Trustworthy Digital Supply Chain Transparency Services

Henk Birkholz ⟨henk.birkholz@sit.fraunhofer.de⟩ on behalf of SCITT contributors (W. Bartholomew, H. Birkholz, S. Clebsch, A. Deligat-Lavaud, Y. Deshpande, C. Fournet, B. Knight, S. Lasker, R. Martin, S. Provine, M. Riechert, A. Stewart, K. Williams, R. Williams, ... see scitt@ietf.org)

SECDISPATCH @ IETF 113, Tue March 22nd, 2022
Supply Chains

Generic Supply Chain

Materials
Design
Production
Distribution
Customer

Software Supply Chain

SCM
Dependencies
Source

CI/CD
Compilers, Tools
Build

Distribution
Sig, Metadata
Package

Applications

Developers
Release Manager
Package Manager
Software Supply Chains Attacks

How can I audit the provenance of all software in my TCB?
Software Supply Chains Attacks

Devs unknowingly use “malicious” modules snuck into official Python repository

The year-long rash of supply chain attacks against open source is getting worse

Backdoors snuck into 12 OSS packages were downloaded hundreds of thousands of times.

Rage-quit: Coder unpublished 17 lines of JavaScript and “broke the Internet”

Disguise over module name in npm registry became giant headache for developers.

Two new supply-chain attacks come to light in less than a week

As drive-by attacks get harder, hackers exploit the trust we have in software providers.

Widely used open source software contained bitcoin-stealing backdoor

Malicious code that crept into event-stream JavaScript library went undetected for weeks.

Source: NIST CSRC
Auditing Supply Chains

- EO14028
- In-toto
- SWID
- SLSA
- SPDX
- CycloneDX

Software BOM

```
{  "_type": "https://in-toto.io/Statement/v0.1",  "predicateType": "cosign.sigstore.dev/attestation/v1",  "subject": [    {      "name": "gcr.io/zebra-testing/distroless",      "digest": {        "sha256": "3ab2f3293a38d1e17f49f1b386dee56f9e253c587bce81",        "type": "SHA-256"      },      "predicate": {        "data": "foo",        "timestamp": "2021-10-107-10:27:27"      }    }  ]}
```

**SLSA compliance levels**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>SLSA 1</th>
<th>SLSA 2</th>
<th>SLSA 3</th>
<th>SLSA 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Verifiable History</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Retained Indefinitely</td>
<td>18 mo.</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Two-Person Reviewed</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
</tbody>
</table>

**Build**

- Isolated: ☑
- Parameterless: ☑
- Hamitic: ☑
- Reproducible: ☑
- Available: ☑
- Authenticated: ☑

**Provenance**

- Service Generated: ☑
- Non-Callable: ☑
- Dependencies Complete: ☑
- Security: ☑
- Access: ☑
- Supervisors: ☑

O - required unless there is a justification.

**Bill of Materials**

<table>
<thead>
<tr>
<th>Part #</th>
<th>Description</th>
<th>Qty</th>
<th>Unit</th>
<th>Unit Cost</th>
<th>Total Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>705</td>
<td>Window frame</td>
<td>4</td>
<td>1</td>
<td>$3.00</td>
<td>$12.00</td>
</tr>
<tr>
<td>35</td>
<td>Brackets</td>
<td>4</td>
<td>1</td>
<td>$0.75</td>
<td>$3.00</td>
</tr>
<tr>
<td>1</td>
<td>PR0045</td>
<td>2</td>
<td>1</td>
<td>$0.50</td>
<td>$1.00</td>
</tr>
<tr>
<td>2</td>
<td>Glass panel</td>
<td>1</td>
<td>1</td>
<td>$5.50</td>
<td>$5.50</td>
</tr>
<tr>
<td>LB1079</td>
<td>Window label</td>
<td>1</td>
<td>1</td>
<td>$0.50</td>
<td>$0.50</td>
</tr>
<tr>
<td>G41958</td>
<td>Hinges</td>
<td>2</td>
<td>1</td>
<td>$2.25</td>
<td>$4.50</td>
</tr>
<tr>
<td>G8964</td>
<td>Screws</td>
<td>1</td>
<td>10</td>
<td>$0.45</td>
<td>$4.50</td>
</tr>
<tr>
<td>S88</td>
<td>Screw hook</td>
<td>1</td>
<td>1</td>
<td>$0.88</td>
<td>$0.88</td>
</tr>
<tr>
<td>G36120</td>
<td>Screws for</td>
<td>1</td>
<td>1</td>
<td>$4.97</td>
<td>$4.97</td>
</tr>
<tr>
<td>812</td>
<td>Plastic wrap</td>
<td>1</td>
<td>1</td>
<td>$0.65</td>
<td>$0.65</td>
</tr>
<tr>
<td>XYZ1231</td>
<td>Carbon fiber</td>
<td>1</td>
<td>1</td>
<td>$0.10</td>
<td>$0.10</td>
</tr>
<tr>
<td>17847</td>
<td>Box label</td>
<td>1</td>
<td>1</td>
<td>$0.10</td>
<td>$0.10</td>
</tr>
</tbody>
</table>

