

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

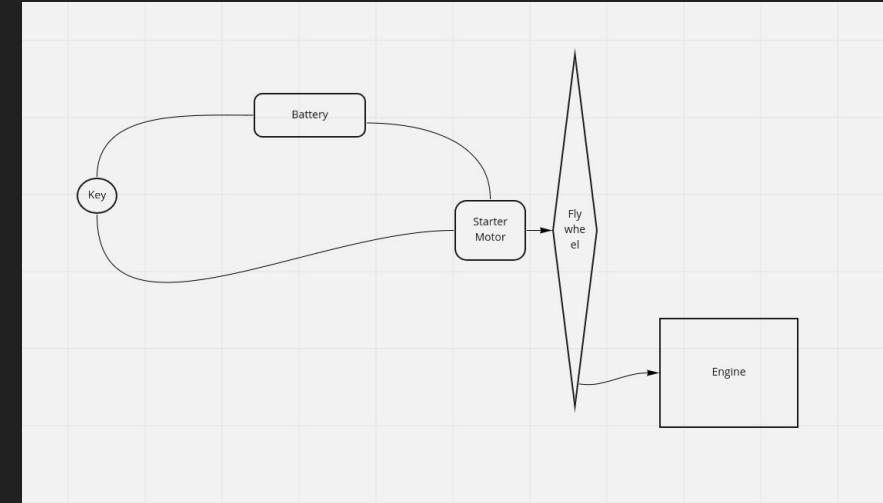
Attack Surface

Attacks

Case studies/Research

Resources

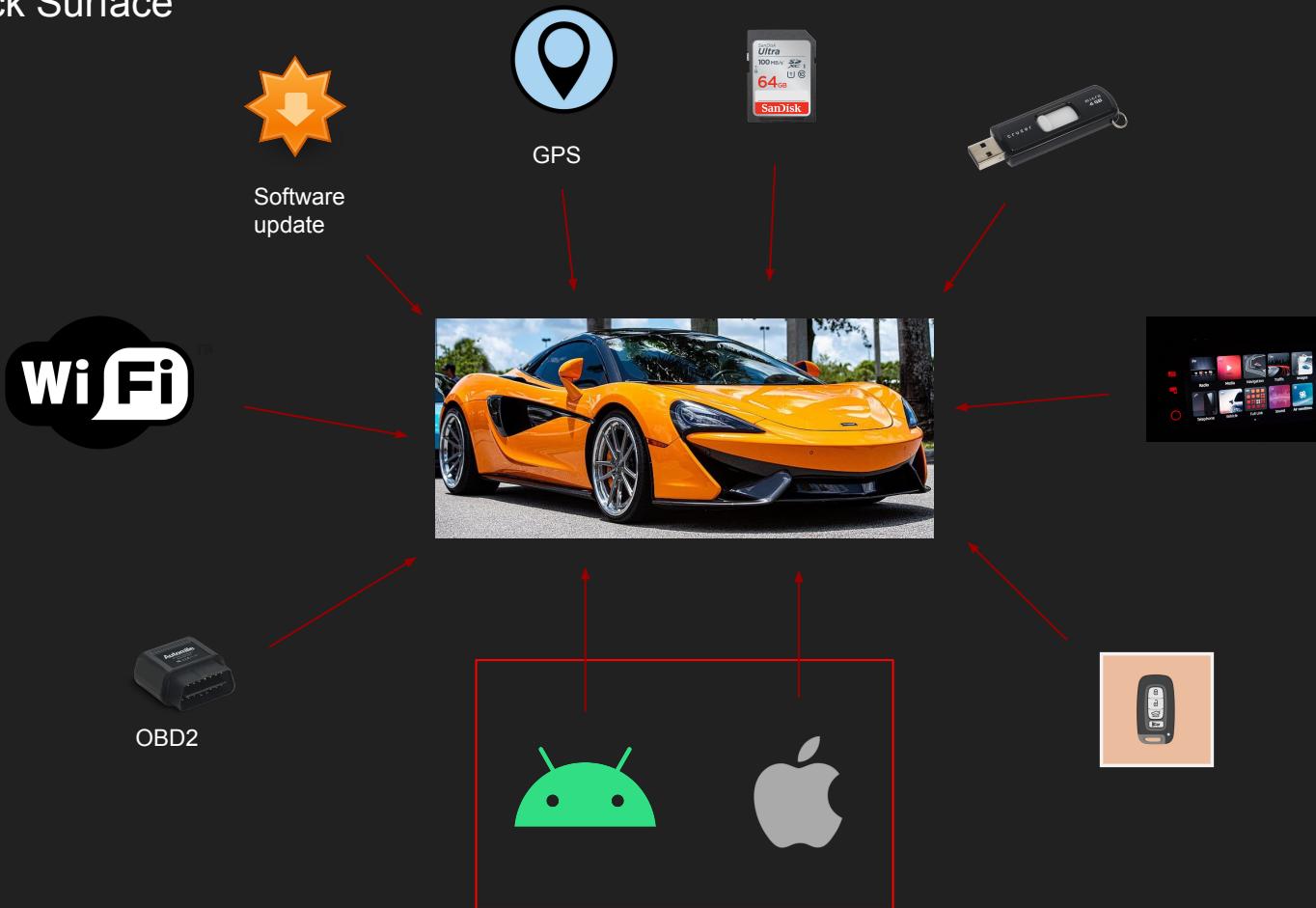
Cars before the 80's



Modern Vehicle



Attack Surface



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



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

```
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);
```



