cybersecurity-Threat-Cars-Drivers

Firmware updates via USB

- A security researcher could install malicious Subaru StarLink head unit firmware via USB and gain persistent root code execution by exploiting a vulnerability (CVE-2018-18203) in the update mechanism.


```
$ ssh root@192.168.0.1

****************************** SUBARU ******************************
Warning - You are knowingly accessing a secured system. That means
you are liable for any mischeif you do.
************************************************************************

root@192.168.0.1's password:
# uname -a
QNX localhost 6.6.0 2016/09/07-09:25:33CDT i.MX6S_Subaru_Gen3_ED2_Board armle
# cat /etc/shadow
root:@S@aaaaaa@56c26c380d39ce15:1042473811:0:0
logger:@S@bbbbbb@607cb4704d35c71b:1420070987:0:0
certifier:@S@cccccc@e0a3f6794d650876:1420137227:0:0
# pidin -F "%n %U %V %W %X %Y %Z" | grep sh
usr/sbin/sshd          0         0         0         0         0         0
usr/sbin/sshd          0         0         0         0         0         0
bin/sh          0         0         0         0         0         0
```

https://github.com/sgayou/subaru-starlink-research/blob/master/doc/README.md#conclusion

Multimedia playback

- The most common entry point to gain access to the IVI.
- Examples
  - old-fashioned
    - CD-ROM/DVD-ROM, local multimedia file stored in USB sticks/SD card
  - new-fashioned
    - Audio over Bluetooth
    - Apple Carplay/Google Android Auto
    - UPnP (Universal Plug and Play)
- Specially prepared media files can be used to tamper media engine services, Bluetooth, and Wi-Fi stacks.

Use Trojan CD to hack car

- By adding extra code to a digital music file, researchers were able to turn a song burned to CD into a Trojan horse.
- When played on the car's stereo, this song could alter the firmware of the car's stereo system, giving attackers an entry point to change other components on the car.
- This type of attack could be spread on file-sharing networks without arousing suspicion.

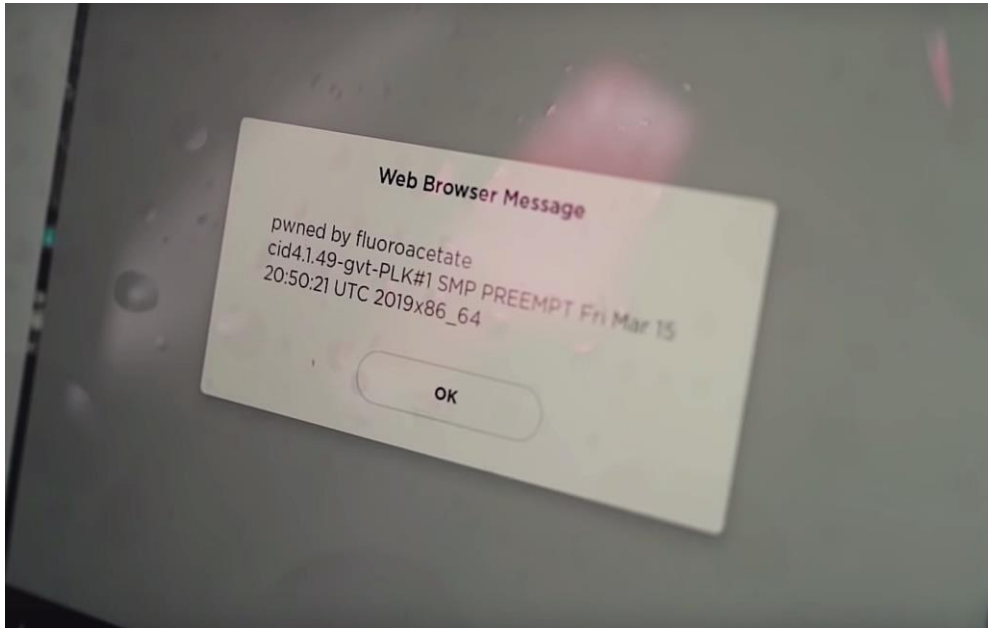
https://www.theregister.co.uk/2016/01/26/hackers_can_take_full_control_of_car_os/

Applications

- Expand the functionality of the native HMI.
- Mainly consists of two parts
  - Apps that are directly installed into the IVI system
  - Apps installed in consumer's smartphone and can remotely connected to the IVI system
- Cloud security
  - Some apps are connected to cloud for data exchange.

