KubeCon | CloudNativeCon

Europe 2019

Deep Dive: TUF / Notary (feat. in-toto)

Justin Cappos
Professor, NYU

Lukas Pühringer
Developer, NYU

There Is An Attack Vector...

Many Victims...

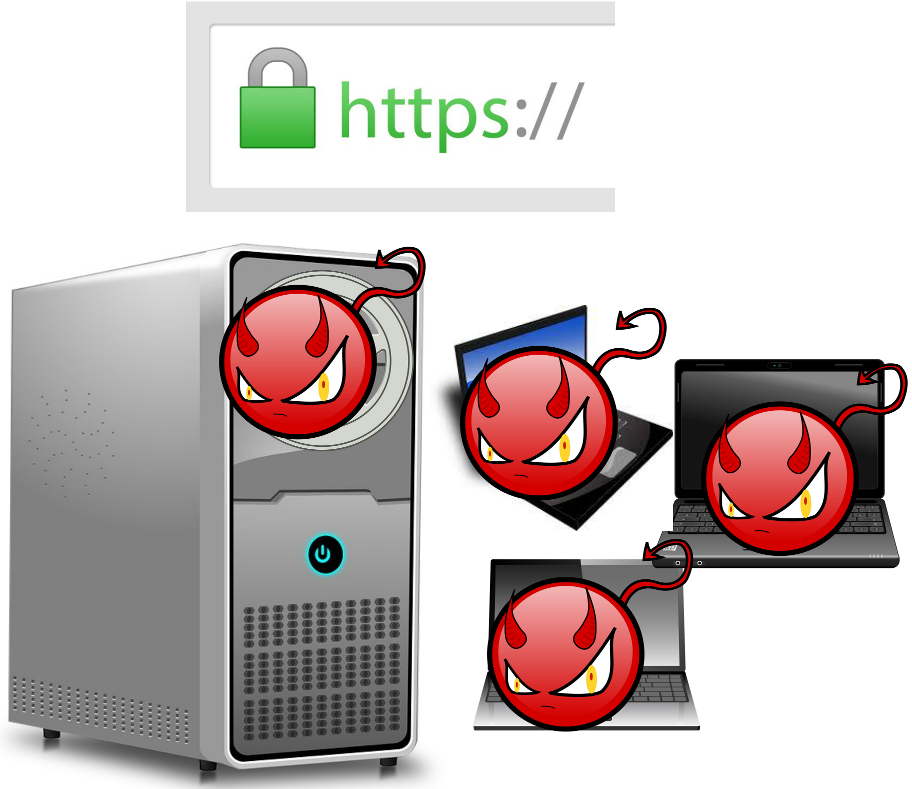
Powered By
GNU/Linux
CentOS
Adobe
fedora
Ruby
Powered by
gentoo
GNU/Linux
OPERA
software
Apache
debian
Google
sourceforge
Windows
GitHub

Easy?

Does crypto just work?

Easy?

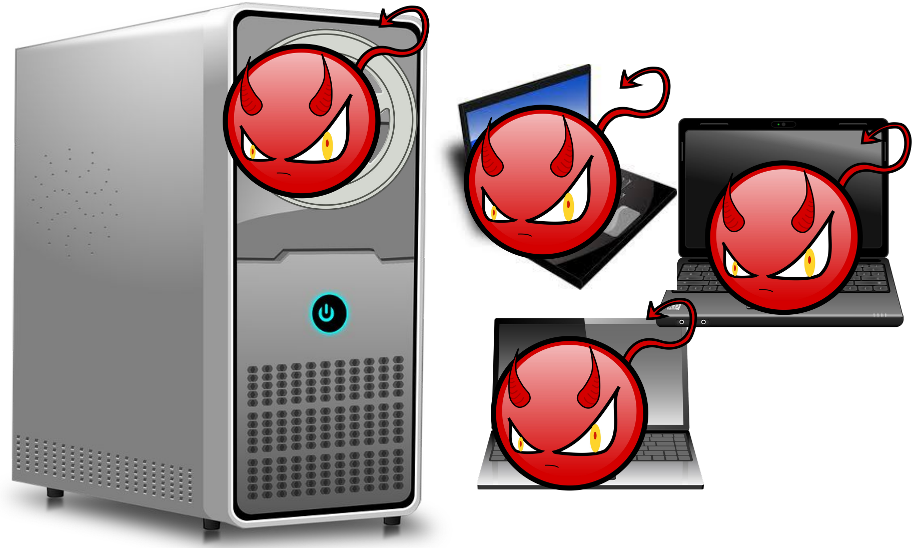
Does a simple solution work?