Source: Roland Berger 2015

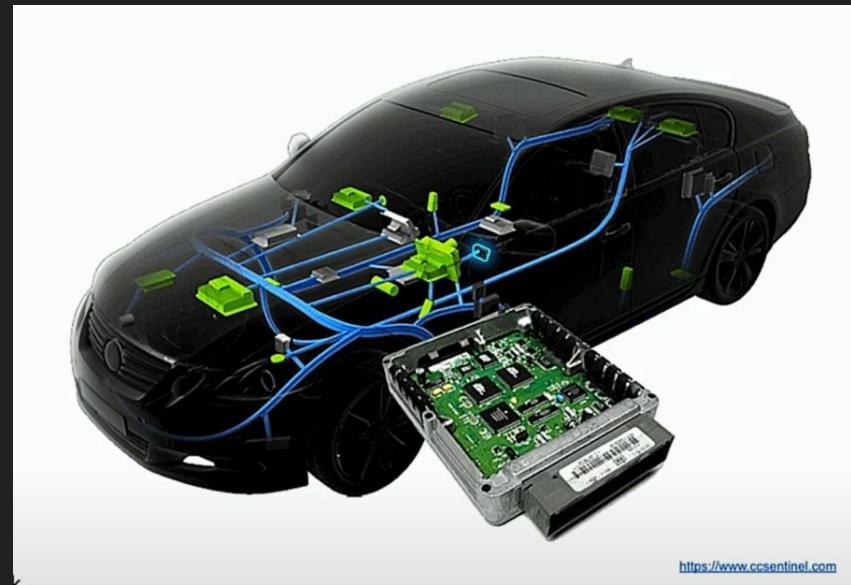
altran

Sensors and ECU

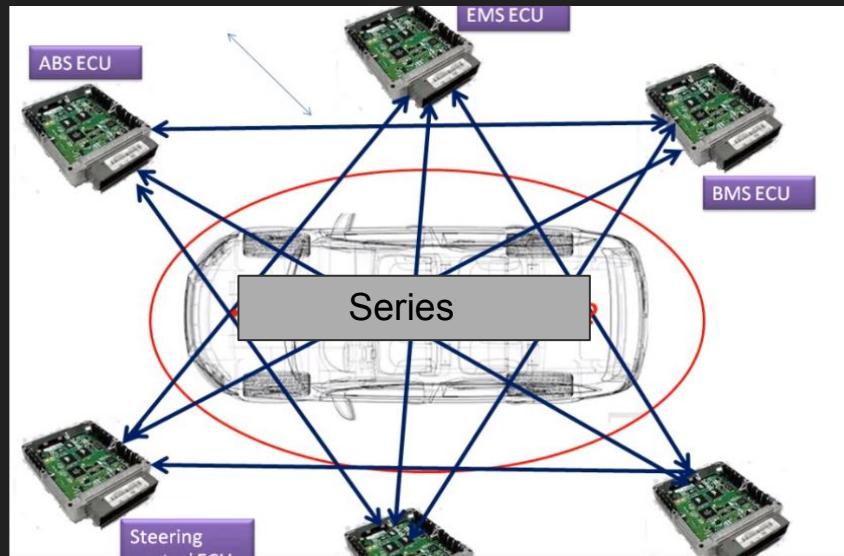
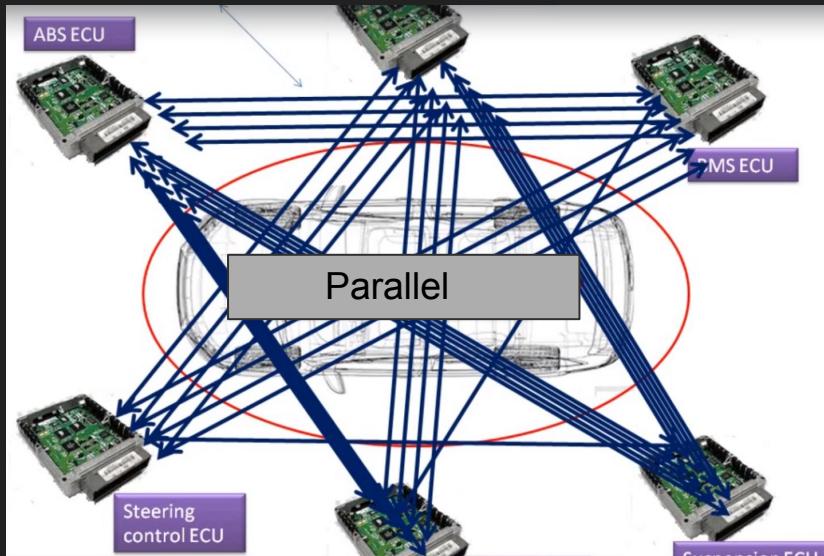
Modern Cars are a combination of Software and Hardware

