RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: MBS-R03

# Fixing the mess of IoT security:

# Sticking plaster over systemic flaws

**Ken Munro**

Partner
Pen Test Partners
@TheKenMunroShow

#RSAC

# Who am I?

An IoT security researcher & penetration tester

Part of a team of >80 who carry out extensive research in to IoT, card payments, ATM & automotive security at @pentestpartners

Known for public research in to hacking vehicle security, Samsung smart TVs, smart fridges, smart kids toys and much more…

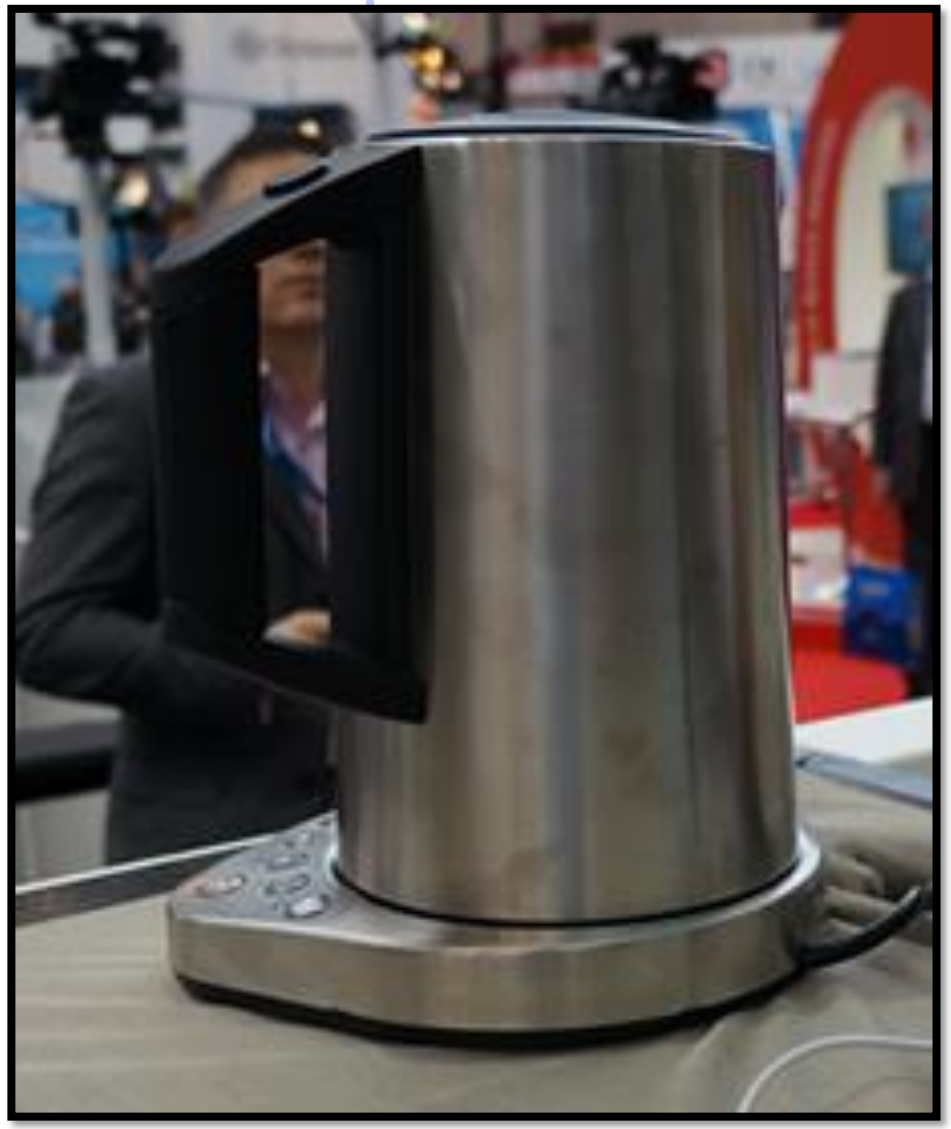
# First, some tea…

# A Wi-Fi tea kettle

A Wi-Fi enabled tea kettle, essential for every home

Comes with mobile app, from which kettle can be boiled

Offers stunning time saving, at a $100 premium over a regular non-smart kettle

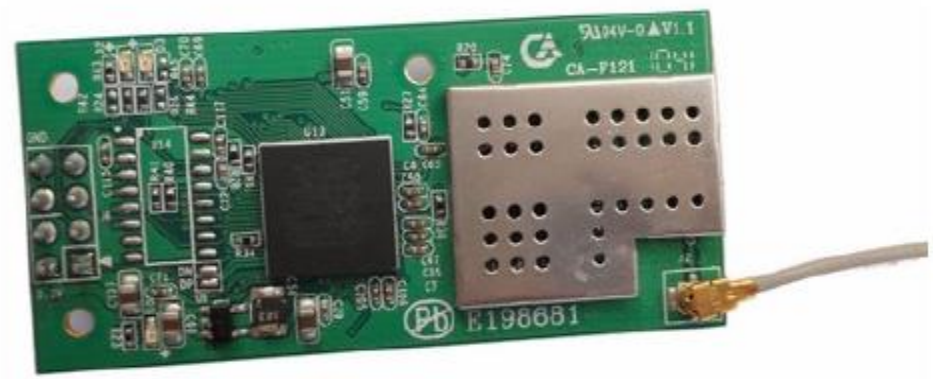


# How to hack a kettle


READ THE MANUAL!

# UART WIFI TRANSPARENT MODULE





### 4.3.7 System parameters

4.3.7.1 System password

Table 4-34 System password

| Parameter name | Parameter | Correlative Command |
|---|---|---|
| System password | Login Password | AT+PASS |
| Description | | |
| The login password for accessing the module through WEB server or wireless configuration.<br>The default setting of system is “000000” . | | |

4.3.7.2 WEB server

6.2.4.6 AT+KEY

**Function:**

Set or query network key. What should br noted is that,before using this command to set network key,user must set the encryption mode with the command AT+ENCRY .

