PCI Security Standards Council

Has IoT Security Improved?

Or Is It Still Down The (Smart) Toilet

PCI Security Standards Council

Ken Munro

CEO
Pen Test Partners

PEN TEST PARTNERS

PCI Security Standards Council

Back to the Beginning

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?

PCI Security Standards Council

But That Was 8 Years Ago

Surely things have improved?


Is your mom at home?
CLICHÉD H4XOR

PCI Security Standards Council

Fails Are Evolving

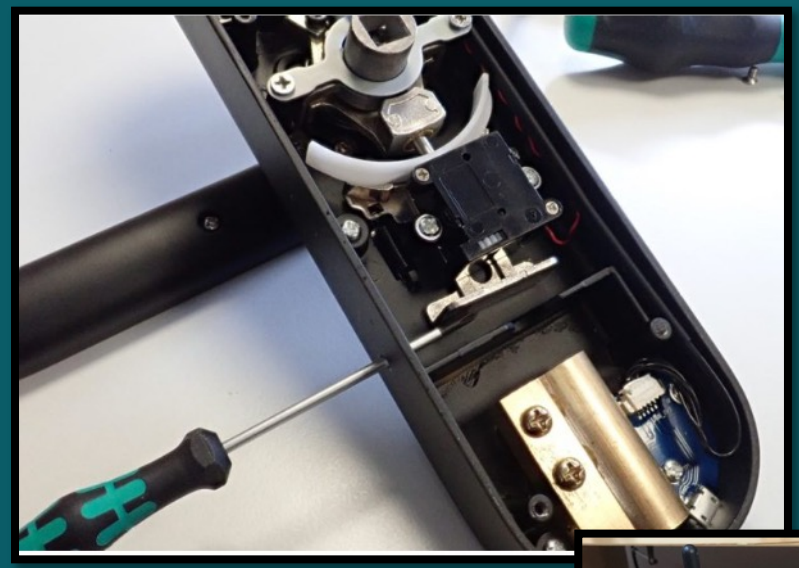
Historically, API flaws

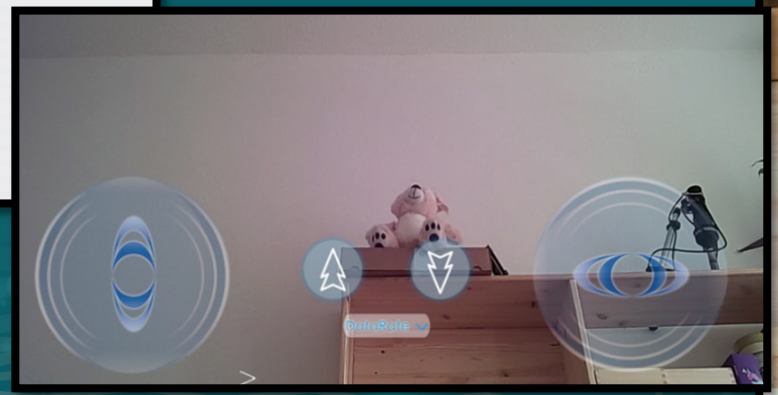
- API authorisation fails *were* our greatest concern
- Take out ALL the devices, owing to a platform authorisation failure
- Fully remote attacks against the entire installed base of users
- Still an issue, but IoT vendors increasingly moving to platforms where API cyber security is harder to get wrong!
- More attention to developers getting it right
- Regulation starting to focus vendor attention

