in-toto:
Securing the Software Supply Chain

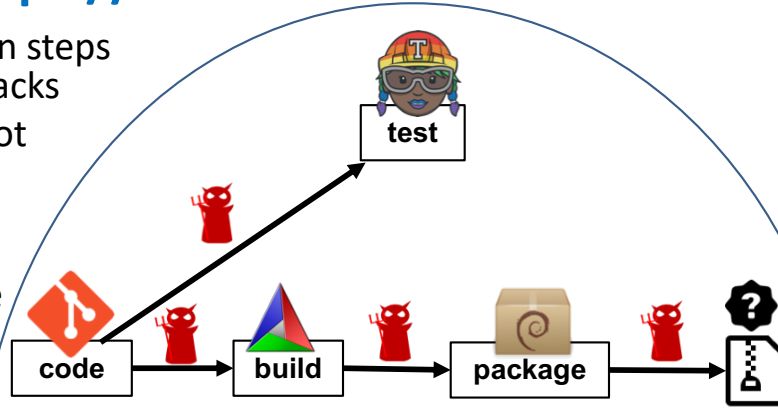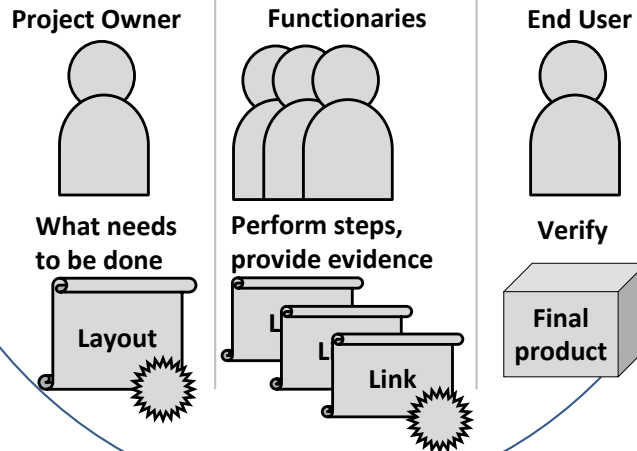**https://in-toto.io**

Challenge:

- Software supply chain steps are vulnerable to attacks
- Point solutions are not enough
- No comprehensive framework to systematically secure the entire chain
- Diversity of supply chains

Solution:

- Generate cryptographically signed metadata for each step in the chain, and link together and carry these metadata throughout the entire chain
- Tool agnostic, seamless integration, expressive enough for any supply chain, compromise resilience

test

code → build → package

Project Owner
What needs to be done
Layout

Functionaries
Perform steps, provide evidence
Link

End User
Verify
Final product

Scientific Impact:

- Raise the bar significantly for many classes of attacks
- Make the software development process transparent and publicly verifiable
- Incentivize developers to follow safe software practices

Broader Impact:

THE LINUX FOUNDATION — CLOUD NATIVE COMPUTING FOUNDATION

Through integrations, used by thousands of companies and improves the security of millions of users

debian — Reproducible Builds — archlinux — Microsoft — Google — controlplane — docker — SPDX — OPEN CONTAINER INITIATIVE

DATADOG — twitter — The Washington Post — NOKIA — FedEx — Lenovo — DREAMWORKS — SAMSUNG — COMCAST — 21ST CENTURY FOX — NGiИX — UBISOFT — Nasdaq — Ferrari — WHOLE FOODS MARKET — Alamo — AARP — CORNELL UNIVERSITY — ACTIVISION — PBS — SIEMENS Ingenuity for life — BOSE — Penn University of Pennsylvania

Justin Cappos (jcappos@nyu.edu)
NYU Tandon School of Engineering

Reza Curtmola (crix@njit.edu)
New Jersey Institute of Technology