**Format:**

AT+KEY=*[!?][format],[index],[key]*<CR>

+OK*[=format,index,key]*<CR><LF><CR><LF>

# Disclosure

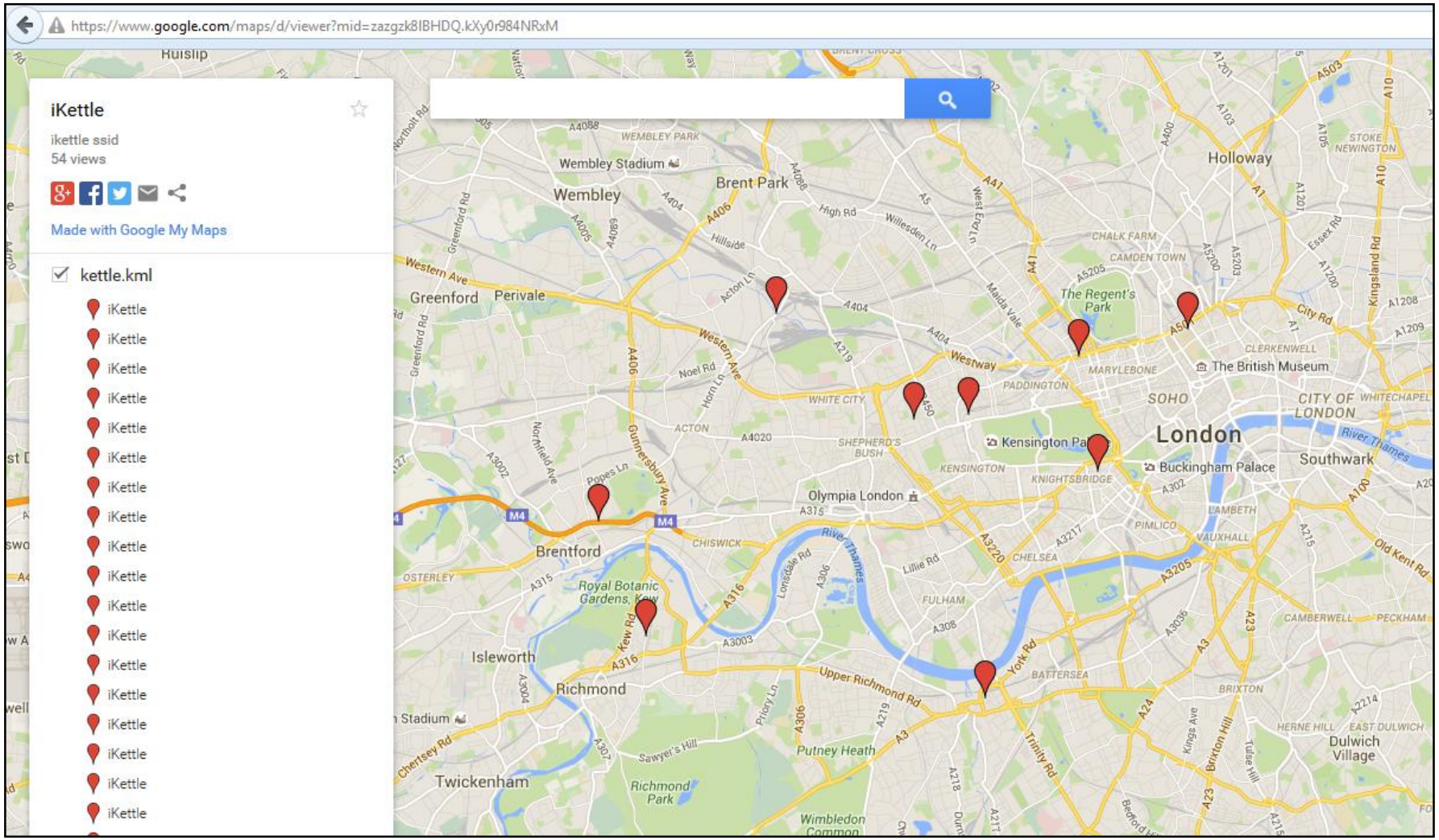
"It's OK" said the manufacturer

…the hack requires specialist knowledge and one would have to be very lucky to find a user with an iKettle

# Wi-Fi is trackable

Find kettles with

https://wigle.net



# iKettle v3.0

Much more secure now. Why?

Because the vendor hired in-house security expertise and outsourced the back end platform provision

