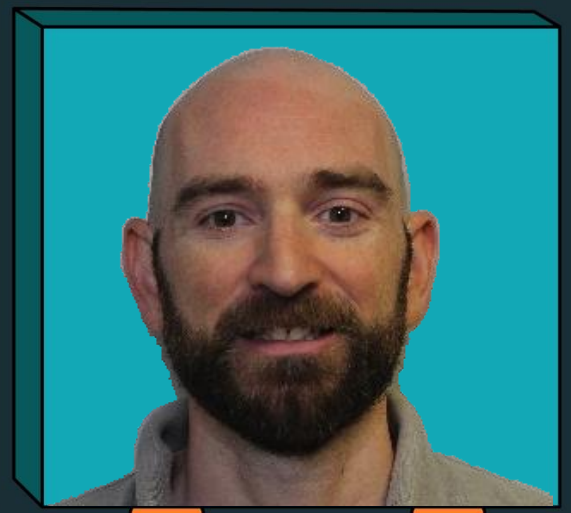


Brent Clausner

Enhancing Validation Through Attestations

PACIFIC NW SOFTWARE QUALITY CONFERENCE

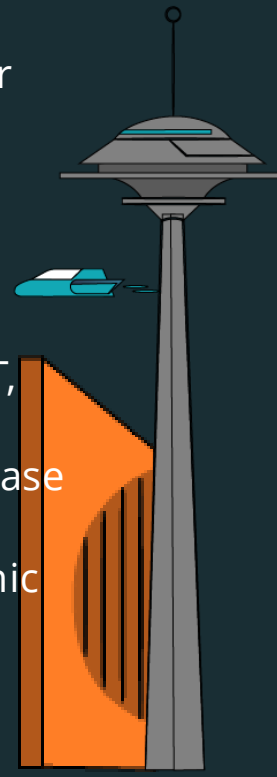
THE FUTURE IS NOW

PNSQC.ORG

OCTOBER 14-16 2024

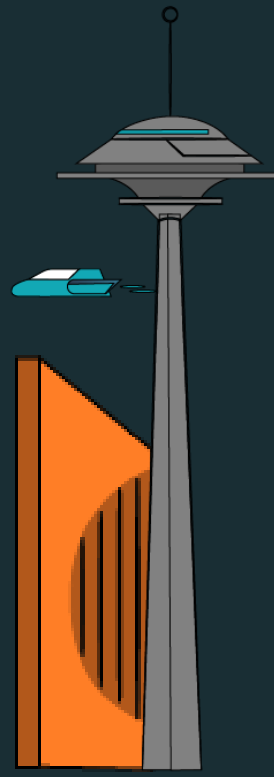
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM24-1071



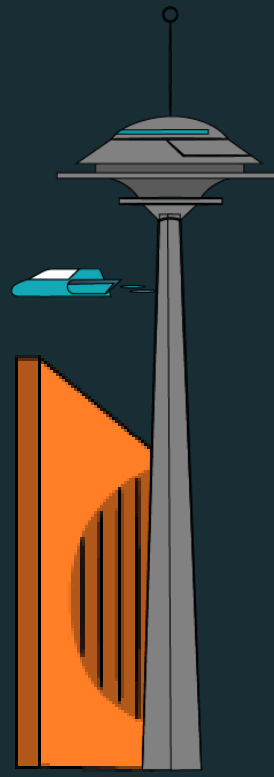
Agenda

- Who I am
- Attestations Overview
  - Why / How
- Current tools
- Terminology
- In-toto normal usage
- In-toto proposed usage
- Demo (Lets see it in action)



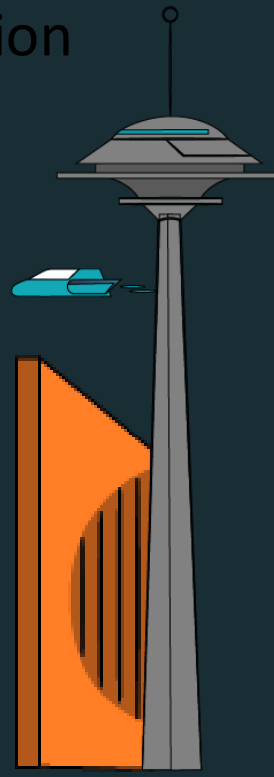
Who I am

- Professional Background
  - Education
  - Positions held
- Interests
  - Professional
  - Personal