ECU- Engine/Electronic Control Unit

Sensors are the input devices



The Network



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

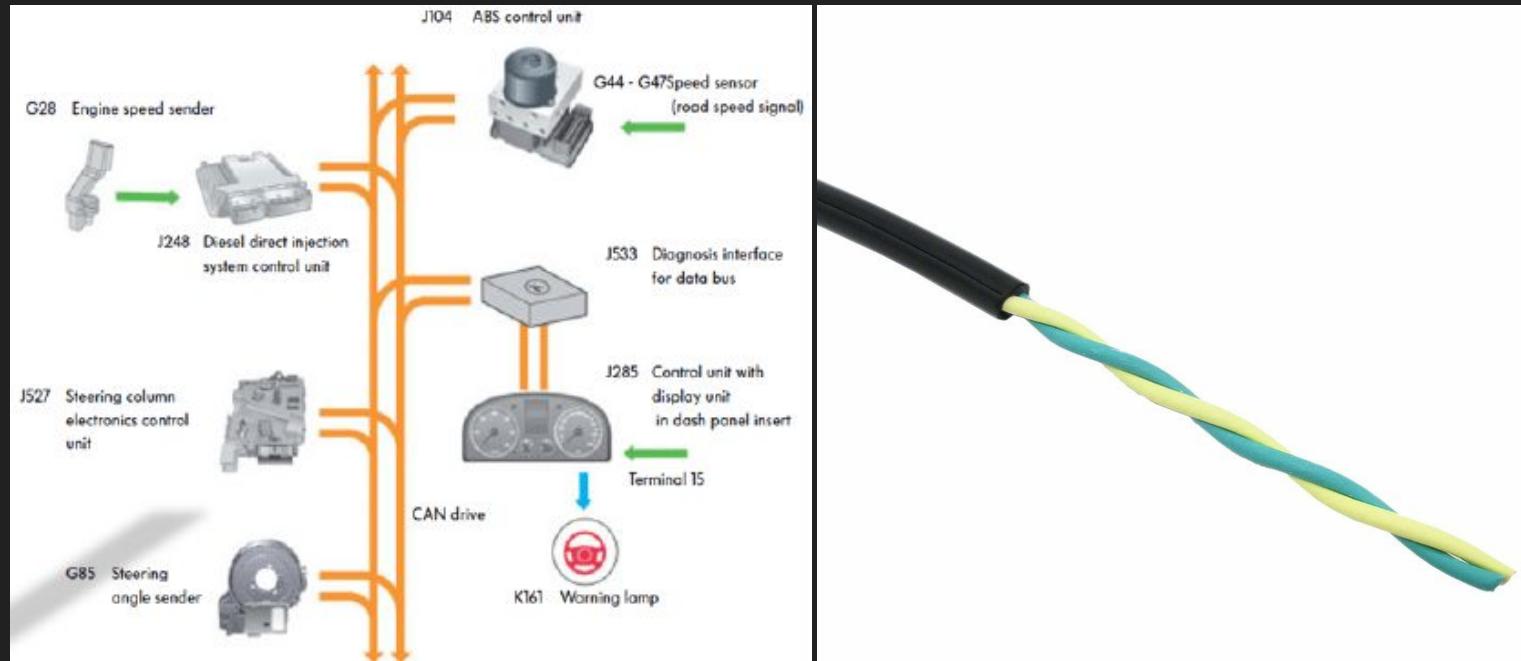
MOST Protocol: For Multimedia Devices

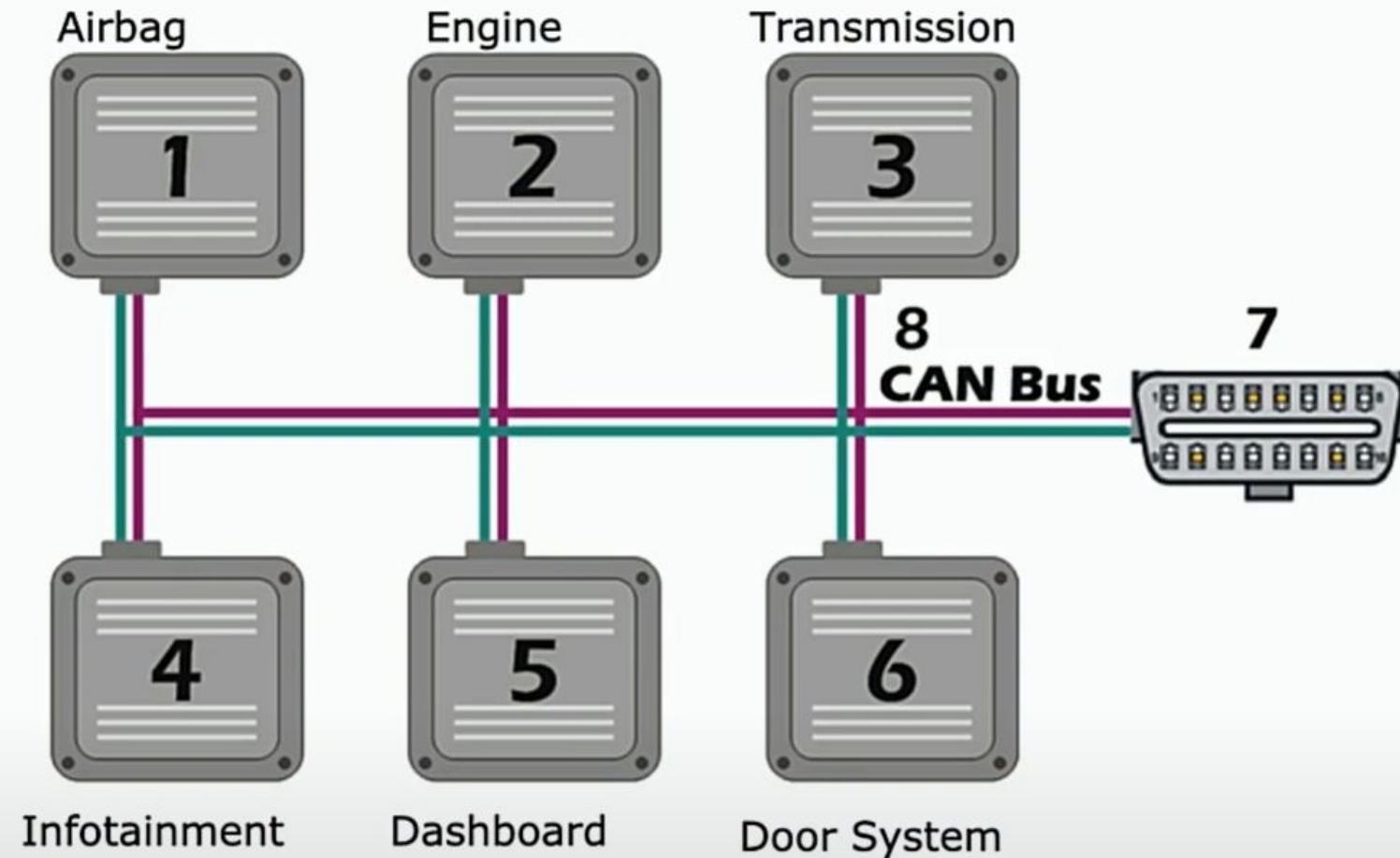
FlexRay : 10 Mbps (Sensitive communication)

Automotive Ethernet: Cheaper alternative to FlexRay and MOST

CAN BUS

Controller Area Network





Timeline

Before CAN : Vehicle Network Communication took place between complex point to point wiring system

1986 : The Protocol was released to SAE by Robert Bosch

1991 : CAN 2.0 was released

1993 : ISO 11898

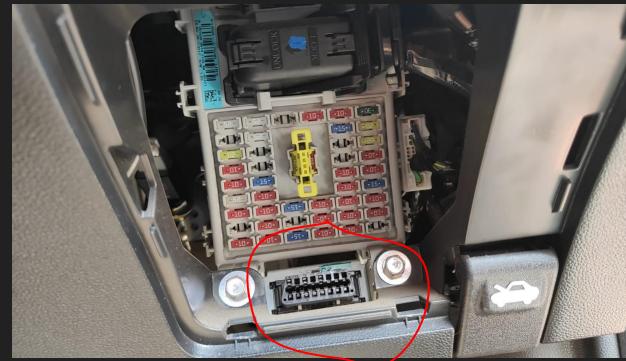
2003 : ISO 11898 became a standard series

