Intro to embedded security: implications for connected healthcare products and services

Jeff Spielberg, River Loop Security

August 24, 2017

River Loop Security

Agenda

- Intro to embedded security
- Healthcare + embedded
- (brief) review of life-sustaining medical device vulnerabilities
- Regs? Best practices? What's next?

Who is this guy?

- Healthcare SAAS product manager
- Hospital surgery system development & integration strategy

XL Scrubs. For the shortest guy in the room >

What about security?

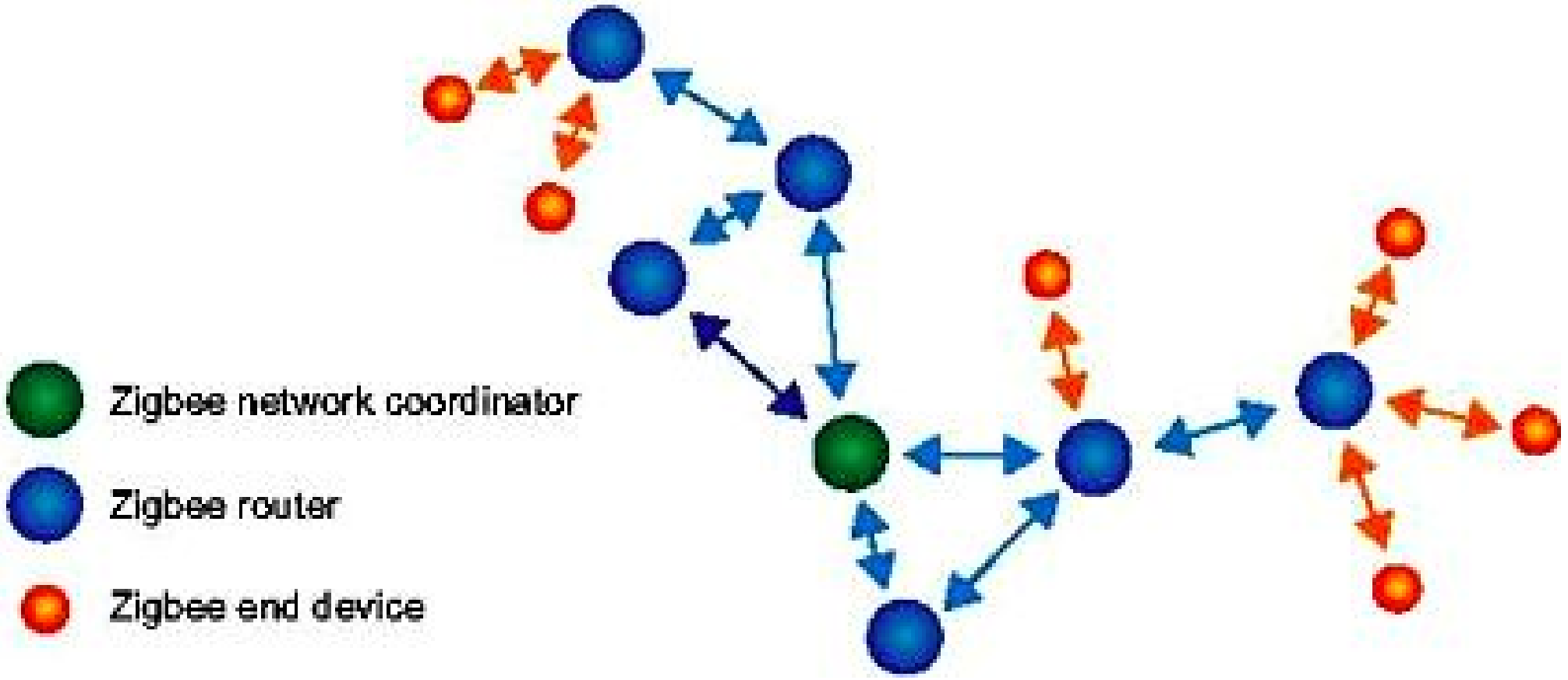
- Founded River Loop Security
  - Embedded, mobile, RF security pen testing, hardware design, incident response
- Electrical engineering at Dartmouth College
  - Smart friends

Embedded - an example

Why embedded? An Example:

www.zigbee.org

Why embedded? ZigBee Network

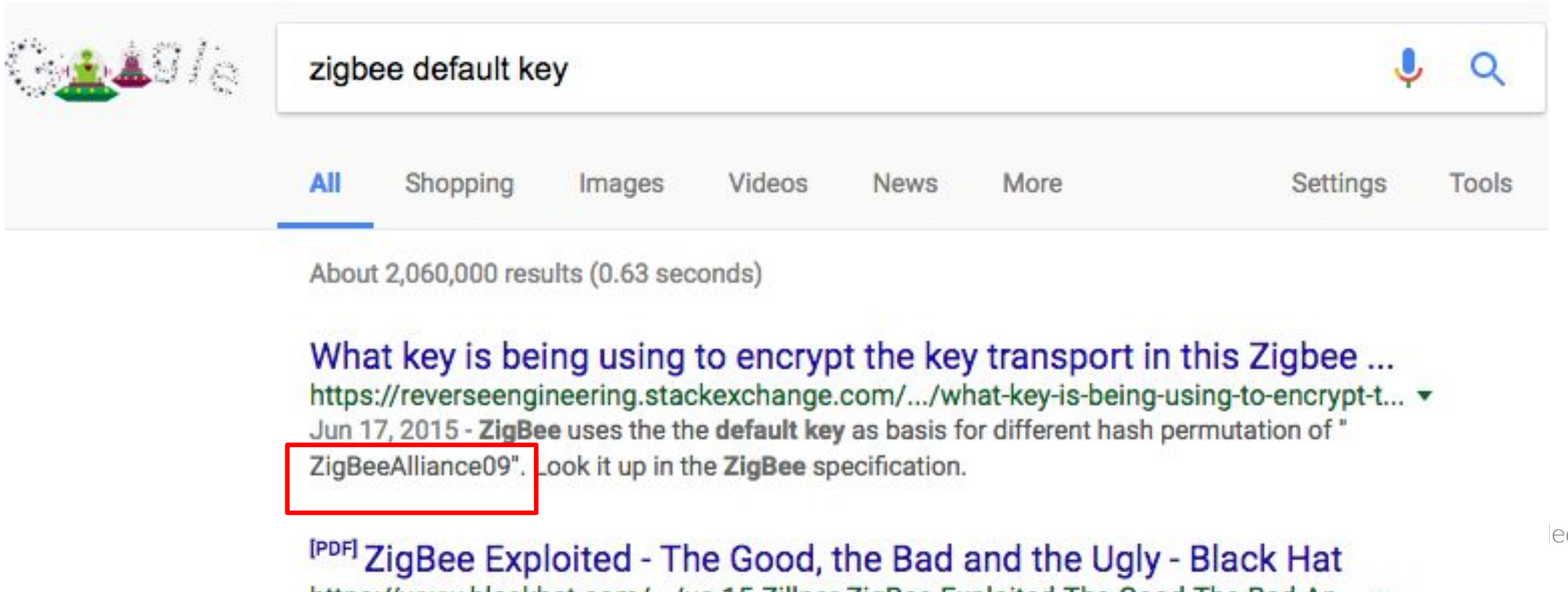


http://www.embedded.com/design/connectivity/4026137/Factors-to-consider-when-selecting-a-Zigbee-controller-for-your-design

