A Need for Tactics, Techniques, and Procedures (TTP)

Mr. Frank Honkus
USCYBERCOM J53 ICS SME

Joint Base Architecture for Secure ICS (J-BASICS) Joint Test Technical Advisor

The overall classification of this briefing is: UNCLASSIFIED
The Situation

- Adversaries appear determined to penetrate US critical infrastructure

- If Plan A of the adversary to penetrate your network does not work they have 25 more letters of the alphabet to try

- As a result there is a good chance ICS networks are going to be penetrated and attacked

The threat, coupled with the cybersecurity challenges and long life span on ICS equipment creates *ideal* conditions for a cyber attack.
The Evolution of the Threat

<table>
<thead>
<tr>
<th>PAST</th>
<th>Present</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal Threat Environment</td>
<td>Successful Defense Against Day-to-day Hackers</td>
</tr>
<tr>
<td>No Internet Connection</td>
<td>Nation State Cyber Attacker Can Succeed</td>
</tr>
<tr>
<td>Individual Hackers &amp; Nation States: No</td>
<td></td>
</tr>
<tr>
<td>Cyber Attack Capability</td>
<td></td>
</tr>
</tbody>
</table>

The endpoint ICS devices have a long life span.
Siege Warfare – Has it ever Worked for the Defender?

Today – DODIN Operations

1992 -1996 - Sarajevo
1954 – Dien Bien Phu

Yorktown - 1781
1574 - Leiden
1099 - Jerusalem
717-718 - Constantinople
52 B.C. - Alesia
149-146 B.C. - Carthage
1194-1184 B.C. - Troy

1940 - Maginot Line

Today DoDIN

Commercial

Adversary

GERMANY

DIB

DOD

DoDIN

Weak fortifications
Strong fortifications
Why ICS Matters: DoD Mission - To Fight and Win

ICS Network

ICS Dependent Hardware

Dependent Systems
Command & Control
Communications
Logistics

Force Employment

ICS – Where Cyber can **physically** alter the Battlespace
Impact on Force Projection
Tasks Require Information

ICS Network

Nation-State Level Cyber Attack

ICS Dependent Hardware

Power

Cooling

OFF

OFF

OFF

Dependent Systems

Command & Control Communications Logistics

COMMS OUT

DOWN SYSTEMS

DELAYS

Force Employment

LOGISTICS PROBLEMS

LATE TO THE FIGHT
A Solution

“Resilient” defensive techniques are more effective in ICS environments
Joint Base Architecture for Secure Industrial Control Systems (J-BASICS) Joint Test
J-BASICS

Charter

FEB 26 2014

“employ multi-Service and other Department of Defense (DoD) agency support, personnel and equipment to develop, test, and evaluate advanced cyber industrial control system (ICS) tactics, techniques, and procedures (TTP) to improve the ability of ICS network managers to detect, mitigate, and recover from nation-state level cyber attacks”

Background

The Joint Base Architecture for Secure Industrial Control Systems (J-BASICS) is an OSD funded, Army Test and Evaluation managed, Joint Test to develop defensive cyber TTPs to detect, mitigate, and Recover ICS/SCADA from nation-state level of cyber attacks.

The Joint Test was chartered in 2014 and is scheduled for closedown on or before 31 Dec 2015.

Problem Statement

Network managers supporting DOD Industrial Control Systems (ICS) lack TTP to detect, mitigate, and recover from nation-state level cyber attacks.

Lead Sponsor

USCYBERCOM

Operational Endorsers

NORAD-NORTHCOM
OASD (AT&L)/EI&E
USPACOM
USSTRATCOM
Tactics, Techniques & Procedures

• Key Considerations
  • The TTP must complement existing policies and procedures
  • The TTP must fill cyber incident response gaps for ICS
  • The TTP must be effective, usable, and applicable to the warfighter’s ICS environment
  • The TTP must be scalable and able to adapt to future requirements

• Related Policy & Guidance
  • CJCSM 6510.01B: Defense Cyber Incident Handling
  • DoDI 8510.01: Risk Management Framework
  • NIST SP800-53: Security & Privacy Controls for Federal Information Systems
  • CNSSI No. 1243: Security Control Overlays for ICS
  • NIST SP800-37: Applying RMF to IT Security Life Cycle
  • NIST SP800-82: ICS Security
Tactics, Techniques & Procedures

• **Methodology Approach**
  • Research existing studies on cyber security procedures in ICS
    • Air Force Institute of Technology (AFIT)
    • Naval Postgraduate School
    • MITRE Cyber Resiliency Metrics
    • Technical Reference – Industrial Network Security, Handbook of SCADA, etc
  • Conduct four site surveys to gather information on existing ICS operations
    • Kitsap Naval Base
    • Joint Base Lewis-McChord
    • Ft Carson Army Base
    • Wright-Patterson Air Force Base
  • Develop TTP to integrate with ICS work flow
Three Main Sections:
- Detect
- Mitigate
- Recover
Understanding Detection

