Spire:
Intrusion-Tolerant SCADA for the Power Grid

Amy Babay*, Thomas Tantillo*, Trevor Aron, Yair Amir
June 25, 2017

Distributed Systems and Networks Lab

Department of Computer Science
Johns Hopkins University
The move to IP makes SCADA vulnerable on several fronts:

• **SCADA system** compromises
  – SCADA Master – *system-wide* damage
  – RTUs, HMIs – limited local effects

• **Network** level attacks
  – Routing attacks that disrupt or delay communication
  – *Isolating critical components* from the rest of the network

• Therefore, SCADA systems must ensure *continuous availability* and *correct operation* in the presence of compromises and attacks at both the *system* and *network* level
Spire Overview

- Spire is a SCADA system that **continues to work** even if some critical components have been **compromised**
- **Intrusion tolerance** as the core design principle protecting several different layers of the system:
  - Intrusion-tolerant network
  - Intrusion-tolerant consistent state
  - Intrusion-tolerant SCADA Master
- Combines **proven open-source** components with new system components **built from scratch** to provide a **complete** top-to-bottom solution
- Open Source - [http://dsn.jhu.edu/spire](http://dsn.jhu.edu/spire)
• **Spines** ([http://spines.org](http://spines.org))
  – Intrusion-Tolerant Network

• **Prime** ([http://dsn.jhu.edu/prime](http://dsn.jhu.edu/prime))
  – Intrusion-Tolerant Replication – BFT with performance guarantees under attack

• **SCADA Master** ([http://dsn.jhu.edu/spire](http://dsn.jhu.edu/spire))

• **PLC/RTU Proxy** ([http://dsn.jhu.edu/spire](http://dsn.jhu.edu/spire))

• **Pvbrowser-based HMI** ([https://pvbrowser.de/pvbrowser/index.php](https://pvbrowser.de/pvbrowser/index.php))
  – Rainer Lehrig and his group

• **OpenPLC** ([http://www.openplcproject.com](http://www.openplcproject.com))
  – PLC Emulation – (Thiago Alves, Tommy Morris) University of Alabama, Huntsville

• **Multicompiler** ([https://github.com/secsystems/sl/multicompiler](https://github.com/secsystems/sl/multicompiler))
  – Diversity (Michael Franz group at UC Irvine, Immunant)
Spire Architecture: Single Control Center

Internal Spines Network

- SCADA Master
  - Prime
- SCADA Master
  - Prime
- SCADA Master
  - Prime
- SCADA Master
  - Prime

External Spines Network

- pvbrowser HMI
- RTU / PLC Proxy
- RTU
- PLC
Pvbrowser is an open source SCADA software solution

- Used in real-world deployments: Romanian power distribution system covering 10,000 km² with 50 power switches
Spire in Action

Spire as used in the DoD ESTCP experiment  March-April 2017
DoD ESTCP Experiment

- DoD ESTCP project at Pacific Northwest National Labs
  - Conducted by Resurgo
  - 3/27/17 to 4/7/17
- Comparing NIST-compliant SCADA architecture with Spire
  - Each attacked by Sandia National Labs red team
DoD ESTCP Results

- NIST-compliant system completely taken over
  - MITM attack from corporate network
  - Direct access to PLC from operational network
- Spire completely unaffected
  - Attacks in corporate and operational network
  - Given complete access to a replica and code
  - Red team gave up after several days
Intrusion Tolerance State-of-the-Art in Research

- $3f+2k+1$ total replicas
- $2f+k+1$ connected correct replicas required to provide bounded delay

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Correct</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proactive Recovery (PR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disconnected/Downed Site</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disconnected/Downed Site + PR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion + PR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disconnected/Downed Site + Intrusion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disconnected/Downed Site + Intrusion + PR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Bounded Delay

- Bounded Delay, except when rejuvenating any correct replica
- Eventual Progress – Human in the loop. Potentially powering up cold backup control center
- Eventual Progress – No bound. Network has to heal, crash has to be repaired, and/or intrusion needs to be cleansed

Incorrect System
Novel Resilient Configurations (7/7)

**3+3+3+3** (progress: 7)

- **Complete solution for 4 total sites:** (2 control centers, 2 data centers)
- **Sweet-spot** balancing the number of data center sites, the number of total replicas, and the communication overhead

---

**Operations:**

- **Control Center 1**
  - Spines
  - HMI
  - SM
  - SM
  - SM

- **Data Center 1**
  - SM
  - SM
  - SM

- **Control Center 2**
  - Spines
  - HMI
  - SM
  - SM
  - SM

- **Data Center 2**
  - SM
  - SM
  - SM

---

- **Substation**
  - RTU
  - Physical Equipment

---

**Legend:**

- **Bounded Delay**
  - Bounded Delay, except when one control center is down and the other control center has only one uncompromised replica and that replica is currently rejuvenating
  - Bounded Delay, except when rejuvenating any correct replica
  - Eventual Progress – Human in the loop. Potentially powering up cold backup control center
  - Eventual Progress – No bound. Network has to heal, crash has to be repaired, and/or Intrusion needs to be cleansed
  - Incorrect System
Wide Area: Update Latency Histogram

- 30-hour wide-area deployment of 3+3+3+3 configuration
  - Control centers at JHU and SVG, data centers at WAS and NYC
  - 10 emulated RTUs sending periodic updates
  - 1.08 million updates (108K from each RTU)
  - Over 99.999% of updates delivered within 100ms (56ms average)
The Spire Forum

- Forum focused on Open Source Intrusion-tolerant control systems for the power grid
- Please join the Spire forum if interested

- [http://dsn.jhu.edu/spire](http://dsn.jhu.edu/spire)