Intel Labs

Understanding the Software Supply Chain Trust Landscape

Marcela Melara

Intel Labs, Security & Privacy Research (SPR)

whoami

- Research Scientist at Intel Labs (over 5 years)
- OpenSSF Technical Advisory Council member
- Key open source involvement:
  - Core maintainer of in-toto Attestation Framework
  - Contributor to Supply-chain Levels for Software Artifacts (SLSA)
- General interests: distributed systems, OS, security

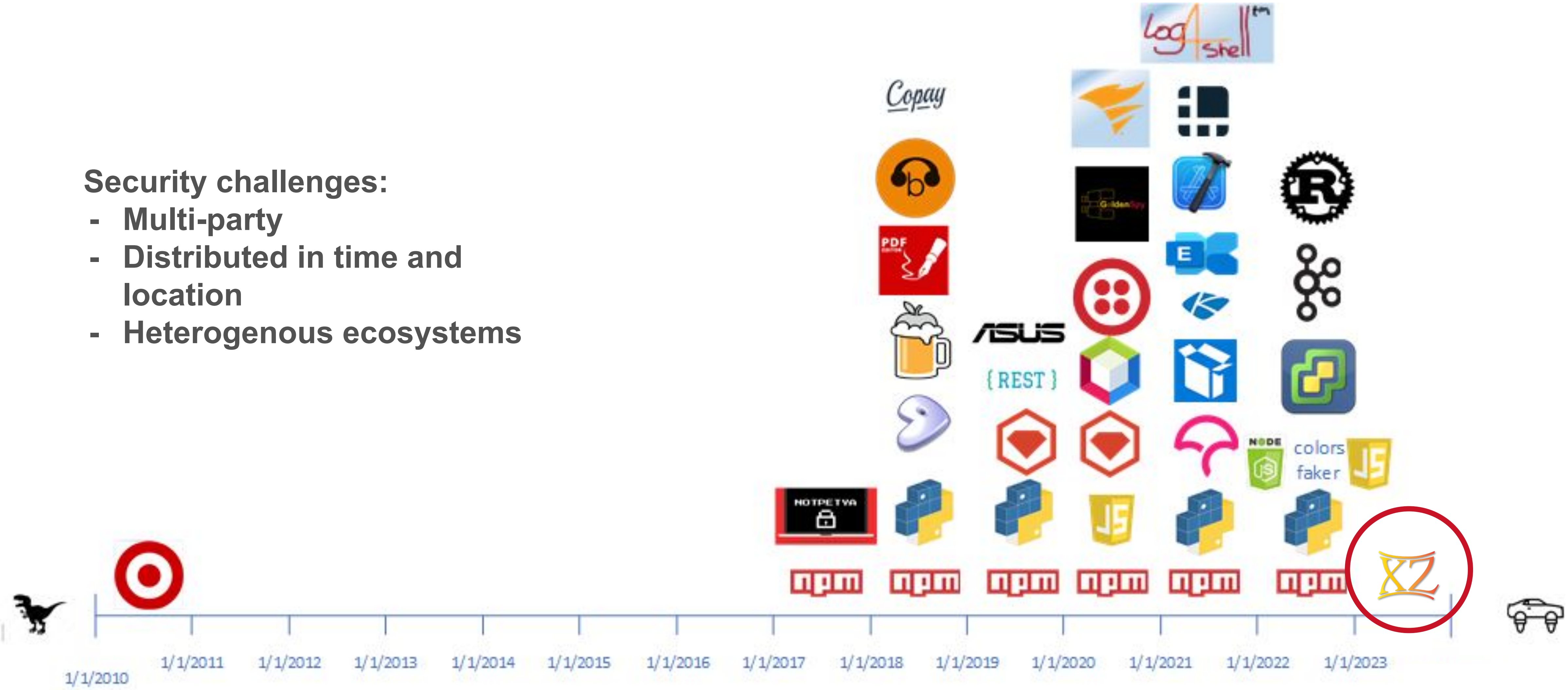
Agenda

- Software Supply Chain
  - Why SW supply chain security matters
  - The SWSC landscape
  - Tech highlights: SBOM, SLSA, in-toto, HW-Attested Builds, SPIFFE, Sigstore
- What's next
  - Attribute-based trust
  - ML Model Supply Chain

The xz-utils backdoor was not an isolated incident.