Onboard browser hacked at Pwn2Own

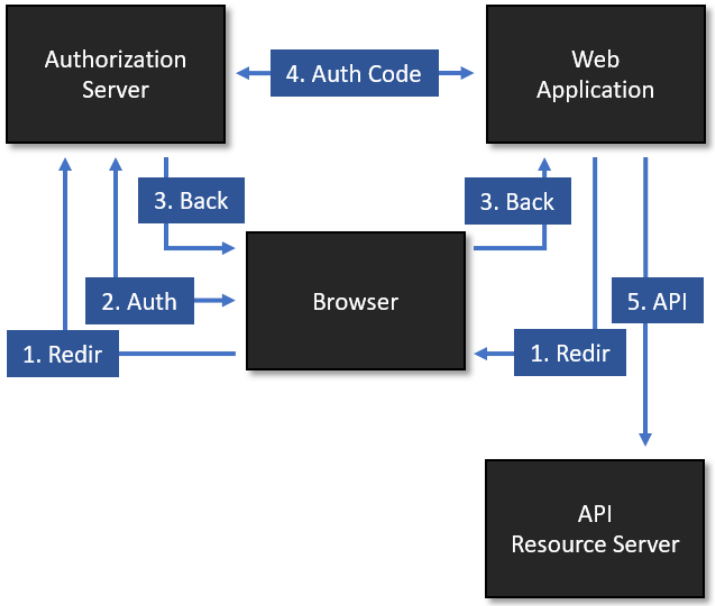
- Researchers from Fluoroacetate hacked the Tesla Model 3 car via its onboard browser. They used a JIT bug in the browser renderer process to execute code on the car's firmware and show a message on its IVI system.

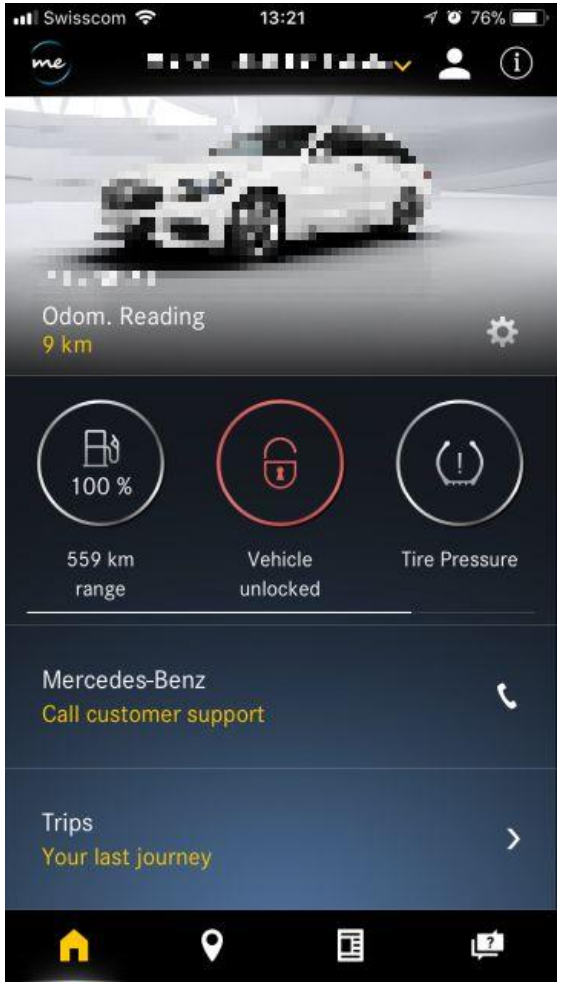


https://www.zdnet.com/article/tesla-car-hacked-at-pwn2own-contest/

Vulnerability in connected vehicle app

- A MITM attack may intercept the encrypted connection between Mercedes me app and server.
- CWE-300
- CVE-2018-18071





https://www.scip.ch/en/?labs.20180405

Short-range wireless communication

- Wi-Fi or Bluetooth
  - Packet sniffing
  - Jamming
  - MITM
  - Protocol-related exploits
- DSRC (Dedicated Short Range Communications)
  - vehicle-to-everything (V2X) communications

CarsBlues

- Found by Privacy4Cars.
- Exploit IVI systems via the Bluetooth protocol.

