Evaluating Effectiveness of an Embedded System Endpoint Security Technology on EDS

Michael Siegel, Gregory Falco, Keman Huang, Weilian Chu, Elizabeth Reilly, Mayukha Vadari
Digitization of Industrial Sector

- Increased demand on utilities industry
- More optimized distribution required
- Digitization of system endpoints
- Two-way communication between consumer & distributor
Industrial IoT EndpointDevices

- Single user device, interacts with larger system of devices
- Interacts with people, usually has IP address
- Smart meters, gas pipes, oil tanks, wind turbines
- Vulnerable to malicious access & tampering
Example - Automated Gas Storage Tank

- Protocol & port # available
- Exact address
- Database information & timestamp

<table>
<thead>
<tr>
<th>TANK</th>
<th>PRODUCT</th>
<th>VOLUME</th>
<th>TC VOLUME</th>
<th>ULLAGE</th>
<th>HEIGHT</th>
<th>WATER</th>
<th>TEMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DIESEL</td>
<td>2529</td>
<td>2522</td>
<td>1481</td>
<td>57.92</td>
<td>0.00</td>
<td>65.86</td>
</tr>
<tr>
<td>2</td>
<td>KEROSENE</td>
<td>576</td>
<td>575</td>
<td>1429</td>
<td>31.65</td>
<td>0.00</td>
<td>64.55</td>
</tr>
<tr>
<td>3</td>
<td>SUPER</td>
<td>2978</td>
<td>2969</td>
<td>7022</td>
<td>32.48</td>
<td>0.00</td>
<td>63.66</td>
</tr>
<tr>
<td>4</td>
<td>REGULAR</td>
<td>4059</td>
<td>4043</td>
<td>5941</td>
<td>40.88</td>
<td>0.00</td>
<td>65.47</td>
</tr>
</tbody>
</table>
Example - Automated Gas Storage Tank

- ASN revealed

- Many devices have open SSH ports that allow for public access

- IP address vulnerable to ssh entry through password crackers
Consequences of Security Compromise

- Information & power theft
- Possibility of malicious control
- Disruption of distribution service to consumers
- Physical and technological infrastructure damage
- User security compromised
Why are Industrial IoT endpoints hard to secure?

- Can’t defend against users with malicious intent
- Industrial endpoints low in memory and storage
- Not enough computation power for conventional IoT security measures
Our Project - Overview

Lightweight Security Architecture

Blockchain Server
Lightweight Security Architecture

- Software enforce security policies from within device
- Written in C & Bash
- Lock down endpoint OS to limit its capabilities
- Prevents unauthorized programs from running in OS
- Small footprint -> works within the kernel -> doesn’t require network access
- Intensive computations are performed in the cloud
Blockchain Technology

- Foundation for command & control
- Sends security updates, stores them in secure & decentralized channel
- Provided by Bitcoin Blockchain
- Controls applications that are black/whitelisted
- Does not interfere with firmware -> no system downtime during updates
Project Demo: Mirai

- Mirai is a famous malware botnet that targets Linux routers
- Ran open source software OpenWRT on Linux virtual machine to simulate a router
- Compiled our security software and installed onto OpenWRT VM
- Attempted to run Mirai botnet on the VM
Project Demo: Mirai

- Software constantly checks for traces of Mirai
- Software has kernel privilege within OS
- Any process outside core system is verified over blockchain
- Any program that doesn’t pass through the black/whitelist is killed
<table>
<thead>
<tr>
<th>Year</th>
<th>Goal Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 2017</td>
<td>Port existing software onto router</td>
</tr>
<tr>
<td></td>
<td>Software updates via VPN</td>
</tr>
<tr>
<td>March 2018</td>
<td>Run software on smart meters</td>
</tr>
<tr>
<td></td>
<td>Develop heuristics for machine learning analysis</td>
</tr>
<tr>
<td>April 2018</td>
<td>Clustering algorithms to detect malicious IP addresses</td>
</tr>
<tr>
<td>May 2018</td>
<td>Port software onto Windows-based devices</td>
</tr>
</tbody>
</table>
Industry Partners

Schneider Electric

Avangrid

Philips Healthcare

ExxonMobil

Engie