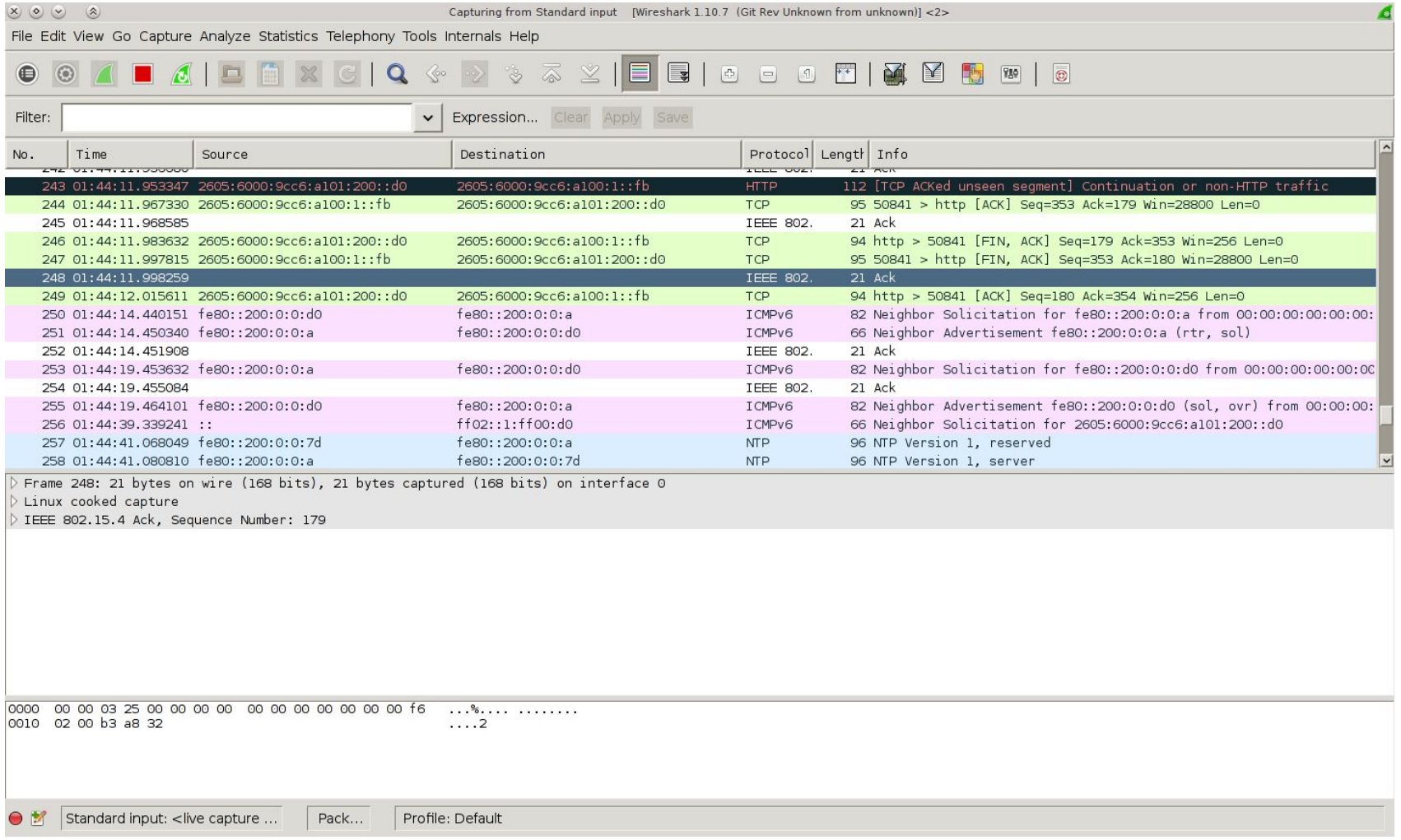
Why embedded? ZigBee Network Security

Built in security!

- Network key: encryption key unique to every network
- Global link key: pre-configured key for all nodes, used to join network

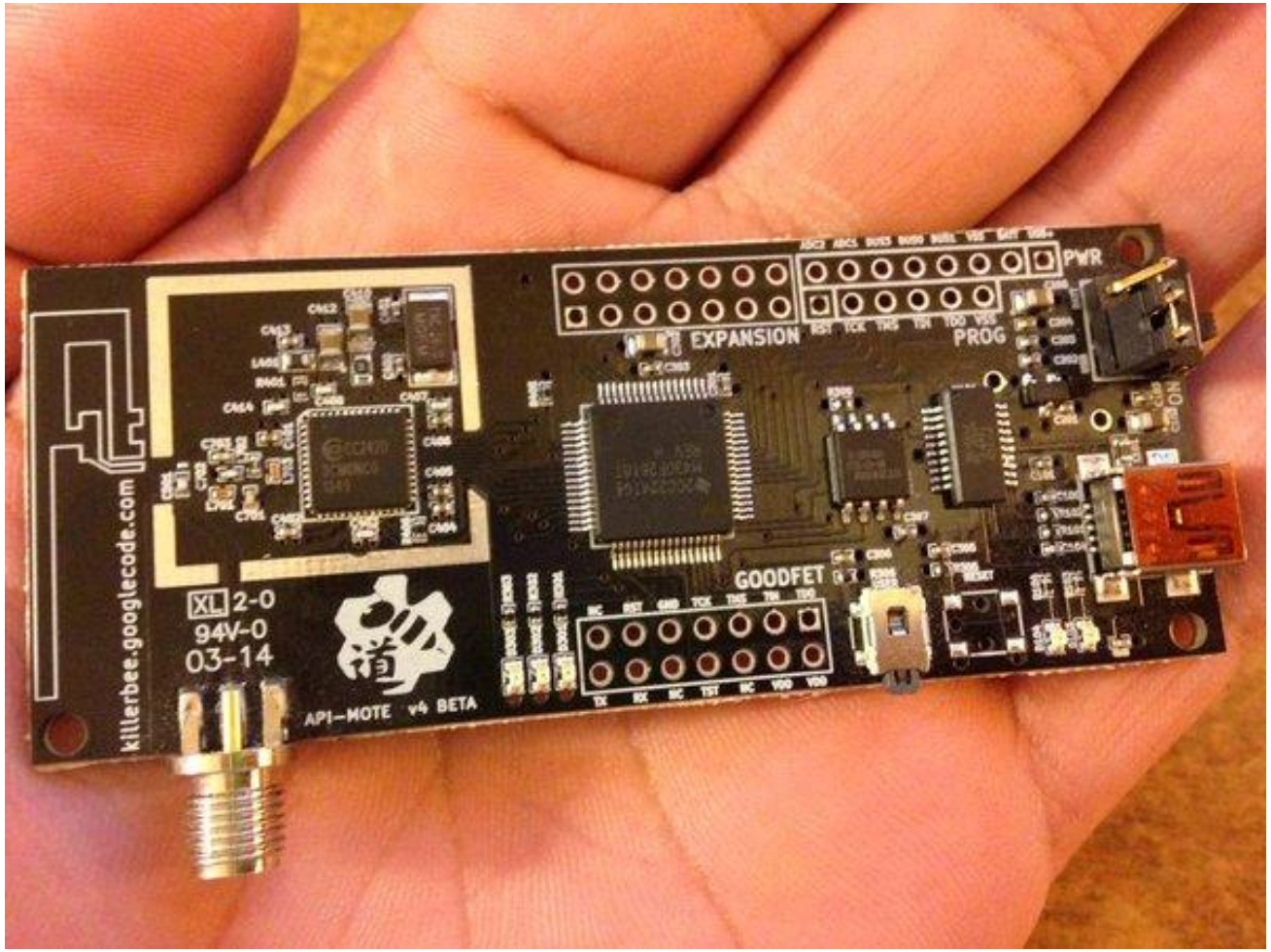


Why embedded? Obscurity to scale… quickly



http://openlabs.co/blog/archives/4-sniffing-802.15.4-packets-natively-with-Raspberry-Pi-and-Wireshark