- The attacker can access stored contacts, call logs, text logs, and in some cases even full text messages without the vehicle's owner/user being aware - and without the user's mobile device being connected to the system.

https://www.privacy4cars.com/can-my-car-be-hacked/default.aspx

Exploitable Wi-Fi connection vulnerabilities

- Vulnerabilities exist in MIB manufactured by Harman.
- A quick port scan shows that there is a telnet service listening, but without valid credentials.

```
$ nmap -sV -vvv -oA gte -Pn -p- 192.168.88.253
Starting Nmap 7.31 ( https://nmap.org ) at 2017-01-05 10:34 CET
Host is up, received user-set (0.0061s latency).
Not shown: 65522 closed ports
Reason: 65522 conn-refused
PORT      STATE    SERVICE         REASON      VERSION
23/tcp    open     telnet          syn-ack     Openwall GNU/*/Linux telnetd
10123/tcp open     unknown         syn-ack
15001/tcp open     unknown         syn-ack
21002/tcp open     unknown         syn-ack
21200/tcp open     unknown         syn-ack
22111/tcp open     tcpwrapped      syn-ack
22222/tcp open     easyengine?     syn-ack
23100/tcp open     unknown         syn-ack
23101/tcp open     unknown         syn-ack
25010/tcp open     unknown         syn-ack
30001/tcp open     pago-services1? syn-ack
32111/tcp open     unknown         syn-ack
49152/tcp open     unknown         syn-ack

Nmap done: 1 IP address (1 host up) scanned in 259.12 seconds
```

- The researchers finally have remote code execution by exploiting the vulnerable internet service on MMX.

```
$ ./exploit 192.168.88.253
[+] going to exploit 192.168.88.253
[+] system seems vulnerable...
[+] enjoy your shell:
uname -a
QNX mmx 6.5.0 2014/12/18-14:41:09EST nVidia_Tegra2(T30)_Boards armle
```

Exploitable Wi-Fi connection vulnerabilities

- ➢ Another component RCC (sharing filesystem with MMX, using Qnet) also has a telnet service running.
- ➢ Finally control RCC through rewriting the original telnet binary on MMX.

```
# /tmp/telnet 10.0.0.16
Trying 10.0.0.16...
Connected to 10.0.0.16.
Escape character is '^]'.


QNX Neutrino (rcc) (ttyp0)

login: root
Password:

      ___            _ _   __   __  ___  _____
     /   |_   _   __| (_) |  \/  | |_ _|  _  \
    / /| | | | | |/ _ | | | |\/| | || ||  |_)_/
   / __  | |_| | (_| | | | |  | | || ||  |_) \
  /_/  |_|__,__|\__,_|_| |_|  |_|___|_____/

/ > ls -la
total 37812
lrwxrwxrwx  1 root      root             17 Jan 01 00:49 HBpersistence -> /mnt/efs-persist/
drwxrwxrwx  2 root      root             30 Jan 01 00:00 bin
lrwxrwxrwx  1 root      root             29 Jan 01 00:49 config -> /mnt/ifs-root/usr/apps/
config
drwxrwxrwx  2 root      root             10 Feb 16  2015 dev
dr-xr-xr-x  2 root      root              0 Jan 01 00:49 eso
drwxrwxrwx  2 root      root             10 Jan 01 00:00 etc
dr-xr-xr-x  2 root      root              0 Jan 01 00:49 hbsystem
lrwxrwxrwx  1 root      root             20 Jan 01 00:49 irc -> /mnt/efs-persist/irc
drwxrwxrwx  2 root      root             20 Jan 01 00:00 lib
drwxrwxrwx  2 root      root             10 Feb 16  2015 mnt
dr-xr-xr-x  1 root      root              0 Jan 01 00:37 net
drwxrwxrwx  2 root      root             10 Jan 01 00:00 opt
dr-xr-xr-x  2 root      root       19353600 Jan 01 00:49 proc
drwxrwxrwx  2 root      root             10 Jan 01 00:00 sbin
dr-xr-xr-x  2 root      root              0 Jan 01 00:49 scripts
dr-xr-xr-x  2 root      root              0 Jan 01 00:49 srv
lrwxrwxrwx  1 root      root             10 Feb 16  2015 tmp -> /dev/shmem
drwxr-xr-x  2 root      root             10 Jan 01 00:00 usr
dr-xr-xr-x  2 root      root              0 Jan 01 00:49 var
/ >
```

