Automotive Security Bugs Explained for Bug Hunters

by Jay Turla / @shipcod3

bugcrowd

> whoami

- Jay Turla aka @shipcod3
- Security Ops Manager (Philippines) at Bugcrowd
- ROOTCON Goon / CFP Review Board
- Not the author of Turla Malware
- One of the main organizers of the Car Hacking Village in ROOTCON and PH → #CarHackVillagePH
- Head of CHV[A] - https://www.carhackingvillage.com/about
- msf contributor (auxiliary & exploit modules)
- I AM your BHAI

Why Car Hacking?

- It’s fun (great community)
- We use it everyday
- We want to ensure we are safe
- More attack surfaces
- My other computer is your car’s computer
- Car Hacking bug bashes pay well
- Cars have IoT Too (Telematics, IVI)

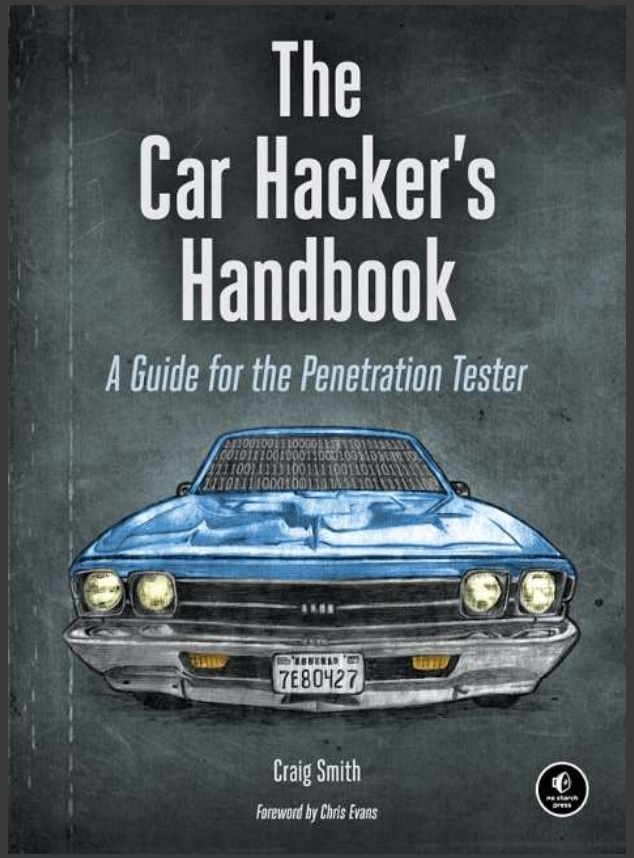
For Example: Car Hacking Bug Bash (from Bugcrowd)

My Favorite Book about Car Hacking

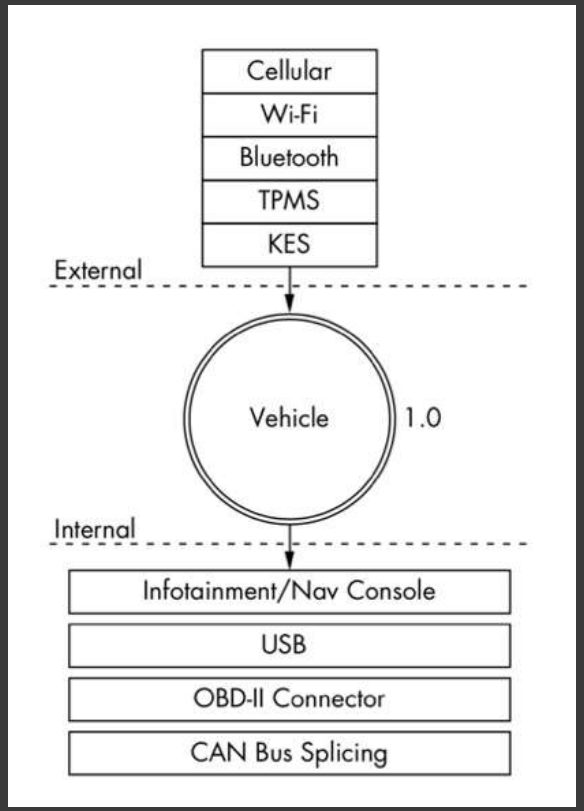
Online version:

