
Introduction to Car Hacking

whoami

AppSec Engineer/Bugbounty Hunter from India

Chapter Lead - ASRG-Kerala

Volunteer at Defcon Trivandrum

Speaker: Car Hacking Village Defcon, CRESTCon UK …

Automotive Photographer, Motorsports Athlete(MX, Cross-Country Rally) - @mohammed_shine

agenda

Modern cars

Automotive Security

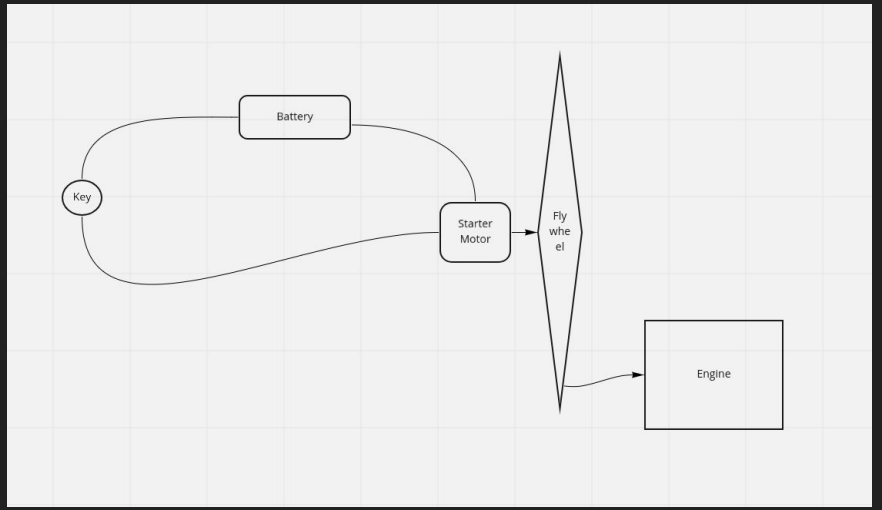
Attack Surface

Attacks

Case studies/Research

Resources

Cars before the 80’s



Modern Vehicle

An F-35 fighter jet has 25 million lines of code; a luxury car 100 million.

```
if (gidsetsize <=
NGROUPS_SMALL)
group_info->blocks[0] =
group_info->
     small_block;

else {
for (i = 0;nblocks; i++)
     {
          gid_t *b;

b = (void
*)__get_free_page
(GFP_USER);
```

```
     small_block;

else {
for (i = 0;nblocks; i++)
     {
```

Source: Roland Berger 2015

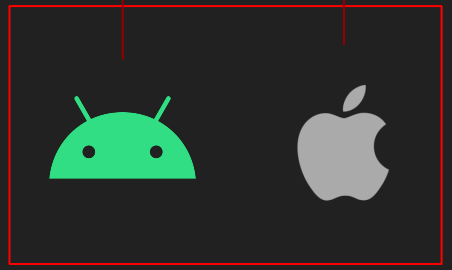
ALTRAN

Attack Surface

Software update

GPS

OBD2

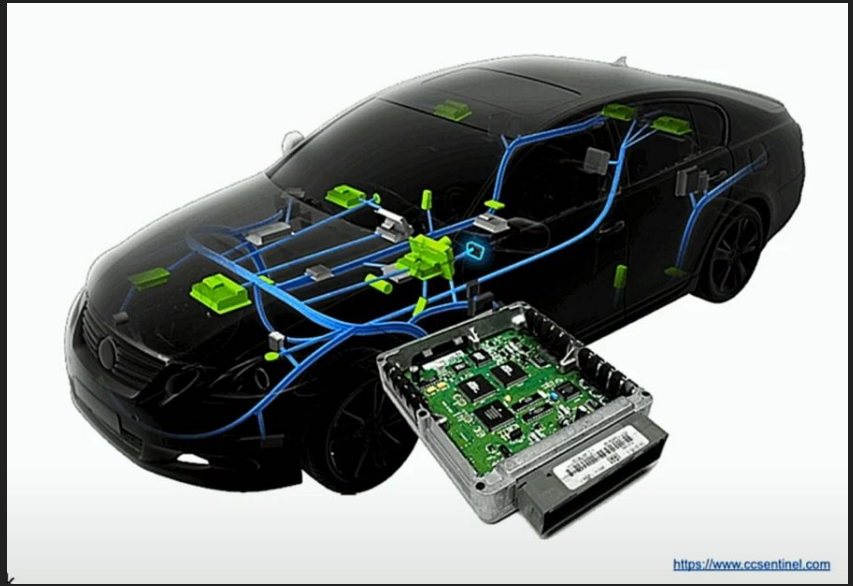


Sensors and ECU

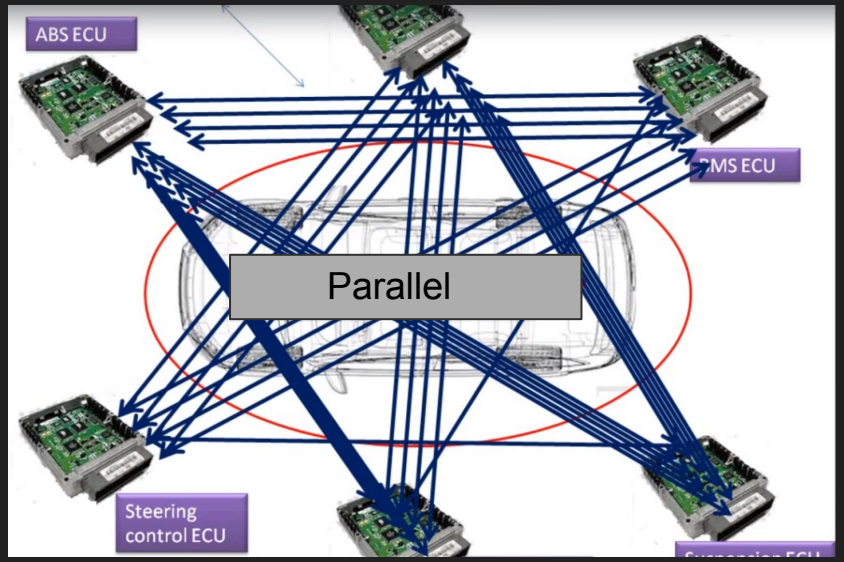
Modern Cars are a combination of Software and Hardware

