Smart Electric Meters: Architectures, Vulnerabilities, and Mitigations

Stephen McLaughlin
2013 Trusted Infrastructure Workshop
Pennsylvania State University
Meter Data Management (for the last 100 years)
Meter Data Management (now and in the near future)

One Day

One Hour

Wednesday, June 5, 2013
One Day

One Hour

Systems and Internet Infrastructure Security Laboratory (SIIS)

Wednesday, June 5, 2013
Meter Data Management (now and in the near future)

- Peak Transient
- Peak Usage
- Hourly Average
- Outages
- Time of Use
- Dirunal patterns
- One Hour
- Power Quality
- Tampering
- Types of appliances
AMI - the justification

• Automated Meter Reading
  ‣ Pre-smart meter automated reading
  ‣ Outage notification and management

• Dynamic pricing schemes
  ‣ Time Of Use (peak load management)
  ‣ Maximum demand
  ‣ Demand response

• Flexible energy generation
  ‣ Enable consumer generation
  ‣ Alternative energy sources
Rest of this talk

• A smart meter is not trustworthy
Rest of this talk

• A smart meter is not trustworthy
  ‣ Neither is a smart meter deployment
Rest of this talk

- A smart meter is not trustworthy
  - Neither is a smart meter deployment
- Smart meters can be made trustworthy
• A smart meter is not trustworthy
  ‣ Neither is a smart meter deployment

• Smart meters can be made trustworthy(er)
Rest of this talk

- A smart meter is not trustworthy
  - Neither is a smart meter deployment
- Smart meters can be made trustworthy(er)
- Smart meters need to be trustworthy
Rest of this talk

• A smart meter is not trustworthy
  ▸ Neither is a smart meter deployment
• Smart meters can be made trustworthy(er)
• Smart meters need to be trustworthy
  ▸ for utilities and customers
Smart Meters
Meter Architectures

- **Cellular**
- **Internet**
- **PSTN**

**Utility Server**

**Backhaul Network**

**Collectors**

**Repeaters**

**Meter LAN 1:** Power Line Communication

**Meter LAN 2:** RF Mesh
Meter Anatomy

TCP/IP Stack
- WAN
- WLAN

Proprietary

I/O Handlers

MCU

Control Loop

Engine

C.T. / Sensor

Infrared Port

Disconnect Switch

LCD Display

Interface

Core

Firmware
Component Vendors

- Renesas - Controllers, Wireless cards
- Lantronix - Embedded TCP/IP
- Intel - With MMU!
- Atmel - BIOS, ROMs
- Simtek - RAMs
- Samsung - Flash
- Abacus - IR Probe
- Meter vendors - PCBs
- Lots of ???
Meter Lifecycle

• Arrive at utility
• Provisioning
• Association
• Normal Operation
  ‣ Accumulation of readings
  ‣ Forwarding to collector
• Breaks / hacked
• Field technician
  ‣ Reprovision / Rip and Replace
Meter Security Measures

• Secure channels: AES, 3DES
• Some auditing and alerting
• Physical security
  ‣ Tilt switches
  ‣ Lid and battery removal sensors
  ‣ Tamper seals
  ‣ Locks
Note for trust models

• A typical question is: “Do I trust this piece of hardware or software?”
Note for trust models

• A typical question is: “Do I trust this piece of hardware or software?”

• “Do I trust the environment it will be living in?”
Vulnerabilities
“The organization assesses the security requirements in the Smart Grid information system on an organization-defined frequency to determine the extent the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the Smart Grid information system.”

-p 117
“The organization assesses the security requirements in the Smart Grid information system on an organization-defined frequency to determine the extent the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the Smart Grid information system.”

-p 117
Penetration Testing

• Tried and true means of security assessment
  
  • 1. Try to break the computer system.
  • 2. Break the computer system.
  • 3. Fix the computer system.
  • 4. GOTO 1.
A means for pen-testing planning

Attack Trees

Tamper Usage Data

(a) Tamper Measurement
- Bypass Meter
  - Disconnect Meter
    - Log In and Clear Event History
      - A1.1
  - Clear Logged Events
- Reverse Meter
  - Meter Inversion
    - A1.2
- AND

(b) Tamper Stored Demand
- Reset Net Usage
  - A2.1
- AND
  - Meter Inversion
  - Log In and Reset Net Usage
    - A2.2
- AND
  - Physically Tamper Storage
    - A2.3
- AND

(c) Tamper in Network
- Intercept Communications
  - A3.1
- OR
  - Man in the Middle
    - A3.2
  - Spoof Meter
    - A3.3
Archetypal Trees

- **Idea**: can we separate the issues that are vendor independent from those that are specific to the vendor/device, e.g., access media?

