NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Security Guideline for the Electricity Sector - Supply Chain

Provenance

The objective of the reliability guidelines is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure bulk power system (BPS). Reliability guidelines are not binding norms or parameters to the level that compliance to NERC's Reliability Standards is monitored or enforced. Rather, their incorporation into industry practices is strictly voluntary.

Introduction

Knowing the source of supply chain threats can help in designing targeted and effective defenses against counterfeiting, unlawful intrusion, industrial espionage, and other cyber-security breaches. The risks of not knowing the sources of threats occur at all stages of planning, development, installation, maintenance, and disposal.[1]

Risks and Possible Outcomes of Poor Provenance Awareness or Management

Table 1.1: Risks and Possible Outcomes. At a minimum, "provenance" helps ascertain whether a source is authentic (genuine or counterfeit). More fully, related to chain of custody and lineage, it entails traceability – having a "record of element origin along with the history of, the changes to, and the record of who made those changes."[2] Acquirers, integrators and suppliers should have best practices in provenance as a part of supply chain cyber-security. Good provenance requires tools and processes for identity management, access, tagging, tracing, and more.

Table 1.1: Risks and Possible Outcomes

Stage	Origination (Provenance) Risk	Possible Outcome
Planning	• Buyers not aware of adversaries or their actions • Provenance not considered in procurement process	• Adversaries operate undetected within active contracts, under subcontracts, or from outside • New contracts signed with no visibility past the immediate vendor

[1] Additional guidance for Supply Chain Security is at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

[2] National Institute of Standards and Technology (NIST) Notional Supply Chain Risk Management Practices for Federal Information Systems

Table 1.1: Risks and Possible Outcomes

Stage	Origination (Provenance) Risk	Possible Outcome
Development	• Equipment and software of unknown or unverified origin	• Adversaries operate invisibly through subcontracts • Open source software used with no vetting • Inadvertent dealings with Denied Persons • Remote connections hacked using stolen credentials or back doors
Installation	• Equipment and software of unknown or unverified origin	• Code is inserted or altered by Adversaries before insertion or use
Maintenance	• Equipment sent for repair or replacement without traceability • Weak access privileges • Weak Human Resource policies on personnel and access • Vendors don’t inform customers of vulnerabilities or threats	• Unknown third parties substitute or alter, inserting malware or security weaknesses, intentionally, to cut cost, or negligently • Adversaries make malicious critical configuration changes • Patches do more harm than good • Adversaries penetrate live sites • Vulnerabilities and threats undetected until it’s too late
Disposal	• No end-of-life disposal process	• Adversaries repurpose obsolete product or code with security vulnerabilities

Initial Best Practices in Supply Chain Provenance Management

Establish a policy that governs and limits development in adversarial environments

Establish a corporate data governance policy that limits the flow of development to riskier development environments. As an example, the U.S. Bureau of Industry and Security (BIS) establishes policies on commerce between the U.S. and foreign countries and maintains a list of Sanctioned Destinations.[3]

Monitor compliance against Denied Persons, Disapproved Vendors, and Related lists and orders

Establish procedural checks against lists of current and potential adversaries. Executive Order 13873 establishes criteria for prohibiting certain trade,[4] and the Department of Commerce maintains a Consolidated Screening List that is built from a Denied Persons List[5], an Entity List, and an Unverified List. In addition to screening, make sure procurement decisions take into account the ultimate beneficial owner, not just the party of record.[6] Most companies' procurement departments have approved vendors and some have a blacklist based on these or similar principles and tools.

Use standard contract language about provenance

Consider standard contract language regarding provenance. EEI provides four pages (pages 8-11) of contract language specifically designed to address CIP-013 Section R1.2.5.[7] Also, "Cybersecurity Procurement Language for Energy Delivery Systems" provides sample contract language for Account Management, Session Management, Logging and Auditing, and Secure Development.[8]

Require internal and external vendors to validate the authenticity and origins of third party hardware and software

Obtain confirmation from integrators and suppliers that outsourced products and services are from where they purport to be, which includes requiring vendors to identify open source products, at the prequalification stage. EEI's contract language (R1.2.5a on page 8) includes two paragraphs on validating origins. NIST IR 7622 provides additional language for procedural requirements, with more specificity and in some cases more directly relation to data lineage.[9] O-TPPS (section 4.2.1.10) offers language specific to open-source software and requires suppliers to provide assurance of reliable component lineage.[10] NATF requires suppliers to be able to ensure the integrity and authenticity of all software and patches.[11]

Require vendors to use strong authentication and cryptographic methods

Ensure that vendors are using strong, multi-factor authentication methods that make it much harder for impostors to make configuration changes to configuration management and other product delivery

[3] https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations

[4] Executive Order 13873: *Securing the Information and Communications Technology and Services Supply Chain*. Federal Register Vol. 84, No. 96. May 17, 2019.

