TESLA

HACKING

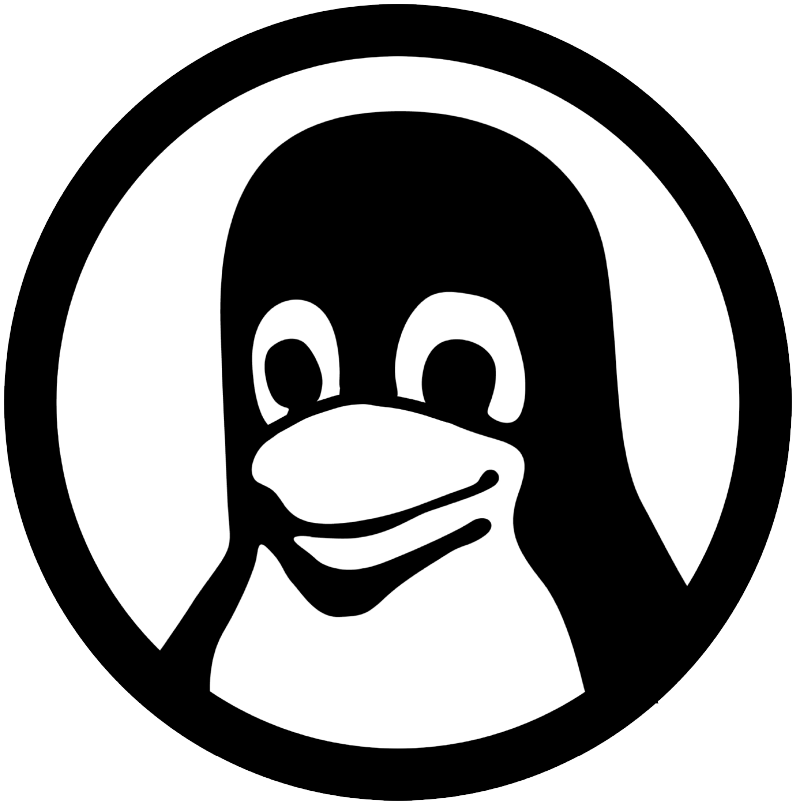
WORLD OF
TECHNOLOGY
& SCIENCE

https://www.slideshare.net/JasperNuyens/tesla-hacking-presentation-wots

Jasper Nuyens
jasper@linux.com
+32478978967
Managing Director
Linux Belgium
http://www.linuxbe.com

Very interested in EVs since Tesla.

Made money with Free and OpenSource Software Training and Consultancy



the business interface to the linux community

www.linuxbe.com

Content

1. Disclaimer and the obvious questions
2. The car
3. The mission
4. Components and network layout
5. How to access
6. Hacks performed by other people
7. Hacks performed by me
8. How ‘hacker friendly’ are Tesla Service and Elon Musk?
9. Other questions
10. Q&A

1. Disclaimer and the obvious questions

Disclaimer

- I am a Tesla **customer**, not a Tesla supplier or employee. I can be considered a ‘security researcher’, ‘thinkerer’ or ‘hacker’, not a ‘cracker’.

- Tesla hacking seems dangerous: it is a +2t car with electric propulsion, electronically steered and with a high voltage battery. Yet all drive controls keep on working even when 3 Linux systems are restarted during driving.

- Tesla can be considered ‘Hacker Friendly’. When registering as a ‘security researcher’, Tesla guarantees car warrantee, helps when you would ‘brick your car’, absolves you from litigation and has a ‘bounty program’.

SMALL PROBLEM

Slight conflict of interests between Tesla and Hackers for now:

- if a new exploit is discovered by creative car owners, and Tesla finds out how, they close the entry point.

GREAT!
BUT NOT GREAT if it's the only way to gain access on your car or help a friend out.

We hope in the future Tesla will allow 'security researchers' a simple or controlled way to gain root. To prevent abuse and enable more FUN!

2. The car

Model X, Enhanced Autopilot 2.0
75kWh battery, premium interior, towing package…

2. The car

"Once you drive electric, there's no going back"

Range: in practice between 230 and 350km

decreases range: high speed, cold weather

never having to go to the petrol station

start 'full' every morning, slow traffic doesn't increase consumption

Supercharging network for long distance: charges at 500km per hour (120kW); no waiting required (lunch, toilet,…)
Ok to drive 1000km per day without waiting to charge.

Autopilot: driver assist system. I discovered a huge leap forward with version 9.0: 2018.39.0.1 and 2018.39.2.1

3. The mission

Tesla's mission is: "***Accelerate the world's transition to sustainable energy.***"

In our case, we drove 52.000 km in 1,5 year with our Model X. We generated the electricity from our solar roof. This avoided air pollution of: 11980kg CO_2 plus all the other nasty stuff we put in the atmosphere.