Easy?

Does a simple solution work?

GnuPG



Easy?

~~Easy?~~

~~Easy?~~

Possible?

Enter TUF!

Goals:

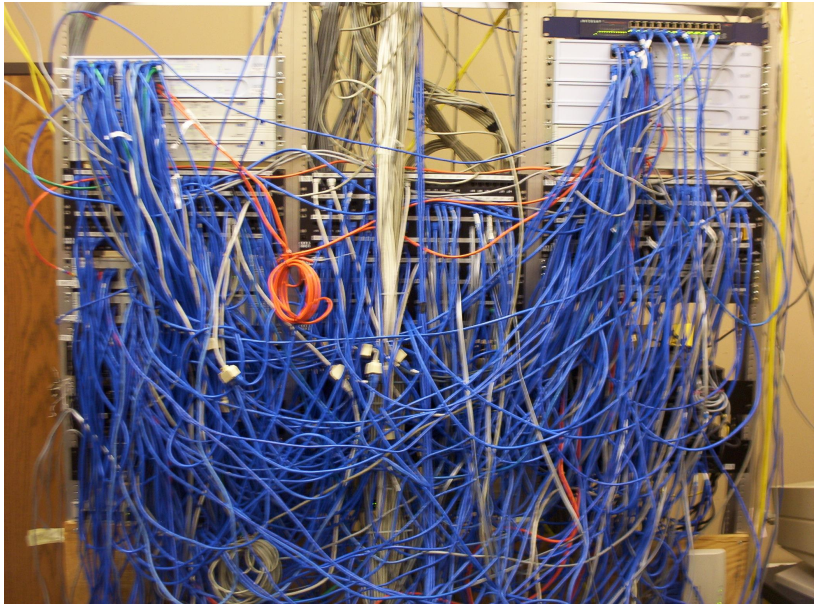
- compromise resilience

DANGER
.DEB
.RPM

Enter TUF!

Goals:

- compromise resilience
- support, don't judge!