[5] https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list

[6] https://www.fincen.gov/sites/default/files/2018-04/FinCEN_Guidance_CDD_FAQ_FINAL_508_2.pdf

[7] Edison Electric Institute (EEI) Model Procurement Contract Language (Version 2)

[8] U.S. Department of Energy (funded) Cybersecurity Procurement Language for Energy Delivery Systems

[9] Edison Electric Institute (EEI) Model Procurement Contract Language (Version 2)

[10] ISO/IEC Open Trusted Technology Provider Standard (O-TTPS) -- Mitigating maliciously tainted and counterfeit products: Part 1.

[11] North American Transmission Forum CIP-013-1 Implementation Guidance

systems. PCI’s Data Security Standard recommends authenticating users based on a multi-factor process consisting of something you know, such as a password, something you have, such as a token device, and something you are, such as a biometric.[12] The Energy Delivery Systems report specifies cryptographic systems. DOE and DHS recommend assigning multifactor credentials for higher-risk access.[13] ISO 27034 favors using a computer-driven security protocols for higher risk access, without human intervention.[14]

Require vendors to manage credentials stringently, including periodic deprovisioning

Examine vendors’ processes for managing their access credentials in order to make it harder for malicious actors to fraudulently gain access to credentials and access privileges. At C2M2’s Maturity Level Indicator (MIL) 2, IT administrators should regularly ensure that credentials are associated with the correct person or entity, and they should deprovision access within defined time thresholds when they are no longer required. At MIL3, the requirements for credentials are determined by a multi-factor risk assessment.[15]

Require vendors to deny communications with risky profiles and log denied access incidents

Maintain a secure boundary and log all traffic and its attributes; log denied access incidents to maximize forensic investigative potential. AICPA’s Trust Services include provisions to authenticate data subjects' identity, as well as to communicate denial of access requests, in order to allow better traceability, diagnostics, and forensics that ultimately would allow for better management of provenance issues.[16] CIS’s “CIS Controls” recommend denying communications with known malicious I.P. addresses.[17]

Use intelligence about active and potential threat sources to mitigate active threats

Integrate knowledge about current threats to mitigate active supply chain cybersecurity risks. SAFECode’s Framework for Supply Chain Integrity recommends referencing a threat library,[18] and NIST 800-53r4 recommends using “All-Source Intelligence.”[19] NIST maintains a National Vulnerability Database,[20] and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) lists cyber threat resources.[21]

Require vendors to establish a documented patch process with safeguards against malicious actors

Review the adequacy of security within vendors’ patch processes and consider requiring suppliers to be capable of ensuring the integrity and authenticity of software and patches, as recommended by NATF.[22] They should define the process flow as well as responsibilities, accountabilities, consulted parties, and informed parties (RACI), and the timeliness of security measures.

[12] PCI (Payment Card Industry) DSS Quick Reference Guide, Data Security Standard version 3.2.

[13] U.S. Department of Energy and U.S. Department of Homeland Security Cybersecurity Capability Maturity Model (C2m2). MIL3.

[14] International Standards Organization ISO 27034, “Information Technology – Security Techniques – Application Security

[15] U.S. Department of Energy and U.S. Department of Homeland Security Cybersecurity Capability Maturity Model (C2m2), p. 26.

[16] *TSP 100—2017 Trust Services Criteria*. American Institute of CPAs System & Organizational Control. Pp. 47-50.

[17] Center for Internet Security CIS Controls

[18] The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain. SafeCODE.

[19] NIST SP 800-53r4. “Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition.”

[20] https://nvd.nist.gov/vuln/search

[21] https://www.us-cert.gov/related-resources

[22] North American Transmission Forum CIP-013-1 Implementation Guidance

Verify patch authenticity via cryptography, hashes, certificates, or 2-factor authentication

Erect authentication barriers that ensure validity of patches and patch processes. EEI provides language for a contractor publishing a hash (see 2.1.5 (b) (i)) as a means to verify legitimacy and safety of a patch. NIST IR 7622 suggests to perform security assessments of configuration management processes and systems to detect ongoing attacks. (Section 4.3).