http://opengarages.org/handbook/ebook/

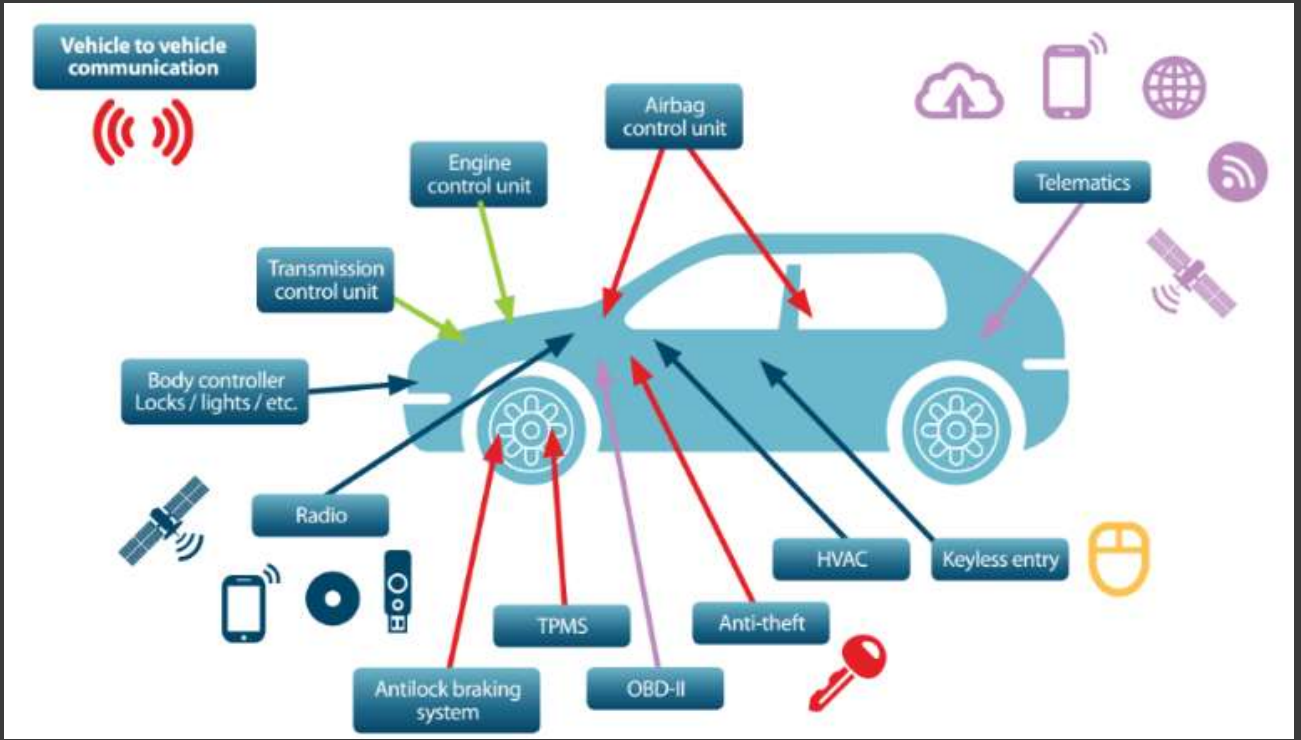
Written by Craig Smith



Common Attack Surfaces by Craig Smith in his book “The Car Hacker’s Handbook”



The Attack Surface of a Connected Vehicle



Reference and Credits: https://argus-sec.com/attack-surface/

Sample Ratings / Common Classification

Vulnerability Rating Taxonomy

Version 1.8 (current) last updated on 25 Sep 2019

automotive ×

Technical severity ▼	VRT category	Specific vulnerability name	Variant / Affected function
P1	Automotive Security Misconfiguration	Infotainment	PII Leakage
P1	Automotive Security Misconfiguration	RF Hub	Key Fob Cloning
P2	Automotive Security Misconfiguration	Infotainment	Code Execution (CAN Bus Pivot)
P2	Automotive Security Misconfiguration	RF Hub	CAN Injection / Interaction
P3	Automotive Security Misconfiguration	Infotainment	Code Execution (No CAN Bus Pivot)
P3	Automotive Security Misconfiguration	Infotainment	Unauthorized Access to Services (API / Endpoints)
P3	Automotive Security Misconfiguration	RF Hub	Data Leakage / Pull Encryption Mechanism
P4	Automotive Security Misconfiguration	Infotainment	Source Code Dump
P4	Automotive Security Misconfiguration	Infotainment	Denial of Service (DoS / Brick)
P4	Automotive Security Misconfiguration	Infotainment	Default Credentials
P4	Automotive Security Misconfiguration	RF Hub	Unauthorized Access / Turn On
P4	Automotive Security Misconfiguration	CAN	Injection (Disallowed Messages)
P4	Automotive Security Misconfiguration	CAN	Injection (DoS)
P5	Automotive Security Misconfiguration	RF Hub	Roll Jam
P5	Automotive Security Misconfiguration	RF Hub	Replay
P5	Automotive Security Misconfiguration	RF Hub	Relay