https://www.computest.nl/documents/9/The_Connected_Car._Research_Rapport_Computest_april_2018.pdf

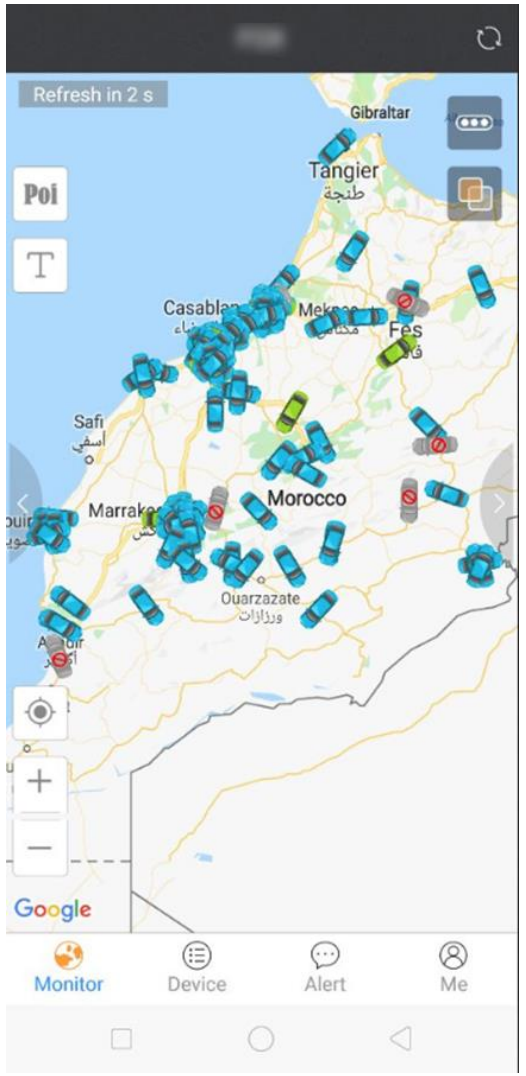
Long-range wireless communication

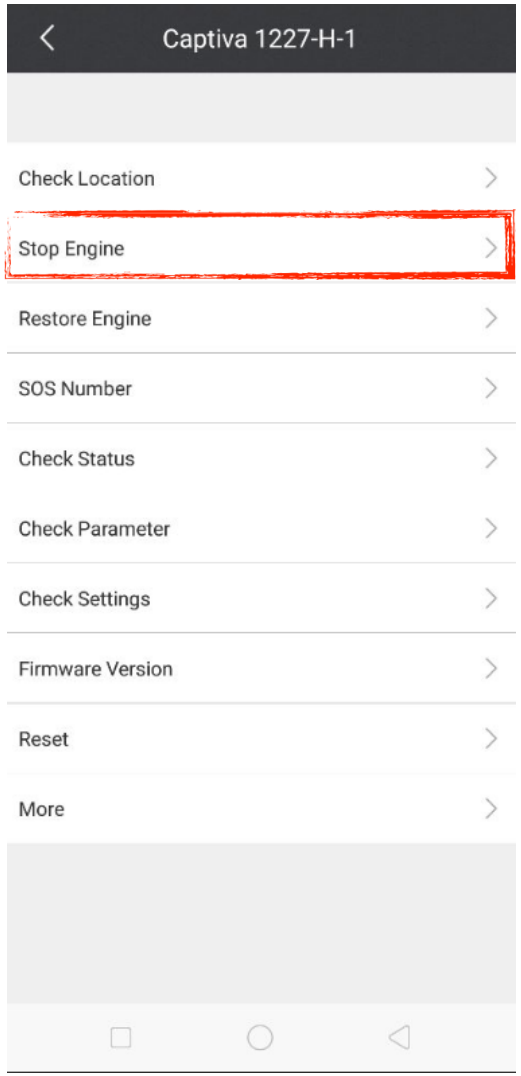
- cellular radio (3G/4G/5G)
  - emergency call, anti-theft tracking, online weather/news
- GPS
  - Usually be used to provide traffic information for some navigation services with RDS (Radio Data System) and TMC (Traffic Message Channel)
  - Attack types
    - GPS Tracking Apps
    - GPS spoofing

