building reproducible builds into apt with in-toto

lukas pühringer <lukas.puehringer@nyu.edu>

NYU TANDON SCHOOL OF ENGINEERING

NJIT New Jersey Institute of Technology

reproducible builds

“a build is reproducible if given the same source code, build environment and build instructions, any party can recreate bit-by-bit identical copies of all specified artifacts” [1]

compare builds → consensus on **“correct”** build → detect **“incorrect”** build

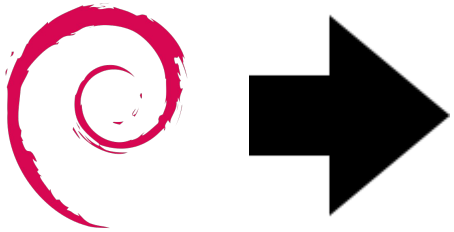
[1] https://reproducible-builds.org/docs/definition/

why should I care?

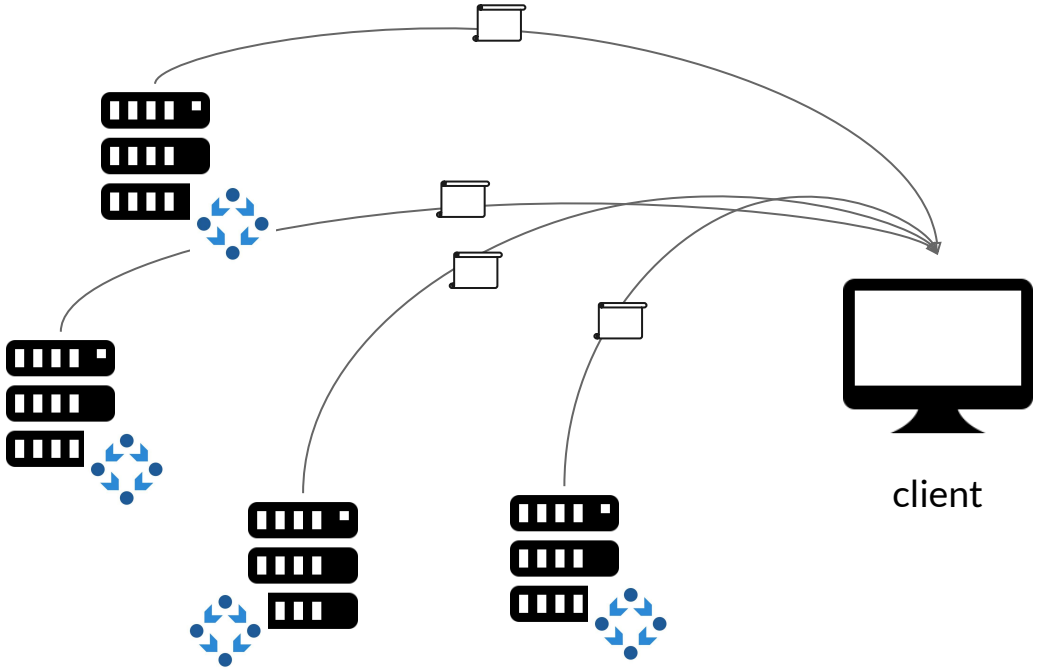
a selection of supply chain compromises:

- ASUS ShadowHammer updater attack, 2019
- NPM “event-stream” hack, 2018
- PyPI “ssh-decorate”, 2018
- NotPetya, 2017
- Kingslayer, 2017
- CCleaner, 2017
- Linux Mint, 2016
- XcodeGhost, 2015

trusted rebuilders



rebuilder periodically fetch buildinfo from debian and rebuild generating evidence



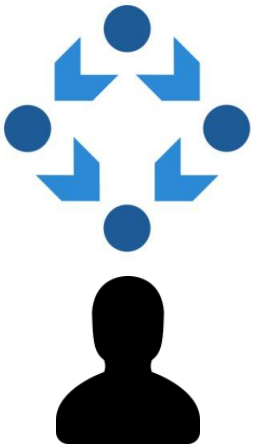
in-toto provides the verification protocol

