NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Supply Chain Security Guidelines on Provenance

Security Training Session

David Steven Jacoby, Provenance Committee Chair
Critical Infrastructure Protection Committee
Orlando, June 4, 2019 – updated June 20

RELIABILITY | RESILIENCE | SECURITY




Provenance: Definition

- Working definition of provenance:
  - Whether some thing is authentic (genuine or counterfeit)
  - Where it came from, how it's been changed, and who has touched it (largely synonymous with "chain of custody" and "lineage") [1]
- Allows targeting of defenses against identifiable counterfeiters, adversarial insiders and outsiders, and industrial cyber-criminals.
- Requires a combination of physical and logical tools and processes, such as identity management, access control, tagging and tracing.

1 Further definition available in National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) 7622: Notional Supply Chain Risk Management Practices for Federal Information Systems.

Best Practices

- 1. Establish a policy that governs and limits development in adversarial environments
  - Establish procedures regarding transfer of data to third countries and named adversaries (e.g., U.S. BIS List of Sanctioned Destinations, Executive Order 13873, etc.)
- 2. Monitor compliance against Denied Persons, Disapproved Vendors, and Related lists
  - Check vendors vs. Executive Order 13873 and vs. US DOC Consolidated Screening List, which includes Denied and Unverified Persons and Entities

Note: The short paper contains more specific citations to the external sources referenced in parentheses.

Best Practices

- 3. Use standard contract language about provenance
  - Adopt or adapt model contract language for CIP-013 R1.2.5 regarding integrity and authenticity (EEI)
  - Adopt or adapt vendor requirements regarding account management, session management, logging and auditing, and secure development (DOE Cybersecurity Procurement Language for Energy Delivery Systems)
- 4. Require internal and external vendors to validate the authenticity and origins of third party hardware and software
  - EEI: contract language (R1.2.5a on page 8) to validate origins
  - NIST IR 7622 (4.1): language regarding acquirer, integrator and supplier provenance methods
  - ISO/IEC O-TPPS (section 4.2.1.10): language about open-source and lineage
  - NATF: vendor to verify integrity and authenticity of software and patches

Note: The short paper contains more specific citations to the external sources referenced in parentheses

Best Practices

- 5. Require vendors to use strong authentication and cryptographic methods
  - PCI: something you know, something you have, and something you are
  - DOE: cryptographic systems
  - DOE and DHS: multifactor credentials for higher-risk access
  - ISO 27034 computer-only protocols for higher risk access
- 6. Require vendors to manage credentials stringently, including periodic deprovisioning
  - Regularly ensure credentials are associated with the correct entity (C2M2)
  - Deprovision access within defined time thresholds after needed (C2M2)
  - Allow access to credentials based on multi-criteria risk assessment (C2M2)

Note: The short paper contains more specific citations to the external sources referenced in parentheses.

Best Practices

- 7. Require vendors to deny communications with risky profiles and log denied access incidents
  - Communicate denial of access requests (AICPA's Trust Services)
  - Deny communications with known malicious I.P. addresses and communication over unauthorized ports (CIS Controls)
- 8. Use intelligence about active and potential threat sources to mitigate active threats
  - NIST National Vulnerability Database
  - U.S. Cybersecurity and Infrastructure Security Agency (CISA) resources

Note: The short paper contains more specific citations to the external sources referenced in parentheses

Best Practices

- 9. Require vendors to establish a documented patch process with safeguards against malicious actors
  - Consider requiring suppliers to be capable of ensuring integrity and authenticity of all software and patches (NATF CIP-013 Guidance)
- 10. Verify patch authenticity via cryptography, hashes, certificates, or 2-factor authentication
  - Adopt contract language for publishing a hash (EEI 2.1.5 (b) (i))
  - Perform security assessments of configuration management processes and systems to detect ongoing attacks (NIST IR 7622 4.3)

Note: The short paper contains more specific citations to the external sources referenced in parentheses

Questions and Answers