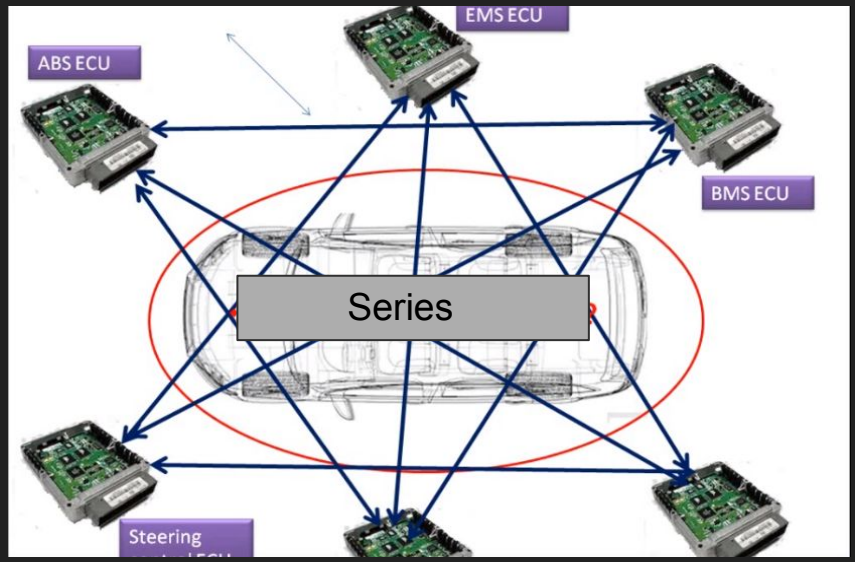
ECU- Engine/Electronic Control Unit

Sensors are the input devices



The Network


ABS ECU
Parallel
Steering
control ECU


EMS ECU
ABS ECU
BMS ECU
Series
Steering

CAR Networks

CAN Bus : Released in 1986, Mandatory from 2008

SAE J1850 : 1994, Slower and Cheaper than CAN

The Keyword Protocol

Local Interconnect Network Protocol : Cheapest among all

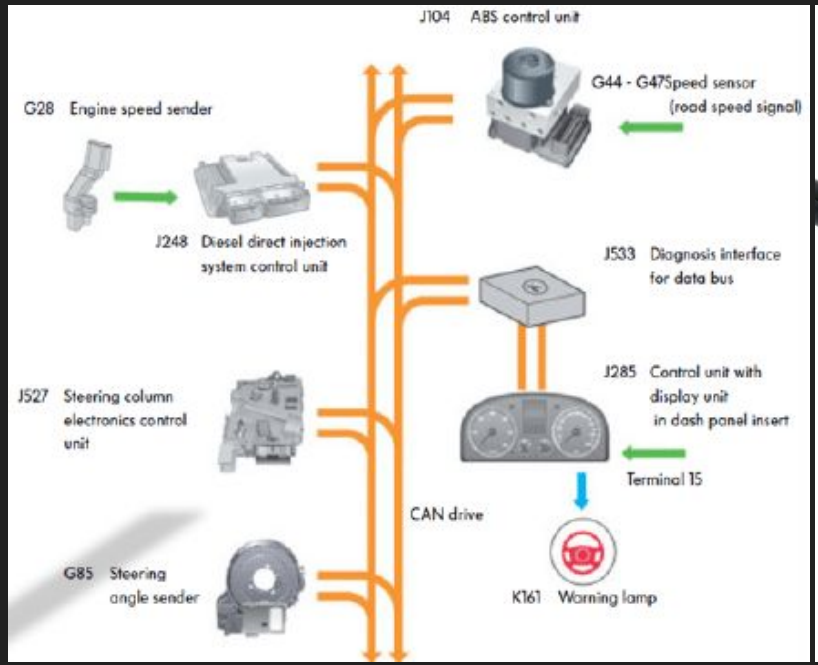
MOST Protocol: For Multimedia Devices

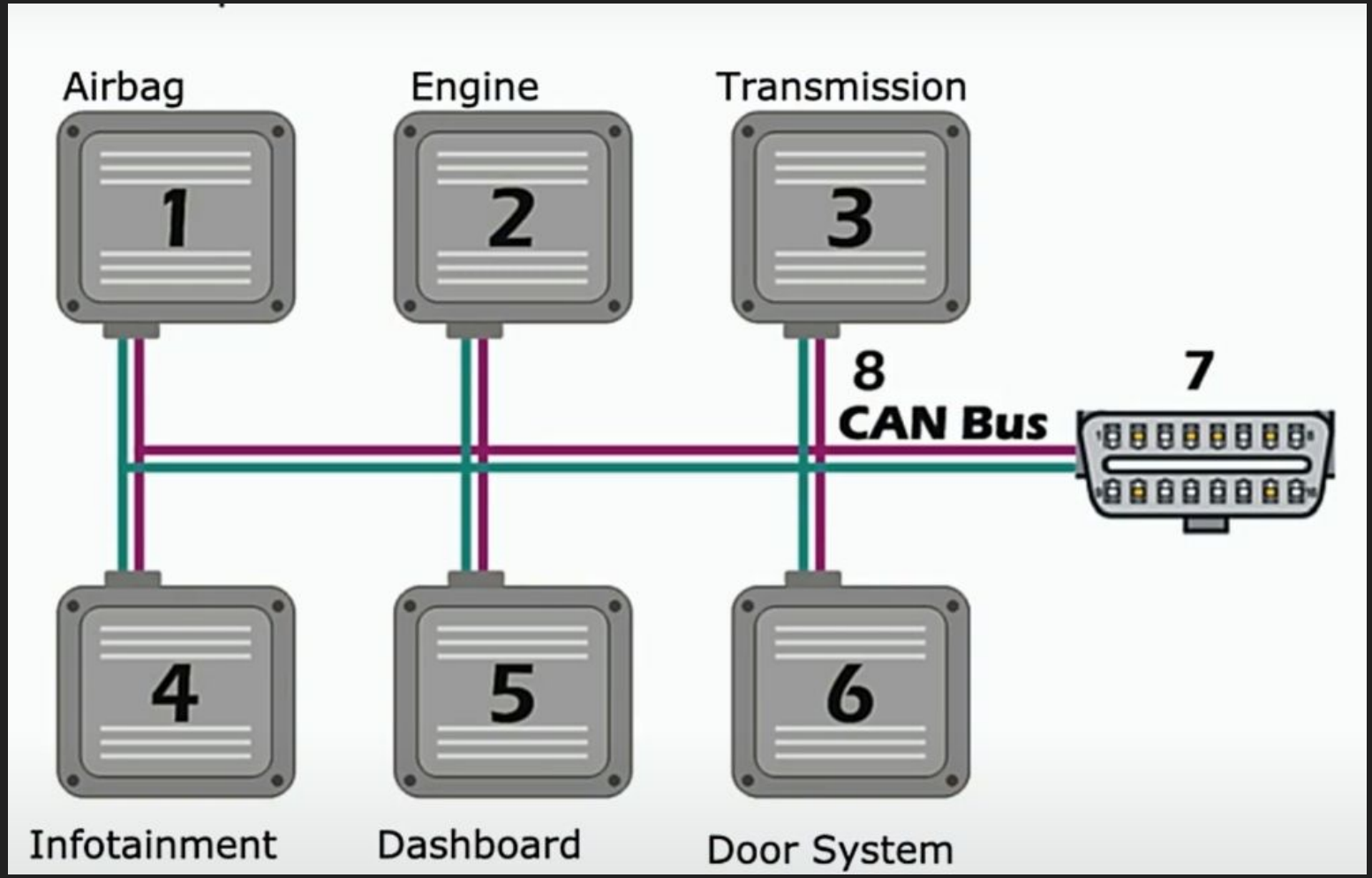
FlexRay : 10 Mbps (Sensitive communication)

Automotive Ethernet: Cheaper alternative to FlexRay and MOST

CAN BUS

Controller Area Network



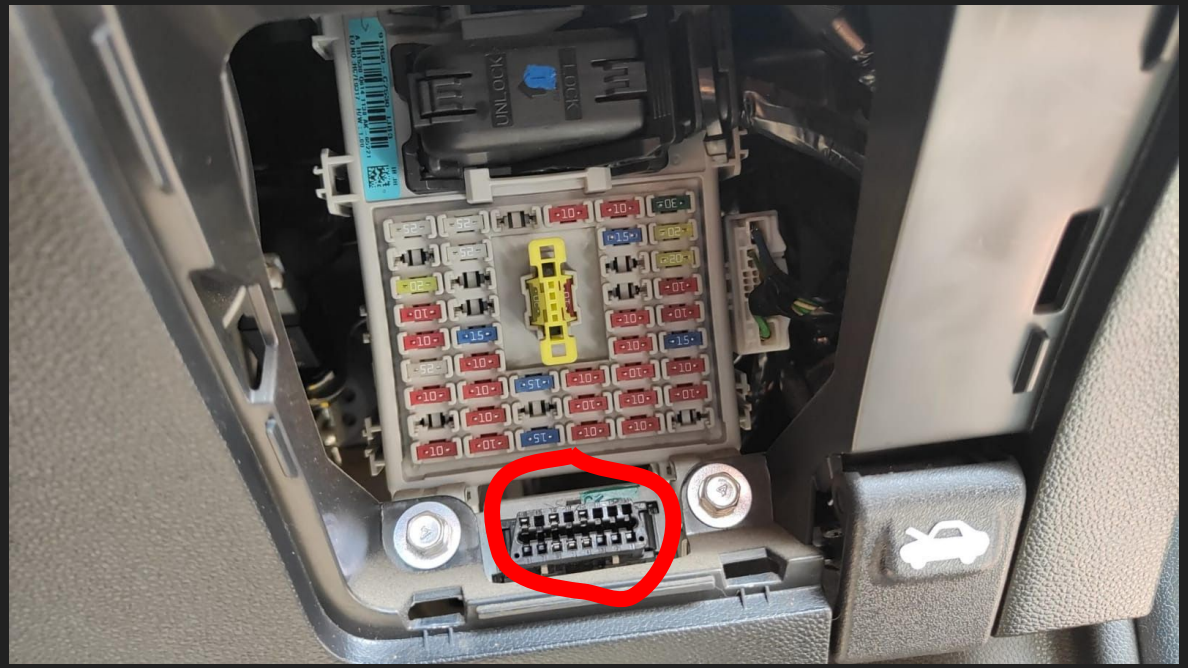

Airbag
Engine
Transmission
1
2
3
8
CAN Bus
7
4
5
6
Infotainment
Dashboard
Door System