TUF Design

Responsibility Separation

Multi-signature Trust

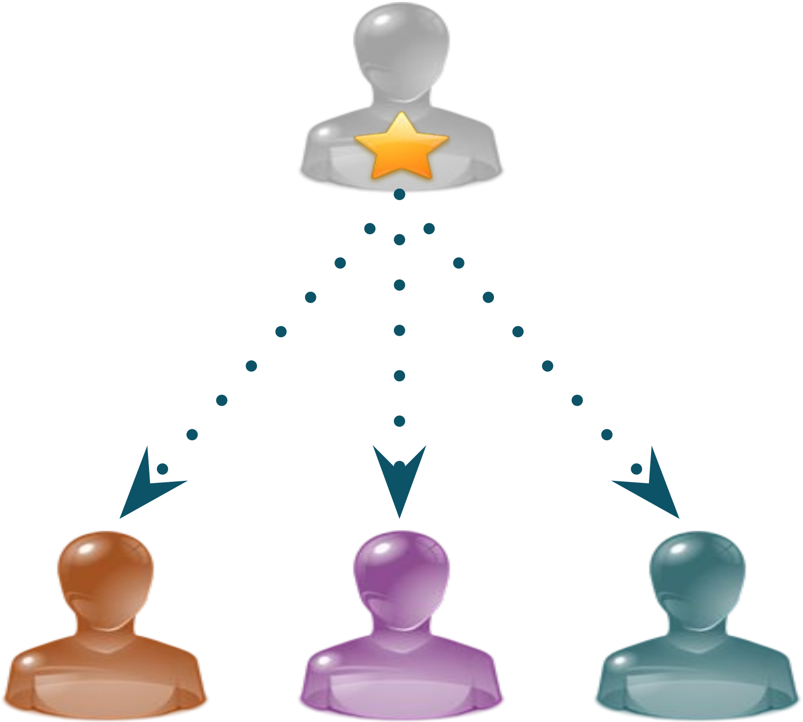
Explicit and Implicit Revocation

Minimize Individual Key and Role Risk

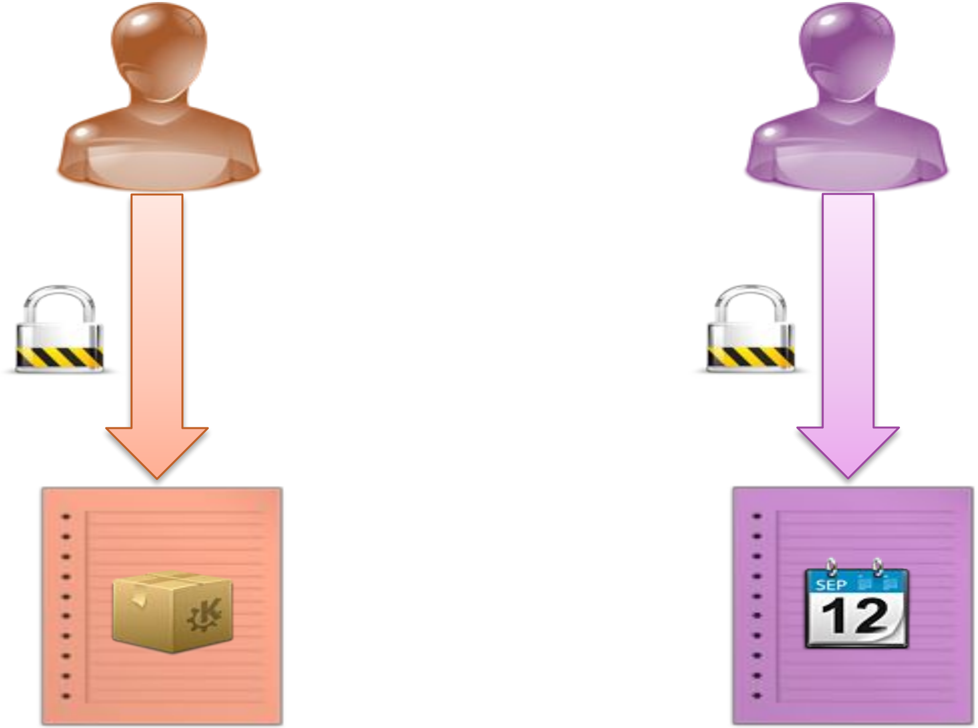
TUF Design Principles

Responsibility Separation

Delegate roles to divide responsibilities



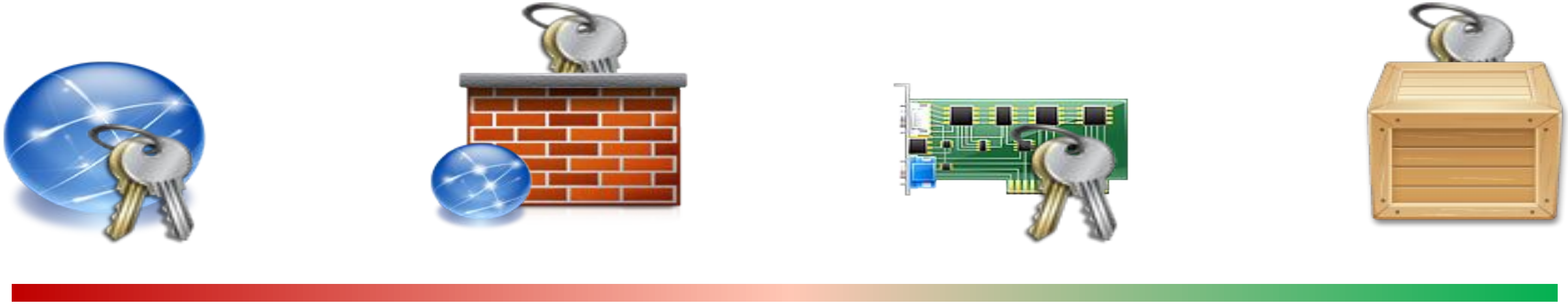
Responsibility Separation



Content

Timeliness

TUF Design Principles



Expected Damage
~=
Probability×Impact

Minimize Individual Key and Role Risk

Minimize Expected Damage

High-impact role? → Highly-secure keys
(e.g. root)

Online keys? → Low-impact role
(e.g. timeliness)

