secarma
CYBERSECURITY EXPERTS

IoT and Cyber Security

PREVENTING ‘MAXIMUM OVERDRIVE’

Agenda

- Who am I?
- Secarma's IoT Capabilities
- Hollywood vs Reality
- What is the IoT Checklist?
- Words on risks
- Six Security Fundamentals
- High-Level advice
- What are you up against?

Who am I?

secarma
CYBERSECURITY EXPERTS

- My name is Paul Ritchie.
- I am the leader of Secarma in Scotland.
- I have been a Penetration Tester since 2005 (Scarily 12 years).
- Undergraduate and MSc level training as a Software Engineer
- Hardware “newbie”
- Online I can be found as “CornerPirate”:
  - https://twitter.com/cornerpirate
  - https://github.com/cornerpirate
  - https://cornerpirate.com/

Secarma's IoT Capabilities

- **Blog Posts**
  - https://www.secarma.co.uk/secarma-scores-big-defcon-global-hacking-convention/
  - https://www.secarma.co.uk/labs
  - DEFCON 25 in Las Vegas (35 thousand hacker's attending)

- SOHOpelesslyBroken Capture The Flag
  - Second Winningest!
  - Same points as first
  - Beaten on time
- SOHOpelesslyBroken 0-Day
  - Officially: we did well.
  - Unofficially: we did very well.

IoT Security: Hollywood

- Full Film available for free on Archive.org
  - https://archive.org/details/MaximumOverdrive19863gp

IoT Security: Hollywood

secarma
CYBERSECURITY EXPERTS

TL; DR

- If our machines attack us, it would be very bad.
- The worry is that bad security allows similar things to happen.

IoT Security: Reality Check

secarma
CYBERSECURITY EXPERTS

What's putting the brakes on driverless cars?

By Matthew Wall
Technology of Business editor, BBC News

28 July 2015 | Business

Smart homes haunted by the cyber-ghost of Christmas future

By Professor Alan Woodward
Department of Computing, University of Surrey

21 December 2016 | Technology

Share

Could hackers turn the lights out?

By Mark Ward
Technology correspondent, BBC News

16 March 2016 | Technology

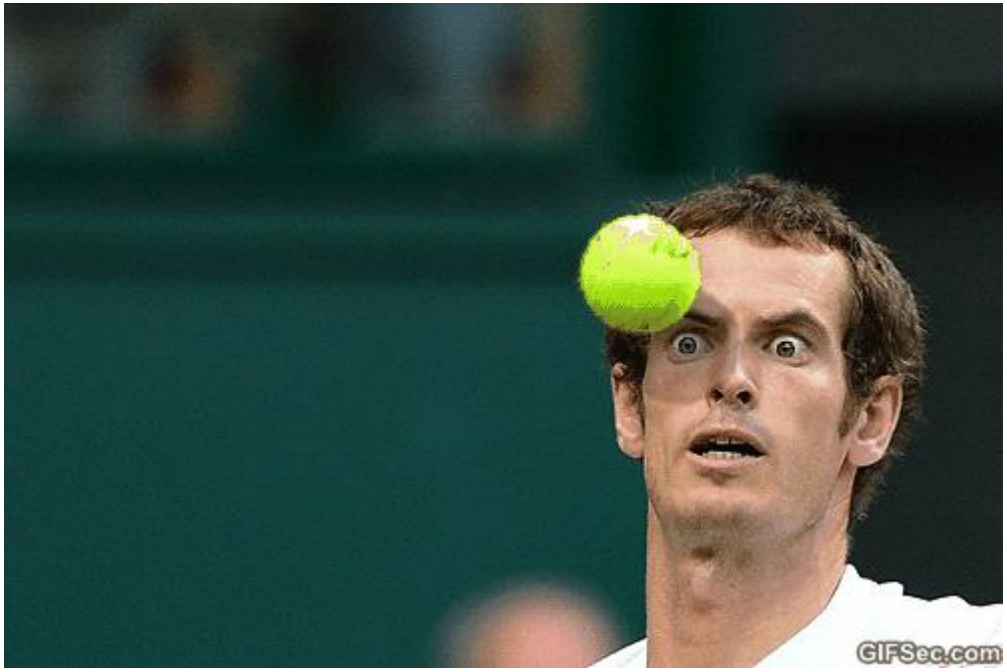
German parents told to destroy Cayla dolls over hacking fears

17 February 2017 | Europe

Share

Why?

