Software Supply Chain Risks That May Need to be Addressed

MITRE’s System of Trust™

Robert Martin
Senior Software and Supply Chain Assurance Principal Engineer
Cyber Solutions Innovation Center
MITRE Labs

Presenting at the ITU Workshop on “Zero Trust and Software Supply Chain Security”
Session 2: Need, security issues, threats and controls for software supply chain security.
Software Supply Chain Attack (a.k.a SolarWinds)

1. Preparatory compromises at SolarWinds date back to October 2019. (Refs 11 & 12)
2. At some point there was a compromise of the build environment itself.
3. Malicious code sent in SolarWinds updates released between March and at least June 2020. (Refs 32 & 33)
4. Approximately 18,000 organizations receive the tainted updates and may have been targeted and impacted.
Software Supply Chain Integrity

Evidence Based Trust

Secure & Hardened Build and Distribution Infrastructure

Code -> Commit -> Build -> Test -> Package -> Release

Deploy -> Operate -> Monitor

Producer

Consumer


© 2023 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 23-01614-17
Software Supply Chain Integrity, Transparency & Trust

Software Supply Chain Risks (Hazards and Threats)*

Threat List Sources:
- Supply-chain Levels for Software Artifacts (SLSA), https://slsa.dev/spec/v1.0/threats-overview
- Taxonomy of Attacks on Open-Source Software Supply Chains (SoK), 2023 IEEE Symposium on Security and Privacy - DOI: 10.1109/SP46215.2023.10179304
- Uncovering Software Supply Chains Vulnerability: A Review of Attack Vectors, Stakeholders, and Regulatory Frameworks, DOI: 10.1109/COMPSAC57700.2023.00281

* See MITRE’s System of Trust repository of potential supply chain risks (SoT.MITRE.ORG)
System of Trust (SoT)
“What Supply Chain Risks to Manage?”

SoT - a strategic, widely-adoptable, holistic, data-driven analysis platform to assess supply chain security risks

Address Chaos, Align & Organize
Simplify, Tailor & Use
Basis of Trust

**Trust Aspects**

**Risk Categories**

- (RC-13) Supplier Financial Stability Risks
- (RC-76) Supplier Organizational Security Risks
- (RC-4) Supplier Susceptibility
- (RC-20) Supplier Quality Culture Risks
- (RC-105) Supplier Organizational Effectiveness Risks
- (RC-7) Supplier Ethical Risks
- (RC-6) Supplier External Influences

**RC-201** Supply (product) Quality Risks

**RC-213** Supply (product) Security Risks

**RC-214** Supply (product) Resilience Risks

**Risk Categories**

- (RC-21) Supply Malicious Taint
- (RC-9) Supply Counterfeit
- (RC-8) Supply Hygiene Risks

**Risk Categories**

- (RC-518) Software supply (product) security process risks
- (RC-519) Software supply (product) security requirements risks
- (RC-520) Software supply (product) architecture and design security risks
- (RC-521) Software supply (product) coding language risks
- (RC-522) Software supply (product) code analysis risks
- (RC-523) Software supply (product) security testing risks
- (RC-524) Software supply (product) secure build risks
- (RC-525) Software supply (product) secure integration and deployment risks
- (RC-526) Software supply (product) secure update risks
- (RC-527) Software supply (product) pedigree and provenance risks
- (RC-528) Third party supply (product) component risks

**Risk Categories**

- (RC-287) Service Quality Risks
- (RC-289) Service Resilience Risks
- (RC-286) Service Security Risks
- (RC-288) Service Integrity Risks

**Risk Categories**

- (RF-113) Software supply (product) includes components that were known to have exploitable vulnerabilities at the time it was in development
- (RC-529) Open source software risks for software supply (product)
- (RF-743) Insufficient security vetting of third party software supply (product) components
# MITRE Supply Chain Security System of Trust Risk Areas

