Agenda

Secure Supply Chains

Brandon Mitchell
Twitter: @sudo_bmitch
GitHub: sudo-bmitch

```
$ whoami
- Solutions Architect @ BoxBoat
- Docker Captain
- Frequenter of StackOverflow
```

What are Supply Chain Attacks

Supply Chain Attacks in the News

- Dependency Confusion Attacks
- SolarWinds

Supply Chain Attacks in the News

- Dependency Confusion Attacks
- SolarWinds
- White House Executive Order

Supply Chain Attacks in the News

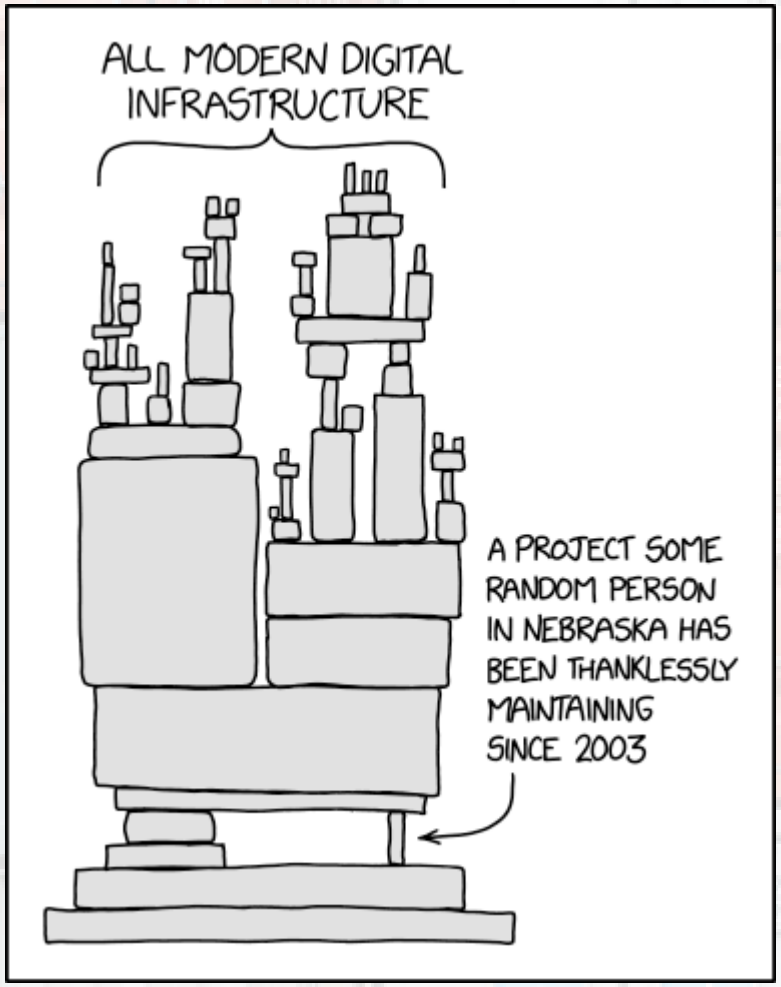
- Dependency Confusion Attacks
- SolarWinds
- White House Executive Order
- Nothing new: Ken Thompson's 1984: Reflections on Trusting Trust

Attackers Have a Variety of Methods

- Physical compromise
- Phishing and social engineering
- Unpatched applications
- Zero days
- Malicious insider
- Supply chain attacks

Supply Chain Attack

- Colonial Pipeline
- Find a soft upstream target before production
- Build servers and dependencies



xkcd.com/2347

Securing the Supply Chain

- Validate inputs
- Harden build infrastructure
- Verify the process
- Signing result
- Distribution
- Admission control

State of the Tooling

SBoMs

- Software Bill of Materials
- Two standards:
  - SPDX: Linux Foundation, focused on licensing
  - CycloneDX: OWASP, focused on security
- Should cover artifact built, dependencies, build infra, runtime infra
- Some tooling to generate, working on distributing and ingesting
- This whole space is under very active development

Attestation

- Verifying truth and authenticaty
- in-toto: verify each build step was performed, development
- Spiffe/Spire: verify trust in the agents and workloads, stable
- Keylime: hardware root of trust, stable

