Embedded Firmware Diversity for Smart Electric Meters

Stephen McLaughlin, Dmitry Podkuiko, Adam Delozier, Sergei Miadzvezhanka, and Patrick McDaniel
Smart Meters

Electromechanical

Smart Meter
3 Concerns

**Fraud** - Hacking meters to reduce energy bill

**Privacy** - Using detailed load profiles to determine behavior

**Blackout** - Exploiting large numbers of meters and cutting power
The Problem of Meter 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

### Diversity Technique

<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>No protected supervisor mode</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>

### Firmware Type

<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

\[ R \oplus K \]

\[ \oplus K \]

\[ R \]

\[ \text{ret, jmp, etc.} \]

Exploit Dereference

Stack

EXPLOIT

Local Variables

Previous Frame

Registers

\[ R' \]

\[ \oplus K \]

\[ R' \oplus K \]

\[ \text{ret, jmp, etc.} \]

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
```
Challenges / Updates

Deployment – Endpoint
- Electric meter supply chain secured
- 138 curb meters set with incorrect programming
- Early indication that 900 MHz may trip customer GFI
- Bakersfield substation bank work is requiring meter redeployment of about 29,000 endpoints

The project has been using interfaces which have not completed testing (60, 50, 104, 66, 67) to enable AMS Ops to discover and initialize installed meters. The conversion approach for the MDMS needs to be revisited to determine if the right approach is to “initialize” the MEM go live weekend, or use ORT to enable “cut-over”.

<table>
<thead>
<tr>
<th>Risks</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation of new technology does not perform as intended. Key drivers: IT systems do not scale to meet volumes, Equipment fails at a higher rate than anticipated</td>
<td>Billing errors, customer complaints, inability to meet endpoint deployment goals</td>
</tr>
</tbody>
</table>
Summary

• Meter monocultures
  ‣ Highly exposed nodes
  ‣ Hard to configure
  ‣ Same pandemic problem as other monocultures

• Diversity
  ‣ Well understood exploit mitigation
  ‣ Significantly slows large scale exploit attempts
  ‣ Embedded diversity schemes will present their own challenges while facing less stringent performance requirements than traditional diversity techniques
Thank You

Seed Questions

• Are there suggestions for approaches besides diversity for mitigating large-scale meter exploitation?

• How could we reduce meter TCB, thus reducing the amount of code that needs to be diversified?

• Should we build redundant address encryption or explore additional diversity techniques?

http://www.cse.psu.edu/~smclaugh
http://siis.cse.psu.edu