<table>
<thead>
<tr>
<th>(RC-1) Supplier Risks</th>
<th>(RC-2) Supply Risks</th>
<th>(RC-3) Service Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(RC-20) Supplier Quality Culture Risks</strong></td>
<td><strong>(RC-6) Supply Management Integrity Risks</strong></td>
<td><strong>(RC-301) Service Specific Security Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-105) Supplier Organizational Effectiveness Risks</strong></td>
<td><strong>(RC-10) Supply Chain Marine Integrity Risks</strong></td>
<td><strong>(RC-302) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-4) Supplier Ethical Risks</strong></td>
<td><strong>(RC-12) Supply (Product) Quality Risks</strong></td>
<td><strong>(RC-303) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-10) Supplier External Influences</strong></td>
<td><strong>(RC-15) Supply Chain Manufacuring Integrity Risks</strong></td>
<td><strong>(RC-304) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-21) Susceptibility to Supply Chain Higeine Risks</strong></td>
<td><strong>(RC-22) Unsanctioned Manufacturing</strong></td>
<td><strong>(RC-305) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-150) Functional Integrity Risks</strong></td>
<td><strong>(RC-202) Supply (Product) Quality Risks</strong></td>
<td><strong>(RC-311) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-120) Corporate Manufacturing</strong></td>
<td><strong>(RC-203) Supply (Product) Quality Risks</strong></td>
<td><strong>(RC-312) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-204) Logistics/Transportation Integrity Risks</strong></td>
<td><strong>(RC-204) Supply (Product) Quality Risks</strong></td>
<td><strong>(RC-313) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-205) Poor Reputation for Integrity</strong></td>
<td><strong>(RC-205) Supply (Product) Quality Risks</strong></td>
<td><strong>(RC-314) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-206) Facilities Integrity Risks</strong></td>
<td><strong>(RC-206) Supply (Product) Quality Risks</strong></td>
<td><strong>(RC-315) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-54) Packaging Integrity Risks</strong></td>
<td><strong>(RC-207) Supply (Product) Quality Risks</strong></td>
<td><strong>(RC-316) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-208) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-317) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-318) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-318) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-320) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-319) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-322) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-320) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-324) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-321) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-326) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-322) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-328) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-323) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-330) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-324) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-332) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-325) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-334) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-326) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-336) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-327) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-338) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-328) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-340) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-329) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-342) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-330) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-344) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-331) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-346) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-332) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-348) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-333) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-350) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-334) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-352) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-335) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-354) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-336) Service Specific Reliability Risks</strong></td>
</tr>
<tr>
<td><strong>(RC-356) Supply Infrastructure Pedigree Risks</strong></td>
<td></td>
<td><strong>(RC-337) Service Specific Reliability Risks</strong></td>
</tr>
</tbody>
</table>

* Supply Chain Security Top 75 Risk Areas Levels 1-3
** System of Trust Expanding to Pharma, Food, and other types of Products

---

MITRE's Supply Chain Security System of Trust™ [https://sot.mitre.org/](https://sot.mitre.org/)

© 2023 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 23-01614-17
14 top-level risk categories
214 detailed risk categories
642 specific measurable risks
**SBOM Definition**

**NTIA Minimal Elements (EO 14028)**

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier Name</td>
<td>The name of an entity that creates, defines, and identifies components.</td>
</tr>
<tr>
<td>Component Name</td>
<td>Designation assigned to a unit of software defined by the original supplier.</td>
</tr>
<tr>
<td>Version of the Component</td>
<td>Identifier used by the supplier to specify a change in software from a previously identified version.</td>
</tr>
<tr>
<td>Other Unique Identifiers</td>
<td>Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.</td>
</tr>
<tr>
<td>Dependency Relationship</td>
<td>Characterizing the relationship that an upstream component X is included in software Y.</td>
</tr>
<tr>
<td>Author of SBOM Data</td>
<td>The name of the entity that creates the SBOM data for this component.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Record of the date and time of the SBOM data assembly.</td>
</tr>
</tbody>
</table>


**Minimum Elements**

<table>
<thead>
<tr>
<th>Data Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.</td>
</tr>
</tbody>
</table>

**Automation Support**

Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.