- steps of the software supply chain
- authorized actors (functionaries)
- no gaps

in-toto -- layout -- steps

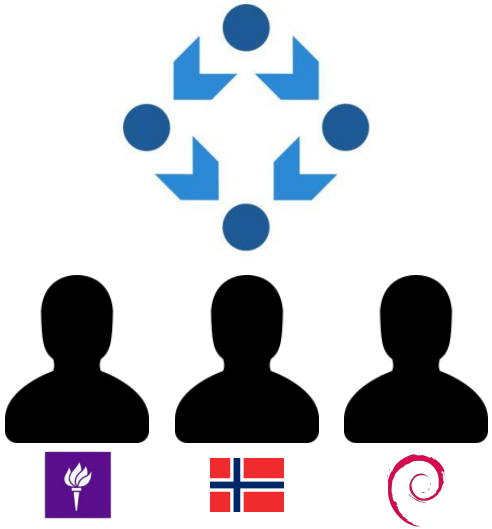
```
{
  "_type": "layout",
  "expires":"2017-08-31T12:44:15Z",
  "keys": {
    "0c6c50": { ... }
  },
  "signatures": [...],
  "steps": [{
    "_type": "step",
    "name": "rebuild",
    "expected_command": ["srebuild", ...],
    "expected_materials": [],
    "expected_products": [
      ["CREATE", "*.deb"], ...],
    "pubkeys": ["0c6c50..."],
    "threshold": 1
    }, ...],
  "inspections": [...]
}
```

in-toto -- layout -- functionaries



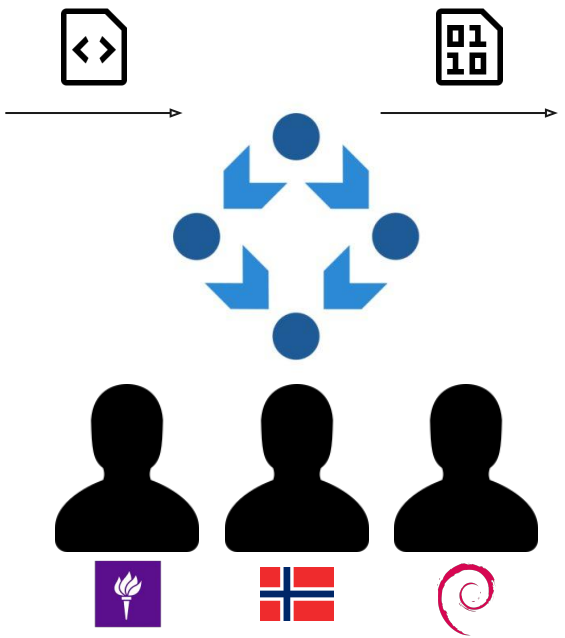
```
{
  "_type": "layout",
  "expires":"2017-08-31T12:44:15Z",
  "keys": {
    "0c6c50": { ... }
  },
  "signatures": [...],
  "steps": [{
    "_type": "step",
    "name": "rebuild",
    "expected_command": ["srebuild", ...],
    "expected_materials": [],
    "expected_products": [
      ["CREATE", "*.deb"], ...],
    "pubkeys": ["0c6c50..."],
    "threshold": 1
    }, ...],
  "inspections": [...]
}
```