Identify the CAN BUS and OBD Port

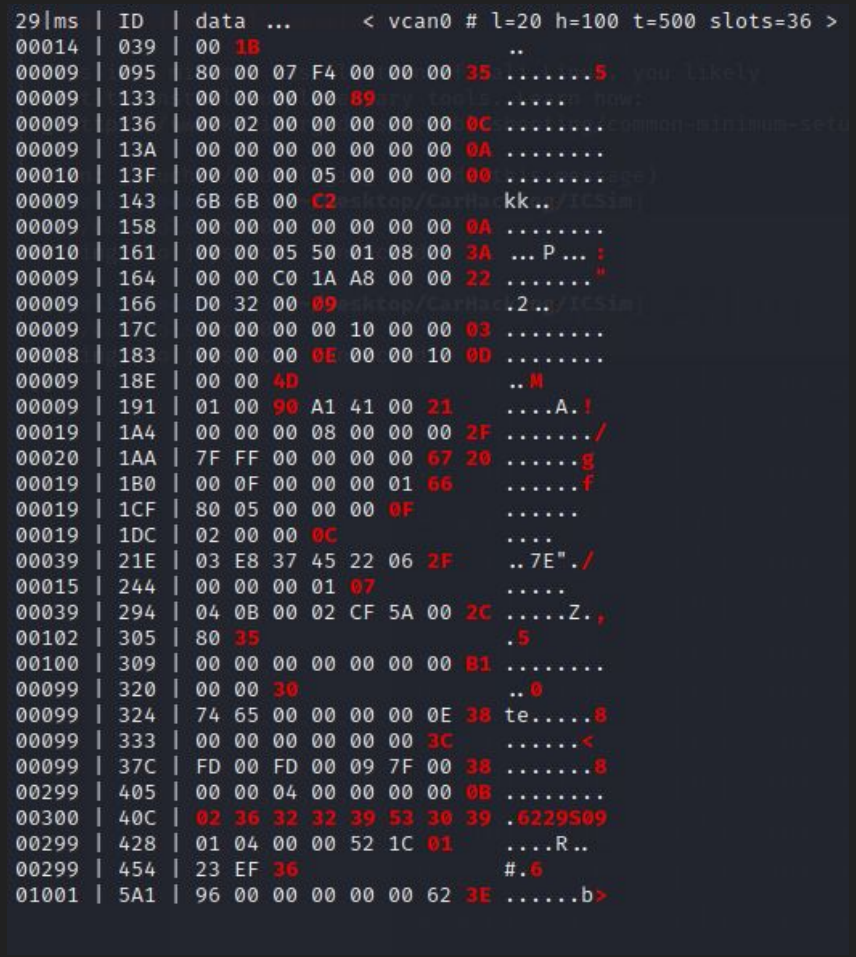
Twisted pair

Use a Multimeter - 2.5V

Resistance - 120 Ohms



Sniffing the CAN



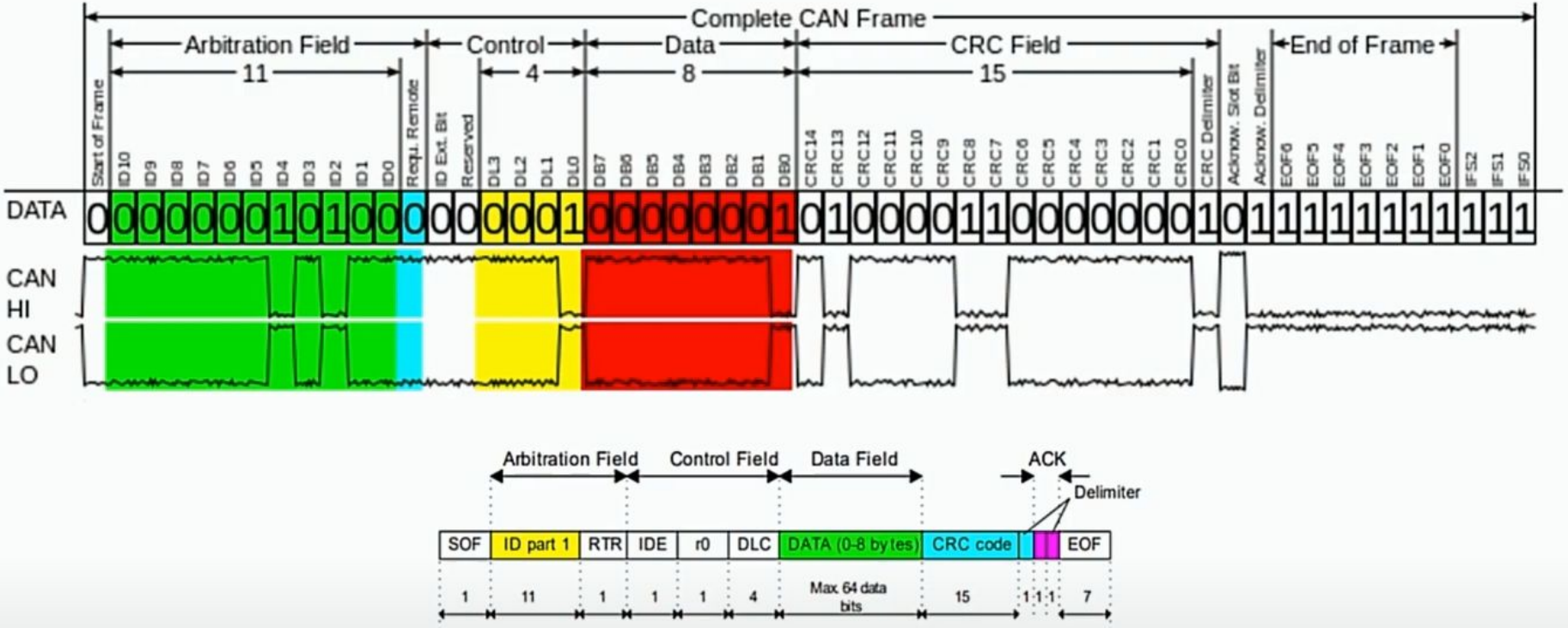
```
29|ms | ID  | data ...      < vcan0 # l=20 h=100 t=500 slots=36 >
00014 | 039 | 00 1B                                  ..
00009 | 095 | 80 00 07 F4 00 00 00 35 .......5
00009 | 133 | 00 00 00 00 89                  .....
00009 | 136 | 00 02 00 00 00 00 00 0C ........
00009 | 13A | 00 00 00 00 00 00 00 0A ........
00010 | 13F | 00 00 00 05 00 00 00 00 ........
00009 | 143 | 6B 6B 00 C2                     kk..
00009 | 158 | 00 00 00 00 00 00 00 0A ........
00010 | 161 | 00 00 05 50 01 08 00 3A  ...P...:
00009 | 164 | 00 00 C0 1A A8 00 00 22 .......“
00009 | 166 | D0 32 00 09                     .2..
00009 | 17C | 00 00 00 00 10 00 00 03 ........
00008 | 183 | 00 00 00 0E 00 00 10 0D ........
00009 | 18E | 00 00 4D                        ..M
00009 | 191 | 01 00 90 A1 41 00 21     ....A.!
00019 | 1A4 | 00 00 00 08 00 00 00 2F ......./
00020 | 1AA | 7F FF 00 00 00 00 67 20 ......g
00019 | 1B0 | 00 0F 00 00 00 01 66     ......f
00019 | 1CF | 80 05 00 00 00 0F        ......
00019 | 1DC | 02 00 00 0C              ....
00039 | 21E | 03 E8 37 45 22 06 2F     ..7E"./
00015 | 244 | 00 00 00 01 07           .....
00039 | 294 | 04 0B 00 02 CF 5A 00 2C .....Z.,
00102 | 305 | 80 35                    .5
00100 | 309 | 00 00 00 00 00 00 00 B1 ........
00099 | 320 | 00 00 30                 ..0
00099 | 324 | 74 65 00 00 00 00 0E 38 te.....8
00099 | 333 | 00 00 00 00 00 00 3C     ......<
00099 | 37C | FD 00 FD 00 09 7F 00 38 .......8
00299 | 405 | 00 00 04 00 00 00 00 0B ........
00300 | 40C | 02 36 32 32 39 53 30 39 .6229S09
00299 | 428 | 01 04 00 00 52 1C 01     ....R..
00299 | 454 | 23 EF 36                 #.6
01001 | 5A1 | 96 00 00 00 00 00 62 3E ......b>
```

