

NIAGARA SUMMIT

CONNECTING THE WORLD

Cyber Security and Application Hardening

James Johnson



Objectives

- Why should you care about security?
- What can you do?
- Where can you find information and updates?
- Best practices for hardening a Niagara application
- PKI overview
- How to deploy PKI certificates in a Niagara application

TRIDIUÑ

Code signing program objects



Read the News Lately?

Yahoo says 500 million accounts stolen

by Seth Fiegerman @sfiegerman (L) September 23, 2016: 10:39 AM ET

Ransomware Attacks Ravage Computer Networks In Dozens Of Countries Hay 12, 2017 - 11:05 AH ET

Recommend 20K C

TECH

US Banks Targeted with Trickbot Trojan

Nearly 1 million new malware threats released every day

LinkedIn Lost 167 Million Account Credentials in Data Breach

IoT Security Incidents Rampant and Costly

FBI Says Threat From 'Ransomware' Is **Expected to Grow**

Law-enforcement agency sees problem of extortion by hackers worsening in 2016

How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet

DEFCON 2.0: Expert warns cyber warfare has reached critical turning point

Updated 11 Oct 2015, 10:15pm

More than 65m Tumblr emails for sale on the darknet

An Army of Million Hacked IoT Devices Almost Broke the Internet Today

🛗 Friday, October 21, 2016 🛛 👗 Mohit Kumar

RISK ASSESSMENT

Double-dip Internet-of-Things botnet attack felt across the Internet

Massive attack combining compromised IoT devices, other bots cripples many sites. SEAN GALLAGHER - 10/21/2016. 5:17 PM

Big Data privacy risks

Not in front of the telly: Warning over 'listening' TV

WANNACRY II? Britain, Europe and Chernobyl hit by 'Petya' ransomware in cyber-attack with chilling echoes of the 'WannaCry' assault which crippled the NHS

Oil firms, government systems and a major shipping firm also come under attack as virus sweeps across the Continent

DDoS Attack Takes Down Central Heating System Amidst Winter In Finland

🏥 Wednesday, November 09, 2016 🛛 🛔 Mohit Kumar

REPORT

FBI: An Account on Clinton's Private Email Server Was Hacked

TRIDIU

Nearly 200 million IoT devices are 'vulnerable to hacking'

VOTE 2016

TECHNOLOGY

FBI investigates cyberattack of **Democratic National Committee**

Up to 400 million accounts in Adult Friend Apploiting Now Acero-day exploit exposed Acero-day exploit exposed Another Day, Another New Threat to Privacy on the Internet Finder breach

() 14 November 2016 Technology

Internet Bought a car recently? Millions of dealership customer details found online

Customers for more than a hundred car dealerships across the US were put at risk because of shoddy database security



IoT Search Engines

- https://www.shodan.io
- <u>https://censys.io</u>
- <u>https://www.punkspider.org</u>
- <u>https://www.zoomeye.org</u>
- <u>https://ivre.rocks</u>







People Forget Physical Security



- Even if you have secure products and great network security, it really doesn't matter if someone can gain physical access to your control system and edge devices.
- Many successful cyber-attacks also begin with a physical attack.
- Malware can be introduced through USB drives.





Protect Against Ransomware

- Educate your people on the safe use of IT assets and the dangers of ransomware.
- Use anti-virus software
- Perform periodic scheduled backups of your systems.
- Treat systems as mission-critical infrastructure, which means it shouldn't be used for surfing the web or checking email.

w.	Wana Decrypt0r 2.0		×
	Ooops, your files have be	een encrypted! English	~
Payment will be raised on 5/16/2017 00:47:55 Time Left 22 # 23 # 57 # 377 Your files will be lost on 5/20/2017 00:47:55 Time Left	Sylid/2017 00:47:55 Time Left 2 * 23 * 57 * 37 Your files will be lost on 5/20/2017 00:47:55 Time Left Your files will be lost on 5/20/2017 00:47:55 Time Left Your files will be lost on 5/20/2017 00:47:55 Time Left C = 23 * 57 * 37		
06:23:57:37	After your payment, click <check payment=""></check>	. Best time to check: 9:00am - 11:00am	v
<u>About bitcoin</u> <u>How to buy bitcoins?</u>	in bitcoin	of bitcoin to this address: lyMgw519p7AA8isjr6SMw	Copy
Contact Us	Check Payment	Decrypt	



Patch Management is Critical

- Organizations such as US-CERT and ICS-CERT provide a great service internationally, reporting vulnerabilities in hardware and software.
- Many advisories affect millions of devices.
- Vendors release security patches and updates, and these organizations point you to where to get them.
- Any unpatched system on your network can be an attackers avenue into your organization.



https://www.us-cert.gov



https://ics-cert.us-cert.gov



TRIDIUÂ 8

Assessments – what are you assets and risks?

