ROE

- Brown Bags are internal
  - Please interrupt/ask for clarification/object
- Send me feedback
  - Improve my communication
  - Improve future brown bags
- Actual lunches encouraged

Build Process: What is it?

Source Code

- Developers write `source code`
- `source code` is often audited for security
- Human readable

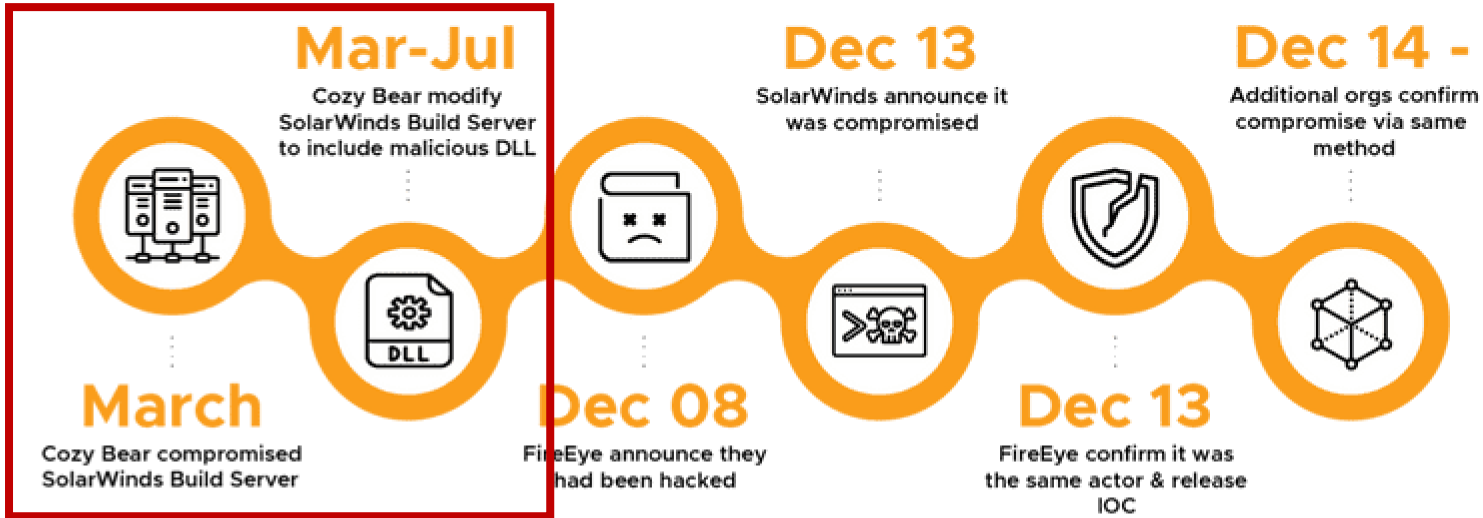
... But `source code` isn’t what `runs` on a computer.

Machine Code (“Executables” or “Binaries”)

- Computer `instructions`
- Built for a specific `processor`
- Not human readable
- Analyzed with `static` or `dynamic` analysis (hard)

Build

- `source code -> executable`
- Language dependent
  - `.c -> .exe / .c -> .dll`
  - `.java -> jar`
- Usually combines many files
  - SolarWinds Orion would have had hundreds of files involved in the build