- The Detection portion of the ACI TTP enables ICS and IT operators to identify symptoms of malicious cyber activity prior to attack including:
  - System status/configuration changes
  - Unauthorized network access
  - Network traffic anomalies
  - Initial mode(s) of access
  - Lateral network movement
  - Network hop points
  - Firmware compromise
Understanding Detection

• The key is early detection
  • Detecting the enabling functions
• Evidence and IOCs determine severity level
• ICS-Specific incident escalation factors
  • What is the impact?
    • Impact of safety of an operation
    • Impact the reliability of an operation
    • Indications of capability to achieve a large scale impact
    • Number of systems impacted by the threat
  • Where does evidence exist?
• What is the function of the system at risk? Safety-related function? Control function? Monitoring function? Auxiliary/Support function?
• Does evidence exist of control system traffic or data leaving the controlled/protected networks?
Understanding Mitigation

• Mitigation is the ability to fight through an attack, enabling mission to move forward, by gracefully degrading the ICS network – while maintaining mission capability

• The Role of Mitigation
  • Minimize negative impact
  • Ensure some level of capability despite attack
  • 24-Hour Survival Plan/Initial Triage

• How do you mitigate a cyber attack?
  • Graduated approach to mitigation
  • Options and Flexibility
  • Network layer or function group segmentation
Understanding Recovery

• What does it mean to recover from a cyber attack?
  • More than restoring back to proper health
    • Full system re-integration (Number of devices to reintegrate)
    • Not getting re-infected
    • Putting everything together correctly

• Recovery Process
  • Not a static process
  • Ok to move between steps based on operational goals and depends on mission and operational priorities

• Return to Routine Monitoring
Field Test 1 Overview

- Location – Sandia National Labs
- 2 Identical but separate ICS networks
- 1 Week of intensive training (Oct 2014)
- 2 Weeks of test trials (Nov 2014)
- 4 Days during Cyber Flag 15
- Concurrent network and ICS technical training

- 13 Participants from across the Services
- 6 Teams: 1 IT and 1 Facility Engineer
Field Test 2 Overview

• Location – Sandia National Labs
• 2 Identical but separate ICS networks
• 1 Week of intensive training (June 2015)
• 2 Weeks of test events (June 2015)
• 4 Days during Cyber Guard 15
• Concurrent network and ICS technical training
• 12 Participants from across the Services
  (6 Teams: 1 IT and 1 Facility Engineer)
## FT-2 Test Accomplishments

<table>
<thead>
<tr>
<th></th>
<th>Planned</th>
<th>Conducted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Required # of FT-2 Events</td>
<td>FT-2 Events</td>
</tr>
<tr>
<td>Detect (AP)</td>
<td>23</td>
<td>23</td>
</tr>
<tr>
<td>Detect (NAP)</td>
<td>22</td>
<td>23</td>
</tr>
<tr>
<td>Mitigate</td>
<td>36</td>
<td>41</td>
</tr>
<tr>
<td>Recover</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>Totals</td>
<td>95</td>
<td>102</td>
</tr>
</tbody>
</table>

FT-2: Field Test 2
CG: Cyber Guard
AP: Adversary Present
NAP: No Adversary Present
FP: Free Play
Test Results: FT-1 and FT-2

<table>
<thead>
<tr>
<th>FT-1 Issues</th>
<th>FT-1 Result</th>
<th>Trials</th>
<th>WEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect (Adversary Present)</td>
<td>61%</td>
<td>36</td>
<td>40%</td>
</tr>
<tr>
<td>Detect (Normal Operations)</td>
<td>100%</td>
<td>12</td>
<td>70%</td>
</tr>
<tr>
<td>Mitigate</td>
<td>87%</td>
<td>31</td>
<td>70%</td>
</tr>
<tr>
<td>Recover</td>
<td>89%</td>
<td>18</td>
<td>60%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FT-2 Issue</th>
<th>FT-2 Results</th>
<th>Events</th>
<th>WEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect (Adversary Present)</td>
<td>62%</td>
<td>36</td>
<td>60%</td>
</tr>
<tr>
<td>Detect (No Adversary Present)</td>
<td>86%</td>
<td>22</td>
<td>70%</td>
</tr>
<tr>
<td>Mitigate</td>
<td>71%</td>
<td>45</td>
<td>80%</td>
</tr>
<tr>
<td>Recover</td>
<td>94%</td>
<td>16</td>
<td>60%</td>
</tr>
</tbody>
</table>
Overall Results

• Detect:
  • TTP allowed Operators to detect as designed. TTP was designed to:
    • Reject false positives (high specificity)
    • Mid-level detect rate (lower than 75% sensitivity)
  • TTP allows for an approximate 10-time increase in the odds of detecting an adversary if the adversary is present
  • Results show that the more information provided to the user, the more successful the operator will be in using the TTP to detect an adversary

• Mitigate: Results show that the more complex the mitigate task, the harder the mitigation becomes

• Recover: TTP was successful in enabling Operators to restore devices to FMC and reintegrate those devices back into network
Defensible Position

There is a reason this soldier is running... and this one is not...

The owner of this network should be running
Questions?