GPS Tracking Apps

- Default user account password found in GPS tracker apps (ProTrack and iTrack) by reverse engineering.

- After breaking into these accounts, the attacker could monitor the locations of vehicles and even turn off the engines of vehicles that are traveling 12 miles per hour or slower.

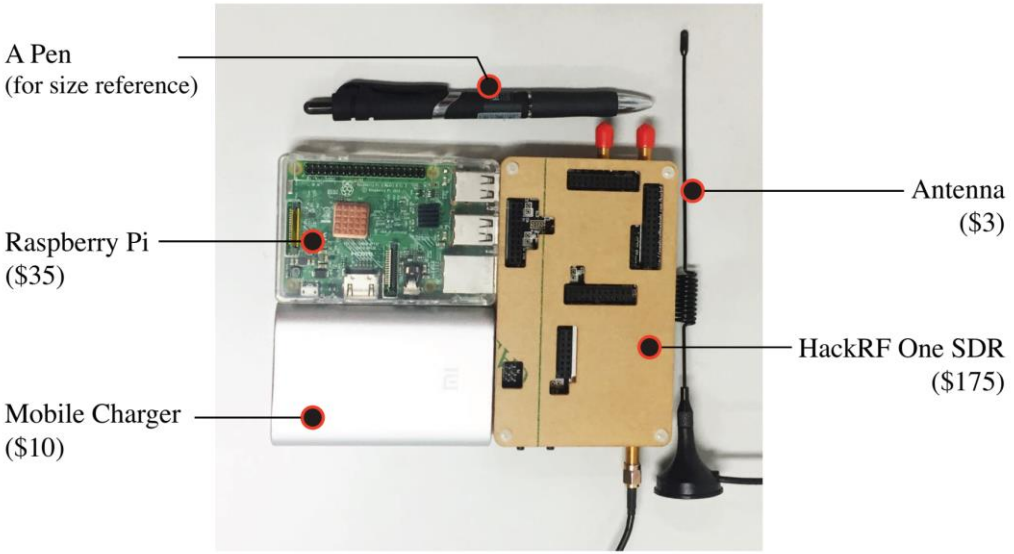




https://www.vice.com/en_us/article/zmpx4x/hacker-monitor-cars-kill-engine-gps-tracking-apps

GPS spoofing

- An attacker can send sat-nav-guided vehicles into oncoming traffic (such as a one-way road) by GPS spoofing.
- A low-cost portable GPS spoofer.

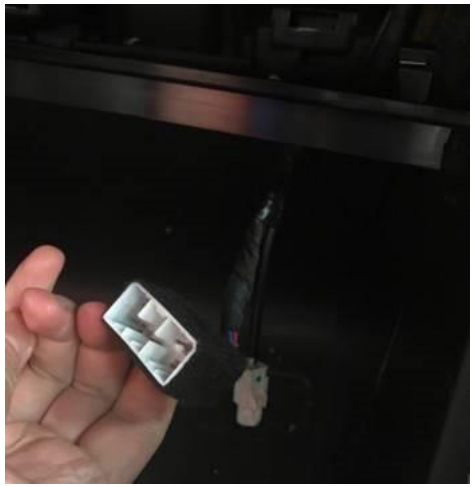


https://people.cs.vt.edu/gangwang/sec18-gps.pdf

External diagnostic interface (OBD-II)

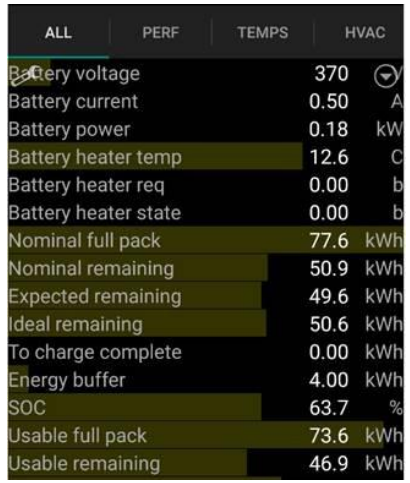
- On-Board Diagnostics (OBD) is vehicle's built-in self-diagnostic system.
- OBD-II, an evolutionary standard introduced in the mid-'90s.
- Initial physical access is needed.