Identify the CAN BUS and OBD Port

Twisted pair

Use a Multimeter - 2.5V

Resistance - 120 Ohms



Sniffing the CAN

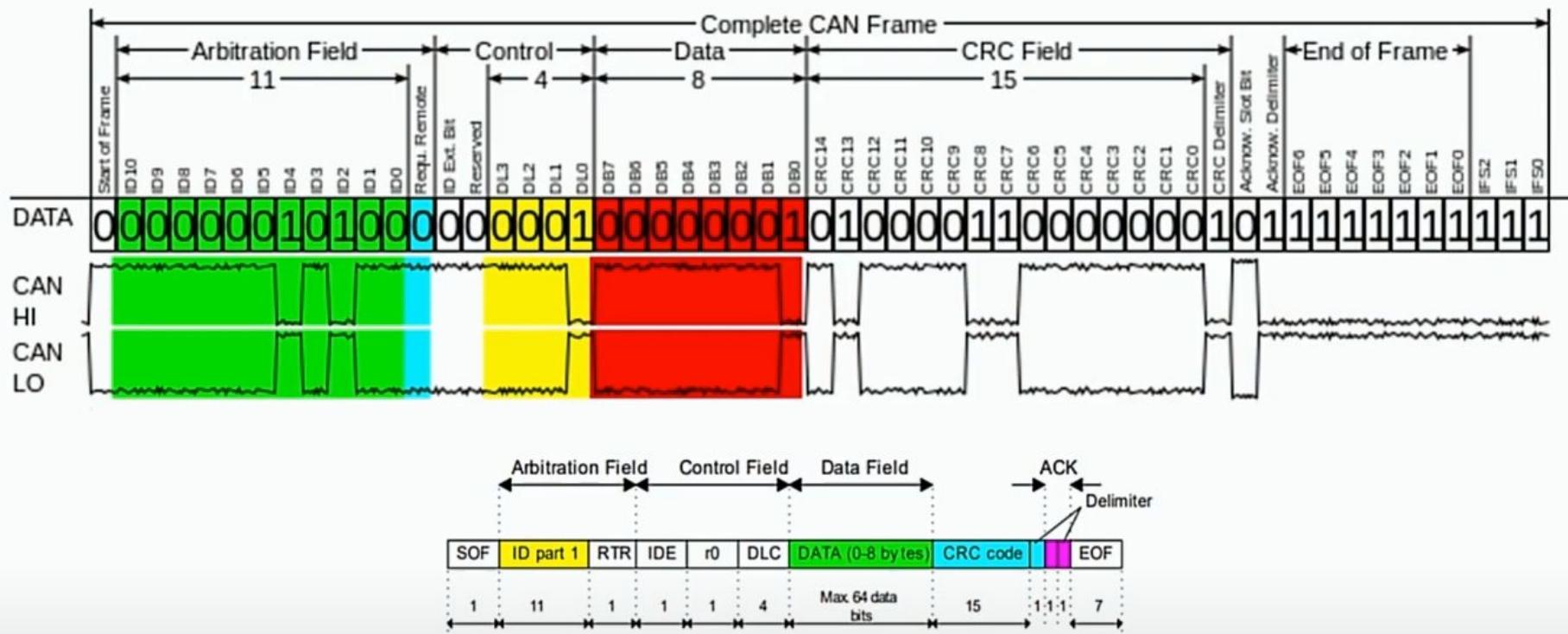
29 ms	ID	data ...	< vcan0 # l=20 h=100 t=500 slots=36 >
00014	039	00 1B	..
00009	095	80 00 07 F4 00 00 00 355 you likely
00009	133	00 00 00 00 89	try tools now:
00009	136	00 02 00 00 00 00 00 0C	common-minimum-setu
00009	13A	00 00 00 00 00 00 00 0A
00010	13F	00 00 00 05 00 00 00 0000
00009	143	6B 6B 00 C2	http://CarHack/ICSim
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	http://CarHack/2.../ICSim
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 21A.! /
00019	1A4	00 00 00 08 00 00 00 2F/
00020	1AA	7F FF 00 00 00 00 67 20g
00019	1B0	00 0F 00 00 00 01 66f
00019	1CF	80 05 00 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 2CZ.,
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 00 388
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 01R..
00299	454	23 EF 36	#.6
01001	5A1	96 00 00 00 00 00 62 3Eb>

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



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 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.

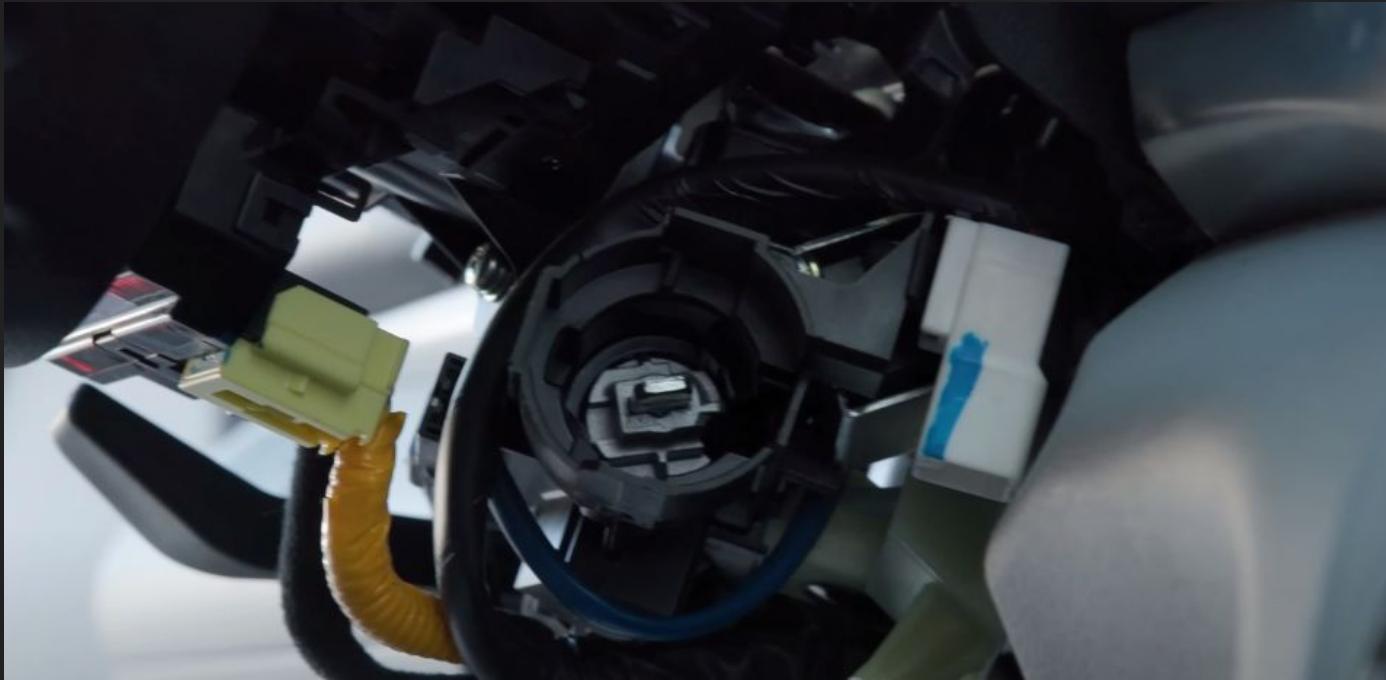
By : AP | Updated on: 23 Sep 2022, 12:07 PM