**Practices and Processes**

Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.


---

**SPDX** (Linux Foundation - Free ISO/IEC 5952:2022)

**CycloneDX** (OWASP Project)

**SWID**
From the Community-led Working Group on SBOM Tooling and Implementation, facilitated by Cybersecurity and Infrastructure Security Agency [cisa.gov/sbom]

<table>
<thead>
<tr>
<th>SBOM Type</th>
<th>Definition</th>
<th>Data Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td>SBOM of intended design of included components (some of which may not exist) for a new software artifact.</td>
<td>Typically derived from a design specification, RFP, or initial concept.</td>
</tr>
<tr>
<td>Source</td>
<td>SBOM created directly from the development environment, source files, and included dependencies used to build an product artifact.</td>
<td>Typically generated from software composition analysis (SCA) tooling, with manual clarifications.</td>
</tr>
<tr>
<td>Build</td>
<td>SBOM generated as part of the process of building the software to create a releasable artifact (e.g., executable or package) from data such as source files, dependencies, built components, build process ephemeral data, and other SBOMs.</td>
<td>Typically generated as part of a build process. May consist of integrated intermediate Build and Source SBOMs for a final release artifact SBOM.</td>
</tr>
<tr>
<td>Analyzed</td>
<td>SBOM generated through analysis of artifacts (e.g., executables, packages, containers, and virtual machine images) after its build. Such analysis generally requires a variety of heuristics. In some contexts, this may also be referred to as a “3rd party” SBOM.</td>
<td>Typically generated through analysis of artifacts by 3rd party tooling.</td>
</tr>
<tr>
<td>Deployed</td>
<td>SBOM provides an inventory of software that is present on a system. This may be an assembly of other SBOMs that combines analysis of configuration options, and examination of execution behavior in a (potentially simulated) deployment environment.</td>
<td>Typically generated by recording the SBOMs and configuration information of artifacts that have been installed on systems.</td>
</tr>
<tr>
<td>Runtime</td>
<td>SBOM generated through instrumenting the system running the software, to capture only what is loaded and executing in memory, as well as external call-outs or dynamically loaded components. In some contexts, this may also be referred to as an “Instrumented” or “Dynamic” SBOM.</td>
<td>Typically generated from tooling interacting with a system to record the artifacts present in a running environment and/or that have been executed.</td>
</tr>
</tbody>
</table>
Software Bill of Materials Types

Source SBOM

- Open source components
- Developed components
- Purchased components

Build SBOM

- Build process
- Libraries
- Build Tools
- Makefiles
- Generated code
- Other documents: Multimedia, text

Target Images

- Micro Controller Firmware
- Disk Images
- Virtual Machine Images
- Container Images
- Package Feeds
- SDKs & Build Tools

Execution

- Dynamic libraries
- External executables

Data to address some SLSA Threats

Deployed SBOM

MITRE

© 2023 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 23-01614-17

13
Software Supply Chain Integrity, Transparency & Trust

Example of the IETF SCITT in SW Development

<table>
<thead>
<tr>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source SBOM</td>
</tr>
<tr>
<td>Build SBOM</td>
</tr>
<tr>
<td>Deployed SBOM</td>
</tr>
<tr>
<td>SLSA Data</td>
</tr>
</tbody>
</table>

Policy Gates

Signed Evidence

Example evidence: Commit signature proof
Example evidence: Build trigger record
Example evidence: Build parameters
Example evidence: Source SBOM signed by expected provider
Example evidence: Build SBOM
Example evidence: Deployed SBOM
Example evidence: SAST/CIAS/scan results
Example evidence: Fuzz test results
Example evidence: Release approval
Example evidence: Release completion

