Best practices for securing Niagara
Agenda

• Exposed on the Internet: Recognizing the threat
• Network security best practices for Niagara
• Niagara 4 security and configuration best practices
• Organizational best practices
• Q&A
Cyber security in the news

IRS Tax Fraud And Phishing Advances
New techniques and automation have bad guys making more money than ever off of unsuspecting taxpayers.
By ERICKA CHICKOWSKI Contributing Writer, Dark Reading, 3/23/2016

Concerned by cyber threat, Obama seeks big increase in funding
WASHINGTON | BY DUSTIN VOLZ AND MARK Hosenball

OMP government data breach impacted 21.5 million
By Jim Sciutto, Chief National Security Correspondent

FBI Says Threat From ‘Ransomware’ Is Expected to Grow
Law-enforcement agency sees problem of extortion by hackers worsening in 2016

DEFCON 2.0: Expert warns cyber warfare has reached critical turning point
Updated 11 Oct 2015, 10:15pm

Biggest data breaches of 2015

TridiumTalk
Best practices for securing Niagara
Shodan – “Google” for hackers
Control systems exposed

“If you talk to these companies, they’ll swear up and down that their controller networks are “isolated” from other computer networks, including the Internet. But many, many times, there’s a connection that the engineers are not aware of…”

“Cyber Risk Isn’t Always in the Computer,” Seth Bromberger, WSJ, Sept 24, 2015
If your JACE® is connected to the Internet…

1. Searches “Niagara” on Shodan
2. Tries published vulnerabilities, default passwords
   - Do you use easy-to-guess passwords?
   - Are you current with security patches?
3. Attempts to log on to device or simply writes a program to automate the process

Successful attacks result in “owning your building,” crashing your system, and/or going farther into your network to attack other things
Network security best practices for Niagara
Practical tip #1: Ask yourself: Do you really need remote access?

- Most Niagara systems can be managed on internal, private networks
- Connecting systems to the Internet introduces risk
- Best approach: Don’t allow remote access at all
  - Manage devices in your own private network; you’re not connected to the Internet and are protected
Practical tip #2: If you need remote access, set it up securely

- Best practice: Use a security gateway that acts as a VPN Server
- Put your Niagara devices behind the security gateway
- Have remote clients authenticate to VPN server to establish VPN tunnel
- Devices behind security gateway are concealed from Internet discovery
- All transmissions will be encrypted

“Using a VPN with Niagara Systems”
Find it at www.tridium.com/en/resources/library
Practical tip #3: Use network defense-in-depth

From “Recommended Practice: Improving Industrial Control Cybersecurity With Defense-In-Depth Strategies”

DHS, ICS-CERT, 2009
Practical tip #4:
IT and Facilities need to talk to each other

• “Shadow IT”: Someone connects systems together without IT’s knowledge

• The IT department’s job is to secure assets on the network

• Too often, IT and Facilities don’t talk, and things become connected without organizational oversight
Niagara 4 security and configuration best practices
Security improvements in Niagara

• Making security easier through “secure by default” principle:
  – Enforcement of stronger passwords
  – Encrypted communications (FoXS and HTTPS)
  – Strongest authentication mechanisms by default
  – Force default credential changes

• Role-based access control

• Encryption of sensitive information at rest

• Signed Tridium code

• JACE® 8000 secure boot

You can enhance Niagara security even more by following best practices
Best practice #1: Disable or rename known accounts

Great example: admin user
- Known account name that could represent a potential security vulnerability
- In Niagara 4: Simply rename the admin user (see image)
- In Niagara AX 3.8: Create a new account with super user permissions; default “admin” account can be disabled

Similar threat exists for commonly used user names – ex: “tenant?”
Best practice #2:
No factory default credentials

• New to Niagara 4: forced change of factory default credentials on initial commissioning

• For older systems, change was not forced

• Niagara AX: Make sure you are NOT still using factory default credentials
  – They are known to the community
  – They are also known by hackers
Best practice #3: Enforce password history & expiration

- You can do this in the Global Password Configuration for each Authentication Scheme
  - By default, passwords expire in a year, with 30-day warning to users
  - Best practice: Change passwords every 90 days; remember last two histories
  - Expiration of password policy can be overridden on a per-user basis when you create/edit a user
Best practice #4: Configure lockouts

These are defaults, but you can customize according to your policy.
Best practice #5: Always use encrypted comms

- By default, Niagara uses encrypted communications (HTTPS and FoXS)

