Operational Technology Cybersecurity

Major Matthew G. Sherburne, P.E.

17 JULY 23
Agenda

1) Purpose
2) About Me
3) Terminology
4) Past OT cybersecurity events
5) Purdue Model
6) MITRE ATT@CK ICS Matrix
7) Federal Level OT Security Documents
8) OT Cybersecurity Documents
9) Industry Specific Guidance
10) Some training programs
11) Q and A
Purpose

• Inform SAME membership about growing focus on OT cybersecurity programs; where to look and how to start.
About Me

• West Point BSEE ’07

• Virginia Tech MSEE ’15
  o Thesis: “Micro Moving Target IPv6 Defense for 6LoWPAN and the Internet of Things”

• Member of IEEE Antennas and Propagation Society and Communications Society

• Amateur Radio Extra Class Operator – KF4WZB

• Licensed Professional Engineer (State of Missouri) since ’19

• Involved in OT cybersecurity since July ’19
  o Former Cyber Protection Team (CPT) Lead – Army OT Focus
• ICS – Industrial Control Systems
• SCADA – Supervisory Control and Data Acquisition
• FRCS – Facility Related Control Systems
• IACS – Industrial Automation and Control Systems
• SIS – Safety Instrumented System
• OT – Operational Technology (catch-all for ICS/SCADA/FRCS/IACS)
• PLC – Programmable Logic Controller
• RTU – Remote Terminal Unit
### Past OT Cybersecurity Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Target</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Australian Sewage Plant</td>
<td>Insider</td>
</tr>
<tr>
<td>2010</td>
<td>Iran Uranium Enrichment</td>
<td>Stuxnet</td>
</tr>
<tr>
<td>2013</td>
<td>ICS Supply Chain attack</td>
<td>Havex</td>
</tr>
<tr>
<td>2014</td>
<td>German Steel Mill</td>
<td>BlackEnergy, KillDisk</td>
</tr>
<tr>
<td>2015</td>
<td>Ukraine Power Grid</td>
<td>CrashOverride</td>
</tr>
<tr>
<td>2016</td>
<td>UKrania Substation</td>
<td>NotPetya</td>
</tr>
<tr>
<td>2017</td>
<td>IoT DDos attack</td>
<td>BrickerBot</td>
</tr>
<tr>
<td>2017</td>
<td>Global shipping company</td>
<td>WannaCry</td>
</tr>
<tr>
<td>2017</td>
<td>Health care, Automotive, many others</td>
<td>TRITON/TRISIS</td>
</tr>
<tr>
<td>2017</td>
<td>Saudi Arabia Petrochemical</td>
<td>LockerGaga</td>
</tr>
<tr>
<td>2019</td>
<td>Norwegian Aluminum Company</td>
<td></td>
</tr>
</tbody>
</table>

Source: www.awa.csis.org/programs/technology-policy-program/significant-cyber-incidents

May 2021 Colonial Pipeline ➔

IT Exploitation can lead to OT disruption, even if not directly targeted.

Figure Source: https://industrial-software.com/community/news/virsec-analysis-of-the-colonial-pipeline-attack/

Table 1: Some notable cyberattacks impacting IACS, [https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf](https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf)
Purdue Model

https://www.sans.org/blog/the-risks-of-an-it-versus-ot-paradigm/
## MITRE ATT@CK ICS Matrix

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Evasion</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Inhibit Response Function</th>
<th>Impair Process Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>Change Operating Mode</td>
<td>Hardcoded Credentials</td>
<td>Exploitation for Privilege Escalation</td>
<td>Change Operating Mode</td>
<td>Network Connection Enumeration</td>
<td>Default Credentials</td>
<td>Adversary-in-the-Middle</td>
<td>Commonly Used Port</td>
<td>Activate Firmware Update Mode</td>
<td>Brute Force I/O</td>
<td>Damage to Property</td>
</tr>
<tr>
<td>Exploitation of Remote Services</td>
<td>Execution through API</td>
<td>Module Firmware</td>
<td>Indicator Removal on Host</td>
<td>Remote System Discovery</td>
<td>Hardcoded Credentials</td>
<td>Data from Information Repositories</td>
<td>Standard Application Layer Protocol</td>
<td>Block Command Message</td>
<td>Module Firmware</td>
<td>Denial of View</td>
<td></td>
</tr>
<tr>
<td>Internet Accessible Device</td>
<td>Hooking</td>
<td>System Firmware</td>
<td>Rootkit</td>
<td>Wireless Sniffing</td>
<td>Program Download</td>
<td>I/O Image</td>
<td>Data Destruction</td>
<td>Denial of Service</td>
<td>Loss of Protection</td>
<td>Loss of Safety</td>
<td></td>
</tr>
<tr>
<td>Remote Services</td>
<td>Modify Controller Tasking</td>
<td>Valid Accounts</td>
<td>Spoof Reporting Message</td>
<td>Remote Services</td>
<td>Monitor Process State</td>
<td>Valid Accounts</td>
<td>Point &amp; Tag Identification</td>
<td>Program Upload</td>
<td>Screen Capture</td>
<td>Loss of View</td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Native API</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rogue Master</td>
<td>Scripting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>User Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transient Cyber Asset</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

as of 06MAY22

https://attack.mitre.org/matrices/ics/
Federal Level OT Security Documents

• Homeland Security Presidential Directive 7, 17DEC03
  o “This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.”

• Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, 12FEB13

  o Identifies 16 critical infrastructure sectors

• Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 11MAY17

• DHS CISA Cybersecurity Incident and Vulnerability Response Playbooks, Nov ‘21

• NSA,CISA: How Cyber Actors Compromise OT/ICS and How to Defend Against It, Press Release – 22SEP2022
  o https://media.defense.gov/2022/Sep/22/2003083007/-1/-1/0/CSA_ICS_Know_the_Opponent_.PDF
OT Cybersecurity Documents

- **NIST 800-82, Rev 3 (draft) – Guide to Operational Technology (OT) Security**

- **NIST Cybersecurity Framework, FEB14**
  - https://www.nist.gov/cyberframework
  - Identify, Protect, Detect, Respond, Recover

- **ISA99.02.01/IEC 62443: Security for Industrial Automation and Control Systems, JUN20**
Industry Specific Guidance

- North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP)
  - https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx

- Transport Security Administration (TSA) Pipeline Security Guidelines, April 21
Training your Workforce (a way)

DHS CISA Virtual Training
• https://www.cisa.gov/ics-training-available-through-cisa

In-person training at Idaho Falls, Idaho
• Industrial Control Systems Cybersecurity 301L (next 4 day course May 15-18)
• Industrial Control Systems Evaluation 401L (next 3 day course May 23-25)
• https://www.cisa.gov/ics-training-calendar

SANS Institute Training
• https://www.sans.org/cyber-security-courses/?focus-area=industrial-control-systems-security
• SANS ICS410: ICS/SCADA Security Essentials
  • Associated Cert: GIAC Global Industrial Cyber Security Professional
• SANS ICS515: ICS Visibility, Detection, and Response
  • Associated Cert: GIAC Response and Industrial Defense
• SANS ICS612: ICS Cybersecurity In-Depth
• SANS ICS456: Essentials for NERC Critical Infrastructure Protection
  • Associated Cert: GIAC Critical Infrastructure Protection
• SANS ICS418: ICS Security Essentials for Managers
(f) SERVICE RESPONSIBILITIES. [abridged]

(1) ensure that relevant local network and cybersecurity forces are responsible for defending operational technology.

(2) ensure that relevant local operational technology-focused system operators, network and cybersecurity forces, mission defense teams and other service-retained forces, and cyber protection teams are appropriately trained,

(3) ensure that all Defense Critical Assets and Task Critical Assets are monitored and defended by Cybersecurity Service Providers,

(4) ensure that operational technology is appropriately sensored and appropriate cybersecurity defenses,

(5) implement Department of Defense Chief Information Officer policy germane to operational technology,

(6) plan for, designate, and train dedicated forces to be utilized in operational technology-centric roles across the military services and United States Cyber Command,

(7) ensure that operational technology, as appropriate, is not easily accessible via the internet and that cybersecurity investments accord with mission risk to and relevant access vectors for Defense Critical Assets and Task Critical Assets.

The cybersecurity of Operational Technology and Critical Resources is a major focus area for the Army.
BACKUP SLIDES
<table>
<thead>
<tr>
<th>Date</th>
<th>Target</th>
<th>Method</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Australian Sewage Plant</td>
<td>Insider</td>
<td>Release of 265,000 gallons of untreated sewage into local parks and rivers</td>
</tr>
<tr>
<td>2010</td>
<td>Iran Uranium Enrichment</td>
<td>Stuxnet</td>
<td>1st reported cyber attack to cause physical damage</td>
</tr>
<tr>
<td>2013</td>
<td>ICS Supply Chain attack</td>
<td>Havex</td>
<td>Wide-spread ICS reconnaissance – 1st identified malware specifically geared to look at common ICS TCP port traffic</td>
</tr>
<tr>
<td>2014</td>
<td>German Steel Mill</td>
<td></td>
<td>2nd Cyber attack to cause physical damage and confirmed by a legitimate government source</td>
</tr>
<tr>
<td>2015</td>
<td>Ukraine Power Grid</td>
<td>BlackEnergy 3</td>
<td>Loss of power to 230,000 customers for 6 hours. (30 substations taken offline)</td>
</tr>
<tr>
<td>2016</td>
<td>Ukraine Substation</td>
<td>Industroyer</td>
<td>Automated attack that hit a single transmission substation in northern Kiev</td>
</tr>
<tr>
<td>2017</td>
<td>Global shipping company</td>
<td>NotPetya</td>
<td>$300 million loss and global delays for Maersk</td>
</tr>
<tr>
<td>2017</td>
<td>IoT DDoS Attack</td>
<td>BrickerBot</td>
<td>Reportedly destroyed 10 million IoT devices and influenced the Silex malware two years later</td>
</tr>
<tr>
<td>2017</td>
<td>Saudi Arabia Petrochemical</td>
<td>TRITON/TRISIS</td>
<td>Specifically engineered to disable safety instrumented systems like Triconex.</td>
</tr>
<tr>
<td>2019</td>
<td>Norwegian Aluminum Company</td>
<td>LockerGoga</td>
<td>Norsk Hydro impacted by ransomware delivered by phishing attack.</td>
</tr>
<tr>
<td>2021</td>
<td>US Oil Pipeline Company</td>
<td></td>
<td>The largest publicly disclosed cyber attack against critical infrastructure in the US. Colonial Pipeline attacked by ransomware. Impacted IT based billing systems. Did not touch OT. Exposed VPN password led to delivery of ransomware by the DarkSide group on 06MAY21. Pipeline restarted on 12MAY21. Separately employee reused a password that also was potentially exploited.</td>
</tr>
</tbody>
</table>