Ecological footprint of production? About the same as with 'old' cars. And Tesla doesn't use 'dirty' cobalt from Congo for it's batteries.
Only 'vegan' leather.

4. Components and network layout

- Instrument Cluster (ic) behind steering wheel
192.168.90.101
- Big screen (cid) in the middle
192.168.90.100
- Gateway (gw)
192.168.90.102
- Autopilot (ape)
192.168.90.103
- Ib (ape gw)
192.168.90.104

4. Components and network layout

Instrument Cluster (ic) behind steering wheel
192.168.90.101
Custom version of NVidia Tegra 2 SoC

```
cat /proc/cpuinfo
Processor  : ARMv7 Processor rev 0 (v7l)
processor  : 0
BogoMIPS   : 897.84

processor  : 1
BogoMIPS   : 897.84

Features   : swp half thumb fastmult vfp edsp vfpv3 vfpv3d16
CPU implementer : 0x41
CPU architecture: 7
CPU variant     : 0x1
CPU part   : 0xc09
CPU revision    : 0

Hardware   : Tegra P852 SKU8 C01
Revision   : 0000
Serial          : 1f78400042408317
```

Boots squashfs compressed read-only filesystem, /var is writeable
Steering wheel buttons are attached to the ic and the input is sent over Ethernet using the (undocumented) ‘Vehicle API’
Settings are stored in sqlite3 db

4. Components and network layout

Massive multimedia 19”screen (cid) in the middle of the car

192.168.90.100

NVIDIA quad core (new cars have it replaced with Intel CPU based board, like in the Model 3)

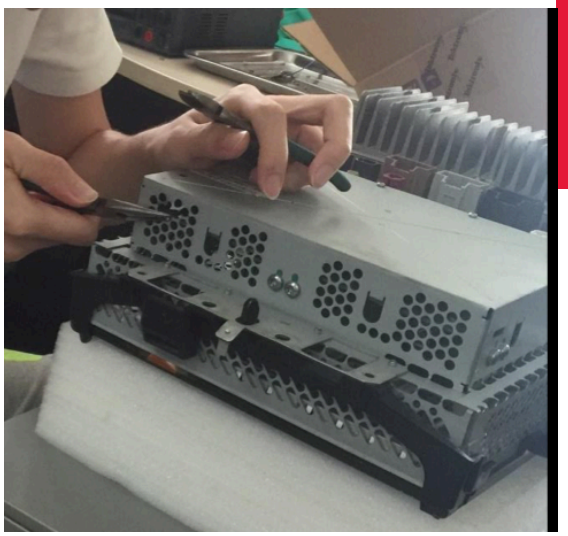
Includes a Qt based Web browser, runs Spotify and allows to control all car settings, doors, keys, sound, and so on…

4. Components and network layout


```
root@ic:~# nmap -v -p 1-65535 -sV -O -sS -T5 192.168.90.100

Not shown: 65090 closed ports, 419 filtered ports
PORT      STATE SERVICE         VERSION
22/tcp    open  ssh             OpenSSH 5.5p1 Debian 4ubuntu4 (Ubuntu Linux; protocol 2.0)
53/tcp    open  domain          dnsmasq 2.78
111/tcp   open  rpcbind         2 (RPC #100000)
2049/tcp  open  nfs             2-4 (RPC #100003)
4030/tcp  open  unknown
4032/tcp  open  unknown
4037/tcp  open  unknown
4050/tcp  open  unknown
4060/tcp  open  unknown
4070/tcp  open  unknown
4090/tcp  open  omasgport?
4092/tcp  open  unknown
4094/tcp  open  unknown
4096/tcp  open  bre?
4102/tcp  open  unknown
4110/tcp  open  unknown
4160/tcp  open  unknown
4170/tcp  open  unknown
4220/tcp  open  vrml-multi-use?
4280/tcp  open  unknown
4500/tcp  open  sae-urn?
20564/tcp open  unknown
25956/tcp open  unknown
43164/tcp open  nlockmgr        1-4 (RPC #100021)
43427/tcp open  status          1 (RPC #100024)
43546/tcp open  mountd          1-3 (RPC #100005)
```