- ... then reuse an archetypal tree as a base for each vendor specific *concrete tree*.
Pen Testing via Archetypal Trees

1. capture architectural description
2. construct archetypal trees (for each attacker goal)
3. capture vendor-specific description (for SUT)
4. construct concrete tree
5. perform penetration testing and graft leaves toward goals

3 Attack trees: fraud, DOS, disconnect, 2 "systems under test" (SUT)
Construction of Archetypal Trees

Forge Demand
Construction of Archetypal Trees

- Forge Demand
- Interrupt Measurement
Construction of Archetypal Trees

Forge Demand

Interrupt Measurement

OR

AND

Disconnect Meter

Meter Inversion

Erase Logged Events
Construction of Archetypal Trees

**Diagram**

- **FORGE DEMAND**
  - **INTERRUPT MEASUREMENT**
    - **DISCONNECT METER**
    - **METER INVERSION**
    - **ERASE LOGGED EVENTS**
      - **EXTRACT METER PASSWORDS**
      - **TAMPER IN FLIGHT**
    - **OR**
    - **AND**
Construction of Archetypal Trees

Forge Demand

Interrupt Measurement

OR

AND

Disconnect Meter

A1.1

Meter Inversion

A1.2

Erase Logged Events

OR

Extract Meter Passwords

Tamper in Flight
Construction of Archetypal Trees

Two rules for termination:

1. Attack is on a vendor-specific component

2. Target may be guarded by a protection mechanism
System Under Test

- PSTN connected collector
- ANSI C12.21
- “intrusion detection”

- 900 MHz wireless mesh collector/meter network
- Infrared “near-field” security for configuration port
Tamper Usage Data

(a) Tamper Measurement
   - Bypass Meter
   - Reverse Meter
   - Disconnect Meter
   - Clear Logged Events
   - Log In and Clear Event History
   - Recover Meter Passwords

(b) Tamper Stored Demand
   - Reset Net Usage
   - Meter Inversion
   - Log In and Reset Net Usage

(c) Tamper in Network
   - Physically Tamper Storage
   - Intercept Communications
   - Inject Usage Data
   - Man in the Middle
   - Spoof Meter

Intercept Communications

- Splice Into Meter I/O Bus
  - Via Telephone
  - Via Wireless Mesh

- Circumvent Intrusion Detection
- Interpose on Collector PSTN Link

- Initiate Session with Utility
  - Run Diagnostic up to Usage Data
- Identify Self as Meter
  - Complete Authentication Round

Spoof Meter
- Transmit Forged Usage Data

A1.1
A1.2
A1.3
A2.1
A2.2
A2.3
A3.1
A3.2
A3.3
A4.1
A4.2
A5.1
A6.1
Enabling Attacks (Fraud)

- Defeating modem “intrusion detection”
  - “off hook” events on the line are detected by sensing presence Foreign Exchange Office (FXO) of dial-tone voltage on the line.
  - current calls are dropped if off hook is detected
  - such events can simply be suppress easily by preventing voltage from arriving at the FXO
Valid Authentication Session

- Identify
- Nonce
- Hash(Password, Nonce)
- Hash(Password, Nonce')
Valid Authentication Session

Utility

Identify

Nonce

Hash(Password,Nonce)

Hash(Password,Nonce')

Valid Authentication Session
Enabling Attacks (Fraud)

• **Replay attack**: I can replay the nonce from a previous session to impersonate the meter.
Enabling Attacks (Fraud)

Valid Authentication Session

- Identify
- Nonce
- Hash(Password, Nonce)
- Hash(Password, Nonce')

Replay attack: I can replay the nonce from a previous session to impersonate the meter.