Security POV

Application Layer

- Ford Escape
  - IDH: 03, IDL: B1, Len: 08, Data: 80 00 00 00 00 00 00 00
- Toyota Prius
  - IDH: 00, IDL: B6, Len: 04, Data: 33 A8 00 95

CAN Frame


Complete CAN Frame
Arbitration Field
11
Control
4
Data
8
CRC Field
15
End of Frame
Start of Frame
ID10 ID9 ID8 ID7 ID6 ID5 ID4 ID3 ID2 ID1 ID0
Requ. Remote
ID Ext. Bit
Reserved
DL3 DL2 DL1 DL0
DB7 DB6 DB5 DB4 DB3 DB2 DB1 DB0
CRC14 CRC13 CRC12 CRC11 CRC10 CRC9 CRC8 CRC7 CRC6 CRC5 CRC4 CRC3 CRC2 CRC1 CRC0
CRC Delimiter
Acknow. Slot Bit
Acknow. Delimiter
EOF6 EOF5 EOF4 EOF3 EOF2 EOF1 EOF0
IFS2 IFS1 IFS0
DATA
0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 1 1 1 1 1 1 1 1 1
CAN HI
CAN LO

Arbitration Field
Control Field
Data Field
ACK
Delimiter
SOF
ID part 1
RTR
IDE
r0
DLC
DATA (0-8 bytes)
CRC code
EOF
1
11
1
1
1
4
Max 64 data bits
15
1 1 1
7

CAN High and Low

Lowest ID = Highest Priority

High priority = ABS, Airbags…

Low priority = AC, Climate control…

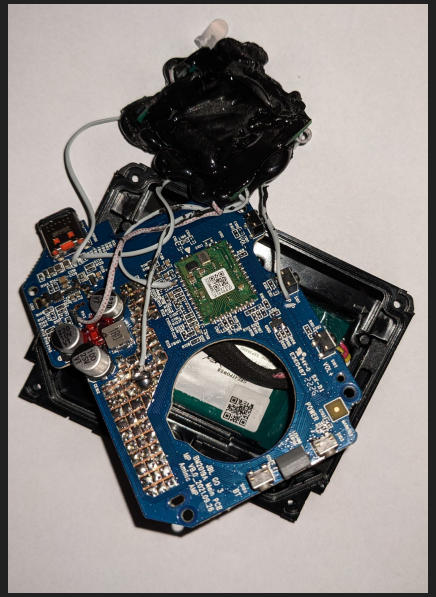
CAN FRAME

ID	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
0x111	0x0B	0xB8	0xED	0xAB	0xEF	0xEE	0xDC	0XAB

ID	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
0x111	0x0B	0xB8	0xED	0xAB	0xEF	0xEE	0xDC	0XAB

Case Study 0

https://kentindell.github.io/2023/04/03/can-injection/



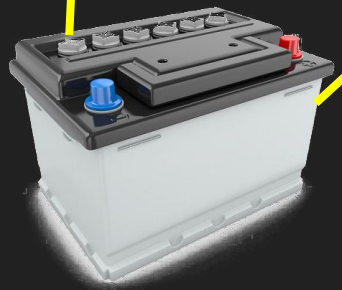
Case Study 1

Own Hyundai, Kia car? Report claims it's easier to steal as thieves can hack key

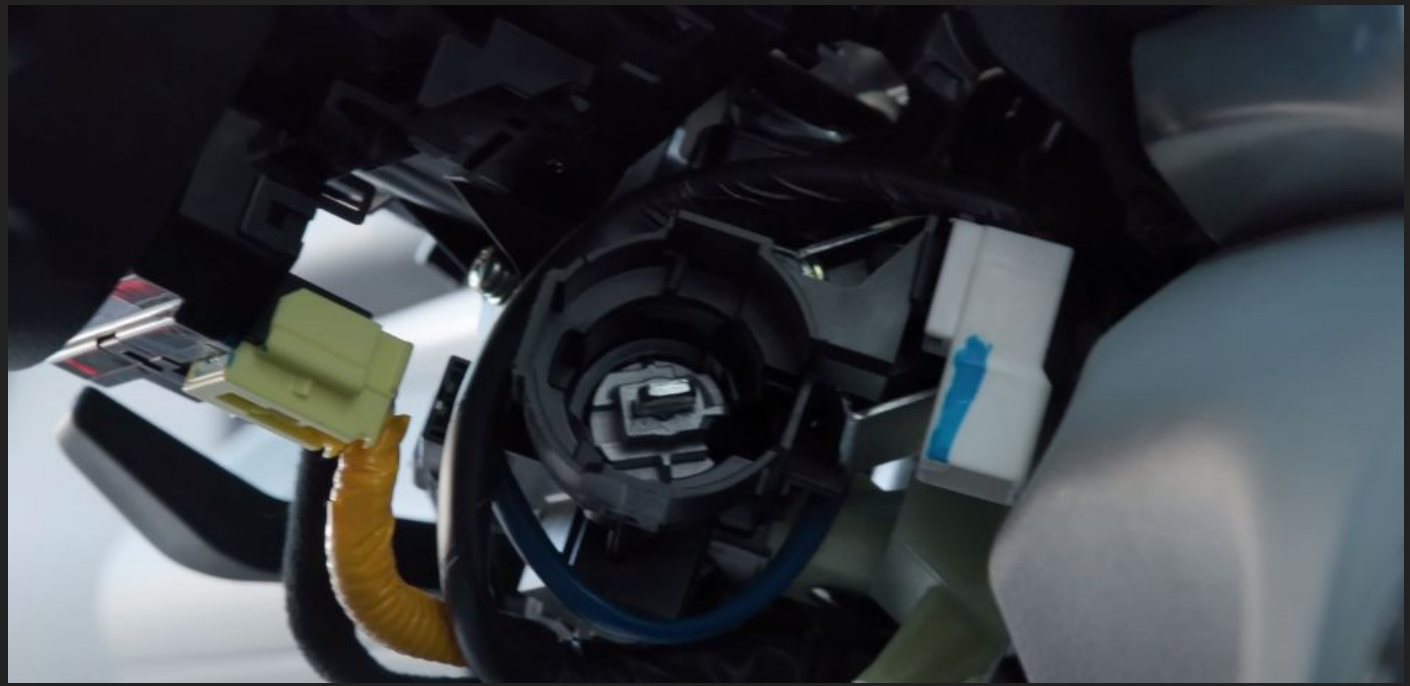
Recent videos show how thieves pry the ignition cover off Hyundai and Kia cars and use a screwdriver or USB cable to start them and drive away.

By : AP | Updated on: 23 Sep 2022, 12:07 PM


LOCK
UNLOCK



Insecure Design



Case Study 2


Premium IN
Search
1:33 / 5:06
Hackers Remotely Kill a Jeep on a Highway | WIRED
4,323,791 views • 21 Jul 2015
39K
DISLIKE
SHARE
DOWNLOAD
CLIP
SAVE

Case Study: 3

Teslamate Hack by David Columbo: TM is a powerful, self-hosted data logger for your Tesla.

Written in Elixir.

Data is stored in a Postgres database.

