Hacking AMI
Problems in AMI

• Embedded systems have received limited attention from the security community
  • Little is known about hacking them (publicly)
  • AMI systems have received even less attention
  • Wild Wild West!

• Implications to Improperly Secured Non-Embedded Systems are Huge
  • Change the face of the western world...
AMI Embedded Systems

- Insecure data busses and serial connections
  - C12.22 bus
  - Data Capture, Injection (both directions)
    - Radios
    - MCU's
- Stealing/Replacing Keys In Memory
  - Network Encryption
  - Authentication and CA keys
- Blown JTAG Fuse Isn't Enough
  - Third-party labs remove top/allow microscopic access to chip
- Firmware-level vulnerabilities similar to x86 systems

- It’s the Latch!
Microscopic Probe

- Decapitated Chip
- Microtuned Placement
  - Access Memory
  - Reset the JTAG fuse
AMI Utility Premise (x86)

- Head-end, MDUS, ERP/OMS, SCADA, Workstations
- Standard Vulnerabilities:
  - Buffer Overflows
  - Format String Exceptions
  - Integer Under/Overruns
  - SQL-Injection / XSS / CSRF
  - Command Injection
  - Clear-text session/credential hijacking
  - Much much more
- Between System Components:
  - Thresholding is a must
    - Are you sure you want to shut off 100,000 meters?!
  - Firewalling is also a must
    - Allow only necessary communication between appropriate systems
    - Nothing that touches the Internet in any way can originate to head-end
AMI-SEC and ASAP

• AMI-SEC Taskforce
  • ASAP (AMI-SEC Acceleration Project)
  • Red Team Testing (hacking)
  • Darren Highfill <darren@enernex.com>
  • http://osgug.ucaiug.org/utilisec/amisec/

• Matthew Carpenter
  • InGuardians
  • ASAP Red Team Lead
  • matt@inguardians.com