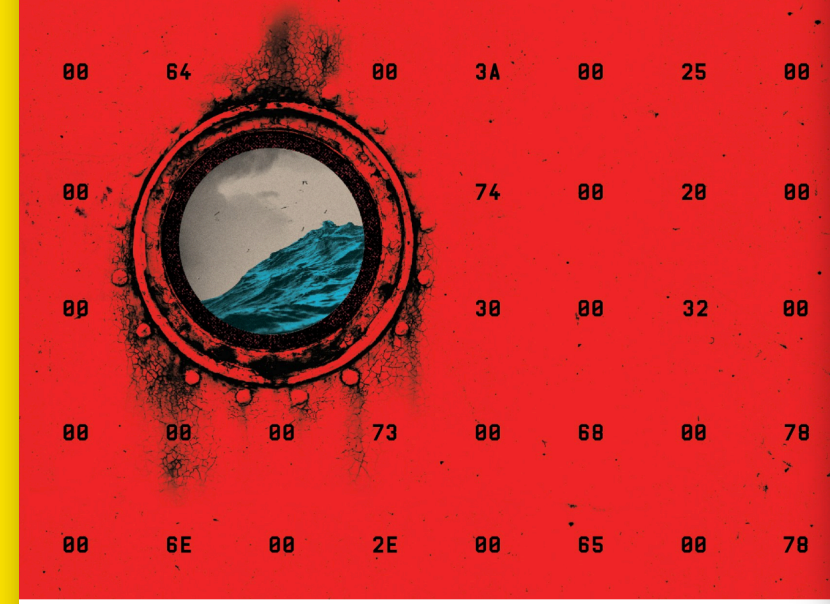
Securing Software Supply Chains with in-toto

Tobias Furuholm • Combient

NotPetya

WIRED BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION



MIKE MCQUADE

ANDY GREENBERG SECURITY 08.22.2018 05:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