PCI Security Standards Council

Changing Focus

Local, Exploitable Security Flaws





PCI Security Standards Council

Local, Exploitable Security Flaws

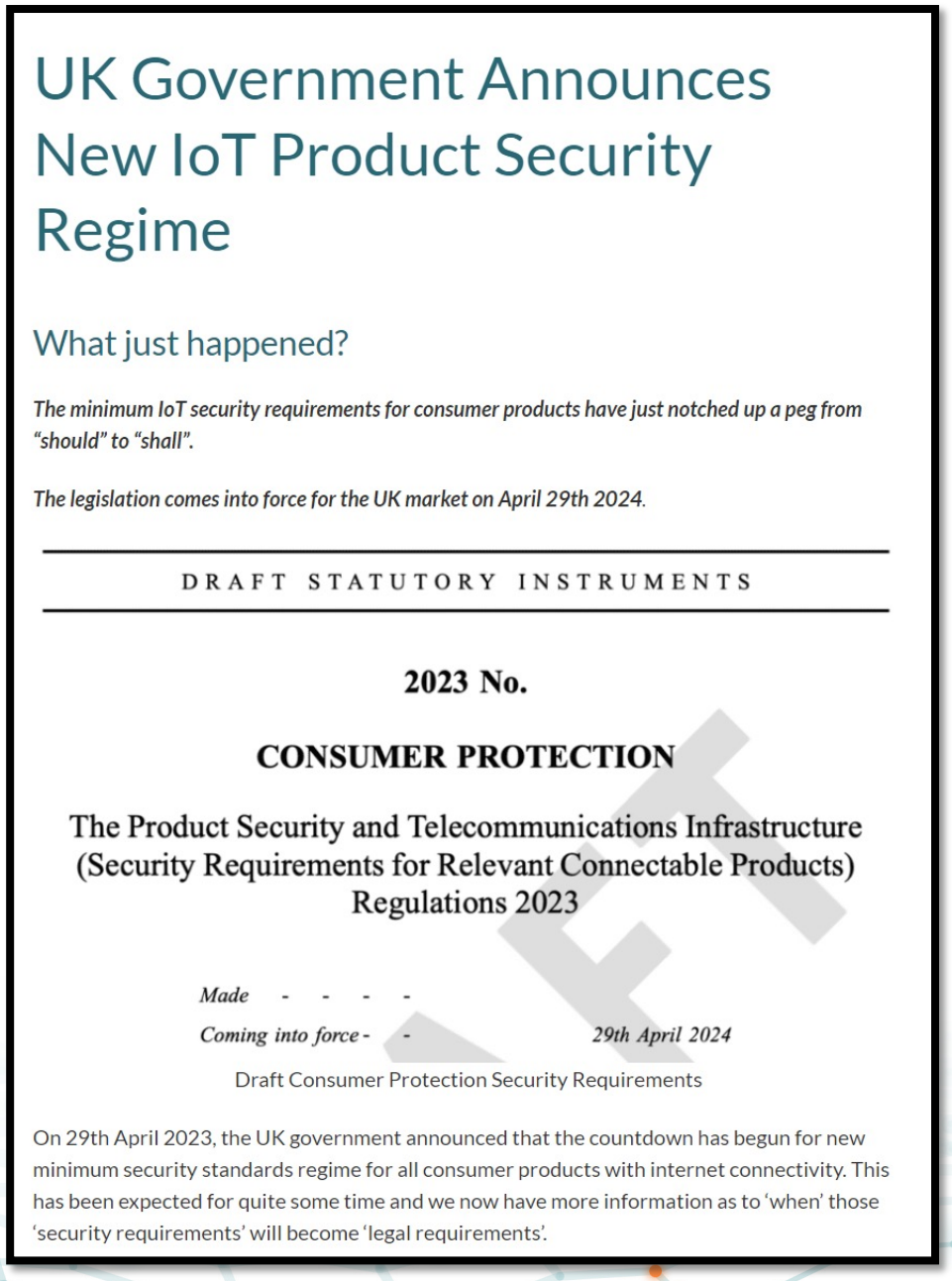

```
                break;
            case w.SONOFABITCH:
                r = function() {
                    for (var a = screen.width, t
                        var l = Math.round(Math.
                        for (c + l > t && (l = t
                            var g;
                          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

