Notary v2

redesigning the secure supply chain for containers

Justin Cormack, Steve Lasker, Omar Paul

Who are we?

- Justin Cormack, Engineer, Docker @justincormack
- Steve Lasker, Principal PM Architect, Microsoft @SteveLasker
- Omar Paul, Product Manager, Amazon

supply chain security

why is it important?

Supply Chain Security

- Back in the pre-cloud native days we had hardware firewalls and fixed infrastructure
- If all your infrastructure is code, then anything can be changed with code
- If an attacker can change your code, she can change *anything*
- The "supply chain" of how your code gets to production becomes incredibly important to secure
- Many supply chain attacks, growing recently
  - NotPetya caused billions in damage in 2018
- We want protections in container ecosystem!

Notary

how we got here

The Update Framework

- Notary v1 is an implementation of The Update Framework *adapted* to containers
- The Update Framework was originally designed for securing package repositories, such as apt or npm
- Linux package repositories turn out to have a bunch of security issues
  - serving up fake packages
  - replay attacks – say an old vulnerable package is a new one
  - freeze attack – say there are no updates when there are
  - change dependencies, so extra vulnerable packages installed
  - mix and match dependencies from different dates
  - and more ...
-

Notary history

- Notary v1 was originally a Docker project implementing TUF for registries
- Saw that making better security guarantees with TUF was great opportunity
- Launched 2015
- Donated to CNCF along with the TUF specification in 2017
- However, back when Notary v1 was designed
  - containers in production were kind of new
  - we didn't have a good feel for how exactly to use them
  - a bunch of design mistakes were made, I think
  - but we need security for supply chain now more than ever

Key issues to fix

- Registry native
  - Notary v1 runs as a sidecar on a registry with its own database
  - cannot move signatures between registries
  - need every registry to support this
  - switch to using native registry capabilities
- Usability and usage
  - expectations are high, yet usage of Notary v1 is low
  - lots of usability complaints
- Observability, understandability and debugging
  - hard to debug and see why things fail
- Security model
  - not widely understood, has issues such as TOFU

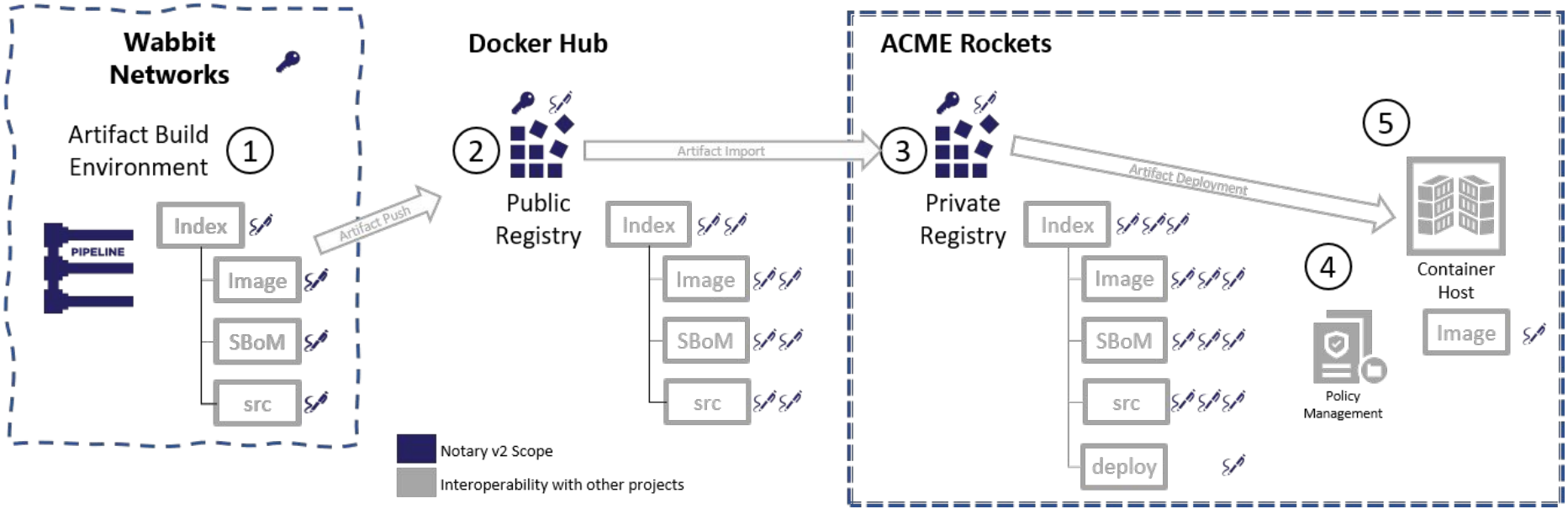
Notary v2

how we are getting there

Notary v2

- Cross registry (and more) team growing consensus to fix these issues
- Docker, Microsoft, Amazon, originally
- Also many others, NYU, IBM, Red Hat, VMware, many more involved
- Started this time last year
- Taken longer than we hoped
  - growing consensus is hard, we are getting there
  - security is a hard thing to design collaboratively
  - Covid
  - however, we are making progress

Notary v2 Scenarios



Registry signatures

building blocks

Signatures in registry

- Want to add generic signature models for registry, not specific to particular use cases
- Long discussion on inline versus detached signatures
- If signatures are part of the content (eg in or linked from manifest) then adding a new signature changes the content hash
- Lots of people want to be able to add signatures without retagging
- Proposing to add to registry APIs a means to find items pointing to an object
- In this way you can look up signatures pointing at an object

Demo

some prototyping

Meta-data services

- Lots of conversation around generic registry apis
- Signatures are a type of meta-data
- We likely want to know more about:
  - Who added the signature
  - What git-commit was the artifact based on
  - When was the signature added
  - What registry was the signature added to
  - …
- A balance of boiling the ocean, vs. a small pond

Next steps
and how you can help?

Next steps

- Prototyping is continuing in 2020
- Key management working group has been busy, consolidating recommendations
- Get agreement on directions from prototypes
- Security analysis from threat models
- A spec will come from the validated prototypes
- Get to production in 2021

- github.com/notaryproject
- Weekly meetings:

  CNCF Calendar www.cncf.io/community/calendar/

  Meeting minutes and recorded videos (link in the calendar)


KEEP CLOUD NATIVE
EVERYWHERE
KubeCon
CloudNativeCon
North America 2020
Virtual
HELM
KV