INL/CON-20-58484-Revision-1

Deconstructing the Nuclear Supply Chain Cyber-Attack Surface

July 2020

Shannon Leigh Eggers, Michael Rowland

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-20-58484-Revision-1

Deconstructing the Nuclear Supply Chain Cyber-Attack Surface

Shannon Leigh Eggers, Michael Rowland

July 2020

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Proceedings of the INMM 61st Annual Meeting
July 12-16, 2020 Baltimore, MD, USA

Deconstructing the Nuclear Supply Chain Cyber-Attack Surface

Shannon Eggers
Idaho National Laboratory
Idaho Falls, ID 83415
shannon.eggers@inl.gov

Michael Rowland
Sandia National Laboratories
Albuquerque, NM 87195
mtrowla@sandia.gov

ABSTRACT

The nuclear supply chain cyber-attack surface is a large, complex network of interconnected stakeholders and activities. The global economy has widened and deepened the supply chain, resulting in larger numbers of geographically dispersed locations and increased difficulty ensuring the authenticity and security of digital assets. Although the nuclear industry has made significant strides in securing facilities from cyber-attacks, the supply chain remains vulnerable. This paper provides further details on each of the elements in the Digital I&C Supply Chain Cyber-Attack Surface [1], including supply chain lifecycle activities, key stakeholders, touchpoints, and attack types. Deconstructing this attack surface provides insights into supply chain threats, vulnerabilities, and consequences. These insights will lead to improvements in cybersecurity supply chain risk analysis, development of new cybersecurity supply chain processes and tools, and enhancement of overall supply chain resilience.

INTRODUCTION

The objective of traditional supply chain risk management (SCRM) is to minimize cost while ensuring product availability and quality in the face of threats, such as environmental, geopolitical, and financial disruptions. The supply chain for digital technology includes an additional security objective to ensure that authenticity, integrity, confidentiality, and exclusivity are maintained in the face of cyber threats. Authenticity assures the components are genuine; integrity assures the components are trustworthy and uncompromised; confidentiality assures there are no unauthorized loss of data or secrets; and exclusivity assures there are limited touchpoints to reduce the number of attack points. With the increasing use of digital instrumentation and control (I&C) in both existing nuclear power plants (NPPs) and in new advanced reactors, the nuclear industry must remain diligent in monitoring and evaluating the evolving cyber threat landscape in their supply chains.

Cybersecurity risk is a function of threats, vulnerabilities, and consequences, including likelihood of attack success given the threats and vulnerabilities. To fully analyze the threats and vulnerabilities in the supply chain, it is first necessary to understand its cyber-attack surface. Deconstructing this supply chain cyber-attack surface and using it to explore vulnerabilities exploited by known supply chain cyber-attacks provides awareness into the cybersecurity controls required to protect an NPP's supply chain. Identifying these controls and any current implementation gaps enables improvement of supply chain protections to defend against increasingly sophisticated supply chain cyber-attacks.

BACKGROUND

Every digital I&C device contains many components and subcomponents including, hardware, firmware, and software. The lifecycle of digital systems (composed of multiple digital devices) typically involves multiple tiers of globally dispersed vendors or suppliers. This network includes designers, developers, contractors, manufacturers, integrators, solution providers, and logistics providers. This complexity provides numerous possibilities for an adversary to compromise a device or acquire system information prior to installation and operation within an NPP. The challenge is how to reduce risks associated with compromise (e.g., cyber-attack) of elements within the supply chain.

Vulnerabilities are weaknesses or flaws that an adversary can exploit. The cyber supply chain is vulnerable at stakeholder and transition touchpoints that lack the necessary security measures to protect against compromise or loss of system information. Since sophisticated adversaries research their target to identify the attack vector with the highest likelihood of success, those stakeholders and touchpoints without effective information and communications technology (ICT) and operational technology (OT) security controls are more vulnerable to supply chain compromises.

Attack surfaces have long been used to provide a measure of an asset’s susceptibility to compromise. Attack surface is defined in [2] as a list of system inputs that an attacker can use to attempt to compromise a system. Reducing a device’s attack surface decreases its susceptibility to attack, thereby decreasing its cybersecurity risk.