March
Cozy Bear compromised SolarWinds Build Server

Mar-Jul
Cozy Bear modify SolarWinds Build Server to include malicious DLL

Dec 08
FireEye announce they had been hacked

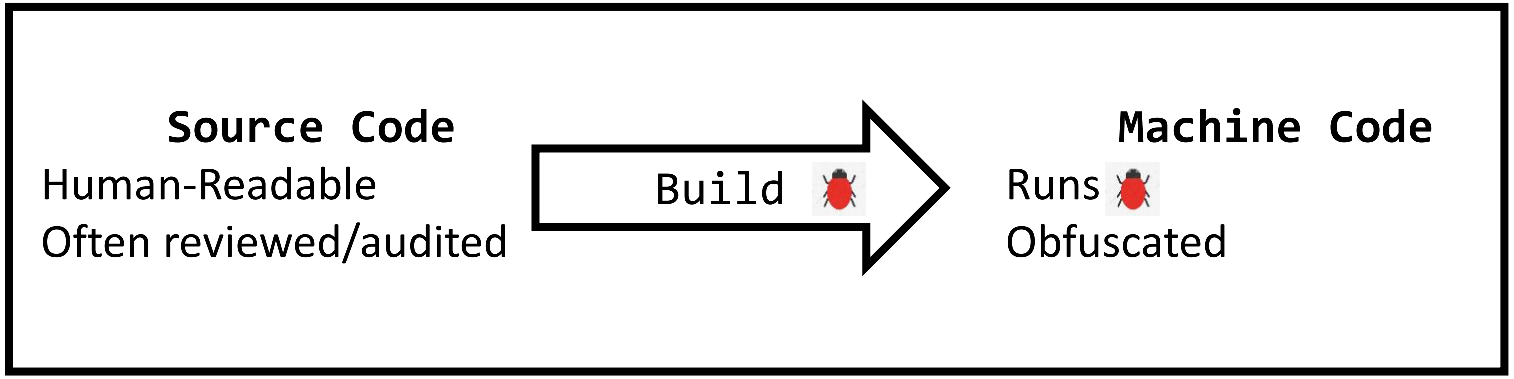
Dec 13
SolarWinds announce it was compromised

Dec 13
FireEye confirm it was the same actor & release IOC

Dec 14 -
Additional orgs confirm compromise via same method

Why attack the build?

- Stealth
  - Devs don’t see the change
  - No change in functionality
  - Pass many standard integrity checks
- Persistence
  - Survive new versions