4. Components and network layout



Gateway
192.168.90.102

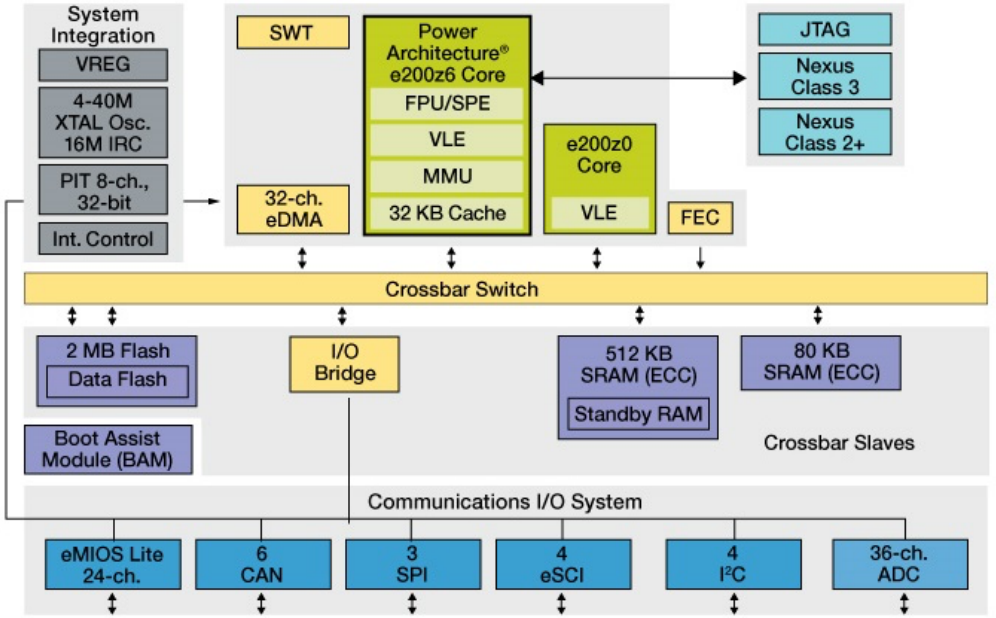
Runs FreeRTOS on **Freescale MPC5668G**
592 KB embedded RAM

Is attached to the 6 CAN-busses:
- Trunk, doors,…
- Vehicle speed, engine speed,…
- Chassis
- BFT
- ODBII

4. Components and network layout

Gateway
192.168.90.102

firmware name: gtw.hex
located on the sd card
of the CID



In the past, it contained in clear text the (unique) pw to get acces. Was a ‘point of entry’, closed by Tesla.

5. How to access

Which data paths exist?

Internet:
- nightmare of Elon Musk
- access from the Tesla Android or IOS App
- mothership.tesla.com

Internal Ethernet network:
- physical connection below CID for Service Centers
- physical connection between IC and CID

CAN busses:
- typical ‘old school car modding’, will probably disappear


Avg. 198 Wh/km
Past 50 km
Life, the Universe, and Everything
193 km 27°C
AMERIKA
Car Off
Jasper
10:57
Navigate
CONTROLS
CLIMATE
Google


MODEL S
75D
Avg. 198 Wh/km
Past 50 km
190 km 26°C


MODEL X
75D
Avg. 198 Wh/km
Past 50 km
188 km 23°C
Life, the Universe, and Everything
Songs

