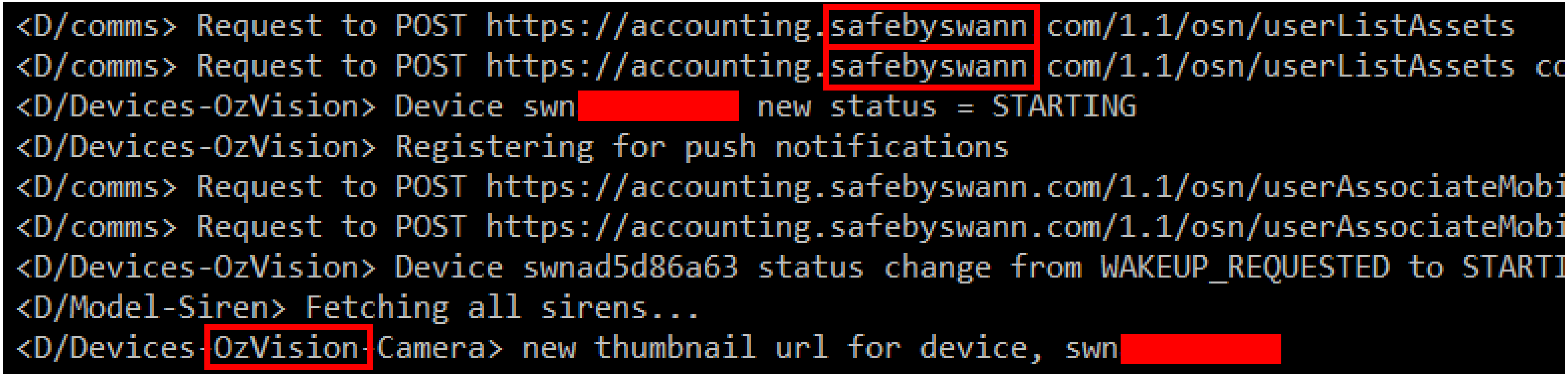
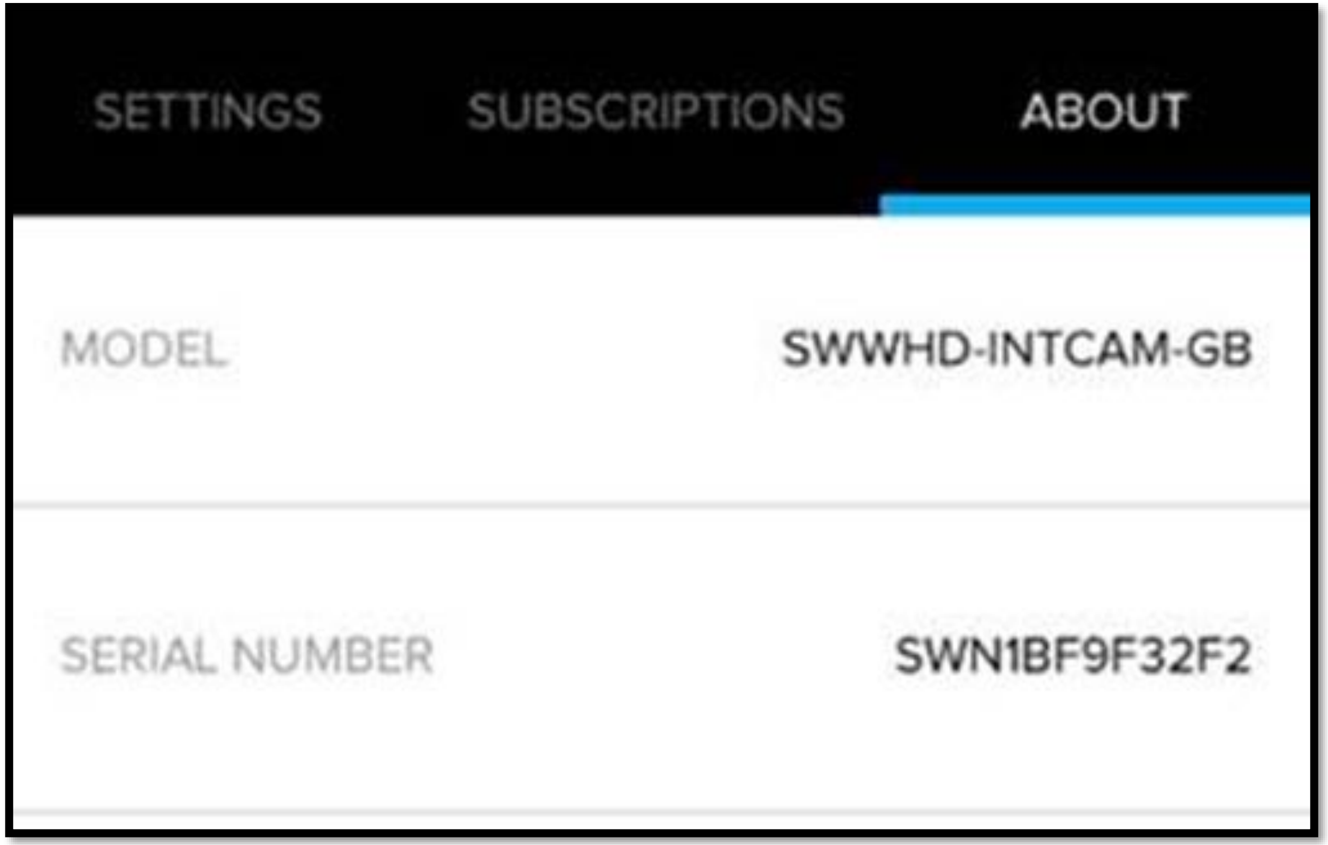
Snooping IoT!

Device Identity is Important

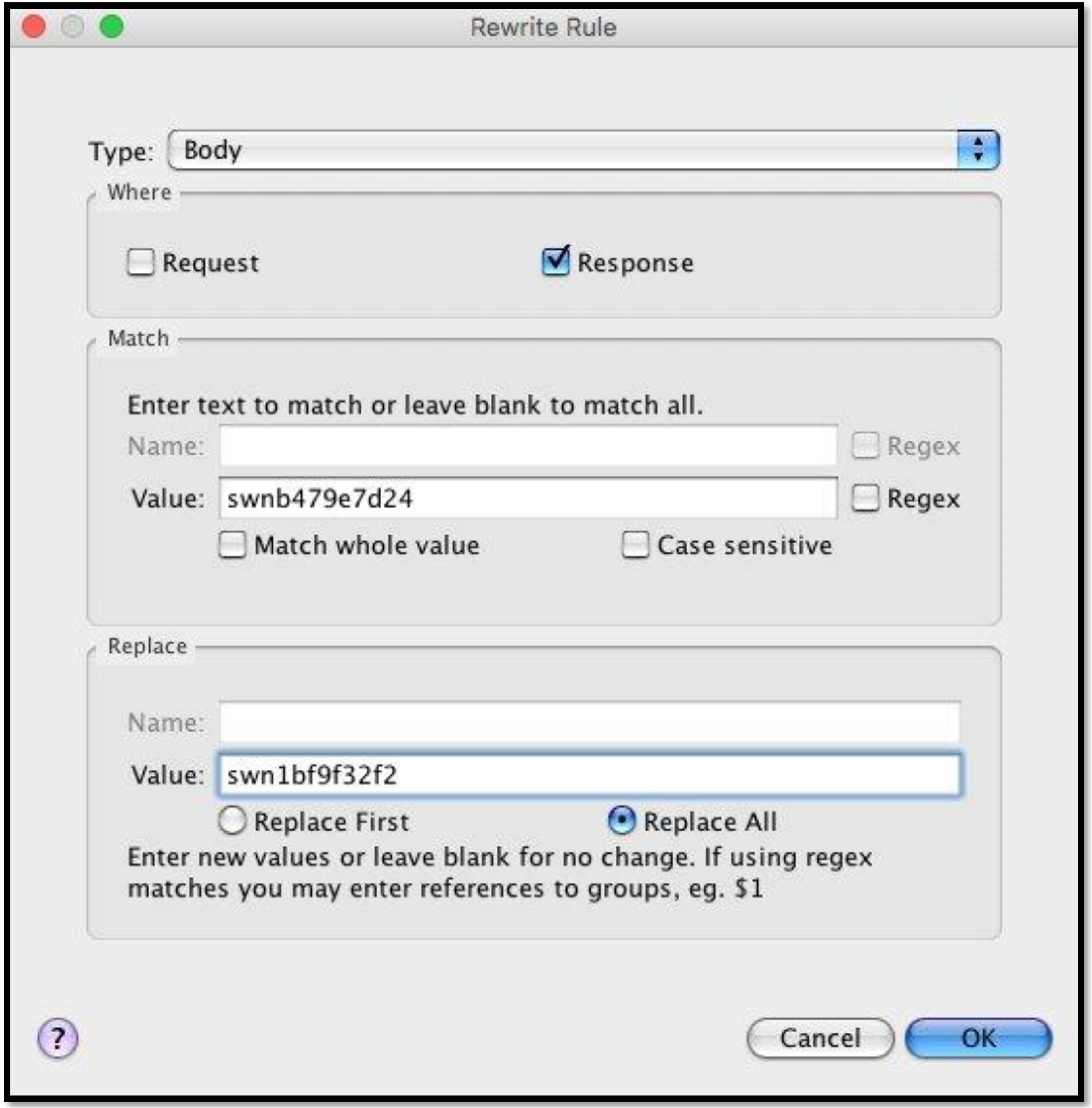
Swann



```
<D/comms> Request to POST https://accounting.safebyswann com/1.1/osn/userListAssets
<D/comms> Request to POST https://accounting.safebyswann com/1.1/osn/userListAssets co
<D/Devices-OzVision> Device swn[redacted] new status = STARTING
<D/Devices-OzVision> Registering for push notifications
<D/comms> Request to POST https://accounting.safebyswann.com/1.1/osn/userAssociateMobi
<D/comms> Request to POST https://accounting.safebyswann.com/1.1/osn/userAssociateMobi
<D/Devices-OzVision> Device swnad5d86a63 status change from WAKEUP_REQUESTED to STARTI
<D/Model-Siren> Fetching all sirens...
<D/Devices-OzVision-Camera> new thumbnail url for device, swn[redacted]
```



MODEL	SWWHD-INTCAM-GB
SERIAL NUMBER	SWN1BF9F32F2



Rewrite Rule

Type: Body

Where

☐ Request ☑ Response

Match

Enter text to match or leave blank to match all.

Name: ☐ Regex

Value: swnb479e7d24 ☐ Regex

☐ Match whole value ☐ Case sensitive

Replace

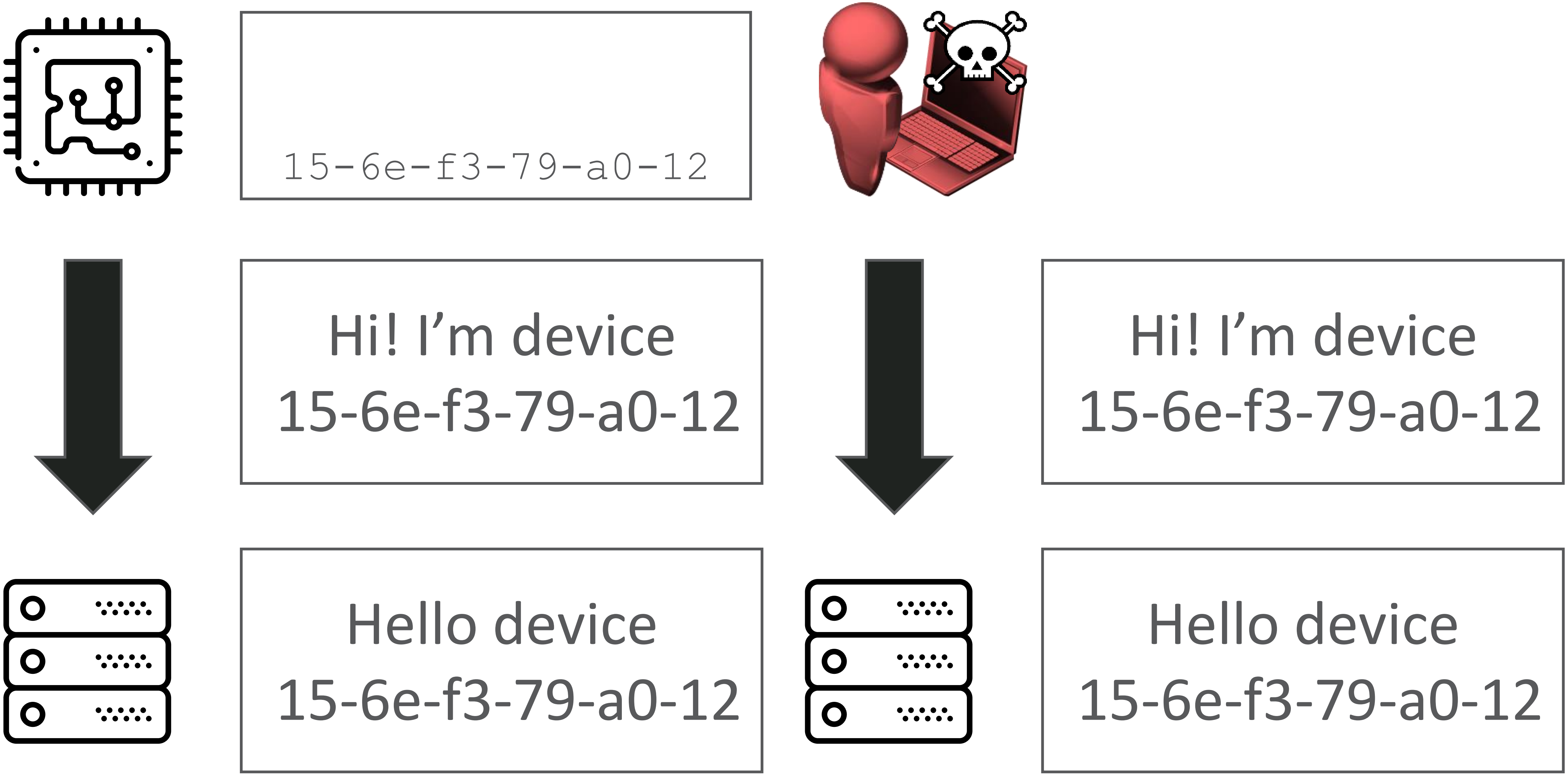
Name:

Value: swn1bf9f32f2

○ Replace First ● Replace All

Enter new values or leave blank for no change. If using regex matches you may enter references to groups, eg. $1