Example policy: Source SBOM matches published package
Example policy: Build SBOM matches deployed SBOM
Example policy: Build configuration acceptable
Example policy: No known unmitigated vulnerabilities
Example policy: Release approved
Example policy: Build output SBOM matches deployed SBOM

Vendor’s SCITT Registry

Policy Entries

Evidence Entries

SW Parts & Tooling Ecosystem
Software Product Ecosystem
Edge Ecosystem

Traceable Value Chain

Code Repositories
Development Tool
Creation & Sourcing
Auto Supply Chain Integrity, Transparency & Trust

Automotive Supply Chain Risks (Hazards and Threats)*

* See MITRE’s System of Trust repository of potential supply chain risks (SoT.MITRE.ORG)
Auto Supply Chain Integrity, Transparency & Trust

Manufacturing Ecosystem

Automotive Ecosystem

IoT Ecosystem

Example policy:
- Parts are untainted during shipment
- Parts made to specification
- Parts from legitimate producer

Example policy:
- Sub-assemblies are undamaged during shipment
- Sub-assemblies made to specification
- Sub-assemblies from legitimate producer
- Sub-assemblies conform to HBOM
- HBOM signed and unaltered

Example policy:
- Approved by quality inspector
- Build output BOM matches design specification
- Tooling within configuration norms
- No known unmitigated flaws
- Meets functional testing

Policy Gates

Signed Evidence

Example of the IETF SCITT in the Automotive Industry

© 2023 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 23-01614-17

MITRE

Vendor's SCITT Registry

Evidence Entries
Smart Supply Chain Integrity, Transparency & Trust

Supply Chain Risks (Hazards and Threats)*

* See MITRE’s System of Trust repository of potential supply chain risks (SoT.MITRE.ORG)
Takeaways and Conclusions

- Software exists as a standalone item and as an embedded capability
- Addressing the software supply chain must align and integrate with the other aspects of smart device supply chains.
- Trust, visibility, and integrity needs to be conveyable across all supply chains.
- Assurance is specific to an item and its use in an environmental / business context.
- Automation is critical to gaining and conveying assurance.
- Broadly utilized standards for assurance attestations, BOMs, integrity, vulnerabilities, weaknesses, and risks are needed

Suggestions for SG17

- Consider making automation guidelines for showing how evolving freely available standardization efforts* across the globe can be used to capture and convey assurance attestations using BOMs and other build claims / statements across supply chains for smart devices and standalone software against appropriately tailored sets of risks for the different environmental / business contexts.

* ISO/IEC 5962 & 5055 (free versions), IETF SCITT, MITRE System of Trust, ITU-T CYBEX (X.1500, X.1520, X.1521, X.1524, X.1525, X.1528), ETSI TR 103 305 (1-4), ETSI TR 103 306, etc.
System of Trust and IETF SCITT

- **MITRE’s System of Trust - SoT.MITRE.ORG**
  - Contact - SOT@mitre.org

- **SCITT IETF Working Group** - focused on specification development. Charter and Meeting schedule outlined by the IETF: [https://datatracker.ietf.org/wg/scitt/about/](https://datatracker.ietf.org/wg/scitt/about/)
  - IETF 118 (Prague) SCITT Session is planned for Thursday 9 Nov. from 9:30-11:30am

- **SCITT Community** - focused on IETF specification adoption [https://github.com/ietf-wg-scitt/](https://github.com/ietf-wg-scitt/) including advocacy, outreach, testing, ensuring interoperability of implementations, rapid prototyping, and open source libraries, tooling and examples, like the SCITT API Emulator [https://github.com/microsoft/scitt-api-emulator](https://github.com/microsoft/scitt-api-emulator), and View COSE tool [https://v.glucose.org/](https://v.glucose.org/).
  - The **SCITT Community** is open to the public and new members are invited to join!