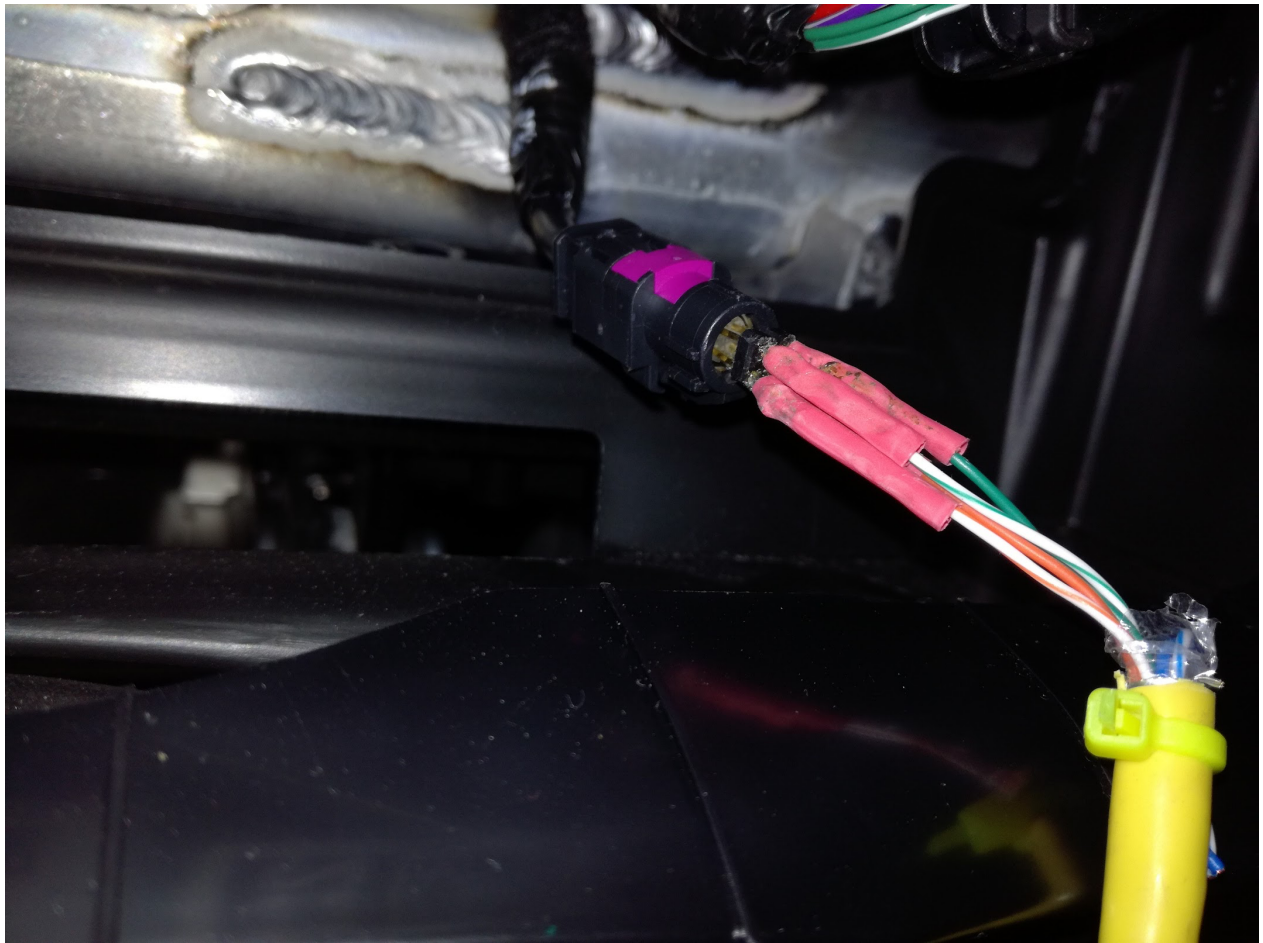

MODEL X
75D
Songs
Avg. 198 Wh/km
Past 50 km
The Moon and the Sky
Life, the Universe, and Everything
Car Off
187 km
23° C

5. How to access

Careful with the special connector which provides power and more (click mechanism)!

5. How to access

Experiment with how the wiring to the Ethernet is done.