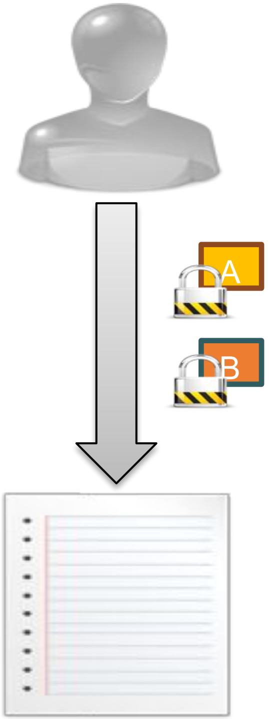
TUF Design Principles

Multi-signature Trust

(*t*, *n*) threshold required for trust

Multi-signature Trust

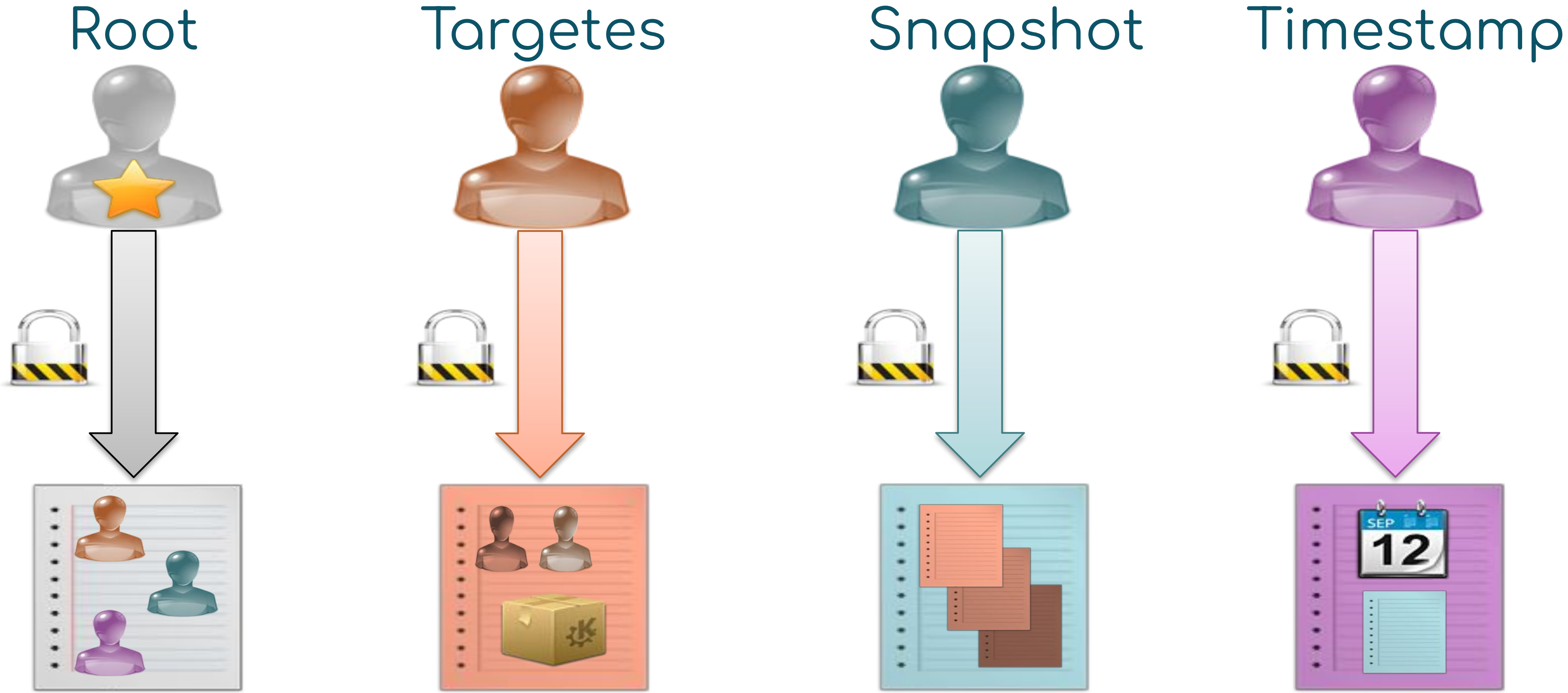
Signature threshold:
Two signatures



No risk to clients.

TUF Design Principles

Explicit and Implicit Revocation



Root

Targetes

Snapshot

Timestamp

Standardized / Used

administrators project developers packages

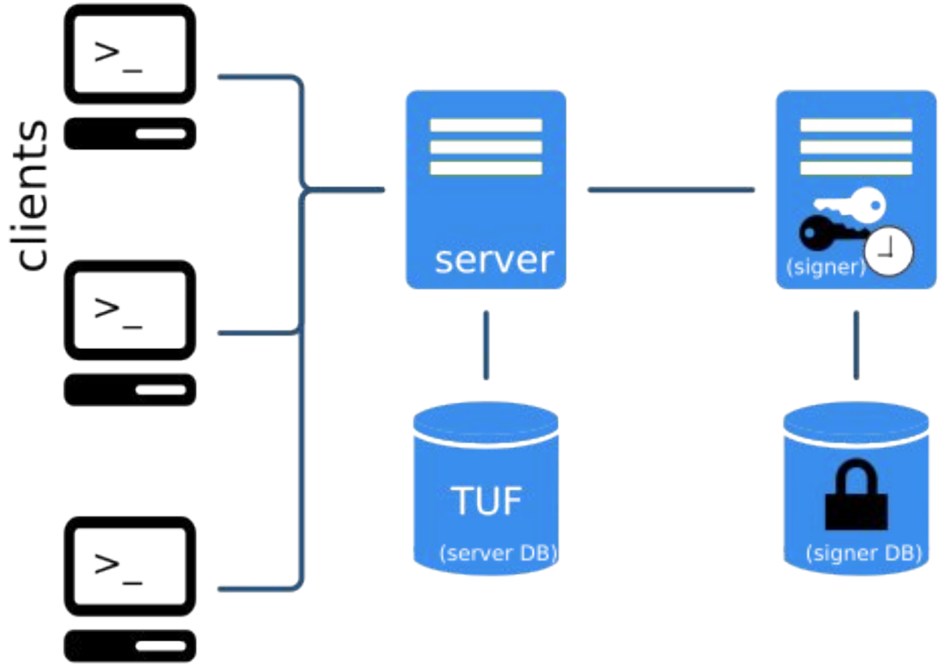
What About Docker?

Is docker vulnerable to these kinds of attacks?

A long time ago
(in technology terms)...

Signing Docker Images

Docker content trust integrates TUF in order to sign and protect Docker manifests.



