in-toto:

Securing the Software Supply Chain



PIs: Justin Cappos (NYU), Reza Curtmola (NJIT)

NSF Award Number 1801430

Team: Santiago Torres-Arias (lead PhD student), Lukas Puhringer (lead programmer)

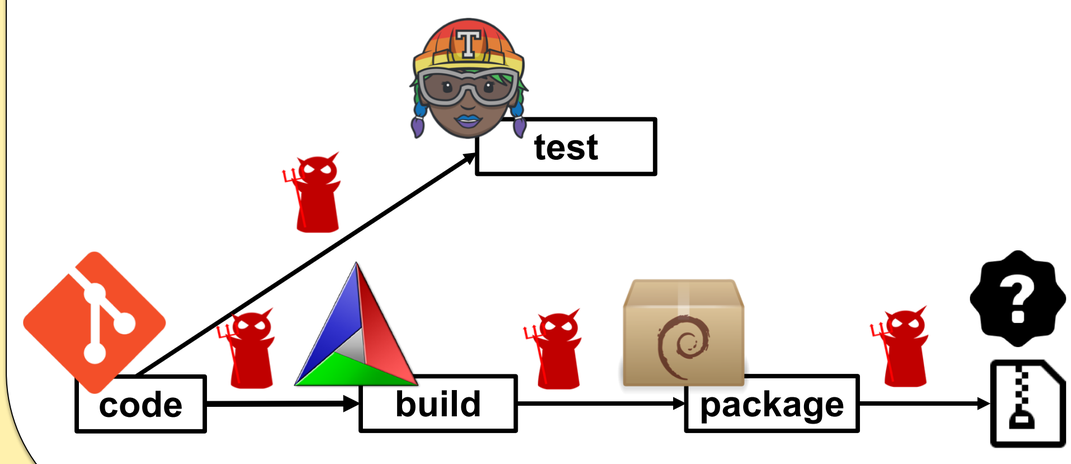
Website: https://in-toto.io

Objective: Transition into widespread practical use a framework that ensures the integrity of the software supply chain

Impact: in-toto is used by thousand of companies, improves the security of millions of users

Challenges:

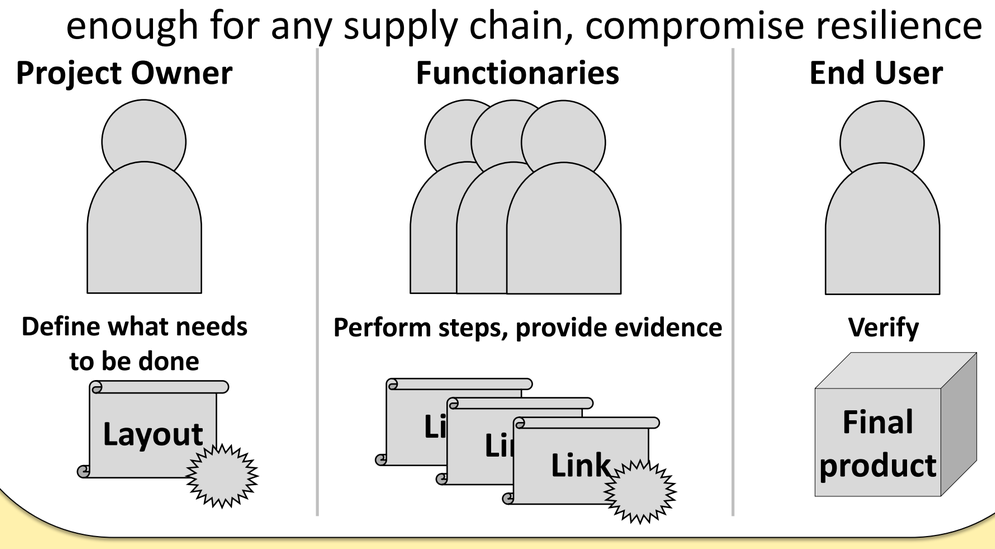
- Software supply chain steps are vulnerable to attacks
- Point solutions are not enough
- No comprehensive framework to systematically secure the entire chain
- Diversity of software supply chains



Solution (entire chain): in-toto

(USENIX Security '19)

- in-toto generates cryptographically signed metadata for each step in the chain, and links together and carries these metadata throughout the entire chain
- Tool agnostic, seamless integration, expressive enough for any supply chain, compromise resilience



Scientific Impact:

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

Solution (individual steps):

- Mitigate metadata manipulation attacks against Git (USENIX Security '16)
- Verifiable web-based Git repositories (AsiaCCS '18)
- Commit signatures for SVN (IFIP SEC '19)

Broader Impact:

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