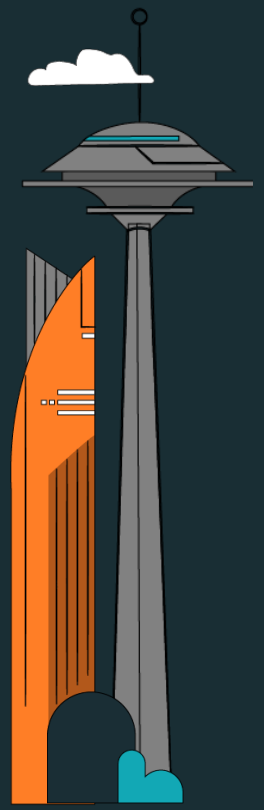


Attestations

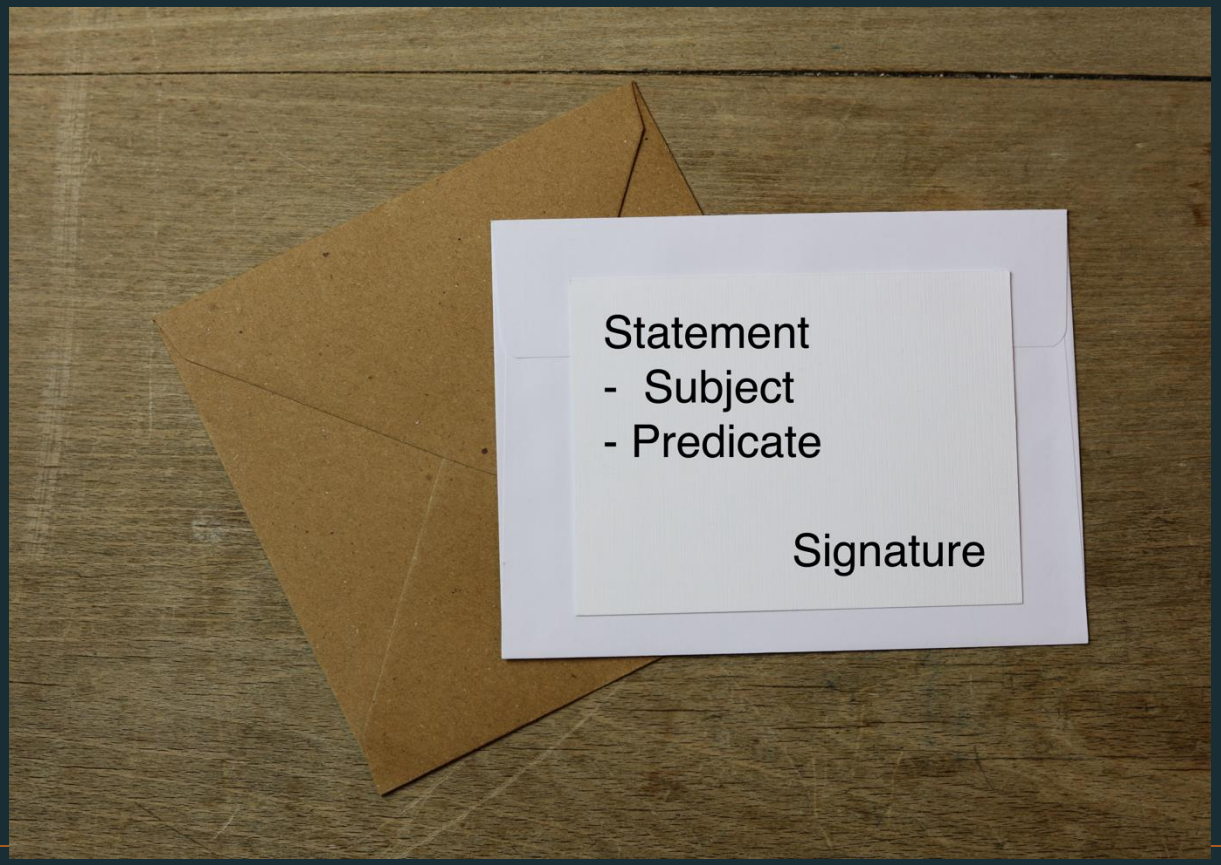
- Software Attestations
  - An authenticated statement (metadata) about a software artifact or collection of software artifacts
- Why?
  - Solar winds supply-chain attack
- How?
  - Beyond normal checksum validation
  - Traceable to who did what
  - Verify commands used to build



