A Defense-in-Depth Model for Industrial Control Systems

Dr. Jess Smith
Secure Engineering Division
Stuxnet

Natanz, Iran
~1,000 centrifuges destroyed
Ukraine
23 Dec 2015

134 MW of load shed
225,000 customers without power
### ICS Security is Different from Information Security

<table>
<thead>
<tr>
<th></th>
<th>Info Sec</th>
<th>ICS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goal</strong></td>
<td>Protect secret information</td>
<td>Maintain service</td>
</tr>
<tr>
<td><strong>Threat vectors</strong></td>
<td>Remote electronic</td>
<td>Remote electronic and physical</td>
</tr>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td>Widespread but usually detectable</td>
<td>Less widespread, but tools to detect are still developing</td>
</tr>
<tr>
<td><strong>Worst Case Consequences</strong></td>
<td>Loss of money, trust</td>
<td>Loss of life</td>
</tr>
</tbody>
</table>
An ICS Defense in Depth Model

• ICS have many critical points – “keeping the lights” on can be anywhere in generation, transmission, or distribution.

• This means our defense in depth model needs to be realigned and redesigned.

• Each level has its own needs and priorities, creating levels within levels.
Humans and Machines

Digital Machines

Analog Machines
Level 0 – Physical

Includes: Valves, Breakers, Sensors

Focus: Availability!

Security: Physical
Level 1 – Protection

Includes: Relays, meters, support devices

Focus: Availability

Security: Physical, alarms, passwords
Level 2 – Automation

Includes: PLCs, Communications Processors, some relays
Focus: Availability, Integrity

Security: Alarms, syslog, passwords, physical
Level 3 – Access

Includes: Firewalls, remote access devices

Focus: Confidentiality, Integrity

Security: Syslog, alarms, firewall rules, multifactor authentication
Level 4 – SCADA

Includes: Networking devices, HMIs, historians, syslog servers, ...
Focus: Integrity

Security: Standard networking and desktop TTP
Level 5 – Perimeter

Includes: Firewalls, VPNs, possibly also physical perimeter security
Focus: Confidentiality

Security: Firewall rules, multifactor authentication, physical protections
Level 6 – People

Includes: Policy, procedure, risk management, training …
Focus: All of the above

Security: Training, controls, auditing, incident response
Security is Dynamic

- Continuous Monitoring
- Risk Analysis
- Auditing and Testing
- Patches and Updates
Questions?

Jess_Smith@SELinc.com

J. Smith, N. Kipp, D. Gammel, and T. Watkins,
United States Department of Defense System