11:06
Scott Test Camera
LIVE
LEGO TECHNIC



15-6e-f3-79-a0-12

Hi! I’m device 15-6e-f3-79-a0-12

Hello device 15-6e-f3-79-a0-12

Hi! I’m device 15-6e-f3-79-a0-12

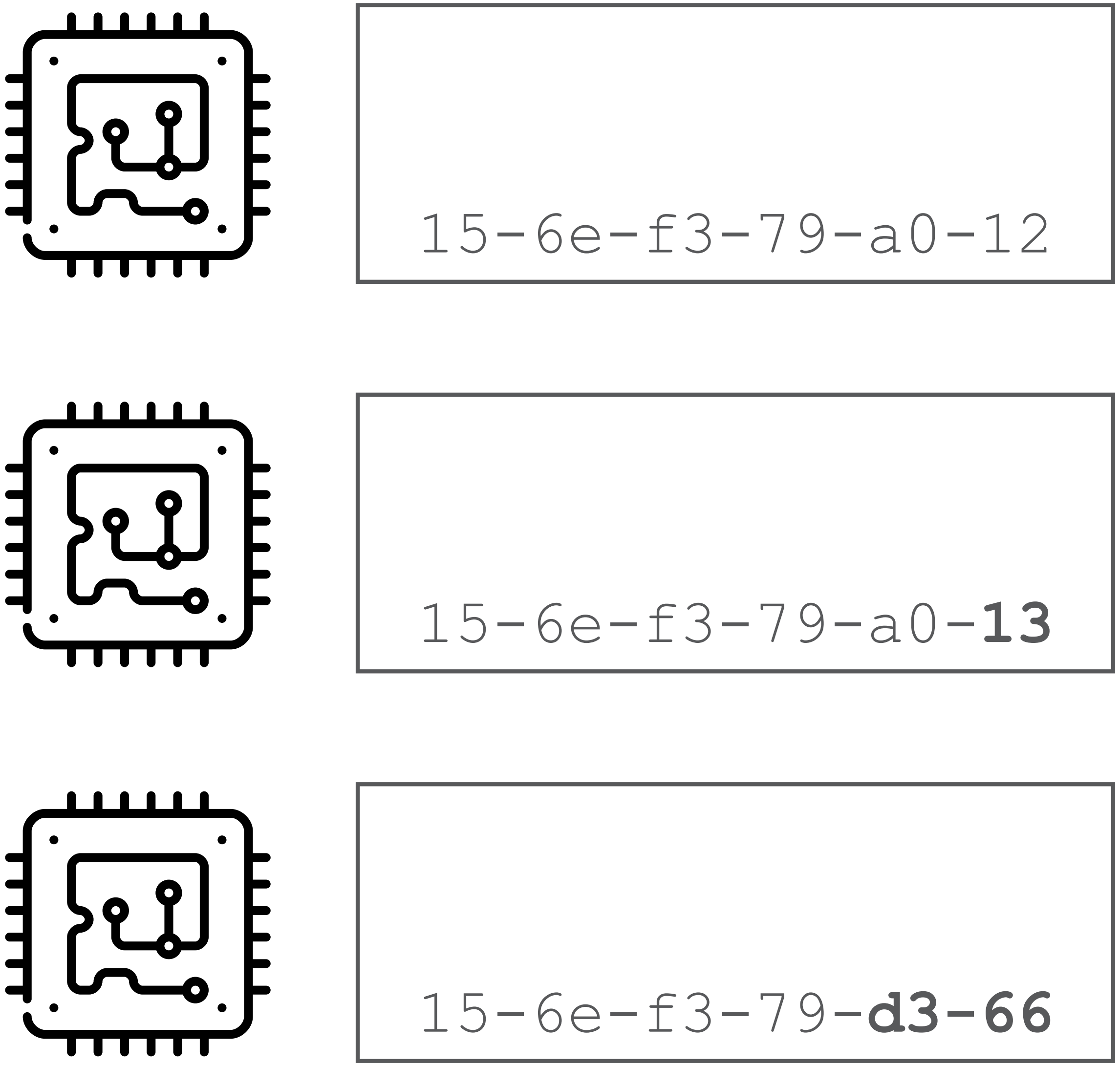
Hello device 15-6e-f3-79-a0-12

Using MAC as identity

MAC address is unique and cheap

Take from Wi-Fi or BLE module

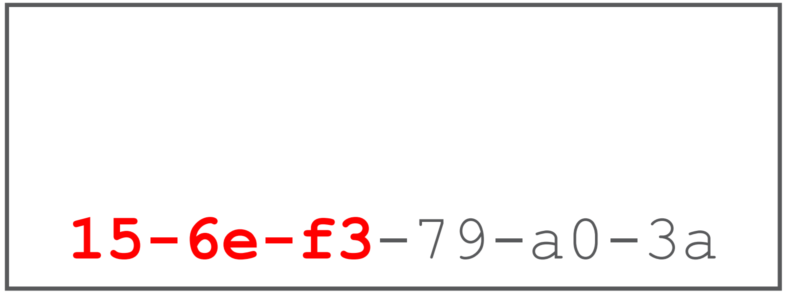
2^{48} permutations, right…



15-6e-f3-79-a0-12

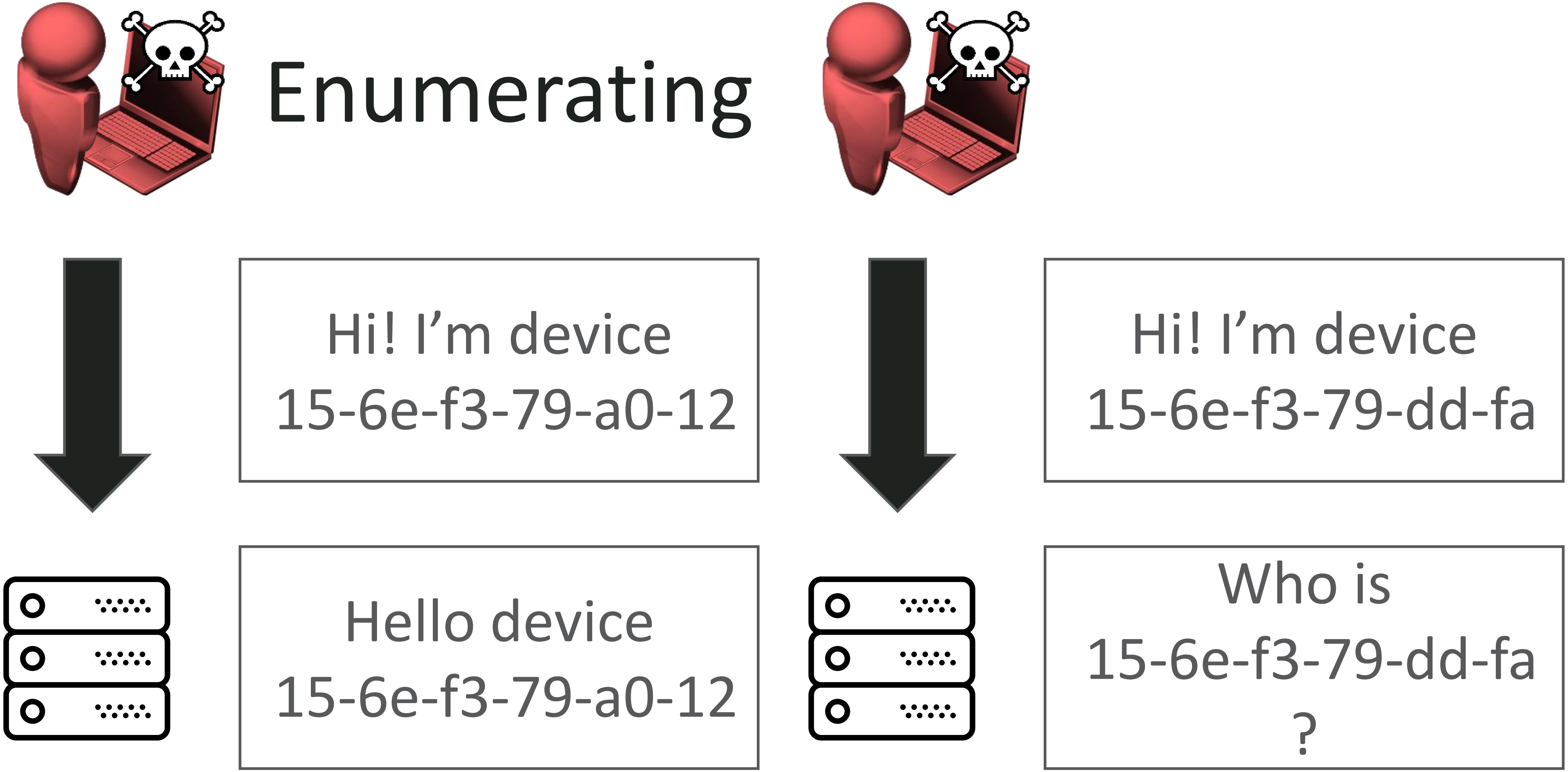
15-6e-f3-79-a0-**13**

15-6e-f3-79-**d3-66**



15-6e-f3-79-a0-3a

Enumerating

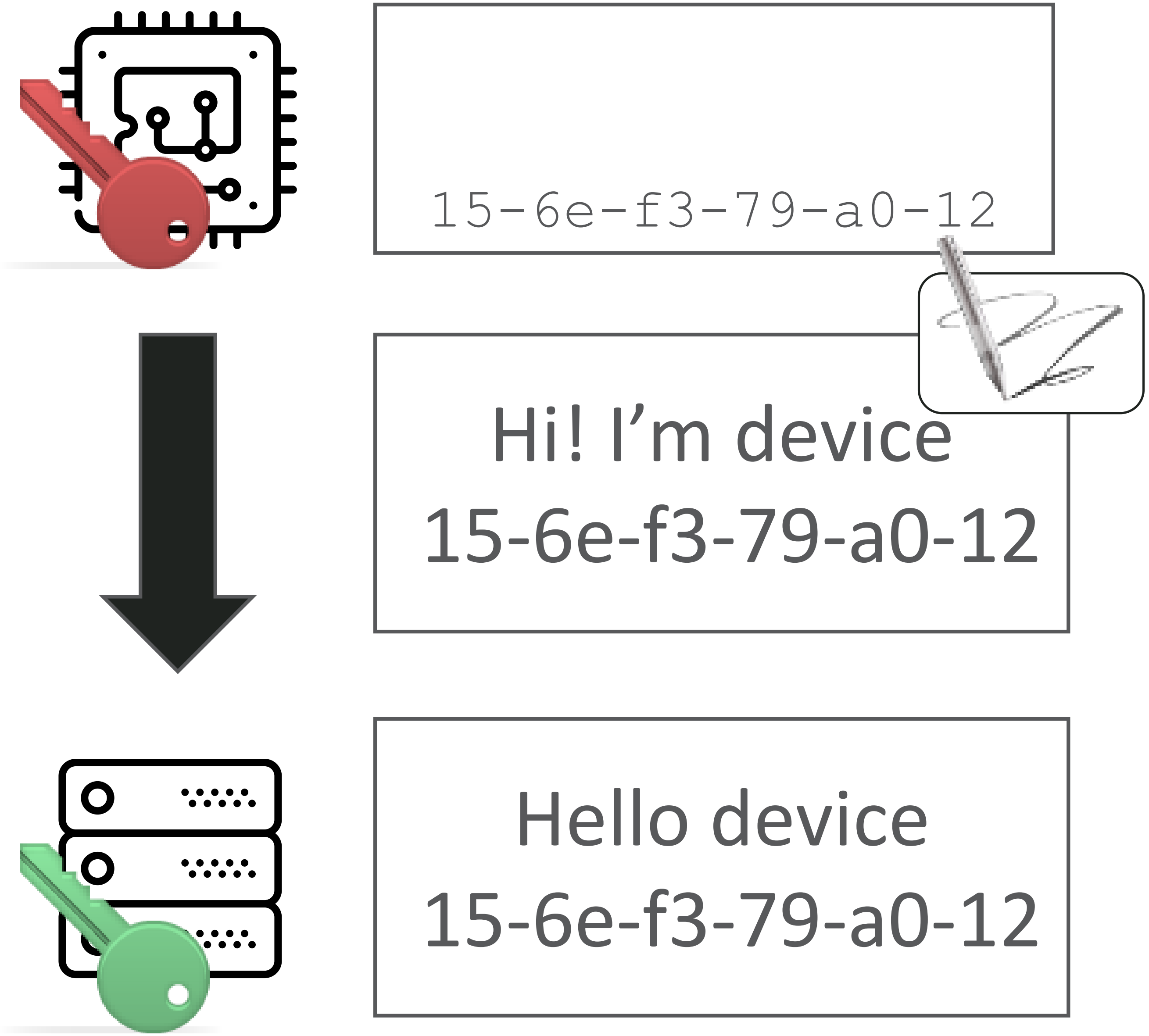


Hi! I’m device 15-6e-f3-79-a0-12

Hello device 15-6e-f3-79-a0-12

Hi! I’m device 15-6e-f3-79-dd-fa

Who is 15-6e-f3-79-dd-fa ?



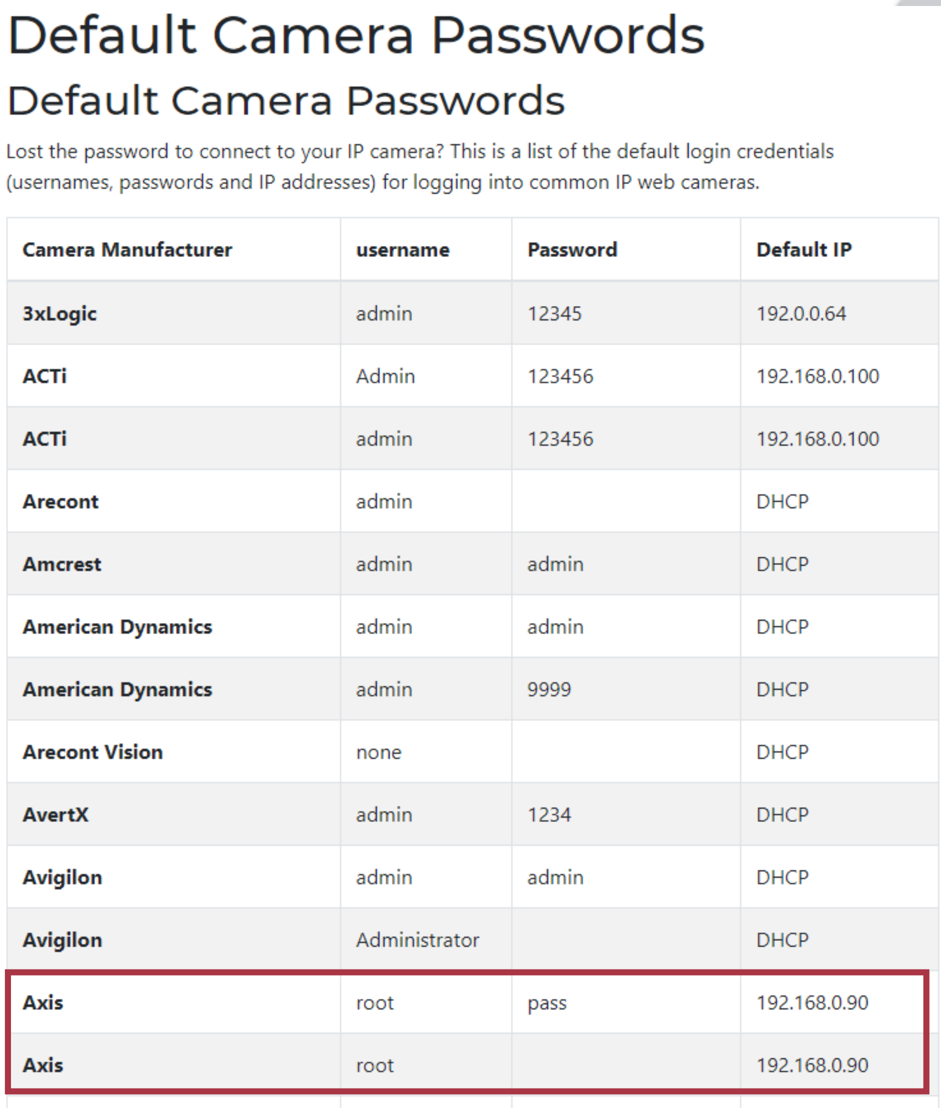
15-6e-f3-79-a0-12

Hi! I’m device 15-6e-f3-79-a0-12

Hello device 15-6e-f3-79-a0-12

Device contains a private key
Messages are signed using private key
Server validates signature

Home (in)security

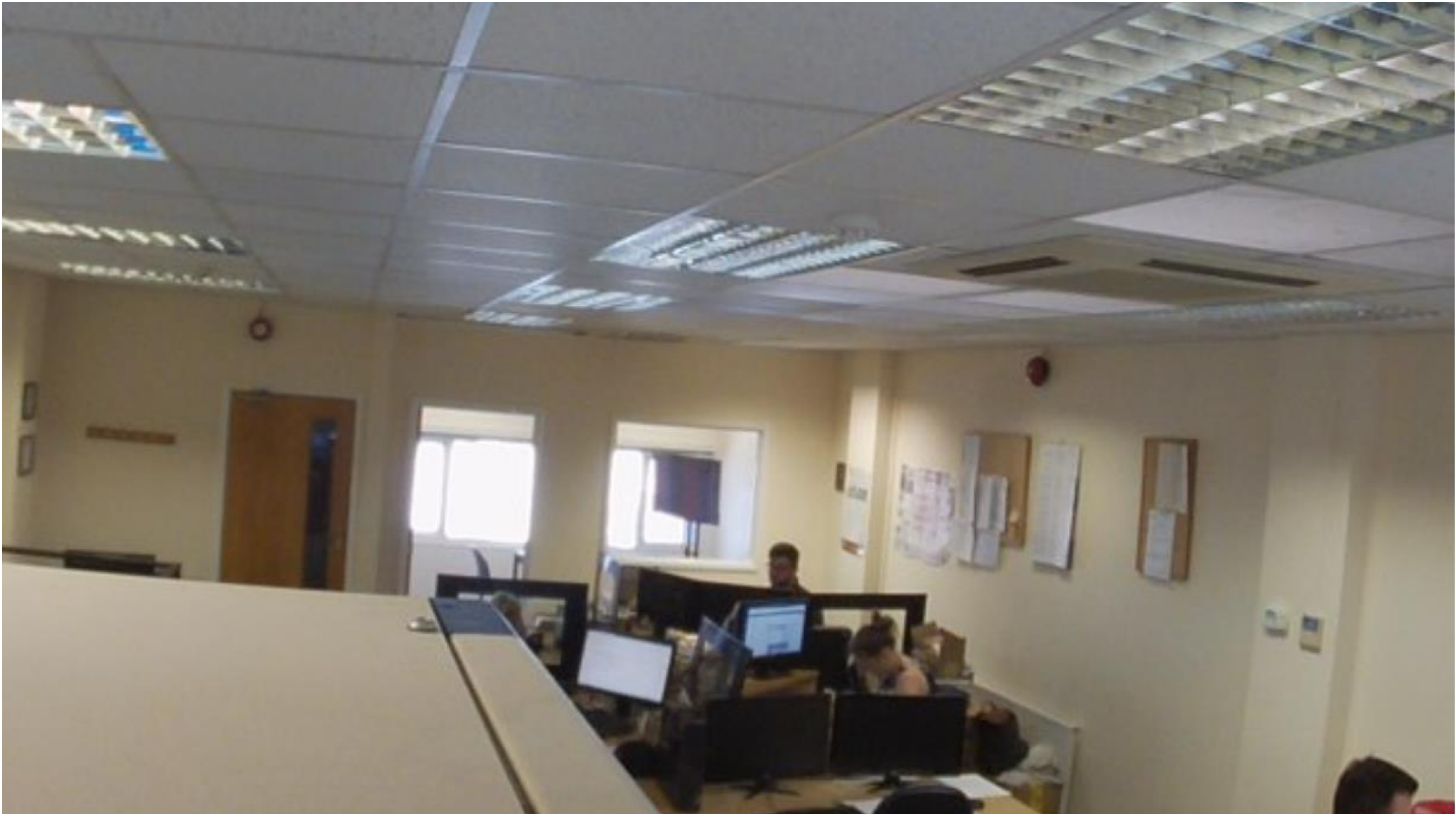


Default Camera Passwords

Default Camera Passwords

Lost the password to connect to your IP camera? This is a list of the default login credentials (usernames, passwords and IP addresses) for logging into common IP web cameras.

Camera Manufacturer	username	Password	Default IP
3xLogic	admin	12345	192.0.0.64
ACTi	Admin	123456	192.168.0.100
ACTi	admin	123456	192.168.0.100
Arecont	admin		DHCP
Amcrest	admin	admin	DHCP
American Dynamics	admin	admin	DHCP
American Dynamics	admin	9999	DHCP
Arecont Vision	none		DHCP
AvertX	admin	1234	DHCP
Avigilon	admin	admin	DHCP
Avigilon	Administrator		DHCP
Axis	root	pass	192.168.0.90
Axis	root		192.168.0.90

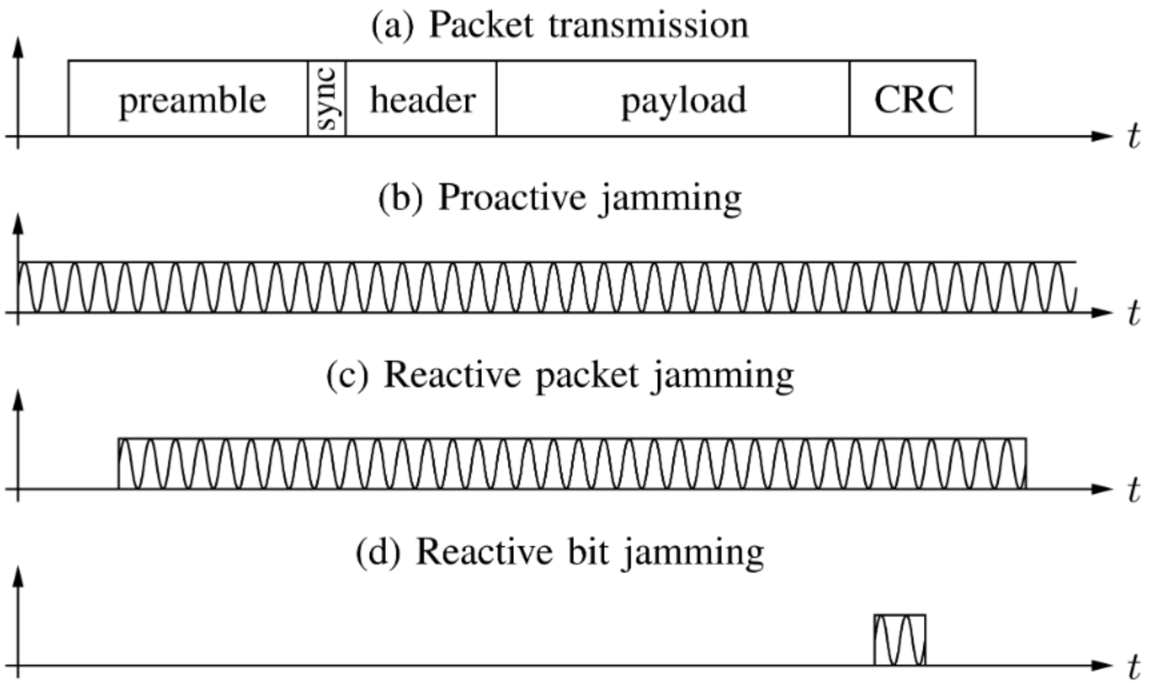


Change my default passwords

Do you need remote access?

Hacking House Alarms

[redacted]



Hacking House Alarms

[redacted]

Jamming is too easy

Many wireless alarms have a remote PIN fob

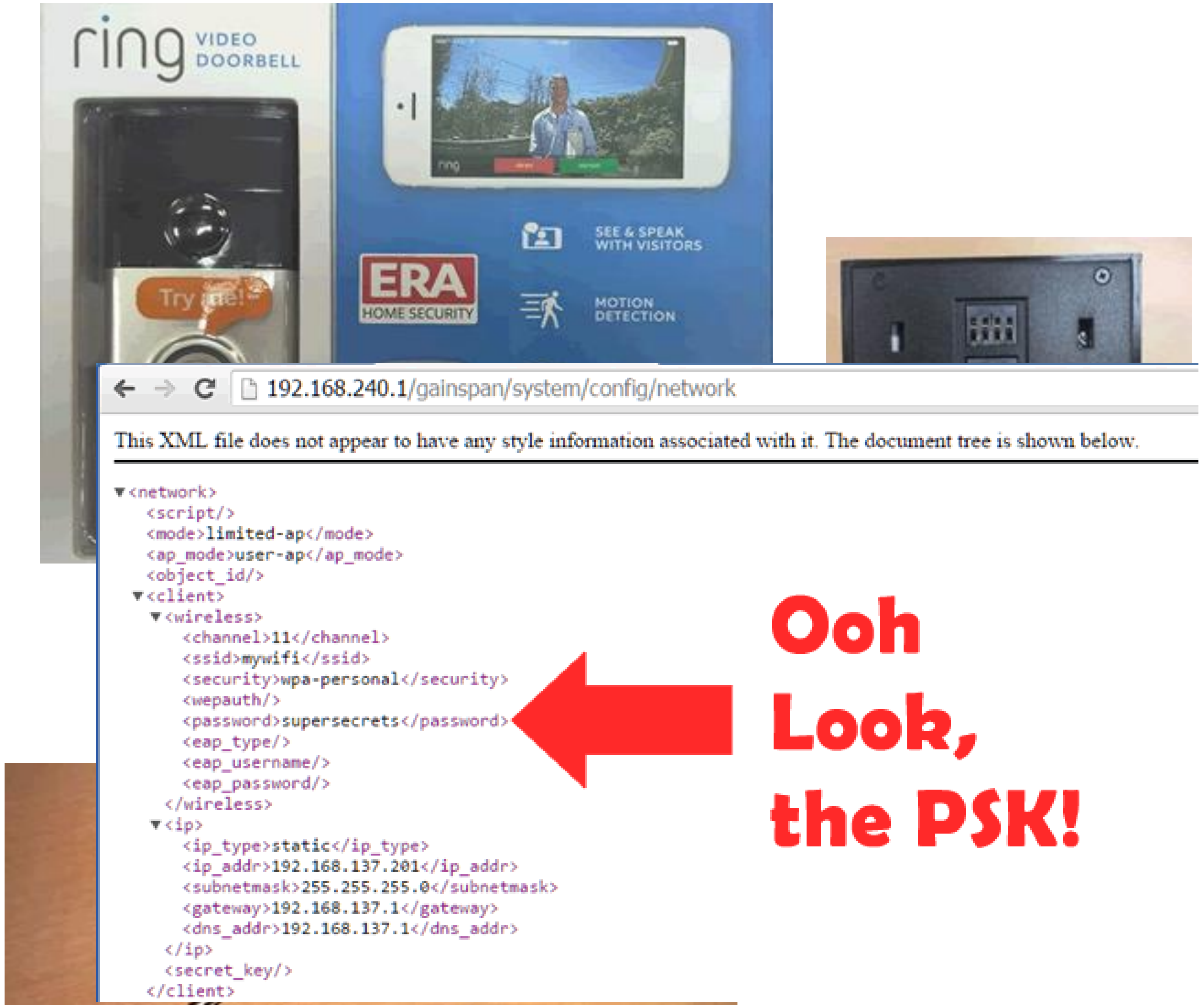
We could disarm many panels by spoofing the radio signal from the fob

Ring smart door bell

Can be unscrewed from outside the house

Simply reset to access a configuration page

That discloses your Wi-Fi password!