Security challenges:

- **Multi-party**
- **Distributed in time and location**
- **Heterogenous ecosystems**



Courtesy of CRob in “The Chain”, 2023.

Organizations Working on SW Supply Chain

CLOUD NATIVE
COMPUTING FOUNDATION

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

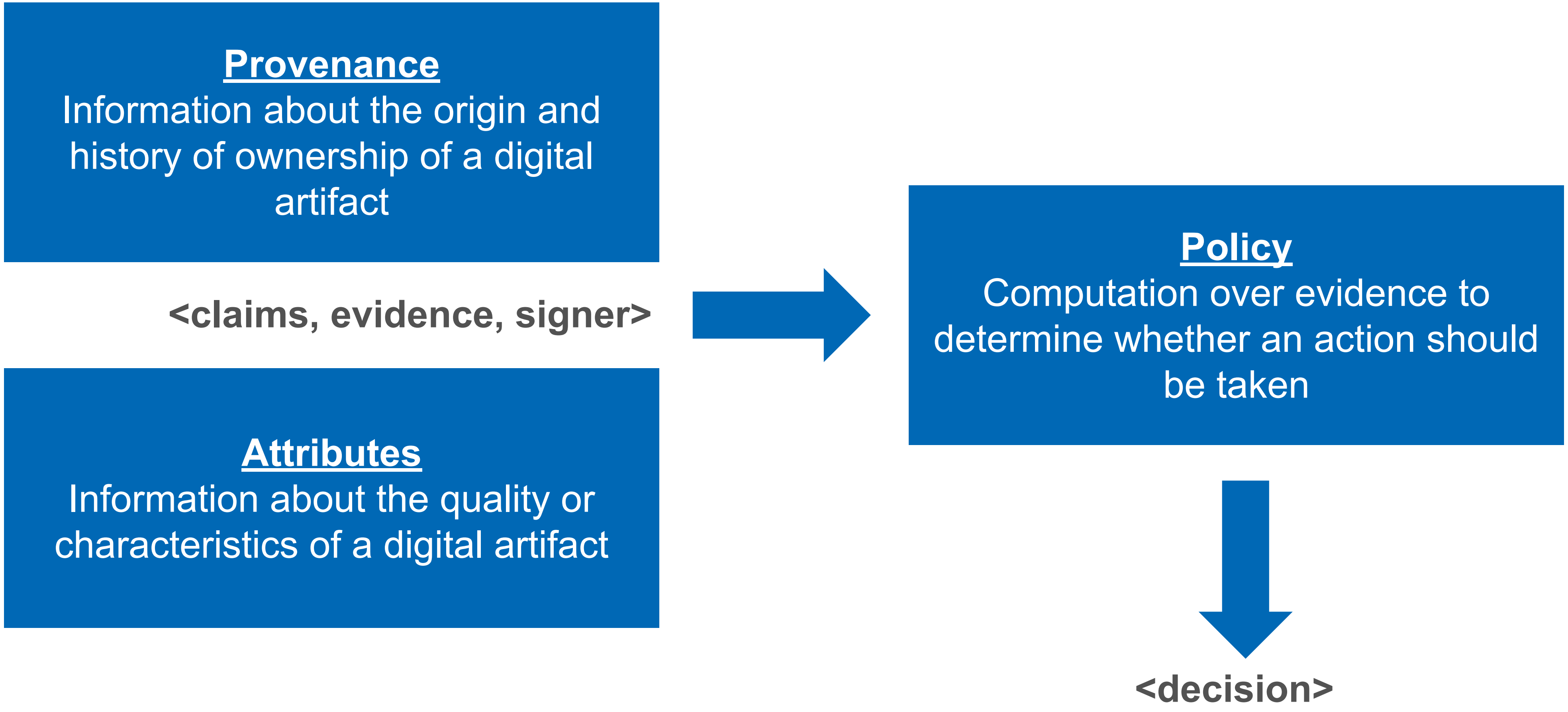
SPDX®

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

IETF®

OWASP®

Some Common Terms & Definitions



Provenance
Information about the origin and history of ownership of a digital artifact

Attributes
Information about the quality or characteristics of a digital artifact

<claims, evidence, signer>

Policy
Computation over evidence to determine whether an action should be taken

<decision>

Common misconception #1

One solution to rule them all.