- Changing these values to allow transmissions on unencrypted channels opens your organization up to risk: potential attacks on confidentiality and systems integrity
Role-based access control overview

- Components are grouped into categories
- Permissions to access categories are granted by roles
- Users are associated with one or more roles
Adding new categories
Assigning components to categories

- Components are grouped into categories

<table>
<thead>
<tr>
<th>Category Browser</th>
<th>Inherit</th>
<th>User</th>
<th>Admin</th>
<th>HVAC-LynnhillFacility</th>
<th>Electrical-LynnhillFacility</th>
<th>AlarmSystem-LynnhillFacility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td>n/a</td>
<td>⬅</td>
<td>⬗</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td></td>
<td>⬗</td>
<td>⬗</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drivers</td>
<td></td>
<td>⬗</td>
<td>⬗</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NiagaraNetwork</td>
<td></td>
<td>⬗</td>
<td>⬗</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LynnhillFacility</td>
<td></td>
<td>⬗</td>
<td>⬗</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LightingSystem</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>HVAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>Alarms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>Apps</td>
<td></td>
<td>⬗</td>
<td>⬗</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Files</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>History</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
</tr>
</tbody>
</table>
Setting up role-based access

Roles assigned permissions on categories

Users associated with roles
User & role best practices

Defining categories, roles and permissions is important
• Focus on determining roles for your system first
• Then, associate roles with appropriate users
• Account management becomes much easier

Use different accounts for each user (for station AND platform)
• One Niagara user that everyone uses is NOT a best practice!

Use “Super users” sparingly!
• Roles make setting up privileges a lot easier – you shouldn’t have to default to making people a super user.
Organizational best practices
Creating strong passwords

- Researchers suggest that weak passwords are most often “the weakest link in the chain” for cyber attacks
- Niagara 4 supports OWASP guidelines for password strength and forces users to choose these strong passwords by default
  - Should be **long and complex enough to be difficult to guess**
  - But should also be **easy to remember**

How?
How many of us choose passwords

(WAS IT TROMBONE? NO, TROUBADOR, AND ONE OF THE O's WAS A ZERO? AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD)

(How many of us choose passwords)

(http://xkcd.com/936/)
The “XKCD” approach

(correct horse battery staple)

THAT'S A BATTERY STAPLE.
CORRECT!

DIFFICULT TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT

(http://xkcd.com/936/)
## Best practice: Turn sentences into passwords

<table>
<thead>
<tr>
<th>Silly sentence</th>
<th>New password</th>
<th>Password strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>When I was 7, my sister threw my stuffed rabbit in the toilet.</td>
<td>WIw7,mstmsritt.</td>
<td>• 15 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• One upper case</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• One digit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Two special characters</td>
</tr>
<tr>
<td>Wow...did something die under that couch? It smells nasty!</td>
<td>W...dsdutC?1sn!</td>
<td>• 15 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• One upper case</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• One digit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Five special characters</td>
</tr>
<tr>
<td>About 6 months ago, John Smith hid a scary toy snake under Nancy's desk!</td>
<td>A6ma,JShastsuNd!</td>
<td>• 16 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Four upper case</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• One digit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Two special characters</td>
</tr>
</tbody>
</table>

https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html
Summary: password best practices

• Use easy-to-remember methods
  – Turn sentences into passwords
• Don’t use dictionary words, even from other languages
  – Single dictionary words (even with substitutions) are easily cracked by dictionary password programs (ex: O->0, E->3, A->@)
• Don’t write passwords down
• Don’t store passwords in a file
• Don’t email your passwords
• Don’t use examples from this presentation
People, processes & technology

- Security isn’t just an “IT thing”
- Policies and procedures are critical
  - Patch management
  - Proper use of IT systems
  - Proper use of Niagara systems
  - Procedures for incident response
- Communicate: Make sure users understand/respect the cyber threat and follow organizational security policies
Top 10 best practices

1. **DO NOT** connect stations directly to the Internet; use VPN
2. Work with IT to establish defense-in-depth network strategy
3. Niagara 4: Rely on secure-by-default options
5. Use common sense user account management: strong passwords, no “guest” user backdoors, configure role-based access
6. Always use encrypted transport (selected by default in Niagara 4)

7. Give users guidance on passwords
8. Keep up with our security bulletins and patches - www.tridium.com/en/resources/library
9. Read our security manuals!
10. Remember: people, processes & technology
Thank You!

Kevin T. Smith, CISSP, CSSLP
Chief Security Architect

ksmith@tridium.com
www.linkedin.com/in/kevintsmith/

www.tridium.com/en/resources/events