Network Security Considerations for the IIoT Challenge

Glenn Longley, Regional Manager - Energy
FreeWave Technologies
Agenda

• How network security expectations have evolved including the role of SCADA in today’s IIoT networks

• The convergence of Operations Technology (OT) and Information Technology (IT)

• How both OT and IT experience trade-offs in building a secure network

• IIoT network security threats and how to address them
  – Real World Examples and Threats

• Considerations for selection secure technology for IoT purposes
• Network security expectations have evolved, including the role of SCADA in today’s IIoT network
IT – New Threats

• Information Technology (IT)
• Focused on protecting from “The Internet”
OT – New Threats

- Operations Technology (OT)
- Local decisions, focused on Operation Needs
IT – OT Convergence

- Convergence of Operations Technology (OT) and Information Technology (IT)
IloT Network Security Threats

- Lack of Security in Initial Planning
- Lack of Security in SCADA Protocols
- Security through obscurity
- Physical Security

What’s the plan?

For added security, after we encrypt the data stream, we send it through our Navajo Code Talker.

... is he just using Navajo words for “zero” and “one”?

Whoa, hey, keep your voice down!
IIoT Network Security Threats

• Air Gapped / Lack of Internet Connection
• Egg Shell Security
• Easy to Use vs. Security
• Consumer Tech moving into Industrial
• Long Equipment Life
Real World Example

- 2005? - Stuxnet
- Most Widely known SCADA Attack
- Discovered in 2010
- Targeted Siemens PLCs
- Iran Nuclear Capabilities
- Physical Damage to Equipment
- Wide Spread & Improved Everyone’s capabilities – Code is now public :: ex. Duqu

<table>
<thead>
<tr>
<th>Country</th>
<th>Share of infected computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iran</td>
<td>58.85%</td>
</tr>
<tr>
<td>Indonesia</td>
<td>18.22%</td>
</tr>
<tr>
<td>India</td>
<td>8.31%</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>2.57%</td>
</tr>
<tr>
<td>United States</td>
<td>1.56%</td>
</tr>
<tr>
<td>Pakistan</td>
<td>1.28%</td>
</tr>
<tr>
<td>Other countries</td>
<td>9.2%</td>
</tr>
</tbody>
</table>

https://en.wikipedia.org/wiki/Stuxnet
Real World Example

• 2011 Night Dragon – Based out of China
• November 2009, coordinated covert and targeted cyberattacks conducted against global oil, energy, and petrochemical companies.
• Social engineering, spearphishing, operating systems vulnerabilities & more
• Competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations
• False Data Threat

Real World Example

• 2015 – Ukrainian Electric Utility
• Multipronged attack
  – DDoS to prevent service techs
  – Malware wiped control systems servers to prevent recovery
• Presumably State Sponsored
• 100,000 people without power for days
• Full Details are not yet released
Threat Example

- Easy to find in the public IP Space
- Vendor Neutral Search for “Oil”
- Top Service – Automated Tank Gauge
- Telnet open on 81 devices
Threat Example

- Let’s Refine and search for “Tank”
- 1595 devices in the US alone
- Location information with In-Tank Inventory
- False Data Threat
Considerations – Selecting Secure Technology

- Understand your Requirements
- Regulatory Environments
- Experience in Secure Environments
- Ability to describe Security Mechanisms
- Do they Understand your Threat vectors
  - Physical vs. Cyber vs. Over the Air
Considerations – Selecting Secure Technology

- Ease of Use vs. Secure vs. Functional Tradeoffs
- External Factors
- Past Vulnerabilities
- Implement Best Practices
- Testing / Evaluation Plan
- On going Improvements
- Ability to Deploy Patches
Considerations – Selecting Secure Technology

- Consider How to Break In & Preparations for Each
- Consider 3rd Party Pen Testing
- Consider Deep Packet Inspection techniques
- Consider How to Isolate SCADA networks
- Consider Security Audits and Assessments (Not just once)
- Consider Ways to Improve Security Culture
Questions?
Copyright

Rights to this presentation are owned by the company(ies) and/or author(s) listed on the title page. By submitting this presentation to the Gas Well Deliquification Workshop, they grant to the Workshop, the Artificial Lift Research and Development Council (ALRDC), and the Southwestern Petroleum Short Course (SWPSC), rights to:

- Display the presentation at the Workshop.
- Place it on the www.alrdc.com web site, with access to the site to be as directed by the Workshop Steering Committee.
- Place it on a CD for distribution and/or sale as directed by the Workshop Steering Committee.

Other use of this presentation is prohibited without the expressed written permission of the author(s). The owner company(ies) and/or author(s) may publish this material in other journals or magazines if they refer to the Gas Well Deliquification Workshop where it was first presented.
Disclaimer

The following disclaimer shall be included as the last page of a Technical Presentation or Continuing Education Course. A similar disclaimer is included on the front page of the Gas Well Deliquification Web Site.

The Artificial Lift Research and Development Council and its officers and trustees, and the Gas Well Deliquification Workshop Steering Committee members, and their supporting organizations and companies (here-in-after referred to as the Sponsoring Organizations), and the author(s) of this Technical Presentation or Continuing Education Training Course and their company(ies), provide this presentation and/or training material at the Gas Well Deliquification Workshop "as is" without any warranty of any kind, express or implied, as to the accuracy of the information or the products or services referred to by any presenter (in so far as such warranties may be excluded under any relevant law) and these members and their companies will not be liable for unlawful actions and any losses or damage that may result from use of any presentation as a consequence of any inaccuracies in, or any omission from, the information which therein may be contained.

The views, opinions, and conclusions expressed in these presentations and/or training materials are those of the author and not necessarily those of the Sponsoring Organizations. The author is solely responsible for the content of the materials.

The Sponsoring Organizations cannot and do not warrant the accuracy of these documents beyond the source documents, although we do make every attempt to work from authoritative sources. The Sponsoring Organizations provide these presentations and/or training materials as a service. The Sponsoring Organizations make no representations or warranties, express or implied, with respect to the presentations and/or training materials, or any part thereof, including any warranties of title, non-infringement of copyright or patent rights of others, merchantability, or fitness or suitability for any purpose.