Visualization and data analysis with Grafana

Research

CVE-2024-39339

```
Starting Nmap 7.92 ( https://nmap.org ) at 2
Nmap scan report for 192.168.41.1
Host is up (0.013s latency).
Not shown: 65529 closed tcp ports (conn-refu
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
1221/tcp  open  sweetware-apps
3490/tcp  open  colubris
7000/tcp  open  afs3-fileserver
29101/tcp open  unknown
```

Information Disclosure

```
Answered, ID: 94, name: Shine Mom, number: +919645991556
Answered, ID: 97, name: Shine Mom, number: +919645991556
Missed, ID: 12, name: Mohd Shine, number: +917593937613
Missed, ID: 13, name: Mohd Shine, number: +917593937613
Answered, ID: 98, name: Mohd Shine, number: +917593937613
Missed, ID: 15, name: Mohd Shine, number: +917593937613
Missed, ID: 16, name: Mohd Shine, number: +917593937613
Missed, ID: 18, name: Mohd Shine, number: +917593937613
Missed, ID: 20, name: Mohd Shine, number: +917593937613
Missed, ID: 24, name: Mohd Shine, number: +917593937613
```

Voice Chat History

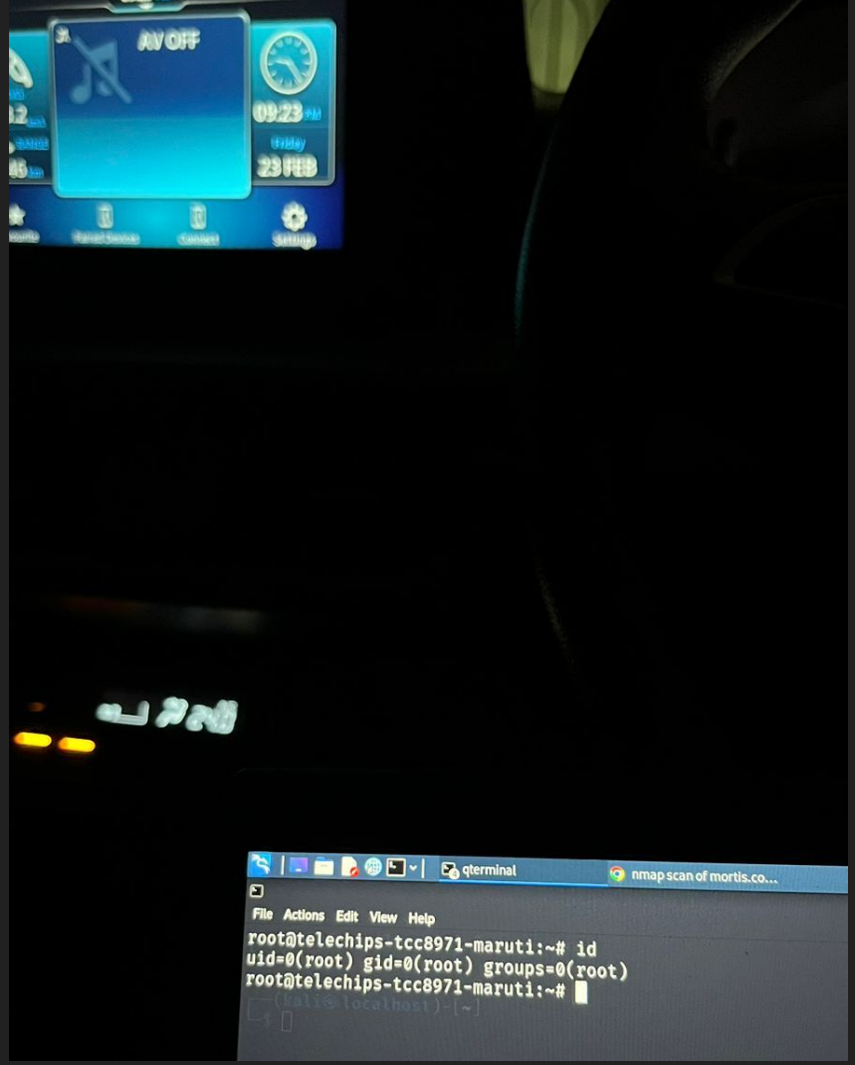
```
Calling SREEDEVI KUNJAMMA at Mobile.
Calling SREEDEVI KUNJAMMA at Mobile...
21:00:24.969 @SpeechMgr    req:play(node(IV_VR), Exit, id(1), text(str(Calling SREEDEVI KUNJAMMA at Mobile.)),message(3))
21:00:24.969 @SpeechMgr    Receive message=[voiceout(SpeechApp)/req:play(node(IV_VR), Exit, id(1), text(str(Calling SREEDEVI KUNJAMMA at Mobile.)),message(3))]
req:play(node(IV_VR), Exit, id(1), text(str(Calling SREEDEVI KUNJAMMA at Mobile.)),message(3))
rcv:req:play(node(IV_VR), Exit, id(1), text(str(Calling SREEDEVI KUNJAMMA at Mobile.)),message(3))
<FlowIfcSpeechMgr.cpp:158>[FlowIfcSpeechMgrRequestStartOutputTextGuide][Message Sent] req:play(node(IV_VR), Exit, id(1), text(str(Calling SREEDEVI KUNJAMMA at Mobile.)),message(3))
<FlowCmdManager.cpp:3374>[FlowCmdMngOutputExecEndGuide] ExecEndGuide:text(str(Calling SREEDEVI KUNJAMMA at Mobile.))
```

GPS History

```
gpsd:ERROR: UBX-NAV-SOL: time=nan lat=nan lon=nan alt=nan track=nan\x0a  speed=nan climb=nan mode=2 status=5 used=0
gpsd:ERROR: NAV-PVT: flags=21 time=nan lat=8.60 lon=76.86 alt=-3.77\x0a  track=194.44 speed=0.00 climb=nan mode=2 status=5 used=0
gpsd:ERROR: UBX-NAV-SOL: time=nan lat=nan lon=nan alt=nan track=nan\x0a  speed=nan climb=nan mode=2 status=5 used=0
gpsd:ERROR: NAV-PVT: flags=21 time=nan lat=8.60 lon=76.86 alt=-3.77\x0a  track=194.44 speed=0.00 climb=nan mode=2 status=5 used=0
gpsd:ERROR: UBX-NAV-SOL: time=nan lat=nan lon=nan alt=nan track=nan\x0a  speed=nan climb=nan mode=2 status=5 used=0
gpsd:ERROR: NAV-PVT: flags=21 time=nan lat=8.60 lon=76.86 alt=-3.77\x0a  track=194.44 speed=0.00 climb=nan mode=2 status=5 used=0
gpsd:ERROR: UBX-NAV-SOL: time=nan lat=nan lon=nan alt=nan track=nan\x0a  speed=nan climb=nan mode=2 status=5 used=0
gpsd:ERROR: NAV-PVT: flags=21 time=nan lat=8.60 lon=76.86 alt=-3.77\x0a  track=194.44 speed=0.00 climb=nan mode=2 status=5 used=0
gpsd:ERROR: UBX-NAV-SOL: time=nan lat=nan lon=nan alt=nan track=nan\x0a  speed=nan climb=nan mode=2 status=5 used=0
gpsd:ERROR: NAV-PVT: flags=21 time=nan lat=8.60 lon=76.86 alt=-3.77\x0a  track=194.44 speed=0.00 climb=nan mode=2 status=5 used=0
gpsd:ERROR: UBX-NAV-SOL: time=nan lat=nan lon=nan alt=nan track=nan\x0a  speed=nan climb=nan mode=2 status=5 used=0
gpsd:ERROR: NAV-PVT: flags=21 time=nan lat=8.60 lon=76.86 alt=-3.77\x0a  track=194.44 speed=0.00 climb=nan mode=2 status=5 used=0
gpsd:ERROR: UBX-NAV-SOL: time=nan lat=nan lon=nan alt=nan track=nan\x0a  speed=nan climb=nan mode=2 status=5 used=0
gpsd:ERROR: NAV-PVT: flags=21 time=nan lat=8.60 lon=76.86 alt=-3.77\x0a  track=194.44 speed=0.00 climb=nan mode=2 status=5 used=0
gpsd:ERROR: UBX-NAV-SOL: time=nan lat=nan lon=nan alt=nan track=nan\x0a  speed=nan climb=nan mode=2 status=5 used=0
gpsd:ERROR: NAV-PVT: flags=21 time=nan lat=8.60 lon=76.86 alt=-3.77\x0a  track=194.44 speed=0.00 climb=nan mode=2 status=5 used=0
gpsd:ERROR: UBX-NAV-SOL: time=nan lat=nan lon=nan alt=nan track=nan\x0a  speed=nan climb=nan mode=2 status=5 used=0
gpsd:ERROR: NAV-PVT: flags=21 time=nan lat=8.60 lon=76.86 alt=-3.77\x0a  track=194.44 speed=0.00 climb=nan mode=2 status=5 used=0
```

Research

CVE-2024-6245



Mobile Apps in IOT device Integration

- Home Automation
- Retail Experience
- IOT wearables
- Automotive Industry

Advantages of using mobile apps in cars?

