Software Provenance

08/28/2019
Roy Wilson, CISSP, CEH, Sec+
roy.wilson@dau.edu
Agenda

• Software provenance defined
• Software provenance logic diagram
• Elements of software provenance
• Importance of software provenance to software assurance (SwA) and cybersecurity
Introductions

PRESENTER
Roy Wilson, CISSP, CEH, Sec+
Professor of Acquisition Cybersecurity
Defense Acquisition University
Foundational Learning Directorate

MODERATOR
Chris Barrett
Professor of Systems Engineering
DAU Mid-Atlantic
WHAT IS SOFTWARE PROVENANCE?

• The word provenance (alternatively spelled provenience) comes from the Latin provenire, meaning “to come forth, originate.

• Thus, software provenance refers to
  • Verifiable information regarding the origin of a software configuration item
  • Development facility or location where it was developed
  • Who wrote the code
  • Application of secure coding standards
  • Security assessment
    • What static and dynamic code analysis methods were used
  • Chain of custody
    • Who possessed the software configuration item since its development
WHAT IS SOFTWARE PROVENANCE?

According to NIST SP 800-161:

Software provenance is the recording of system and component origin along with the history of, the changes to, and the recording of who made the changes.

- Acquirers and their system integrators should maintain the provenance of systems and components under their control to understand where the systems and components originated, their change history while under government control, and who might have had an opportunity to change them.

- Provenance allows for changes from the baselines of systems and components to be reported to specific stakeholders.

- Creating and maintaining provenance within the Information and Communications Technology (ICT) supply chain helps government agencies to achieve greater traceability in case of an adverse event and is critical for understanding and mitigating risks.

NIST SP 800-53, Rev 4, lays out security and privacy controls for Federal and DoD Information Systems. Originally there were 18 ICT SCRM control families or categories. Supplemental guidance established Provenance as the 19th control family.
WHAT IS SOFTWARE PROVENANCE?

The “Readers Digest” Version

Origin and Chain of Custody
ELEMENTS OF SOFTWARE PROVENANCE

• Development Facility
  • COTS
    • Inherently “unprovenanced”
      • Overseas
      • 3rd party vendors
  • Test, test, test
  • DoD funded
    • DFARS 252-204-7012 (CDI on unclassified networks)
    • DSS authorization (classified networks)

• Personnel
  • Insider threat
  • Cleared
  • Trained

• Secure Code Standards
  • CMU SEI
ELEMENTS OF SOFTWARE PROVENANCE

- Code Security Analysis
  - CAPEC, CWE, CVE
  - Peer Reviews
  - Static, Dynamic Tools
    - Using more than one tool
    - Subsystem and system penetration testing
ELEMENTS OF SOFTWARE PROVENANCE

- Chain of Custody
  - SCRM
    - DFARS 252.239-7017 (Notice of Supply Chain Risk)
    - DFARS 252.239-7018 (Supply Chain Risk)
  - Code Signing
  - Encryption
  - Out-of-Band Hash
  - Keyless Signature Infrastructure (KSI) aka Blockchain
  - Origin to End Platform Supply Chain Control
  - Transmission security (TRANSEC)
  - Positive Handoff
  - Operations Security (OPSEC)
  - Obfuscation
SOFTWARE PROVENANCE

- Systems Engineering
  - Systems Security Engineering
  - Cybersecurity
    - Software Assurance
      - Software Provenance
        - Origin
        - Chain of Custody
Additional Related Resources

- Joint Federated Assurance Center (JFAC), https://jfac.navy.mil/
- CMU SEI, https://www.sei.cmu.edu/
- DAU CLE 081, Software Assurance Awareness
Questions?