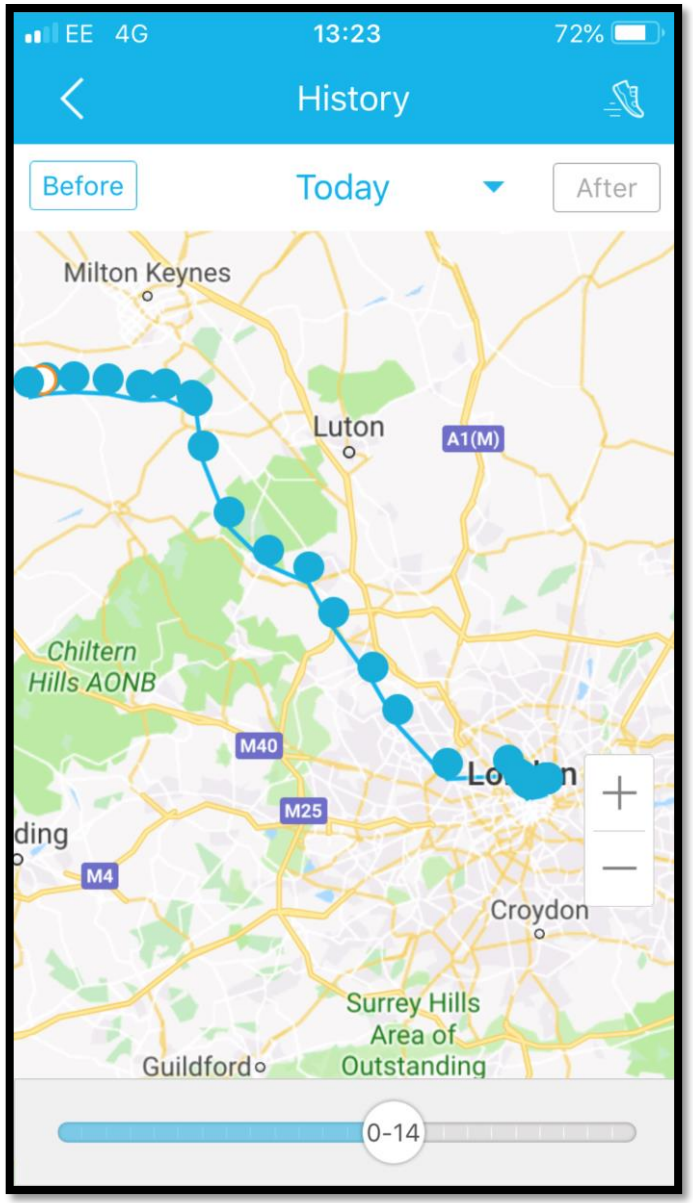
**Stalking your children:**

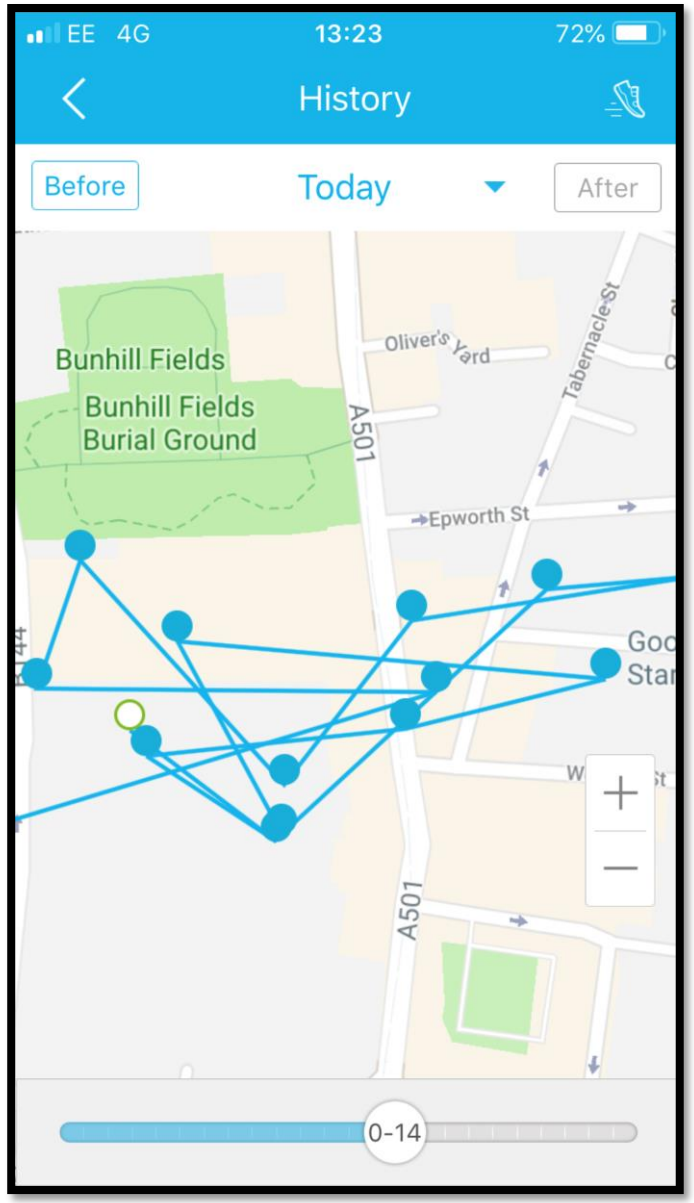
**IoT security issues become systemic**

**The problems are accelerating**


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

# Another smart watch exposing systemic flaws

Icelandic data protection authority found issues in Enox smart watch, issued immediate ban and used EU RAPEX notification to highlight ban across Europe

We went back to our earlier research:

Enox watch uses API from thinkrace, Chinese ODM

Systemic: API connects to 7 million tracking devices, 367 different device types

RSAConference2019

# Remote listening


I’m listening to your child
**** You!