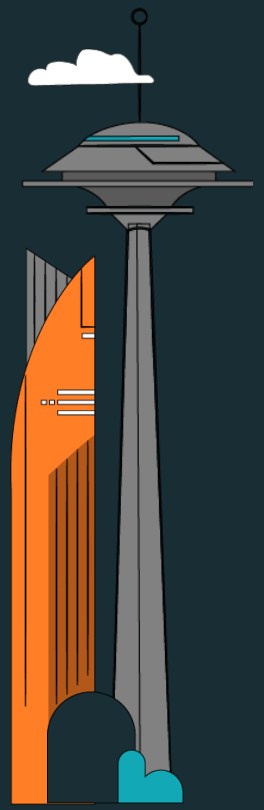
Attestations Overview



- Envelope
  - Statement
    - Subject
    - Predicate
  - Signature



Attestations Overview

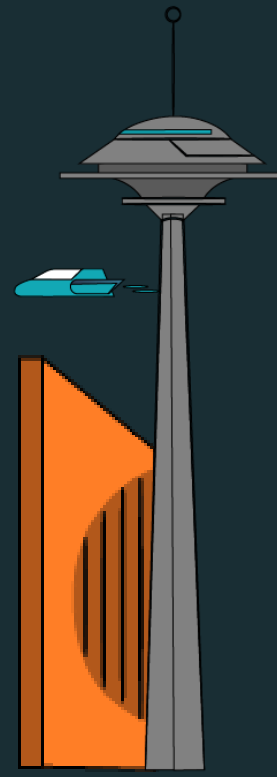


- In-toto Attestation
  - Statement
    - Subject
      - “Cargo.toml”
    - Predicate
      - “sha256: f8c…”
  - Signature
    - “sig: 4e7…”


```
{
 "signatures": [
  {
   "keyid": "fe5a11cf9...",
   "sig": "4e70b0fd28f128..."
  }
 ],
 "signed": {
  "_type": "link",
  "byproducts": {
   "return-value": 0,
   "stderr": "warning: `/path/user/.cargo/config` is deprecated...",
   "stdout": ""
  },
  "command": [
   "cargo", "build"
  ],
  "environment": {},
  "materials": {
   "Cargo.toml": {
    "sha256": "f8c0089161e8d025..."
   },
   ...
  },
  "name": "building",
  "products": {
   "Cargo.lock": {
    "sha256": "7624a5..."
   },
   ...
  }
 }
}
```

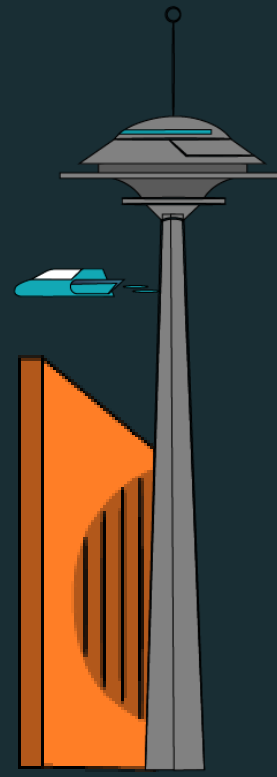
Current Tools

- In-toto (Main focus tool)
  - Allows generation and verification of attestations
  - Open source
- Witness
  - Implements in-toto's ITE-5, ITE-6, and ITE-7
  - Open source
- Binary Authorization
  - Google based for Kubernetes images



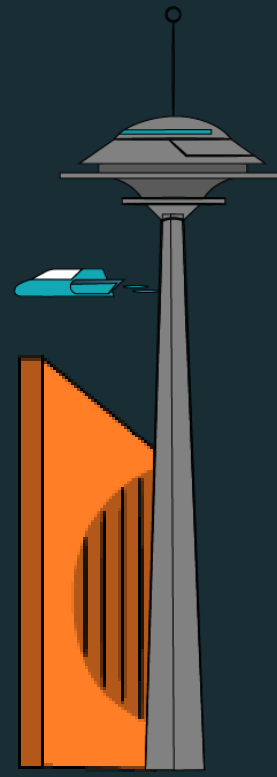
Terminology

- Layout
  - Specifies each step to be done
- Step
  - Contains command, materials, products, and signature
- Materials
  - Files that are expected to exist prior to running command
- Products
  - Files that are existing, created/deleted after command
- Inspection
  - Additional command for validation that errors on non-zero