Replay Attack

- Identify
- Nonce
- Hash(Password, Nonce)
- Hash(Password, Nonce')

- All subsequent messages are the same
- Attacker need not know password
Targeted Disconnect AT

Targeted Disconnect

- OR
  - Directly Issue Disconnect
    - OR
      - Issue from Network
        - AND
          - Determine Target ID or Address
            - R1.1
        - AND
          - Issue Remote Disconnect
            - R1.2
      - Issue via Optical Port
        - AND
          - Recover Meter Passwords
            - R1.3
      - Issue Local Disconnect
        - R1.4
  - Tamper with Switch
    - AND
      - Remove Meter Cover
        - R2.1
      - Manipulate Switch to Disconnect
        - R2.2
    - Replace Tamper Seal
      - R2.3
Enabling Attacks (Disconnect)

- Physical tamper “evidence”
  - Limited tamper seals, *which enables* ...

- Passwords are stored in EEPROM
  - Physical access to the device can yield all of the data held in non-volatile memory, *which enables* ...

- Authentication secrets derived from passwords
  - Bypass the authentication system, *which enables* ...

- Issue disconnect command.

*Note: if you can break the dependency chain, you can prevent the attack, i.e., simple measures can often prevent complex attacks.*
Disconnect Concrete

- Targeted Disconnect
  - Directly Issue Disconnect
    - Issue from Network
      - Determine Target ID or Address
        - Mutually Authenticate with Meter
          - r2.1
    - Issue via Optical Port
      - Issue Remote Disconnect
        - r1.2
      - Trojan Optical Port
        - r1.1
  - Tamper with Switch
    - Remove Meter Cover
      - r2.1
    - Manipulate Switch to Disconnect
      - r2.2
    - Replace Tamper Seal
      - r2.3
- OR
- AND
- (AND)

Systems and Internet Infrastructure Security Laboratory (SIIS)

Wednesday, June 5, 2013
# Attacks Summary

## Energy Fraud in S1

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Description</th>
<th>Enabling Feature or Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>a2.1</td>
<td>Interpose between utility and collector</td>
<td>Telephone line may be accessible.</td>
</tr>
<tr>
<td>a2.2</td>
<td>Defeat modem intrusion detection</td>
<td>The mechanism cannot detect an FXS.</td>
</tr>
<tr>
<td>a4.1</td>
<td>Identify self as meter</td>
<td>A meter's ID is printed on its faceplate.</td>
</tr>
<tr>
<td>a4.2</td>
<td>Complete authentication round</td>
<td>Lack of nonce-tracking allows replayed authentication.</td>
</tr>
<tr>
<td>a5.1</td>
<td>Run diagnostic up to usage data</td>
<td>Protocol is standardized.</td>
</tr>
<tr>
<td>a6.1</td>
<td>Transmit forged usage data</td>
<td>Usage data is not integrity protected.</td>
</tr>
</tbody>
</table>

## Denial of Service in S2

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Description</th>
<th>Enabling Feature or Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>d1.1</td>
<td>Determine collector ID</td>
<td>The ID is transmitted in the clear.</td>
</tr>
<tr>
<td>d1.2</td>
<td>Initiate association with utility</td>
<td>Initialization uses a simple HELLO message.</td>
</tr>
<tr>
<td>d1.3</td>
<td>Receive and drop packets</td>
<td>The utility uses the IP address of the initiator of the most recent association.</td>
</tr>
<tr>
<td>d2.1</td>
<td>Determine meter listening port</td>
<td>The collector is responsive to port scanning.</td>
</tr>
<tr>
<td>d2.2</td>
<td>Allocate sessions until failure</td>
<td>The collector does not handle many sessions robustly.</td>
</tr>
</tbody>
</table>

## Targeted Disconnect in S1

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Description</th>
<th>Enabling Feature or Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>r1.2</td>
<td>Physically extract passwords</td>
<td>Passwords are stored in the clear in EEPROM storage.</td>
</tr>
<tr>
<td>r2.1</td>
<td>Mutually authenticate with meter</td>
<td>The encryption key is derived from passwords.</td>
</tr>
<tr>
<td>r2.2</td>
<td>Issue disconnect command</td>
<td>Administrative software is commercially available.</td>
</tr>
</tbody>
</table>
Meters as Monocultures
The Problem of Meter Monocultures
The Problem of Meter Monocultures
The Problem of Meter Monocultures
A Known Mitigation: Diversity

Software Diversity: *Uniqueness added to the implementation, but not interfaces of a program.*

Caveat: Uniqueness must depend on good randomness
## Limitations of Embedded Systems