in-toto -- layout -- thresholds



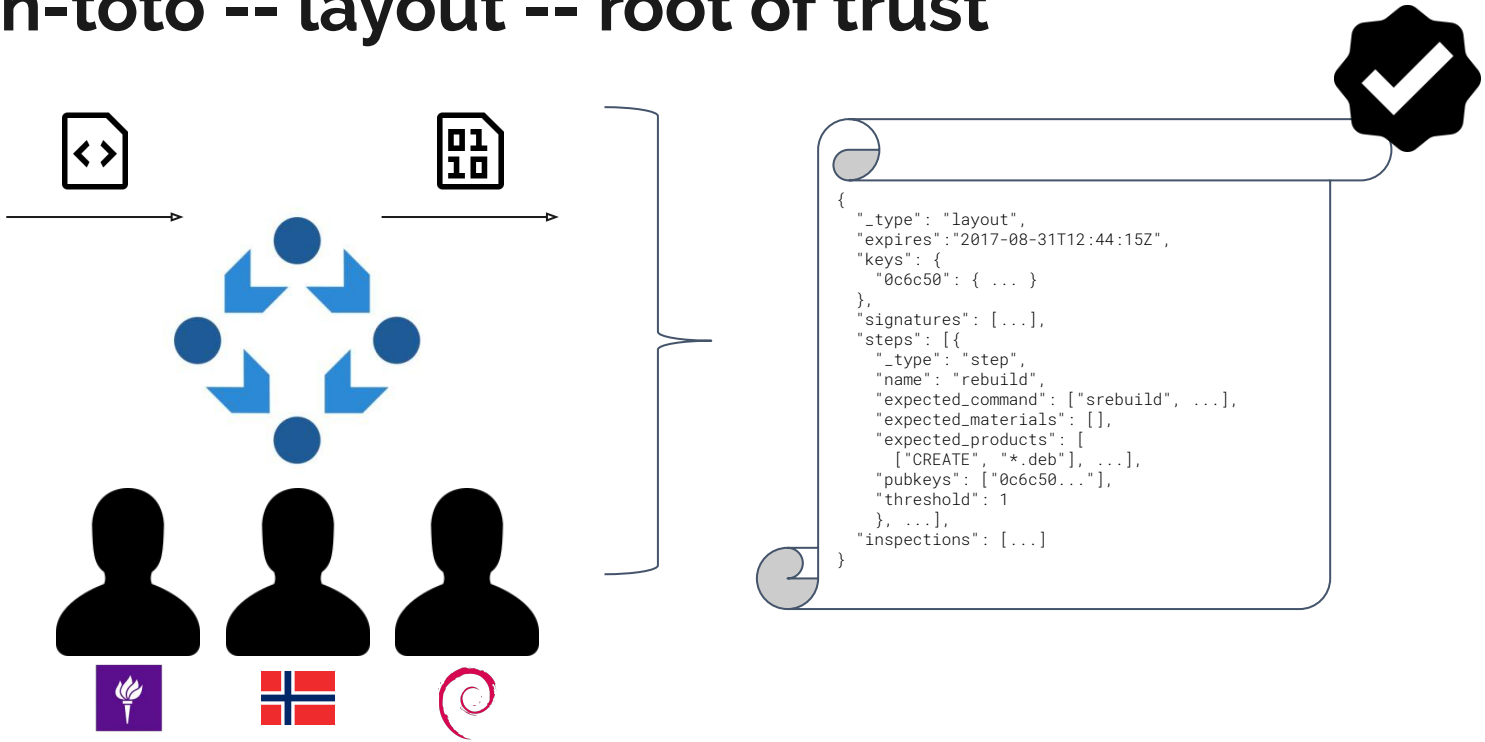
```
{
  "_type": "layout",
  "expires":"2017-08-31T12:44:15Z",
  "keys": {
    "0c6c50": { ... }
  },
  "signatures": [...],
  "steps": [{
    "_type": "step",
    "name": "rebuild",
    "expected_command": ["srebuild", ...],
    "expected_materials": [],
    "expected_products": [
      ["CREATE", "*.deb"], ...],
    "pubkeys": ["0c6c50..."],
    "threshold": 1
    }, ...],
  "inspections": [...]
}
```

in-toto -- layout -- materials and products



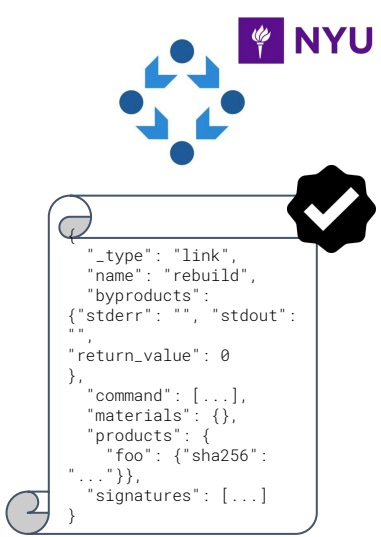
```
{
  "_type": "layout",
  "expires":"2017-08-31T12:44:15Z",
  "keys": {
    "0c6c50": { ... }
  },
  "signatures": [...],
  "steps": [{
    "_type": "step",
    "name": "rebuild",
    "expected_command": ["srebuild", ...],
    "expected_materials": [],
    "expected_products": [
      ["CREATE", "*.deb"], ...],
    "pubkeys": ["0c6c50..."],
    "threshold": 1
    }, ...],
  "inspections": [...]
}
```