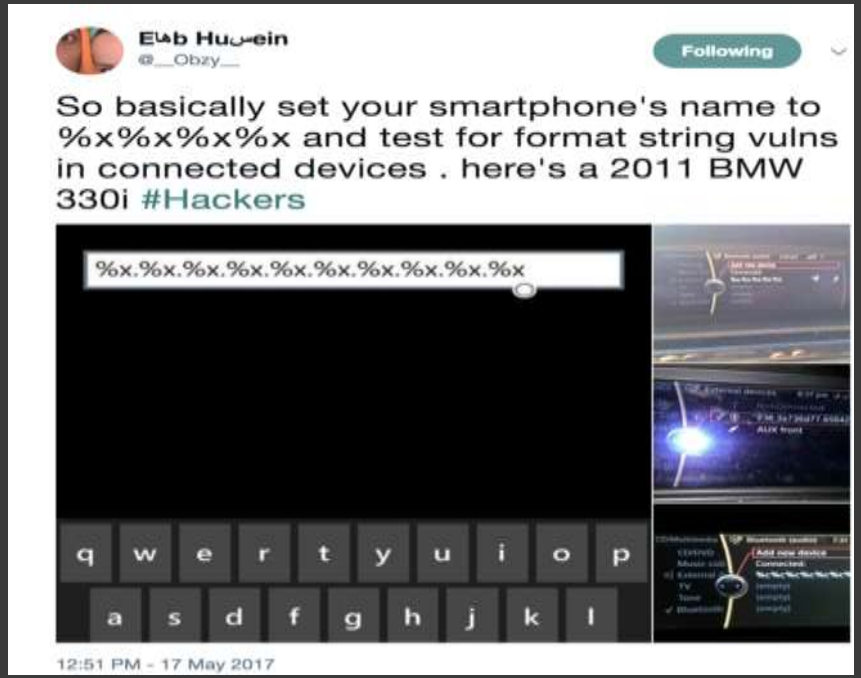
Other Vulnerabilities

- Bypassing Authentication Mechanism for Security Gateways or Firewalls [P1]
- Dumping of Bootloader for Security Gateways or Firewalls [P1]
- Flashing or Programming the ECU by bypassing the Security Gateways or Firewalls [P1]
- Android or iOS App Vulnerabilities [Varies]
- Web Vulnerabilities connected to the Cloud, Telematics, Firmware Update Server [Varies]

Some Insights on common & known vulnerabilities and somehow tie it to the vulnerability classification [limited because of time]

Infotainment DoS through Format String Vulnerabilities [P4]

- Some Bluetooth stacks on infotainment systems can be crashed via %x or %c format string specifiers in a device name, address book name, song title, etc.
- CVE-2017-9212: a researcher from IOActive renamed his device with format string specifiers & connected his device via Bluetooth to his car which eventually crashed his system. (BMW 330i 2011)



Infotainment Default Creds [P4 but sometimes not an issue]

- Try brute forcing the credentials - most of these have weak passwords

- Get to know the default passwordof accessing the system (could be used for further attacks)

- ROOT pass?

Code Execution through USB HID in the infotainment (P3)

- No CAN bus pivot but if yes P2
- PoC: https://github.com/shipcod3/mazda_getInfo/

ECU Resets bypassing the Security Gateway is a P1

- I don’t have a PoC about this but seen One (lemme explain)
- Chris Valasek and Charlie Miller has a book about Advanced Can Injection attacks which could help: http://illmatics.com/can%20message%20injection.pdf

Exploiting Wi-Fi Stack on Tesla Model S by Keen Labs [P3 but I'm leaning to P2]

Reference: https://keenlab.tencent.com/en/2020/01/02/exploiting-wifi-stack-on-tesla-model-s/

Disclaimer: My personal opinion on the priority but could be upgraded to P1 as well (maybe -> depends)

