Q&A
TridiumTalk: Defending your business against cyber threats
09-19-17

The following are answers to many of the questions we received but were unable to completely answer during the time allotted for the TridiumTalk.

Q: I have seen reports that using caps, lower case, numbers and symbols have been discovered to be easier to hack than using a phrase. Do you have any feedback on that vs. the default security credentials?

A: I really like Bruce Schneier's explanation and approach here. It's easy to read and makes a lot of sense. https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

A few months ago, NIST released new guidance for passwords in NIST SP 800-63-3 (Digital Identity Guidelines) this year. The new recommendations from them include removing periodic password change requirements, dropping arbitrary complexity requirements, and requiring screening of new passwords against lists of commonly used or compromised passwords. You can find the guidance here: https://pages.nist.gov/800-63-3/sp800-63b.html

By default, Niagara uses the Open Web Application Security Project (OWASP) policy on password complexity when you add users, but you can certainly modify the complexity rules to conform to your standard. See OWASP's section on password complexity here: https://www.owasp.org/index.php/Authentication_Cheat_Sheet#Password_Complexity.

We also recommend you look at the Niagara 4 Hardening Guide. The first section of that document (pages 5-12) focus on configuring password strengths, expiration of passwords, making sure that users don't use previously used passwords, and more. Niagara has features that can be configured based on the security policy of your organization. Finally, Appendix A of that document has a section on "choosing strong passwords that are actually strong." The Niagara 4 Hardening Guide with all that information can be found here: https://www.tridium.com/~/media/tridium/library/documents/niagara%204%20hardening%20guide.ashx?la=en

Q: What about using password vaults?

A: There are definitely some good software-based password managers/password vaults on the market. As a policy, we don't recommend one particular brand, but there is a good article on PCMag.com from last week analyzing some of them: https://www.pcmag.com/g00/article2/0,2817,2407168,00.asp

Q: What's the difference between SSL and TLS? I know that there have been vulnerabilities associated with SSL and some versions of TLS. What version of TLS does Niagara support?

A: Here's some history:

1. Secure Sockets Layer (SSL) was invented by Netscape for the Netscape browser over 20 years ago. After it was mostly finalized, it was sent to a standards body (IETF), who did more work on the specification and released it as SSL 3.0 back in 1996.

2. Transport Layer Security (TLS) 1.0 was then released as a minor upgrade of SSL 3.0. This is why, for so long, people used TLS and SSL interchangeably. Most of us kept calling it "SSL." TLS also was created with the ability to "downgrade" to older versions (so downgrading to a SSL connection from TLS)
3. TLS 1.1. was released in 2006 with security enhancements
4. TLS 1.2 was released in 2008 with more security enhancements.
5. TLS 1.3 is still in draft and hasn't been released.

Starting around 2014, a series of vulnerabilities were reported against SSLv3, starting with the POODLE attack. When these occurred, Tridium responded to them with Technical Bulletins which can be found on our web page https://www.tridium.com/en/resources/library, providing guidance for all users of Niagara systems to configure their systems to disable SSL completely and instead use TLS.

Since then, a number of vulnerabilities were reported against TLS – some of these involved the ability to "downgrade versions from TLS to SSL", and some related to the cipher suites used by TLS. As a result, we did security update builds of AX and have continued to update Niagara 4 to make sure that we only use the accepted Ciphers and disabled the use of SSL.

Right now, Niagara 4 uses TLS 1.2 and the accepted ciphers. The JACE-8000, running either Niagara 4 or Niagara AX uses the same. The latest version of Niagara AX uses TLS 1.0 and accepted ciphers, but an upcoming release (3.8 update 3) will include TLS 1.2.

Q: Where can we find information about TLS Certificates when using HTTPS or TLS? When using the higher security, the browser tends to throw warnings to the user when the self-signed or default certificate is used. Is there a way no to have the warning come up for the customer?

A: In order to make certain that Niagara systems have encrypted protocols running by default, your installation generates and sets up a self-signed certificate for your Niagara system just so that you can have confidentiality and integrity of your communications.

