It’s My Job To Secure Our Control Systems

Should I Patch?

Dale Peterson of Digital Bond
peterson@digitalbond.com
Twitter: @digitalbond / Instagram: @s4xphoto
It’s a Big and Difficult Job

- Technology challenges
- Cultural challenges
- Budgeting challenges
- Measurement challenges

Good Security Practices
Good Security Practice

✓ Patching is a good security practice
✓ Patching will reduce risk

But By How Much?

Disclaimer: Periodic (annual, bi-annual) patching and updates are part of a cyber maintenance program to maintain a supportable system ... but not necessarily warranted for risk reduction related to a cyber attack
Run to failure is a maintenance strategy?

**TRUE**

**FALSE**
Important Term: Insecure By Design

• An attacker does not need a vulnerability to accomplish his goal
  – Loss of control, loss of view, deceptive view
  – Search Digital Bond Project Basecamp for videos and info
• Attacker uses legitimate features and functions to achieve goal

Insecure By Design Is Much Worse Than
A Lack of Secure By Design
Keep Two Divergent Thoughts In Your Head

1. ICS protocols, design, deployment, operation and maintenance need dramatic changes if you believe there are people who want to do bad things

   Push Hard For Secure, True NextGen Solutions

2. I’m stuck with an Insecure By Design legacy system or Insecure By Design choices for new solutions (TRAGIC in 2016)

   Triage: Efficient Risk Reduction
Efficient Risk Reduction

Where will you maximize risk reduction for the next dollar or hour spent?
ICS-CERT Issues An Alert / Advisory
Should I Patch?

How much risk reduction for the effort?

1. Insecure By Design Devices
Case 1: Insecure By Design Devices

- 2015: 1 Modicon Alert & 2 Advisories
  - Hard coded credential, stack overflow on TCP/80, XSS / RFI
  - Firmware upgrades
- Function code 90
  - All an attacker would want/need
  - Modicon_stux_transfer
    Metasploit module
  - Unity/EWS software capability
- No need for a vulnerability
Another Insecure By Design Case

• CoDeSys Gateway and Runtime Tools
  – 3 Advisories in 2015: 2 x Null Pointer Denial of Service, 1 x Heap Overflow
  – Patches issued, yes but ...

• Replay of my 2013 SANS talk
  – Unauthenticated logic / program upload still there
  – CoDeSys is ported to numerous OS
  – Some OS allow attacker to gain root on the device and use it as an attack platform for the ICS
Warning #1

ICS patches often stop the exploit code, but don’t fix the vulnerability
Warning #2

Engineering Work Station (EWS) authentication is typically only authenticating the user to the EWS application, not to the PLC

Attackers go right at the PLC
ICS-CERT Issues An Alert / Advisory
Should I Patch?

How much risk reduction for the effort?

1. Insecure By Design Devices
2. Insecure By Design Zone
Insecure By Design Zone

- Main reason why most security patching provides minimal risk reduction
Examples

• Windows XP Panels connected to Insecure By Design PLC/RTU
  – Hacking the panel is actually an extra, unnecessary step for an attacker
• Hacking RSLogix/RSLinx or most other engineering workstations
  – If an attacker is on the network he doesn’t need the EWS or HMI
• Hacking a SCADA Server
  – Depends if there are internal ICS zones

Most ICS are flat at Levels 1 and 2
“EVERYDAY I’M HUSTLIN’”
Prioritized Security Patching

- Create groups and patch frequency based on efficient risk reduction
- Example:
  - Priority 1 (ASAP / Monthly): Anything accessible from an untrusted zone, such as systems in an ICS DMZ, perimeter security devices, removable media transfer stations
    - Typically don’t affect operations
    - Should be a very small number or you are doing something wrong
  - Priority 2 (Quarterly): Anything that communicates with Priority 1 computers ... or ... most critical ICS components in a further segmented zone ... or ...
  - Priority 3 (Annual): Everything else for cyber maintenance
2015 Examples