# Hacking Cayla

**Evil phone, modified app**

**Tamper with anti-swearing process**

**No Bluetooth PIN**

Voice recognition

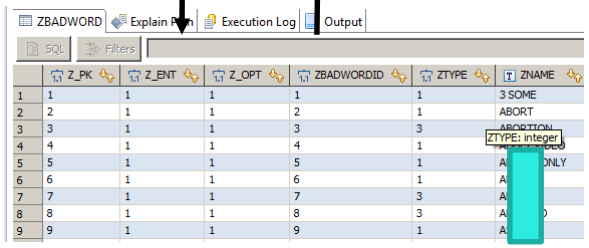
MITM

Wikipedia API

**API call broken when Wikipedia enforced SSL!**

**Modify unencrypted data in transit**

Evil API



Local Q database + ‘badwords’

# Vendor updates the app

Our attack stopped working a while back, after the application was finally updated

They ‘fixed’ it by encrypting the database contents with SQLcipher

```
public DatabaseHelper(Context paramContext)
{
  super(paramContext, paramContext.getDatabasePath("cayla.cd").getAbsolutePath(), null, 4, (File)null, "DJKNTIVtVAf7geQOVOfyCw==");
  DatabaseInitializer localDatabaseInitializer = new DatabaseInitializer(paramContext, "cayla.cd");
  try
  {
    localDatabaseInitializer.createDatabase();
    localDatabaseInitializer.close();
    return;
  }
```

```
"DJKNTIVtVAf7geQOVOfyCw==");
```

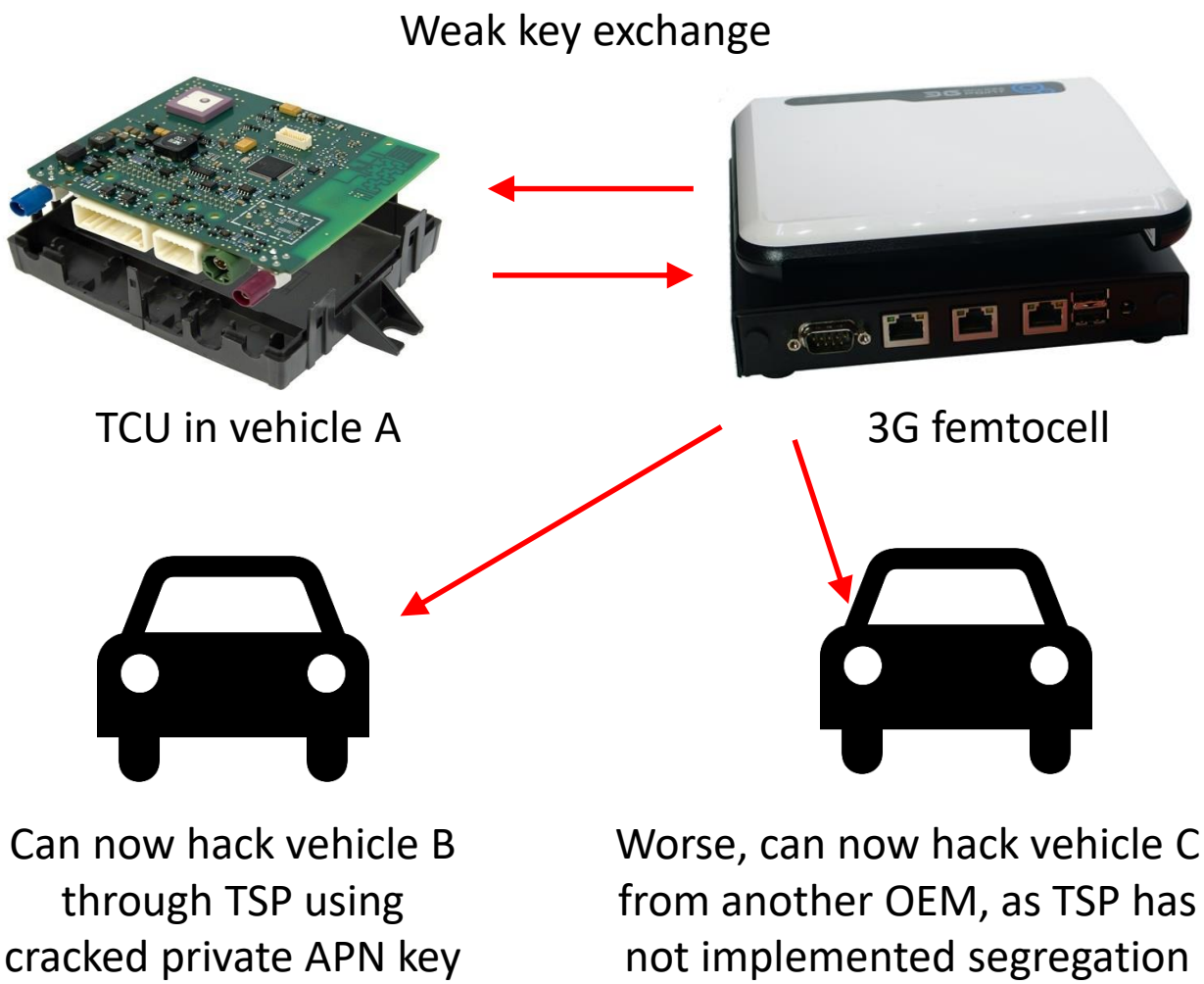
Ignoring the issues that actually mattered