MOTHERBOARD
TECH BY VICE

NotPetya Ushered In a New Era of Malware

EternalBlue and NotPetya through the eyes of influence.

By Roel Schouwenberg

Aug 26 2019, 2:00pm Share Tweet

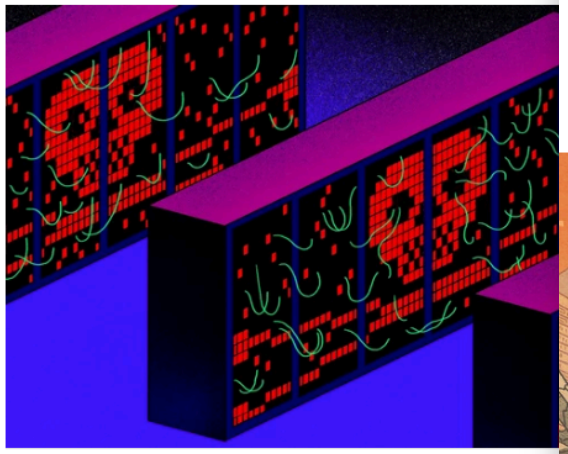
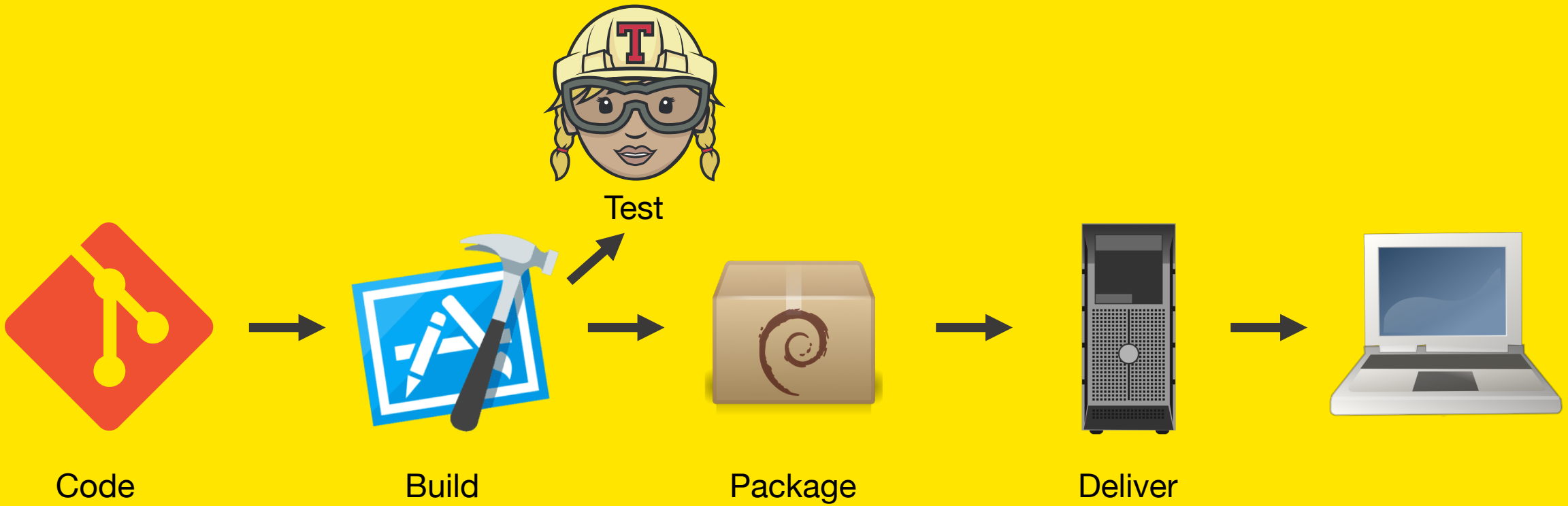