Signing

- PARSEC: access to hardware security, development
- TUF: framework for signing, stable
- Notary v2: signs artifacts on an OCI registry, design/prototype
- Cosign: competing image signing project, early stable
- Rekor: transparency logs, development

Distribution and Admission Control

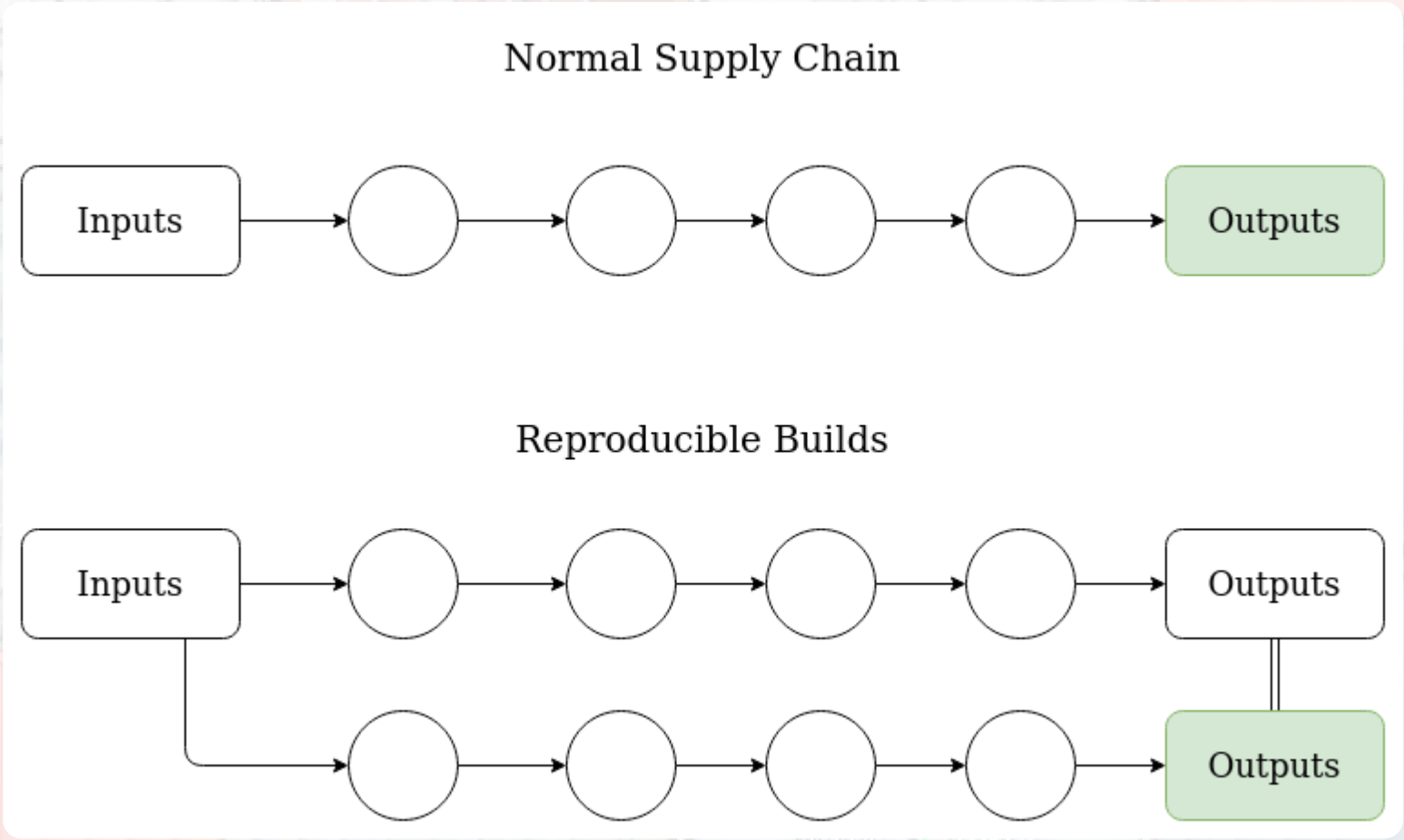
- OCI, stable with new development
- OPA/Gatekeeper, stable