Typically, a cyber-attack surface defines entry points for a device or system an adversary can use to compromise a system during operation. A supply chain cyber-attack surface, on the other hand, defines entry points an adversary can use to compromise a system during supply chain activities. The supply chain cyber-attack surface includes all possible touchpoints for each of the components within the design of the final product.

The concept of attack surface has been applied to SCRM. Most notably, Miller developed a supply chain attack framework based on the Department of Defense systems acquisition lifecycle that incorporated concepts from NIST SP 800-30 Rev 1 [3], Common Attack Pattern Enumeration and Classification (CAPEC) [4], and Threat Assessment and Remediation Analysis (TARA) [5]. Miller identified eight different points of attack at supply chain locations and logistical linkages, as shown in Figure 1 and Figure 2. From this framework, 41 supply chain attack patterns were enumerated using 12 different attack attributes [6].

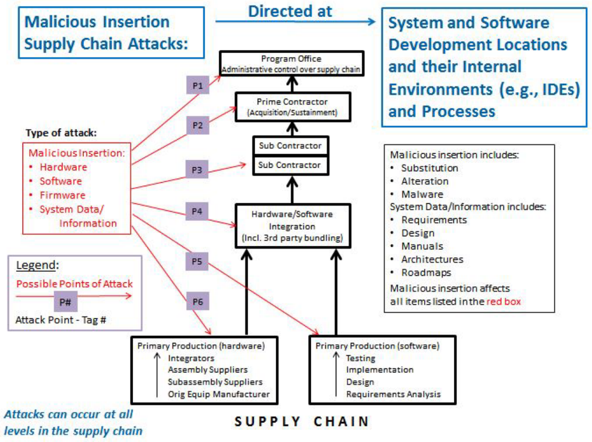
Malicious Insertion
Supply Chain Attacks:
Directed at
System and Software Development Locations and their Internal Environments (e.g., IDEs) and Processes
Program Office
Administrative control over supply chain
Prime Contractor
(Acquisition/Sustainment)
Sub Contractor
Sub Contractor
Hardware/Software Integration (Incl. 3rd party bundling)
P1
P2
P3
P4
P5
P6
Type of attack:
Malicious Insertion:
• Hardware
• Software
• Firmware
• System Data/ Information
Malicious insertion includes:
• Substitution
• Alteration
• Malware
System Data/Information includes:
• Requirements
• Design
• Manuals
• Architectures
• Roadmaps
Malicious insertion affects all items listed in the red box
Legend:
Possible Points of Attack
P#
Attack Point - Tag #
Primary Production (hardware)
Integrators
Assembly Suppliers
Subassembly Suppliers
Orig Equip Manufacturer
Primary Production (software)
Testing
Implementation
Design
Requirements Analysis
Attacks can occur at all levels in the supply chain
SUPPLY CHAIN

Figure 1. Points of attack—supply chain locations [6].

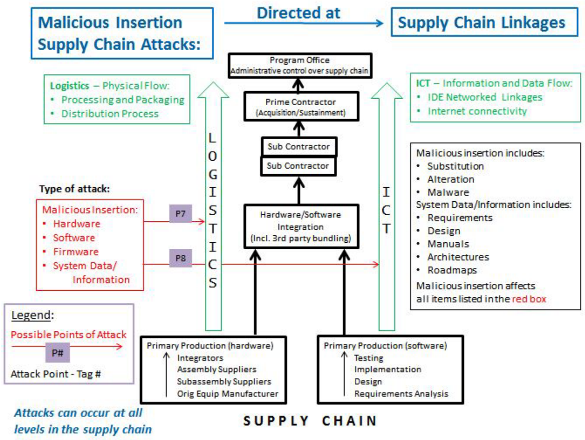

Figure 2. Points of attack—supply chain linkages [6].