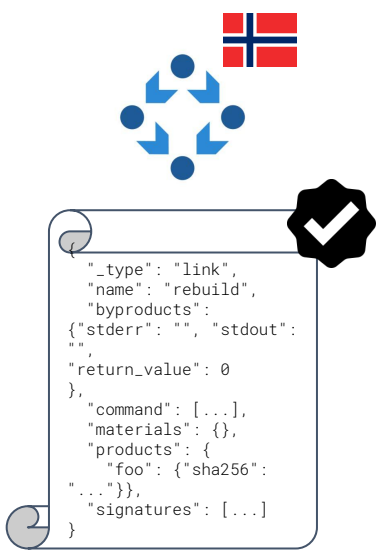
in-toto -- layout -- root of trust

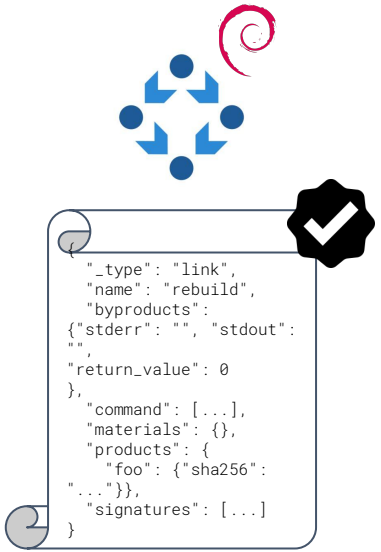


```
$ in-toto-run --key <signing key> [...] -- srebuild
```