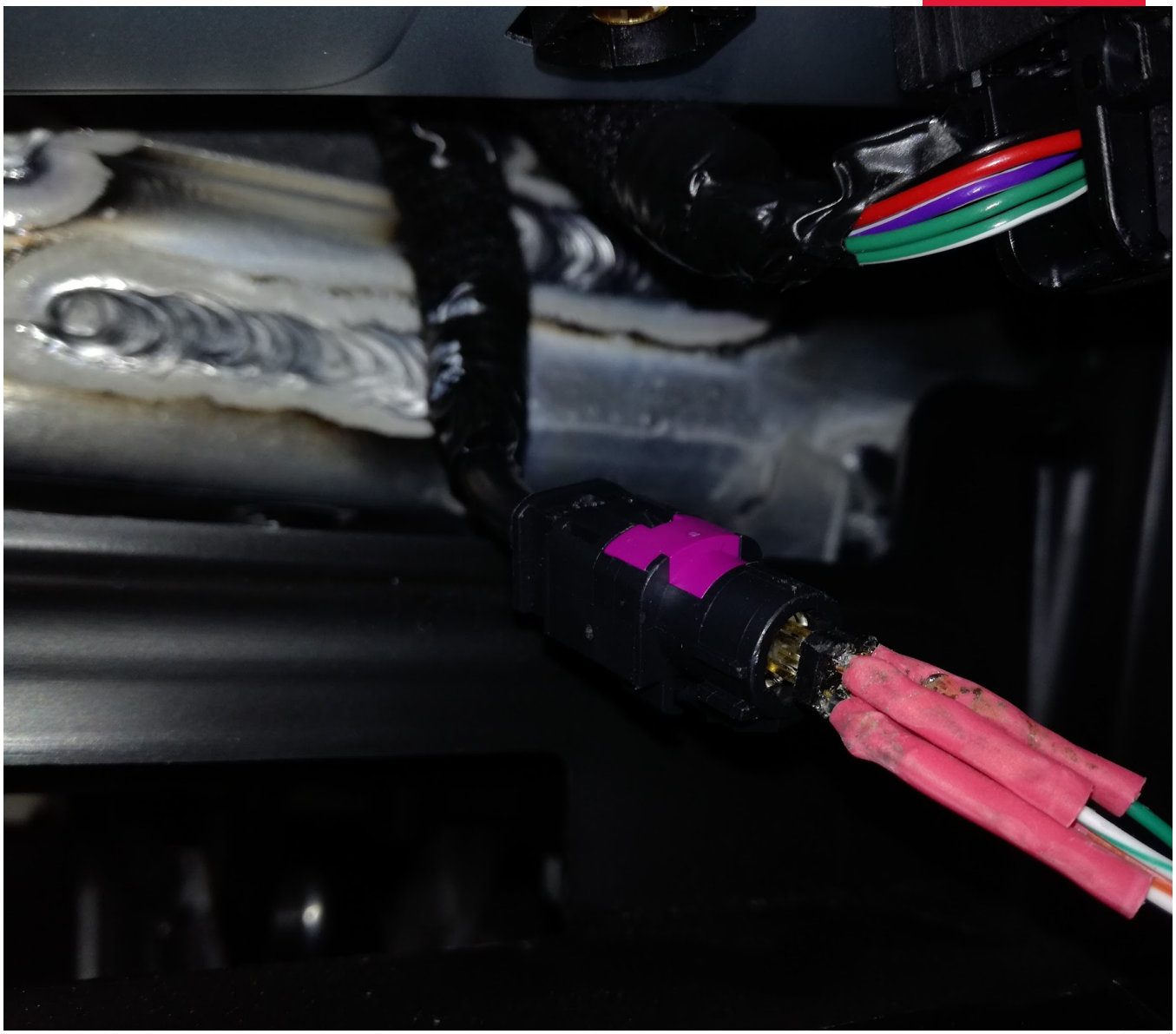


5. How to access

Fakra?

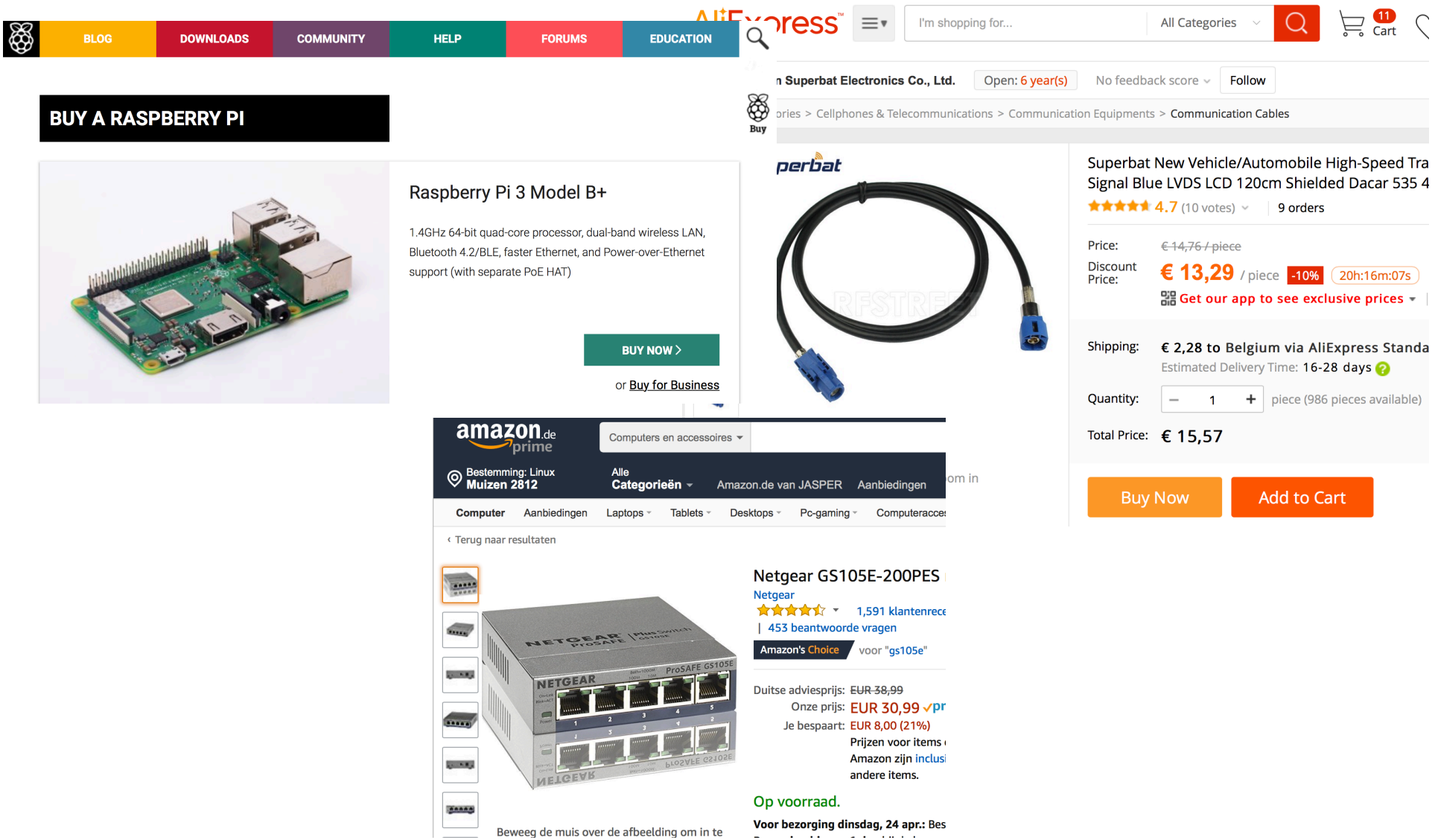
4 Ethernet wires:
green, orange
green/white
orange/white