DECONSTRUCTING THE SUPPLY CHAIN CYBER-ATTACK SURFACE

Figure 3 provides a single dashboard for managing overall cyber supply chain risk [1]. This supply chain cyber-attack surface extends the work of Miller [6] and incorporates insights from other leading researchers [7-10]. The attack surface includes systems engineering and supply chain lifecycle activities, including individual flow paths for hardware, firmware, and software design and development activities as well as flow paths for final integration, testing, installation, maintenance, and decommissioning activities. The supply chain attack surface also includes the various design and programming tools as well as the confidential and proprietary system information that has the potential to be exposed or compromised along each of the pathways.

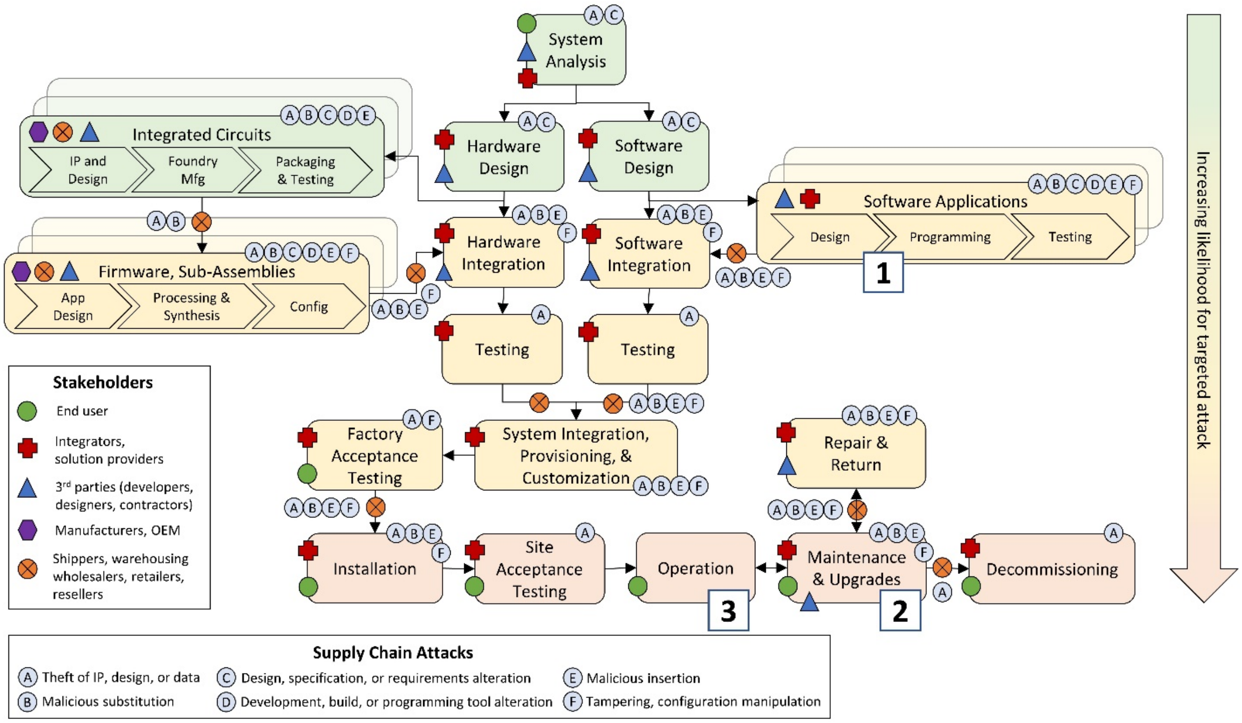

Figure 3. The digital I&C supply chain cyber-attack surface [1].

Attack Types

Whereas the CAPEC hierarchy of 41 supply chain exploits is grouped, in part, by lifecycle phase (i.e., during manufacture, during distribution), the taxonomy of supply chain attacks listed in Figure 3 are related to "how" the attack at a stakeholder is conducted. These supply chain cyber-attack types are described in Table 1.

The supply chain attacks listed in Table 1 are not specific to a certain stakeholder or lifecycle phase. For instance, malicious software insertion could occur at various locations throughout the lifecycle, such as during software development, integration or factory acceptance testing, final installation during commissioning activities, as well as all the storage locations or repositories along the way. Figure 3 identifies those touchpoints where the attacks are likely to occur.