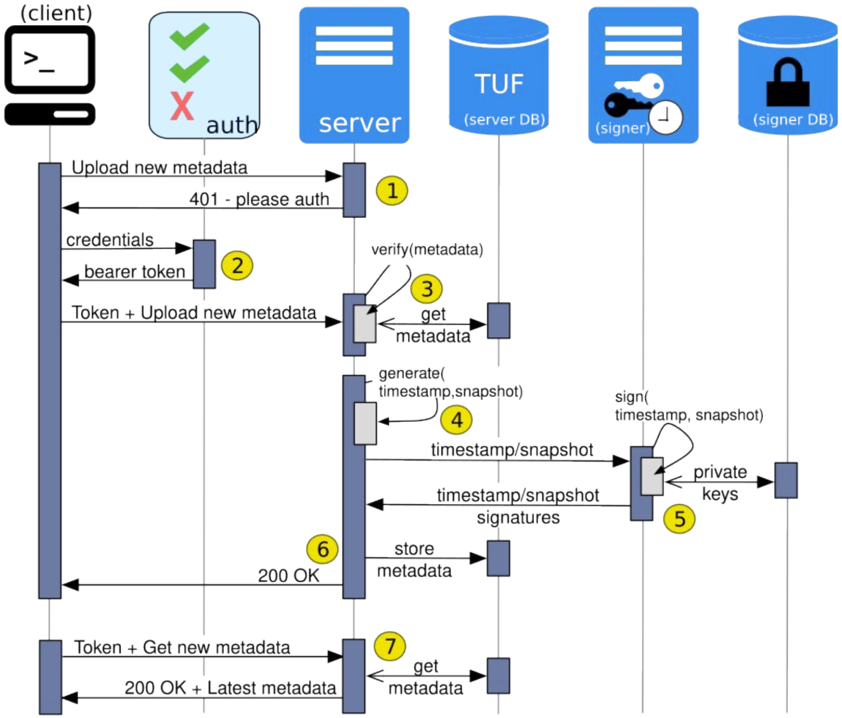
Role Breakdown

The TUF specific roles are as follows

- Root: user
- Targets: user
- Snapshot: content-trust*
- Timestamp: content-trust

How To Sign

In order to sign the metadata, the docker cli tool will talk to the content trust server before pushing to the registry.



Docker Today

Key Compromise

Key compromised	Malicious content	Rollback, freeze, mix and match	Denial of service
Timestamp (online)	No	No	Limited
Snapshot (online*)	No	No	Limited
Targets (offline)	No (*)	No (*)	Limited
Root (offline)	Yes	Yes	Yes