```
                trace("Receive err
                break;
            default:
                trace("unhandled SSL shit status"), r.scheduleReconnect()
        }
    },
    scheduleReconnectCallback = function() {
```

Barriers to Market Entry Are Emerging

Market Cyber Barriers

- Current regs are fairly ‘light touch’ but will develop
- UK PSTI principles:
  - No default / blank passwords
  - Statement / commitment to product security updates at point of sale
  - Vulnerability disclosure program
- Significant fines for non-compliance
- IoT Cybersecurity Improvement Act also creates barriers to US Federal markets



UK Government Announces New IoT Product Security Regime

What just happened?

The minimum IoT security requirements for consumer products have just notched up a peg from “should” to “shall”.

The legislation comes into force for the UK market on April 29th 2024.

DRAFT STATUTORY INSTRUMENTS

2023 No.

CONSUMER PROTECTION

The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023

Made - - - -

Coming into force - - 29th April 2024

Draft Consumer Protection Security Requirements

On 29th April 2023, the UK government announced that the countdown has begun for new minimum security standards regime for all consumer products with internet connectivity. This has been expected for quite some time and we now have more information as to ‘when’ those ‘security requirements’ will become ‘legal requirements’.

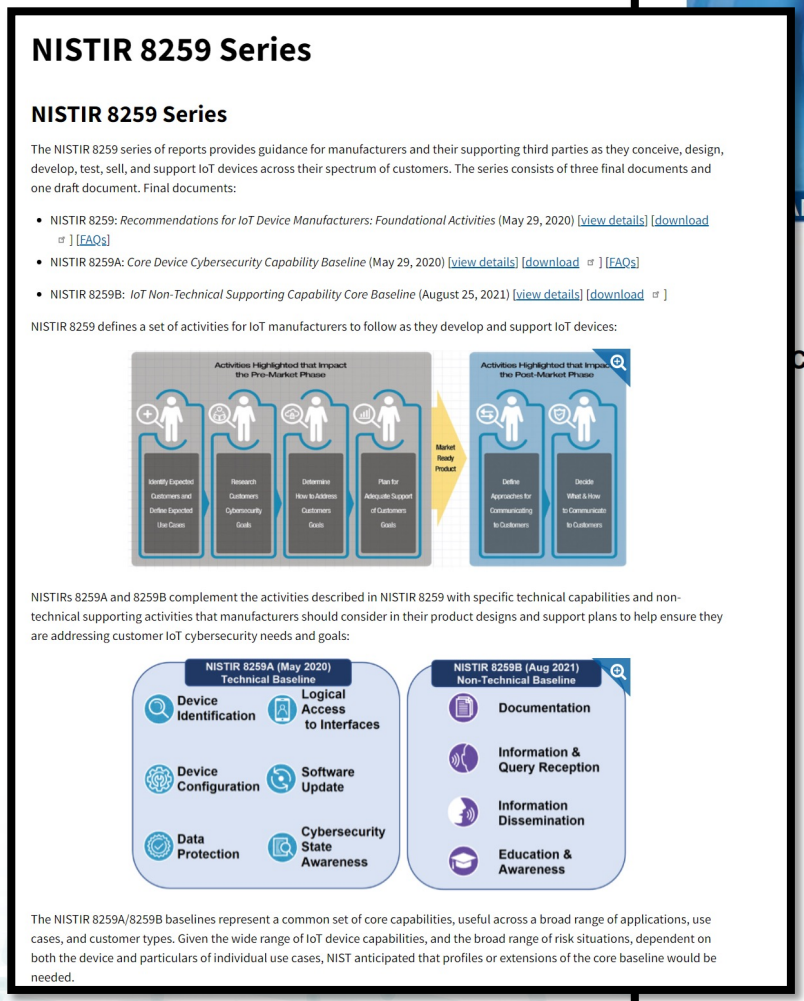
PCI Security Standards Council

PCI Security Standards Council

Standards Have a Lot In Common

Standards

- Challenge of standards compliance wasn't easy when there weren't standards!
- Frustrating for vendors when standards conflict or bring too high a burden of compliance
- EU Cybersecurity Act IoT compliance based on ETSI 303 645
- NIST labelling based on 8259



NISTIR 8259 Series

NISTIR 8259 Series