Why embedded? Obscurity to scale… quickly



Wright's Law

"Security won't get better until tools for practical exploration of the attack surface are made available"

-- Joshua Wright (ZigBee Security Expert), 2011

Embedded Overview

Embedded is in the spotlight due to rapid shifts in capability

The good old days:

- Bare metal
- Assembly
- 8051
- Dishwashers

Embedded devices are advancing but still small footprint + low power

Power: Duty cycling, not “always on”

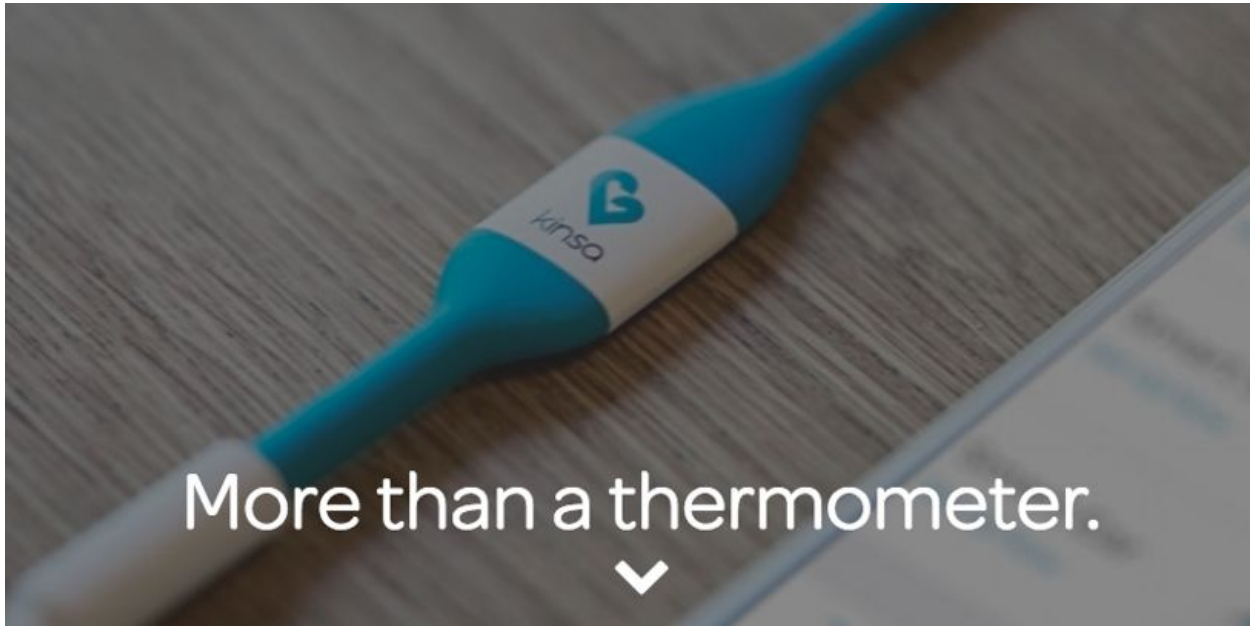
Deployment: Wireless, easy config, backward compatibility

Updates: One-time programming, dependent on supply chain

Embedded is in the spotlight due to rapid shifts in capability

Today's reality:

- GHz processors; GB memory, persistent storage
- 2G, 3G, LTE, IP, custom RF, Zigbee, Z-wave, LoRa



http://www.wired.co.uk/article/strangest-internet-of-things-devices

Exploits are becoming more and more common

Local (external port)

Home Routers / modems

- Root serial console - modify speed value

Cell Phones

- Android phones via audio jack
- Motorola SMS via audio jack

Remote (via cell)

Jeep UConnect Flaw:

- 1.4 million cars recalled
- Sprint network, UDP port 6667 open

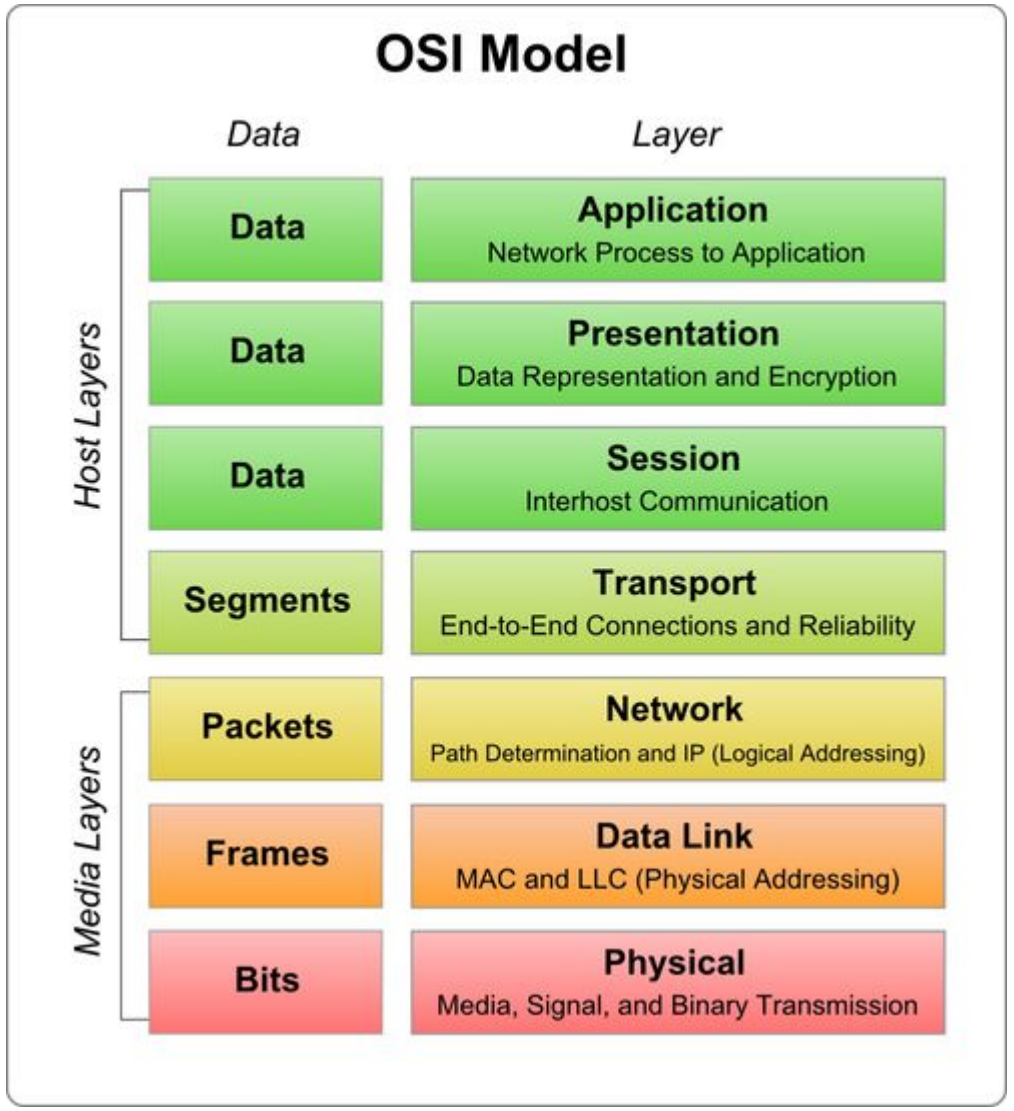
2015: BMW Door Unlocks

- 2.2 million cars, but fixed OTA

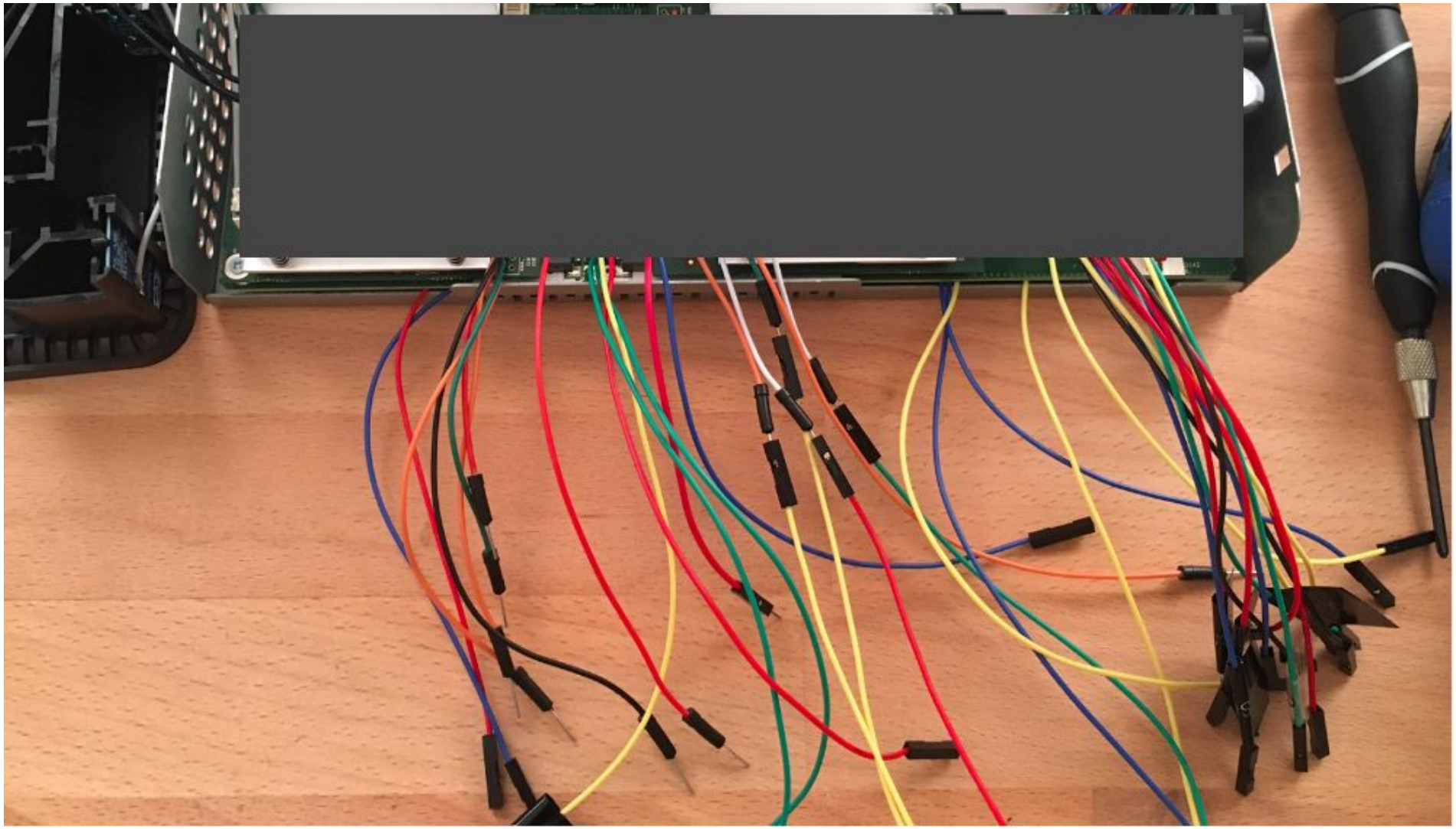
2010: 100 Vehicles 'Bricked'

How we look at embedded

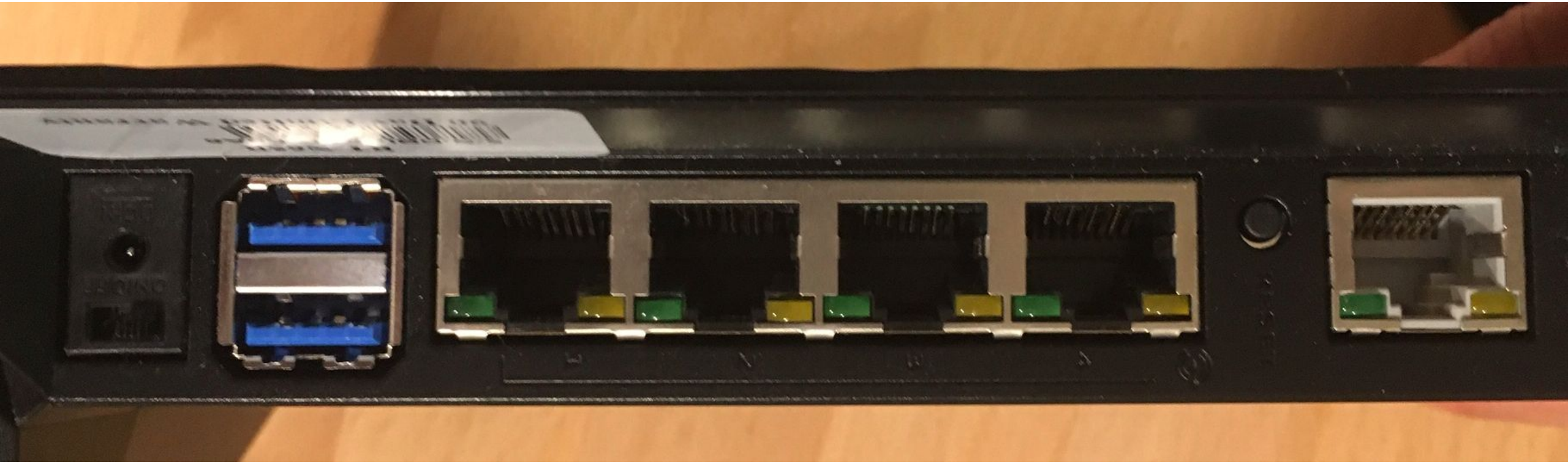
We tend to work at the lowest and least explored levels of the OSI model