Table 1. Taxonomy of supply chain cyber-attack types in Figure 3.

Attack Type	Description
Theft of IP, design, or data	Unauthorized disclosure of information from a stakeholder who has a trust relationship with the end target, enabling future attacks and/or causing economic loss. This may include but is not limited to intellectual property (IP), design information, operational/configuration data, or stored secrets (i.e., private key, digital certificates).
Malicious substitution	Complete replacement of digital technology, including hardware, firmware, and/or software. Hardware clones or counterfeits may not impact all end users depending on the distribution, whereas a substituted software package may compromise all end users even if only a few were targeted.
Design, specification, or requirements alteration	Unauthorized modification of design, specifications, or requirements that compromises the design stages and results in the purposeful inclusion of latent design deficiencies (e.g., requirements that result in vulnerabilities) or built-in backdoors.
Development, build, or programming tool alteration	Unauthorized modification of the development environment, including platform, build and programming tools, with the intent to corrupt the device under development.
Malicious insertion	Addition or modification of information, code, or functionality directly into a device to cause malicious intent, such as impairing or altering device operation or function.
Tampering, configuration manipulation	Unauthorized alteration or fabrication of configuration, non-executable data, or sending of unauthorized commands with the goal of impacting device operation or function.

Stakeholders

Consistent with the Responsible, Accountable, Consulted, Informed (RACI) matrix, the stakeholders identified in Figure 3 reflect the entity or entities responsible for performing the activities within a specific systems engineering lifecycle phase. While a stakeholder may also have other roles throughout the lifecycle, only the responsible role is identified on the diagram. For example, an NPP end user will typically have responsibilities during the initial systems analysis phase but then may have no further responsibilities until the factory acceptance phase.

The RACI roles may vary depending on whether the item or system procured is commercial-off-the-shelf (COTS), engineered, or built in-house. Depending on the type of item and its unique supply chain lifecycle, an entity may have multiple stakeholder roles. For instance, an NPP that designs and custom builds a system for a unique application will have different RACI roles than an NPP procuring a COTS intelligent pressure transmitter.

Often, there is much better visibility with first-tier suppliers and contractors than with second-tier or lower providers. In fact, current regulatory guidance in the nuclear industry primarily focuses on how the NPP (i.e., end user) can develop security controls and acquisition guidance for buying and transporting products from an integrator or solutions provider to the plant.

Touchpoints

Touchpoints in the supply chain cyber-attack lifecycle are defined as those points where a component or system could be compromised, such as the stakeholder's physical location, as well as electronic storage locations or repositories. Touchpoints also include the transitions between stakeholders, whether it is shipment of an integrated circuit (IC) to the assembly location or electronic transmission of a software update from a website to an end user's installed product. Devices are often most vulnerable during transitions moving from one trustworthy environment through an unsecured distribution channel to another trustworthy environment.

Mapping of Publicly Acknowledged Supply Chain Attacks

Table 3 includes a listing of publicly acknowledged supply chain attacks. Each of these attacks are mapped back to the attack types identified in the supply chain cyber-attack surface. The lifecycle phase during which the exploit occurred is also indicated. In some attacks, such as ShadowHammer, a supplier's update utility was compromised during one lifecycle phase (i.e., digital distribution and storage phase), while the end user was compromised during another phase (i.e., maintenance and upgrades) when they downloaded the compromised software. Using the supply chain cyber-attack surface to analyze and characterize prior attacks can identify whether an NPP's existing supply chain security controls implemented based upon regulatory guidance would effectively prevent or detect the attack.

U.S. NUCLEAR SUPPLY CHAIN CYBERSECURITY GUIDANCE

In the U.S. nuclear industry, SCRM historically involved efforts to detect and mitigate risks associated with Counterfeit, Fraudulent, and Suspect Items (CFSI) to ensure that only products and services of the required quality were used within nuclear facilities [11]. Since CFSI is a quality issue, safety analyses and processes evolved to cover these risks. However, with the increasing risks associated with cyber-attacks, the U.S. Nuclear Regulatory Commission (NRC) issued 10 CFR 73.54, *Protection of digital computer and communication systems and networks* [12]. Acquisition guidance was specifically provided in section C.3.3.3.1 [13] of Regulatory Guide 5.71 and section E.11 of NEI 08-09 [14]. Subsequent publication of NEI 08-09 Addendum 3 in 2017 updated section E.11 with further guidance as outlined in Table 2.

