• Questions will be answered at the end.

• Please submit questions to Erick Mendoza using the chat function.
Securing Niagara, Part 2

- Java 1.7.0.25 Update Announcement
- Review basic hardening steps
- Discuss basic usage of SSL functionality
- Discuss VPNs
- Highlight recent update changes
- The Future
- Questions
Review

- System security is like an onion:
  - No, not because it smells bad (although it can)
  - It is made up of LAYERS
Review

Passwords

• Change the Default Platform Credentials
• Use Strong Passwords
• Enable the Account Lockout Feature
• Use the Password History
• Use the Password Reset Feature
• Leave the “Remember These Credentials” Box Unchecked
Account Management

• Use a Different Account for Each User
• Assign the Minimum Required Permissions
• Use a Single Super User
• Require Super User Permissions for Program Objects
• Use the Minimum Required Permissions for External Accounts
Authentication

• Use “Digest” Authentication in the FoxService
• Set the FoxService Legacy Authentication to “Strict”
• Use “cookie-digest” Authentication in the WebService
Review

TLS/SSL & Certificate Management

- Enable Platform SSL Only (3.7+ only)
- Enable Fox SSL Only (3.7 only)
- Enable Web SSL Only
- Enable SSL on Other Services
- Set Up Certificates
Review

Additional Settings

- Disable FTP and Telnet
- Remove the serial shell jumper
- Disable Unnecessary Services
- Blacklist Sensitive Files and Folders
- Update NiagaraAX to the Latest Release
Review

External Factors

• Install JACEs in a Secure Location (locked room, wiring in conduit, etc)
• Make Sure that Stations Are Behind a VPN
• Even internally, make sure that stations are behind a firewall with only necessary ports open
• Protect your backups
SSL

- Key Pair
- Certificate
- Self Signed Certificate
  - Trusted Certificate
- Certificate Authority (CA)
- Certificate Chain
- SSL Handshake
- SSL and NiagaraAX
SSL – Key Pair

Common sizes: 1024 and 2048 bits
SSL – Certificate

Certificate

Public Key

Metadata
- Issuer
- Subject
- expiration

• key usage
• serial number
• etc

Signature

Private

TRidium
SSL – Self Signed Certificate

Certificate

Public Key

Metadata
- Issuer
- Subject
- expiration

key usage
serial number
etc

Signature

Private Key

• Issuer
• Subject
• expiration
• key usage
• serial number
• etc
SSL – Trusted Certificate

Certificate

Public Key

Metadata
• Issuer
• Subject
• expiration

• key usage
• serial number
• etc

Signature

Trusted Source

Private Key
SSL – Signed Certificate

CA Certificate

- CA Public Key
- Signature

CA Private Key

Certificate

- Public Key
- Signature

Private Key

TRiDiUM

Components:
- CA Certificate
- CA Public Key
- CA Private Key
- Certificate
- Public Key
- Signature
- Private Key

Format:
- Chart illustrating the components and relationships of SSL – Signed Certificate.
SSL – Certificate Chain

- **Root CA Certificate**
  - Root CA Public Key
  - Signature

- **Intermediate CA Certificate**
  - Intermediate CA Public Key
  - Signature

- **End Certificate**
  - End Public Key
  - Signature

- **Root CA Private Key**

- **Intermediate CA Private Key**

- **End Private Key**
SSL – Certificate Validation

From the trust store

- Root CA Certificate
  - Root CA Public Key
  - Signature

Intermediate CA Certificate

- Intermediate CA Public Key
- Intermediate CA Certificate
  - Signature

End Certificate

- End Public Key
- End Certificate
  - Signature

Sent to the client by the server
SSL – Certificate Validation

• Certificate chain is valid and trusted

• Distinguished name matches server address

• Key usage is valid

• Certificate is in the valid date range
SSL – Handshake

Client

Browser Requests
Secure Socket
(https://yadda.com)

Session Key Seed
is Encrypted with
SSL Public Key
From Server

Encrypted Data

Server

Server Responds
with SSL Certificate
Chain

Server Indicates All
Transmissions Are
Encrypted

Encrypted Data

Encrypted Data
SSL – Certificate Tools

The image shows a certificate signing request window for www.tridium.com. The properties include:
- Version: v3
- Certificate Signing
- Certificate Signing Request (CSR) generation window
- Dates: Not Before: 04-Apr-2012 03:15 PM EDT, Not After: 04-Apr-2014 03:15 PM EDT
- CA Alias
- CA Password

The extensions section is visible as well.
SSL – Client Interface
SSL – Server Configuration

- Web Service (port 443)
- Fox Service (port 4911)
- Niagarad (port 5011)
SSL – Small Network Example

CA Certificate Installed on Client Machines in Their Trust Store

CA Private Key Used to Sign Server Certificates
SSL – Large Network Example

Root CA Certificate Installed on Client Machines in Their Trust Store

Intermediate CA Private Key Used to Sign Server Certificates

Root CA Private Key Used to Intermediate CA Certificates

Intermediate CA Certificate
VPN

**Typical Niagara Setup**
- with all ports forwarded, it gives full access to web, fox, niagarad
A port scan would reveal all open Niagara ports
Attackers could use weak credentials or known vulnerabilities to exploit the system.
A port scan would only reveal the VPN port.
Once connected, the client PC is effectively part of the local network.
• The VPN Guide discusses all this in great detail
• It also provides an example setup using a ZyWall USG 20
• Supports the built in VPN clients in Windows, Android and iOS.
• In addition to client to server connections, a VPN can also support a persistent connection between remote networks
  – Station to station connections
Niagara Updates

• Enhanced password management
  – PBKDF2-SHA256
  – AES-256

• Enhanced digest authentication
  – SCRAM-SHA256

• Miscellaneous other security fixes
The Future…

• Always improving!
• Encrypted backups
• Rolling keys
• Two factor authentication
• Sandboxing
• …and more!!
FAQ

- Won’t SSL slow things down?
- What is the difference between a firewall and a VPN?
- If I’m using a VPN, do I need to use SSL?
- If I’m using SSL, do I need to use a VPN?
- If Tridium is pushing “secure by default”, why isn’t SSL enabled by default?
Sources for Good Information

- Niagara Hardening Guide
  - Available next week
- VPN Guide
  - Available next week
- Niagara SSL Documentation (docSSL)
  - In 3.7 release
- SNA Forum on LinkedIn
- ICS-CERT
  - http://ics-cert.us-cert.gov/
- Niagara Central
  - http://www.niagara-central.com
- Schneier on Security
  - http://www.schneier.com/
Questions