- Use it instead of key fobs
- RSA
- Easy to use
- Track your car

TCU

Telematics control unit (TCU) is the embedded onboard system that controls wireless tracking, diagnostics and communication to and from the vehicle.

It has the following components:

- A satellite navigation system / GNSS unit
- A microcontroller
- A mobile networking unit
- An external unit for cellular communication (GSM, GPRS, Wi-Fi, WiMax, LTE or 5G) which provides the tracked values to a centralized geographical information system (GIS) database server
- A unit that processes electrical signals
- A storage unit
- Battery module

Story

Internet-Connected Trucks Can Be Tracked and Hacked, Researcher Finds

Insecure configurations expose car telematics to hacking

Mar 6, 2016 23:28 GMT · By Catalin Cimpanu · Comment · Share:

Industrial vehicles like trailer trucks, delivery vans, or buses that have an Internet connection, can be tracked, and even hacked, if they use insecure and improperly-configured TGUs (Telematics Gateway Units), security researcher Jose Carlos Norte claims.

Telematics expose trucks, vans, and buses to ...

TGU devices, or telematics, are basically a portable 3G, 4G, GPRS, LTE, Edge, HDSPA Internet modem. Most companies use TGUs in their vehicles as a way to track the movement of their trucks, and to keep in touch with the drivers, optionally sending them new routes, orders, and other valuable information they might need to ship their cargo.

What is a Telematics Gateway Unit?

Telematics Gateway Unit – A Telematics Gateway Unit has a high-performing Application Processor Hardware Platform at its core. It offers various advantages when compared to a TCU. This includes higher data throughput and capacity to store offline data for a longer time.

SHODAN | Explore | Downloads | Pricing | port:23 [redacted] | Account

View Report | Download Results | Historical Trend | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

TOTAL RESULTS

228

TOP COUNTRIES

Spain	138
Morocco	41
Germany	35
France	11
Belgium	2

More...

TOP ORGANIZATIONS

GLOBAL MOBILE OPERATOR	78
Telekom Deutschland GmbH	35
Office National des Postes et Telecommunications ONPT (Maroc Telecom) / IAM	29
VODAFONE ESPANA S.A.U.	24
ONO_Mobile&Wifi	18

More...

[redacted]

Telekom Deutschland GmbH

Germany, Bayreuth

2022-04-27T18:53:43.861189

[redacted]

GLOBAL MOBILE OPERATOR

Spain, Barcelona

2022-04-27T09:26:13.691903

[redacted]

Office National des Postes et Telecommunications ONPT (Maroc Telecom) / IAM

Morocco, Tangier

2022-04-27T08:32:50.758364

[redacted]


root@jarvis:~# telnet
Trying
Connected to
Escape character is '^]'.
Welcome on console
Help :
cmd [option1|option2]{string}(number)
Builtins :
cversion Console version
help Display help
screen [(X)] Change to screen X. If no argument, display screens list
color [0|1] Enable/Disable color output
lang [{str}] Set the console language
reboot [(waitTime)] Reboot
completion Activate advanced completion
exit Quit
Basics :
1wire Display 1wire information
iostate Display input/output state
modem Display modem state
gpspos Retrieve last GPS position
list [all|{module}][dl] List available modules.
[all] List all available modules parameters.
[module] List available module parameters.
[dl] Download result.
g {module} {parameter} [(index)] Get module parameter value
s {module} {parameter} [(index)] {value} Set module parameter value
listdb List available DB parameters
gdb {name} Get a DB parameter
sdb {name} {value} Set a DB parameter
log [print|debug|warn|error|{str}] Display last logs
logdump [print|debug|warn|error|{str}] Display all logs
configure Upload a new conf file
Basics[C4E]>
Basics[C4E]> screen
screen 0 Basics
screen 1 Advanced
screen 2 Commands

Getting GPS info

```
Basics[C4E]> gpspos
Internal antenna
GPRMC Frame value is
$GPRMC,201728.21,A,5241.1211,N,00850.1809,E,0.000,0.000,270422,0,W,A*39

GPGGA Frame value is
$GPGGA,201728.21,5241.1211,N,00850.1809,E,1,12,0.739,86.411,M,42.300,M,0,0*5C
```

Advanced Screen

```
Advanced :
ip [{str}]              Display all ip addresses. If str, display only str address.
stats                   Display stats.
llog [soft|gps|update|kstart|mAT|mPPP] Display last logs of:
                        software, gps, kernel start, modem AT, or modem PPP
skey [update|delete] Update|Delete server key
ukey [update|delete] Update|Delete user key
logs [get|delete][all|{filename}|crashes] Retrieve or Delete logs of sofware
stopsoft                Stop the software
usercpn [list|start|stop|remove][all|{cpnName}] List user components
gprsupdate [start|stop] Enable / Disable GRPS update
geomap [update|delete] Update / Delete a geofencing map
update                  Upload an update package
restore [all|write|pdm|db|user] Restore parameters of write, db or pdm
restoreFull             Restore device to the initial configuration state
version                 Display software/hardware version
remote [{ip}]           Console on remote device
cpu [{cpnName}]         Get CPU usage for group

Advanced[C4E]> ip
lo      127.0.0.1
usb0:1  192.168.10.3
ppp0    [redacted]
```

Screen 2 : Commands

```
Advanced[C4E]> screen 2
Commands :
clist               List available commands
chelp {cmdName}     Display command help
cxelp {cmdRName}    Find and display command help
crun {cmdName}[{cmdArgs}] Run the command
cexe {cmdRName}[{cmdArgs}] Find and run the command (example : cexe .*_EnergyReferee.cmd  ... )
```

List of commands

```
Commands[C4E]> clist
MainProc_ChronoTachyGraph.cmd
bootProc_DB.cmd
networkProc_DataWatchdog.cmd
MainProc_VersionManager.cmd
networkProc_GatewayMode.cmd
MainProc_Can.cmd
networkProc_NetMonitoring.cmd
bootProc_DBTools.cmd
pdmProc_Pdm.cmd
MainProc_GpsOdometer.cmd
MainProc_AnalogInputs.cmd
MainProc_Gps.cmd
MainProc_Alarm.cmd
bootProc_ConfigAccess.cmd
MainProc_UsbManager.cmd
bootProc_BootCommand.cmd
bootProc_EnergyReferee.cmd
networkProc_SerialPPPManager.cmd
networkProc_HfkControl.cmd
bootProc_Config.cmd
networkProc_CriticalCommandManager.cmd
bootProc_IdleCommand.cmd
networkProc_Update.cmd
MainProc_DigitalOutputs.cmd
bootProc_MessageBroker.cmd
bootProc_Watchdog.cmd
MainProc_Ignition.cmd
networkProc_Modem.cmd
networkProc_SmsControl.cmd
MainProc_DigitalInputs.cmd
```

Google Ads


HONDA
The Power of Dreams
ALL NEW
CITY
CITY
CONTROL THE ALL-NEW CITY WITH JUST YOUR VOICE.
The All-New City works with Ok Google.
works with
Ok Google
Google is a trademark of Google LLC.