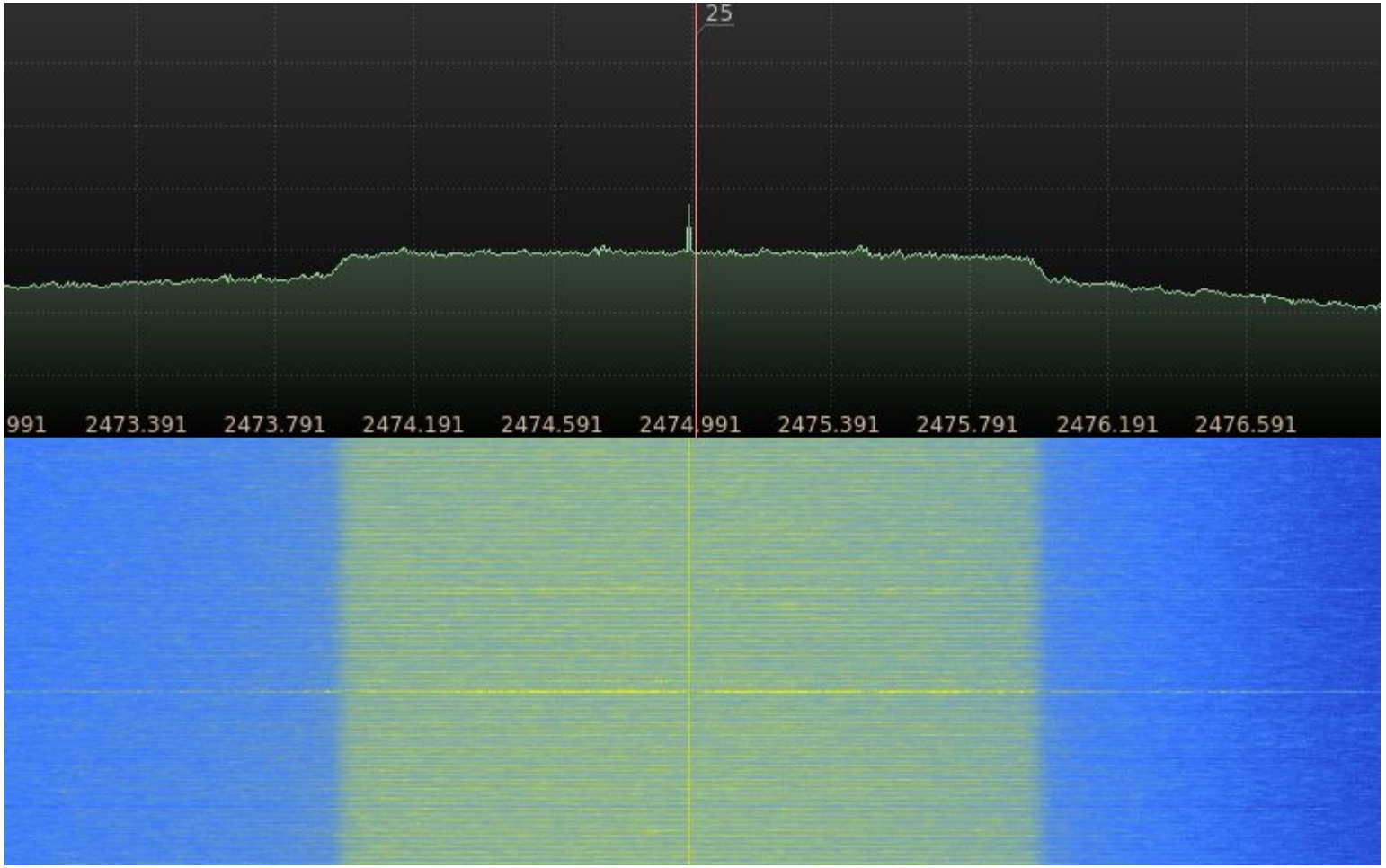
http://www.tech-faq.com/wp-content/uploads/2009/01/osimodel.png