Bluetooth diagnostic module



Tesla's diagnostics connector

OBD-II Bluetooth module



Some diagnostic information

- Will lead to a lot of error messages, even rear motors going offline and then lost all power by fuzzing.

https://www.pentestpartners.com/security-blog/tesla-killer-the-fuzzed-and-the-furious/

Exploit techniques behind IVI hacking

- Malware injection
  - Tricking users into installing by USB
  - Clicking on unknown links or installing fake software from untrusted sources
  - Utilizing the design flaw in the upgrade mechanism
- Security vulnerabilities exploitation
  - Existing exploits in operating systems or applications
  - Compromise insecure networks
- MITM attack

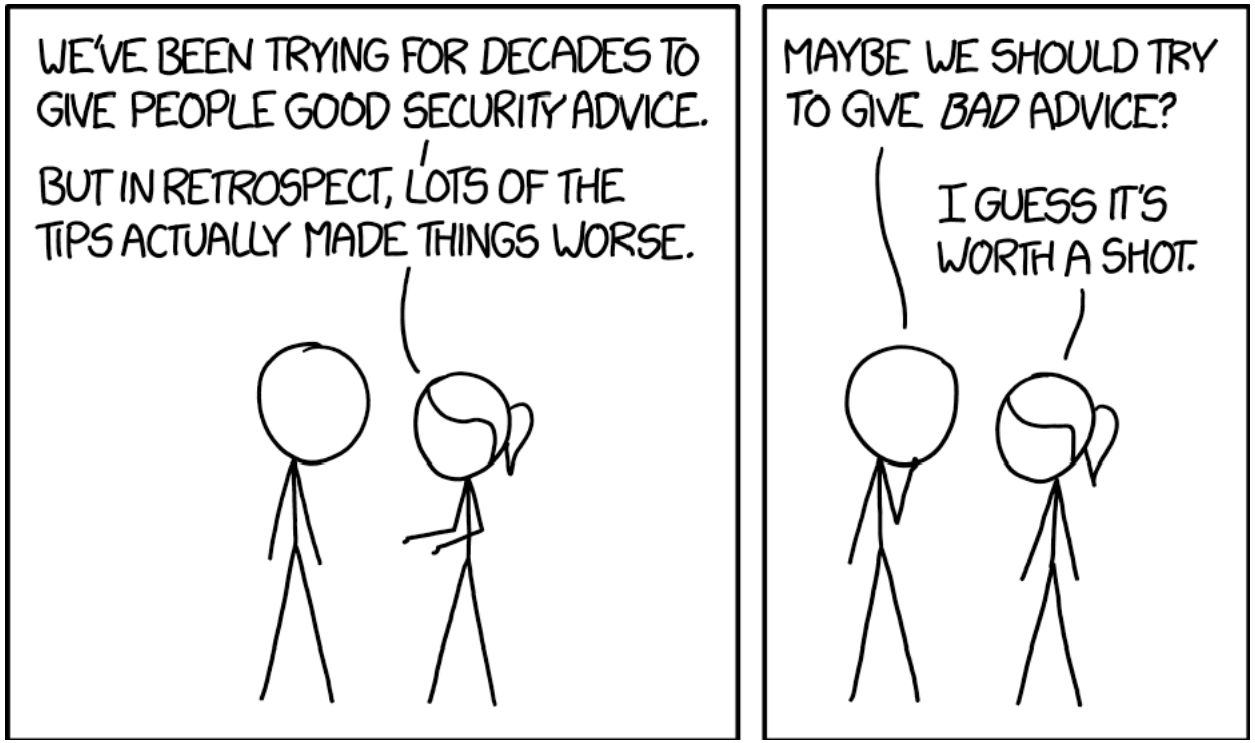
Exploit techniques behind IVI hacking

- Reverse engineering
  - Sensitive data disclosure
    - PII (personally identifiable information), VIN (vehicle identification number)
    - cryptographic keys
  - Discover key APIs and even tampering code
  - Firmware/software can be got by online downloads, after-sales support or insecure OTA
- Spoofing
- DoS attacks by fuzzing