- Understand your organization's appetite for risk and determine a risk threshold using a CVSS score.
- Identify electronic assets you wish to protect and document security requirements.
- Engage an independent security team to assess threats and potential vulnerabilities for your network and assets.
- Follow up with action items.
- Perform on a periodic basis because assets and requirements change over time.



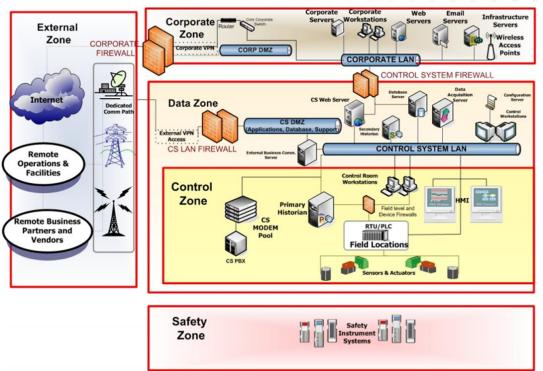




Networking – Defense-In-Depth

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

DHS, ICS-CERT, 2009







Helpful Resources

Resources	Where to Find
NIST SP 800-50: Building and Information Technology Security Awareness and Training Program	www.nist.gov
NIST SP 800-82: Guide to Industrial Control System (ICS) Security	www.nist.gov
NIST SP 800-61: Computer Incident Security Handling Guide	www.nist.gov
ICS-CERT – "Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies"	https://ics-cert.us-cert.gov





Helpful Resources

Resources	Where to Find
ICS-CERT – "Developing an Industrial Control Systems Cybersecurity Incident Response Plan	https://ics-cert.us-cert.gov
ICS-CERT – "Remote Access for Industrial Control Systems."	https://ics-cert.us-cert.gov
Niagara 4 & AX Hardening Guides	www.tridium.com/en/resources/library
Tridium Security Bulletins	www.tridium.com/en/resources/library
Niagara Smart Building Guide Specification	www.tridium.com/en/resources/library





Niagara – Good Behavior Through Technology

- Secure by Default
 - Forcing default credential changes upon commissioning
 - Strongest authentication mechanisms by default
 - Enforcement of strong passwords
 - Encrypted communications (FOXS and HTTPS)
- Role-based Access Control Make user management easier with rolebased abstractions.
- Encryption of sensitive information at rest
- **Digitally-signed code**, validated for integrity and source at run time.
- Secure Boot





Flexible Authentication Schemes

- Lightweight Directory Access Protocol (LDAP) / Active Directory (AD)
 - Integrates to existing directory information services.
 - Supports using Kerberos for SSO.
- Security Assertion Markup Language (SAML)
 - Provides SSO functionality.
 - Works with popular on premise and cloud based SAML Identity Providers (IdP) such as OpenAM, Salesforce, Active Directory, etc.
- Google
 - Provides two factor authentication using Google Authenticator app.
 - Available for Android, BlackBerry and iOS devices.





LDAP and Kerberos and SAML, Oh My!

Another session to come focusing on these features

10:30 AM Tomorrow – Active Directory and SAML Integration





FIPS 140-2

- Federal Information Processing Standard (FIPS) is a government security standard used to accredit cryptographic modules.
- Cryptographic modules undergo a thorough certification process to ensure that all cryptographic algorithms adhere to the government security guidelines.
- Workbench clients and stations running in FIPS mode are restricted to using FIPS certified algorithms.

Session Info for BuildingJACE



You are connected as SystemAdmin.



Hostname is jace.NS2018.lan.

The identity of this host has been verified by Niagara Summit 2018 Intermediate Certificate.