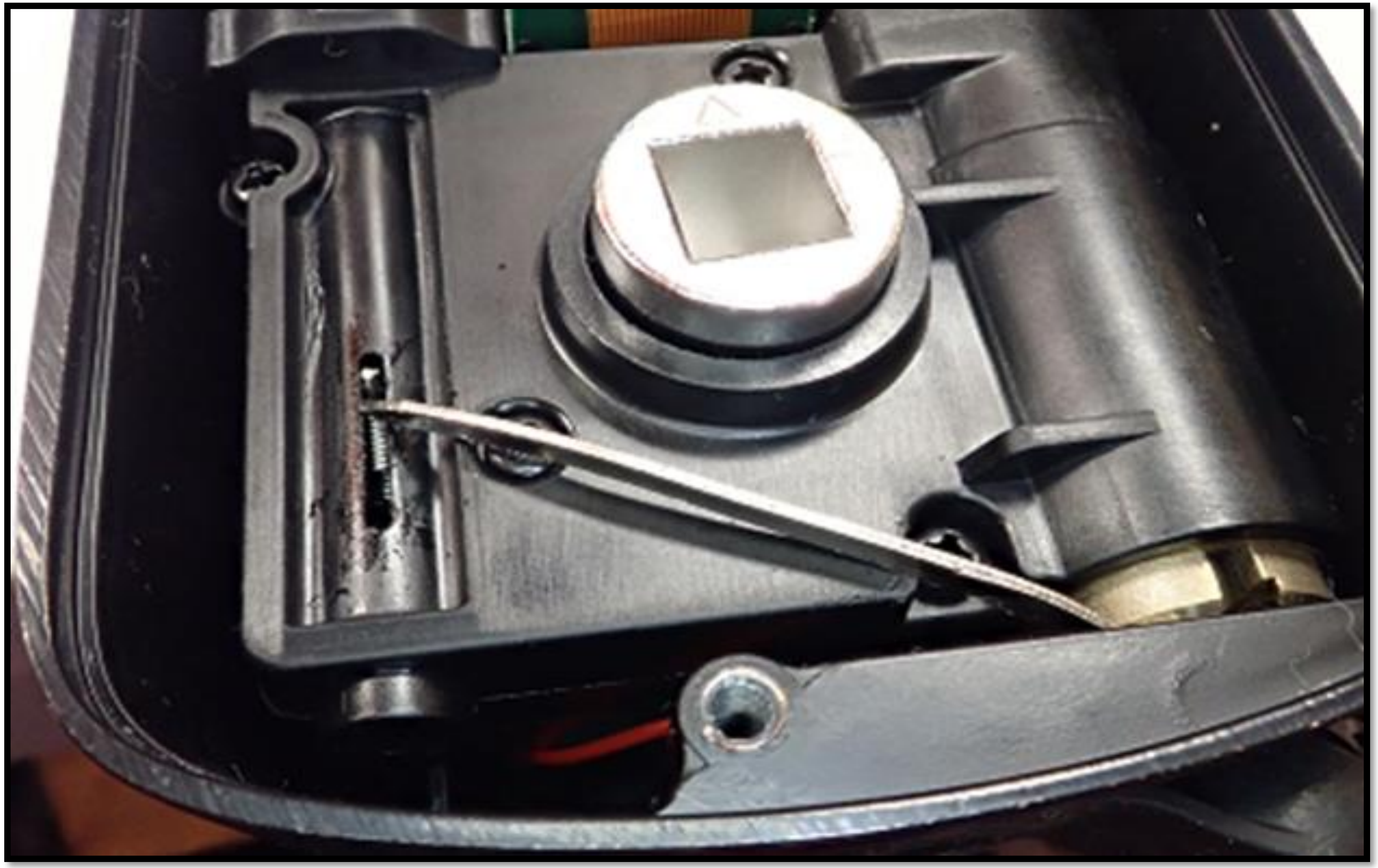
192.168.240.1/gainspan/system/config/network

This XML file does not appear to have any style information associated with it. The document tree is shown below.

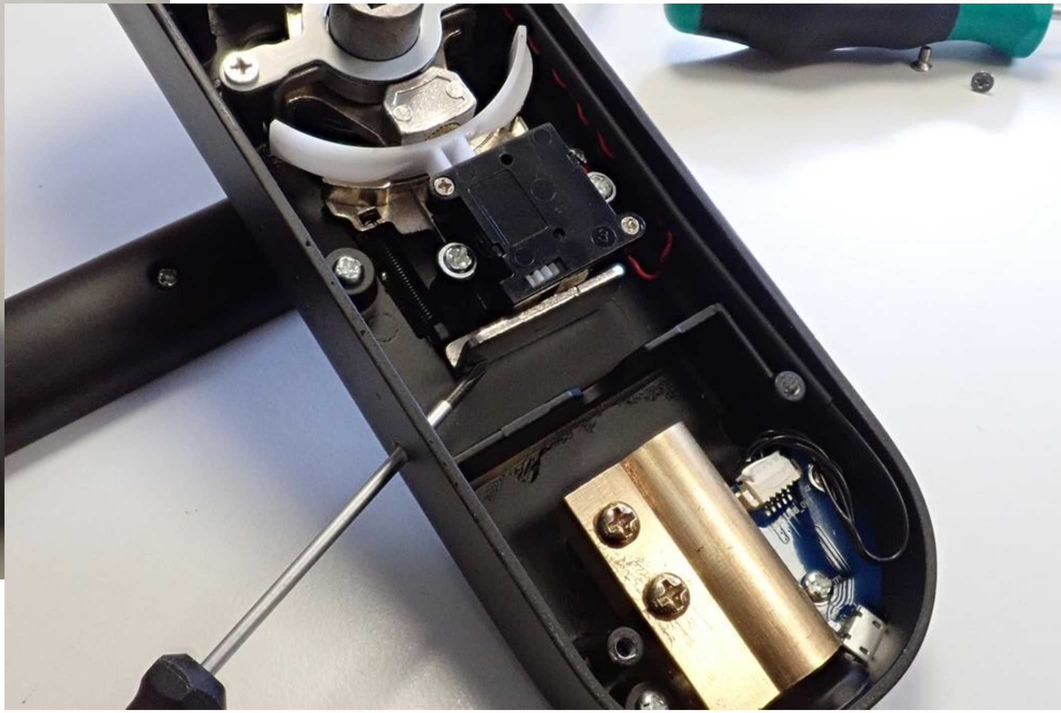
```
▼<network>
   <script/>
   <mode>limited-ap</mode>
   <ap_mode>user-ap</ap_mode>
   <object_id/>
 ▼<client>
   ▼<wireless>
      <channel>11</channel>
      <ssid>mywifi</ssid>
      <security>wpa-personal</security>
      <wepauth/>
      <password>supersecrets</password>
      <eap_type/>
      <eap_username/>
      <eap_password/>
    </wireless>
   ▼<ip>
      <ip_type>static</ip_type>
      <ip_addr>192.168.137.201</ip_addr>
      <subnetmask>255.255.255.0</subnetmask>
      <gateway>192.168.137.1</gateway>
      <dns_addr>192.168.137.1</dns_addr>
    </ip>
    <secret_key/>
  </client>
```

Ooh Look, the PSK!

A ‘smart’ door lock



Another not-so-smart lock



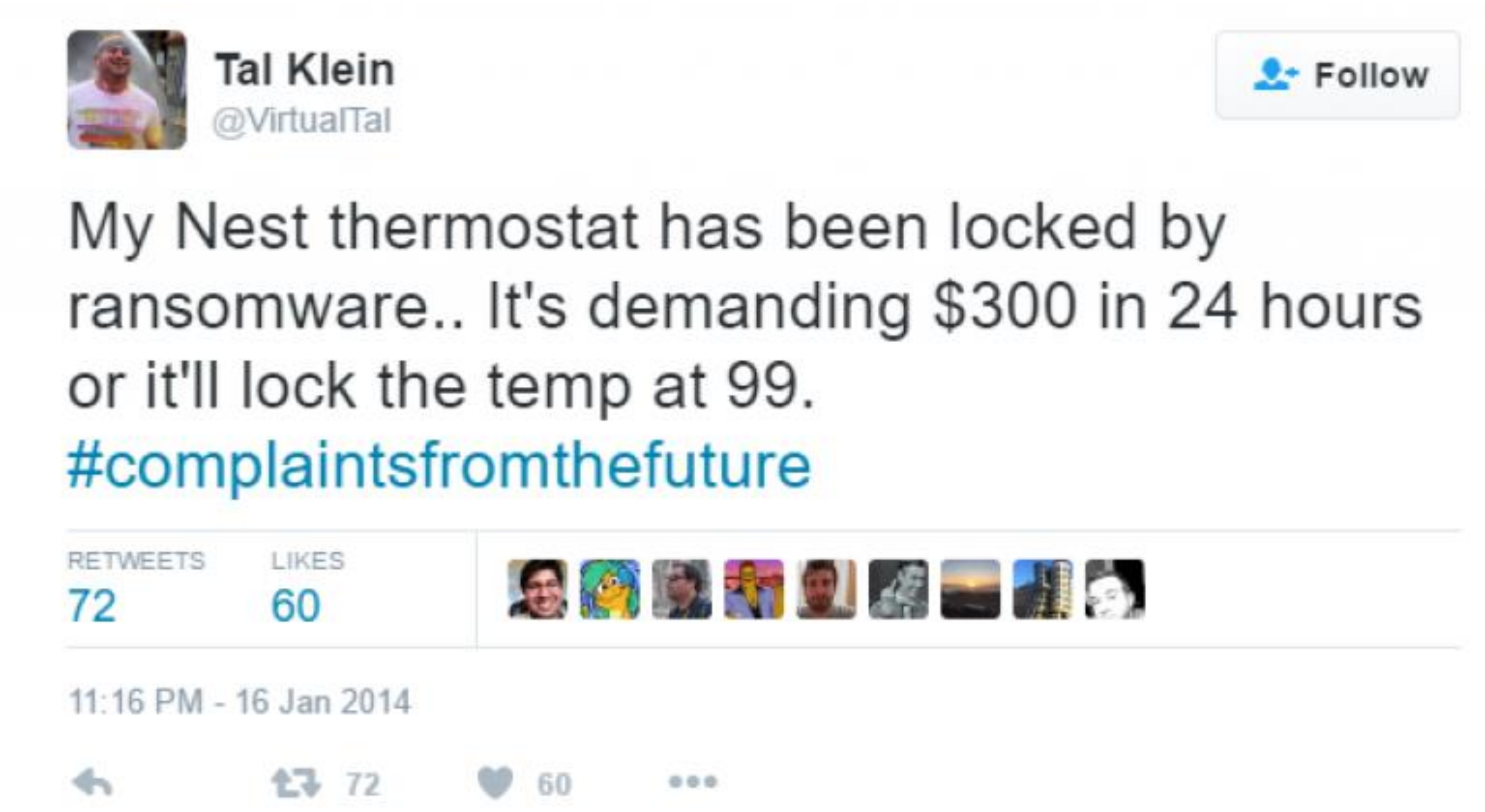
> A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

- Auguste Kerchoffs (not Kirchoffs, and pronounced differently)

The device is already in the hands of the attacker

Thermostat hack

Thermostat hack



Tal Klein
@VirtualTal

My Nest thermostat has been locked by ransomware.. It's demanding $300 in 24 hours or it'll lock the temp at 99. #complaintsfromthefuture

RETWEETS 72

LIKES 60

11:16 PM - 16 Jan 2014

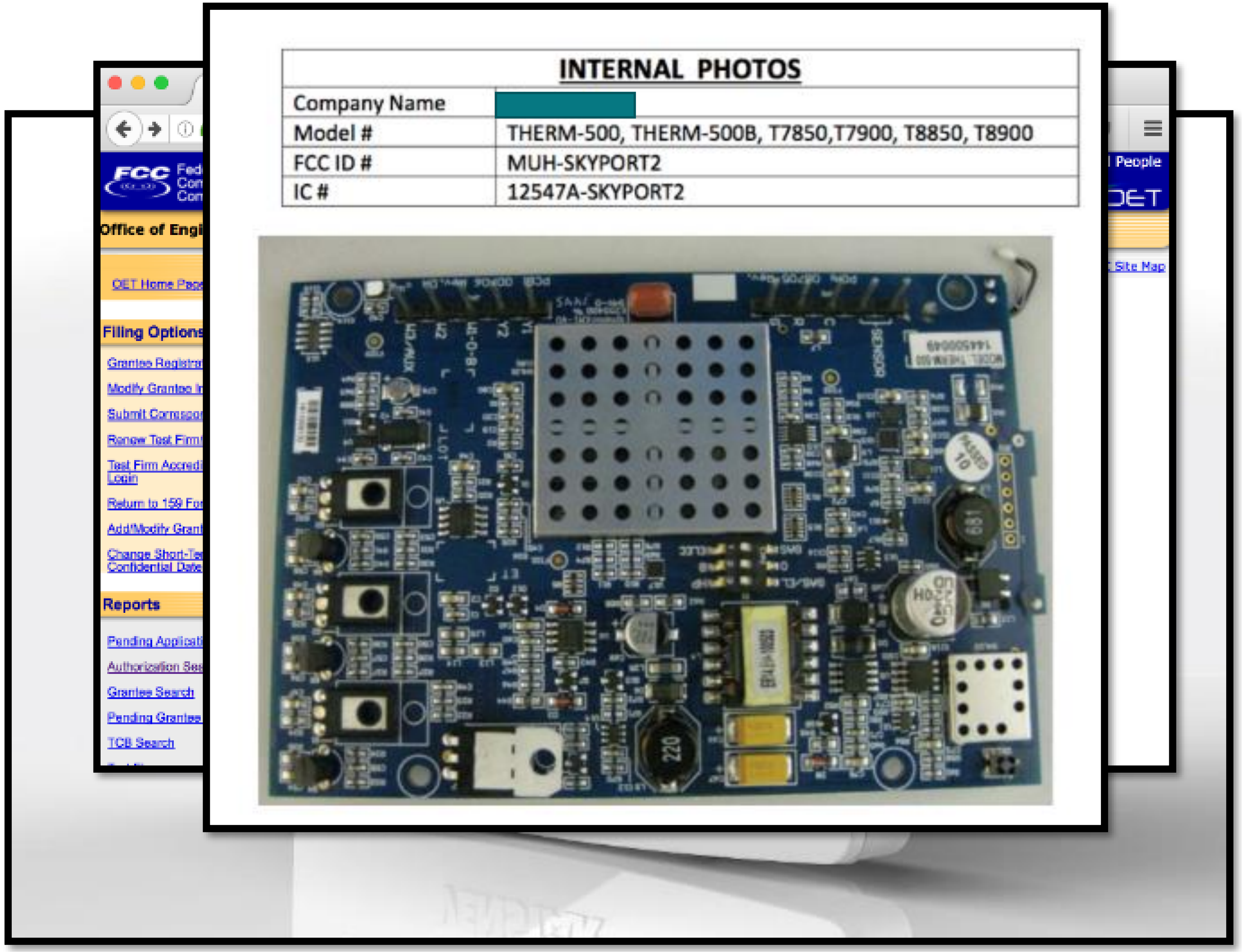
Ransomware

Could we take control of a smart thermostat?

Could we lock the user out and hold their heating/cooling to ransom?

A likely candidate found on Amazon

Quick check of FCC search suggested ARM/Linux



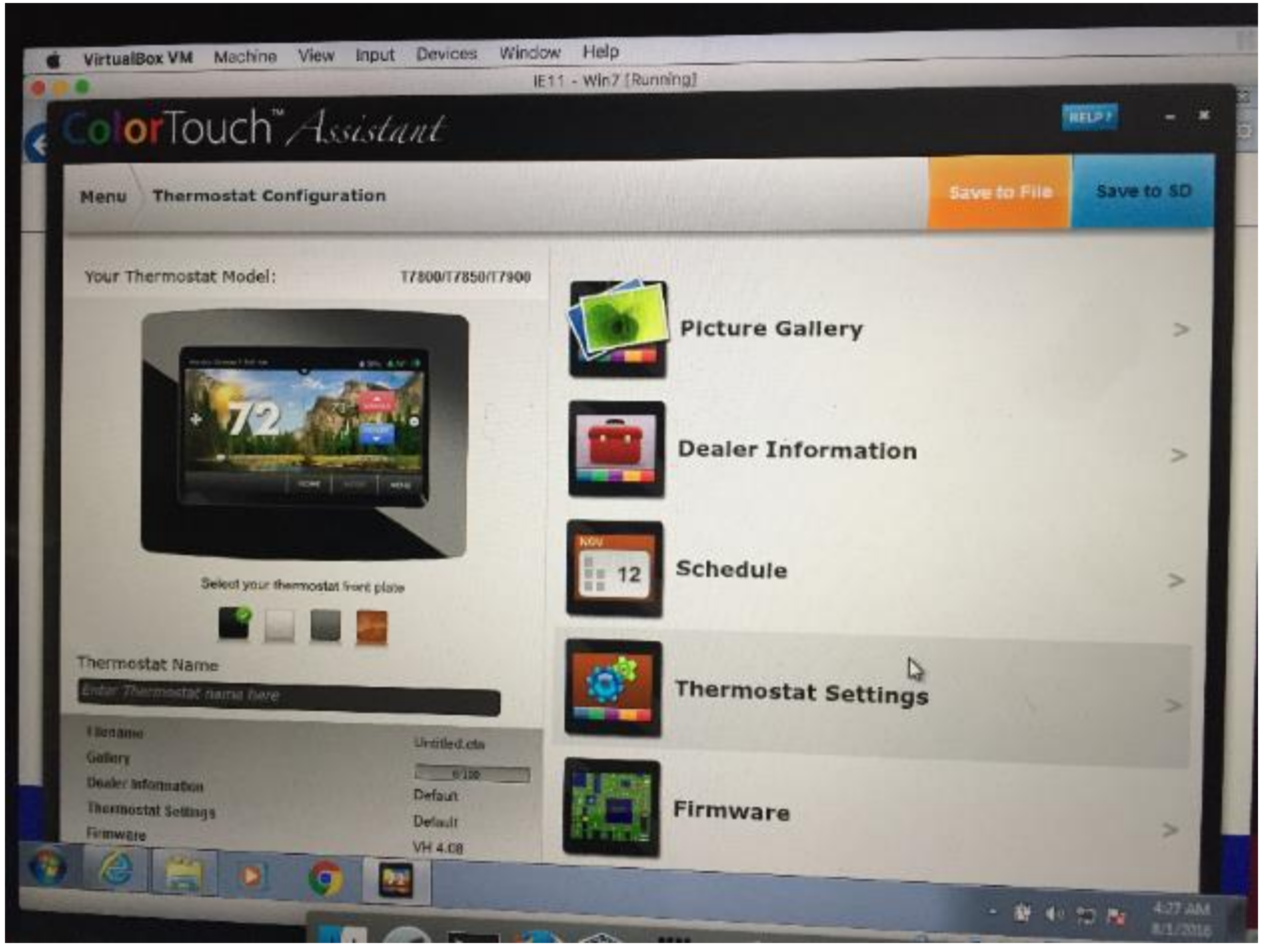
INTERNAL PHOTOS	
Company Name	[redacted]
Model #	THERM-500, THERM-500B, T7850,T7900, T8850, T8900
FCC ID #	MUH-SKYPORT2
IC #	12547A-SKYPORT2

The way in

Awkward for user to create complex schedules from the on-board user interface

A lovely Adobe Air app is available to allow customization on a PC, then load to thermostat from SD card

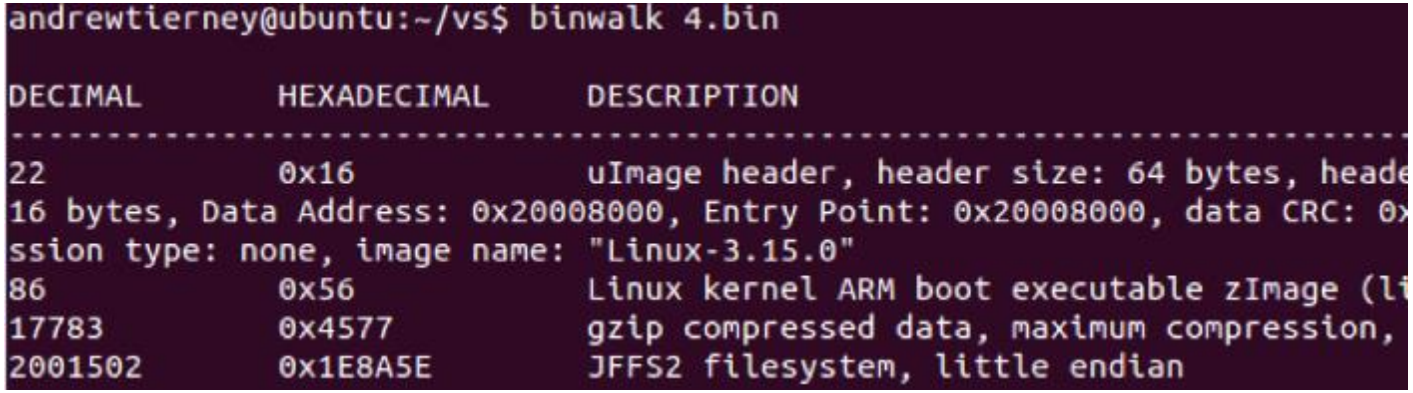
Includes the entire firmware, should an upgrade be required!!