Table 2. NEI 08-09 Addendum 3, Appendix E, Section E.11, System and Services Acquisition [15].

Section #	Heading	Content
E.11.1	System and Services Acquisition Policy and Procedures	Development of formal policy
E.11.2	Supply Chain Protection	Validation of vendors, establishment of a trusted distribution path, and use of tamper-evident or tamper-proof seals
E.11.3	Trustworthiness	Apply software quality assurance and minimize flaws
E.11.4	Integration of Security Capabilities	Threat-informed procurement with vulnerability management
E.11.5	Developer Security Testing	Inclusion of security control testing in factory acceptance tests
E.11.6	Licensee Testing	Inclusion of security control implementation validation in site acceptance testing

Table 3. Publicly acknowledged supply chain attacks mapped to the supply chain cyber-attack types and lifecycle phase of the supplier.

Attack Type	Phase	Public Attack	Supplier	Attack Description	End Target
Theft of IP	Software design	Stuxnet	RealTek JMicron	Theft of private key used for signing software (digital certificates) [16].	Iran's Natanz Facility
Theft of IP	Maintenance	Target Breach	Fazio Mechanical Services	Theft of credentials via Citadel Malware to gain access to Target's web application hosted on Target's internal network [17].	Target customer & their financial institution
Theft of IP	Software design	Duqu 2.0	Foxconn	Theft of private key used for signing software (digital certificates) [18].	Kaspersky
Malicious substitution	Digital storage, upgrades	ShadowHammer	Asus	Substitution of Asus Update utility with malicious copy containing backdoor [19].	600+ MAC addresses; end user/consumer
Malicious substitution	Digital storage, upgrades	Dragonfly/Havex	eWon MB Connect Line Mesa Imaging	Vendor software downloads were compromised to include Remote Access Trojan (RAT) malware.	Initial belief—Energy sector. Current belief—pharmaceutical industry [20]
Design, specification, or requirements alteration	Software design and programming	Dual_EC_DRBG random number generator	RSA	Weakness in the cryptographically secure pseudorandom number generator design allowed for a hidden backdoor [21-23].	Multiple targets—end user of RSA BSafe for the entity with the private key to the potential backdoor
Development, build, or programming tool alteration	Software design and programming	XcodeGhost	Apple App Store	Malicious version of Xcode (Apple's development environment) available on 3rd party sites. Compiler resulted in compromised apps [24].	Apple iOS device data and user information [25].
Malicious insertion	Maintenance	Stuxnet	Iranian ICS Vendors	Malicious insertion of malware into five Iranian ICS vendors [26, 27].	Iran Natanz Facility
Malicious insertion	Maintenance	Target Breach	Target point of sale devices	Insertion of custom malware during maintenance to capture Target customer credit card data [17].	Target customer & their financial institution
Tampering, configuration alteration	Maintenance	SQL Slammer Worm	Davis Besse NPP consultant	Consultant connected a T1 line behind the corporate firewall bypassing all access control policies. The worm propagated to the plant network, causing a buffer overflow, and unavailability of plant systems.	SQL Server implementations with windows authentication.
Tampering, configuration alteration	Maintenance	Target Breach	Target Corporation	Addition of new Domain Admin User "best1_user" [17]	Target customer & their financial institution

NEI 08-09 Addendum 3 provides a set of supply chain security controls applicable from the factory acceptance testing (FAT) stage through decommissioning stage of the lifecycle (as also indicated as the end user on Figure 3). These controls are specifically focused on those activities where the licensee has responsibility within the supply chain. While overall cyber supply chain risk generally increases as the product progresses through the lifecycle (as indicated by the attack surface in Figure 3), compromises can still occur upstream of the FAT in phases where the licensees have little to no responsibility or visibility. Failure to address cybersecurity earlier in supply chain may result in unmitigated cyber risk if downstream security controls do not detect or prevent the compromise.