RSAConference2019

# Smart vehicle security:

# More systemic flaws

# Vehicle telematic service platforms - TSPs




Private APNs used for cellular communications with vehicle TCUs over TSPs

We found the GSM authentication mechanism & found it to be surprisingly weak

The private APN key is hashed with MD5, as specified by RFC1994 (PPP CHAP), so keys <12 chars in length are trivially cracked

Some telematics service platforms had not implemented vehicle-vehicle segregation

OR EVEN OEM-OEM SEGREGATION

# Vehicle telematic service platforms - TSPs

14-02-2019 10:53:32.39212154 QoS 0


```
        "BIN": "123",
        "TimeStamp": "2019-02-14T10:53:31Z",
        "CorrelationId": "2d43b6cb-cf15-46d7-b405-1f9852134129",
        "DCMVersion": "1.4.3.5"
    },
    "ApplicationData": {
        "TS": "2019-02-14T10:53:31Z",
        "rluac": "Lock",
        "rluop": "AllDoors",
        "rluop1": "NA"
    }
}
```


Found last week

Major TSP left MQTT endpoint on the public internet

Discovered via shodan

Flagged & fixed very quickly


```
<sms udpport="9003" udpaddress="10.221.13.127" channel="SMS" phonenum="88313026
  <SMSApplicationCommandMessage>
    <SMSAppCommand>
        <Header_IE>0</Header_IE>
            <Header_MFlag>0</Header_MFlag>
```