IMAGE: CATHRYN VIRGINIA

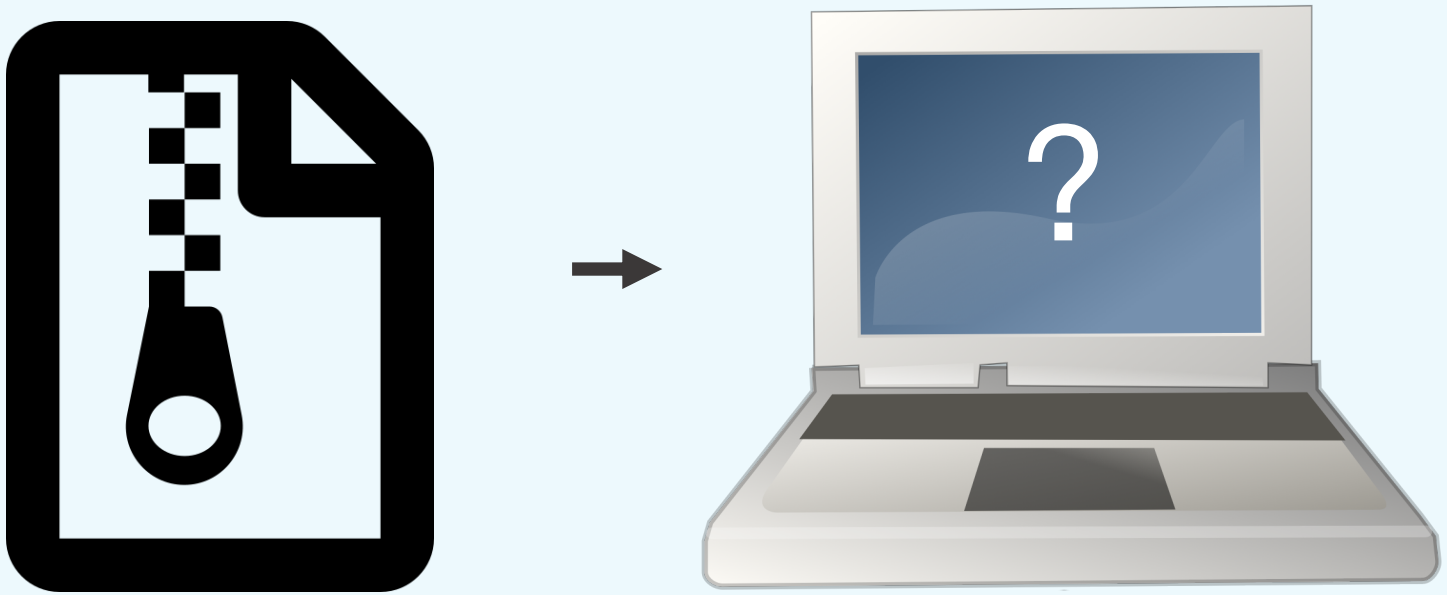
The New York Times

Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.