Addendum 3 does not include security control requirements for subcomponents, such as ICs or software libraries, that comprise the final product. While the intent of Addendum 3 is to shift those subcomponent requirements to the integrator by requiring use of a ‘validated vendor,’ the ultimate cyber risk falls on the licensee. Failure of the licensee to address subcomponents leaves the licensee vulnerable to unmitigated cyber supply chain risk.

More recently in 2018, the Electric Power Research Institute (EPRI) published revision 2 of the ‘Cyber Security in the Supply Chain’ technical report [28]. This EPRI supply chain report integrates EPRI’s Technical Assessment Methodology (TAM), which is intended to provide a risk-informed approach to vulnerability identification and mitigation [29]. The EPRI supply chain report provides a graded approach to procurement based on whether a component is a COTS or catalog product, an engineered product, or a custom/integrated product. The acquisition methodology outlined includes supplier questionnaires, cyber-related procurement language, secure product transitions, supplier certifications, testing, configuration management, and installation considerations [28].

In comparison to NEI 08-09 Addendum 3, the EPRI report provides a clear methodology for stepping through the creation of high-level supplier questionnaires and procurement specifications to help identify vulnerabilities and reduce risk. While this process provides additional support to the licensee, establishing a risk-informed supply chain by using the asset’s operational attack surface and the product type (i.e., COTS, catalog, engineered product) may not fully identify and address all the risks within the supply chain cyber-attack surface. For instance, a COTS item may be purchased either as a stand-alone component or as a component within a more complex custom solution developed by in-house personnel or outside suppliers and integrators. In addition, the ubiquitous use of COTS components, such as ICs, open-source software, and third-party libraries in catalog, engineered, and in-house custom products expands the supply chain attack surface since these common components may be purchased from a wide selection of distributors or downloaded from multiple online sources. Often, the end user is unaware that these subcomponents exist or that common design and development tools were used.

CASE STUDY: HYPOTHETICAL SUPPLY CHAIN ATTACK DURING PROCUREMENT OF ENGINEERED, NON-SAFETY CRITICAL DIGITAL ASSETS

This case study considers a hypothetical attack using a combination of two attack types—theft of IP and malicious substitution—to compromise an end user’s digital device or system. During the initial attack, a reputable vendor’s private keys used to sign code are stolen during the software design and development phase (Figure 3, Step 1). The adversary then corrupts vendor update channels and maliciously substitutes a software package using the stolen digital signature or hash. The end user downloads the compromised software package during the maintenance and update lifecycle phase

(Figure 3, Step 2). Once installed on the targeted device, the malware activates after any applicable triggering conditions are met (Figure 3, Step 3).

In accordance with E.11.1 in NEI 08-09 Addendum 3, cyber security requirements for non-safety-related direct critical digital assets must be included in plant procurement programs [15]. The other five controls listed in Table 2 are also applicable. Analysis of this hypothetical attack against these Addendum 3 requirements suggests that the recommended security controls may be inadequate to prevent the attack. For instance, the theft of private keys used in signatures would allow for an adversary to directly avoid the controls of E.11.2 (Supply Chain Protection), specifically the ability to overcome the checking of digital signatures and/or hashes. Similarly, the EPRI recommendations for use of secure electronic delivery and integrity tools, such as secure storage areas, cryptographic hashes, and digital signatures would not guarantee prevention or detection of an attack if the adversary has access to the vendor's private key(s).

Additionally, compromising a vendor's digital storage environment and deploying maliciously substituted software would circumvent the E.11.5 (Developer Security Testing) controls and EPRI supply chain report test recommendations as these tests look for known vulnerabilities and malware. Since this attack exploits undisclosed (or untestable) vulnerabilities, these testing security controls and recommendations would not detect it.

