Covering your BAS: Simple Steps to Address Cybersecurity Concerns in Your BAS Installations

Pook-Ping Yao, CEO
Optigo Networks Inc.
Objectives

• Understand cybersecurity threats in Building Internet of Things (B-IoT)
• Understand what can be done to secure B-IoT
Agenda

- Why cybersecurity matters
- Demo
- Basics of cybersecurity
- Secure building networks
- Conclusion
Why cybersecurity matters
Cyber Crime Costs Projected to Reach $2 Trillion by 2019
- Forbes, January 17, 2016

“IBM’s X-Force team hacks into smart building” – CSO Online

“take down a power plant by physically destroying a generator with just 21 lines of code” – Wired.com

“Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges.”
- Wikipedia
Smart Buildings
A Back Door for Hackers?
Connected Building Systems Fly under the Cybersecurity Radar, Creating "Shadow IoT"

![Diagram showing connected devices and systems statistics]

- 206.2 million connected devices in use in commercial smart buildings
- 84% Building Automation System managers with internet-connected systems
- 29% Building Automation System managers who are improving cybersecurity for their systems

[Source: csOnline.com/article/3031649/security/ibm-x-force-team-hacks-into-smart-building.html]
Types of hackers

- Script kiddies
- Hacktivist
- Cyber criminals
- National states / sponsored
~1500 exposed BACnet systems in one search in the USA
Remote control of building automation devices
No one would know
Basics of cybersecurity
Basics of cybersecurity

People

Process

Technology

Assets

Confidentiality

Availability

Integrity

Assets
Resources

NIST Cybersecurity Framework

SANS Institute: Training and Research

ISA/IEC-62443:
Standard for securing IACS

ICS-CERT:
US DHS Alerts, training and assessments
Secure building networks
Protecting B-IoT by securing the network

Why the network? Because...

- Common to all systems
- Everything* goes through it
- Scalable
- IoT communications is predictable
Three key principles to secure building networks

<table>
<thead>
<tr>
<th>1) Isolation</th>
<th>2) Observability</th>
<th>3) Controllability</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Dedicated networks</td>
<td>• Reports</td>
<td>• Port control</td>
</tr>
<tr>
<td>• VLAN</td>
<td>• Logs</td>
<td>• Port security</td>
</tr>
<tr>
<td>• VRF</td>
<td>• Notifications</td>
<td>• ACL</td>
</tr>
<tr>
<td>• Firewall</td>
<td>• Monitoring</td>
<td>• ...</td>
</tr>
<tr>
<td>• ...</td>
<td>• ...</td>
<td></td>
</tr>
</tbody>
</table>
Take action today

1) Isolate your Building Systems from IT
   • Dedicated Building Network
   • Separate VLAN for each service and vendor

2) Observe what is happening
   • Ask for regular reports of # of connected devices and # of disconnected ports
   • Review network management log files for user login

3) Control the flow of information
   • Disable unused ports
   • Set MAC filtering/security rules
Conclusion

- Cybersecurity is serious and needs to be addressed.
- Protect the network, protect the system.
- Start today.
- Q&A

Pook-Ping Yao
CEO, Optigo Networks Inc.
ping@optigo.net