SWSC Technology Areas

Policy & Insight Decide over aggregate information	CNCF in-toto Policies, NIST SSDF, OpenSSF SLSA-verifier
Aggregation & Synthesis Derive meaning from metadata	OpenSSF Scorecard, OpenSSF GUAC, CNCF Archivista, OpenSSF bomctl
Software Attestations Represent & collect security claims and evidence	CNCF in-toto, OpenSSF SLSA, SPDX/CycloneDX SBOM, NIST OSCAL
Resilient Infrastructure Provide high-integrity systems and automation	GitHub Actions, GitLab CI, Jenkins, Tekton Chains, OpenSSF gittuf
Trust Foundation Provide robust authentication and integrity primitives	OpenSSF Sigstore, IETF SCITT, CNCF SPIFFE/SPIRE, CNCF TUF

Adapted from https://security.googleblog.com/2022/10/announcing-guac-great-pairing-with-slsa.html

SWSC Technology Areas – Highlights

Policy & Insight
Decide over aggregate information

Aggregation & Synthesis
Derive meaning from metadata

Software Attestations
Represent & collect security claims and evidence

Resilient Infrastructure
Provide high-integrity systems and automation

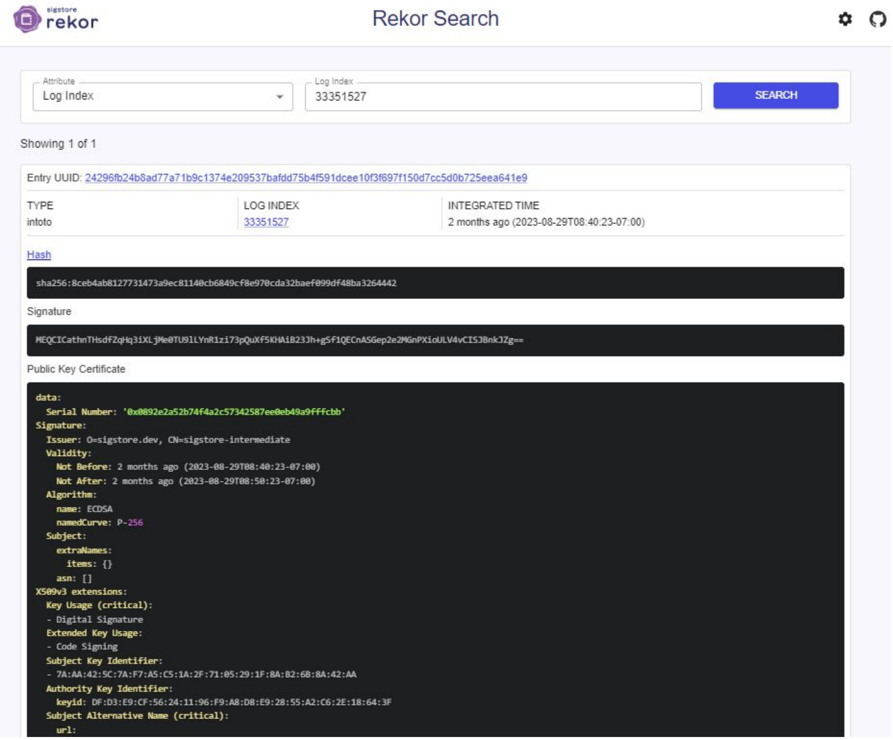
Trust Foundation
Provide robust authentication and integrity primitives