Source Code

Human-Readable

Often reviewed/audited

Build 🐞

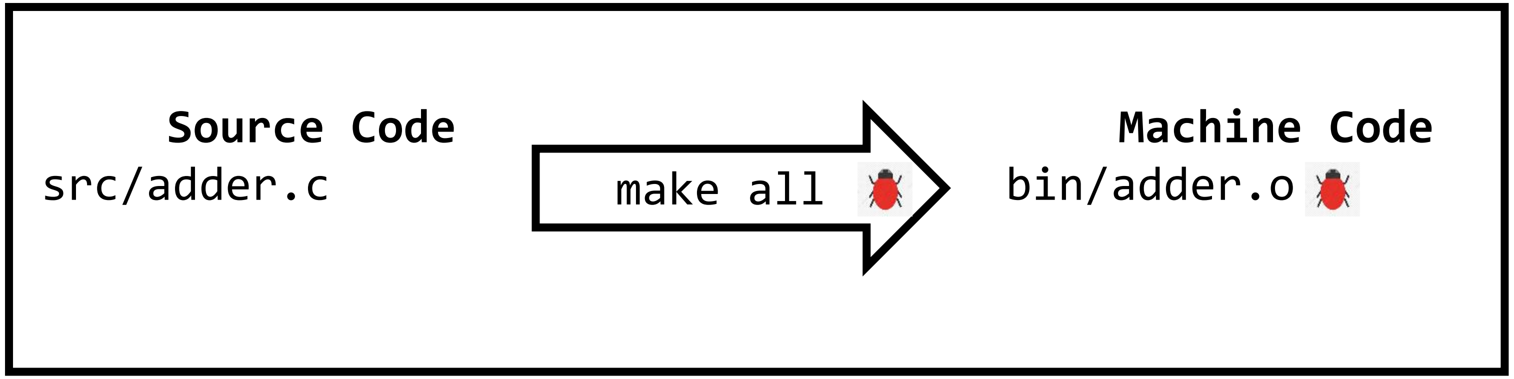
Machine Code

Runs 🐞

Obfuscated

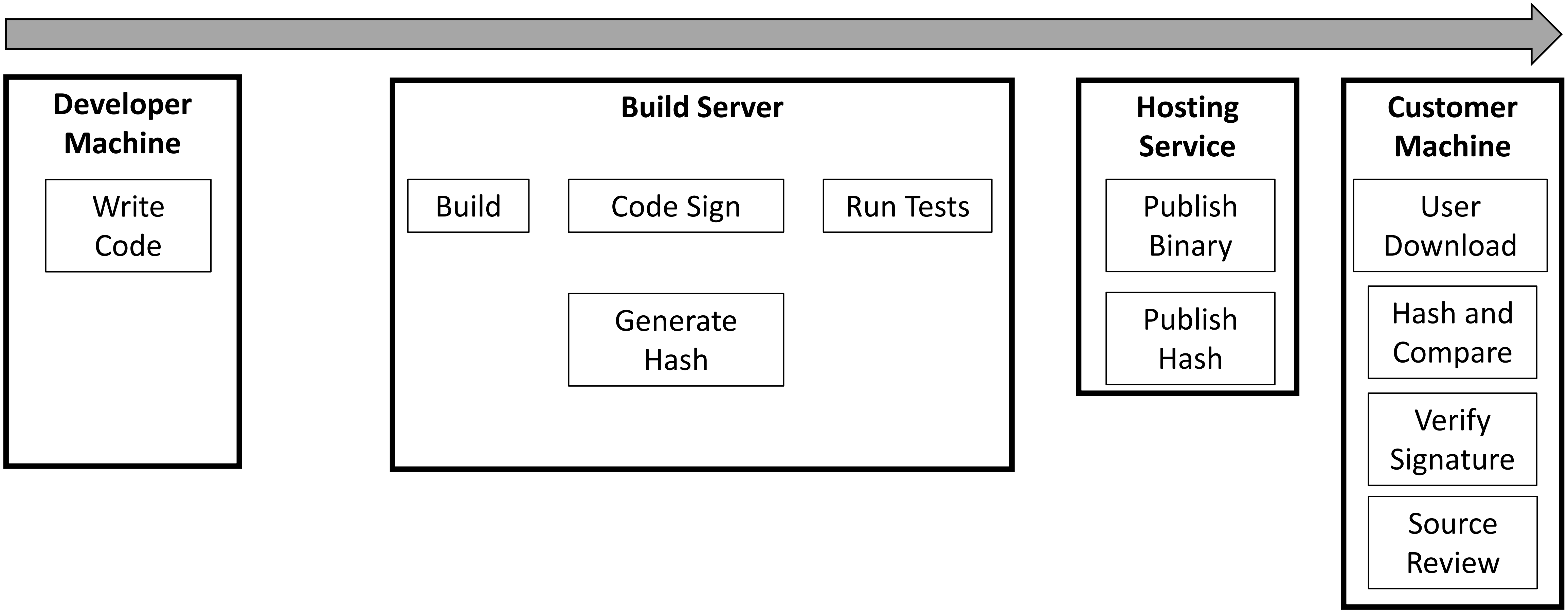
Attack the build

- Stealth
- Persistence



What about…

- Automated tests?
- Code signing?