Certificate Information

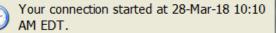
Your connection to BuildingJACE is encrypted with 256-bit encryption.

The connection uses TLSv1.2.

The connection is encrypted using AES_256_CBC, with SHA384 for message authentication and ECDHE_RSA as the key exchange mechanism.



The server is running in FIPS mode.



TRIDIUÂ





Public Key Infrastructure (PKI)

- An infrastructure that supports the distribution of certificates containing public identification keys that are used to both securely identify entities and also provide confidentiality in transmissions.
- A **Certificate Authority** (CA) is an organization which stores, issues and signs digital certificates.
- A **digital certificate** is an electronic document used to identify an entity, digitally signed by a trusted third party (the CA).
- Certificates for a web server also binds together the organization's identity with the web server's identity using the server's domain name, server's name, host name or IP address.





Public Key Cryptography

- Uses a **private** and **public key pair**, used together for encrypting and signing.
- Keys are asymmetric, meaning each key is unique but only two specific keys work together.



- Each participant has a private and public key. The public key is not a secret and is available to everyone, while each participant keeps its private key a secret.
- A sender encrypts data with a recipient's public key, and only someone who holds the private key (the recipient) can decrypt the data.
- A sender can sign data with their own private key, and everyone who has access to the signer's public key can validate the sender signed it.
- TLS uses an asymmetric public key pair (2048 to 4096 bit) to establish a TLS connection, and then a symmetric session key (128 to 256 bit) for encryption of data for performance reasons.



TRIDIUÑ

What Does a TLS Certificate Provide

- Through a handshake process, the client establishes an encrypted connection with the server.
- Verifies the identity of the server.
- Validate the authenticity of the server's certificate.
- Session info displays details regarding the server's identity, cipher strength, protocol, and key exchange mechanism.
- A connection can be encrypted without verifying the server's identity or validating the certificate authenticity.

Security overview This page is secure (valid HTTPS). Certificate - valid and trusted The connection to this site is using a valid, trusted server certificate issued by Microsoft IT TLS CA 4. View certificate Connection - secure (strong TLS 1.2) The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with X25519 (a strong key exchange), and AES_128_GCM (a strong cipher). Resources - all served securely All resources on this page are served securely.

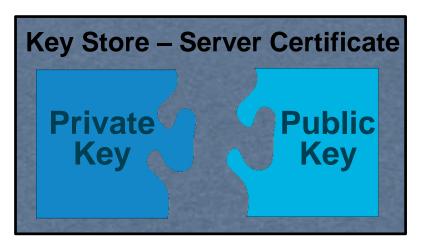


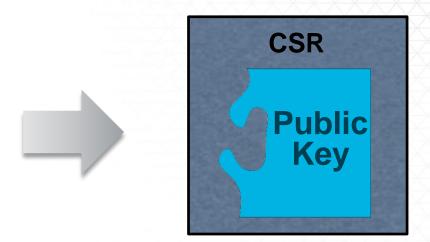
Certificate Authority (CA)

- In cryptography, an organization that issues digital certificates.
- A trusted third party organization who vets the organization seeking to have their certificate signed.
- The vetting process varies depending on the specific type of certificate.
- The CA typically charges a fee for the process.
- Certificates are typically only valid for a period of 1 year.
- Could be well known public organizations such as Thawte, GoDaddy or Verisign, or could be a local authority.



Creating a Certificate Signing Request (CSR)



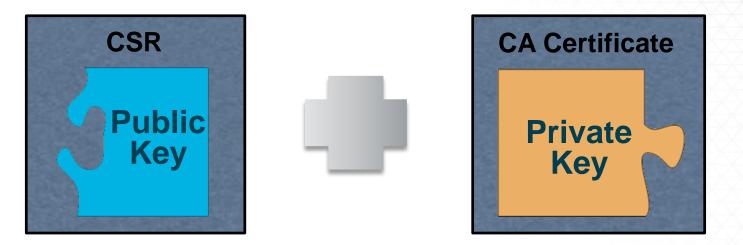


- Only includes the **public key** from the server's certificate.
- The original private key must remain in the server's key store.





Signing a Certificate Signing Request (CSR)



- After validating the request, the certificate authority signs the CSR using their private key.
- The certificate authority sends the signed certificate and other information to the applicant.