Test: steering wheel audio volume passes through Ethernet



5. How to access

Better (version 2):



5. How to access

1st way:

Ethernet (Fakra) from CID to switch
Ethernet (Fakra) from IC to switch
Extra ethernet cable below CID for attaching laptop
Ethernet cable for Raspberry Pi for wired and/or wireless network
Raspberry Pi allows to modify stuff ‘permanently’ without changing something to the rootfs
Easy access at a side panel to ‘reverse’ all changes (before going back to Tesla Service)

5. How to access

2nd step:

Reverse ssh tunnel directly from CID

-> allows hacking in bed and on holiday :-D

-> allows a chrooted ubuntu on a USB stick

6. Hacks performed by other people

Tesla itself created ‘Easter Eggs’ like Model X Chrismas Tree, Mars driving map, drawing app,…

3 minute movie

https://www.youtube.com/watch?v=1fmm6Hg7k1U

6. Hacks performed by other people

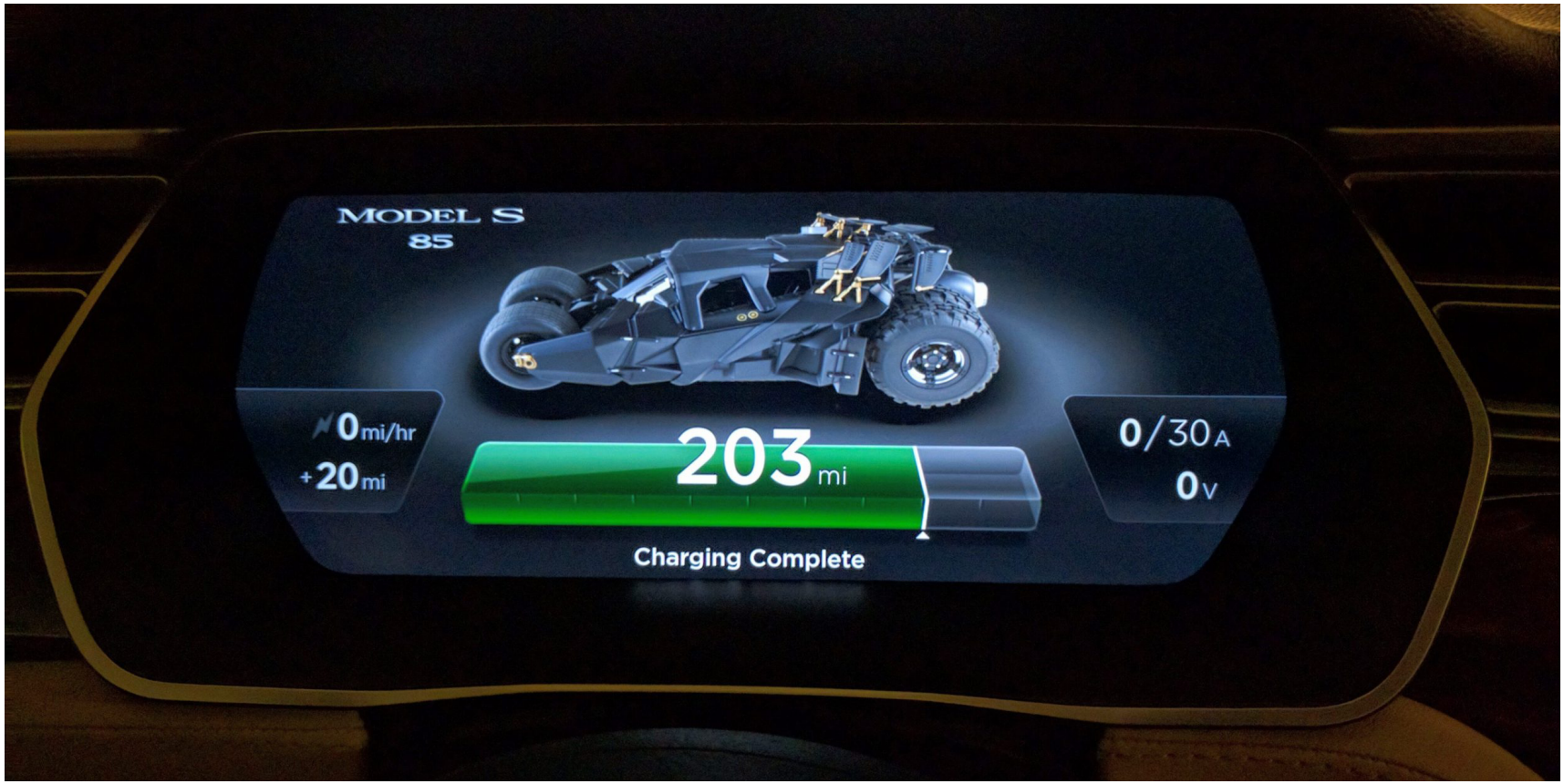
All IC’s can be accessed using the same (leaked) ssh key for the root account (once you are on the Ethernet network between IC and CID). Might not remain so after an update?