- FOCUS (come on Andy!)
  - Bigger Picture
  - Features
  - User experience
- Education
- Someone else will do it?



What is the IoT Checklist?

secarma
CYBERSECURITY EXPERTS

- A work in progress!
- A starting point when considering security of IoT Devices.
- Analysis of IoT security articles:
  - Boiling them down I found *trivial* and recurring root causes.
- Free advice that is intended to help.
- **Where to get it?**
  - **Blog Post**
    - https://www.secarma.co.uk/internet-of-things-iot-security-checklist/
  - **Secarma Labs - GitHub**
    - https://github.com/SecarmaLabs/IoTChecklist

Risky Business

secarma
CYBERSECURITY EXPERTS

- **Consumer Risks**
  - Data Protection Breaches (and fines) for vendors [Cayla]
  - Identity theft or embarrassment for consumer.
- **Collateral Risks to Connected Network**
  - A device which is connected to a Wi-Fi/Ethernet becomes a node.
  - Compromising that device gives access to those networks.
- **Collateral Risks**
  - Compromised devices used in DDoS attacks [Mirai Botnet]
  - The impact here is to unknown third parties
  - Not your users or yourself directly.
- **Reputational Risks**
  - Failure to provide security affects Reputation of Vendor and Product.

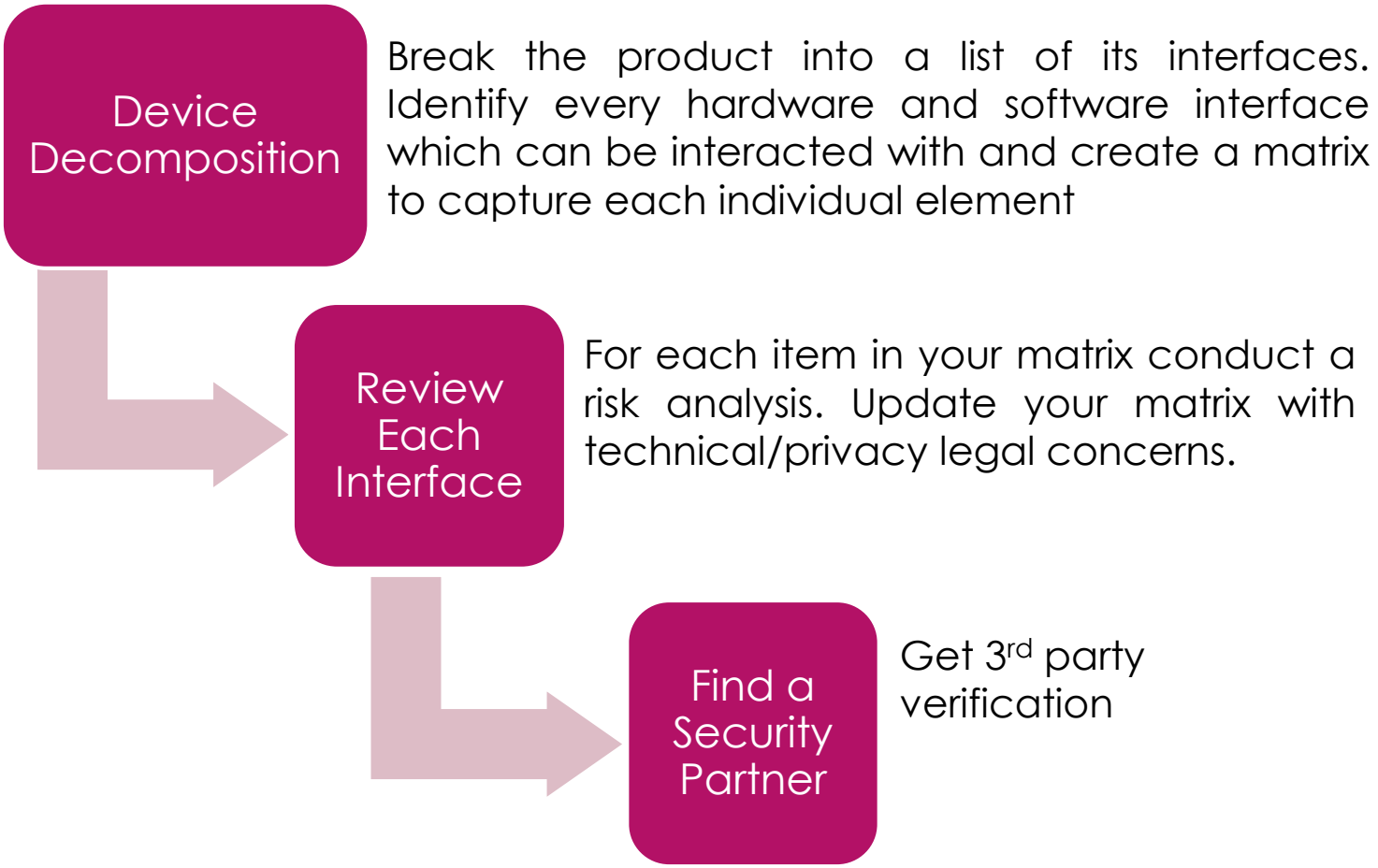
Categories of Risk

secarma
CYBERSECURITY EXPERTS

- **Technical Flaws**
  - The IoT CheckList helps to guard against these.
  - We will show the six fundamentals later.
- **Privacy/Legal Flaws**
  - If the device handles user data or the sensor can be used to breach privacy.
  - Then special consideration should be given to the legal aspect.
  - Identify the potential of privacy breaches.
  - Implement technical controls to guard against them when possible.
  - **CONSULT** legal advice to determine where liability for breaches will lie: will they be on the end user or you as the provider?

IoT CheckList Process

secarma
CYBERSECURITY EXPERTS



Security Principals

- The Six Security Fundamentals of the checklist:

Default/Weak Passwords
Missing Security Updates
Insecure Web Administration
Use of Insecure protocols
Check for known configuration weaknesses
Insecure Data Storage

High-Level Advice [1/2]

- **Secure by Default** – Ask yourself if configurations are secure out of the box, or if the user must do something to enable protection? As cybersecurity has evolved over the last decade, the strategy of securing out-of-the-box is preferred to relying on users. General tips would include disabling features until they are enabled and generating random per-device passwords, for example.
- **Provide an Update Function** – Even the best engineered solution will eventually have some functional or security bug that would require an update. To support this, design a robust update mechanism which can protect users long term.

High-Level Advice [2/2]