The NISTIR 8259 series of reports provides guidance for manufacturers and their supporting third parties as they conceive, design, develop, test, sell, and support IoT devices across their spectrum of customers. The series consists of three final documents and one draft document. Final documents:

- NISTIR 8259: *Recommendations for IoT Device Manufacturers: Foundational Activities* (May 29, 2020) [view details] [download] [FAQs]
- NISTIR 8259A: *Core Device Cybersecurity Capability Baseline* (May 29, 2020) [view details] [download] [FAQs]
- NISTIR 8259B: *IoT Non-Technical Supporting Capability Core Baseline* (August 25, 2021) [view details] [download]

NISTIR 8259 defines a set of activities for IoT manufacturers to follow as they develop and support IoT devices:

NISTIRs 8259A and 8259B complement the activities described in NISTIR 8259 with specific technical capabilities and non-technical supporting activities that manufacturers should consider in their product designs and support plans to help ensure they are addressing customer IoT cybersecurity needs and goals:

The NISTIR 8259A/8259B baselines represent a common set of core capabilities, useful across a broad range of applications, use cases, and customer types. Given the wide range of IoT device capabilities, and the broad range of risk situations, dependent on both the device and particulars of individual use cases, NIST anticipated that profiles or extensions of the core baseline would be needed.

ETSI EN 303 645 V2.1.1 (2020-06)

ETSI

N STANDARD

CYBER;
Cyber Security for Consumer Internet of Things:
Baseline Requirements

PCI Security Standards Council

PCI Security Standards Council®

‘Smart’ Green Technology is My Current Concern

Connected PV Inverters

- “Horus Scenario”
- EV charger research led to similar API issues with Solax PV inverters
- Also, Shenzen Growatt and many others
- Potential to take control of gigawatts of solar PV generation
- Switching on/off/on/off synchronously during times of peak demand will destabilize power grid

You Saw It in the Movies First

- Leave the World Behind
- Ships crashing - nah
- Planes crashing - nah