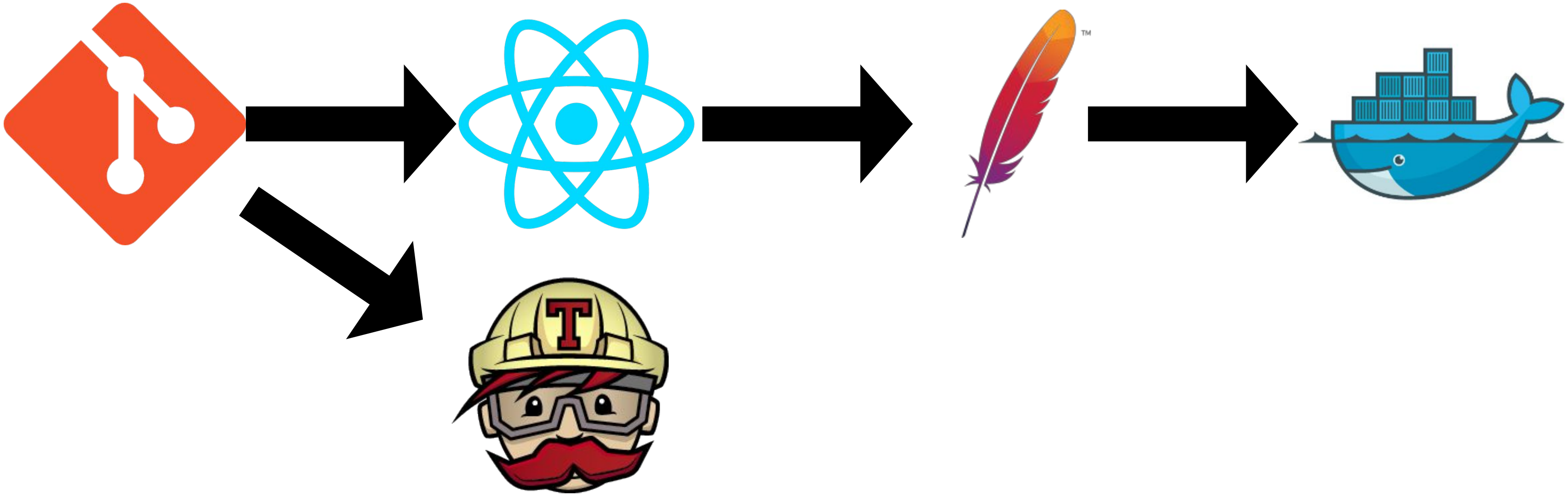
Key Compromise

Key compromised	Malicious content	Rollback, freeze, mix and match	Denial of service
Timestamp (online)	No	No	Limited
Snapshot (online*)	No	No	Limited
Targets (offline)	No (*)	No (*)	Limited
Root (offline)	Yes	Yes	Yes