<table>
<thead>
<tr>
<th>Diversity Technique</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Space Layout Randomization</td>
<td>No MMU</td>
</tr>
<tr>
<td>Software Fault Isolation</td>
<td>Requires some policy</td>
</tr>
<tr>
<td>Non-Executable Stacks</td>
<td>No NX bit</td>
</tr>
<tr>
<td>Stack Cookies</td>
<td>Check code not segmented</td>
</tr>
<tr>
<td>Address Encryption</td>
<td>Works, but failed exploits can cause random errors</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Firmware Type</th>
<th>Processor Type</th>
<th>MMU</th>
<th>Privileged Mode</th>
<th>NX Bit</th>
<th>RAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repeater Controller</td>
<td>Renesas M16C</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>20KB</td>
</tr>
<tr>
<td>Wireless Mesh</td>
<td>Renesas H8S</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Embedded TCP/IP</td>
<td>Lantronix DSTni-EX 186</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>256KB</td>
</tr>
<tr>
<td>Gateway Controller</td>
<td>Intel i386EX</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>8MB</td>
</tr>
</tbody>
</table>
More Embedded Challenges

• Diversity scheme hardness depends on secret size, which is related to machine word size.

• Smart meter components range from 32- down to 8-bit MCUs.

• This will affect the layout of some data structures in 8- and 16-bit systems, where multiple machine words will be needed to store the diversified value.
Address Encryption

Normal Dereference

Stack

Local Variables

\[ R \oplus K \]

Previous Frame

Registers

\[ R \oplus K \]

\[ \oplus K \]

\[ R \]

ret, jmp, etc.

Exploit Dereference

Stack

Local Variables

\[ \text{EXPLOIT} \]

Previous Frame

Registers

\[ R' \]

\[ \oplus K \]

\[ R' \oplus K \]

ret, jmp, etc.

What is normally a fault will cause unpredictable errors in embedded architectures with single, real-mode address spaces.
Redundant Address Encryption

For three keys on a 16 bit MCU:
- $2^{48}$ probes to compromise
- $2^{32}$ probes to random error

A 15,000 node deployment that is rate limited to 3 request/second for each meter requires approx. 10 years to fully compromise when using three keys.
Binary Instrumentation

• Feasible for embedded smart meters:
  ‣ Statically linked code
  ‣ Explicit call and return instructions
  ‣ Loose performance constraints

• Code size must be minimized!

Original function call:

```
push A ; Save address
jmp B ; Perform branch
```

Instrumented function call:

```
mov D [key1_addr] ; D = K_1
mov C A ; C = A
xor C D ; C = C XOR D
push C ; Save encrypted address
mov D [key2_addr] ; D = K_2
mov C A ;
xor C D ; Second redundant encryption
push C ;
mov D [key3_addr] ; D = K_3
mov C A ;
xor C D ; Third redundant encryption
push C ;
jmp B ; Perform branch
```
Rate limiting compromise

• Triple redundant address encryption
• Small deployment \( \sim 15,000 \)
• Attacker can probe each meter 3 times per minute
• 10 years to compromise deployment
• \( \sim .8\% \) of meters in a month
  ‣ A month of 24/7 probing to all meters would hopefully be noticeable ...
• Realistically, probes can be limited to a few a day.
Additional Challenges
Privacy

- Fine-grained power consumption data can reveal appliance usage!

- Solutions
  - Privacy preserving protocols (Requires trust in meter)
  - Battery-based load modifications (No trust in meter)
Trustworthy foundations

• Cummulative Attestation Kernels
  ‣ LeMay et al.

• Physical tamper detection
  ‣ McLaughlin et al. - AMIDS

• Pen testing along with check list style security ...
NERC CIP Overview

Access Points

Electronic Security Perimeter(s)

Critical Cyber Assets

😊 The Responsible Entity

CIP-007-3
Systems Security Management
**R2.** Ports and Services — The Responsible Entity shall establish, document, and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

**R2.1.** The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

Describe, in narrative form, how you meet compliance with this requirement:

*(Registered Entity Response Required)*
What about ports the Responsible Entity never knew were enabled in the first place?
Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

Was the anti-virus software correctly configured? Can malware disable the anti-virus software?
Need for a new type of regulation

- Attack trees can standardize pen-testing by combining different expert’s knowledge using the AND/OR connectives.
- The *leaves* of the attack trees form an auditable list of attacks that should be attempted against a system.
- The root (goal) of the attack tree specifies the impact of a vulnerability.
- Attack trees are succinct and unambiguous.
Thanks!

smclaugh@cse.psu.edu