- Teslas crashing - maybe
- Power outages - perhaps

PCI Security Standards Council

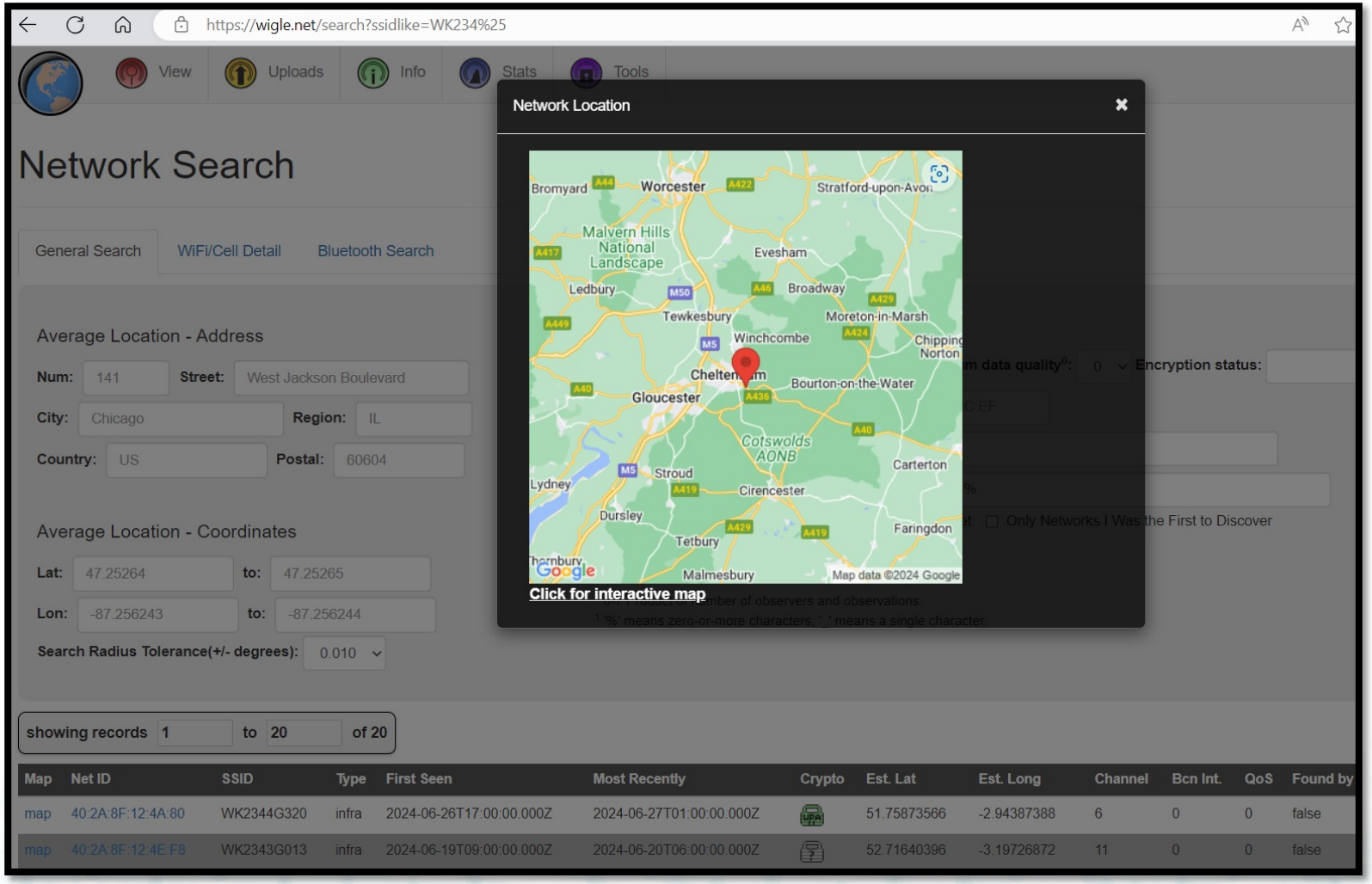
Smart Home Power Batteries

- Huge environmental benefits
- Absorb power at times of peak generation, dump it at times of peak demand
- Grid balancing opportunity
- The same rush to market as we saw with consumer IoT to gain first mover advantage
- Ripe for cyber mistakes
- Ultimate is V2G / V2H / H2V – using significant capacity of EV car battery

PCI Security Standards Council

Smart Home Power Batteries

- Our batteries at PTP
- Unusual Wi-Fi AP, default set as ‘12345678’
- Installers now encouraged to change it…
- … to the serial number
- Except the serial number is broadcast in the Wi-Fi SSID
- Syntax ‘WKxxxxxxx’



PCI Security Standards Council

Smart Home Power Batteries

- Easy to geo-locate batteries
- Web interface creds are admin/admin
- Battery is also a client on the customer's home network
- Home network PSK is stored in plain text on the router
- BACK DOOR!

PCI Security Standards Council®

Smart Home Power Batteries

- There’s an RJ45 port on the battery too
- Most installers pop in an ethernet cable if the customer’s home router is nearby
- BACK DOOR

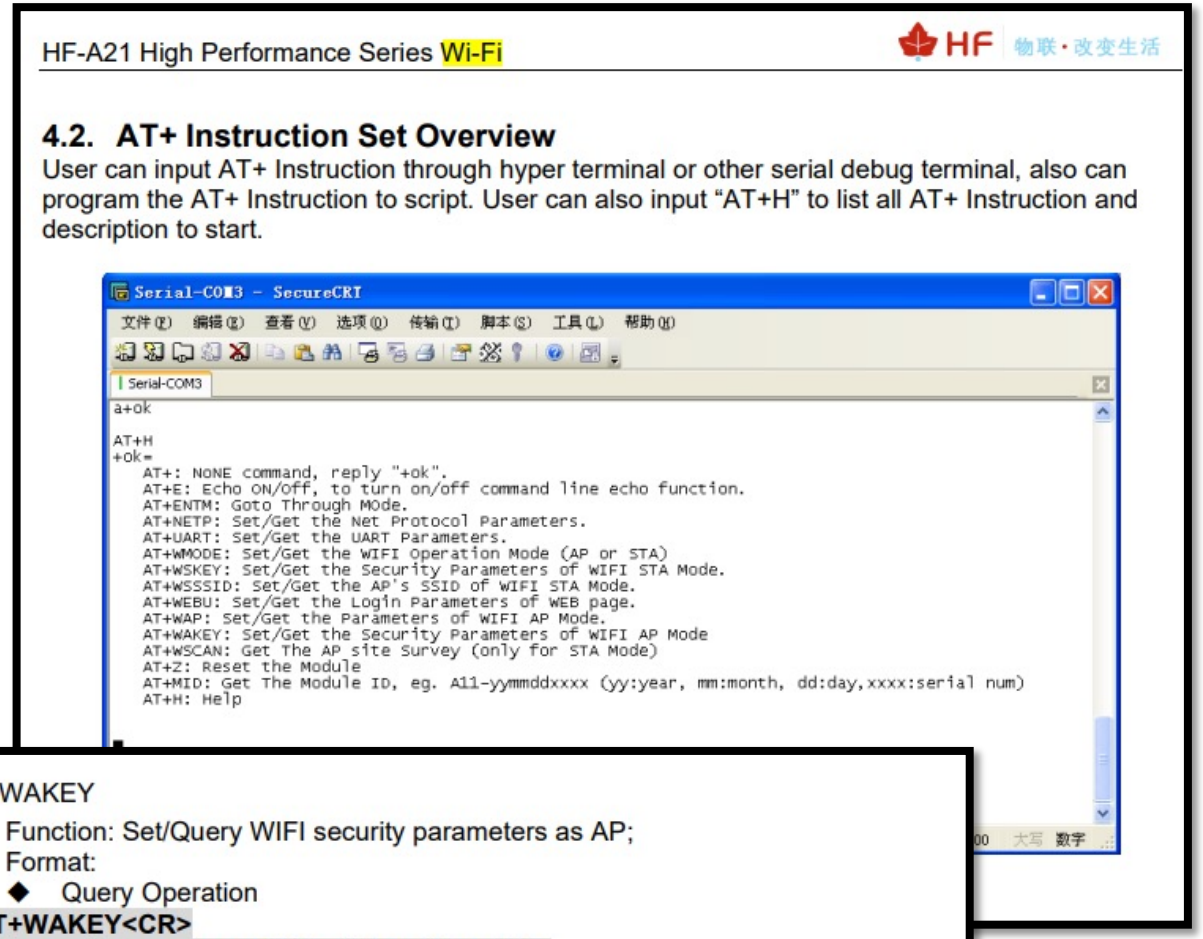
PCI Security Standards Council

Smart Home Power Batteries

- Once on the exposed Wi-Fi access point, TCP port 23 is exposed
- Does this sound familiar?
- Wi-Fi module is HF-A21-SMT
- Searching online reveals:

Smart Home Power Batteries

- AT command set support
- AT+WAKEY can be used to recover the PSK (wifi password) over the air from outside the house
- It's Groundhog Day



HF-A21 High Performance Series Wi-Fi

HF 物联·改变生活

4.2. AT+ Instruction Set Overview

User can input AT+ Instruction through hyper terminal or other serial debug terminal, also can program the AT+ Instruction to script. User can also input "AT+H" to list all AT+ Instruction and description to start.

Serial-COM3 - SecureCRT

文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)

Serial-COM3

