Attacking
Critical Infrastructure

Justin Searle
Managing Partner – UtiliSec
justin@utilisec.com // @meeas
What is Critical Infrastructure?

Assets that are essential for the functioning of a society and economy

- Food and Agriculture
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy

- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Transportation Systems
- Water
Critical Infrastructure Control

Controlling Servers → Intermediate Network Devices → Controlled Field Device

Attacker → Intermediate Network Devices → Controlled Field Device
Penetration Testing Methodology

- Green: Tasks most frequently and require the most basic of penetration testing skill
- Yellow: Tasks commonly performed and require moderate penetration testing skill
- Orange: Tasks that are occasionally performed but require higher levels of expertise
- Red: Tasks performed infrequently and require highly specialized skills
Can Attackers Reach Field Assets?

- Many field deployed Critical Infrastructure devices have tamper detection and tamper protection mechanisms
- Locked cases and enclosures
  - usually trivial to pick
- Tilt and vibration detection components
  - can often be disabled before triggering once you locate them
- Cameras
  - often not monitored
  - long response times if they trigger
What To Do With Field Devices?

• Attacking data at rest
  – Power down the device, expose its circuit board, and interact directly with each component
  – Extract contents of accessible RAM, Flash, and EEPROM
  – Identify cryptography keys or firmware

• Attacking data in motion
  – Boot and normally operate the device in a lab, monitoring bus activity between major chips (MCU, Radio, Flash, RAM)
  – Crypto keys can often be found in key load operations between a microcontroller and crypto accelerator
  – Firmware can often be found in boot processes (between Flash and MCU) and firmware updates (between Radio, MCU, and Flash)
Embedded Device Pentest Tasks

- Penetration Test Planning
- Architecture Review
- Target System Setup
- Embedded Device Pentest Tasks
  - Network Communication Penetration Tasks
  - Server OS Penetration Tasks
  - Server Application Penetration Tasks
- End-to-End Penetration Test Analysis
- Result Interpretation and Reporting

Embedded Device Penetration Tasks

- Electronic Component Analysis
  - Device Disassembly
  - Circuit Analysis
  - Datasheet Analysis
  - Dumping Data at Rest
  - Bus Snooping Data in Motion
  - String Analysis of Retrieved Data
  - Entropy Analysis of Retrieved Data
  - Systematic Key Search Through Data
  - Decoding of Retrieved Data
- Embedded Hardware Exploitation

Embedded Device Penetration Tasks

- Field Technician Interface Analysis
- Firmware Binary Analysis

Copyright 2012, 2013 Justin Searle
http://www.utilisec.com
Embedded Field Device Disassembled

1. 240v Connections
2. Microcontroller (Teridian 71M6531F SOC)
3. Dual Operational Amplifier (LM2904)
4. ISM Band RF Amplifier (RFMD RF2172)
5. ISM Band RF (TI CC1110F32)

Embedded Device Testing
Bus Pirate to EEPROMs

CAT25080 – SPI

24LC088 – I2C

GND +3V3 +5V VPU CLK CS MOSI MISO +3V3 GND +3V3 +5V VPU CLK CS MOSI MISO

Mode | MOSI | CLK | MISO | CS
--- | --- | --- | --- | ---
HiZ | | | | |
1-Wire | OWD | TX | | RX
UART | | | | |
I2C | SDA | SCL | | |
SPI | MOSI | CLOCK | MISO | CS
JTAG | TDI | TCK | TDO | TMS

24XX08* is a 8 Kbit Electrically Erasable PROM. The Microchip Technology Inc. 24AA08/24LC08B EEPROM devices internally organized as 1024x8/2048x8 bits. They feature a 32-byte page write buffer and support the Serial Peripheral Interface (SPI) protocol. The device is enabled through a Chip Select (CS) input. In addition, the required bus signals for the 24XX08* part are a clock input (SCK), data input (SI) and data output (SO). The 24XX08 is also available in the 5-lead SOT-23 package.

*24XX08 is used in this document as a generic part number for the 24AA08/24LC08B devices.
I2C Protocol

I2C Write Command: 0xA0 0x00 0x00 0x00 0xB0

- Chip Address: 00000
- Memory Location: 00
- Data to Write: 

Memory Block: Write = 0 Read = 1

Set Address to Read 0xA0 0x00 0x00 0x00 0x00

I2C Write Command: 0xA1

- Chip Address: 00000
- Memory Bank: Not Used
- Write = 0 Read = 1

Each "r" = read 1 byte
Dumping EEPROMs and Flash
Bus Snooping Data in Motion
Using Entropy to Find Keys

- Asymmetric keys have high entropy (very random)
- RAM and Flash is filled with non-random data
- Graphing entropy of flash reveals a spike in randomness
- This spike is the location of the asymmetric key in flash
Systematic Crypto Key Search

• Perform basic string searches for obvious keys
• Develop custom tools to do more advanced searches:
  – GoodFET: Abuses vulnerability in TI, Ember radios to access RAM even when chip is locked
  – zbgoodfind: Search for ZigBee key using RAM dump as a list of potential keys
  – Combined they can recover the ZigBee network key

```
$ sudo goodfet.cc dumpdata memdump.hex
Target identifies as CC2430/r04.
Dumping data from e000 to ffff as chipcon-2430-mem.hex.
...
$ objcopy -I ihex -O binary memdump.hex memdump.bin
$ zbgoodfind -R 802154_encr_sample.dcf -f memdump.bin
zbgoodfind: searching the contents of 802154_encr_sample.dcf for encryption keys with the first encrypted packet in memdump.bin.
Key found after 6264 guesses:  c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf
```
Decompiled Code
Conclusion

• Critical Infrastructure needs more testing!
  – Testing needs to be constant and remain agile
  – Testing needs to go deeper and include field controlled assets

• Research is needed in all major areas of security
  – Apply your talents and find your niche!

• Pentesting methodology for energy sector is publically available
  – Provides a detailed methodology for performing penetration tests from controlling servers all the way to the controlled embedded field devices
  – Methodology is directly applicable for any critical infrastructure organization and the systems they use to control critical assets

• UtiliSec's Assessing and Exploiting Control Systems course
  – Offered live at all SANS ISC Summits and Training events
  – Based on SamuraiSTFU (Security Testing Framework for Utilities)
Contact Information

www.utilisec.com
sales@utilisec.com

Justin Searle
personal: justin@meeas.com
work: justin@utilisec.com
cell: 801-784-2052
twitter: @meeas