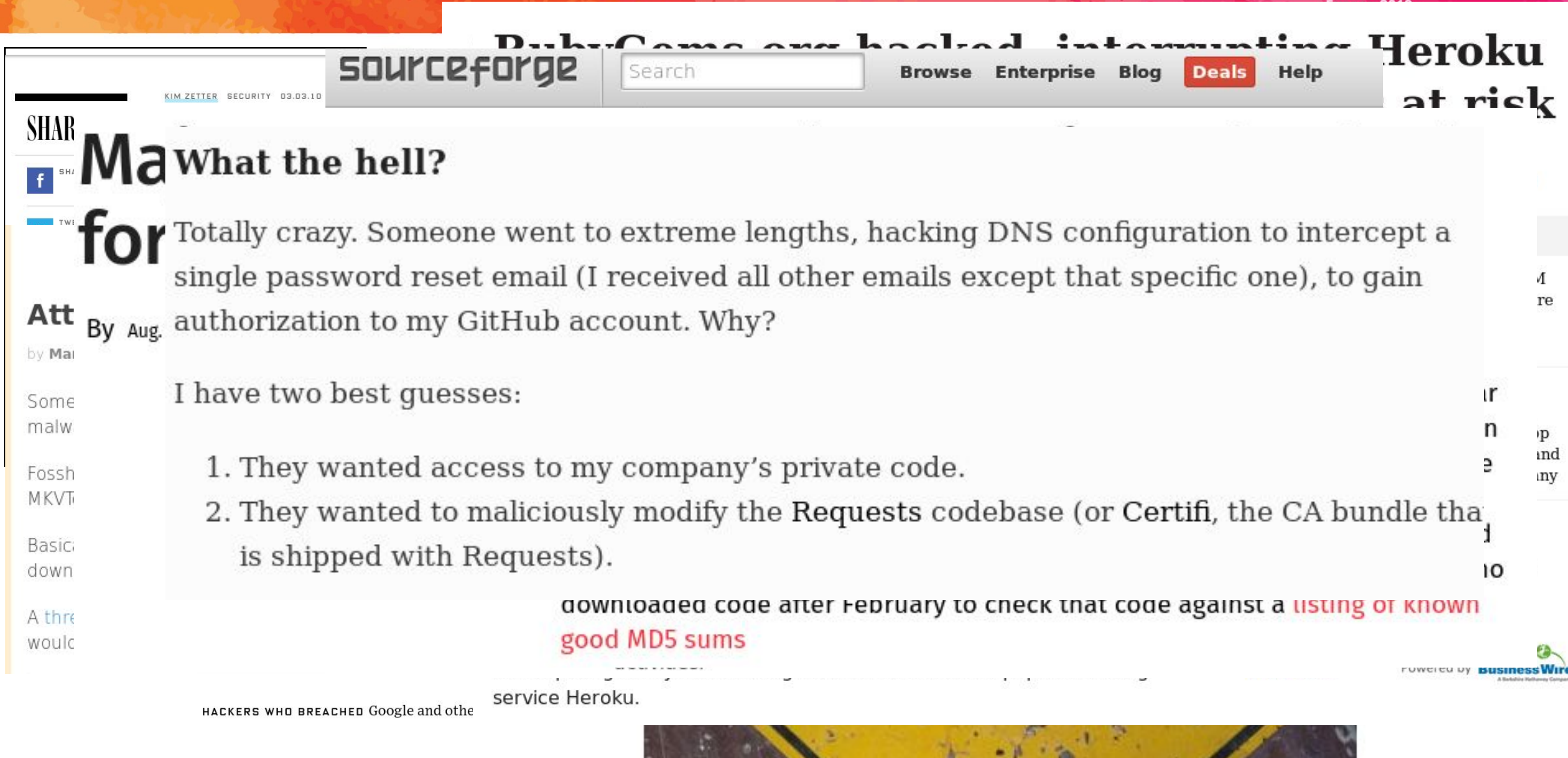
Beyond TUF

Things TUF does not protect against…

A Software Supply Chain



Supply Chain Compromise



What the hell?

Totally crazy. Someone went to extreme lengths, hacking DNS configuration to intercept a single password reset email (I received all other emails