Having said that, the self-signed certificate is really just a *placeholder* to get you started, and even though it is valuable because it enables your system to have encrypted communications, you miss out on the other things that certificates typically bring you. As your question highlights, your browser will give you a warning because of two reasons: (1) the default certificate is *self-signed* and (2) it doesn't match the host name of your system, so the browser doesn't have non-repudiation of your station's identity. Here's why your browser will give you warnings:

1. Because your certificate is *self-signed*, it means that the certificate hasn't been issued by a trusted third party Certificate Authority (CA) that is in your browser's trust store. (Your browser comes preloaded with trusted certificates of CAs from places like DigiCert or Symantec). If your certificate isn't signed by one of those that are installed in your browser, it means that the browser will throw a warning because it only trusts certain CAs to sign certificates.
2. Because your certificate doesn't match the hostname of your web site, your browser will throw a warning, because it thinks that there may be a risk that a web site is pretending to be another web site.

In order to not have the warnings, a CA that is trusted by your browser needs to issue a certificate to your system that *matches your machine's hostname*. This could be an *internal* CA

that you have for your organization (and you can certainly set one up, and you can even set up a CA with Niagara Certificate management tools), but the trick is that your browsers also need to trust the Certificate Authority. The process goes something like this:

- For your host machine, you generate a private-public key pair and a Certificate Signing Request (CSR) that is sent to a Certificate Authority (CA). You do this using Niagara Certificate management tools, and when you do this, make sure you issue a request for a certificate that matches your machine's hostname.
- The CA takes that CSR that it receives, validates your identity and then issues your certificate (which is essentially your public key, plus your hostname and other identifying information, all signed by the CA).
- You then import the certificate you received into Niagara's User Key Store of the platform/station, using Niagara's Certificate Management tools
- You will need to import the CA certificate into the Niagara User Trust Store, so that Niagara will trust it.
- If the CA is not already in the trust store of your browsers (and if it is an internal CA, it won't be), your browser clients will also have to import the CA certificate so that it trusts the server certificate. (Chrome, Firefox, and IE all have instructions on how to do this.)

Once your station and platform is set up with a certificate that (1) matches your hostname, and (2) is trusted by your browser, you should no longer see those warnings.

You can see more information in Niagara's Station Security Guide that comes with Niagara (in docSecurity).

Q: Will there be a separate session on certificates? It is a very important part of securing communications and is sometimes difficult to comprehend, what and why one would replace certificates and so on.

A: This is a great suggestion. James Johnson provides great training in this area, and did so at the last Niagara Summit. We will see if we can schedule something like this in the future.

Q: If only a single port is exposed on the internet through firewall like 4911, why is a single port such a risk?

A: There are multiple reasons (and I'll get to this later in my answer), but one big reason comes to mind - If *any* system is exposed on the Internet, even if it is communicating via an encrypted protocol, it can be vulnerable to a Denial of Service (DoS) attack that can threaten the operations of your system. Because of the nature of how TCP/IP works, any request sent to a port on a system needs to be parsed and processed by that system even if it is not a legitimate request. If a large number of these requests happen in a short period of time, *any* system has the potential of becoming overwhelmed to the point of exhausting its resources (CPU, memory), and the system might slow down, lose the ability to process legitimate data, or even lose the ability to perform its operations. This is exactly what happens in a DoS attack.

In October 2016, a large number of IoT devices were hacked and repurposed together in a massive botnet to inundate DNS servers with requests in what is known as a Distributed Denial of Service (DDoS) attack, and as a result, many sites on the Internet were brought down. This is certainly not a new type of attack, but it does demonstrate that *all* systems (even DNS servers which are fairly fault-tolerant and redundant) can potentially be at risk.

So, as an answer to your question, a malicious attacker could inundate your system with requests, and because your system has a finite amount of memory and processing power, it could slow down your system to the point where *all* operations are at risk.

When you expose a device on the Internet, you expose its capabilities. Port scanning can reveal what type of software your product is running, and in many cases, what version of your software to give any potential attacker valuable information that can be used in an attack against your system. In the Tridium Talk, I mentioned an analogy involving your home – even if you have a great security system and state-of-the-art locks, would you put a sign in your front yard advertising the contents of your house? Exposing a system on the Internet is a lot like that. Don't tempt potential hackers.

We strongly recommend not exposing your systems on the Internet. See our presentation from the Tridium Talk about setting your network up with Defense-in-Depth principles, and protecting your systems behind other security infrastructure and a VPN security gateway to protect your systems.

Q: On encryption: can you encrypt BACnet communication?