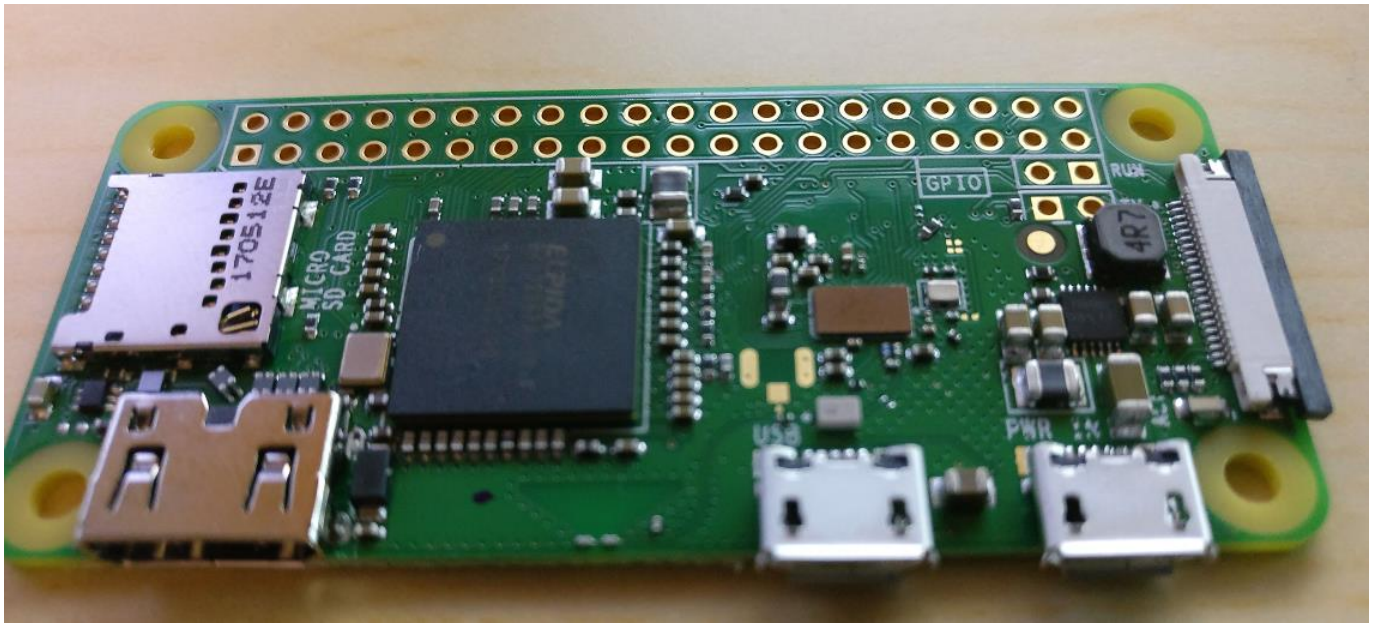
secarma
CYBERSECURITY EXPERTS

- **Assume the source code is visible** – Make sure that there are no hard-coded secrets on the device which have a security impact for all devices. Attackers will have physical access to your products over many years. These are ideal conditions from which to reverse engineer. If you need hard-coded secrets then design them to be unique for each device. So that finding the default admin password within firmware will not expose all other devices. Additionally, be aware that the source for any admin interfaces is equally exposed.
- **Plan for Decommissioning** – IoT products are consumer electronics in most cases. Give users an easy way to remove their data from the device so that they can sell it on or dispose of it securely.

What are you up against?

secarma
CYBERSECURITY EXPERTS

- Bluetooth, Wireless, USB
  - Raspberry Pi (this is our Zero W) - ~£30



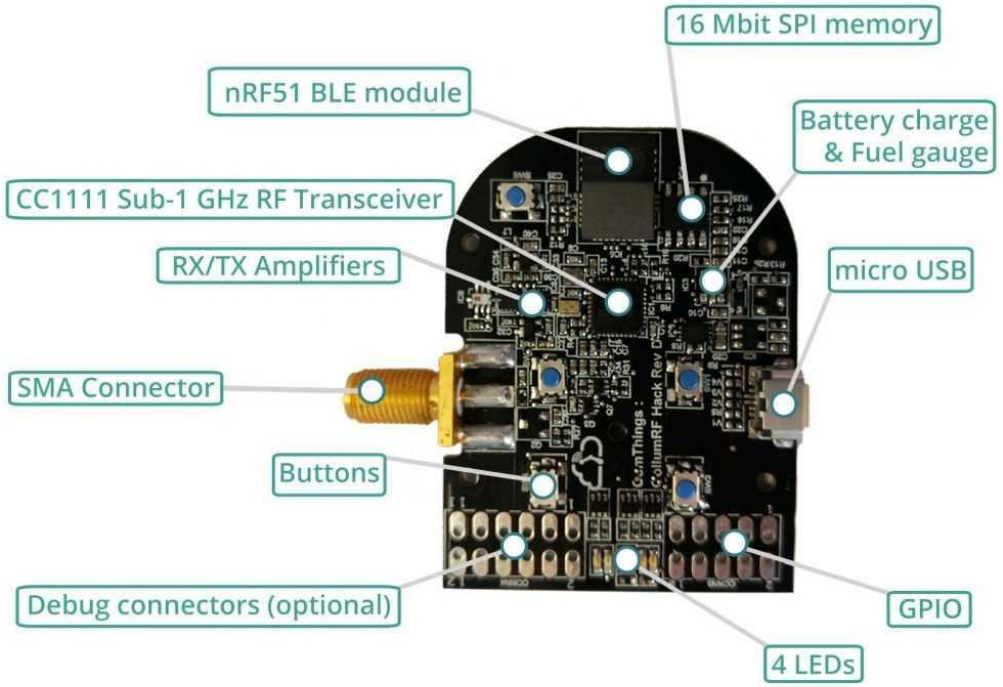
What are you up against?

