Objectives

• Intro
• Challenges
• Why problems occur
• We’re doing a security 🎉
Who’s this guy?

• Security person...

• ... Specifically... a security person at ecobee, an IoT company
Existing IoT Talks…

“Oh look, old $thing! << redo old $thing talk >>”

“Normal webapp stuff, that happens to be in an IoT device”

“So, with physical access to the hardware….”
Existing IoT Talks...

Focus on impact of hack, less on root cause

Largely presented by people outside of IoT

Lots of guesswork
We’ve seen the headlines
We’ve seen the headlines

Amazon's Ring Is a Perfect Storm of Privacy Threats

Microsoft Nabs Russian Hackers Exploiting 'Sloveana' Vulnerability

Amazon and Google are listening to your voice recordings. Here's what we know about that

First Amazon admitted it -- now Google says it's listening, too. Here are the specifics, and the questions we still want answered.
But why?!
We should do an IoT avocado.
💡 We should do an IoT
Never caused a problem!
Building Hardware

Evaluation & Discovery

Iteration

EVT

DVT

PVT

Mass Production

Design Validation & Testing

Production Validation & Testing

Engineering Validation & Testing
Building Hardware

- PCB Fabrication
- Sourcing & Shipping components
- Assembly
- Build Quality Testing
- Case, accessories, etc
- Packaging
- Shipping
Languages

- Resource constraints
- Kernel Drivers, etc
- Blackbox Drivers
Key Management is hhhhhhaaaaaaaarrrrrrrrrrddddddd
IoT Key Management is hard
Shipping Keys

• Shared vs Individual keys?
• Private keys with 3rd parties?
• How about some TOFU?
Erp! We’re an OS vendor now!

Urgh, dependancies!
WaterAgileFall Development
Logistics

$\text{things are in } \$\text{places}$

$\text{time to } \$\text{thing being online} = $

$\text{geo of } \$\text{thing at } \$\text{time} =$
Remember this?
Oh yeah, that
All about the Benjamins Bordens

Retail Price
- Taxes
- Retailers take
- Shipping & Packaging
- Parts & Labour
- R&D Costs
- Marketing

.... oh yeah, some profit $ 

Wait, no subscription revenue ??
- Tech Support
- Customer Service
- Replacements / Returns
- Hosting / Bandwidth (APIs)
- Free Mobile App
- Free online portal

...... and then ......
With what’s left…

• Patch / Update Development Costs
• Operate a security team
• Pen Tests & Bug Bounties
Let’s talk updates
Let's talk updates

- OTA
- Automatic Signed
- Manually Initiated Signed
- Manually Initiated
- OTA
- Manually Uploaded binary

None?! 😞
Speaking of updates..

:-(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. (67% complete)

If you like your house, you can press the button on the screen.

error: no such partition.
Entering rescue mode...
grub rescue> _

Software Failure. Press left mouse button to continue.
Guru Meditation 0000000.05863330
Quality & Testing

• Bad updates are BAD
• Makes modern agile practices more challenging, sometimes, ish
Recycle, Refurb, and RMA

• Also makes agile hard, sometimes, ish

• Let’s talk about JTAGs
Low Friction Deployment

.... ah! The eternal ease of use vs security balancing act
Hey, it’s not all bad…

• (Some) companies are waking up
• (Some) are being forced
• Public awareness is moving up ✌️
So, what’s happening?
- Insufficient privacy protection
- Insufficient data transfer and storage
- Lack of device management
- Insecure default settings
- Lack of physical hardening

- Weak, guessable, or hardcoded passwords
- Insecure network services
- Insecure ecosystem interfaces
- Lack of secure update mechanism
- Use of insecure or outdated components

OWASP IoT Top 10
Research...
Summer’y Summary

Everything’s fine, don’t worry 😳
Thanks for your time.

Any Questions?