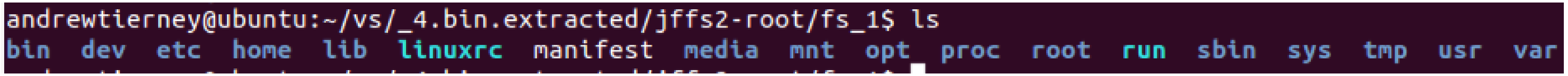
Your Thermostat Model: T7800/T7850/T7900

Filename Untitled.cta
Gallery 0/100
Dealer Information Default
Thermostat Settings Default
Firmware VH 4.08

Unpacking firmware



```
andrewtierney@ubuntu:~/vs$ binwalk 4.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
22            0x16            uImage header, header size: 64 bytes, heade
16 bytes, Data Address: 0x20008000, Entry Point: 0x20008000, data CRC: 0x
ssion type: none, image name: "Linux-3.15.0"
86            0x56            Linux kernel ARM boot executable zImage (li
17783         0x4577          gzip compressed data, maximum compression,
2001502       0x1E8A5E        JFFS2 filesystem, little endian
```



```
andrewtierney@ubuntu:~/vs/_4.bin.extracted/jffs2-root/fs_1$ ls
bin  dev  etc  home  lib  linuxrc  manifest  media  mnt  opt  proc  root  run  sbin  sys  tmp  usr  var
```

BINGO! We have the filesystem

Examining firmware

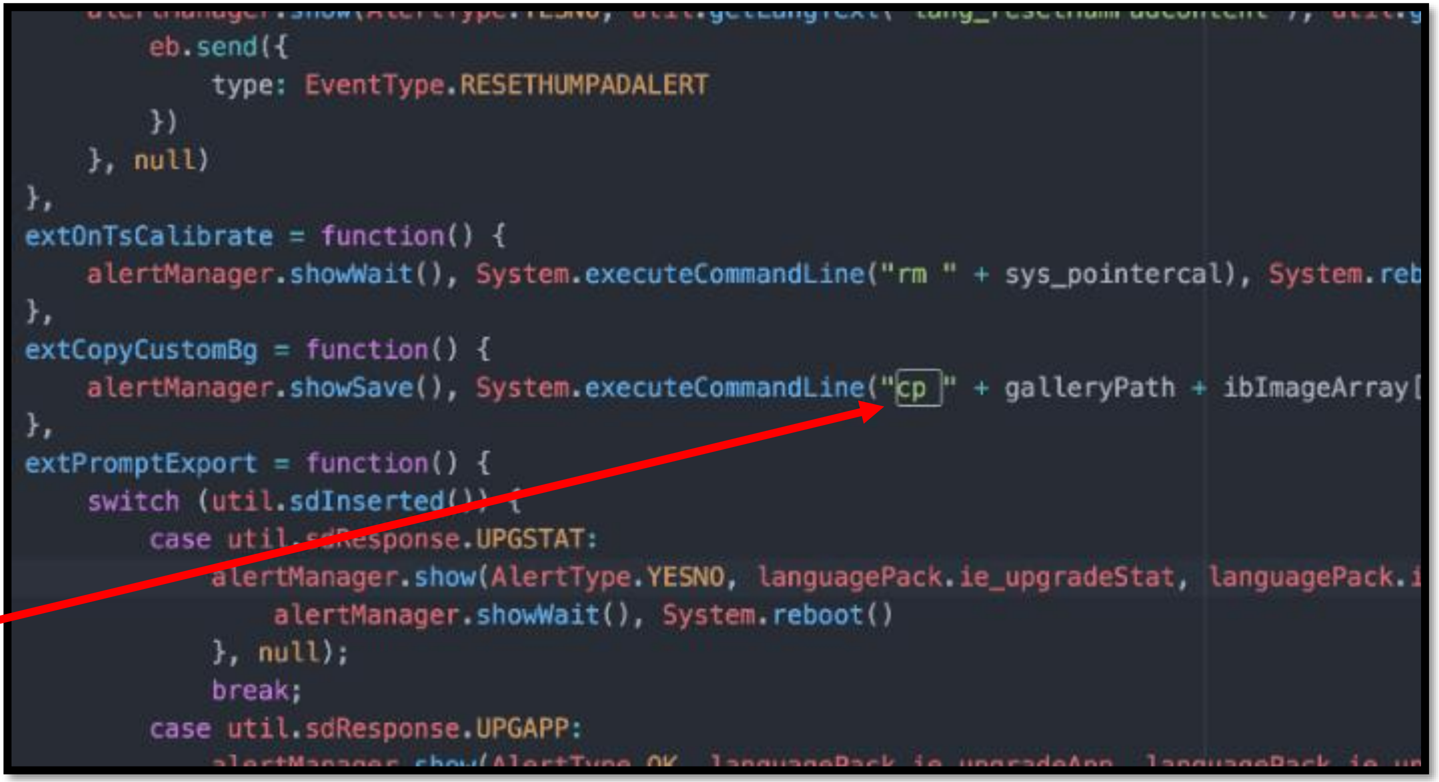
Remember SQL injection for web applications?

We can carry out similar attacks against filesystems using command injection

User input is not validated in some cases

The upload function for the screen background image is not validated correctly, so arbitrary commands can be executed

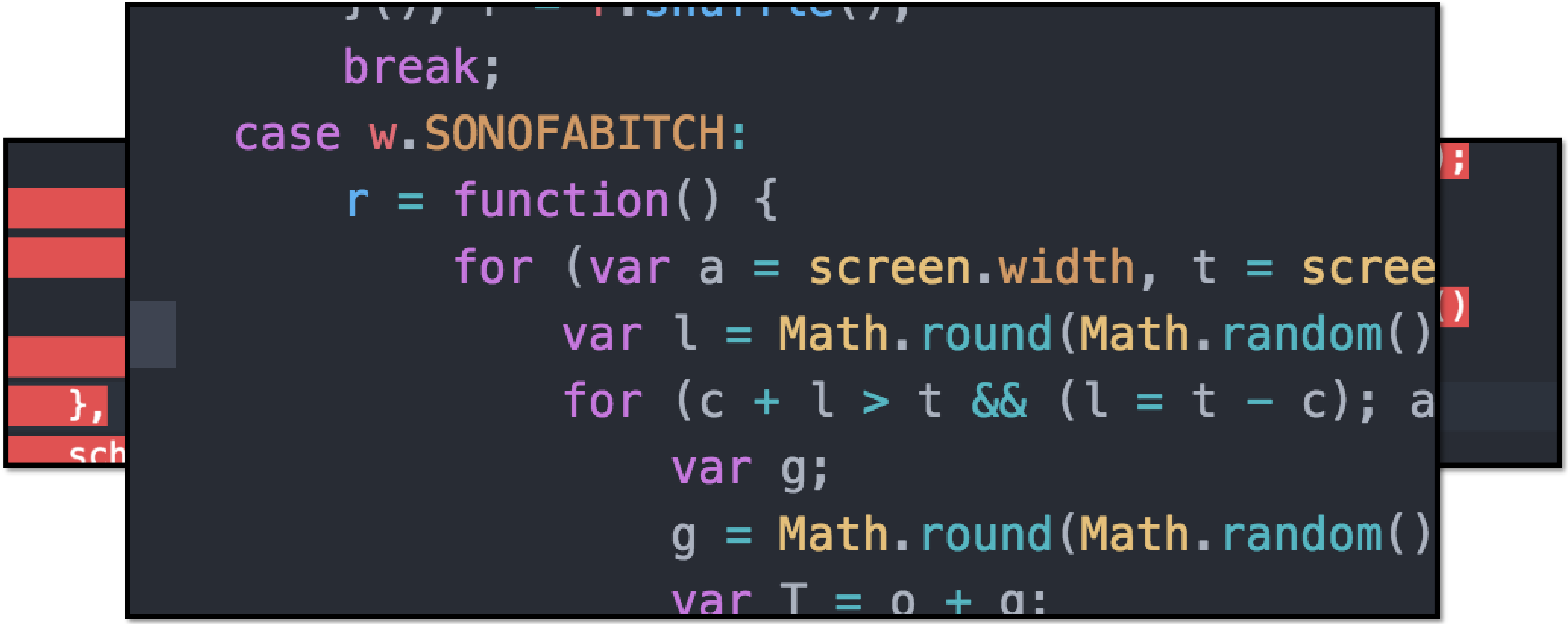
The developer gave no thought to attackers getting hold of the firmware:



```
    alertManager.show(AlertType.YESNO, util.getLangText("lang_resetHumpadContent"), util.g
        eb.send({
            type: EventType.RESETHUMPADALERT
        })
    }, null)
},
extOnTsCalibrate = function() {
    alertManager.showWait(), System.executeCommandLine("rm " + sys_pointercal), System.reb
},
extCopyCustomBg = function() {
    alertManager.showSave(), System.executeCommandLine("cp " + galleryPath + ibImageArray[
},
extPromptExport = function() {
    switch (util.sdInserted()) {
        case util.sdResponse.UPGSTAT:
            alertManager.show(AlertType.YESNO, languagePack.ie_upgradeStat, languagePack.i
                alertManager.showWait(), System.reboot()
            }, null);
            break;
        case util.sdResponse.UPGAPP:
            alertManager.show(AlertType.OK, languagePack.ie_upgradeApp, languagePack.ie_up
```

More developer issues

This dev really didn’t think their code would ever be seen!



```
    }(); r = r.shuffle();
    break;
case w.SONOFABITCH:
    r = function() {
        for (var a = screen.width, t = scree
            var l = Math.round(Math.random()
            for (c + l > t && (l = t - c); a
                var g;
                g = Math.round(Math.random()
                var T = o + g;
```

```
},
sch
```

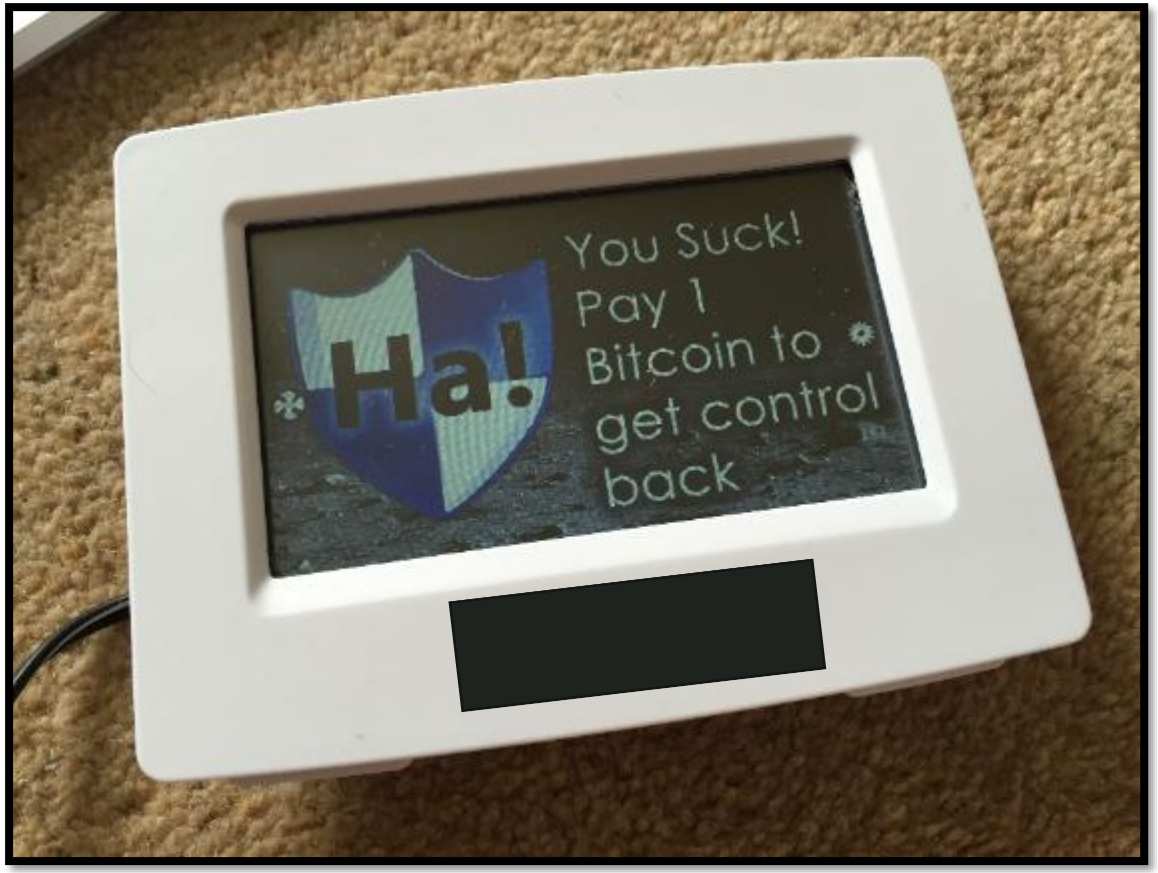
```
);
()
```

Taking control

Now we can upload a shell and gain full control of the thermostat, it even survives a reboot:

- Create an IRC channel so we can control the stat remotely
- Change the screen lock PIN to lock the user out
- Change the screen background to some ransomware
- Send on/off messages to boiler & a/c 3 times per second until they fail

All because a filename was implicitly trusted by device



[redacted]

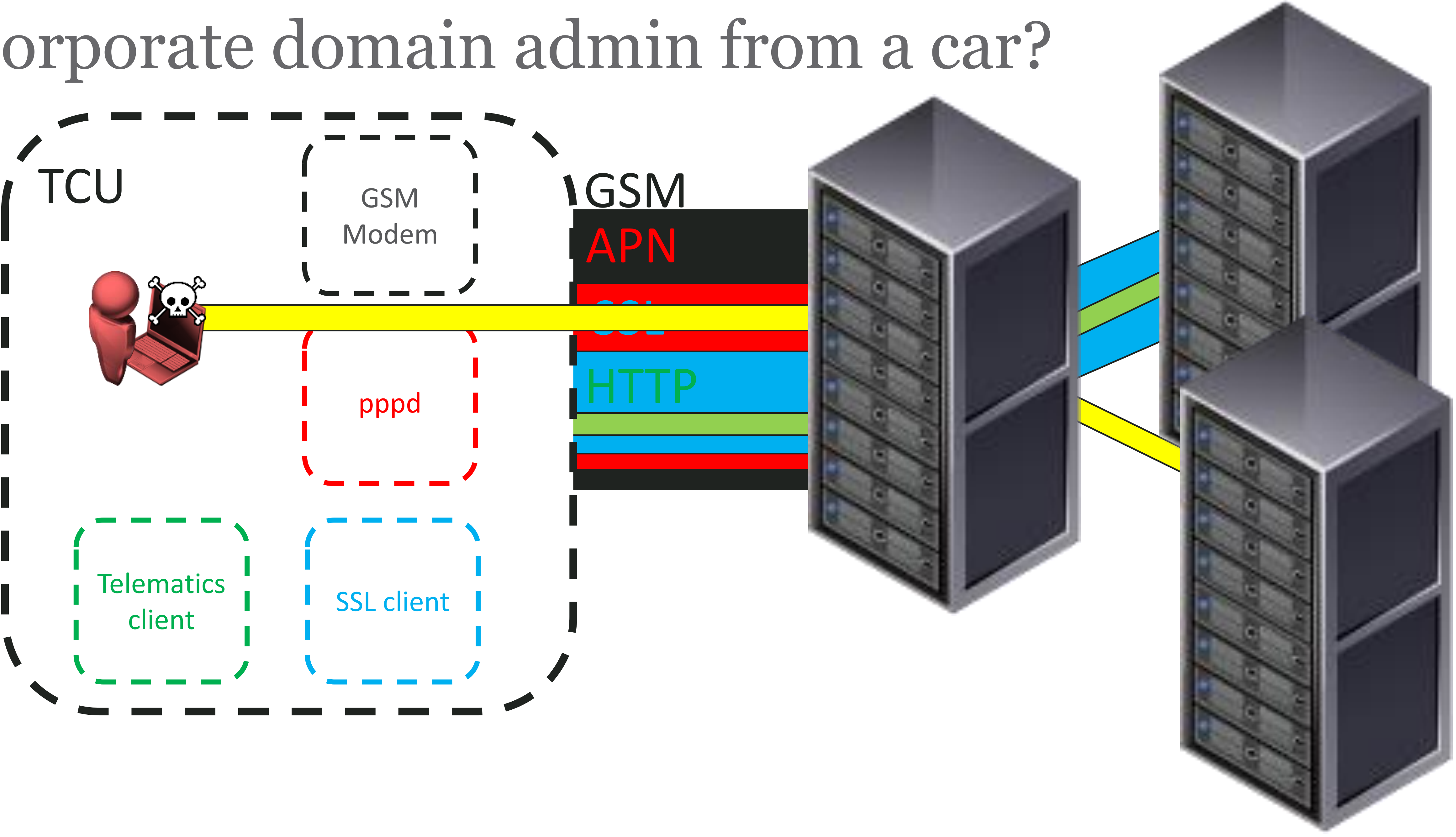
“ Physical access should not mean game over! ”

The device is already in the hands of the attacker

Solved, right…

The device is already in the hands of the attacker

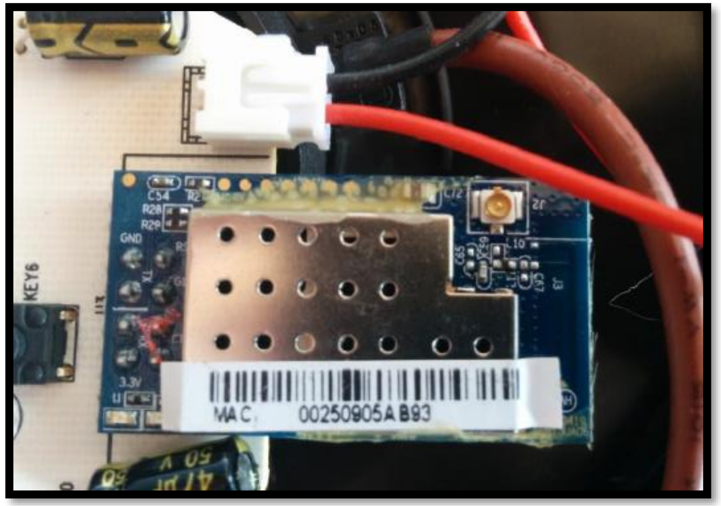
Corporate domain admin from a car?



