AMI-SEC ASAP Red-Team Initiative

Matthew Carpenter

InGuardians
matt@inguardians.com
http://www.inguardians.com

# Purpose of Red-Team Testing

- Test the relative-security of existing meter solutions

- Identify Vulnerability Classes using a Bottom-Up Approach

- Real-World Security Pen-Testing Guidelines

Why Bottom-Up?

- Security Initiatives Start Top-Down.

  - Often identify things to protect

- Hacking often starts Bottom-Up

  - Identify what really exists

    - Keeping the "Prize" (at the top) in mind

    - Creatively leverage opportunities at the bottom

      - To impact Value-Streams at the top
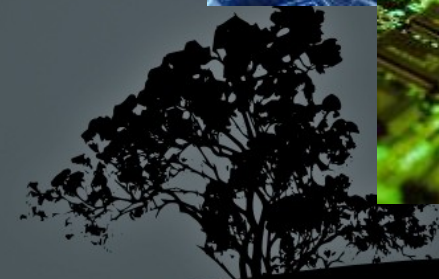
Hacker's Serenity Prayer

- God give me the Serenity to:

  - Alter the Alterable

  - Get around the Unalterable

  - The Creativity and Tenacity to 0wn the System

  - and Never Give Up...

What is Alterable? (aka. What Can We Tickle?)

- Network Traffic

- Network Access

- Meter Access

- "Collector"/Bridge/Network Gear

- Head-End?

Network Traffic

- Capture

- Injection/Becoming a node

- Man-In-The-Middle

  - Firmware update

  - Interception/Modification of Command and Control

    - All your meters are belong to us

- Denial of Service

  - Complete

  - Selective

- Route-Manipulation

Network Access (HAN/NAN/WAN)

- Attacking Services provided by other Nodes on the Network

  - Similar to Internet-Attacks with Metasploit or Core Impact

    - Weak Authentication/Authorization

    - Buffer Overflows

    - Integer Over/Underruns

    - Format String Flaws

    - Sandbox Issues (and other Logic Flaws)

      - Bleed from HAN to NAN, etc...

Meter/Collector/Network Gear

- Firmware removal and overwriting

- BSL Password Cracking

- Password/Crypto-key Capture

  - From Memory

  - Over I2C/SPI Bus

- More Man-In-The-Middle Attacks

Head End

- Not yet in scope for project, but...
  - Analyze Head-End System
    - Include Architecture and Code
    - Common IT Vulnerabilities?
    - Common Programming Errors?
  - Meter Impersonation?
    - False Data

Supporting Attacks:

- Crypto:
  - Steal from memory
  - Steal from circuitry (BUS attacks)
  - Crack over network
- BSL Cracking
  - Passwords
  - Bypassing Security Routines
- Firmware updates
  - Steal / Inject "Custom"
  - Stop "Security Bits"
- Timing and Power-manipulation Attacks
  - Skip/Stop execution of certain instructions
  - Manipulate erase procedures
  - Avoid setting the "Security Bits" during firmware upgrade
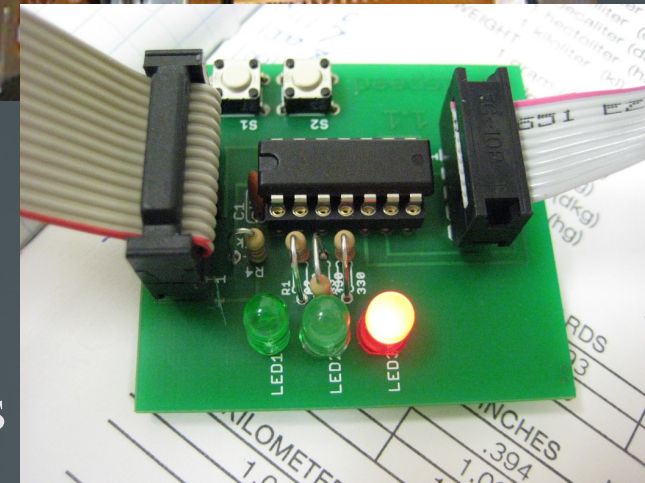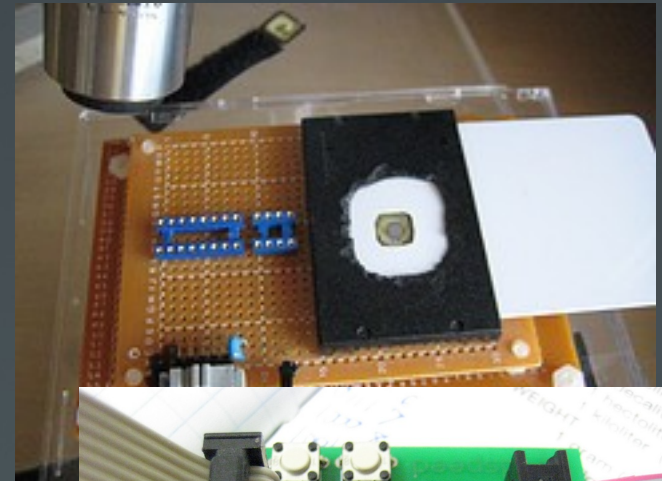
Control and Pwnership Metrics

- How damaging is any one vulnerability?
- Some architectures are supposedly more secure than others
- Prove it

Summary

- Identify key interfaces attackers can manipulate

- Analyze the outcome of that manipulation

- Test for Proof

- Evaluate Impact to Value-Streams