Total number parts: 27.50
Total cost: $54.95

**In-toto statement**

```
PACKING SLIP

[Company Name]  
[Company Address]

BILL TO:
[COMPANY NAME]
[Address]
[City, ST, ZIP]
[Phone]
[Email]

SHIP TO:
[COMPANY NAME]
[Address]
[City, ST, ZIP]
[Phone]

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
<th>QTY</th>
<th>ORDER QTY</th>
<th>UNIT ORDER</th>
<th>UNIT Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>10240232</td>
<td>Product A</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>10240233</td>
<td>Product B</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Compliance Certificate

Shipment records
Transparency: Core Intuitions & Prior Work

We cannot stop supply chain actors from making false claims, but we can make them accountable by requiring their claims to be registered in verifiable Transparency Ledgers.

This ensures that malicious actors who make contradictory claims to different entities (customers, auditors, regulators) can be detected and held accountable.

All consumers of claims must first verify the proof of ledger registration to ensure a claim is auditable; this verification is cheap and can be done offline.

Examples of Transparency Systems

Certificate Transparency [RRC 6962] Adam Langley, Emilia Kasper, Ben Laurie (Google)
Keeping authorities “honest or bust” based on large-scale decentralized witness cosigning (IEEE S&P ’16)
CHAINiAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds (Usenix’17, EPFL)
Contour: A practical system for binary transparency, logging on bitcoin the latest authorized binary version.
M. Al-Bassam, S. Meiklejohn (Data Privacy Management, Cryptocurrencies and Blockchain Technology, 2018)

7
Transparency: Terminology

A Ledger is a consistent, append-only and distributed data store
A Receipt is a compact, offline verifiable cryptographic proof that a claim is stored in a ledger (example: Signed Cert Timestamp TLS extension in RFC 6962)

Claims are statements signed by Issuers, using keys they distribute through DID. Transparent Claims are countersigned with receipts of ledger registration.

- Incorrect or inconsistent claims can be discovered by auditing the ledger

An artifact is Transparent if it comes with valid Transparent Claims.

- Relying parties verify claims before use and/or audit claims later
- Receipts prove the existence of claims in the ledger to offline 3rd parties
- Transparency is known to scale well in practice (e.g., CT: ~6B certs in ledger)
Architecture Overview:

Supply
Chain
Integrity,
Transparency, and
Trust

SCITT
Issuing Claims (COSE)

<table>
<thead>
<tr>
<th>Issuer Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature algorithm, key ID</td>
</tr>
<tr>
<td>Artifact Name</td>
</tr>
<tr>
<td>payload type &amp; contents</td>
</tr>
<tr>
<td>Additional metadata used to apply registration policy</td>
</tr>
<tr>
<td>integrity for whole envelope+ payload</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Header</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>issuer</td>
<td>did:web:firmware.sec.fpga.com</td>
</tr>
<tr>
<td>alg, kid</td>
<td>ES384,</td>
</tr>
<tr>
<td>feed</td>
<td>Cxxx FPGA Firmware</td>
</tr>
<tr>
<td>cty</td>
<td>application/x-ms-boot-manifest-v1</td>
</tr>
<tr>
<td>registration_info</td>
<td>timestamp, version number, ...</td>
</tr>
</tbody>
</table>

Payload

Signature 3045022100e7d0...

COSE as Universal Signing Envelope Format

- Standardized (RFC 7049, 8152)
- Efficient (for resource constrained devices)
- Direct payload encoding
- Extensible & crypto agile
- Not tied to X.509

COSE_Sign1 = [
  protected : bstr .cbor { * label => values },
  unprotected : { * label => values },
  payload : bstr / nil,
  signature : bstr
]

label = int / tstr
values = any
Countersigning Envelopes with Transparency Receipts

Receipts are implemented by signing the root of the binary Merkle Tree (root hash) over the whole ledger contents.

They can be issued efficiently:
• One hash per transaction
• One signature per transaction batch

The signing key is supported by attestation results and governance transactions, also recorded in the ledger.

```
ReceiptContents = [
    signature: bstr
    node_certificate: tstr
    proof: [+ ProofElement]
    leaf_info: LeafInfo
]
```

; Signature over tree root
; Certificate of TS node that signed receipt
; Intermediate hashes (Merkle path)
; Extra data beyond claim stored in leaf
Federating Transparency Services

Multiple, independent transparency services can be governed and operated by different organizations

- Each transparency service enforces its own registration policy
- Relying parties may trust issuers and transparency services to different extents
- All Issuers, Transparency Services, Verifiers, and Auditors interoperate on claim envelopes and their interpretation using shared tools and formats
Prototype of SCITT Transparency Service & Verifier

Prototype based on Confidential Consortium Framework (CCF) framework: https://ccf.dev & https://github.com/Microsoft/ccf

The ledger implementation is a chronological Merkle Tree, distributed in a CFT network of SGX protected enclaves.

The ledger implements draft-00 COSE claims and receipts, including a client library for checking receipts, as a basis for discussion.
Related Work and Working Groups in the IETF

- Envelopes & Receipts are based on COSE WG output
- Transparency service operations trustworthiness involves RATS WG output
- Transparency services borrow concepts and terms from the concept of Certificate Transparency defined in RC 6962
(Bar) BoF onsite

- 1700 CEST (30 min after the SECDISPATCH WG meeting)
- Meeting Point: Yard and Park Ensemble (Park Pavilion)
- Hybrid "Bar" BoF today come with online meeting links:
  - [https://teams.microsoft.com/l/meetup-join/19%3ameeting_OWUwMDhiZjEtYjkwNS00NDA0LTlImMTgtNGZhOGE0NmU3ZTcz%40thread.v2/0?context=%7b%22Tid%22%3a%22272f988bf-86f1-41af-91ab-2d7cd011db47%22%22Oid%22%3a%22bced92fe-7c20-456e-9af-5b18c383de81%22%7d](https://teams.microsoft.com/l/meetup-join/19%3ameeting_OWUwMDhiZjEtYjkwNS00NDA0LTlImMTgtNGZhOGE0NmU3ZTcz%40thread.v2/0?context=%7b%22Tid%22%3a%22272f988bf-86f1-41af-91ab-2d7cd011db47%22%22Oid%22%3a%22bced92fe-7c20-456e-9af-5b18c383de81%22%7d)
- If you are spontaneous and/or have the time, join in. It's soon and (physically) in the same building