A: BACnet communication can be encrypted between sites using industry standard VPN technologies, but the typical use of BACnet in most facilities does not include transmission confidentiality and integrity. Niagara can communicate with a BACnet network and BACnet devices using the Niagara Bacnet driver, but the JACE itself should not expose those devices on a TCP/IP network at this time. Instead, it is important that the JACE isolates BACnet devices from the rest of the network (which is what it is designed to do.)

Q: When will code signing be supported for both 3rd party modules and program objects?

A: While code signing for 3rd party code is *supported*, it isn't mandatory at this point. For example, if you sign a JAR that is used in Niagara, the Java Runtime Engine will confirm that it has not been tampered with. We do eventually want Niagara developers to sign their code, but before we actually enforce that and make it mandatory in the framework, we want to make sure that we (1) add tools to make this easier for developers, and (2) communicate this and educate the community well in advance.

Q: Is there a tutorial about how to sign a program object?

A: There is new documentation that will be released as part of Niagara 4.4 on signing program objects, so that will be coming soon.

Q: Can you tell us about SAML user authentication coming up in Niagara 4?

A: In an upcoming release, we will be including the ability for you to configure your Niagara system to do Single Sign-On with a SAML2-based Identity Provider (IdP). So, if your organization utilizes a SAML-based IdP, you will be able to configure all of your Niagara systems to utilize that IdP for Single Sign-On across all of your Niagara stations. Stay tuned!

Q: There was mention of Cloud services to be released by the end of this month. Any word on what those are?

A: Backup as a Service will be released at the end of this month. Stay tuned!

Q: Backup as a Service: will the backup be scanned for malicious code? Is there any information on how to set it up?

A: Backup as a Service creates a backup much like a Niagara backup is created today – with one exception – your backup will be encrypted using your Niagara system's passphrase, before it is streamed to the Cloud over an encrypted tunnel that provides both confidentiality, integrity, and non-repudiation of the identity of the streamed-to service. So, although we don't have plans to scan your Niagara backup for specific threats, the multiple layers of encryption in our solution (both at rest and in motion) will provide significant protection that would reduce any risk of any malicious third party altering a backup that you create. You'll see more information on this soon.

Q: When we post data on Cloud, is it not the responsibility of the Cloud companies to provide cybersecurity?

A: The Cloud provider is typically responsible for providing a certain level of cybersecurity and security controls for its customers, and the developer of the services and applications on those Cloud providers is responsible for developing and implementing those services and applications in a secure manner with proper security controls.

Q: Can you explain "sandboxing" and how this affects security embedded in JACE modules.

A: Niagara 4 introduced the Java Security Manager, which places authorization restrictions in code running in Niagara. Many modules do not have the permissions to run code that handles sensitive data or accesses files. This helps protect Niagara 4 systems from inadvertent or malicious tampering.

Starting in Niagara 4 version 4.2, modules can request additional permissions to the baseline granted to all modules. These permissions allow modules to perform certain specific tasks such as authenticating users via an authentication scheme, opening sockets, or reading system properties.

When installing new modules, care should be taken to inspect what permissions these modules are requesting and make sure that they match up with the functionality the module claims. For example, a module claiming to add a new UI scheme should probably not be opening a socket to www.super-suspicious-URL.com. For more information, please see our Niagara 4 Hardening Guide on our web site.

Q: How is Tridium addressing DOD ufc_4_010_06_2016_c1? It is based on ICS but not the same?

A: The Department of Defense Unified Facilities Criteria includes requirements for incorporating cybersecurity into the design of facility related control systems in order to address the federal Risk Management Framework (RMF) security controls during design and subsequent construction. RMF is the unified information security framework for the entire federal

government, replacing the legacy Certification and Accreditation (C&A) process within government departments and agencies. Niagara is now eligible for accreditation under the federal Risk Management Framework (RMF). Tridium has completed a suite of RMF artifacts for Niagara 4 and JACE 8000 to be used for pending type authorization under RMF. For more information, see:
https://www.tridium.com/~/media/tridium/government/tridium%20rmf%20overview%20and%20faq.ashx?la=en

Q: I might've missed this but are you planning on putting a VPN client that is integrated into the JACE or web Supervisor?

A: Right now, we recommend complementing the capabilities of the JACE with separate security infrastructure and a VPN solution.