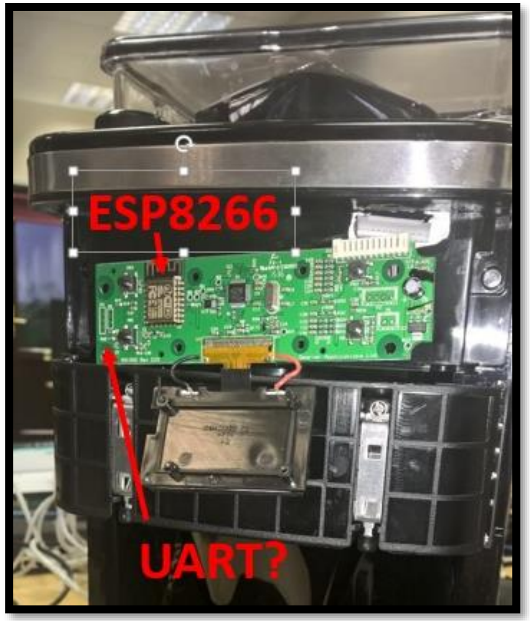
Key Extraction

Key extraction

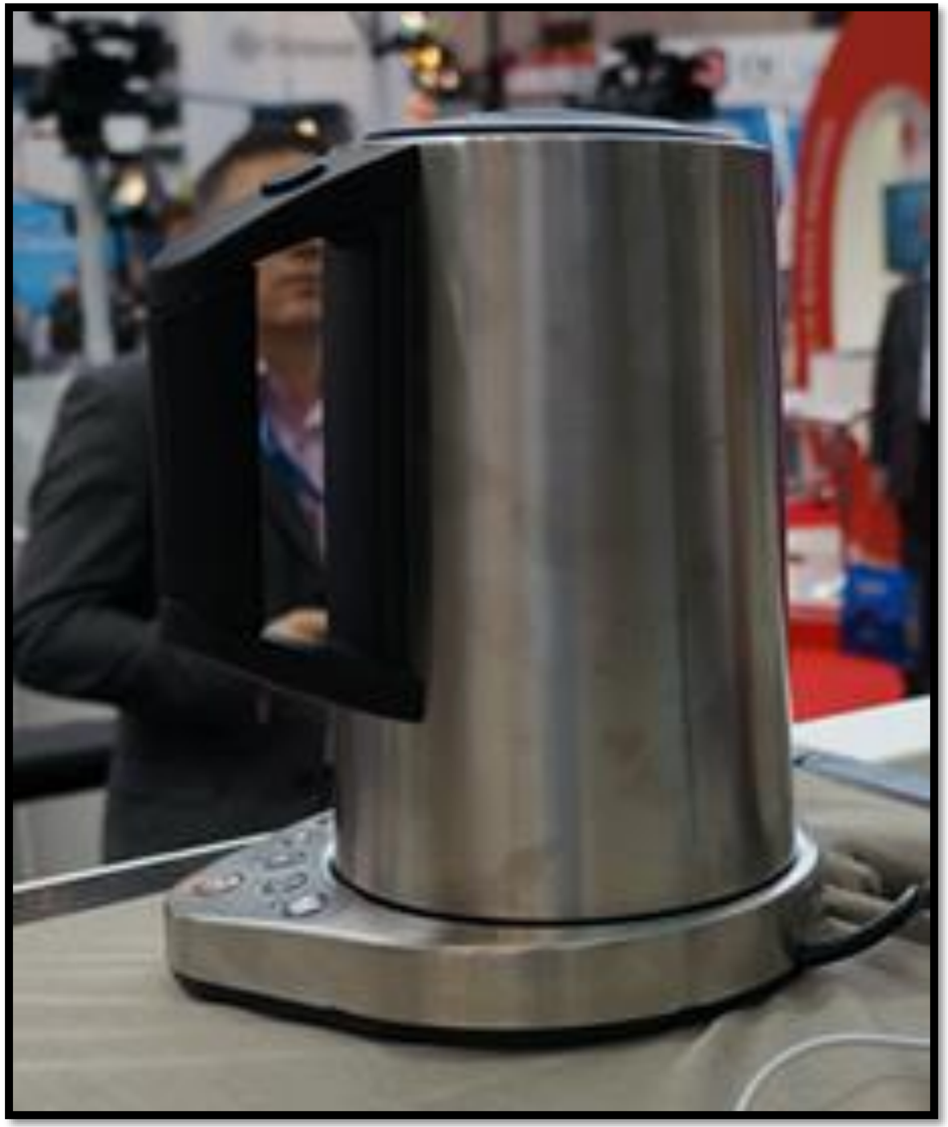
VSD-03 module has no secure storage



V2.0 used ESP8266, also with no secure storage



ESP32 offers better security functionality, but has been thoroughly broken



Key Distribution

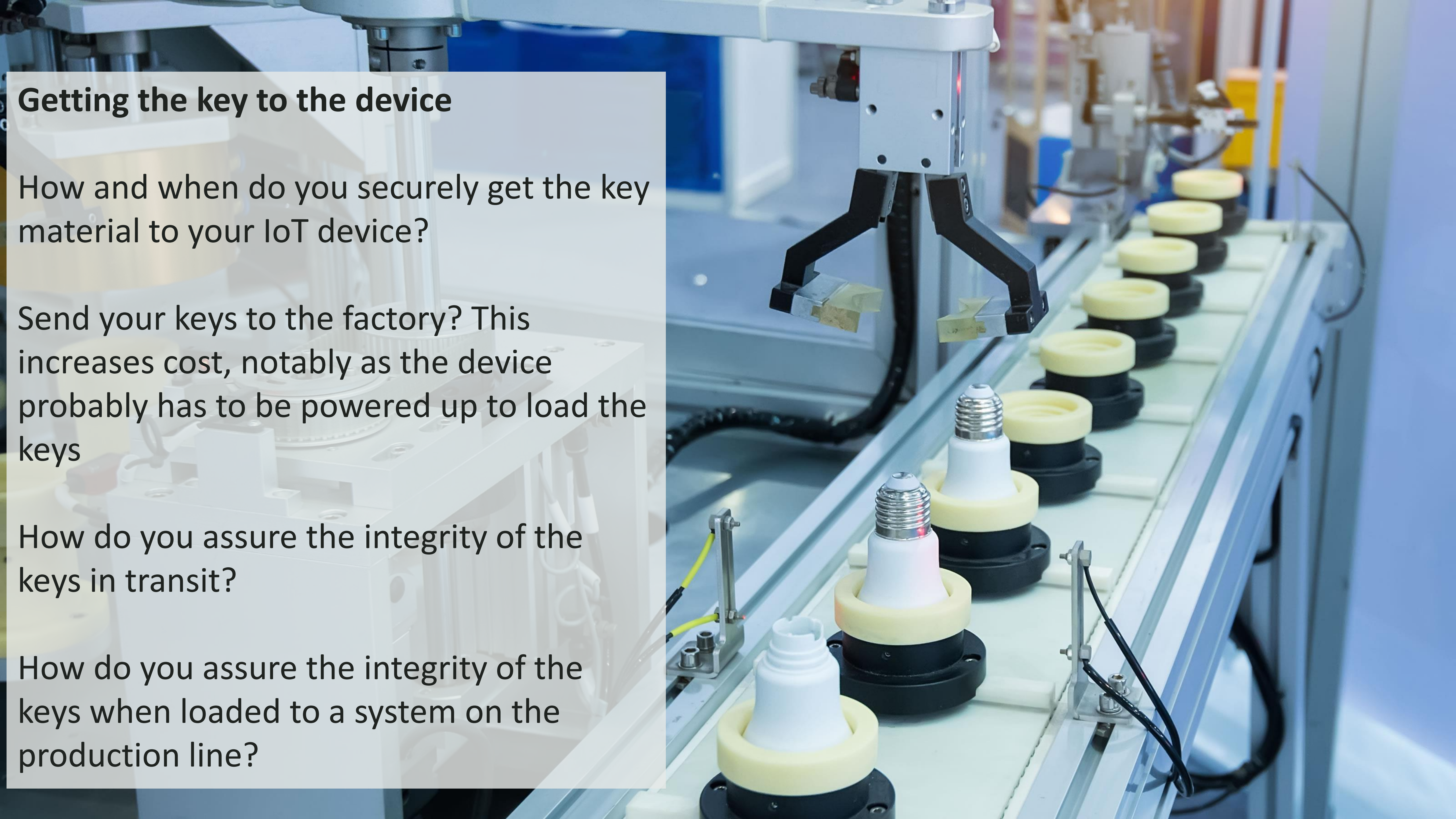
Getting the key to the device

How and when do you securely get the key material to your IoT device?

Send your keys to the factory? This increases cost, notably as the device probably has to be powered up to load the keys

How do you assure the integrity of the keys in transit?

How do you assure the integrity of the keys when loaded to a system on the production line?

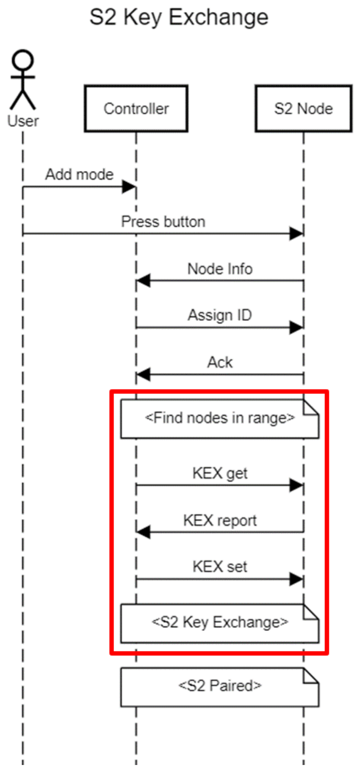


How do you know that your manufacturer actually loads the keys correctly & doesn't just flash the same key on to every device?

How do you know someone hasn't copied your keys?

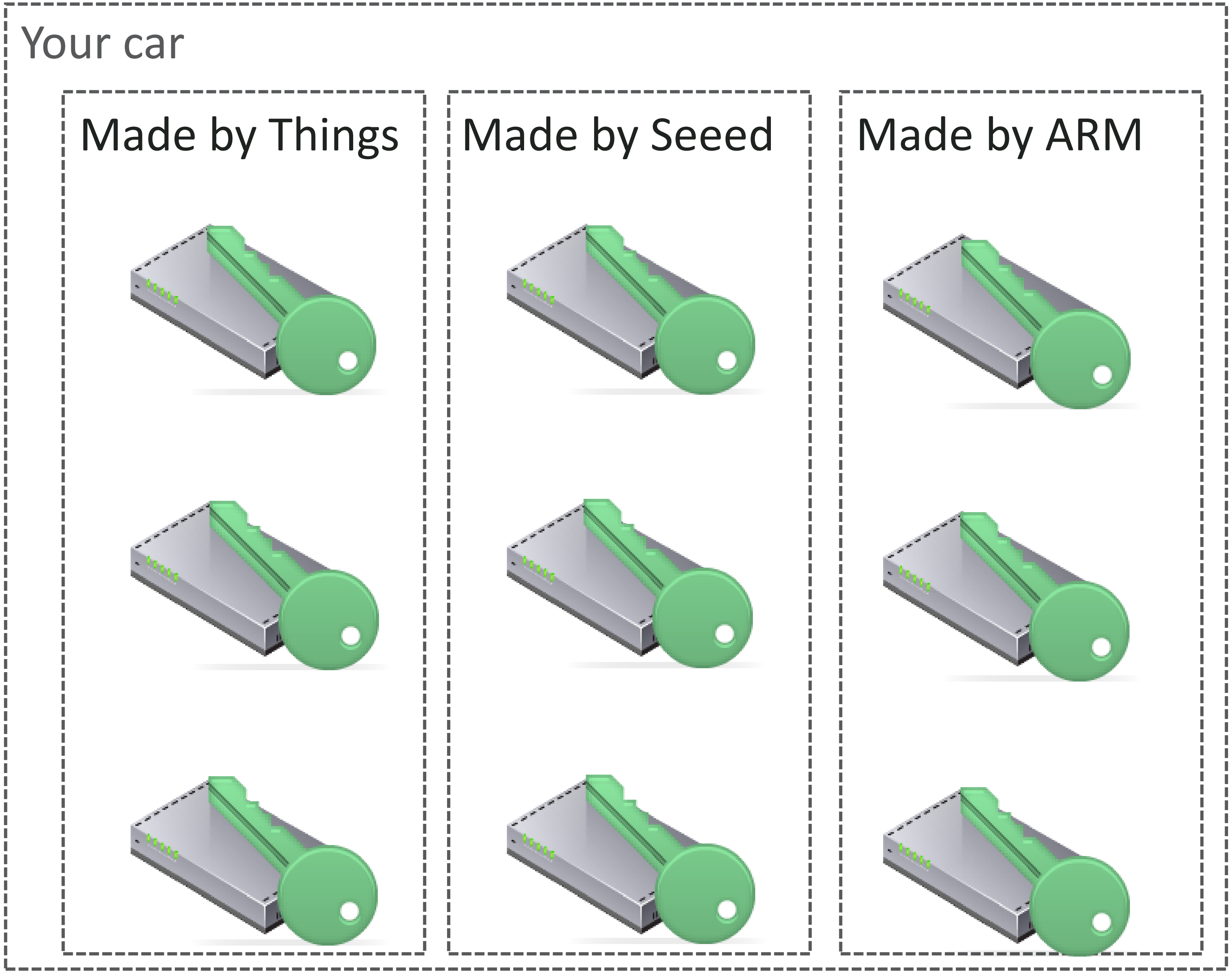
Other options include having the user configure the device on first use, maybe using a smart phone

Interception or tampering with that configuration process is a real issue



Further device challenges

Devices made by tens of makers
Who is the trust authority?
Who manages these keys?
Who is the certificate authority?



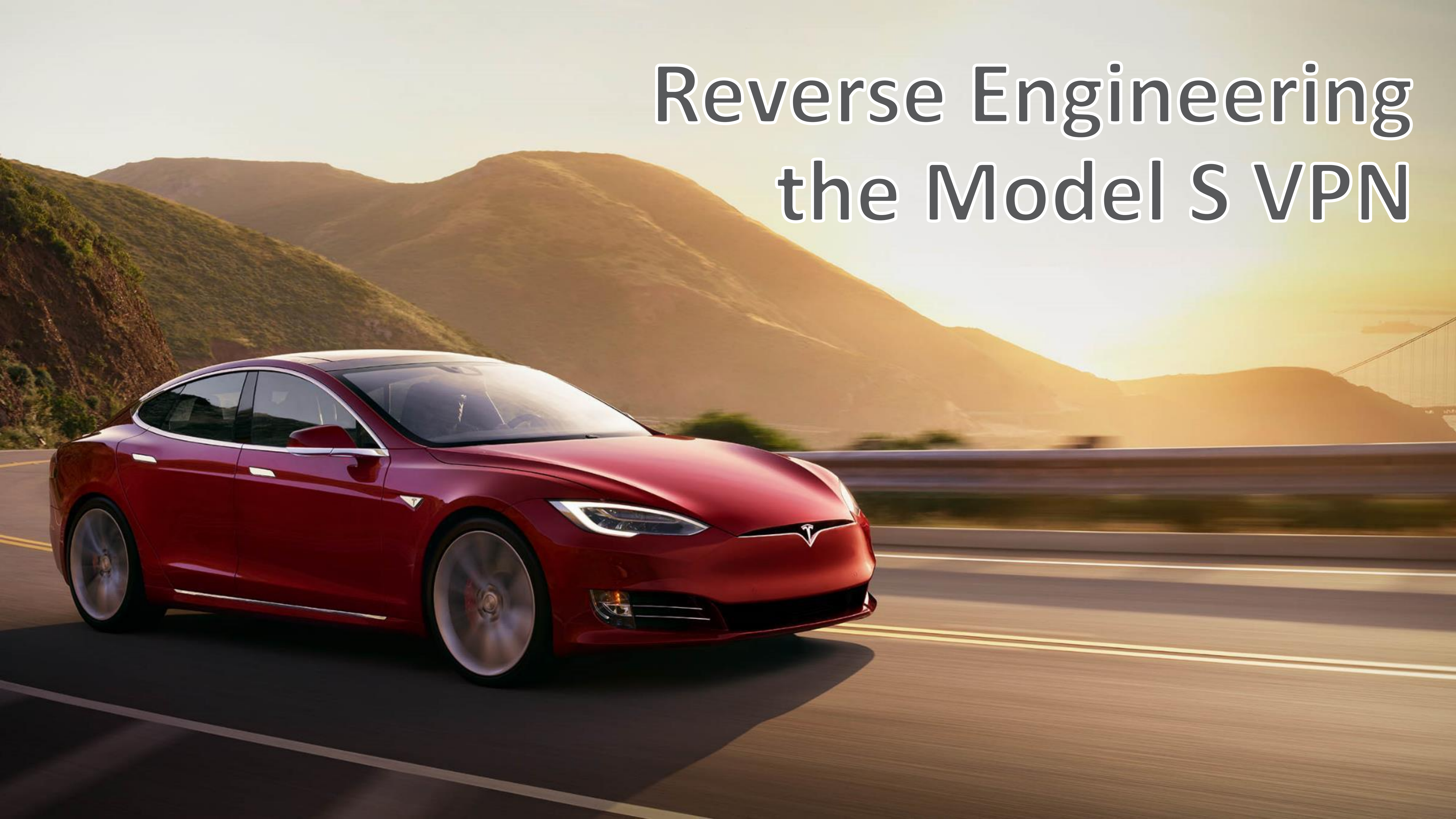
Your car

Made by Things

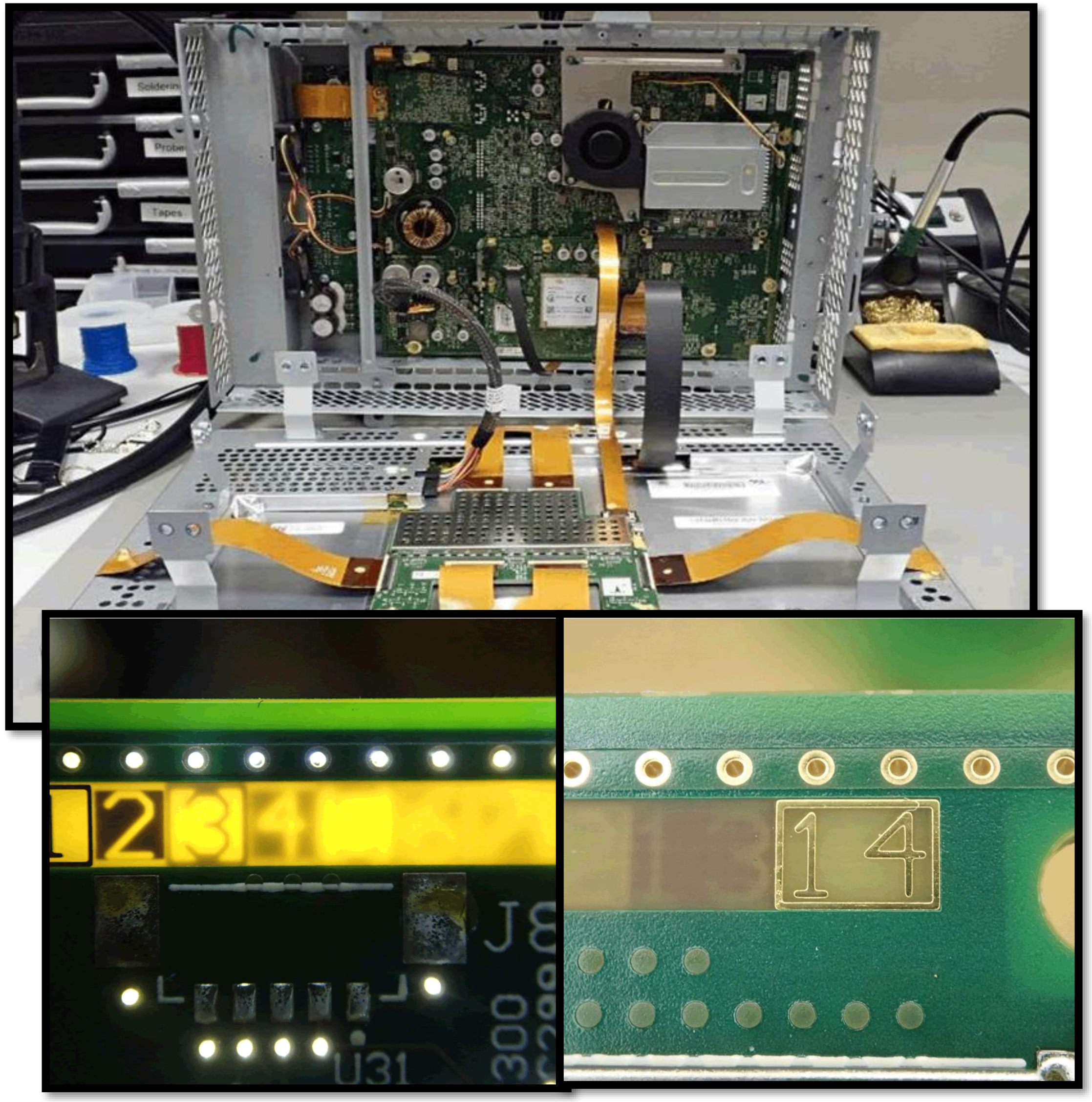
Made by Seeed

Made by ARM

Reverse Engineering the Model S VPN



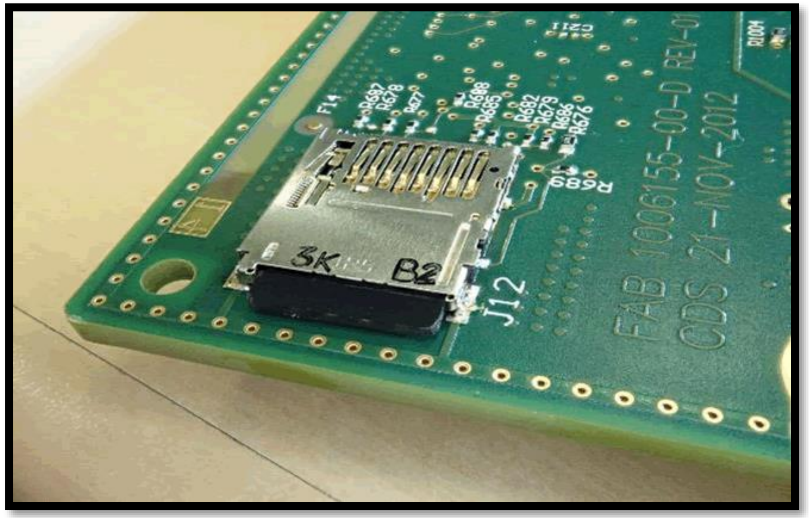
Model S VPN & Firmware Update Process



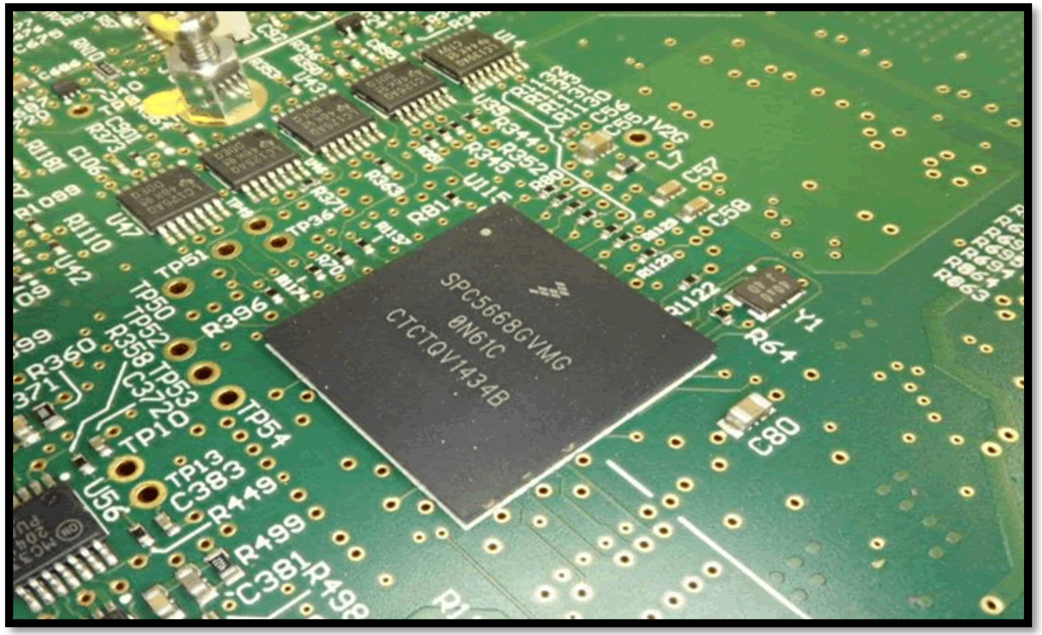
All done within terms of Tesla bug bounty programme

