Exploiting SCADA Systems
Jeremy Brown
Vulnerability Research Engineer
@ Tenable
<table>
<thead>
<tr>
<th>General</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Run/Stop Switch</td>
<td>ON</td>
</tr>
<tr>
<td>Water Tank</td>
<td></td>
</tr>
<tr>
<td>Tank Level (L)</td>
<td>388.712</td>
</tr>
<tr>
<td>Output Flow (L/s)</td>
<td>13.448</td>
</tr>
<tr>
<td>High Level Set Point (L)</td>
<td>902.499</td>
</tr>
<tr>
<td>Mid Level Set Point (L)</td>
<td>400.89</td>
</tr>
<tr>
<td>Low Level Set Point (L)</td>
<td>106.344</td>
</tr>
<tr>
<td>Valve 1</td>
<td></td>
</tr>
<tr>
<td>Limit Switch</td>
<td>OPEN</td>
</tr>
<tr>
<td>Limit Switch</td>
<td>OFF</td>
</tr>
</tbody>
</table>
Attack Vectors via Software Vulnerabilities
Client-side attacks from web browsers, e-mail, and malicious servers
Server-side attacks from the internet or internal network
Clickjacking!?
So.. what's wrong?
Security has been implemented as an add-on instead of being built around the product from the ground up.
Systems are typically installed for long term, and software upgrades may require new hardware.
Something somewhere is connected to something that is connected to the Internet
Vendors can take their time with updates, and managers may also take their time updating.
There are a ton of vulnerabilities in SCADA software!
Who may find the bugs?
Employees
Hackers (up to no good)
Security Researchers
Anyone who cares to look really..
Sploitware
A framework designed specifically to penetration test SCADA systems
Similar concept to Metasploit or CANVAS, yet focused on SCADA software
Can check systems for potentially vulnerable software
Exploitation is optional but readily available
Methods for identifying vulnerabilities? Manual testing to fuzzing to reverse engineering
R&D findings range from RCE to DoS to Integrity Loss
DEMO!
Recommendations
Vendors...

Try to break it before you ship it!
Clients...

Do a security evaluation before you make the purchase.
SCADA software can be just as vulnerable as your typical download.com application.
Proficy HMI/SCADA - CIMPPLICITY Free Trial DVD Program

GE Intelligent Platforms is pleased to announce the availability of CIMPPLICITY Version 8.1, the latest addition to our family of HMI/SCADA products. Version 8.1 maximizes the power of your information with new innovative features for both the development and runtime environments.

Thank you for your interest in Proficy HMI/SCADA CIMPPLICITY. Please fill out the form below to receive your free CD containing a fully functional copy of CIMPPLICITY 8.1, which will allow you to evaluate the power of CIMPPLICITY 8.1 in both development and runtime modes.

CIMPPLICITY Version 8.1

- **Change Approval/Signature** - Achieve regulatory compliance, avoid regulatory penalties and conform with good manufacturing practices by using the new change approval feature. This feature delivers an audit trail, approval before operating, multi-signature and commenting capabilities.
- **Alarm variable association** - CIMPPLICITY 8.1 brings a new ability to easily log up to 6 additional points when an alarm occurs or changes state. This information can be easily viewed in the A&E table and in the historical alarm viewer which enables instant analytics for quick operator resolution.
- **More flexible classes** - 8.1 introduces enhancements that enable more flexible classes which speed new product development and lower the total cost of maintaining large scale systems. Classes improvements include:
  - Data item fields can be configured through class attributes using expressions
  - Data items (points) can be optional in the object instance

Related Products
- CIMPPLICITY - GlobalView

Success Stories
- Dell Computers

GlobalCare Customers
- Click here to request an upgrade!
Thank you