Ethernet port below CID is only enabled after mothership opens it for Tesla Service through their own cryptographically signed applications/internal network.

Access from IC to CID is restricted (was a dead end).

6. Hacks performed by other people

Replacing an image on Instrument Cluster



7. Hacks performed by me

7. Peeking into version 9.0

Configurable through web based API:

Enable Factory Mode:

```
curl –s "http://192.168.90.100:4035/set_data_value?name=GUI_factoryMode&value=true"
```

Launch an update:

```
socat -,icanon=0,echo=0 tcp:192.168.90.100:25956;
install http://www.freedomev.com:80/develop-2018.39.2.1-13-cbbcef4da9.img
```

Thanks to **@nemSoma** for the image

Turn on the experimental ‘Navigation on Autopilot’ in Europe:

```
curl –s “http://192.168.90.100:4035/set_data_value?name=FEATURE_dasDriveOnNavEnabled&value=true"
curl –s "http://192.168.90.100:4035/set_data_value?name=FEATURE_dasNoConfirmULCEnabled&value=true"
```

Amazing _next level_ capabilities unlocked!
BUT: obviously we need to be careful with ‘development’ features.
In this way they are not persistent, but that’s probably the best idea.

http://www.youtube.com/salamimovies

7. Hacks performed by me

Replacing lots of images ‘subtle’ to add the Linux logo - and a ‘peace’ sign.

7. Hacks performed by me

Images stored in /usr/tesla/UI/assets/night/car/modelx/

No permanent changes are made: small script to bind mount the individual files from /var/added and relaunch the Qt based IC process (beware of wife).

Re-verifies every minute out of crontab.

```
root@ic:~# crontab -l
* * * * /teslascript.sh > /dev/null 2>&1
```

7. Hacks performed by me


```
cat /teslascript.sh
#!/bin/bash

nohup ssh  -i /root/id_dsa root@192.168.90.101 bash /var/added/addedtotesla.sh &
```

ON IC:

```
bash /var/added/mount-modfiles.sh

cat mount-modfiles.sh
#!/bin/bash
#if an argument is provided multiple directories are allowed

#first umount

for bindmount in $(mount | grep bind | awk '{ print $1 }')
do
 umount $bindmount
done

cd /var/added/modfiles$1
for modfile in $(find . -type f)
do
 mount --bind $modfile /$modfile
done
```

7. Hacks performed by me

Gives:

```
 mount
/dev/mmcblk3p3 on /var type ext3 (rw,noexec,nosuid,nodev,data=ordered,barrier=1,commit=20)
/dev/mmcblk3p4 on /home type ext3 (rw,noexec,nosuid,nodev,data=ordered,barrier=1,commit=20)
none on /var/run type tmpfs (rw)
none on /var/lock type tmpfs (rw)
cid:/opt/navigon on /opt/navigon type nfs (ro,noexec,nosuid,nodev,nolock,soft,fg,intr,retry=1,retrans=10,addr=192.168.90.100)
/var/added/modfiles/home/tesla/.Tesla/data/QtCarClusterSettings.db on /home/tesla/.Tesla/data/QtCarClusterSettings.db type
none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/car/modelx/doors/trunk_closed_paint.png on /usr/tesla/UI/assets/night/car/
modelx/doors/trunk_closed_paint.png type none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/car/modelx/doors/trunk_open.png on /usr/tesla/UI/assets/night/car/modelx/doors/
trunk_open.png type none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/car/modelx/drive/body_paint.png on /usr/tesla/UI/assets/night/car/modelx/drive/
body_paint.png type none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/car/modelx/hero/frunk_open_paint.png on /usr/tesla/UI/assets/night/car/modelx/
hero/frunk_open_paint.png type none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/car/modelx/hero/frunk_closed_paint.png on /usr/tesla/UI/assets/night/car/modelx/
hero/frunk_closed_paint.png type none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/car/modelx/top/frunk_open.png on /usr/tesla/UI/assets/night/car/modelx/top/
frunk_open.png type none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/car/modelx/top/frunk_closed_paint.png on /usr/tesla/UI/assets/night/car/modelx/
top/frunk_closed_paint.png type none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/car/modelx/park/car_paint.png on /usr/tesla/UI/assets/night/car/modelx/park/
car_paint.png type none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/car/modelx/ghost/body-5.png on /usr/tesla/UI/assets/night/car/modelx/ghost/
body-5.png type none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/about/badge_model_x.png on /usr/tesla/UI/assets/night/about/badge_model_x.png
type none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/cluster/background_noise.jpg on /usr/tesla/UI/assets/night/cluster/
background_noise.jpg type none (rw,bind)
/var/added/modfiles/usr/tesla/UI/assets/night/cluster/hi_res/badges/badge_model_x.png on /usr/tesla/UI/assets/night/cluster/
hi_res/badges/badge_model_x.png type none (rw,bind)
```