Furthermore, the E.11.6 (Licensee Testing) control will not detect this hypothetical attack if the licensee's testing environment does not contain the expected characteristic or attribute to activate the malicious code. ShadowHammer is an example of an exploit that requires activation—the attack is only launched if the device has a predefined MAC address [19]. The Volkswagen emissions scandal is another example—the software, or 'defeat device,' activates emissions controls only when it senses a vehicle is placed into emissions testing [30]. Similar techniques have also been deployed by adversaries to evade sandbox detection [31]. The EPRI supply chain report includes mitigations such as downloading and reinstalling software separately, vulnerability, malware, and forensics scans, and additional functional testing; however, similar to the Addendum 3 controls, these recommendations would likely result in the compromise remaining undetected if the attack elements remain untriggered in the test environment.

From the analysis of this hypothetical attack, it is evident that many historical supply chain attacks, including ShadowHammer and Dragonfly, may remain undetected if an NPP operator (i.e., end user) relied solely on Addendum 3 controls. In contrast, use of the supply chain cyber-attack surface assists in identifying additional security controls that could prevent or detect this attack. Specifically, adding additional requirements for suppliers (and the Certificate Authorities) to increase activities with respect to digital signatures, such as increased vigilance and protection of private keys as well as declaration of signature dates and versions from an alternate channel, could allow for both developer (E.11.5) and licensee (E.11.6) testing to explicitly validate that verified signatures are used. This requirement could be added to the E.11.4 (Integration of Security Capabilities) control. In addition, including requirements on the use of digital certificates in the E.11.3 (Trustworthiness) control could assist with verification of the sender's trustworthiness. And finally, requirements for detecting or mitigating 'defeat devices' or sandbox evasion techniques could be included into the E.11.4 control to inform testing methodologies.

CONCLUSIONS

This paper deconstructs the supply chain cyber-attack surface established in [1], providing additional detail on supply chain lifecycle phases, stakeholders, and touchpoints. It also introduces descriptions of the attack types and maps them to publicly disclosed supply chain attacks. An analysis of a hypothetical, dual-threat supply chain cyber-attack indicates that an NPP operator using only the supply chain security controls outlined in NEI 08-09 Addendum 3 needs to emphasize the importance of the E.11.4 control to 'threat-inform' the other controls. In the absence of this E.11.4 control, the NPP operator will potentially be more susceptible to supply chain cyber-attacks. Follow-up analysis using the supply chain cyber-attack surface advocates that use of the diagram provides improved vulnerability identification leading to threat-informed security controls. Future research will explore how this supply chain cyber-attack surface can improve supply chain cybersecurity resilience by providing a roadmap for comprehensive and systematic risk reduction through risk identification, assessment, evaluation, and treatment.

ACKNOWLEDGEMENTS

Idaho National Laboratory is operated by Battelle Energy Alliance for the U.S. Department of Energy Office of Nuclear Energy under DOE Idaho Operations Office, contract DE-AC07-05ID14517. Sandia National Laboratories is a multi-program laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy National Nuclear Security Administration under contract DE-NA0003525.

REFERENCES

[1] Eggers, S., "The nuclear digital I&C system supply chain cyber-attack surface," in *Transactions of the American Nuclear Society*, Annual Meeting 2020, vol. 122: American Nuclear Society.

[2] Cole, E., "ICS Attack Surfaces," in *SANS Asia Pacific ICS Security Summit and Training*, Singapore, 2013.

[3] *NIST Special Publication 800-30. Revision 1. Guide for conducting risk assessments*, 2012.

[4] *CAPEC: Common Attack Pattern Enumeration and Classification*. The MITRE Corporation. Available: https://capec.mitre.org/

[5] Wynn, J. *et al.*, "Threat assessment & remediation analysis (TARA): Methodology description, Version 1.0," The MITRE Corporation, 2011.

[6] Miller, J.F., "Supply chain attack framework and attack patterns," The MITRE Corporation, MacLean, VA, 2013.

[7] Boyens, J., C. Paulsen, R. Moorthy, N. Bartol, and S.A. Shankles, "NIST Special Publication 800-161 Supply chain risk management practices for federal information systems and organizations," 2015.

[8] Heinbockel, W.J., E.R. Laderman, and G.J. Serrao, "Supply chain attacks and resiliency mitigations," The MITRE Corporation, 2017.