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Become a Member | Best Practice Guide | Our Membership

Our Members

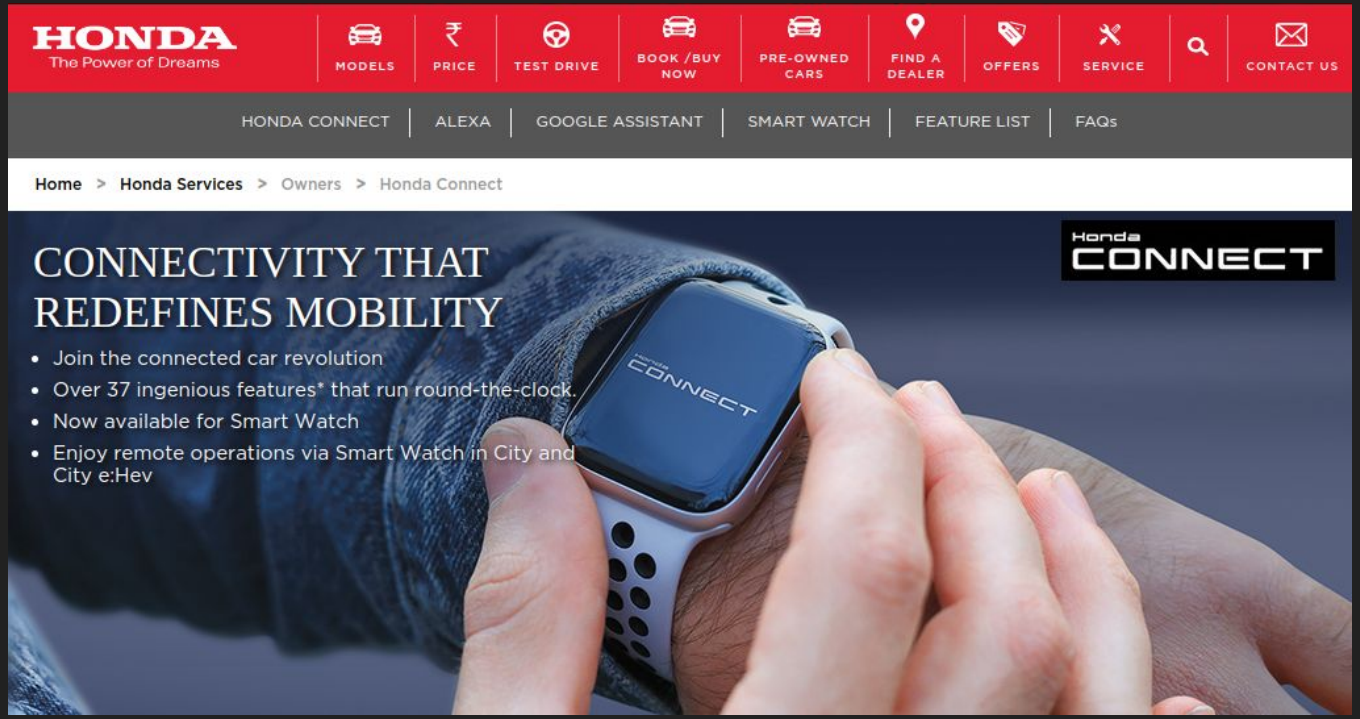

Search

AUTO-ISAC

Auto-ISAC, Inc. • 20 F Street NW, Suite 700 • Washington DC 20001 • Privacy Policy

Auto-ISAC Issues “Software Bill of Materials” Informational Report

Honda Connect



Vehicle used for testing

- Honda City 5th Generation

Features of Honda Connect

- Tire Deflation Alert
- Roadside Assistance
- Service Scheduler
- Payment Gateway
- Tow Away Alert
- Find My Car
- Remote Operations
- Car Dashboard
- Share Car Location
- Trip Diary
- Live Car Location
- Stolen Vehicle Tracking
- Geo-Fence Alert
- Contextual Speeding Alert
- Auto Crash Notification
- Unauthorized Access Alert

Interesting Features of Honda Connect

- AC On/Off
- Door Lock/Unlock
- Boot Open
- Car Finder

Static Analysis

```
68.
69.     invoke-interface {v1}, Lg0/a/a;->get()Ljava/lang/Object;
70.
71.     move-result-object v1
72.
73.     check-cast v1, Lokhttp3/OkHttpClient;
74.
75.     .line 2
76.     invoke-static {v0}, Ljava/util/Objects;->requireNonNull(Ljava/lang/Object;)Ljava/lang/Object;
77.
78.     .line 3
79.     new-instance v1, Lj0/e0$b;
80.
81.     invoke-direct {v1}, Lj0/e0$b;-><init>()V
82.
83.     const-string v2, "https://prodapi.hondaconnect.in"
84.
85.     .line 4
86.     invoke-virtual {v1, v2}, Lj0/e0$b;->a(Ljava/lang/String;)Lj0/e0$b;
87.
88.     .line 5
89.     invoke-static {}, Lj0/k0/a/a;->c()Lj0/k0/a/a;
90.
91.     move-result-object v2
92.
93.     .line 6
94.     iget-object v3, v1, Lj0/e0$b;->d:Ljava/util/List;
95.
```