With support from Tesla

Key to it was a 4GB SD card used for staging updates to the vehicle



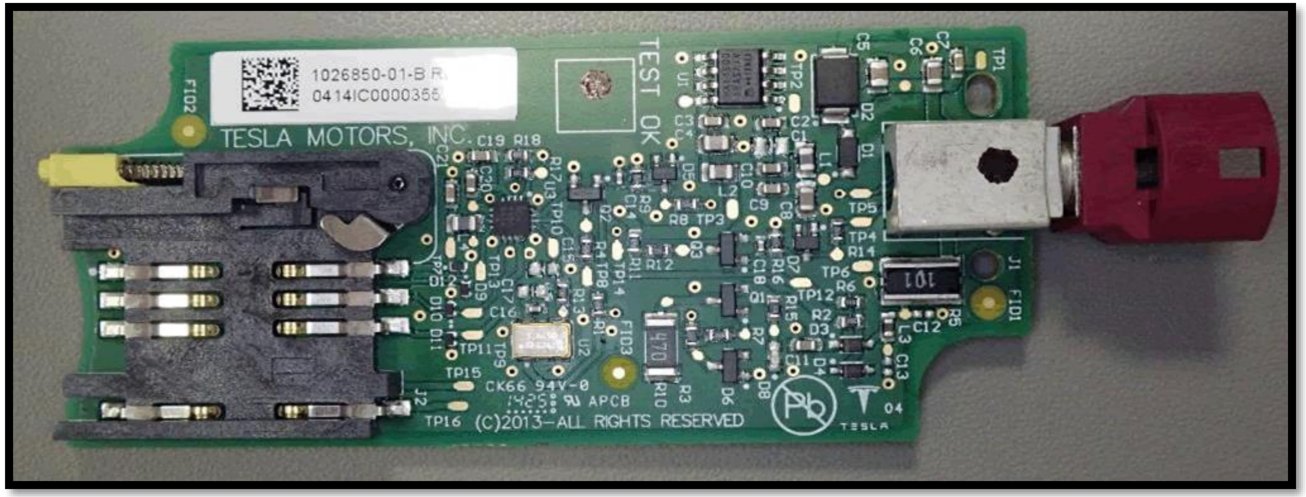
Model S VPN

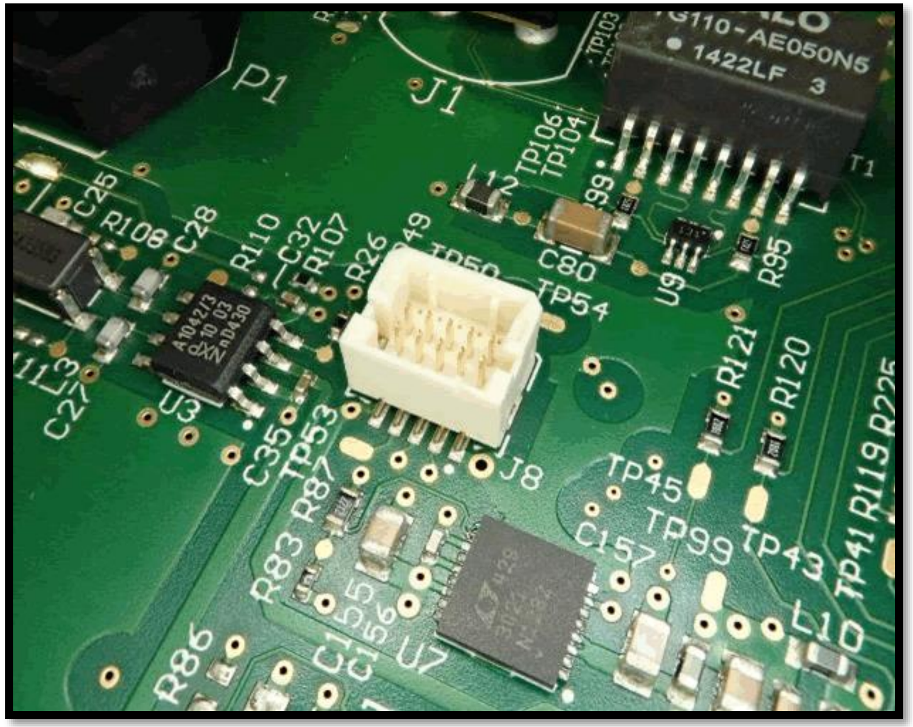


Broadly, done very well. Good CAN gateway

Hardware well configured

JTAG and other programming interfaces locked & securely passworded





Basics

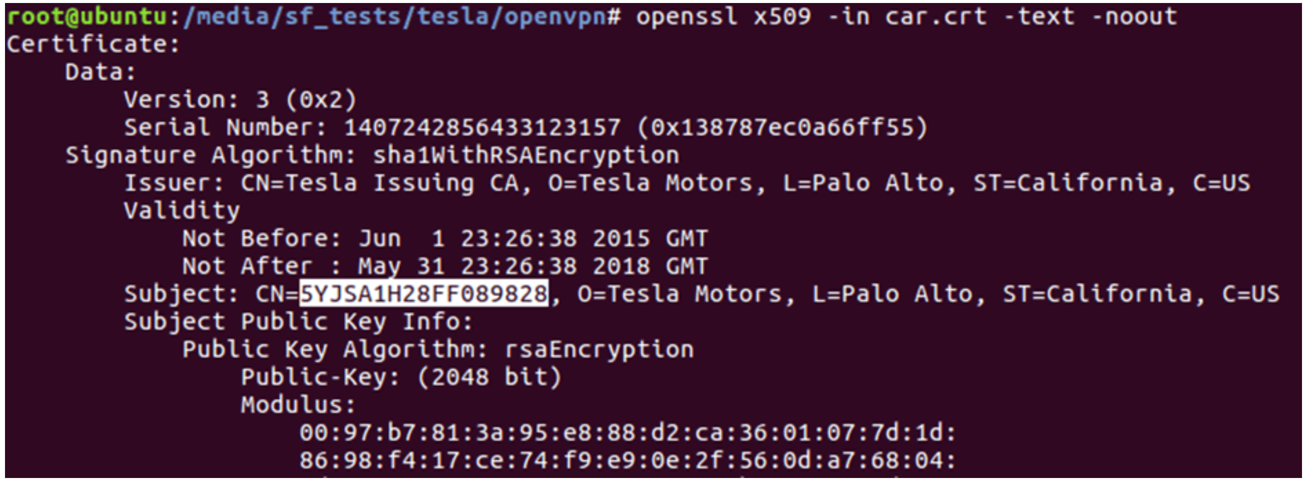
Per-vehicle keys & certificates used

Can be extracted locally from CID

Can be re-used on another system

Otherwise, well configured VPN

Interesting affinity for Wi-Fi over cellular for larger downloads



```
root@ubuntu:/media/sf_tests/tesla/openvpn# openssl x509 -in car.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1407242856433123157 (0x138787ec0a66ff55)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=Tesla Issuing CA, O=Tesla Motors, L=Palo Alto, ST=California, C=US
        Validity
            Not Before: Jun  1 23:26:38 2015 GMT
            Not After : May 31 23:26:38 2018 GMT
        Subject: CN=5YJSA1H28FF089828, O=Tesla Motors, L=Palo Alto, ST=California, C=US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:97:b7:81:3a:95:e8:88:d2:ca:36:01:07:7d:1d:
                    86:98:f4:17:ce:74:f9:e9:0e:2f:56:0d:a7:68:04:
```

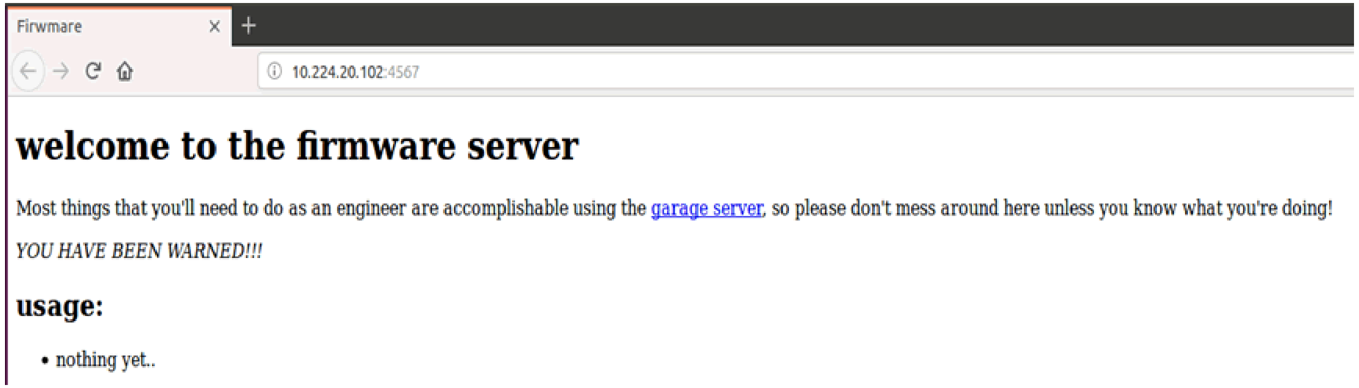
Early reports showed VPN keys stored on removable SD card

Not the case in this and later cars: stored on NAND flash in the CID, recoverable with work

Recovering firmware

Now that we have VPN keys, we are effectively a vehicle in the eyes of the Mothership

Odd JSON responses, probably as second IC module we were using was from a wrecked US vehicle



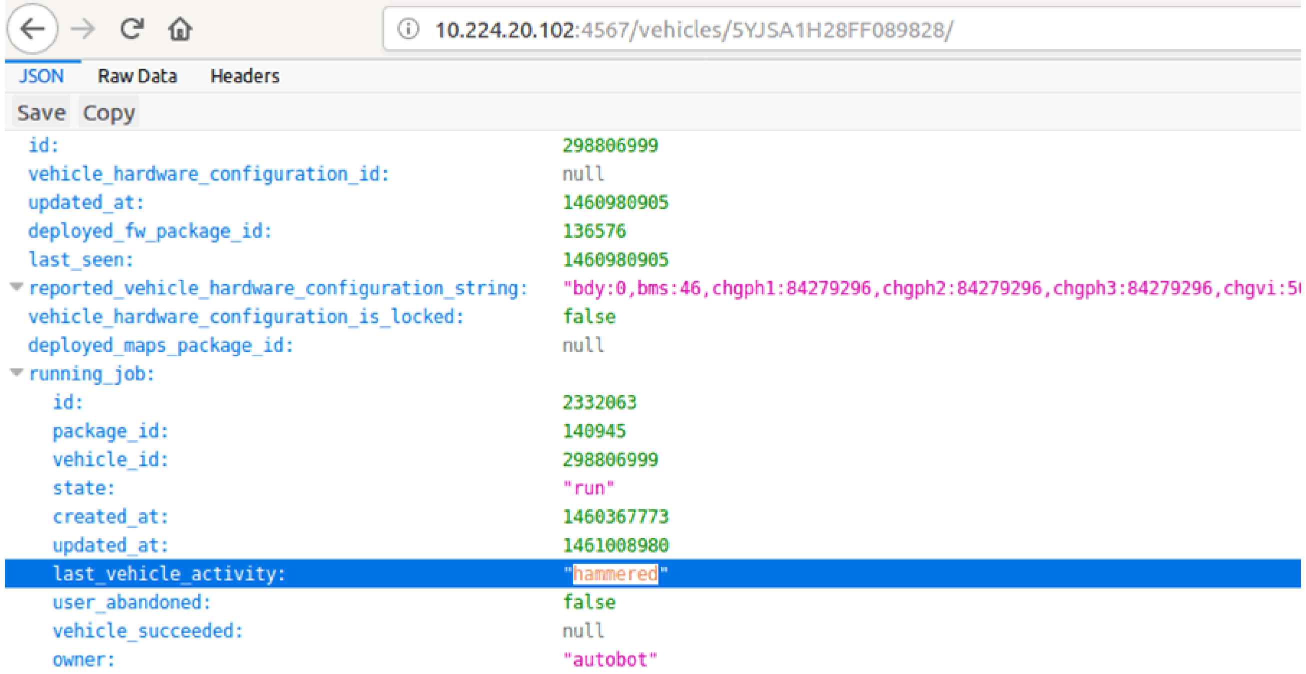
welcome to the firmware server

Most things that you'll need to do as an engineer are accomplishable using the garage server, so please don't mess around here unless you know what you're doing!

YOU HAVE BEEN WARNED!!!

usage:

- nothing yet..



```
  id:                                               298806999
  vehicle_hardware_configuration_id:                null
  updated_at:                                       1460980905
  deployed_fw_package_id:                           136576
  last_seen:                                        1460980905
▼ reported_vehicle_hardware_configuration_string:   "bdy:0,bms:46,chgph1:84279296,chgph2:84279296,chgph3:84279296,chgvi:5
  vehicle_hardware_configuration_is_locked:         false
  deployed_maps_package_id:                         null
▼ running_job:
    id:                                             2332063
    package_id:                                     140945
    vehicle_id:                                     298806999
    state:                                          "run"
    created_at:                                     1460367773
    updated_at:                                     1461008980
    last_vehicle_activity:                          "hammered"
    user_abandoned:                                 false
    vehicle_succeeded:                              null
    owner:                                          "autobot"
```

Recovering firmware

http://firmware.vn.teslamotors.com:4567/vehicles/<VIN>/handshake

Firmware_download_url – the location of the file we will be downloading

Firmware_download_file_md5 – the MD5 checksum of the file we will be downloading

Download_status_url – a URL to post back the status of the upgrade

Vehicle_job_status_url

Unpack_size – size of the unpacked firmware file

Install_size – size required to install the firmware file

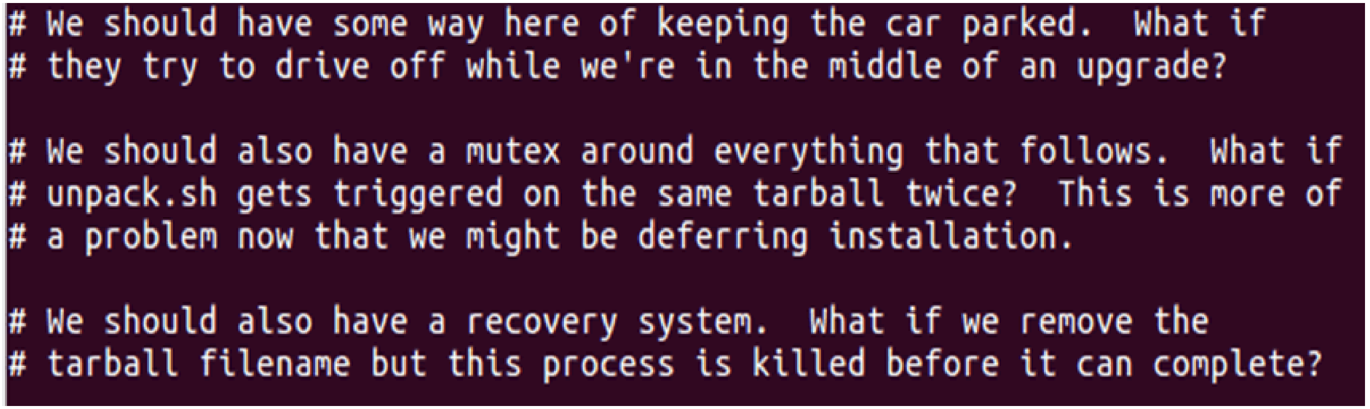
Recovering firmware

Shell scripts are run, unpacking firmware

First checking that vehicle is in ‘park’

Install.sh runs, with only MD5 checksum for integrity

ONLY layer of security is the VPN



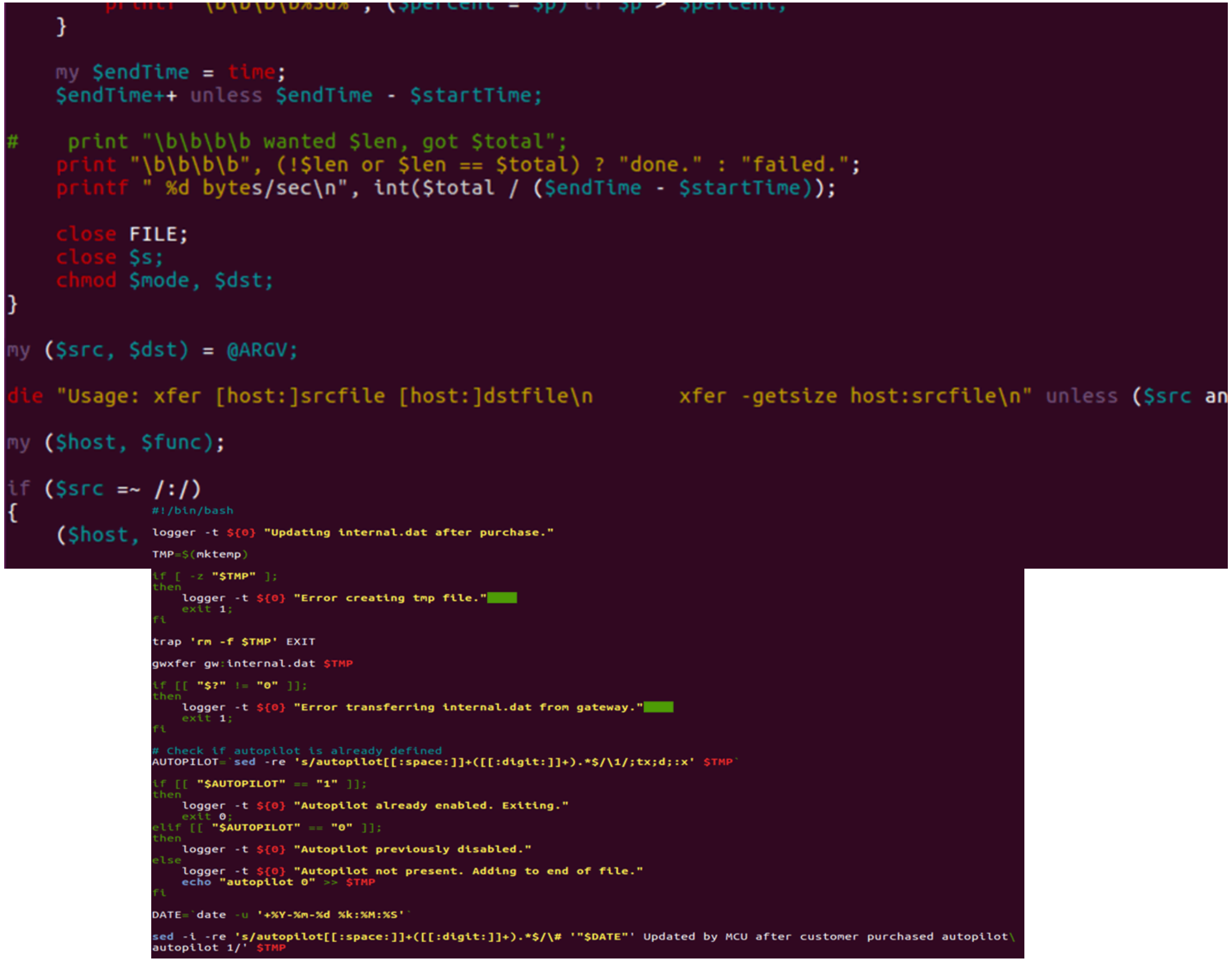
```
# We should have some way here of keeping the car parked.  What if
# they try to drive off while we're in the middle of an upgrade?

# We should also have a mutex around everything that follows.  What if
# unpack.sh gets triggered on the same tarball twice?  This is more of
# a problem now that we might be deferring installation.

# We should also have a recovery system.  What if we remove the
# tarball filename but this process is killed before it can complete?
```

Analysing firmware update

Surprising lack of authentication from CID to ECUs

Ability to enable premium features, such as autopilot

Not clear how battery range was extended remotely by Tesla



```
        printf "\b\b\b\b%3d%", ($percent = $p) if $p > $percent;
    }

    my $endTime = time;
    $endTime++ unless $endTime - $startTime;

#    print "\b\b\b\b wanted $len, got $total";
    print "\b\b\b\b", (!$len or $len == $total) ? "done." : "failed.";
    printf " %d bytes/sec\n", int($total / ($endTime - $startTime));

    close FILE;
    close $s;
    chmod $mode, $dst;
}

my ($src, $dst) = @ARGV;

die "Usage: xfer [host:]srcfile [host:]dstfile\n       xfer -getsize host:srcfile\n" unless ($src an

my ($host, $func);

if ($src =~ /:/)
{
    ($host,
```

```
#!/bin/bash

logger -t ${0} "Updating internal.dat after purchase."

TMP=$(mktemp)

if [ -z "$TMP" ];
then
    logger -t ${0} "Error creating tmp file."
    exit 1;
fi

trap 'rm -f $TMP' EXIT

gwxfer gw:internal.dat $TMP

if [[ "$?" != "0" ]];
then
    logger -t ${0} "Error transferring internal.dat from gateway."
    exit 1;
fi

# Check if autopilot is already defined
AUTOPILOT=`sed -re 's/autopilot[[:space:]]+([[:digit:]]+).*$/\1/;tx;d;:x' $TMP`

if [[ "$AUTOPILOT" == "1" ]];
then
    logger -t ${0} "Autopilot already enabled. Exiting."
    exit 0;
elif [[ "$AUTOPILOT" == "0" ]];
then
    logger -t ${0} "Autopilot previously disabled."
else
    logger -t ${0} "Autopilot not present. Adding to end of file."
    echo "autopilot 0" >> $TMP
fi

DATE=`date -u '+%Y-%m-%d %k:%M:%S'`

sed -i -re 's/autopilot[[:space:]]+([[:digit:]]+).*$/\# '"$DATE"' Updated by MCU after customer purchased autopilot\
autopilot 1/' $TMP
```

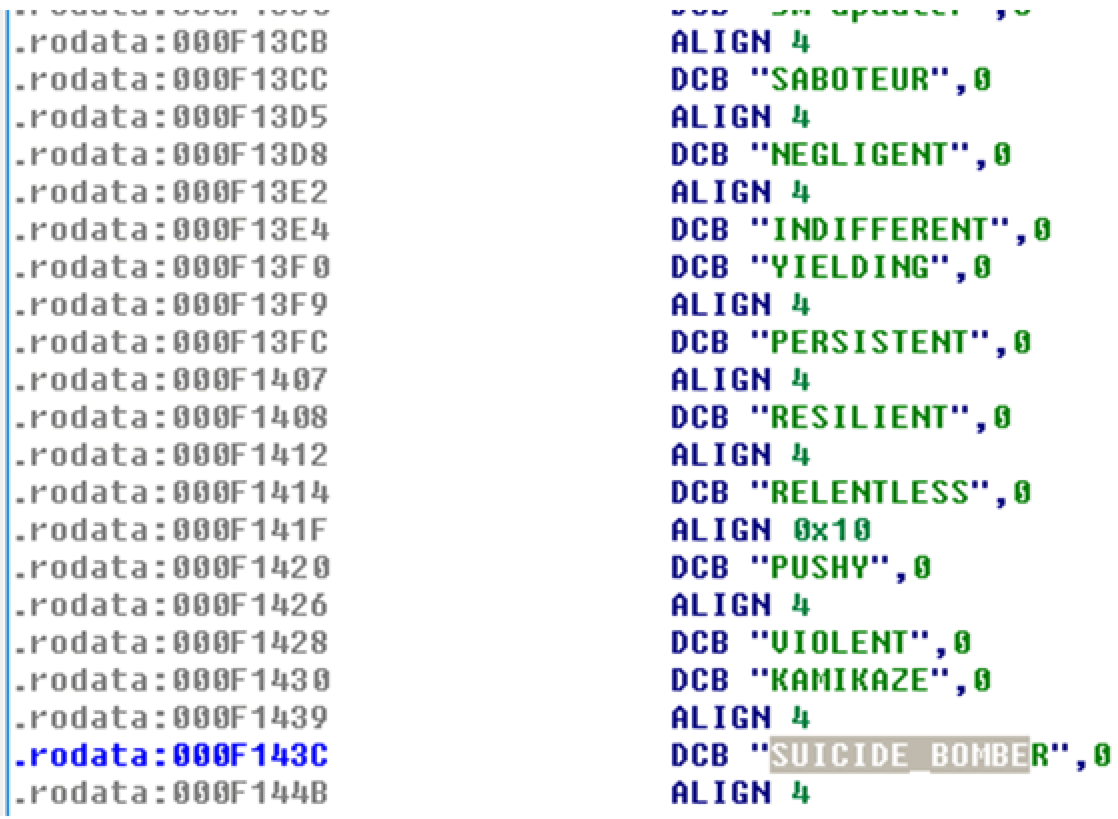
Some interesting Easter Eggs

Sometimes firmware refuses to apply

Mismatch between ID of CID and replaced IC

Tesla kindly fixed this for us!