The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse

Security researchers Charlie Miller and Chris Valasek. WHITNEY CURTIS FOR WIRED

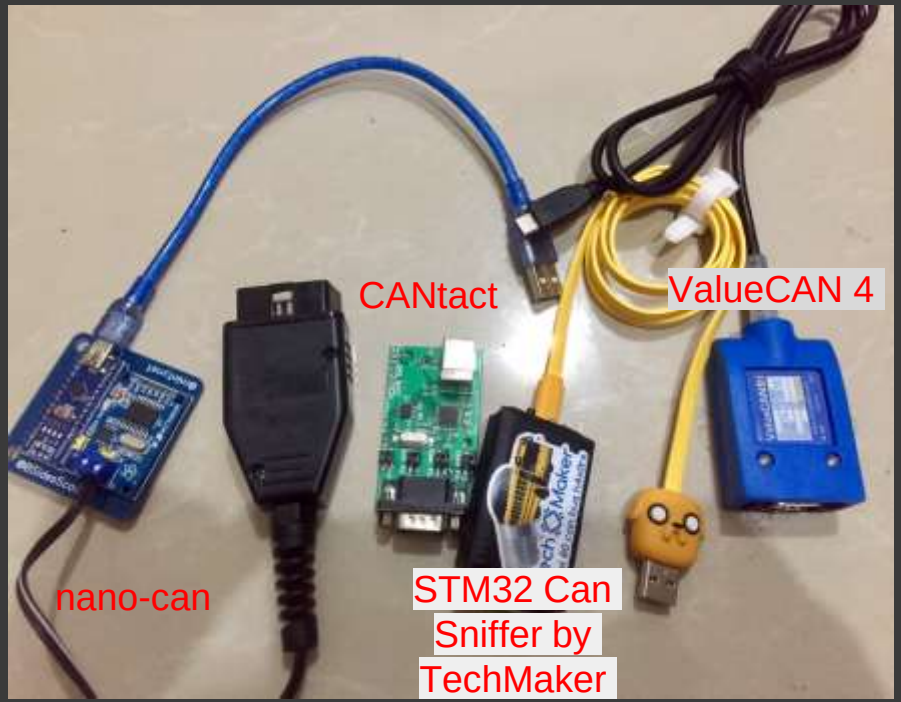
http://illmatics.com/Remote%20Car%20Hacking.pdf


DEMO TIME!


gifs.com

Prerequisites in Replicating the DEMO or Simple Setup [Focus: CANBus]

Instrument Cluster w/ Nano-Can



Some Tools

- https://github.com/jaredthecoder/awesome-vehicle-security
- Great collection of tools and resources to start Car Hacking

CarHacking.Tools by jgamblin

- collection of scripts to help jump start car research and hacking
- All the scripts are designed to run on Ubuntu
- Install via Virtual Machine:
  https://carhacking.tools/install/beta/CarHackingToolsCHVBeta.ova
- Or can be installed via the repo:

```
git clone https://github.com/jgamblin/carhackingtools
cd CarHackingTools
sudo chmod +x *.sh
./toolinstall.sh
```

Using msf hwbrdige

```
# hwbridge_connect.rc
# Author: @shipcod3


# This sample resource script will setup a web server to
bridge communications to a hardware particulary an
automotive and will also establish a session to the
hwbridge server
# Generally used for Car Hacking with msf
# usage: msfconsole -r hwbridge_connect.rc


use auxiliary/server/local_hwbridge
set uripath testbus
run
use auxiliary/client/hwbridge/connect
set targeturi testbus
run
```

```
[*] Moving the accelorometer and speedometer...
hwbridge > run post/hardware/automotive/mazda_ic_mover CANBUS=vcan0

[*] Moving the accelorometer and speedometer...
hwbridge > run post/hardware/automotive/mazda_ic_mover CANBUS=vcan0

[*] Moving the accelorometer and speedometer...
hwbridge > run post/hardware/automotive/mazda_ic_mover CANBUS=vcan0

[*] Moving the accelorometer and speedometer...
hwbridge > info post/hardware/automotive/mazda_ic_mover

       Name: Mazda 2 Instrument Cluster Accelorometer Mover
     Module: post/hardware/automotive/mazda_ic_mover
   Platform: Hardware
       Arch:
       Rank: Normal

Provided by:
  Jay Turla

Compatible session types:
  Hwbridge

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  CANBUS                    no        CAN Bus to perform scan on, defaults to connected bus
  SESSION                   yes       The session to run this module on.

Description:
  This module moves the needle of the accelorometer and speedometer of
  the Mazda 2 instrument cluster


Module options (post/hardware/automotive/mazda_ic_mover):

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  CANBUS                    no        CAN Bus to perform scan on, defaults to connected bus
  SESSION                   yes       The session to run this module on.

hwbridge >
```

QUESTIONS?