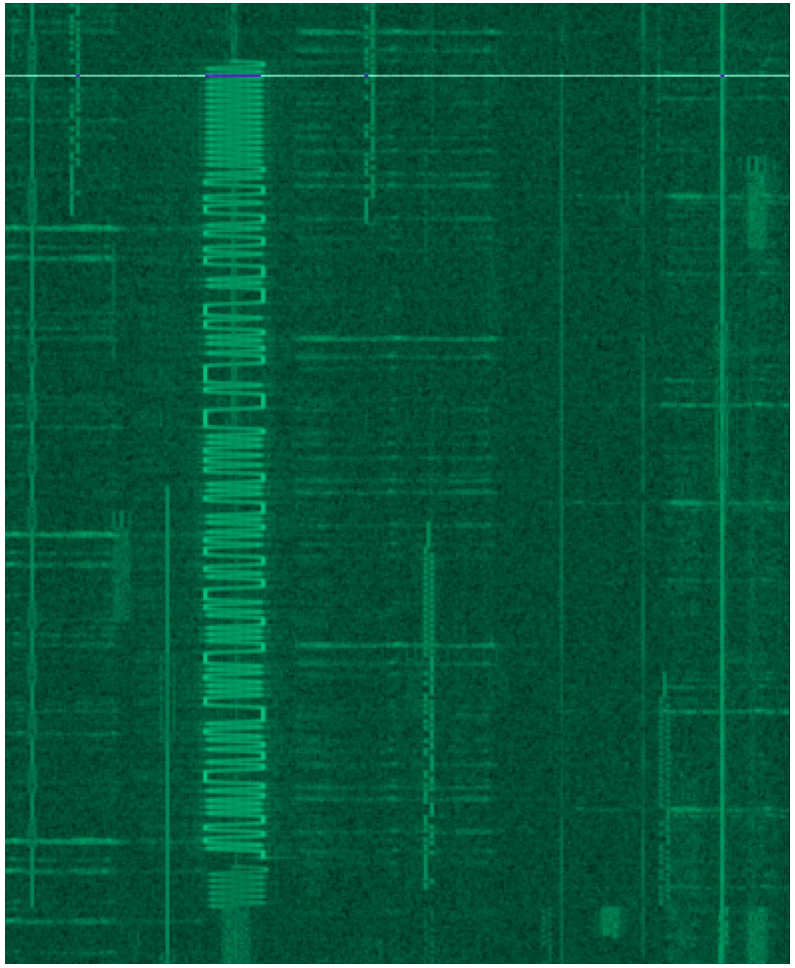


External ports often provide access manufacturers don't advertise

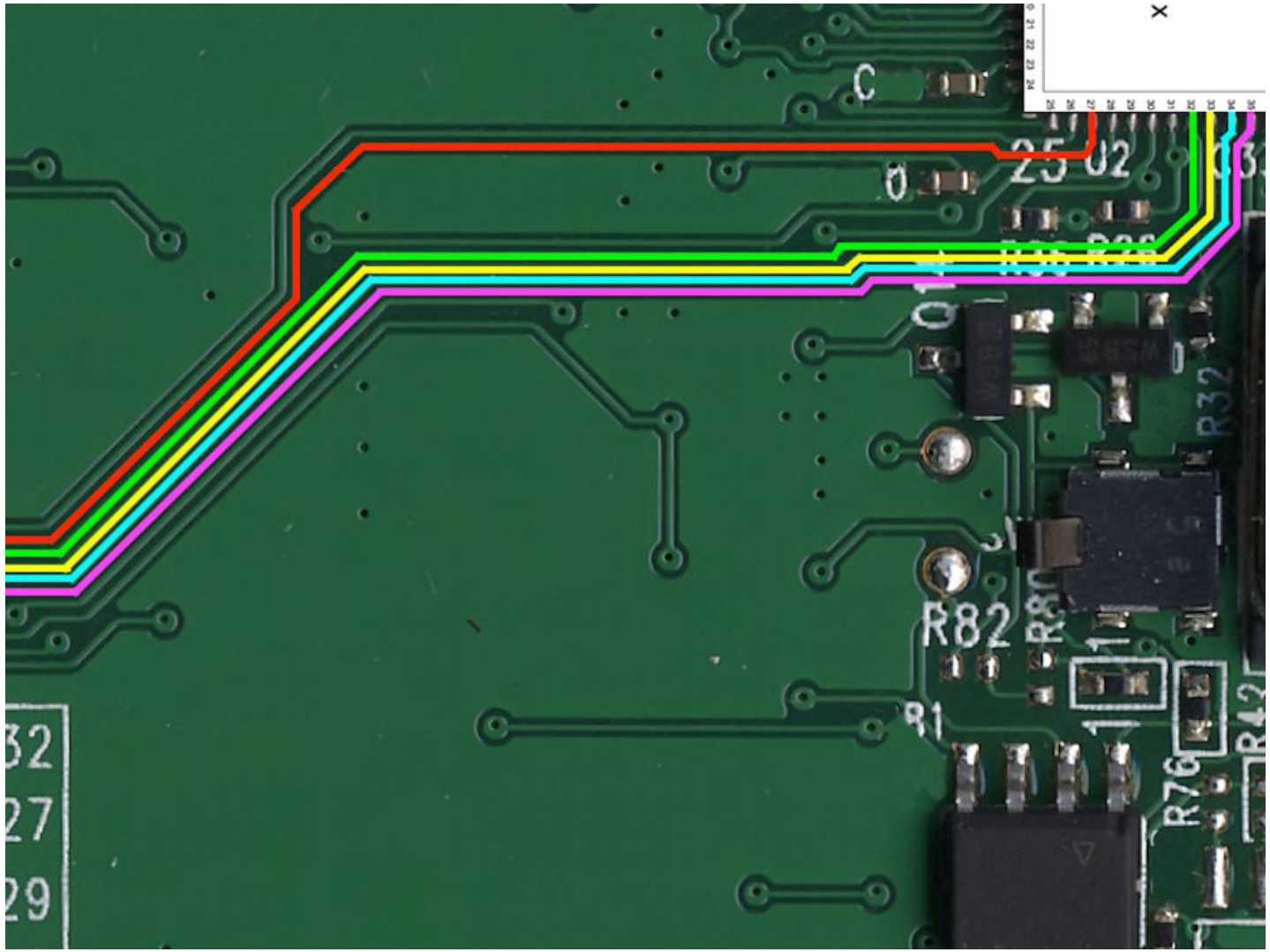


Black box RF analysis yields information on (lack of) cryptographic implementations

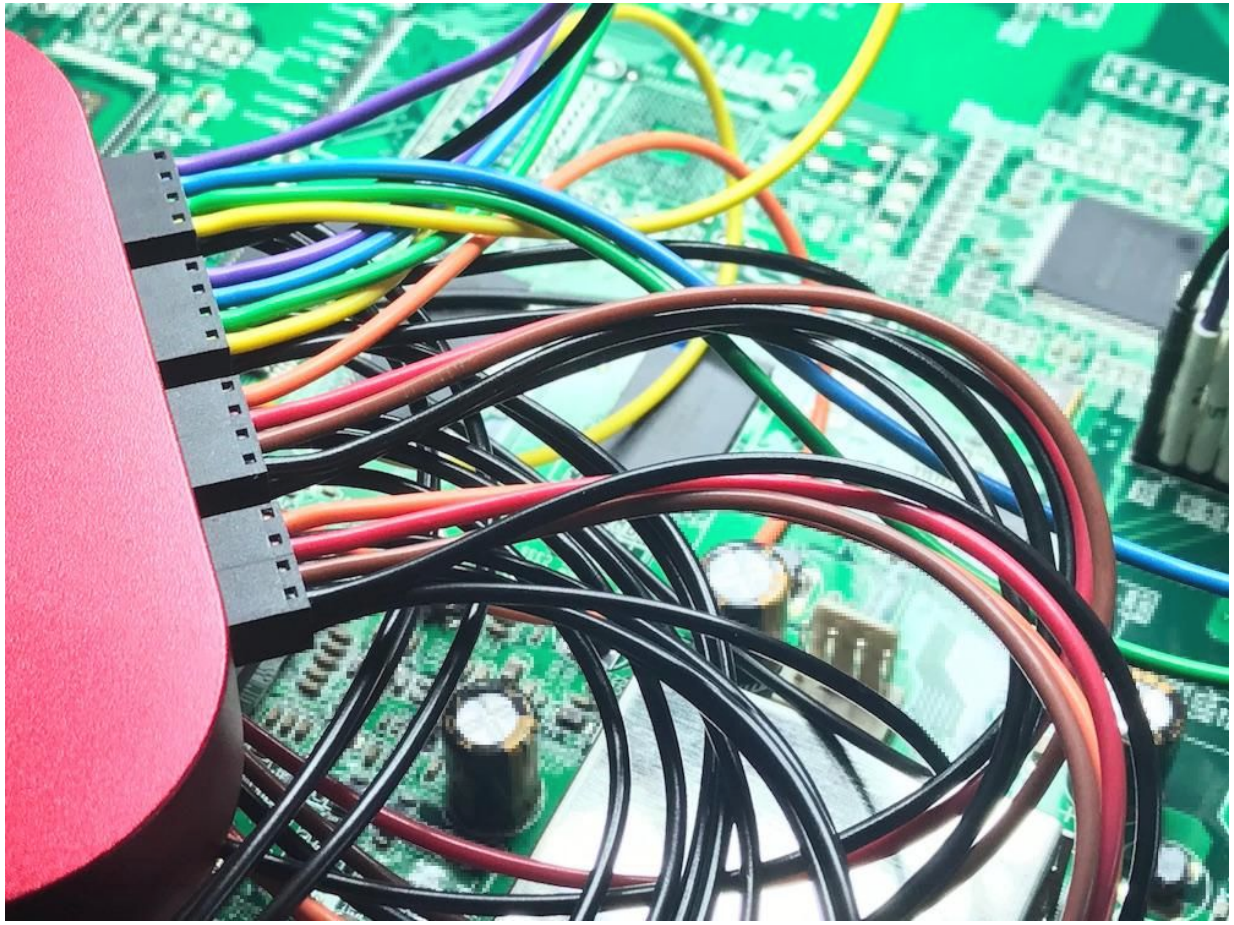




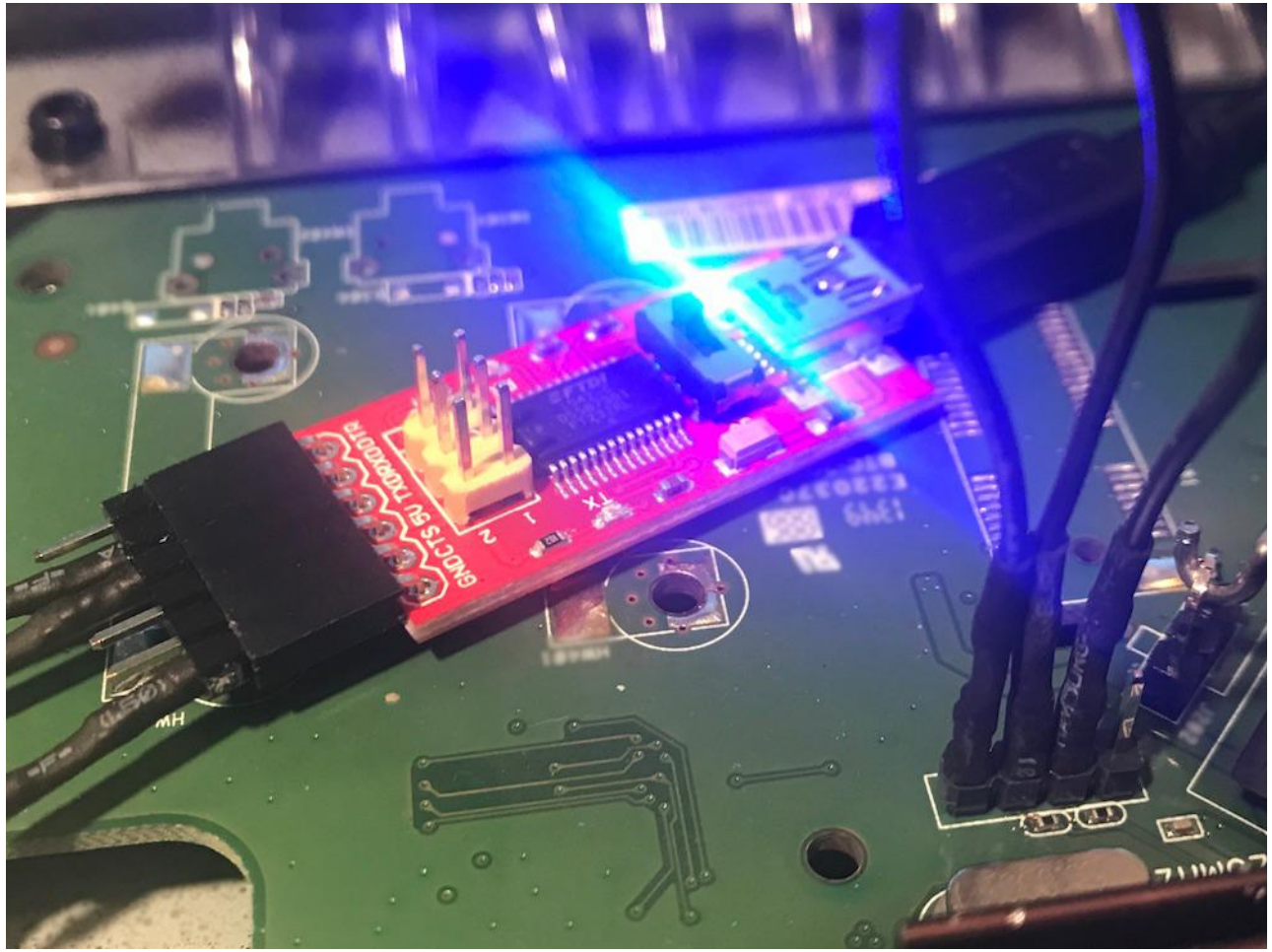
PCB Reverse Engineering can help with low-level logic and power exploitation