```
a+ok

AT+H
+ok=
   AT+: NONE command, reply "+ok".
   AT+E: Echo ON/off, to turn on/off command line echo function.
   AT+ENTM: Goto Through Mode.
   AT+NETP: Set/Get the Net Protocol Parameters.
   AT+UART: Set/Get the UART Parameters.
   AT+WMODE: Set/Get the WIFI Operation Mode (AP or STA)
   AT+WSKEY: Set/Get the Security Parameters of WIFI STA Mode.
   AT+WSSSID: Set/Get the AP's SSID of WIFI STA Mode.
   AT+WEBU: Set/Get the Login Parameters of WEB page.
   AT+WAP: Set/Get the Parameters of WIFI AP Mode.
   AT+WAKEY: Set/Get the Security Parameters of WIFI AP Mode
   AT+WSCAN: Get The AP site Survey (only for STA Mode)
   AT+Z: Reset the Module
   AT+MID: Get The Module ID, eg. A11-yymmddxxxx (yy:year, mm:month, dd:day,xxxx:serial num)
   AT+H: Help
```

4.2.2.15. AT+WAKEY

- Function: Set/Query WIFI security parameters as AP;
- Format:
  - Query Operation

AT+WAKEY<CR>
+ok=<auth,encry,key><CR>< LF ><CR>< LF >

  - Set Operation

AT+ WAKEY=< auth,encry,key><CR>
+ok<CR>< LF ><CR>< LF >

- Parameters:
  - auth: Authentication mode