Insecure Design



Case Study 2

The image shows a screenshot of a YouTube video player. The video itself is titled "Hackers Remotely Kill a Jeep on a Highway | WIRED". It depicts two men, one in a blue jacket and one in a dark shirt, standing in front of a white wall. The video is playing at 1:33 / 5:06. The YouTube interface includes a search bar, a volume icon, and various interaction buttons like like, dislike, share, download, clip, save, and more.

YouTube Premium IN

Search

Hackers Remotely Kill a Jeep on a Highway | WIRED

4,323,791 views • 21 Jul 2015

1:33 / 5:06

39K DISLIKE SHARE DOWNLOAD CLIP SAVE ...

Case Study: 3

A 19-year-old security researcher describes how he remotely hacked into over 25 Teslas

Grace Kay

January 25, 2022 · 3 min read



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 2024-02-24 01:02 IST
Nmap scan report for 192.168.41.1
Host is up (0.013s latency).
Not shown: 65529 closed tcp ports (conn-refused)
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

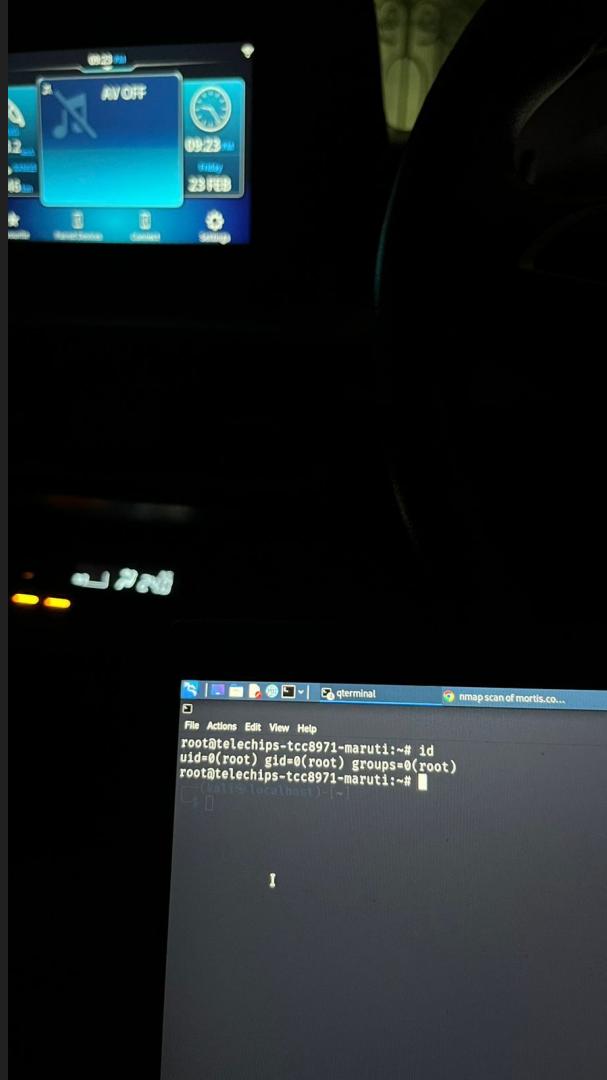
Voice Chat History

```
Calling SREEDEVI KUNJAMMA at Mobile. nam lon-nan alt-nan track-nan\x0a speed-nan climb-nan mode=2 status=5 used=0
Calling SREEDEVI KUNJAMMA at Mobile... -8.60 lon=76.86 alt=-3.77\x0a tracks19\x0a speed=0.00 climb-nan mode=2 status=5 used=0
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)) mode=2 status=5 used=0
rcv:req:play(node(IV_VR), Exit, id(1), text(str(Calling SREEDEVI KUNJAMMA at Mobile.)),message(3)) limb=nan mode=2 status=5 used=0
<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.)) mode=5 used=0
```

GPS History

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

Vehicle used for testing

- Honda City 5th Generation



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 [Twitter](#) · Comment · Share: [Twitter](#) [Reddit](#) [Facebook](#) [Google+](#) [Print](#)

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](#).