A simple logic analyzer can often decode intra-chip communication



Unprotected Headers + Debug Ports are ubiquitous



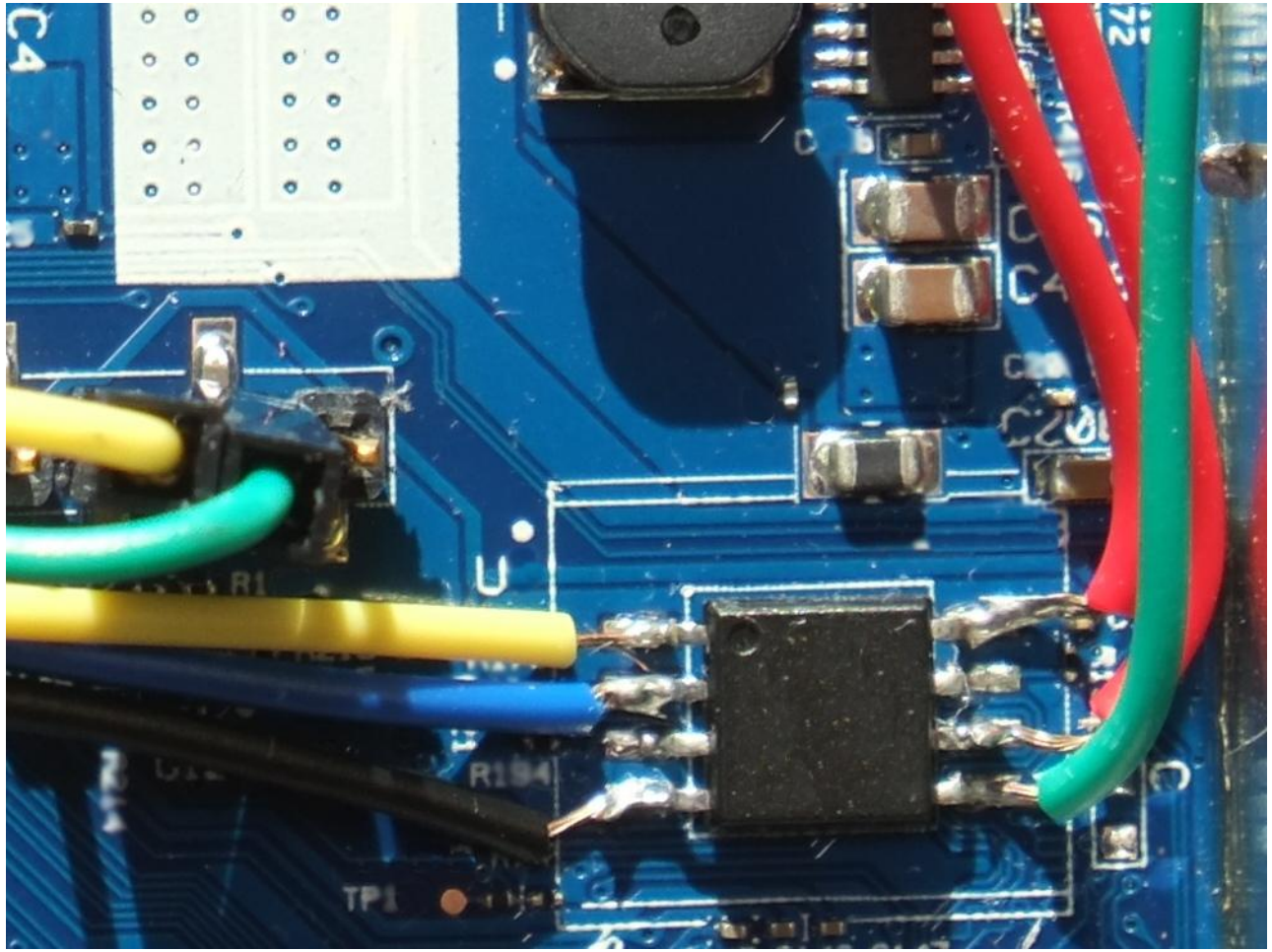
Unprotected Headers + Debug Ports are ubiquitous

```
U-Boot 1.2.0-dirty (Jul 27 2015 - 18:17:31) Cisco-Boot 3.4.22.4

MMC info:
  Manufacturer ID: 0
  OEM ID: 0
  Name: MMC128
  MMC version 4.4
  High Capacity: No
  Dual Data Rate (DDR): No
  Bus Width: 8-bit
  Clock: 50000000
  Rd Block Len: 512
  Capacity: 112.4 MB (117833728 bytes)

Press SPACE to abort autoboot in 2 second(s)
=> help
?       - alias for 'help'
autoscr - run script from memory
base    - print or set address offset
bdinfo  - print Board Info structure
boot    - boot default, i.e., run 'bootcmd'
bootd   - boot default, i.e., run 'bootcmd'
bootm   - boot application image from memory
bpinfo   - Print Docsis IP Boot Parameters
cmp     - memory compare
coninfo - print console devices and information
cp      - memory copy
crc32   - checksum calculation
```

Widely unprotected persistent storage leaks secrets



At the lowest levels of the OSI model we find common easy exploits

Full USB + network stacks

Storage in the clear w/o secure boot

Jamming + poorly encrypted wireless connections

Unencrypted communication channels (hardware)

Unlocked serial console, bootloader console, JTAG

Where does this leave us with embedded devices?

1. Obscurity doesn't cut it anymore
2. The tools are still lacking
3. Patch and device management is almost non-existent
4. People are catching on (good and bad)

Healthcare + Embedded

Technical capabilities vary widely between hospitals

~1350 of 5500 US hospitals are “critical access”

Advanced facilities are limited by legacy devices

http://www.matherhospital.org/laboratory.php

Clinicians have an expectation of device connectivity that is unrealized

What do they want?

- Patient monitors
- Anesthesia, OR equipment
- Ventilators
- Medication pumps
- Lab equipment

Where do they want it?

https://www.ifixit.com/Device/iPhone

We will continue to see a shift to more connected devices

Fig. 1: Segmentation of Devices Based on Access Vector

Function	Stand-alone	Programmable / Readable	Connected (Wireless, IP)
Therapeutic	Patient controlled analgesia pump, Infusion Pump, Ventilator	Holter Monitor, Portable EKG, Hospital glucometer	Anesthesia Systems
Diagnostic	Home blood pressure monitor, Hand-held blood gas analyzer	ICD, Insulin pump, Neurostimulator, Cochlear implant, Foot drop implant	Patient monitoring systems, Continuous glucose monitor

Accessibility

Where's the risk to patients (us)?