‘Aggresiveness’ of firmware push can be changed



```
.rodata:000F13CB                ALIGN 4
.rodata:000F13CC                DCB "SABOTEUR",0
.rodata:000F13D5                ALIGN 4
.rodata:000F13D8                DCB "NEGLIGENT",0
.rodata:000F13E2                ALIGN 4
.rodata:000F13E4                DCB "INDIFFERENT",0
.rodata:000F13F0                DCB "YIELDING",0
.rodata:000F13F9                ALIGN 4
.rodata:000F13FC                DCB "PERSISTENT",0
.rodata:000F1407                ALIGN 4
.rodata:000F1408                DCB "RESILIENT",0
.rodata:000F1412                ALIGN 4
.rodata:000F1414                DCB "RELENTLESS",0
.rodata:000F141F                ALIGN 0x10
.rodata:000F1420                DCB "PUSHY",0
.rodata:000F1426                ALIGN 4
.rodata:000F1428                DCB "VIOLENT",0
.rodata:000F1430                DCB "KAMIKAZE",0
.rodata:000F1439                ALIGN 4
.rodata:000F143C                DCB "SUICIDE_BOMBER",0
.rodata:000F144B                ALIGN 4
```

High level conclusions

Better than many, but surprising oversights, given ‘clean sheet’ start

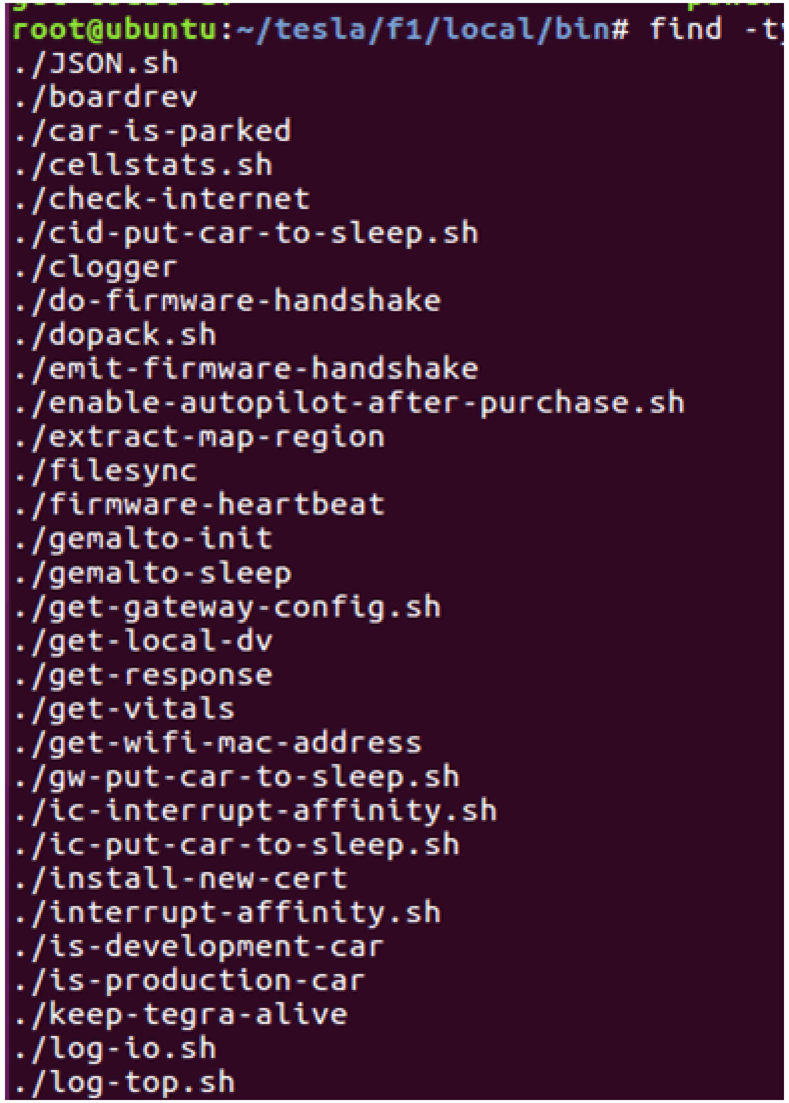
Reliance on VPN only, no defence in depth

- Keying per-vehicle, but trivial to extract keys

Bash on four wheels – trivial to enable premium functions

Access to CAN allows for reflashing of arbitrary ECUs

Taking root on the CID is probably possible, in time



```
root@ubuntu:~/tesla/f1/local/bin# find -t
./JSON.sh
./boardrev
./car-is-parked
./cellstats.sh
./check-internet
./cid-put-car-to-sleep.sh
./clogger
./do-firmware-handshake
./dopack.sh
./emit-firmware-handshake
./enable-autopilot-after-purchase.sh
./extract-map-region
./filesync
./firmware-heartbeat
./gemalto-init
./gemalto-sleep
./get-gateway-config.sh
./get-local-dv
./get-response
./get-vitals
./get-wifi-mac-address
./gw-put-car-to-sleep.sh
./ic-interrupt-affinity.sh
./ic-put-car-to-sleep.sh
./install-new-cert
./interrupt-affinity.sh
./is-development-car
./is-production-car
./keep-tegra-alive
./log-io.sh
./log-top.sh
```

User Identity is Important Also

My Friend Cayla

Interactive kids doll

Voice recognition, listens continuously whilst powered on

“Internet Safe” “Kid friendly”

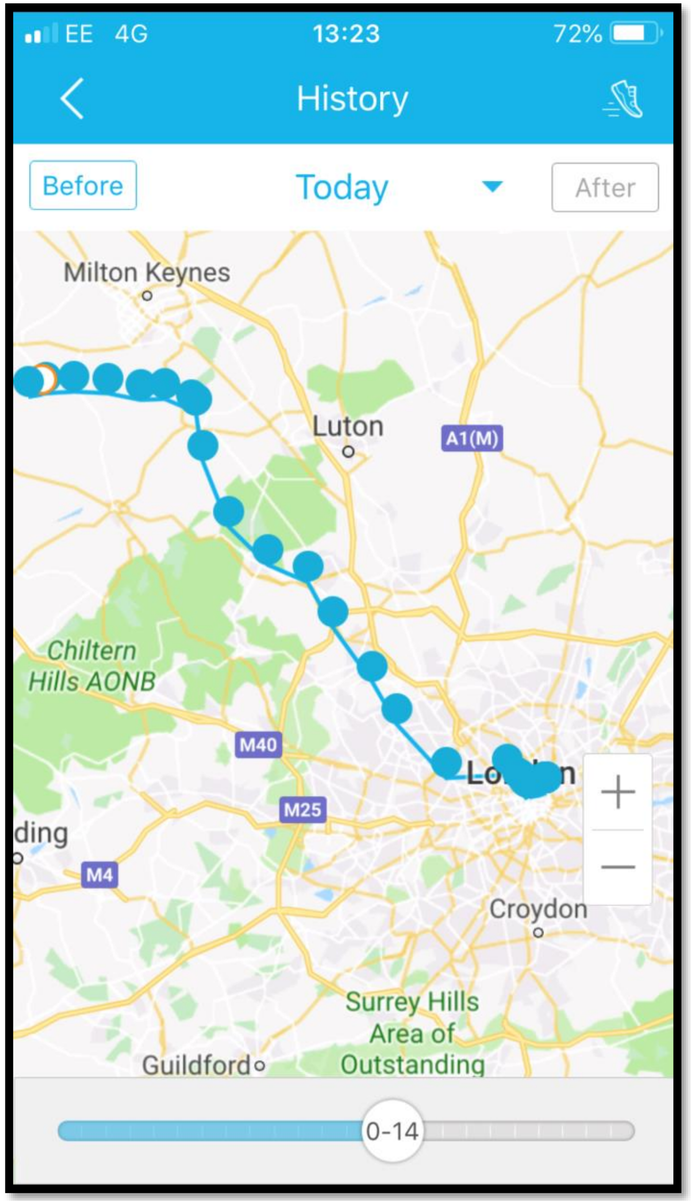
Anti-profanity filters

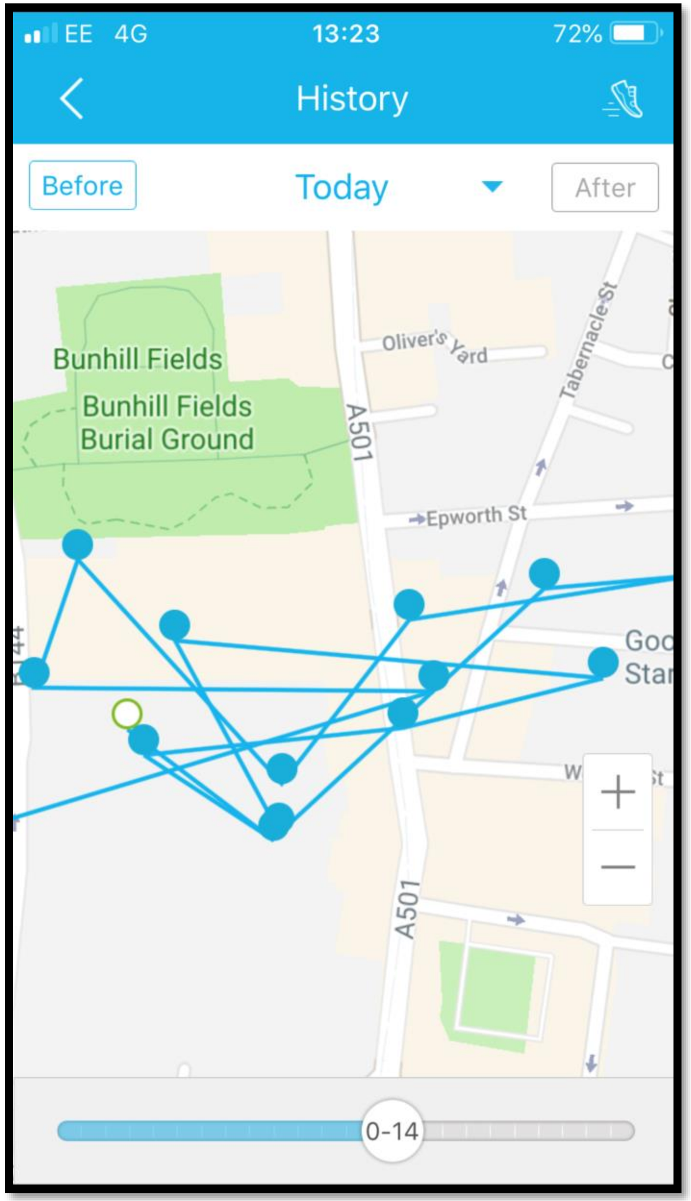
… so can we make her swear?

… could someone use her to spy on kids?

10:06
wed
03|24
PLUS
Kid's watcher
one-press phone call

Insecure Direct Object References





Change the child’s location

Set off geo-fencing alerts

Can also call the child

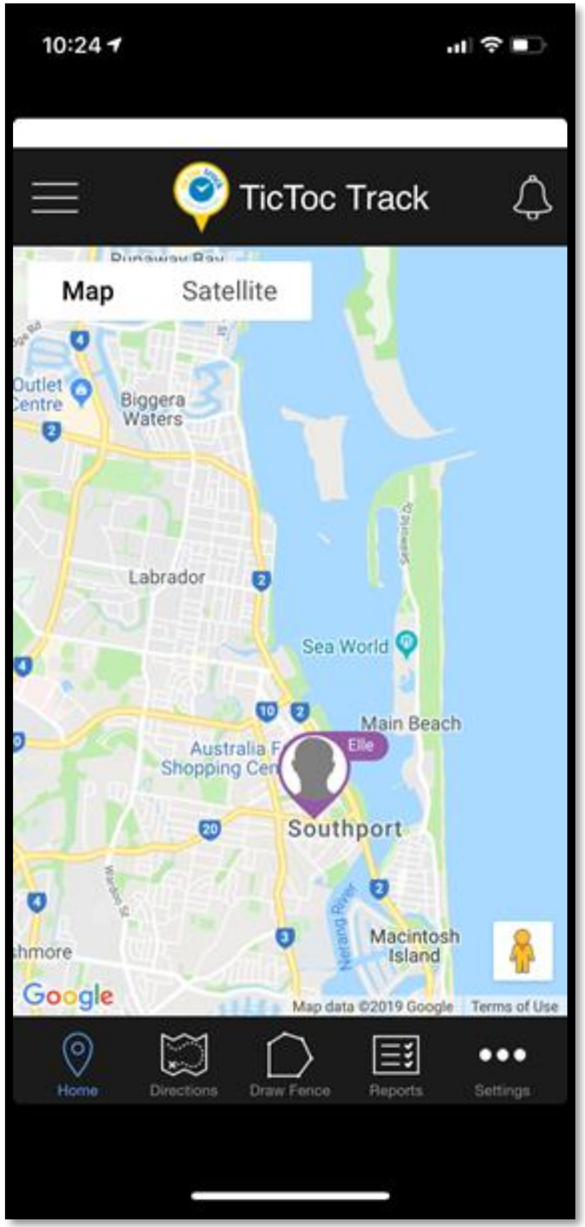
But worst, anyone can spy on the child silently

Systemic: affects around 3 million watches, multiple brands
Same API

GPS position

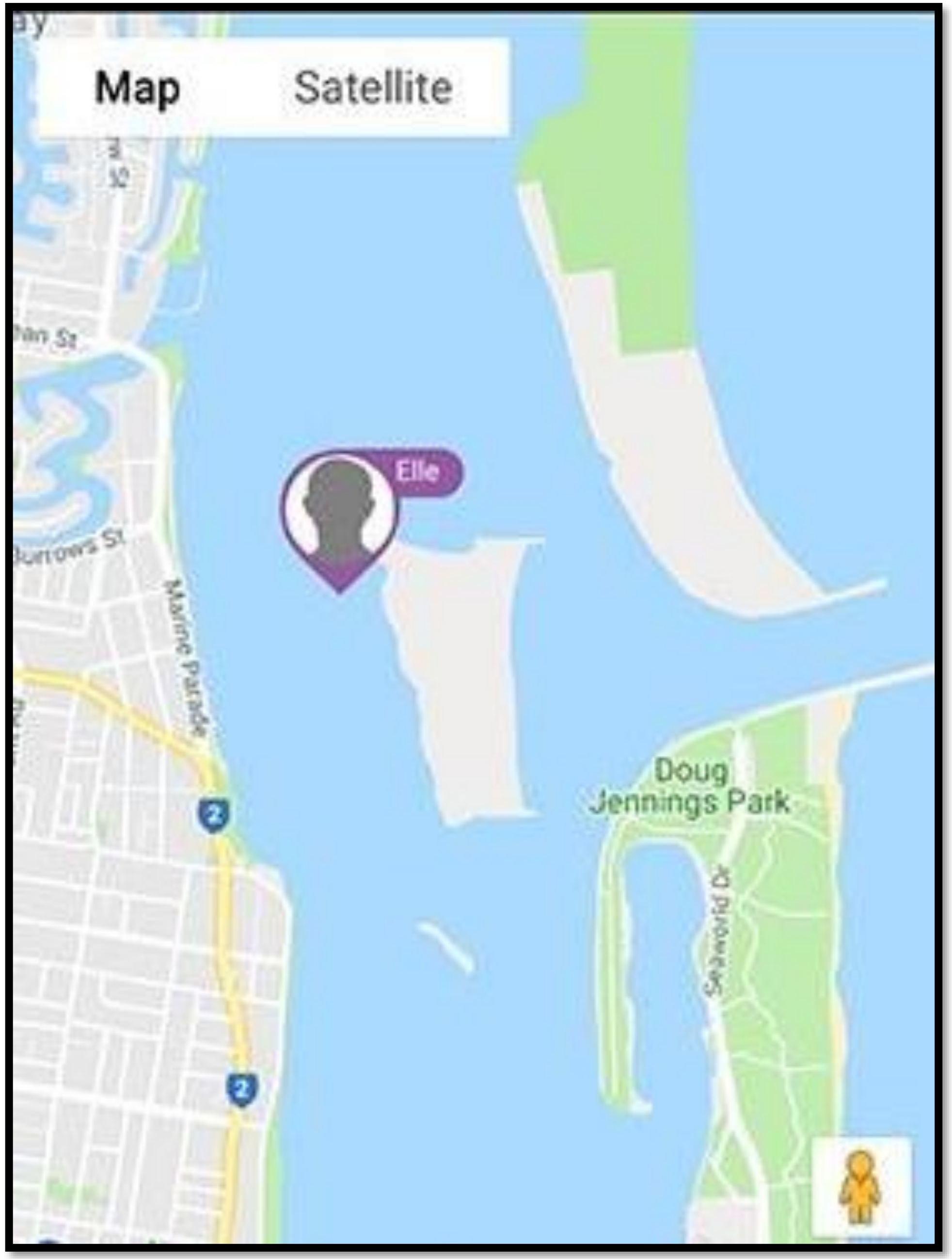
Then we change it

```
"odata.type":
"Nibaya.CsApi.GPS.DataLayer.BusinessLogic.Dto.NewestLocationDto",
"odata.id":
"https://tracker.tictoctrack.com/api/NewestLocations('34XX%7Cxxxxx
xx')",
"Family@odata.navigationLinkUrl":
"https://tracker.tictoctrack.com/api/NewestLocations('34X%7Cxxxxxx
')/Family",
"FamilyDevice@odata.navigationLinkUrl":
"https://tracker.tictoctrack.com/api/NewestLocations('34XX%7Cxxxxx
x')/FamilyDevice",
"Recorded@odata.type": "Edm.DateTime",
"Recorded": "2019-04-10T06:38:00",
"DeviceTerminalID": "xxxxxxx",
"DeviceTime@odata.type": "Edm.DateTime",
"DeviceTime": "2019-04-10T16:38:00",
"Latitude@odata.type": "Edm.Decimal",
"Latitude": "-27.XXXXXXX",
"Longitude@odata.type": "Edm.Decimal",
"Longitude": "153.XXXXXXX",
"Speed@odata.type": "Edm.Decimal",
"Speed": "0.000",
```