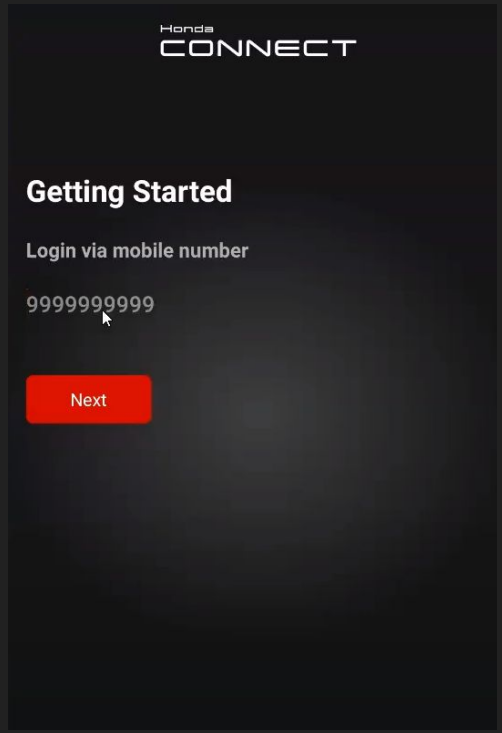
Security Controls

- Root Detection
- SSL Pinning

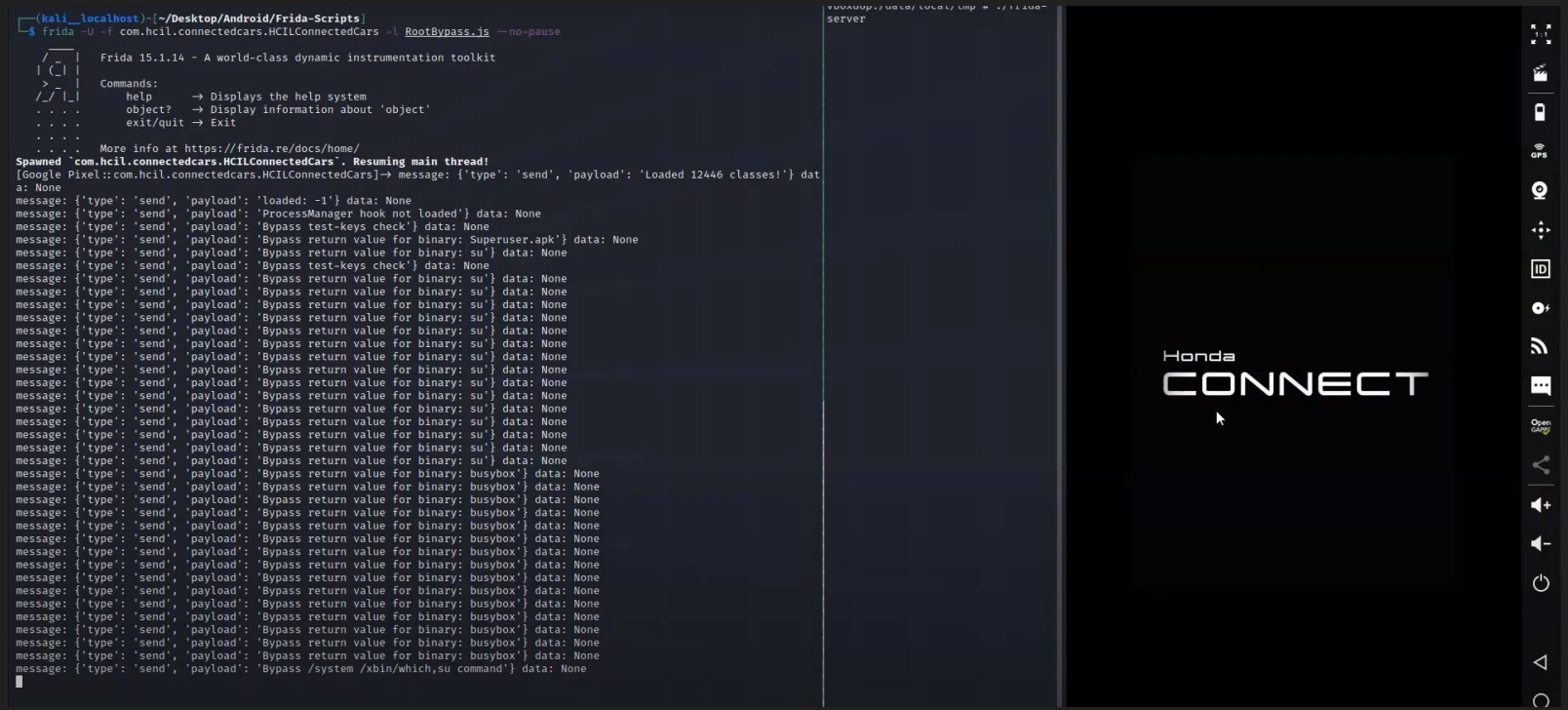
Tools of the trade

- Genymotion
- Frida
- BurpSuite/Httptoolkit

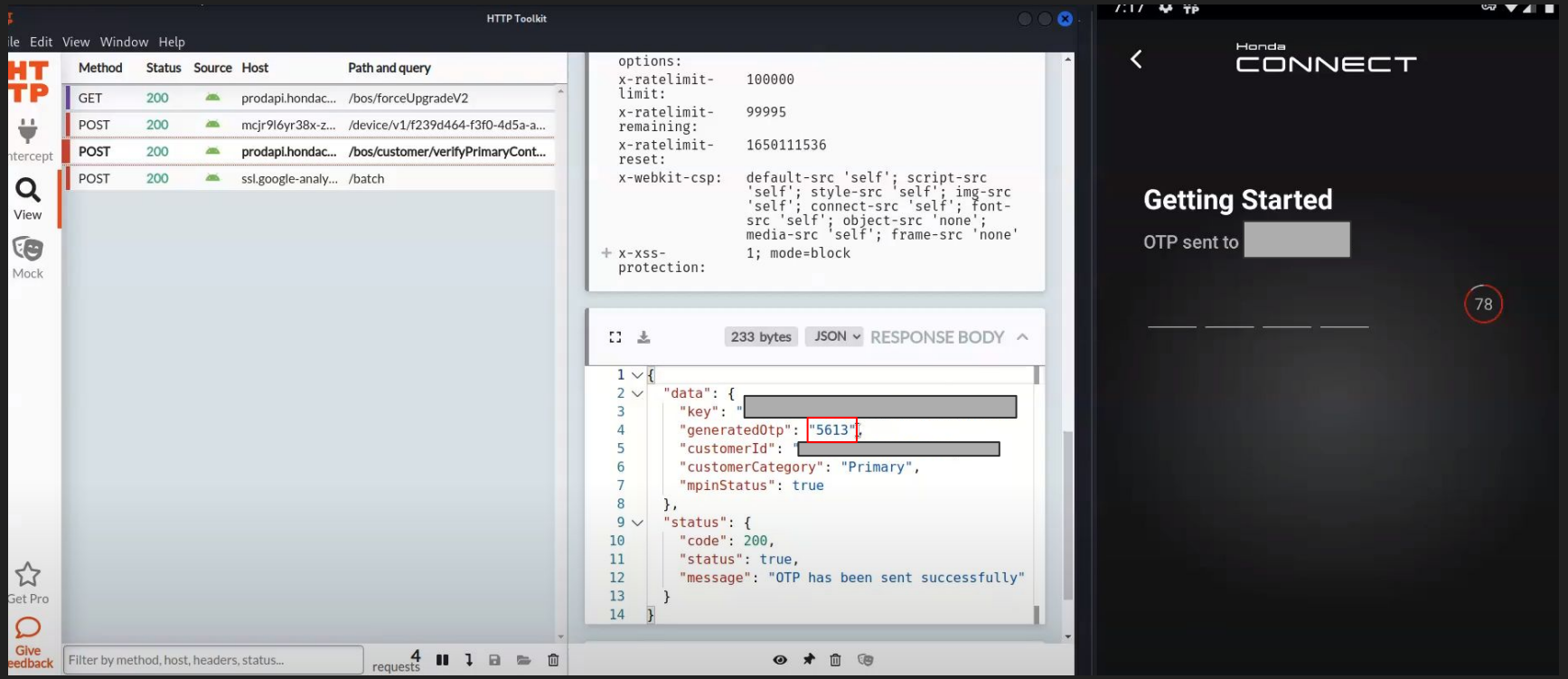
Getting started



Bypassing the Root Detection



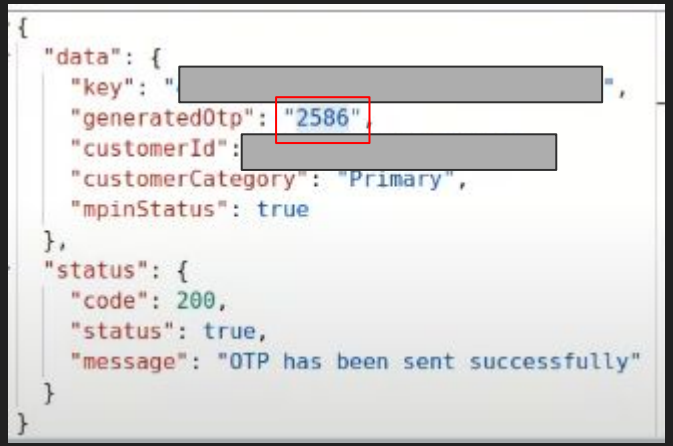
Traffic Analysis



Honda CONNECT

Enter mPIN

Forgot mPIN?

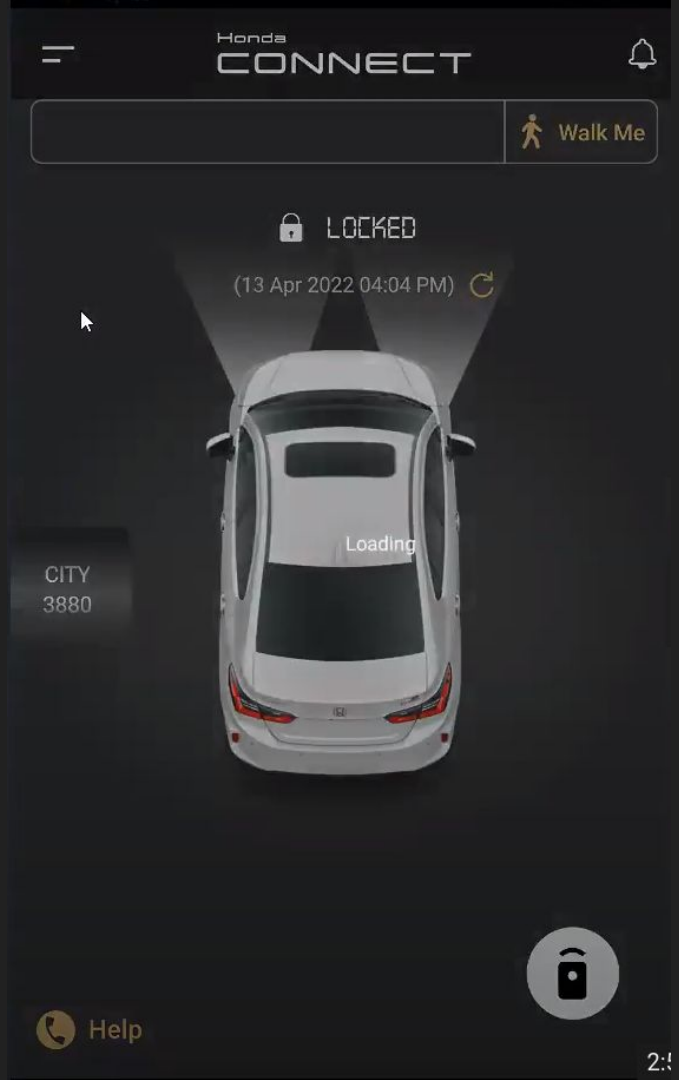


Honda CONNECT

Reset mPIN

Enter mPIN

Confirm mPIN


Honda
CONNECT
Walk Me
LOCKED
(13 Apr 2022 04:04 PM)
Loading
CITY
3880
Help

Exploitation

Disclosure

AutoISAC

ASRG

Bugcrowd/Hackerone/Intigriti

Thank you