[9] Liu, B. and G. Qu, "VLSI supply chain security risks and mitigation techniques: A survey," *Integration*, vol. 55, pp. 438-448, 2016.

[10] Shackleford, D., "Combatting cyber risks in the supply chain," *SANS.org*, 2015.

[11] *Guidance documents and background information for Counterfeit, Fraudulent, and Suspect Items (CFSI)*. U.S. Nuclear Regulatory Commission, Accessed on: March 10, 2020. Available: https://www.nrc.gov/about-nrc/cfsi/guidance.html

[12] *10 C.F.R. § 73.54, Protection of Digital Computer and Communication Systems and Networks,* U.S. Nuclear Regulatory Commission, 2009.

[13] "Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities," U.S. Nuclear Regulatory Commission, January 2010.

[14] "NEI 08-09, Cyber security plan for nuclear power reactors, Revision 6," Nuclear Energy Institute, April 2010.

[15] "Addendum 3 to NEI 08-09, Cyber security plan for nuclear power reactors, Revision 6, Systems and Services Acquisition," Nuclear Energy Institute, August 2017.

[16] Bencsáth, B., G. Pék, L. Buttyán, and M. Félegyházi, "Duqu: A Stuxnet-like malware found in the wild," *CrySyS Lab Technical Report,* vol. 14, pp. 1-60, 2011.

[17] "The untold story of the Target attack step by step," Aorato Labs, August, 2014, Available: https://aroundcyber.files.wordpress.com/2014/09/aorato-target-report.pdf.

[18] GReaT, "The Duqu 2.0 persistence module," Kaspersky, June 15, 2015, Available: https://securelist.com/the-duqu-2-0-persistence-module/70641/.

[19] GReAT and AMR, "Operation ShadowHammer: a high-profile supply chain attack," Kapersky, April 23, 2019, Available: https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/, Accessed on: November 14, 2019.

[20] "How Dragonfly hackers and RAT malware threaten ICS security," Belden, September 15, 2014, Available: https://www.belden.com/blog/industrial-security/how-dragonfly-hackers-and-rat-malware-threaten-ics-security, Accessed on: May 6, 2020.

[21] Kelsey, J. *Dual EC in X9.82 and SP 800-90*. National Institute of Standards and Technology. Available: https://csrc.nist.gov/csrc/media/projects/crypto-standards-development-process/documents/dualec_in_x982_and_sp800-90.pdf

[22] Schneier, B. (November 15, 2007) Did NSA put a secret backdoor in new encryption standard? *Wired*. Available: https://www.wired.com/2007/11/securitymatters-1115/

[23] Shumow, D. and N. Ferguson, "On the possibility of a back door in the NIST SP800-90 Dual EC Prng," in *Crypto 2007 Rump Session*, 2007.

[24] Xiao, C., "Malware XcodeGhost infects 39 iOS apps, including WeChat, affecting hundreds of millions of users," PaloAlto Network Unit 42, September 18, 2015, Available: https://unit42.paloaltonetworks.com/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/, Accessed on: May 6, 2020.

[25] Xiao, C., "Update: XcodeGhost attacker can phish passwords and open URLs through infected apps," PaloAlto Network Unit 42, September 18, 2015, Available: https://unit42.paloaltonetworks.com/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/, Accessed on: May 6, 2020.

[26] Zetter, K., *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. New York: Broadway Books, 2014.

[27] Falliere, N., L.O. Murchu, and E. Chien, "W32.Stuxnet dossier, Version 1.4," Symantec, 2011.

[28] "Cyber Security in the supply chain: Cyber security procurement methodology, Revision 2," Electric Power Research Institute, 2018.

[29] "Cyber security technical assessment methlodology, Vulnerability identification and mitigation," Electric Power Research Institute, 2016.

[30] Schiermeier, Q., "The science behind the Volkswagen emissions scandal," *Nature News,* 2015.

[31] Roccia, T., M.R. Lopez, and C. Shah, "Evolution of malware sandbox evasion tactics - A retrospective study," McAfee, September 9, 2019, Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/.