# Story breaks at 11pm tonight

Demonstrate how to hijack & steal ~3 million vehicles, worth ~$250Bn

Track you & your vehicles in real time

Unlock your car to order

And LISTEN silently to drivers conversations in ~2M vehicles

IoT security flaws are becoming systemic

RSAConference2019

# Mirai v1 was systemic, did anyone realise?

# What you thought Mirai v1 was

An IoT botnet affecting 300,000 printers, cameras, VoIP phones exploited in 2016

Then used to DDoS DNS provider to Facebook, Twitter etc

Except it wasn't

# Mirai v1 was…
# …a DVR botnet

# How people missed that Mirai v1 was systemic

QVIS DVR

Mezory DVR

Dreambox DVR/PVR

Realtek DVR

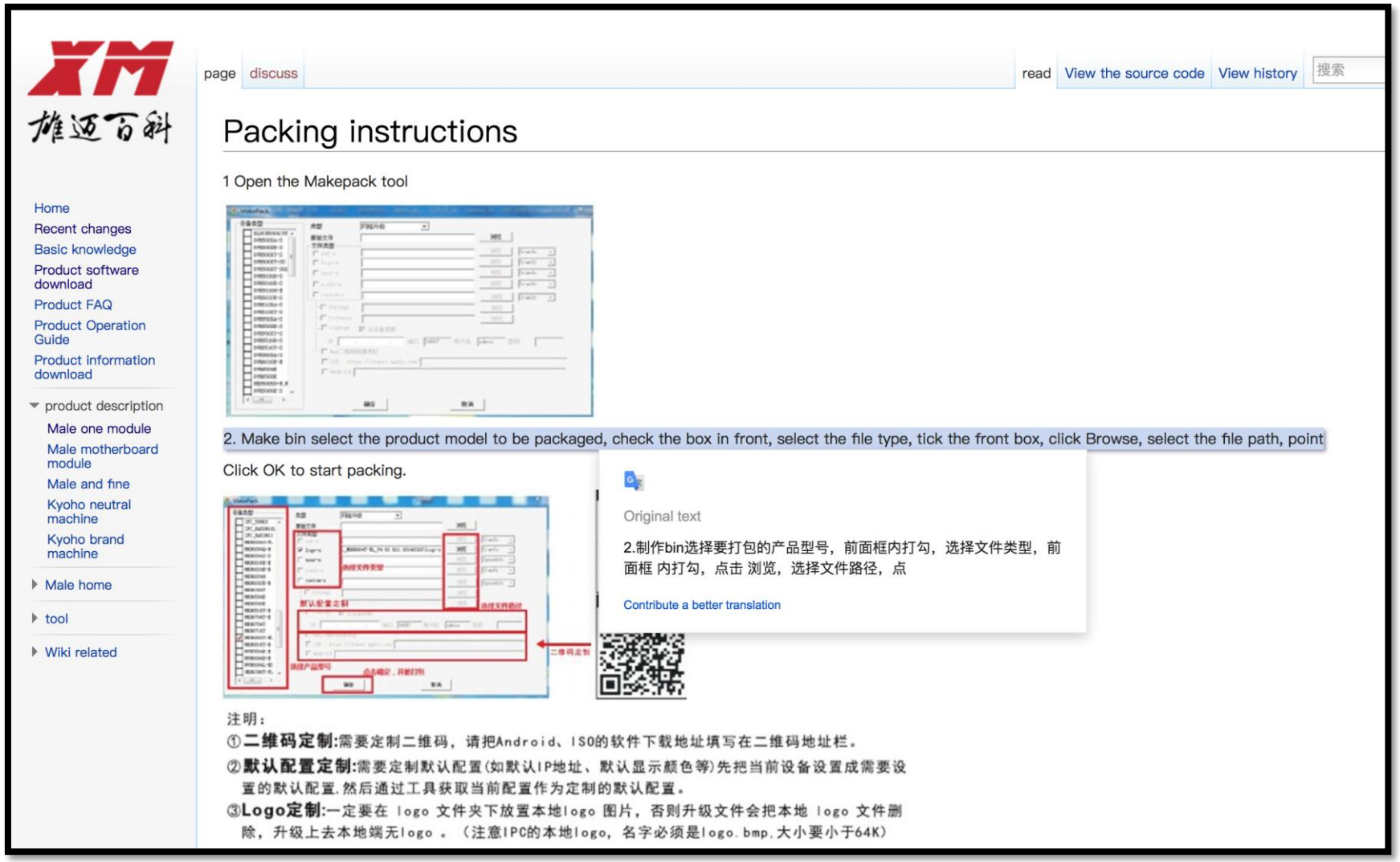
| Username/Password | Manufacturer | Link to supporting evidence |
|---|---|---|
| | | |
| admin/123456 | ACTi IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/anko | ANKO Products DVR | http://www.cctvforum.com/viewtopic.php?f=3&t=44250 |
| root/pass | Axis IP Camera, et. al | http://www.cleancss.com/router-default/Axis/0543-001 |
| root/vizxv | Dahua Camera | http://www.cam-it.org/index.php?topic=5192.0 |
| root/888888 | Dahua DVR | http://www.cam-it.org/index.php?topic=5035.0 |
| root/666666 | Dahua DVR | http://www.cam-it.org/index.php?topic=5035.0 |
| root/7ujMko0vizxv | Dahua IP Camera | http://www.cam-it.org/index.php?topic=9396.0 |
| root/7ujMko0admin | Dahua IP Camera | http://www.cam-it.org/index.php?topic=9396.0 |
| 666666/666666 | Dahua IP Camera | http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C |
| root/dreambox | Dreambox TV receiver | https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/ |
| root/zlxx | EV ZLX Two-way Speaker? | ? |
| root/juantech | Guangzhou Juan Optical | https://news.ycombinator.com/item?id=11114012 |
| root/xc3511 | H.264 - Chinese DVR | http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15 |
| root/hi3518 | HiSilicon IP Camera | https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/ |
| root/klv123 | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/klv1234 | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/jvbzd | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/admin | IPX-DDK Network Camera | http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/ |
| root/system | IQinVision Cameras, et. al | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| admin/meinsm | Mobotix Network Camera | http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/ |
| root/54321 | Packet8 VOIP Phone, et. al | http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411 |
| root/00000000 | Panasonic Printer | https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html |
| root/realtek | RealTek Routers | |
| admin/1111111 | Samsung IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/xmhdipc | Shenzhen Anran Security Camera | https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI |
| admin/smcadmin | SMC Routers | http://www.cleancss.com/router-default/SMC/ROUTER |
| root/ikwb | Toshiba Network Camera | http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en |
| ubnt/ubnt | Ubiquiti AirOS Router | http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm |
| supervisor/supervisor | VideoIQ | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/<none> | Vivotek IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| admin/1111 | Xerox printers, et. al | https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/ |
| root/Zte521 | ZTE Router | http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html |