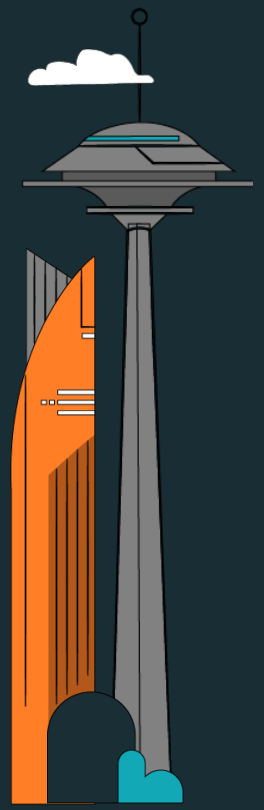


In-toto usage

- Layout
  - Python
  - JSON
  - Expires
- Single Layout Usage
  - Build step attestations
  - Publish layout, public keys, attestations, and software



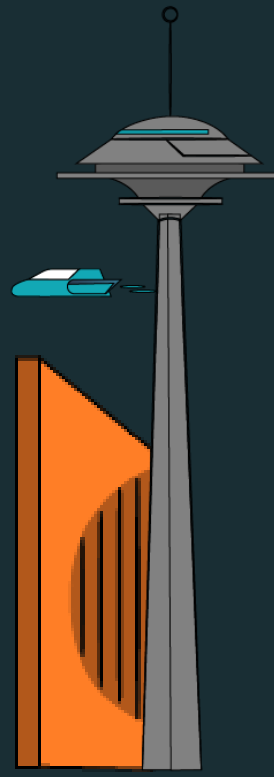
In-toto Usage - Build



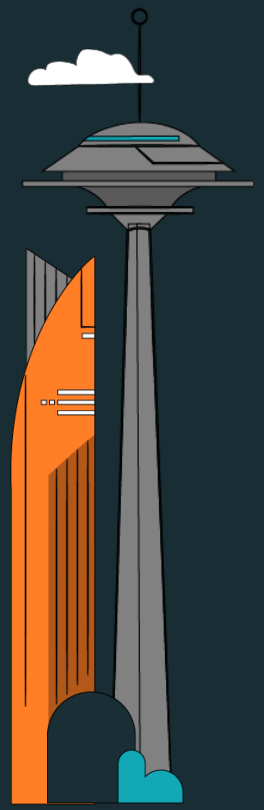
```
layout = Layout.read({
    "_type": "layout",
    "keys": {
        key_owner["keyid"]: key_owner,
    },
    "steps": [
        {
            "name": "building",
            "expected_materials": [
                ["ALLOW", "src/*"], ["ALLOW", "*.link"], ["ALLOW", "*.pub"],
                ["ALLOW", "*.layout"], ["ALLOW", "Cargo.toml"],
                ["DISALLOW", "*"]
            ],
            "expected_products": [
                ["MATCH", "*", "WITH", "MATERIALS", "FROM", "building"],
                ["CREATE", "target/*"], ["CREATE", "Cargo.lock"],
                ["DISALLOW", "*"]
            ],
            "expected_command": [
                "cargo", "build"
            ],
            "threshold": 1,
            "pubkeys": [key_owner["keyid"]],
        },
        # Continued ---------------------->
        {
            "name": "package",
            "expected_materials": [
                ["MATCH", "*", "WITH", "MATERIALS", "FROM", "building"],
                ["MATCH", "*", "WITH", "PRODUCTS", "FROM", "building"],
                ["DISALLOW", "*"]
            ],
            "expected_products": [
                ["MATCH", "*", "WITH", "MATERIALS", "FROM", "building"],
                ["MATCH", "*", "WITH", "PRODUCTS", "FROM", "building"],
                ["CREATE", "package.tar"],
                ["DISALLOW", "*"]
            ],
            "expected_command": [
                "tar", "-cf", "package.tar", "target/debug/simple",
            ],
            "threshold": 1,
            "pubkeys": [key_owner["keyid"]],
        },
    ],
    "inspect": [],
})
```

Proposed Usage

- Build Layout
  - Build
  - Static Analysis
  - Package
- Multiple Layout(s) – QA Team based
  - Verify the First layout
    - Ensures everyone is testing the same software
  - Test the software
- Release based layout
  - Verifies all test-based layouts in one layout