• Priority 1 Examples
  – Historians like OSIsoft PI family (2 Advisories)
  – DNP3 Stacks in SCADA system with unmanned remote sites
    • Project ROBUS vulnerabilities were hugely important
    • 2 Advisories (Kepware and TOP Server)
  – OT firewalls: 1 advisory for mGuard but only denial of service
  – Remote access solutions ... Siemens SPCanywhere Advisory

• Not in ICS-CERT
  – IT firewall and router vulns, RDP vulns, database vulns, ...
Consider All Of The Software

- Operating System
- 3rd Party Applications
- ICS Applications
- Libraries and Components that are often hidden
  - Triangle Microworks DNP3 Stacks (from Robus in 2013/2014)
  - CoDeSys

Software Inventory is Key
Many companies rely on CoDeSys

A large number of renowned companies, mostly manufacturers of automation hardware use CoDeSys and its derivatives for their systems. In the list below you will surely find some you already know or even work with.

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>3xS Smart Systems Solutions S.r.l.</td>
<td>Genova / Italy</td>
</tr>
<tr>
<td>A&amp;R TECH Automatisierungs- und Regelungstechnik GmbH</td>
<td>Wien / Austria</td>
</tr>
<tr>
<td>Aartec AG</td>
<td>Schönener / Switzerland</td>
</tr>
<tr>
<td>ABB Automation Products GmbH</td>
<td>Ladenburg / Germany</td>
</tr>
<tr>
<td>ABB Oy Distribution Automation</td>
<td>Vaasa / Finland</td>
</tr>
<tr>
<td>ABB Schweiz AG</td>
<td>Baden / Switzerland</td>
</tr>
<tr>
<td>ABG Allgemeine Baumaschinen Gesellschaft mbH</td>
<td>Hameln / Germany</td>
</tr>
<tr>
<td>ACD Antriebstechnik GmbH</td>
<td>Achstetten / Germany</td>
</tr>
<tr>
<td>ADLINK TECHNOLOGY Inc.</td>
<td>CHungho City, Taipei / Taiwan</td>
</tr>
<tr>
<td>AEG ursatronics GmbH</td>
<td>Berlin / Germany</td>
</tr>
</tbody>
</table>
ICS-CERT Numbers Are Almost Meaningless

• They do:
  – Indicate the level of effort by researchers willing to disclose vulns
  – Indicate what products researchers can access

• They do not:
  – Provide any metric related to ICS code quality
  – Provide any metric to what vendors are better or worse in security
  – Provide any metric related to quantity or skill level of threat agents
  – Provide any data about what sectors are being targeted by attackers
Better ICS-CERT Statistics To Track

- Does the vendor have a published security contact with PGP key?
- How long did it take the vendor to respond to ICS-CERT?
- Did the vendor test and disclose if the vuln was in other products?
- Is the vulnerability in an insecure by design product?
- Did the vendor fix the vuln and has the fix been validated?
- Does the vendor have key elements of an SDL

DHS/ICS-CERT Should Focus Efforts
ICS-CERT Issues An Alert / Advisory
Should I Patch?

How much risk reduction for the effort?

1. Insecure By Design Devices
2. Insecure By Design Zone
3. Low Impact If Compromised
Low Impact If Compromised

- Many components provide low value
  - Monitoring of tank farm when a human checks level daily
  - Metering when back end checks will detect fraud
- Many components have mechanical, offline or secondary processes in place to prevent medium or high impact events

WARNING: Be sure, assume a malicious directed attack, and don’t rely on a networked safety system for low impact
ICS-CERT?

• Why are they wasting time on obscure, unused products

• Well ... actually this was less the case in 2015

• But it would help the community more if they focused on unique ICS vulnerabilities and vulnerabilities with a potential high impact
So What Should I Be Doing

- Focus on your physical and cyber security perimeter
- Focus on devices accessible through the cyber security perimeter
- Insure you have Recovery Time Objectives (RTO) set by management and can meet them
  - RTO is based on recovering capabilities not computers
- Detect when you are being attacked / have been compromised

- Develop and measure a Cyber Maintenance Program