7. Hacks performed by me

And then the script does:

```
killall -HUP QtCarCluster
```

The monitoring on the IC will restart the process fairly rapidly (beware of wife if you do this while driving)

7. Hacks performed by me

7. Hacks performed by me

Next step…

- Color animation script!

cat moonshine.sh

```
#!/bin/bash
export DISPLAY=:0.0

while true
do
 for color in rgamma ggamma bgamma
 do
  for gamma in 0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1.0
  do
   xgamma -${color} $gamma 2> /dev/null
   sleep 0.1
  done
 done
done
```

https://www.youtube.com/watch?v=XfkuS-ypUTU

7. Hacks performed by me

Discovered:
Sound is sent over the Ethernet network :)

```
cat gameofthrones.wav | nc 192.168.90.100 4102
```

Possibility for denial of service attack? (yet not practical)

Special sound format needed:

```
file park_assist_red_repeat.wav
park_assist_red_repeat.wav:    RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 48000 Hz
RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 48000 Hz
```

Something like this:

```
sox -S --norm gameofthrones-orig.wav -c 1 -r 48000 gameofthrones-good-format.wav \
            reverse silence 1 0 0.05 reverse \
            pad 0 0.100
```

7. Hacks performed by me

- Every day a new ‘token’ received in: /var/etc/saccess/tesla1

- SQLite3 database containing settings /home/tesla/.Tesla/data/QtCarClusterSettings.db

```
sqlite3 QtCarClusterSettings.db
sqlite> select key, quote(value) from data;
select key, quote(value) from data where key='DataValues/GUI_developerMode';
DataValues/GUI_developerMode|X’000000010000'
UPDATE data SET value=X'000000010001' WHERE key='DataValues/GUI_developerMode';
```

7. Hacks performed by me

Root on CID

Obtained though a - now patched - way during an upgrade mechanism to perform commands on the CID; extracting the daily changing security token.
Thanks to someone on TMC forum for helping me!

CID has an Internet connection (through usb-connected ‘parrot’).
-> reverse ssh tunnel for easy remote access
-> extra backdoors to prevent becoming locked out as a result of an update

Only /var is writeable

7. Hacks performed by me

Root on CID

CID has 2 USB connections in the central display
-> allows to run ARM/Ubuntu in a mounted chrooted environment

Big display is not rotated at kernel level; QT application is written rotated.
Fixed with running X applications in a rotated **Xephyr** (nested X server).

7. Hacks performed by me

Root on CID

Sound possible with gstreamer.

Possible to display messages on the CID

7. Hacks performed by me

Root on CID - romance mode

For the 4th anniversary of being married to my sweet wife, i put this into crontab:

```
*/15 * * * * bash /var/added/romance_mode.sh >/dev/null 2>&1
```

Executing:

bash /var/added/speak "Kissy, kissie"
/disk/usb.*/freedomev/talk "I love you, Baby!"

7. Hacks performed by me

Root on CID

Romance Mode

https://www.youtube.com/watch?v=w-gLSPzLo6Q

7. Hacks performed by me

Goals

Integrate touchscreen driver and build application launcher with free software repository

www.FreedomEV.com
www.FreedomEV.com/wiki
www.github.com/jnuyens/freedomev

“Download/extract the tarball to a usb stick, add one crontab entry in the CID as root and enjoy the power of the OpenSource community”

7. Hacks performed by me

Goals

Integrate anbox to run Android apps like Waze on the CID

Allow anybody to contribute fun stuff back easy to package and distribute.

Fun, Fun, Fun!

8. How ‘hacker friendly’ are Tesla Service and Elon Musk?

I am not interested in doing illegal things like:
- changing the VIN number (it might help stolen car sales)
- faking the mileage
- abusing the (free) data usage

I prefer also not to:
- mess with the autopilot (I prefer to live ;)
- mess with the drive motor steering


The Hague
Rotterdam
Münster
Dortmund
Essen
Düsseldorf
Cologne
Bonn
Aachen
Koblenz
Mainz
Trier
Saarbrücken
Karlsruhe
Metz
Nancy
Dunkirk
Ghent
Belgium
Charleroi
Arras
Canterbury
43
2
44
3
61
E40
E34
E314
E42
E411
E25
A16
A26
A25
A2
A28
A1
A4
A10
A31
A5
66
63
65
6
5
1

9. Other questions

Or use other charging networks…