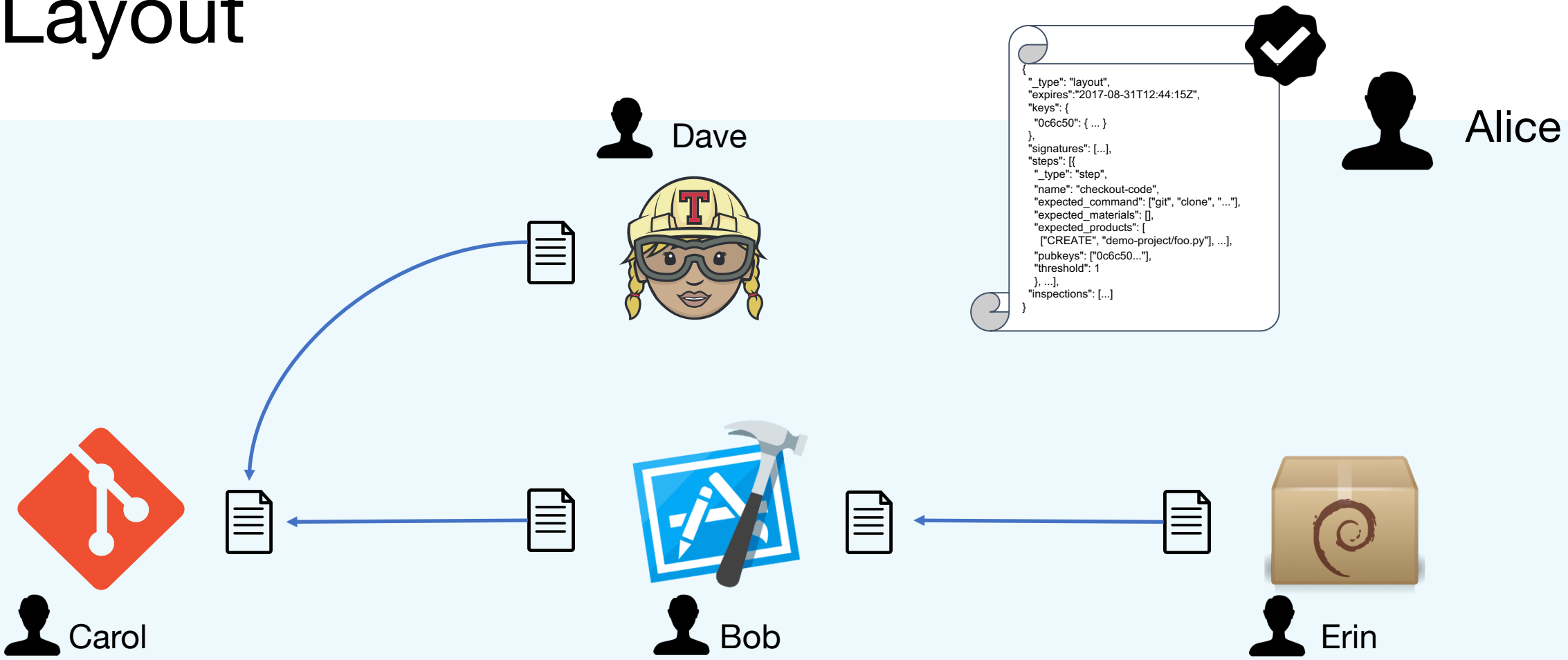
Software Supply Chain



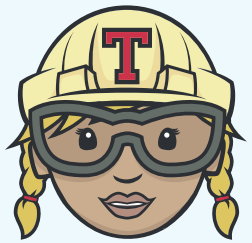
Supply chain verification with in-toto

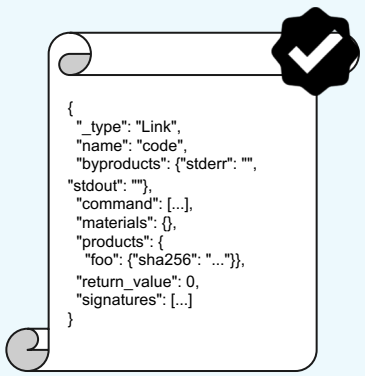


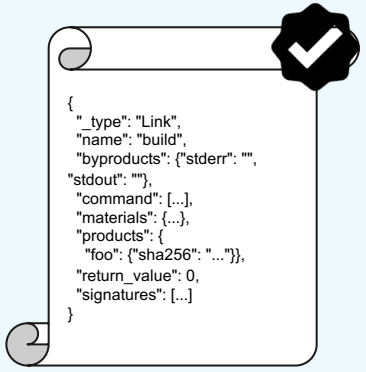
Layout

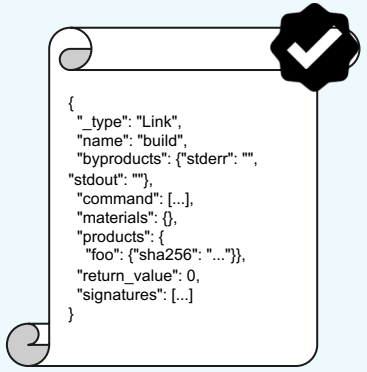

{
"_type": "layout",
"expires":"2017-08-31T12:44:15Z",
"keys": {
"0c6c50": { ... }
},
"signatures": [...],
"steps": [{
"_type": "step",
"name": "checkout-code",
"expected_command": ["git", "clone", "..."],
"expected_materials": [],
"expected_products": [
["CREATE", "demo-project/foo.py"], ...],
"pubkeys": ["0c6c50..."],
"threshold": 1
}, ...],
"inspections": [...]
}
Alice
Dave
Carol
Bob
Erin