Sigstore, SPIFFE

Adapted from https://security.googleblog.com/2022/10/announcing-guac-great-pairing-with-slsa.html

Tech Highlight: OpenSSF Sigstore

- Framework for SW artifact signing:
  - Auditable credential management
  - Transparency log of artifact signatures, incl. signed metadata
- Focus on ease of use and integration with legacy tools (e.g., Docker)



Attribute: Log Index

Log Index: 33351527

Showing 1 of 1

Entry UUID: 24296fb24b8ad77a71b9c1374e209537bafdd75b4f591dcee10f3f697f150d7cc5d0b725eea641e9

TYPE	LOG INDEX	INTEGRATED TIME
intoto	33351527	2 months ago (2023-08-29T08:40:23-07:00)

Hash

```
sha256:8ceb4ab8127731473a9ec81140cb6849cf8e970cda32baef099df48ba3264442
```

Signature

```
MEQCICathnTHsdfZqHq3iXLjMe0TU9lLYnR1zi73pQuXf5KHAiB23Jh+gSf1QECnASGep2e2MGnPXioULV4vCISJBnkJZg==
```

Public Key Certificate

```
data:
  Serial Number: '0x0892e2a52b74f4a2c57342587ee0eb49a9fffcbb'
Signature:
  Issuer: O=sigstore.dev, CN=sigstore-intermediate
  Validity:
    Not Before: 2 months ago (2023-08-29T08:40:23-07:00)
    Not After: 2 months ago (2023-08-29T08:50:23-07:00)
  Algorithm:
    name: ECDSA
    namedCurve: P-256
  Subject:
    extraNames:
      items: {}
    asn: []
X509v3 extensions:
  Key Usage (critical):
  - Digital Signature
  Extended Key Usage:
  - Code Signing
  Subject Key Identifier:
  - 7A:AA:42:5C:7A:F7:A5:C5:1A:2F:71:05:29:1F:8A:B2:6B:8A:42:AA
  Authority Key Identifier:
    keyid: DF:D3:E9:CF:56:24:11:96:F9:A8:D8:E9:28:55:A2:C6:2E:18:64:3F
  Subject Alternative Name (critical):
    url:
```