Certificate Chain of Trust

- Shows the chain of certificates used to digitally sign the certificate.
- Typically includes at least an intermediate and root certificate.

Certificate X	Certificate
General Details Certification Path	General Details Certification Path
Certificate Information	Certification path DigiCert DigiCert SHA2 High Assurance Server CA www.tridium.com
This certificate is intended for the following purpose(s): • Ensures the identity of a remote computer • Proves your identity to a remote computer • 2. 16.840.1.114412.1.1 • 2.23.140.1.2.2	
* Refer to the certification authority's statement for details.	
Issued to: www.tridium.com Issued by: DigiCert SHA2 High Assurance Server CA	View Certificate
Valid from 6/ 28/ 2017 to 9/ 5/ 2018	Certificate status: This certificate is OK.





Certificate Trust Store

- A collection of root and intermediate certificates including their public encryption keys.
- Typically populated by the operating system or application provider with well known public certificate authorities.
- Can import additional certificates from other certificate authorities.

File Action View Help		
🗢 🔿 🚈 🗊 📋 🖸 🖂 🖛		
Certificates - Current User	Issued To	Issued By
Personal	🔄 AddTrust External CA Root	AddTrust Exte
Trusted Root Certification Authorities	🔄 Affirm Trust Commercial	AffirmTrust C
Certificates	🔄 Baltimore CyberTrust Root	Baltimore Cyl
Enterprise Trust Intermediate Certification Authorities	🔄 Certum CA	Certum CA
Active Directory User Object	🔄 Certum Trusted Network CA	Certum Trust
Trusted Publishers	Class 3 Public Primary Certification Authority	Class 3 Public
Indiced Publishers Indiced Publishers	COMODO RSA Certification Authority	COMODO RS/
Third-Party Root Certification Authoritie	🔄 Copyright (c) 1997 Microsoft Corp.	Copyright (c)
Trusted People	🔄 Deutsche Telekom Root CA 2	Deutsche Tele
Other People	🔄 DigiCert Assured ID Root CA	DigiCert Assu
Certificate Enrollment Requests	🔄 DigiCert Global Root CA	DigiCert Glob
Smart Card Trusted Roots	🔄 DigiCert Global Root G2	DigiCert Glob
	🔄 DigiCert High Assurance EV Root CA	DigiCert High
	DST Root CA X3	DST Root CA
	Entrust Root Certification Authority	Entrust Root (
4		

• Use by the client to validate the digital signatures used in a certificate's chain of trust.





Default Self-Signed Certificate

- The issuer and subject properties match.
- Can only be used to **encrypt** the connection and data being transferred.
- **Cannot** be used to **verify the identity** of the server or to establish trust.

A Not secure https://jace.ns2018.lan	
Certificate	x
General Details Certification Path	
Certificate Information	
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.	
	_
Issued to: Niagara4	
Issued by: Niagara4	



Workbench Certificate Management Tools

Used to manage the server's key store, trust store and host exceptions.

Config	🖨 Services 🛛 🗏 I	PlatformServices	🔁 CertManagerS	Gervice		🖻 👔 Certificate M	1anagement 🝷
rtificate N	1anagement						
ertifica	ate Managem	ent for "jace	e.NS2018.lan"				
Jser Key	Store System	Trust Store Us	er Trust Store	llowed Hosts			
You hav	ve local certifica	tes:	· · · · ·				
User Key	/ Store						2 objects
Alias	Subject	Not After		Key Algorithm	Key Size	Valid	₽
🖲 jace	jace.ns2018.lan	Wed Mar 27 0	0:00:00 EDT 2019	RSA	2048	true	
🖲 tridiun	n Niagara4	Wed Mar 27 12	2:16:43 EDT 2019	RSA	2048	true	
		/iew	Sew 2	Sert Reque	ct	Delete	
		lew	New	Cert Reque	st	o Delete	
			Import 🕞 Exp	ort 🥜 Res	et		





Workbench – Create a Self-Signed Certificate

- Common Name (CN) should be the domain name which the server will be accessed using.
- Alternative Server Name should contain CN and possibly other DNS aliases.
- Not all fields are required, verify with your CA which fields they require.
- Typically only valid for 1 year.
- Verify supported key size.