Systematic review of life-sustaining devices

Technical Details	• Inherent to architecture? • 0day? • Confidentiality, integrity, availability risk
Disclosure Methods	• CVE filed? • FDA involved?
Vendor Response	• Bueller?

Implantable Cardioverter Defibrillator - 2008

http://www.medtronic.com/us-en/about/news/micra-fda-approval.html

Implantable Cardioverter Defibrillator - 2008

Device	2003 Medtronic Pacemaker
Researchers	Halperin et al
Technical Details	• Unencrypted RF communication with programmer • Pt data leakage • Battery drain attack
Disclosure Methods	Direct to FDA
Vendor Response	• "We feel this is an industry-wide issue best handled by the FDA" • Newer models have "security features"

Implantable Cardioverter Defibrillator - 2012

http://www.nasdaq.com/article/pacemakers-cars-energy-grids-the-tech-that-should-not-be-hackable-is-cm263089

Implantable Cardioverter Defibrillator - 2012

Device	Undisclosed ICD
Researchers	Barnaby Jack
Technical Details	• Wireless reprogramming (30-50 ft) 400 MHz ISM band • Deliver 830V shock
Disclosure Methods	Public disclosure
Vendor Response	N/A

Implantable Cardioverter Defibrillator - 2016

http://www.medicalexpo.com/prod/st-jude-medical/product-70886-642777.html

Implantable Cardioverter Defibrillator - 2016

Device	St Jude Pacemaker + Merlin@Home
Researchers	Medsec
Technical Details	• Wireless battery draining attacks • Remote (IP) reprogramming • Static keys, unencrypted file systems, etc. etc. etc.
Disclosure Methods	Coordinated stock short w/hedge firm
Vendor Response	Issued Merlin@Home firmware updates; “partnered” with FDA, DHS, and ICS-CERT

These threats are not unique to old ICDs

- Whitescope (2017): review of four ICDs with encrypted wireless, file systems, no firmware validation
- Jack, Radcliffe (2011): unencrypted communication in wireless insulin pumps
- Radcliffe (2013): Unsafe boot state in Animas insulin pumps
- Rios (2014): Commands issued on same LAN as Hospira IV drug pump interpreted similarly to button presses

The threats fall into similar categories

- Inadequate protection of custom RF implementations
- Lack of secure boot, firmware validation
- Lack of adequate network authentication on embedded devices

Difficulty in device management and upgrades makes a vulnerability from 2008 still relevant.

Where are the regs?
The Best practices?

The FDA is starting to issue non-binding guidance

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (2014):

- Develop a set of cybersecurity controls
- Consider some key security principles when designing devices (e.g. limiting access through authentication, security update paths, and prevent use of hardcoded passwords)
- Have methods to detect, respond to, and record cybersecurity incidents

We may soon have to find a way to locate devices

Office of the National Coordinator for Health Information Technology (ONC), requiring tracking implantables by unique device identifier:

> "to prevent device-related adverse events, enhance clinical decision-making related to devices, improve the ability of clinicians to respond to device recalls and device-related safety information, and achieve other important benefits"

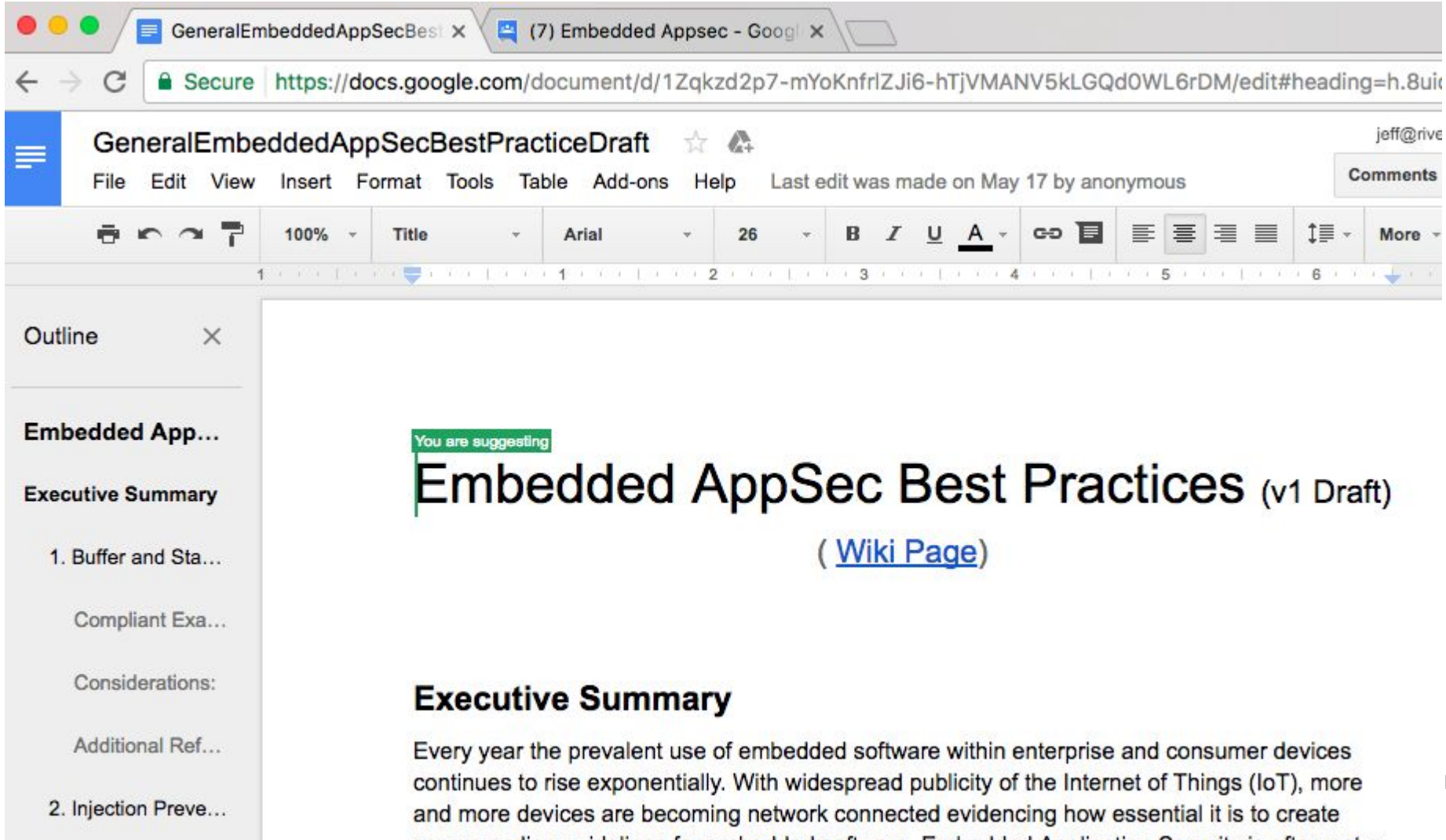
So what does all this mean?

We have relied on obscurity for too long - though the barrier is dropping, we need better tools and methods for embedded

A college EE TA could do the majority of my job

The vulnerabilities fall into common themes that are ripe for best practices to be adopted

I write the standards! You write the standards! We all write the standards!



Where does this leave us?

We must:

- Build better research tools and methods
- Work to develop standards for embedded security (OWASP top 10)
- Start being more selective with devices coming into our institutions
- Look at our regulatory landscape, especially when it comes to life safety
- Make it cheaper and more valuable for companies to invest in cybersecurity

Thanks!

Any questions?

You can reach me at:
jeff@riverloopsecurity.com
www.riverloopsecurity.com