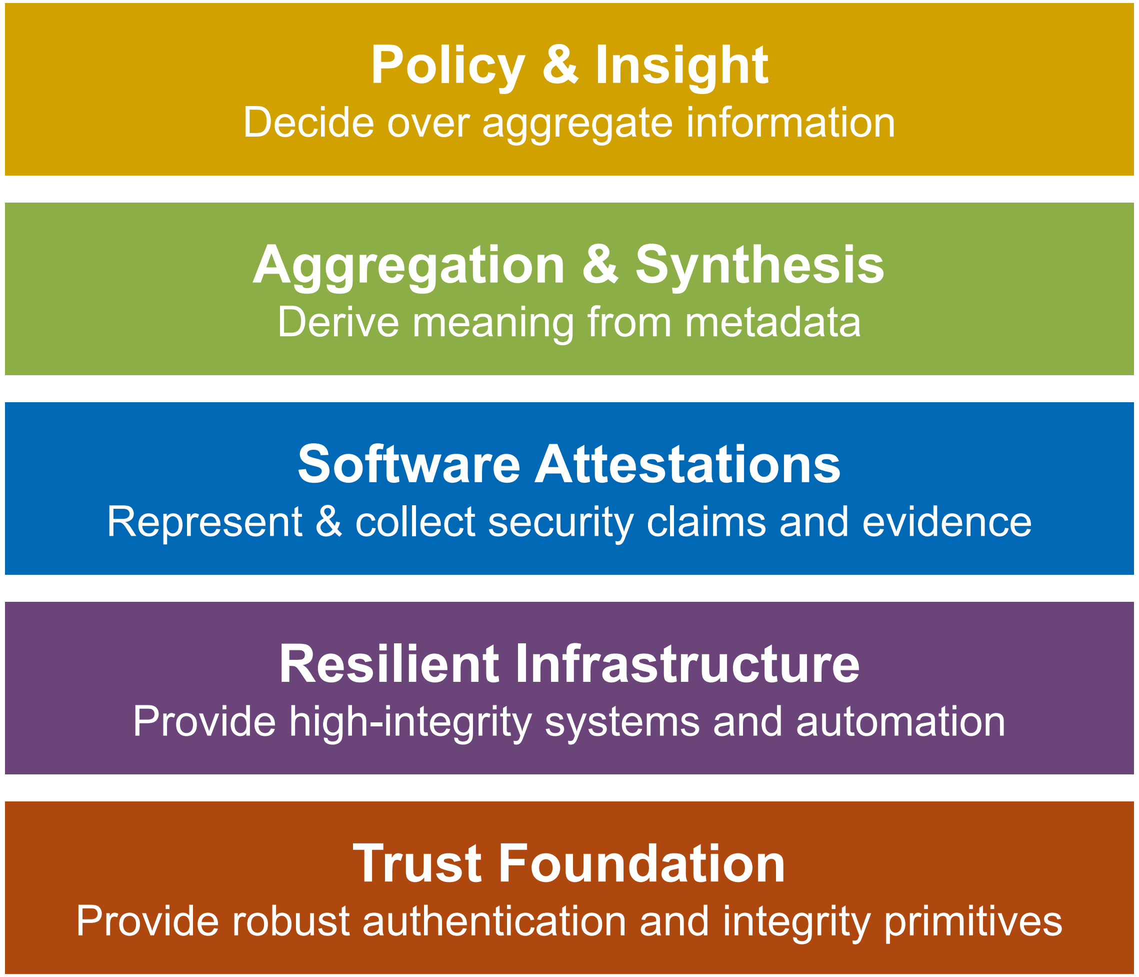
Source: https://docs.sigstore.dev/

Tech Highlight: CNCF SPIFFE

- SPIFFE = Secure Production Identity Framework for Everyone
- Framework for identifying *deployed* workloads
  - Ranges from single process to replicated web server
  - IDs are URIs identifying a trust domain and specific workload
- SPIRE asserts and validates claims about workload IDs