in-toto -- signed evidence

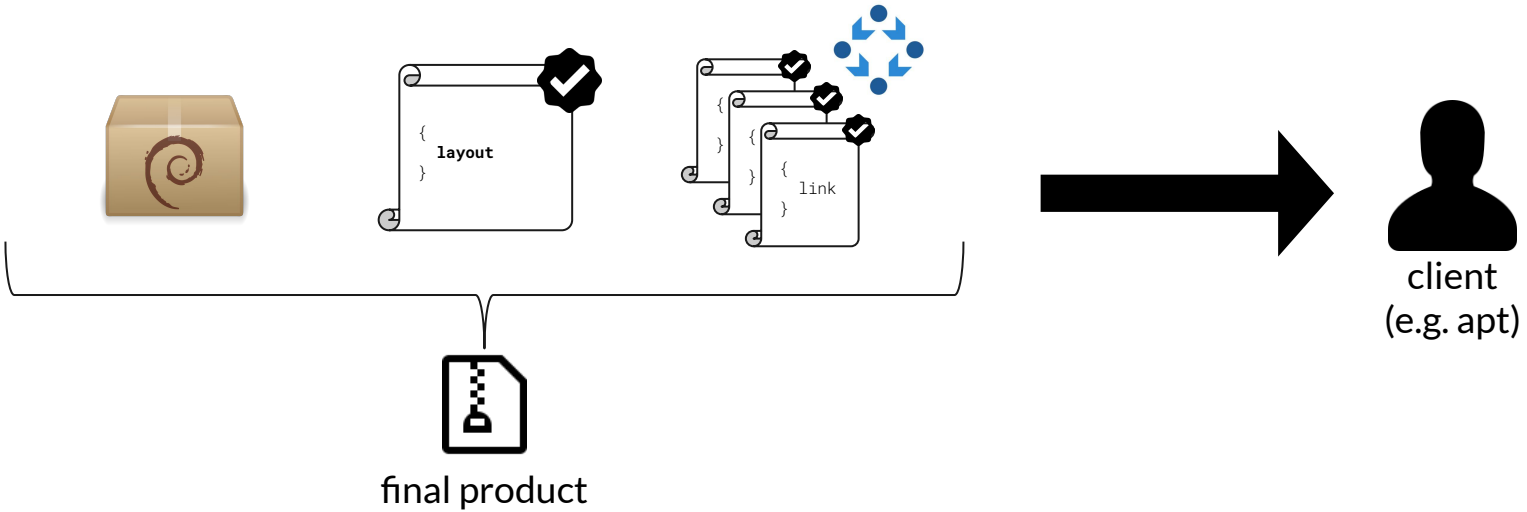






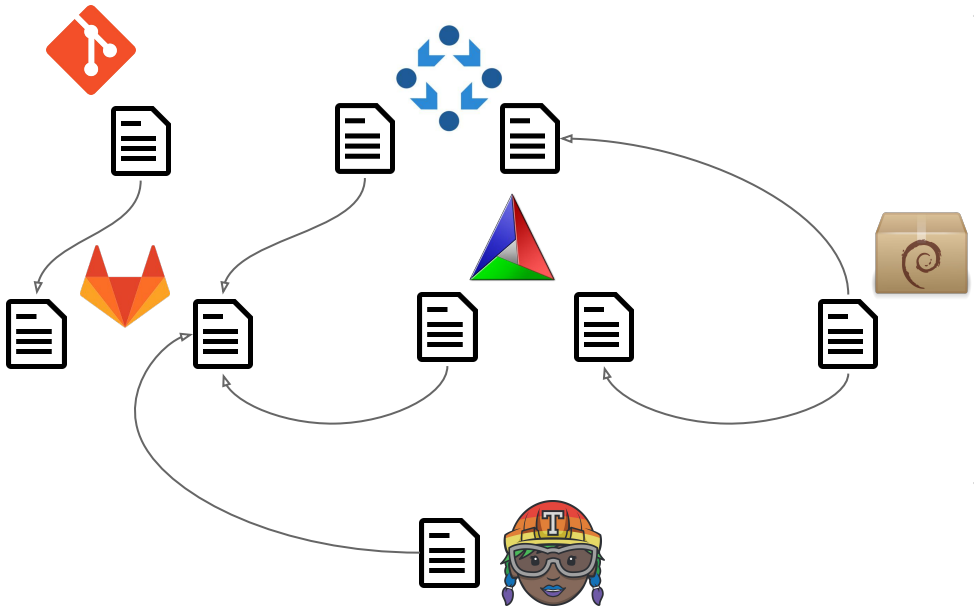
```
$ in-toto-verify --layout <layout> --key <pub key>
```

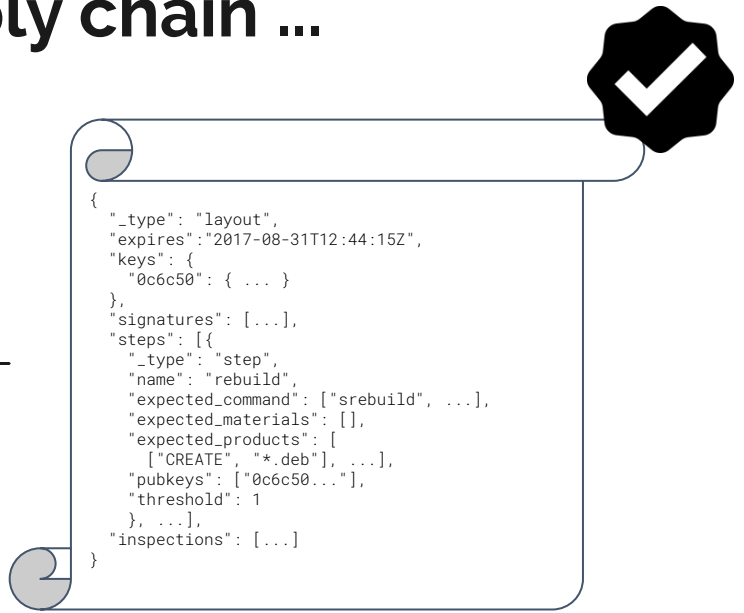
in-toto -- verification



demo

think the entire software supply chain ...





```
{
  "_type": "layout",
  "expires":"2017-08-31T12:44:15Z",
  "keys": {
    "0c6c50": { ... }
  },
  "signatures": [...],
  "steps": [{
    "_type": "step",
    "name": "rebuild",
    "expected_command": ["srebuild", ...],
    "expected_materials": [],
    "expected_products": [
      ["CREATE", "*.deb"], ...],
    "pubkeys": ["0c6c50..."],
    "threshold": 1
    }, ...],
  "inspections": [...]
}
```

thanks! questions?

in-toto.io

github.com/in-toto/apt-transport-in-toto

lukas.puehringer@nyu.edu