Time for a swim

Then we change it



Stealing your Car

Car theft trackers

Car stolen, GPS reports position using SIM

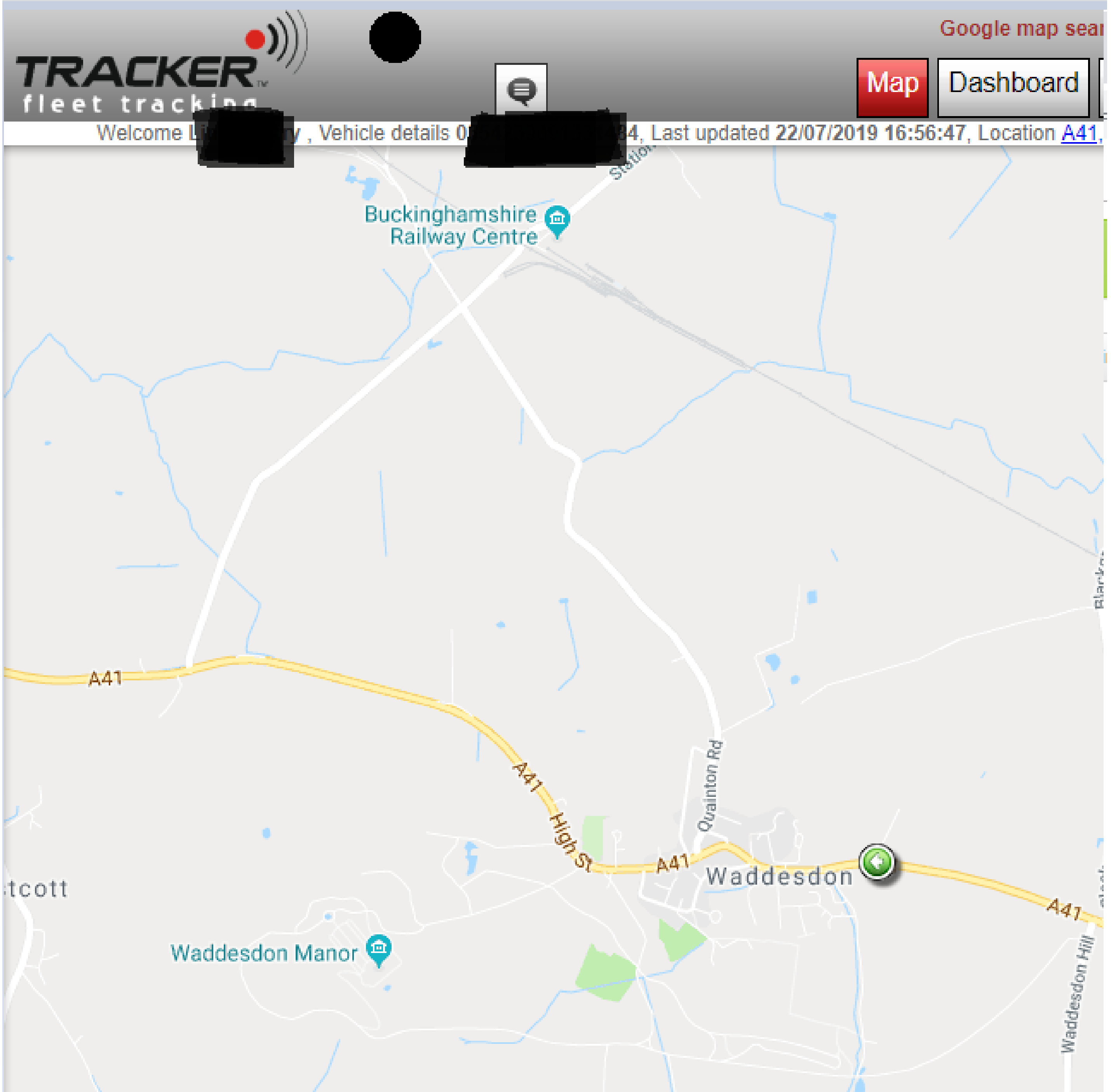
Geo-fence busted

Car alerts monitoring center

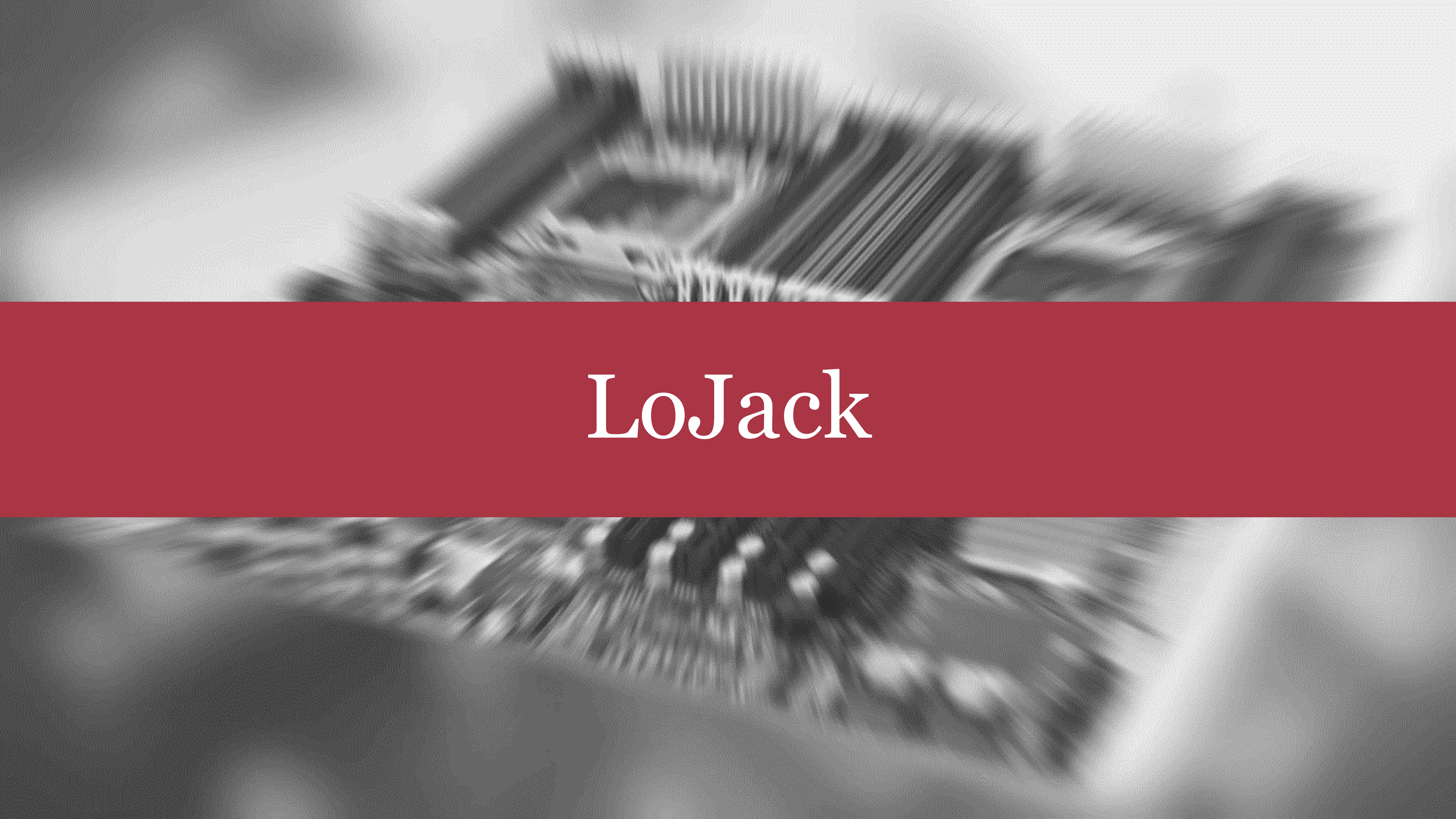
Triggers alert to driver by SMS, email & call

Cops alerted, GPS position shared

Recover vehicle



Welcome Li [redacted] y , Vehicle details 0 [redacted] 4, Last updated 22/07/2019 16:56:47, Location A41,



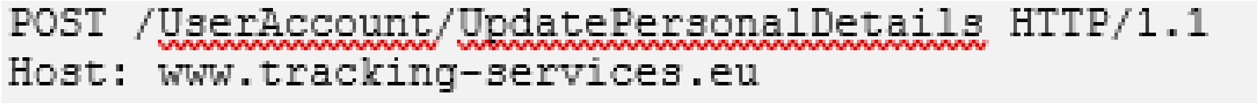
LoJack

IDORs, IDORs everywhere

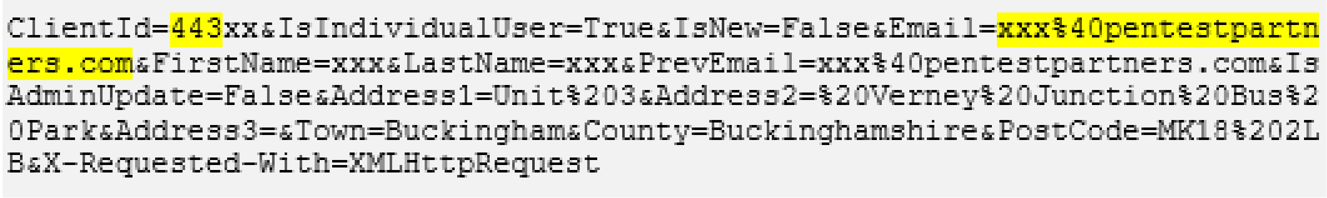
Change account email address

Trigger ‘forgot password’

Take control of account



```
POST /UserAccount/UpdatePersonalDetails HTTP/1.1
Host: www.tracking-services.eu
```

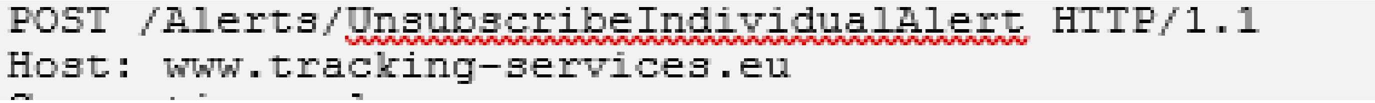


```
ClientId=443xx&IsIndividualUser=True&IsNew=False&Email=xxx%40pentestpartn
ers.com&FirstName=xxx&LastName=xxx&PrevEmail=xxx%40pentestpartners.com&Is
AdminUpdate=False&Address1=Unit%203&Address2=%20Verney%20Junction%20Bus%2
0Park&Address3=&Town=Buckingham&County=Buckinghamshire&PostCode=MK18%202L
B&X-Requested-With=XMLHttpRequest
```

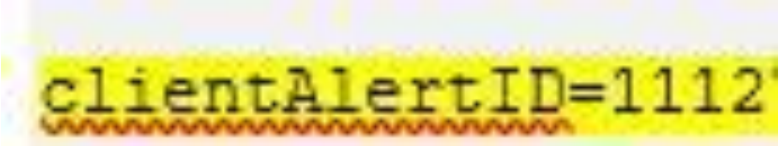
IDORs, IDORs everywhere

IDOR 2:

Delete theft alerts individually



```
POST /Alerts/UnsubscribeIndividualAlert HTTP/1.1
Host: www.tracking-services.eu
```



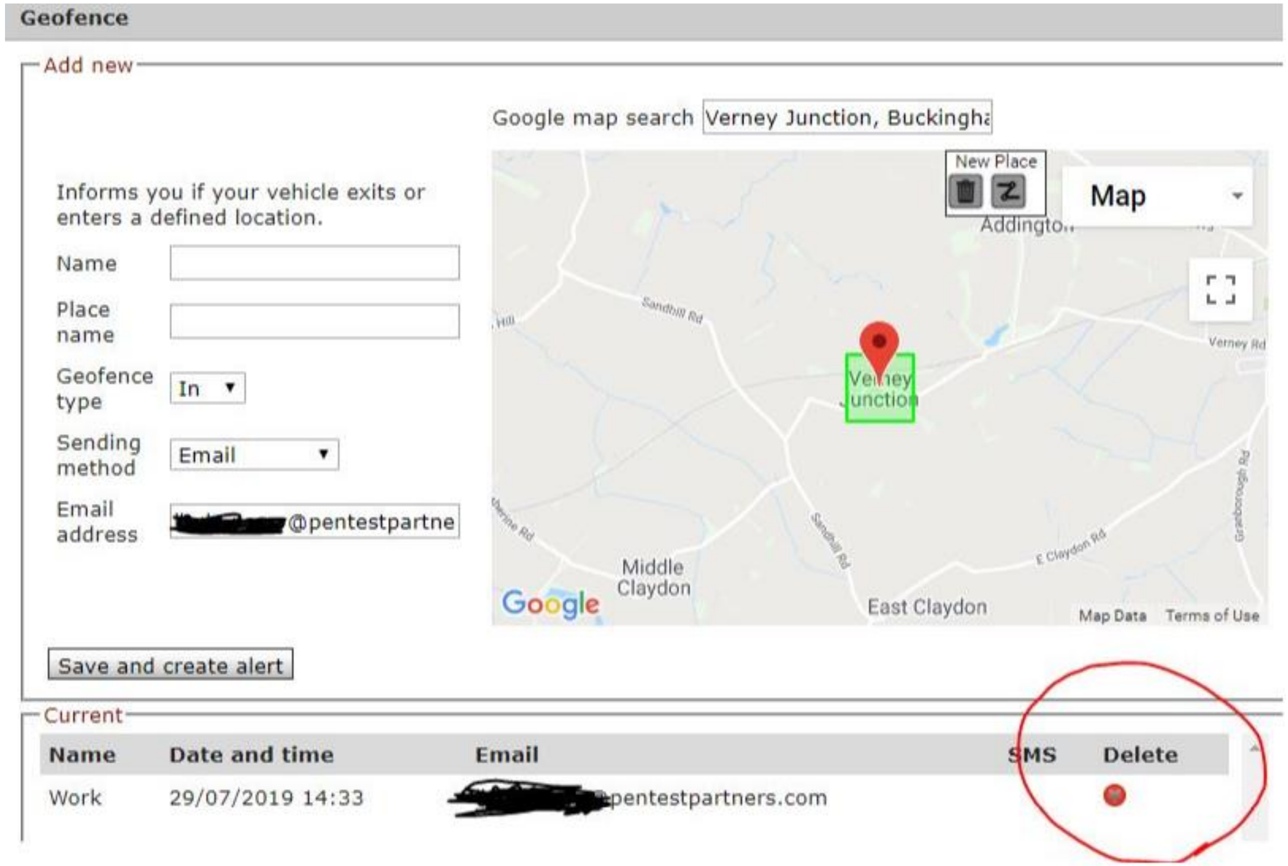
```
clientAlertID=1112
```

IDORs, IDORs everywhere

IDOR 3:

Or delete geo-fences

Either directly via API IDOR, or manually from the web app



Geofence

Add new

Informs you if your vehicle exits or enters a defined location.

Name	
Place name	
Geofence type	In ▾
Sending method	Email ▾
Email address	[redacted]@pentestpartne

Google map search: Verney Junction, Buckinghz

Save and create alert

Current

Name	Date and time	Email	SMS	Delete
Work	29/07/2019 14:33	[redacted]pentestpartners.com		●

New Laws around IoT

EU / ENISA

Some good progress in the EU

Good guidance & a move towards a certification framework

BUT, not mandatory & regulation perhaps not until 2023

enisa

Good Practices for Security of Internet of Things

in the context of Smart Manufacturing

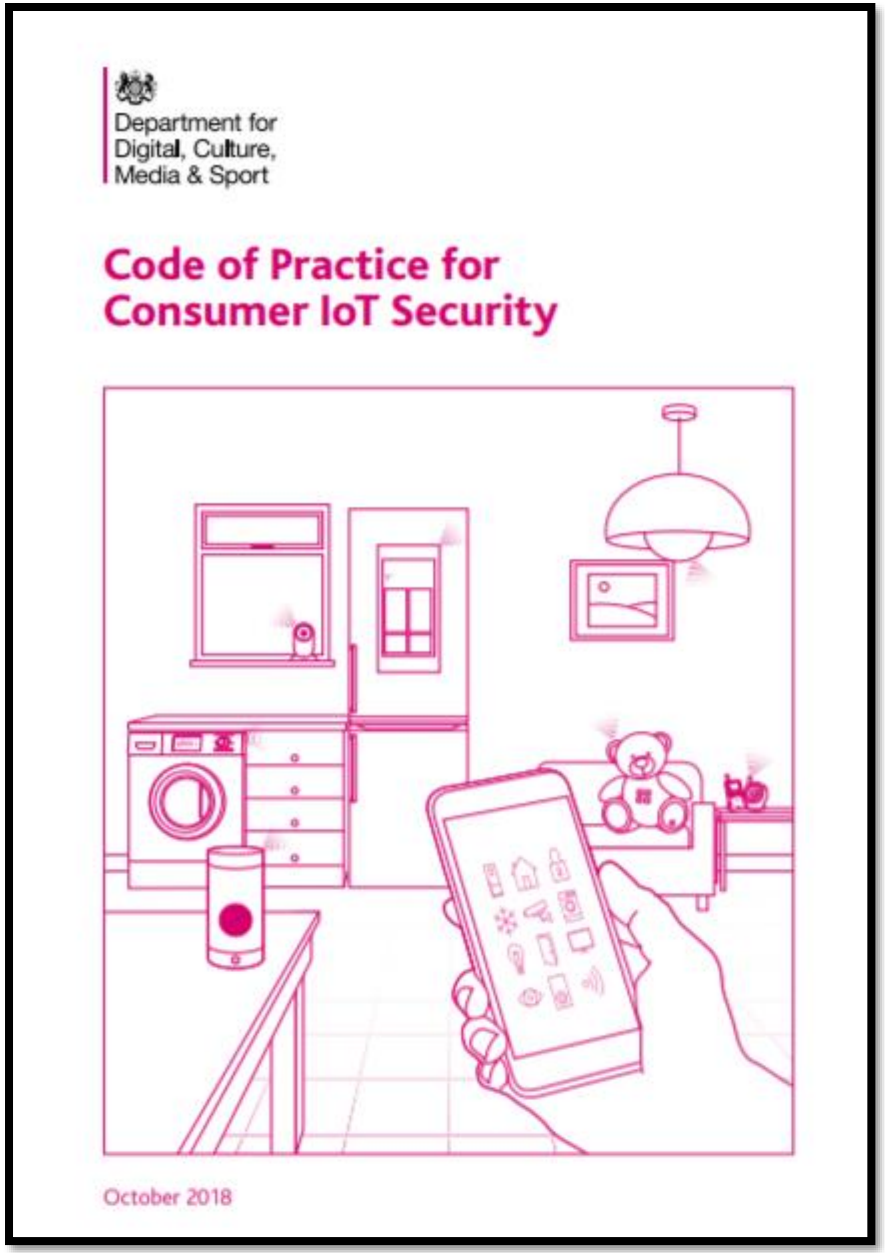
NOVEMBER 2018

UK IoT Security Code of Conduct

Has taken a different direction, which I support

Simple approach, to ensure basics are covered by IoT vendors

Regulation pending this year



Department for
Digital, Culture,
Media & Sport

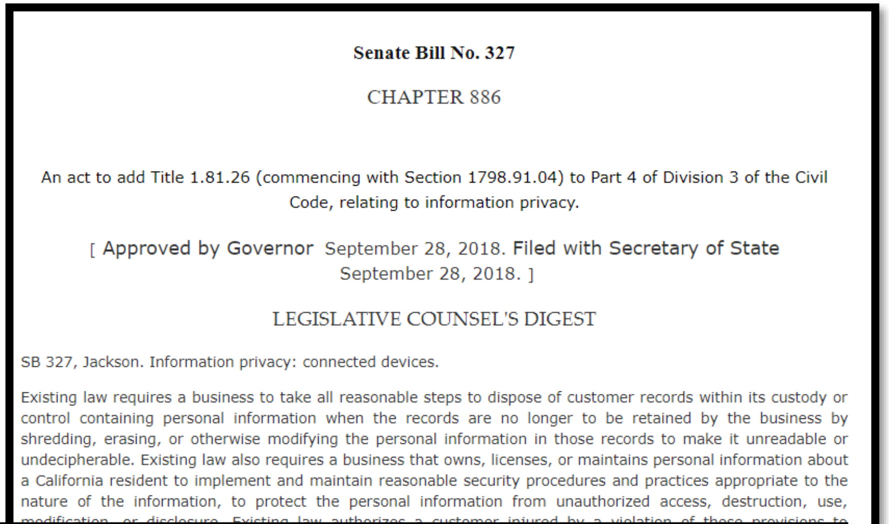
Code of Practice for
Consumer IoT Security

October 2018

California Senate Bill 327

Cited My Friend Cayla

Made ‘reasonable security features’ mandatory from Jan 1 2020



Senate Bill No. 327

CHAPTER 886

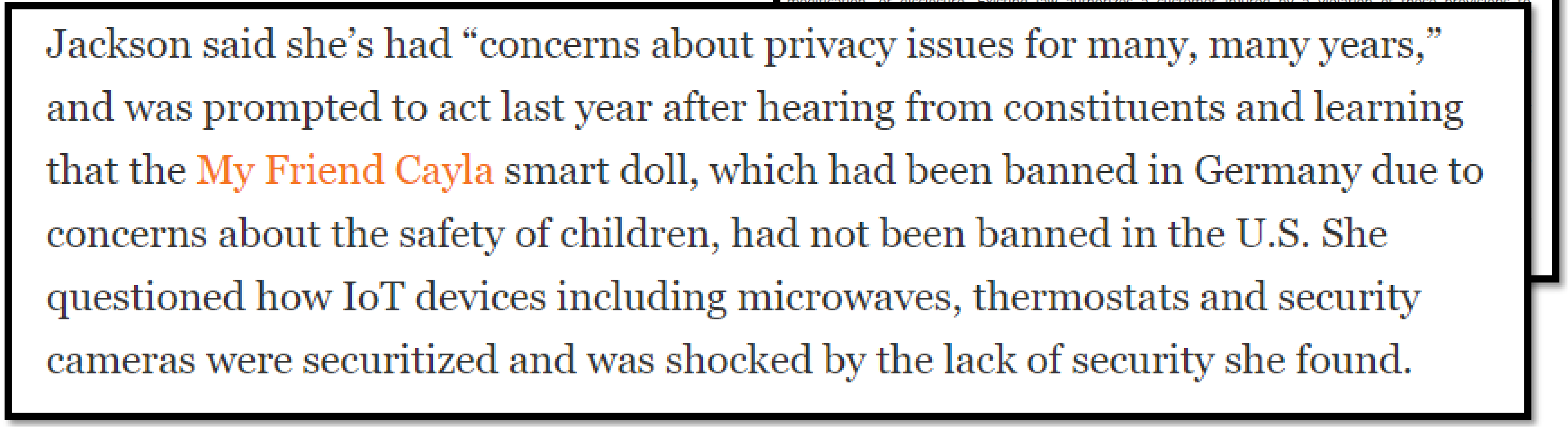
An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to



Jackson said she’s had “concerns about privacy issues for many, many years,” and was prompted to act last year after hearing from constituents and learning that the My Friend Cayla smart doll, which had been banned in Germany due to concerns about the safety of children, had not been banned in the U.S. She questioned how IoT devices including microwaves, thermostats and security cameras were securitized and was shocked by the lack of security she found.

@thekenmunroshow

@pentestpartners

LinkedIn: Ken Munro + cyber

Blog: www.pentestpartners.com

Pen testers: CBEST, STAR-FS, GBEST, CREST, CHECK