Source:
https://spiffe.io/docs/latest/spiffe-about/overview/

SWSC Technology Areas – Highlights



Policy & Insight
Decide over aggregate information

Aggregation & Synthesis
Derive meaning from metadata

Software Attestations
Represent & collect security claims and evidence

Resilient Infrastructure
Provide high-integrity systems and automation

Trust Foundation
Provide robust authentication and integrity primitives

Hardware Attested Build Environments*

Sigstore, SPIFFE

*in-flight

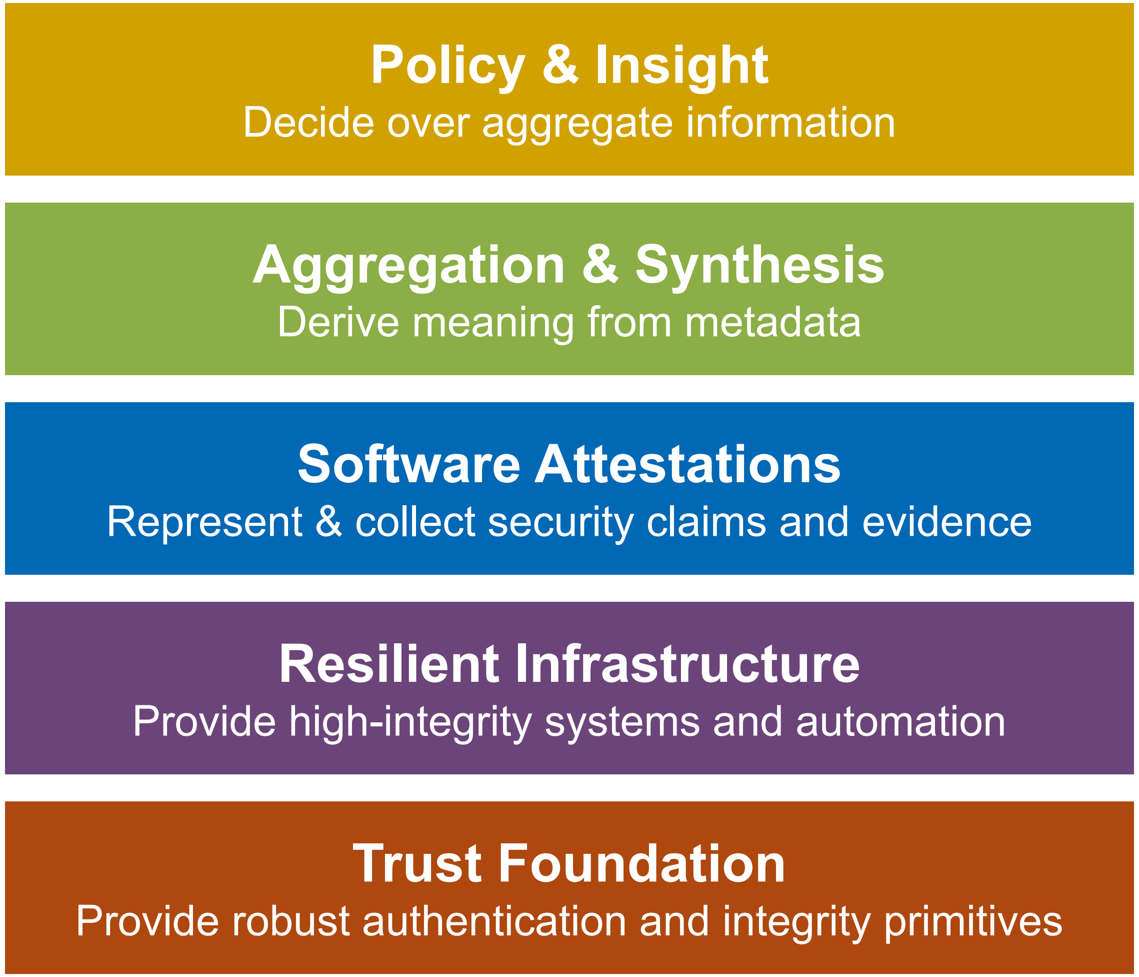
Adapted from https://security.googleblog.com/2022/10/announcing-guac-great-pairing-with-slsa.html

Tech Highlight: Hardware-Attested Build Environments

- Framework for provenance of the compute environment of software builds
  - Rely on trusted hardware (TPMs, confidential computing) as root of trust
  - Capture chain of custody of build VMs/containers
- Focus on integration with CI/CD platforms
- Upcoming enhancement to OpenSSF SLSA spec

Source:
https://ossna2024.sched.com/event/1aBOt/

SWSC Technology Areas – Highlights



Policy & Insight
Decide over aggregate information

Aggregation & Synthesis
Derive meaning from metadata

Software Attestations
Represent & collect security claims and evidence

Resilient Infrastructure
Provide high-integrity systems and automation

Trust Foundation
Provide robust authentication and integrity primitives

Adapted from https://security.googleblog.com/2022/10/announcing-guac-great-pairing-with-slsa.html

SBOM, SLSA, in-toto

Hardware Attested Build Environments*

Sigstore, SPIFFE

*in-flight

Tech Highlight: Software Bill of Materials (SBOM)

- List of “ingredients” that make up a piece of software
- Different types of SBOM for SW dev lifecycle phases
- Two main standards: SPDX and CycloneDX

Sources: https://ntia.gov/page/software-bill-materials
https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf

Common misconception #2

An SBOM contains all the information you need about a piece of SW.