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.



[+ Telematics expose trucks, vans, and buses to ...](#)

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



Account

TOTAL RESULTS

228

[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](#)

2022-04-27T18:53:43.861189

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 29

ONPT (Maroc Telecom) / IAM 29

VODAFONE ESPANA S.A.U. 24

ONO_Mobile&Wifi 18

[More...](#)

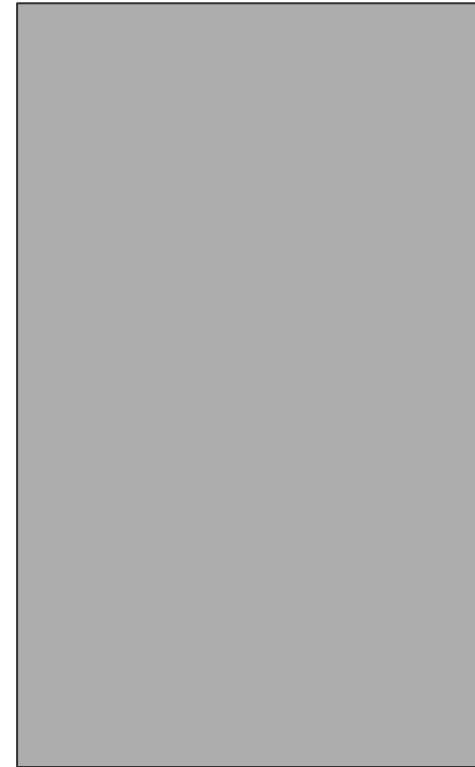
Telekom Deutschland GmbH

Germany, Bayreuth

GLOBAL MOBILE OPERATOR

Spain, Barcelona

2022-04-27T09:26:13.691903



2022-04-27T08:32:50.758364

```
root@jarvis:~# telnet [REDACTED]
Trying [REDACTED]
Connected to [REDACTED]
Escape character is '^J'.
Welcome on console
[REDACTED] 90.117.13.20 23
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]> screen

screen 0	Basics
screen 1	Advanced
screen 2	Commands

Basics[C4E]>

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 software
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

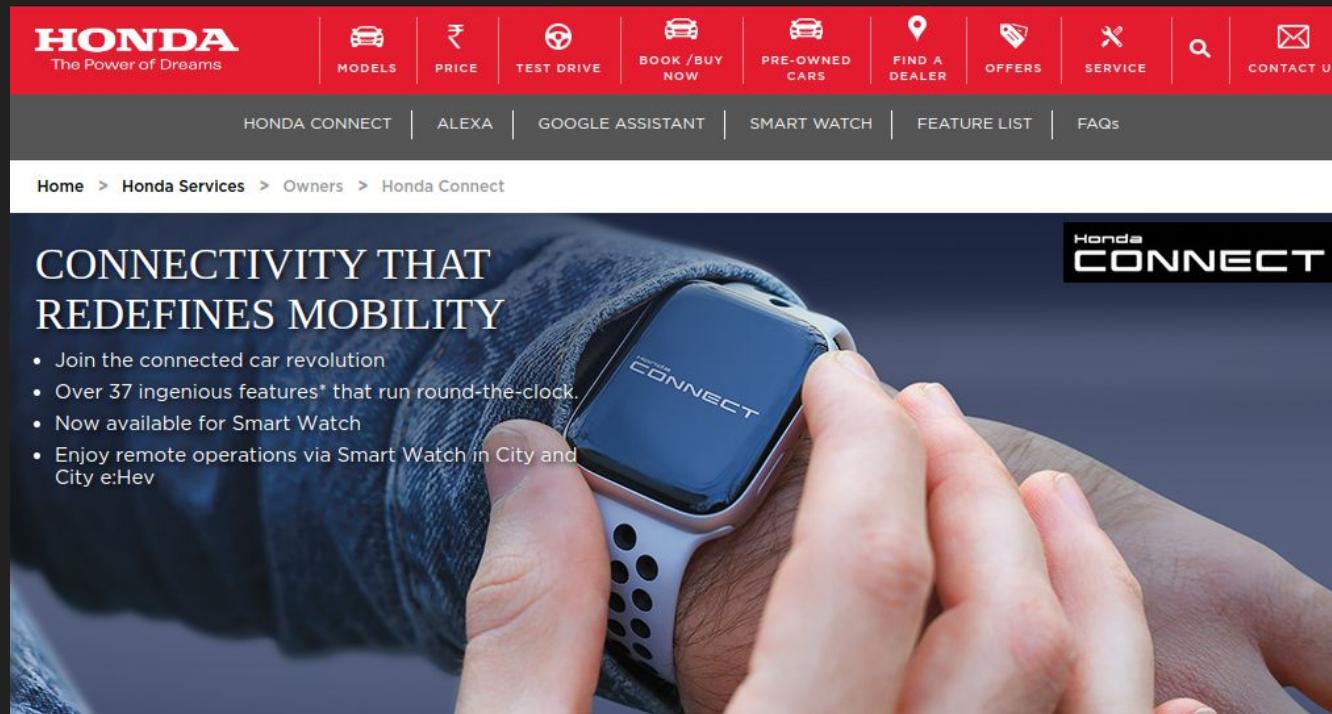
CITY

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.

Honda Connect



HONDA
The Power of Dreams

MODELS PRICE TEST DRIVE BOOK / BUY NOW PRE-OWNED CARS FIND A DEALER OFFERS SERVICE CONTACT US

HONDA CONNECT | ALEXA | GOOGLE ASSISTANT | SMART WATCH | FEATURE LIST | FAQs

Home > Honda Services > Owners > Honda Connect

CONNECTIVITY THAT REDEFINES MOBILITY

- Join the connected car revolution
- Over 37 ingenious features* that run round-the-clock.
- Now available for Smart Watch
- Enjoy remote operations via Smart Watch in City and City e:Hev

Honda CONNECT

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, L okhttp3/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.    igure-object v3, v1, Lj0/e0$b;->d:Ljava/util/List;
```