Related Projects / Groups

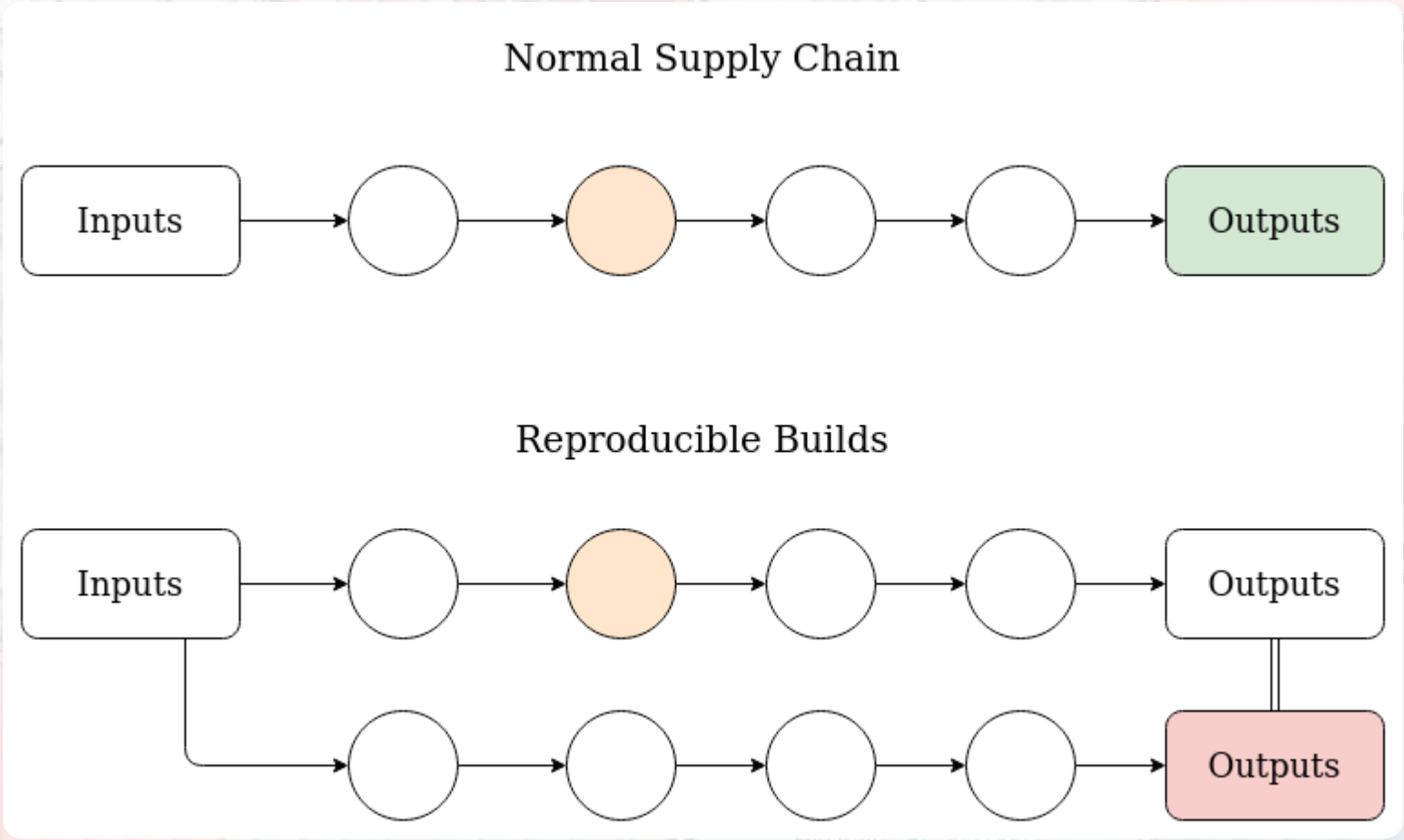
- CNCF Security TAG and Supply Chain WG
- OpenSSF
- SLSA

Reproducible Builds

Hardened Supply Chain vs Reproducible Builds



Hardened Supply Chain vs Reproducible Builds



Reproducible Builds

- reproducible-builds.org
- Nix
- Bazel
- Buildpacks

Wrapping Up

Wrapping Up

- This was not an exhaustive list
- Secure supply chains are a complex process
- Multiple tools need to integrated
- Many of them are still being developed
- Help wanted

Thank You

github.com/sudo-bmitch/presentations

Brandon Mitchell
Twitter: @sudo_bmitch
GitHub: sudo-bmitch