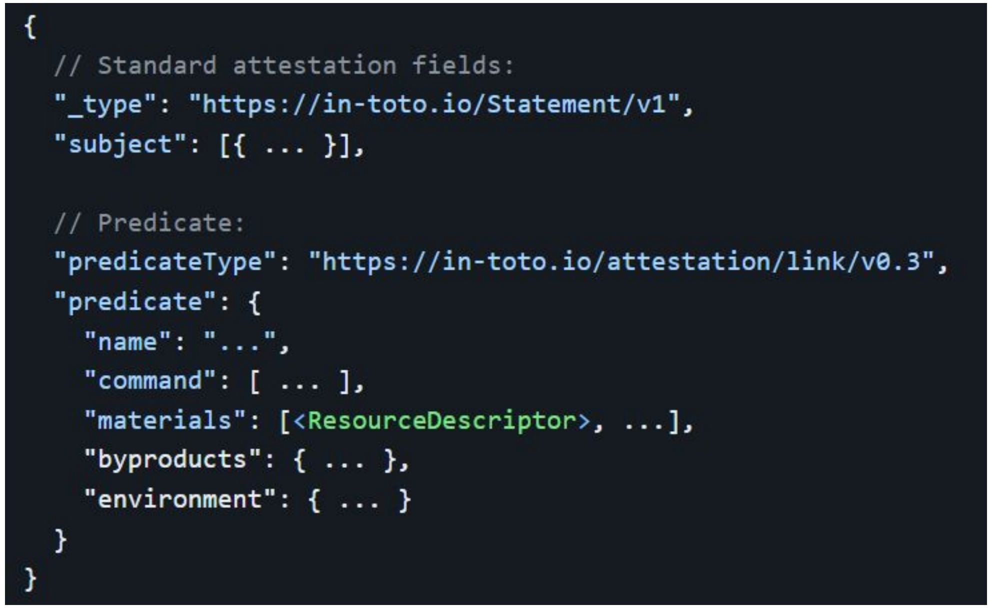
Tech Highlight: OpenSSF SLSA

- SLSA = Supply-chain Levels for Software Artifacts (pronounced “salsa”)
- Standard for build process provenance: describes the “recipe” for how a piece of software was created from its source
- Spec and tooling for collecting/verifying build provenance
- Complements SBOM

Source:
https://slsa.dev

Tech Highlight: CNCF in-toto

- Framework for authenticated claims about any aspect of the SW supply chain
- Spec and tooling for:
  - Expressing SW supply chain policy
  - Collecting claims/evidence