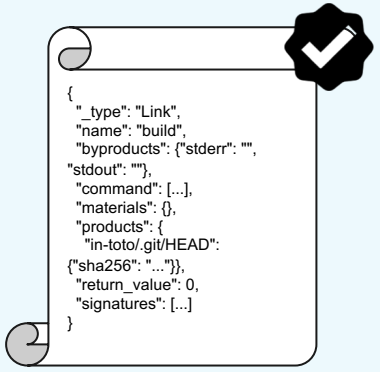
Links



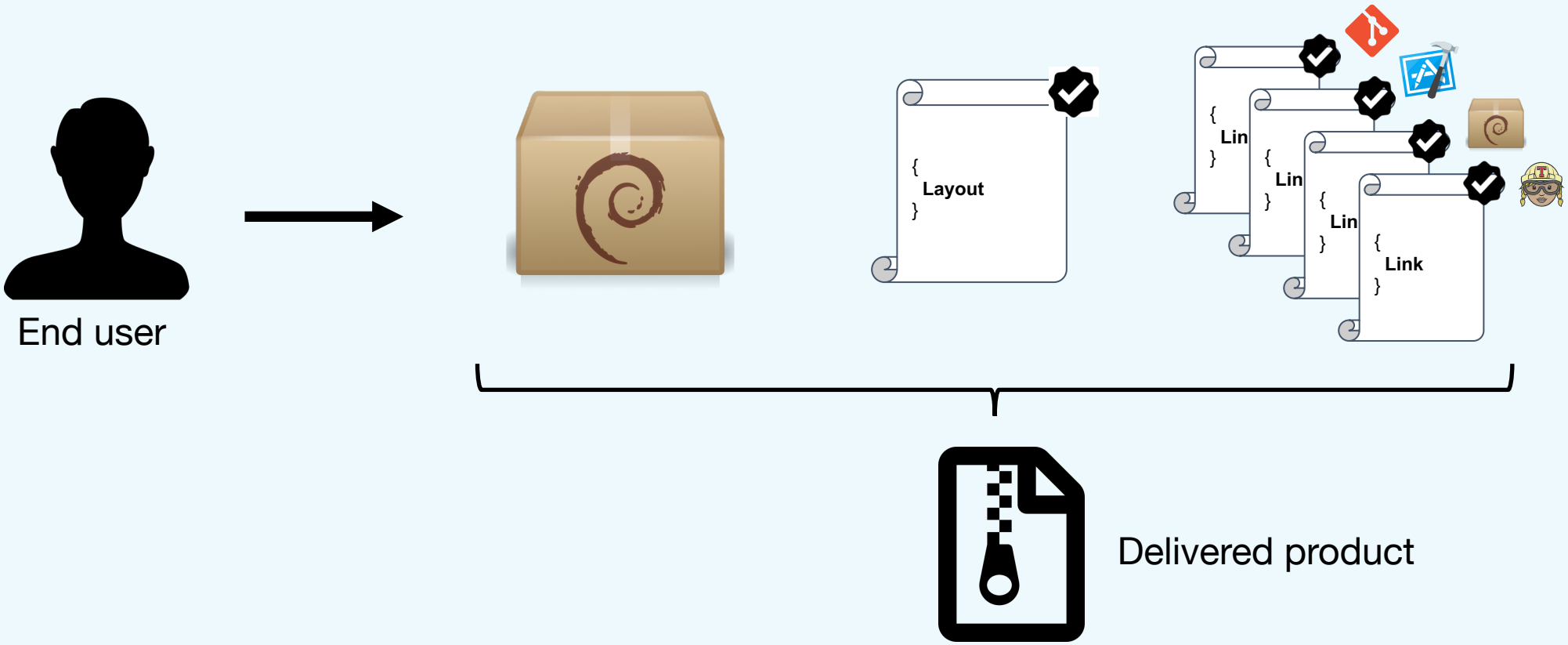

{
"_type": "Link",
"name": "code",
"byproducts": {"stderr": "",
"stdout": ""},
"command": [...],
"materials": {},
"products": {
"foo": {"sha256": "..."}},
"return_value": 0,
"signatures": [...]
}


{
"_type": "Link",
"name": "build",
"byproducts": {"stderr": "",
"stdout": ""},
"command": [...],
"materials": {...},
"products": {
"foo": {"sha256": "..."}},
"return_value": 0,
"signatures": [...]
}


{
"_type": "Link",
"name": "build",
"byproducts": {"stderr": "",
"stdout": ""},
"command": [...],
"materials": {},
"products": {
"foo": {"sha256": "..."}},
"return_value": 0,
"signatures": [...]
}


{
"_type": "Link",
"name": "build",
"byproducts": {"stderr": "",
"stdout": ""},
"command": [...],
"materials": {},
"products": {
"in-toto/.git/HEAD":
{"sha256": "..."}},
"return_value": 0,
"signatures": [...]
}