Developer Machine

Write Code

Build Server

Build

Code Sign

Run Tests

Generate Hash

Hosting Service

Publish Binary

Publish Hash

Customer Machine

User Download

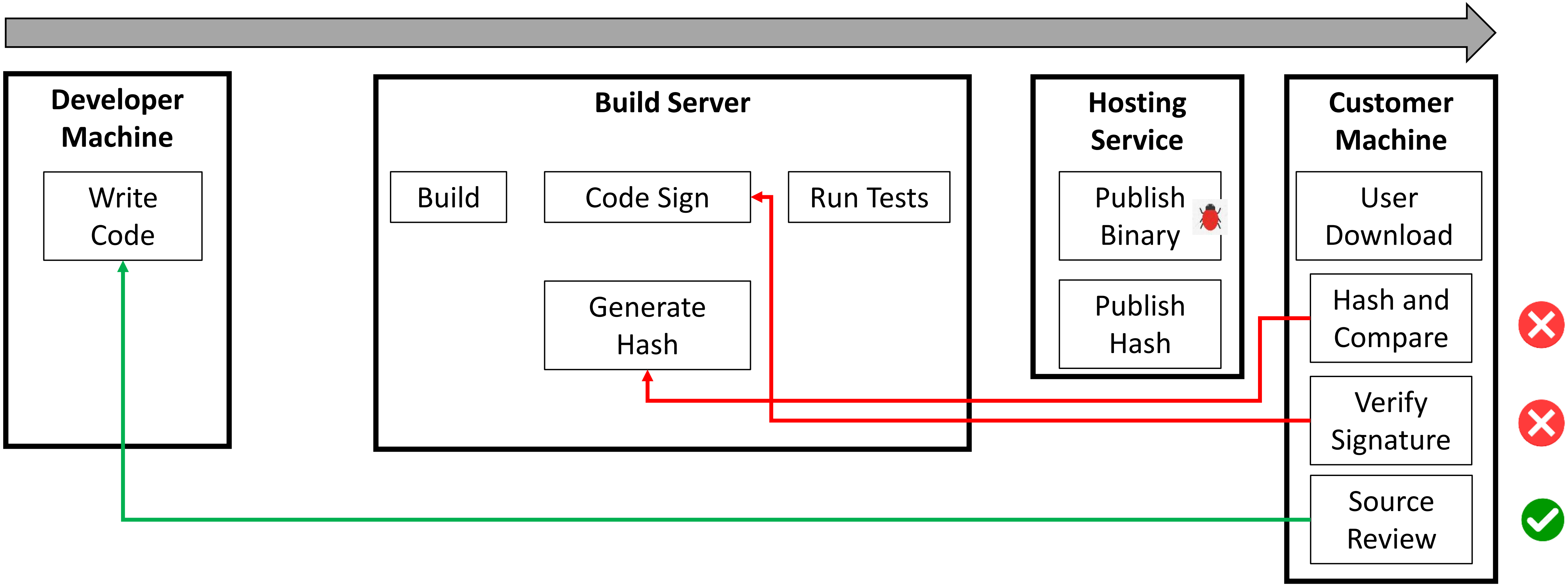
Hash and Compare

Verify Signature

Source Review

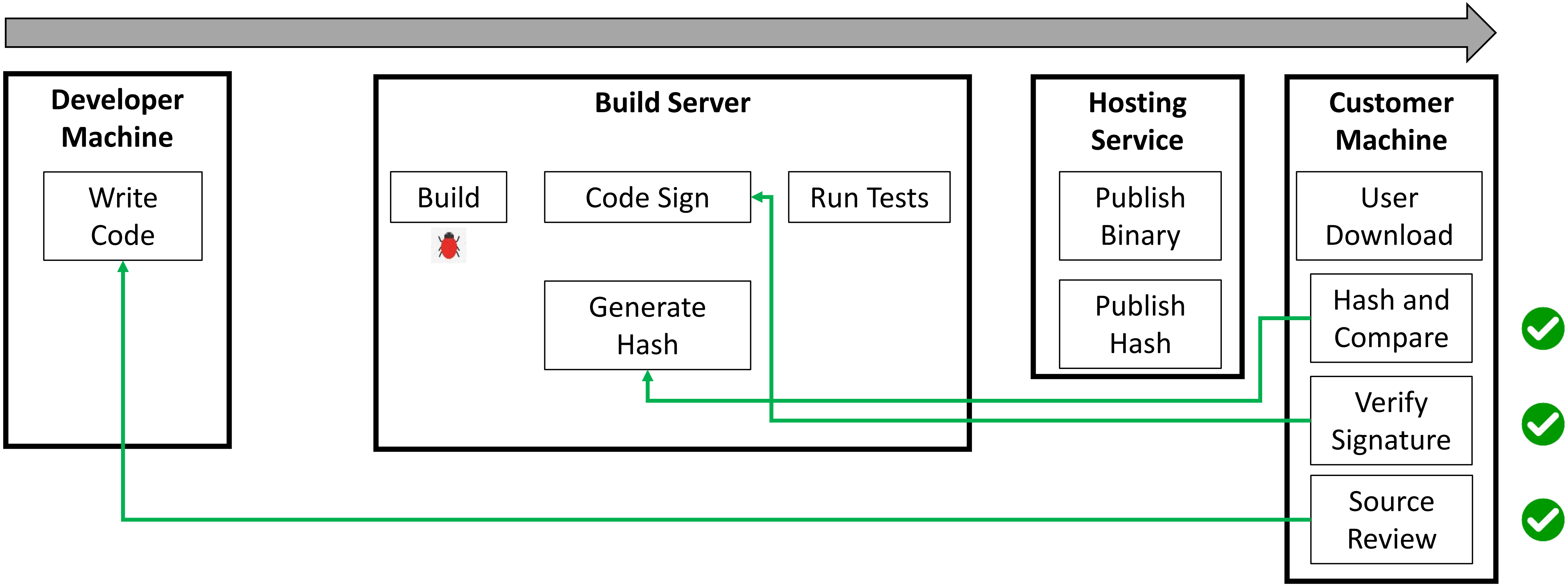
Those protect against a different attack vector

- Still supply chain, but not as subtle



What about…

- Automated tests?
- Code signing?


Developer Machine
Write Code
Build Server
Build
Code Sign
Run Tests
Generate Hash
Hosting Service
Publish Binary
Publish Hash
Customer Machine
User Download
Hash and Compare
Verify Signature
Source Review
✓
✓
✓