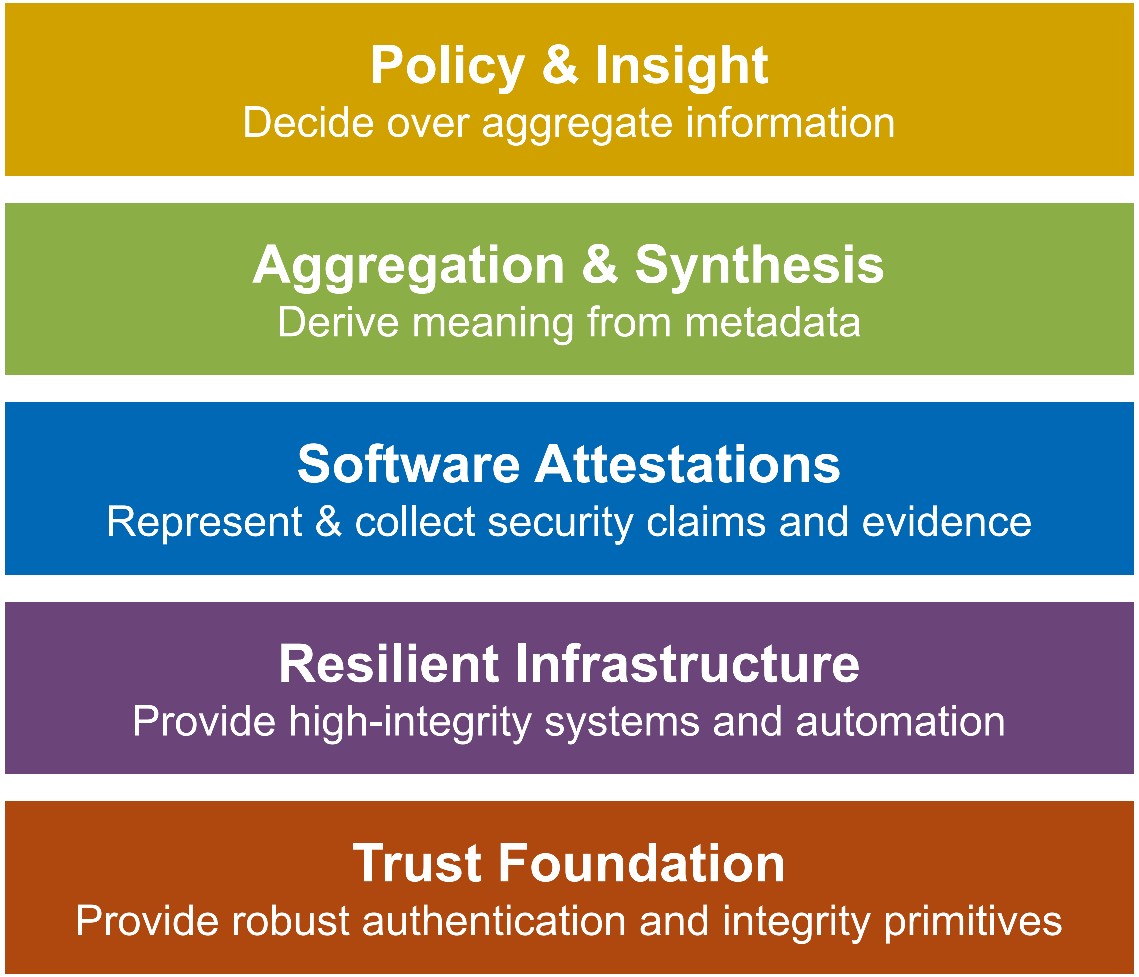


```
{
  // Standard attestation fields:
  "_type": "https://in-toto.io/Statement/v1",
  "subject": [{ ... }],

  // Predicate:
  "predicateType": "https://in-toto.io/attestation/link/v0.3",
  "predicate": {
    "name": "...",
    "command": [ ... ],
    "materials": [<ResourceDescriptor>, ...],
    "byproducts": { ... },
    "environment": { ... }
  }
}
```

Source:
https://github.com/in-toto/attestation

SWSC Technology Areas – Highlights



Policy & Insight
Decide over aggregate information

Aggregation & Synthesis
Derive meaning from metadata

Software Attestations
Represent & collect security claims and evidence

Resilient Infrastructure
Provide high-integrity systems and automation

Trust Foundation
Provide robust authentication and integrity primitives

SBOM, SLSA, in-toto

Hardware Attested Build Environments*

Sigstore, SPIFFE

*in-flight

Adapted from https://security.googleblog.com/2022/10/announcing-guac-great-pairing-with-slsa.html

Agenda

- Software Supply Chain
  - Why SW supply chain security matters
  - The SWSC landscape
  - Tech highlights: SBOM, SLSA, in-toto, HW-Attested Builds, SPIFFE, Sigstore
- What's next
  - Attribute-based trust
  - ML Model Supply Chain

Attribute-based Trust

- Can we collect an extra layer of information about code behavior *before it's deployed*?
- Good news: Info is already available through the supply chain!
- Examples:
  - Vulnerability analysis
  - Static code analysis
  - ML-based code analysis
  - Runtime traces of build systems
  - Compiler flags that affect code properties

Adding support through in-toto

Ongoing Work towards ML Model Provenance

- Defining the ML model supply chain: All steps from data and algorithm sourcing to model deployment
- Threat modeling: What are ML-specific supply chain threats?
- Efficient representations of ML models, esp. LLMs
  - End goal: cryptographic integrity checking and signing
  - Ex. OpenSSF Model Signing Project

Final Thoughts – Opportunities for Supply Chains

- A lot of prior work on SW supply chain provenance that can be reused/adapted for the ML setting.
- Data provenance (e.g., C2PA) needs to play a central role in ML model supply chain trust along with software provenance.
- Rethink trust as provenance + attributes + policy verification.

Thank You!

Contact: marcela.melara@intel.com