- **PandwaRF**

- Pocket-sized, portable RF analysis tool
- Sub-1 GHz range.
- Capture
- Analysis; and
- re-transmission of RF

~ £190

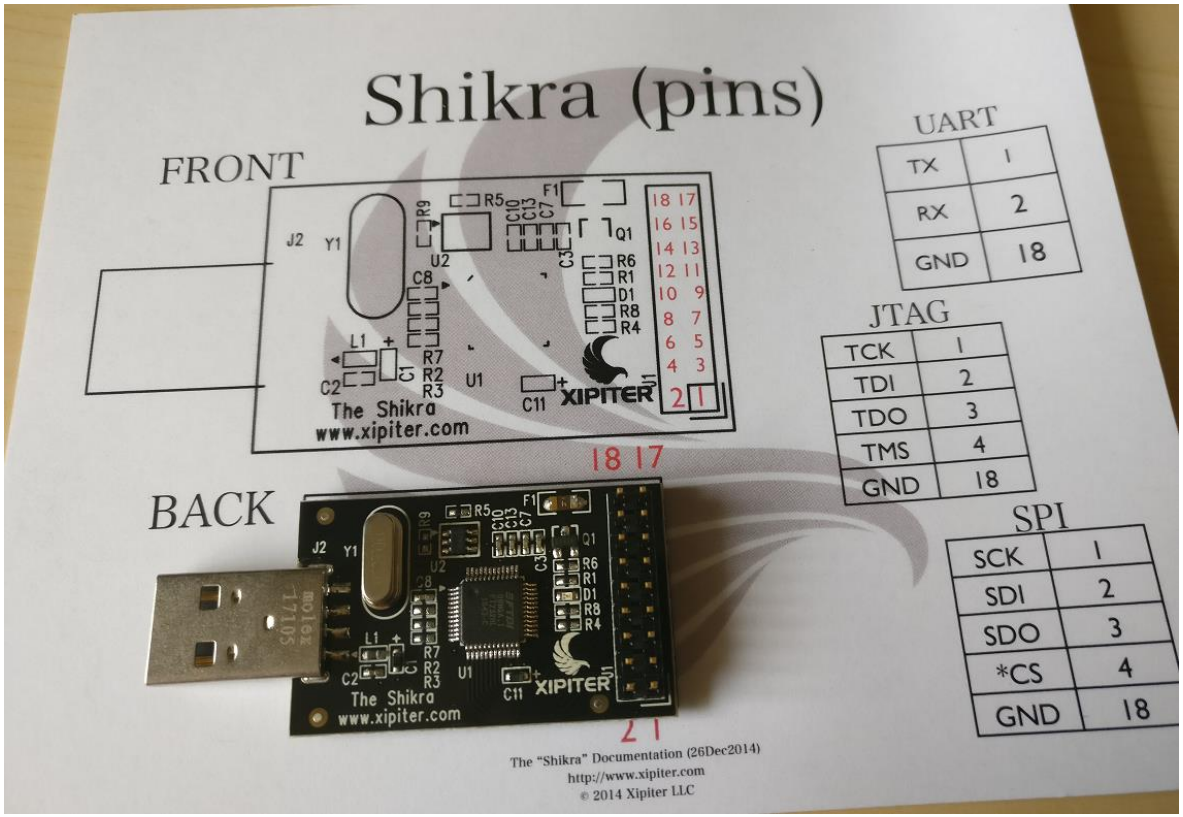
- Alternatives:
  - RfCAT ~ £66



What are you up against?

- Dumping Firmware
  - JTAG
  - UART
  - SPI
  - I2C
  - GPIO

~ £35



Questions?

- No gifs were harmed in the making of this.