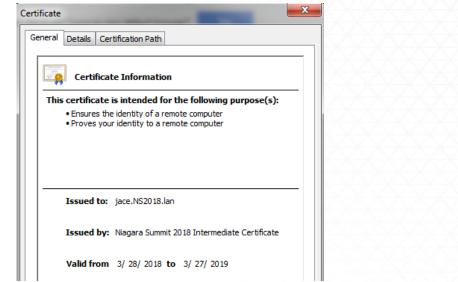
Generate Self Signed Certificate	"Jaco Million"	×
	Signed Certificate gned certificate and inserts it into the keystore	
Alias	jace	(required)
Common Name (CN)	jace.NS2018.lan	(required)
	\ast this may contain the host name or address of the server	
Organizational Unit (OU)	Tridium Support]
Organization (O)	Tridium	(required)
Locality (L)	Richmond]
State/Province (ST)	Virginia]
Country Code (C)	US (required)	
Not Before	28-Mar-2018 12:00 AM EDT	
Not After	28-Mar-2019 12:00 AM EDT	
Key Size	\otimes 2048 bits \diamond 3072 bits	
Certificate Usage	\otimes Server \diamond Client \diamond CA \diamond Code Signing	
Alternate Server Name	jace.NS2018.lan]
Email Address]
	OK Cancel	



Using a Signed Certificate

- Issued to and issued by are different.
- Provides encryption, verifies the identity of the server and establishes trust between the client and server.

🔒 🛛 jac	e.ns2018.lan/logir	1
	Secure connect	ion
C	jace.ns2018.lan The connection is <u>Hide details</u>	secure.
	First visited:	Monday, March 26, 2018
	Certificate:	<u>jace.NS2018.lan</u> Tridium
	Connection:	TLS 1.2 AES_256_CBC HMAC-SHA1 ECDHE_RSA (23)







Code Signing

Code Signing (Options
👔 Code Signing Opt	ons
Signing Cert	vykon code
🔘 Tsa Url	http://sha256timestamp.ws.symantec.com/s

- The process of digitally signing executables and scripts to confirm the software author and guarantee the code has not been altered or corrupted since it was signed.
- Trusted timestamping is the process of securely keeping track of the creation and modification times of a document.
- Timestamping Authority (TSA) URL Server which timestamps the code signature so client can verify when the code was digitally signed.
- All core modules from Tridium are code signed.
- Third party developers may optionally code sign their modules.
- Program objects may optionally be code signed.





Provisioning Tools

- Batch tools for managing security related features on JACEs under a supervisor.
- Certificate steps for creating and installing signed server certificates to the key store or installing CA certificates to the trust store.
- Steps for setting the system passphrase, platform credentials and TLS levels.

Select the type of step to add to t below:	he job from the list		
Туре	Description		
🛯 🚇 Backup Stations	Back up each station in the job		
Copy Local File	Copy a local file to each station in the job		
Copy Supervisor File	Copy a file from the supervisor's filesystem to each station in the job		
🔁 Deploy Template	Deploy a template file to each station in the job		
😣 Generate Certificate	Generate and install a certificate on each station		
异 Install Certificate	Install a certificate to the user trust store of each station		
🞼 Install Software	Install software to the stations in the job		
🔊 Reboot	Reboot each station in the job		
Rename Device Station	Rename device station to match station proxy name.		
🗇 Run Robot	Run a robot on each station		
👼 Security Job Steps	Add all security related job steps		
🚘 Set Minimum TLS Level	Set Minimum TLS level for the platform, fox, and web services		
Set Platform Credentials	Set platform credentials		
🤌 Set System Passphrase	Set System Passphrase		
😼 Sign Certificate	Sign a certificate on each station		
Connection Connection	Update station connection information using discovered devices.		
🞼 Upgrade Out-of-date Software	Upgrade out-of-date software for each station in the job		
🖺 Upgrade Template	Upgrade deployed template instances on each station in the job		





Summary

- Everyone must care and be aware of cybersecurity.
- Multiple layers of security provide defense in depth.
- Secure systems require active management including but not limited to managing certificates, installing software patches and performing periodic security audits.
- PKI certificates are used to establish trust between a client and server by verifying the identities and encrypting data exchanged over the network.





Questions