Security Controls

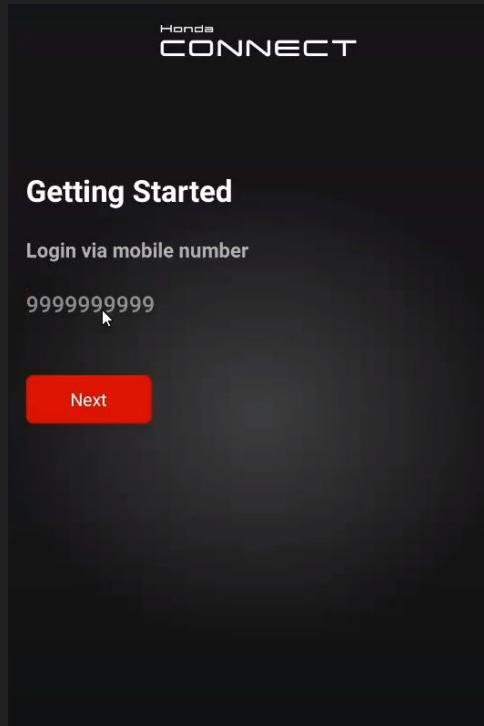
- Root Detection
- SSL Pinning



Tools of the trade

- Genymotion
- Frida
- BurpSuite/HttpToolkit

Getting started



Bypassing the Root Detection

Traffic Analysis

The screenshot displays the HTTP Toolkit interface on the left and the Honda CONNECT mobile application on the right.

HTTP Toolkit (Left):

- Toolbar:** File, Edit, View, Window, Help.
- Left Sidebar:** HT, TP, Intercept, View, Mock, Get Pro, Give feedback.
- Table:** Shows a list of API requests with columns: Method, Status, Source, Host, Path and query.
- Request Details:** A detailed view of a POST request to `/bos/customer/verifyPrimaryCont...` with status 200. Headers include:

 - options: x-rateLimit- 100000
 - limit: 99995
 - remaining: 1650111536
 - reset: 1650111536
 - x-webkit-csp: default-src 'self'; script-src 'self'; style-src 'self'; img-src 'self'; connect-src 'self'; font-src 'self'; object-src 'none'; media-src 'self'; frame-src 'none'
 - + x-xss-protection: 1; mode=block

- RESPONSE BODY:** JSON format showing the response data. The "generatedOtp" field is highlighted with a red box.

Honda CONNECT (Right):

- Header:** Honda CONNECT
- Section:** Getting Started
- Text:** OTP sent to [REDACTED]
- Notification:** A red circle with the number 78 is visible in the top right corner.

Enter mPIN

Forgot mPIN?

```
{  
    "data": {  
        "key": "██████████",  
        "generatedOtp": "2586",  
        "customerId": "██████████",  
        "customerCategory": "Primary",  
        "mpinStatus": true  
    },  
    "status": {  
        "code": 200,  
        "status": true,  
        "message": "OTP has been sent successfully"  
    }  
}
```

Reset mPIN

Enter mPIN

██████████

Confirm mPIN

██████████ |

Honda
CONNECT



Walk Me

LOCKED

(13 Apr 2022 04:04 PM)



CITY
3880



Help

2:
3

Exploitation



Disclosure

AutolSAC

Honda India

Thank you