Securing COTS Devices for IIoT
Why do we need to talk about COTS?

I've been a professional hacker for more than 15 years. I find cybersecurity problems in technology in order to make that technology more secure. But after doing this for many years, I'm frustrated.

I see the same problems over and over again. We are not getting better. And while we depend more and more on technology, technology is becoming more and more insecure.

- Cesar Cerrudo, IOActive Labs CTO, Forbes Technology Council
  Why Cybersecurity Should be the Biggest Concern of 2017, Jan 2017
Agenda

- Intro
- High Level Basics
- Effective Methods
- Lessons Learned
Jon Taylor

- B.S. Electrical Engineering, Bradley University 2009
- Started Caterpillar in 2007
- Joined Monico in 2014
- Returned to Caterpillar in late 2017
The Allure of Free Stuff…

- Chipset Manufacturers Want Your Business…
- All Provide Board Support Packages (BSPs)

Most Provide NO Security Enabled by Default
Hardware Based Security

- TPMs and Secure Boot Devices
- Hardware Key Storage

Secure Boot Does Not Make You Superman
Trust But Verify
Basic Hardening 1

- Uboot Halt
- Hash Methods
- Manage Drive Mounting
Basic Hardening 2

- Turn off all Unused Hardware
  - Device Tree vs. Driver

- Depop Reference Design

- Remove all Unneeded Software from Build

- Security Early and Often
Identity Management

- Don’t Skimp – This is the future for IoT
- Bi-Directional Authentication (Mutual)
- Unique Device IDs if possible
- Don’t Use Device Root for Anything Except ID
Opposing Use Cases and System Segmentation

Breaks IT Rules

Breaks SANS Rules
Process Isolation

- Chrooting
- Namespace Segmentation
- Dockers
Removing Root

- EVERYTHING is run as root!
- Adding users and groups
- Segment based on criticality to system
Dear Engineering...

Hackers don’t care how you meant for your software to work...
Application Hardening

- Don’t Overdo it – Focus on Isolation
- Give the Soft Ground
Seems like common sense...

- Remove Uncontrolled Points of Access
- Use HW Drive Encryption if Available
Seems like common sense…

Don’t Leave Keys in Memory