It was all one vendor of DVR firmware:

XiongMai

Makepack allowed ODMs to customize per-brand

Including several code execution flaws that we found, never used by Mirai



# Swann camera


Access anyone's video stream

Fixed now, fortunately

Authorisation flaws on the API

Transpired to be a problem with back end provider, affected multiple brands and millions of cameras

IoT security flaws are becoming systemic

RSAConference2019

# Hacking your hot tub…

## We pwned a smart hot tub for Xmas 2018

## Did this really matter?

Yes

Why?

Back end service provision

Lack of authorisation didn't just affect hot tubs

It affects trucks, cars, medtech and more

RSAConference2019

# Fixing this mess

# Advice for IoT vendors

Systemic flaws arise from, for example

Lack of API authorisation (IDOR)

Hard coded back doors

Remote Code Execution

Default credentials on published services

Missing client segregation

# Advice for IoT vendors

If you outsource your back end service provision, you need certainty that their security is robust

Marketing claims are no substitute for reality

“How do you verify & prove that users are correctly authorised?”

Work through the OWASP Top 10 if you like

RSAConference2019

# Advice for businesses using IoT

# Find out who looks after the security of your:

Building management system

Door access controllers

Gatelines

CCTV

Lift control system

Industrial controls

Room booking system

Smart TVs, media casters

Drinks machines

Fridges

**If you don't ask for security, you won't get it**

# The stick

# EU / ENISA

Some good progress in the EU

Good guidance & a move towards a certification framework

BUT, not mandatory & regulation perhaps not until 2023

# UK IoT Security Code of Conduct

Has taken a different direction, which I support

Simple approach, to ensure basics are covered by IoT vendors

Whilst not mandatory, regulation is in discussion. Potential for 2020?


Department for Digital, Culture, Media & Sport

Code of Practice for Consumer IoT Security

October 2018

# California State Bill 327

Cited My Friend Cayla

Makes reasonable security features mandatory from Jan 1 2020

Open to interpretation, but a huge step forward

**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 institute a civil action to recover damages.

This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.

This bill would become operative only if AB 1906 of the 2017–18 Regular Session is enacted and becomes effective.

Vote: majority Appropriation: no Fiscal Committee: yes Local Program: no

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

# Legal cases

Several products banned in Germany for telecommunications law violations

Several banned in other countries for DPA violations

Several class action suits for excessive data collection, in breach of vendors own terms!

# If we don’t address this now, systemic flaws will accelerate further

# Thank you

@TheKenMunroShow

@PenTestPartners

LinkedIn: Ken Munro + cyber

Blog: www.pentestpartners.com/blog/

Penetration testers of IT, OT, IoT, vehicles, planes, trains, ships and ATMs