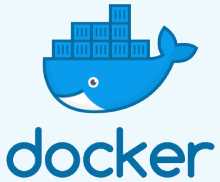
Verification



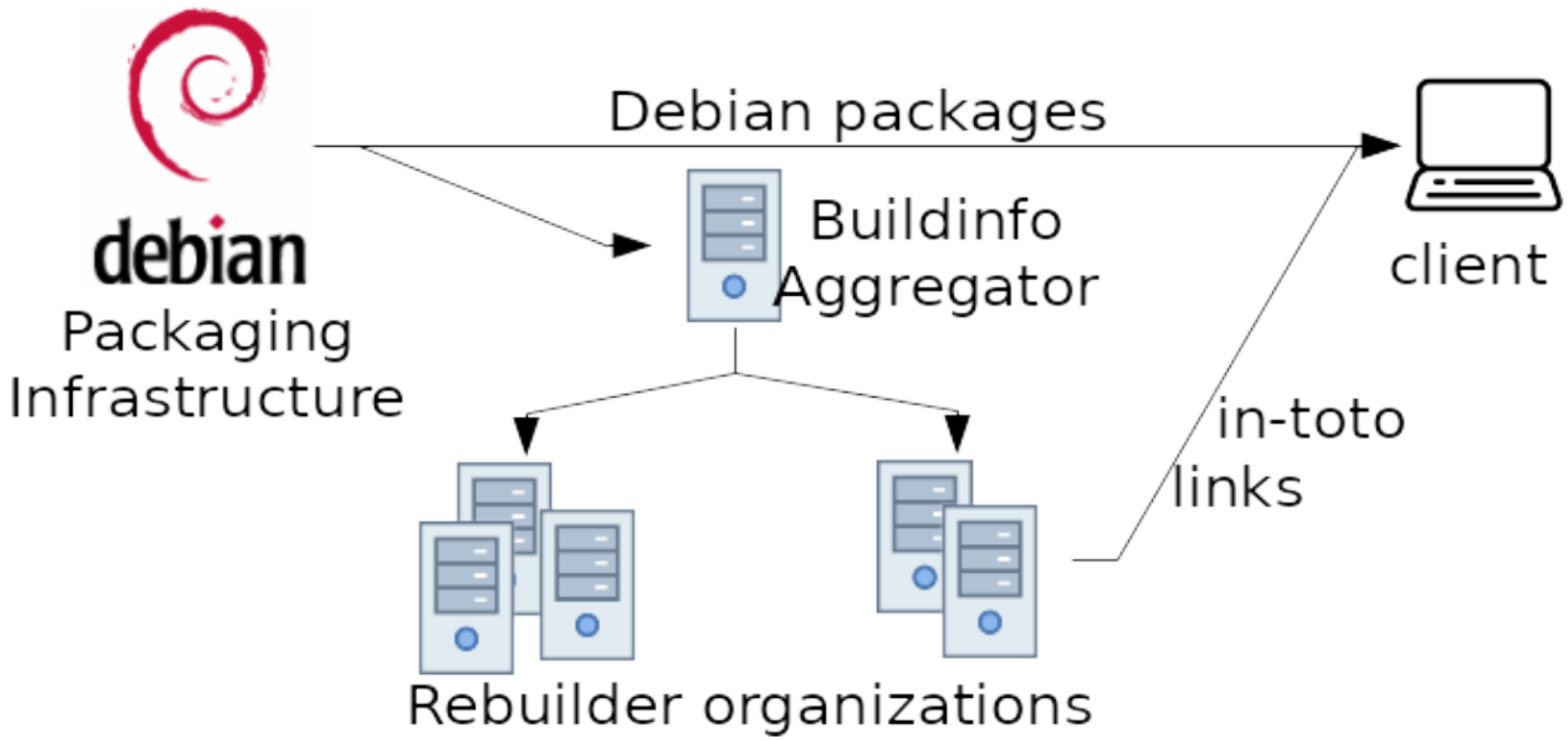
Noteworthy aspects

- Compromise resilience
- Tool agnostic
- Sub layouts

In-toto integrations



Debian in-toto integration



Let's be careful out there!

References and further reading

- in-toto: Providing farm-to-table guarantees for bits and bytes, Torres-Arias et al. - https://www.usenix.org/conference/usenixsecurity19/presentation/torres-arias
- in-toto website, https://in-toto.io
- In-toto demo: https://github.com/in-toto/demo
- Secure Publication of Datadog Agent Integrations with TUF and in-toto, Datadog, https://www.datadoghq.com/blog/engineering/secure-publication-of-datadog-agent-integrations-with-tuf-and-in-toto/
- Reproducible Builds, https://reproducible-builds.org
- Petya (malware), Wikipedia, https://en.wikipedia.org/wiki/Petya_(malware)
- The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- NotPetya Ushered In a New Era of Malware, Vice, https://www.vice.com/en_us/article/7x5vnz/notpetya-ushered-in-a-new-era-of-malware
- Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong, The New York Times, https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html

Thanks to the in-toto team for
letting me use some of their slide material!