Operations: Cybersecurity – What To Know
BCWWA SCADA & IT Conference
2019-11-20
INDUSTRIAL CYBERSECURITY

Priorities:

» Safe physical operations

» Reliable operations
  • Continuous
  • Correct
  • Efficient
  • No equipment damage

At many sites, security programs are part of safety programs
HUMAN MACHINE INTERFACE (HMI)
ISA SP99 (PURDUE) MODEL

Level 4
Enterprise Systems
(Business Planning & Logistics)

Level 3
Operations Management

Level 2
Supervisory Control

Level 1
Safety and Protection

Level 0
Process
(Equipment Under Control)

Industrial Automation and Control Systems
DATA VS MONITORING VS CONTROL

- IT history: leger books / accounting data / transactions
- Industrial network history
  - Gauges = monitoring = IT data
  - Switches & dials = control = safety/reliability critical
- IT experts say “it’s all data,” but this blinds us to crucial difference between monitoring and control
- Correct control is vital to physical safety and physical reliability

*Control is not AIC, CIA or “IT data” – control is really important*
FIRST THREE LAWS OF SCADA SECURITY

» Nothing is secure
» All software can be hacked
» All cyber attacks are information, and every bit of information can be an attack

In the worst case a compromised CPU will issue every unsafe instruction to the physical process that the CPU is physically able to issue
ATTACKERS PREFER PERMISSIONS

- Remote access attacks piggy-back on legitimate sessions / permissions, such as remote access sessions
- Phishing attacks steal credentials
- Pass-the-hash attacks re-use existing credentials
- Databases & other servers permit remote execution
- Remote Access Trojans (RATs) provide remote control to understand target, steal credentials & make next move

Why write code to exploit vulnerabilities when attackers can log in and execute what they want?
## WHO’S COMING AFTER US

<table>
<thead>
<tr>
<th>Threat</th>
<th>Resources</th>
<th>Attacks</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation-State Military</td>
<td>Nearly unlimited</td>
<td>Autonomous Targeted Malware</td>
<td>Stuxnet, Shamoon(?)</td>
</tr>
<tr>
<td>Intelligence Agencies</td>
<td>Professional</td>
<td>Remote Control – Exploit Vulns</td>
<td>Black Energy, TRITON</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>Skilled Amateur</td>
<td>Remote Control – Exploit Permissions</td>
<td>Ukraine(?), Anonymous</td>
</tr>
<tr>
<td>SCADA Insiders</td>
<td>Amateur</td>
<td>Exploit Permissions</td>
<td>Maroochy</td>
</tr>
<tr>
<td>Organized Crime</td>
<td>Professional</td>
<td>Indiscriminate Malware, Exploit Known Vulns</td>
<td>Zeus, Ransomware</td>
</tr>
<tr>
<td>Corporate Insiders</td>
<td>Amateur</td>
<td>Exploit Permissions</td>
<td>Fake Vendor Fraud</td>
</tr>
</tbody>
</table>
FAILED DEFENSE IN DEPTH

- Start with HFLI attacks – firewalls, AV, patch programs
- Insiders: background checks, detailed auditing - deterrence
- IDS cost: false alarms
- IDS takes average 2-3 months while attacker has remote control
- Data exfiltration prevention does not detect sabotage

Can’t restore equipment & human lives “from backups”

<table>
<thead>
<tr>
<th>Threat</th>
<th>Defense</th>
<th>Cost</th>
<th>Eff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation-State Military</td>
<td>Escalate to national agencies</td>
<td>n/a</td>
<td>Not</td>
</tr>
<tr>
<td>Intelligence Agencies</td>
<td>IDS / Exfiltration prevention</td>
<td>$$$</td>
<td>Poor</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>Intrusion detection systems</td>
<td>$$$</td>
<td>Fair</td>
</tr>
<tr>
<td>ICS Insiders</td>
<td>Physical security, detailed auditing</td>
<td>$$</td>
<td>Good</td>
</tr>
<tr>
<td>Organized Crime</td>
<td>Encryption, AV, security updates</td>
<td>$$$</td>
<td>Good</td>
</tr>
<tr>
<td>Corporate Insiders</td>
<td>Firewalls, role-based permissions</td>
<td>$</td>
<td>Good</td>
</tr>
</tbody>
</table>
INTERNET / FIREWALLS

» Internet = hosts + routers + connections between them – all talking using the Internet Protocol (IP)

» Hosts – sources & destinations of IP messages

» Routers – figure out which connection to send each message down, to get message to its destination

» Firewalls – routers with filters
  • Filter (software) looks at each message
  • Decides if it is allowed
  • If so, hands to router to send

For details – see my ISA InTech paper “13 Ways To Break A Firewall”
SECURE OPERATIONS TECHNOLOGY

IT-SEC:
protect the information

SEC-OT:
protect physical operations
from the information
OFFLINE CONTROLS

Offline Survey
Test Beds
Removable Media
Removable Devices
New Cyber Assets
Insider Attacks
Deceived Insiders
Nonessential Equipment
REMOVABLE MEDIA

» Media = information storage without an embedded CPU – CDs, DVDs, floppies

» Software policies preventing media from mounting

» Multi-AV-scanning kiosks at physical perimeters

» Physically blocking or removing devices on all equipment except kiosks

» Publish scanned files to test bed or control-critical network

Removable media is the most frequent source of common malware on industrial networks
REMOVABLE DEVICES

» Vendor laptop program
» Network Access Control
» Alerts
» Contracts forbidding devices
» Labelling control-critical devices
» USB charger program – reduces temptation

SEC-OT sites report that these programs essentially eliminate the use of IT-exposed removable devices
DECEIVED INSIDERS

» Well-meaning insiders can be deceived into acting on false information with physical consequences

» Insiders must be trained to be suspicious of and seek verification of externally-sourced information and information that has traversed a non-critical network

Emailed information and instructions should be verified verbally before taking action
Unidirectional Security Gateways are a combination of **hardware and software**

- The hardware is physically able to send information in only one direction
- The software replicates servers & emulates devices from the OT network to the IT network
- IT replicas are normal participants in IT networks
- All cyber attacks are information – no attack, no matter how sophisticated, can propagate back to the industrial network through the gateway
Waterfall enables secure operations, preventing remote cyber attacks on industrial, OT and mission-critical environments.

Customers worldwide use Waterfall's array of OT security products to integrate OT networks with external environments.

We provide the strongest security solutions that fit the need: access to operations data, OT security monitoring, and disciplined remote access and remote control.

**Redefining OT security with Waterfall’s innovative Unidirectional Gateway technologies**
Guests from across the industrial security space

**Vendors**: issues, technology & approaches

**Government agencies**: programs & resources

**Owners & operators**: priorities & approaches

**Other**: recruiters, educators & more

https://waterfall-security.com/podcasts
SECURE OPERATIONS TECHNOLOGY

- **Thorough** – address all attack vectors – offline and online
- **Robust** – physical & hardware protections, not just software
- **Disciplined** – not waiting on “edge of seat” for actionable intel
- **Futureproof** – cyber attacks will always be information