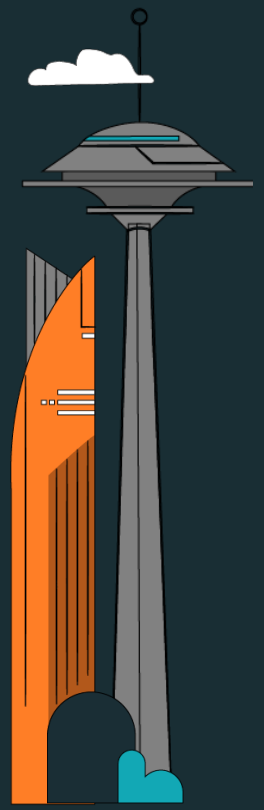


Proposed Usage - QA



```
layout = Layout.read({
    "_type": "layout",
    "keys": {
        key_owner["keyid"]: key_owner,
    },
    "steps": [
{
                "name": "verify",
                "expected_materials": [
                    ["ALLOW", "*.link"], ["ALLOW", "*.pub"],
                    ["ALLOW", "package.tar"], ["ALLOW", "*.layout"],
                    ["ALLOW", "target/debug/simple"],
                    ["DISALLOW", "*"]
                ],
                "expected_products": [
                    ["MATCH", "*", "WITH", "MATERIALS", "FROM", "verify"],
                    ["DISALLOW", "*"]
                ],
                "expected_command": [
                    "in-toto-verify", "-l", "./build.layout",
                    "--verification-keys", "./owner.pub", "--link-dir",
                    "./"
                ],
                "threshold": 1,
                "pubkeys": [key_owner["keyid"]],
            },
# Continued ---------------------->
            {
                "name": "testing",
                "expected_materials": [
                    ["MATCH", "*", "WITH", "MATERIALS", "FROM", "verify"],
                    ["DISALLOW", "*"]
                ],
                "expected_products": [
                    ["MATCH", "*", "WITH", "MATERIALS", "FROM", "verify"],
                    ["DISALLOW", "*"]
                ],
                "expected_command": [
                    "echo", "PASS"
                ],
                "threshold": 1,
                "pubkeys": [key_owner["keyid"]],
            }
    ],
    "inspect": [],
})
```

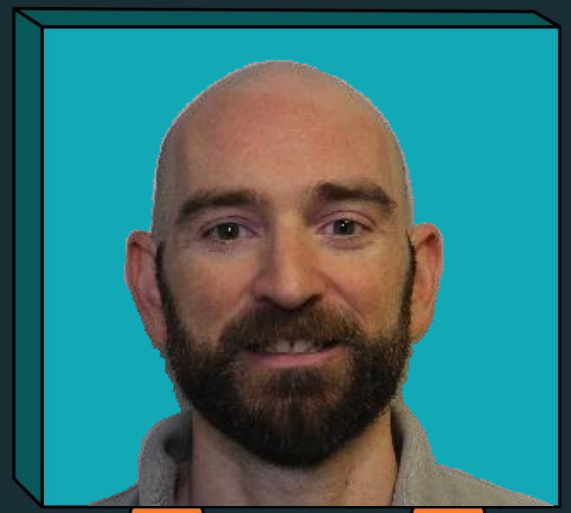
Proposed Usage - Release



- Final layout
- In-toto-verify only
  - Output is free from internal outputs
- Chain of layouts
  - Each verify with attestation links the materials throughout

```
layout = Layout.read({
      "_type": "layout",
      "keys": {key_owner["keyid"]: key_owner},
      "steps": [
         {
            "name": "release",
            "expected_materials": [
               ["ALLOW", "in-toto-files.tar"], ["ALLOW", "*.link"],
               ["ALLOW", "*.pub"], ["ALLOW", "package.tar"],
               ["ALLOW", "*.layout"], ["ALLOW", "target/debug/simple"],
               ["DISALLOW", "*"]
            ],
            "expected_products": [
               ["MATCH", "*", "WITH", "MATERIALS", "FROM", "release"],
               ["ALLOW", "*.layout"], ["ALLOW", "target/debug/simple"],
               ["DISALLOW", "*"]
            ],
            "expected_command": [
               "in-toto-verify", "-l", "./internal.layout", "--verification-keys", "./owner.pub", "--link-dir",
               "./"
            ],
            "threshold": 1,
            "pubkeys": [key_owner["keyid"]],
         }
      ],
      "inspect": []
   })
```

Demo



THANK YOU

PACIFIC NW SOFTWARE QUALITY CONFERENCE

THE FUTURE IS NOW

PNSQC.ORG

OCTOBER 14-16 2024