Agenda

- Background information
- Attack surfaces and related hacking incidents
- Possible mitigations
- Practices for automotive security testing
- Conclusion

Not just a joke



True wisdom is, ultimately, not in the knowing, but in the doing.

https://imgs.xkcd.com/comics/security_advice.png

For USB port

- Check the file system of a USB stick and only supported file systems can be allowed to mount.
- Enhance security permission with read-only, nodev, nosuid and noexec options.
- Minimize USB configuration to make sure only necessary USB device classes are enabled.

For update mechanisms

- Always sign or encrypt update packages.
- Ensure the upgrade procedure is to be authenticated.
- Allow secure boot for integrity validation.
- Secure key storage.
- Rescue mode to fall back in case of update failure.

For onboard applications

- Can only be installed from the official/specific sources.
- Divide different security domains for application management and apply strict access model (RBAC, PBAC, ...).
- Isolated “high-risk” applications into containers/VMs.
- An update mechanism should be used that allows deployment of security updates.

For remotely connected applications

- Secure connections from the backend cloud service to the application/vehicle endpoint.
- Improve the authentication mechanism to defend against man-in-the-middle attacks.
- Weak password detection.

For wireless communication

- All wireless protocols need to be properly configured.
- All unused Bluetooth profiles should be disabled.
- Restrict network routing to pre-defined normal behavior, block and alert security systems about any invalid attempts.

For GPS spoofing

- SAASM (Selective Availability Anti-Spoofing Module)
  - But SAASM-enabled GPS receiver is only available to government or military authorized users.
- Use receiver that can track multiple GNSS signals (such as GPS, GLONASS, Galileo, and BeiDou) simultaneously.

Agenda

- Background information
- Attack surfaces and related hacking incidents
- Possible mitigations
- Practices for automotive security testing
- Conclusion

Before this part begins

- The practices to share are from our team's experience of Celadon project (https://01.org/projectceladon/).
- Certainly, they also can be applied to benefit other projects.

Break large overall tests into small tasks

- Figure out different components/interfaces and test separately for different parts.
- Break down any large multi-action tests into smaller, more specific single-action tests.

Discover vulnerabilities in early stage

- Manual review:
  - Forward review of enumerated list of entrypoint functions.
  - Pick a feature and find common weaknesses across different implementations.
  - Find variants of known issues.
- Fuzzing:
  - Corpus creation
  - Parameter optimization
  - Coverage feedback
  - Crash analysis

Select the right tools

- For static code analysis/vulnerability scanning
  - Klocwork, Coverity, CAST, cve-bin-tool, BDBA, WhiteSource
- For USB
  - USB Rubber Ducky, Facedancer21, USB Kill, umap from NCC Group
- For wireless communication
  - HackRF, BladeRF, Ubertooth One, RF Signal Analyzer
  - Wireshark, Burp Suite, Fiddler
- For general fuzzing
  - Syzkaller

Create custom test for specific attack scenarios

- DMA attack
- Side channel attack

Continuous Security

- Testing tools automation.
- DevSecOps
  - Solve the bottleneck effect of older security models on the modern continuous delivery pipeline.
  - Avoid last-minute delays.

Agenda

- Background information
- Attack surfaces and related hacking incidents
- Possible mitigations
- Practices for automotive security testing
- Conclusion

Conclusion

- **You can't have safety without security.** The quality of materials used and the security of the embedded software is equally important.
- **It's important to know your enemy.** Defense is more difficult because it requires consideration of various attack surfaces and means.
- **Deliver software with security built into it, not on or around it.** The security development lifecycle (SDL) will help ensure that security and privacy tasks integrated into each stage of development as part of a seamless process.

Thanks!

Q&A

Notices and Disclaimers

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others