    - OPEN
    - SHARED
    - WPAPSK
  - encry:Encryption algorithm
    - NONE: When "auth=OPEN", effective;
    - WEP: When "auth=OPEN", effective or "SHARED", effective;

PCI Security Standards Council

Smart Home Power Batteries

- PCI SSC CM November 2015
- Almost exactly the same fail
- 9 years later
- Actually, slightly worse this time

MY WI-FI KETTLE

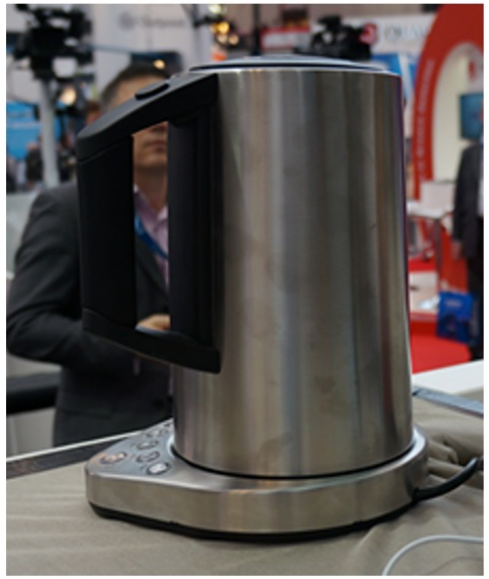
Er yeah. Why?

Nice idea, if pointless

Future potential quite interesting

Coffee machine shipping too

Security-fail central



PCI Security Standards Council

PCI Security Standards Council

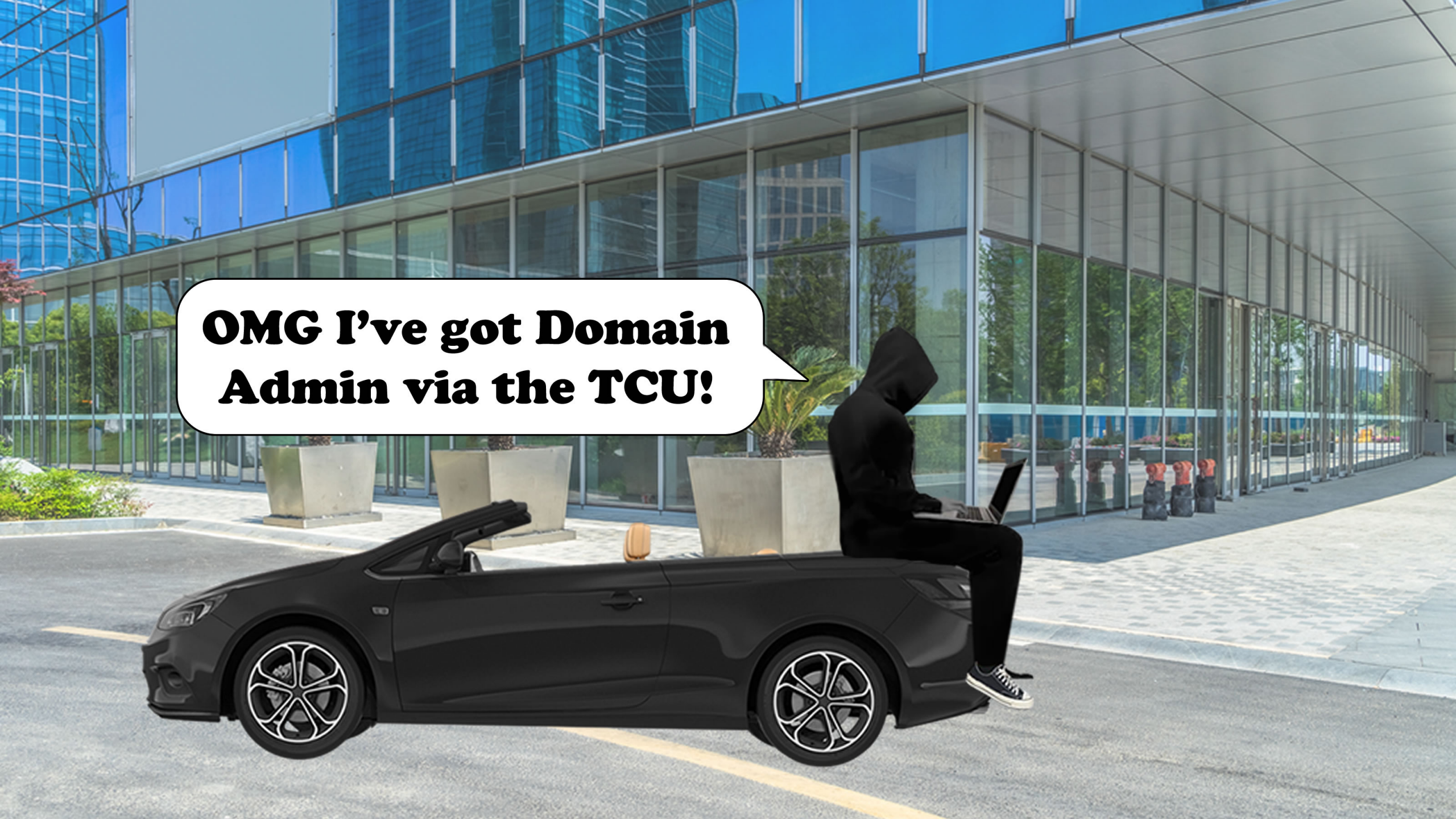
What Can We Take From This?

What Have We Learned in the Last 10 Years of IoT?

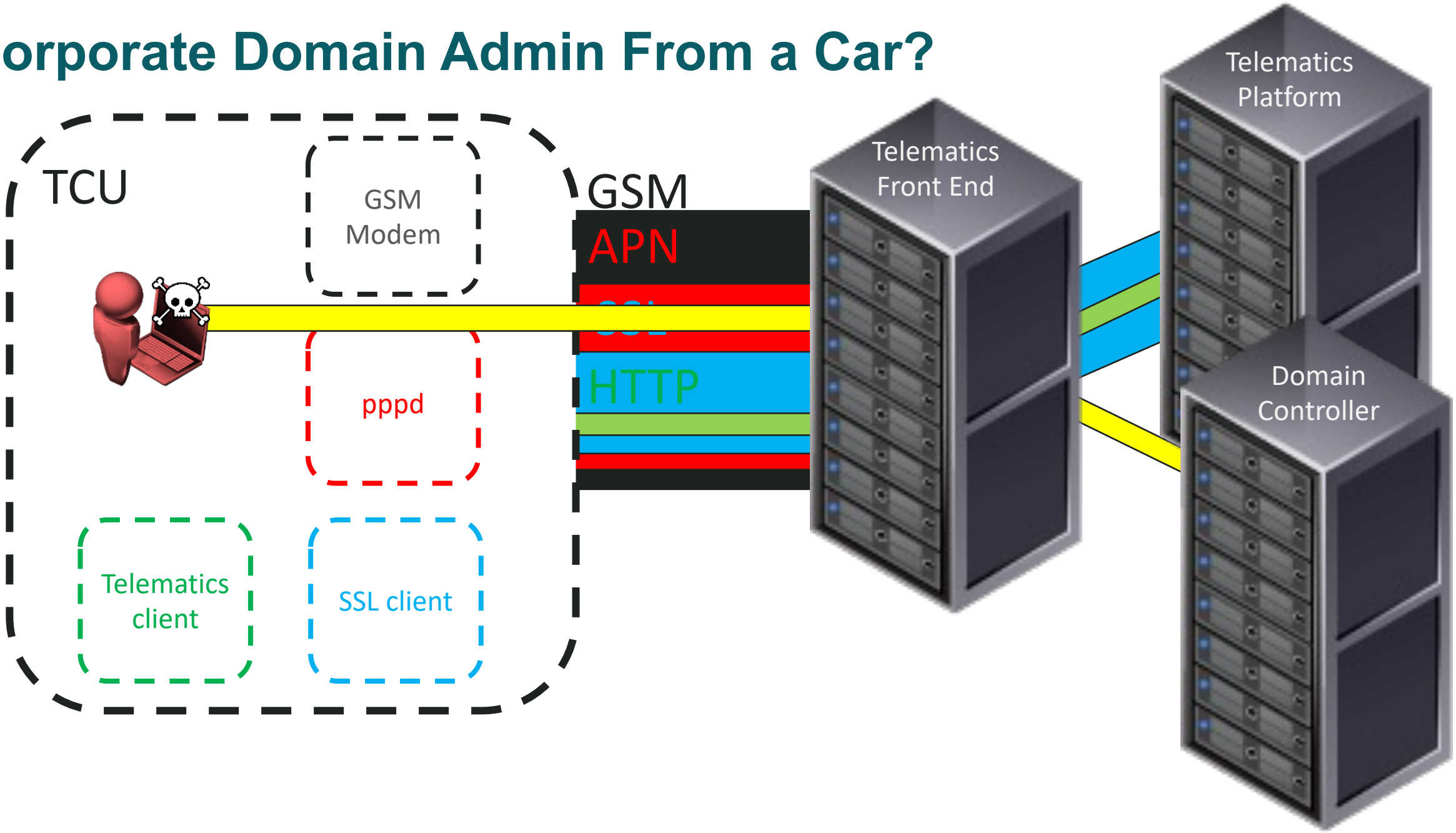
- Consumer IoT has definitely improved
- Failures have evolved, perhaps fewer remote API flaws now
- Vendors are rushing, but security is at least getting some consideration now!
- Standards are starting to create barriers to market entry, forcing more secure development

Where It's Still Going Wrong

- New markets, new products, new vendors, new rush, same lack of understanding
- Lack of regulatory clarity around products that must be installed by 3rd parties
- The 'soft underbelly' of our connected systems, exposing us in ways we hadn't thought of before


OMG I’ve got Domain Admin via the TCU!

Corporate Domain Admin From a Car?



Advice

- Get advice early on in a project. Don’t wait until your pre-live penetration test shows everything is screwed!
- Hardware choice in IoT is really important and very hard to change later on
- It’s not just IoT that we pen test: smart stuff is only one way in to your network, so make sure to red team your organization
- The PCI Council do a great series of podcasts on IoT and similar. One day my toaster will truly be connected!
- Security in IoT can genuinely be a market enabler: security is cited as the second largest obstacle to adoption by consumers

PCI Security Standards Council

Ken Munro
CEO
Pen Test Partners inc

www.pentestpartners.com
LinkedIn: Ken Munro + cyber