except that specific one), to gain authorization to my GitHub account. Why?

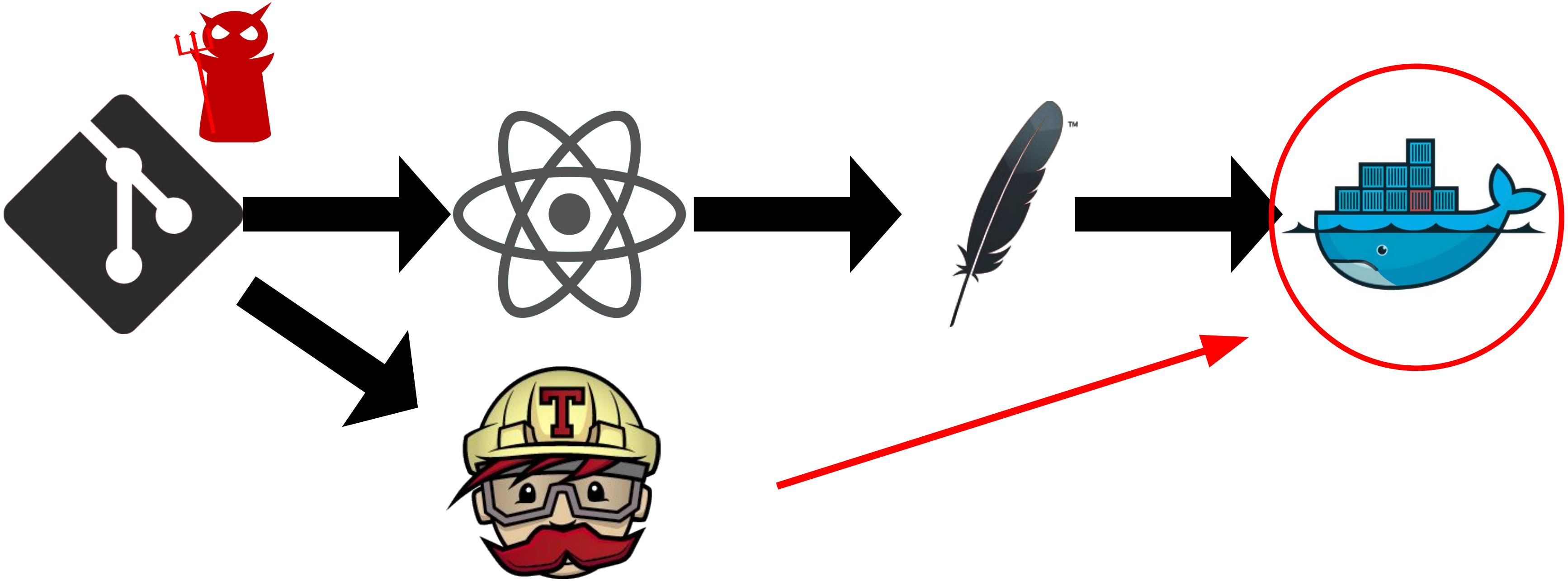
I have two best guesses:

1. They wanted access to my company's private code.
2. They wanted to maliciously modify the Requests codebase (or Certifi, the CA bundle tha is shipped with Requests).

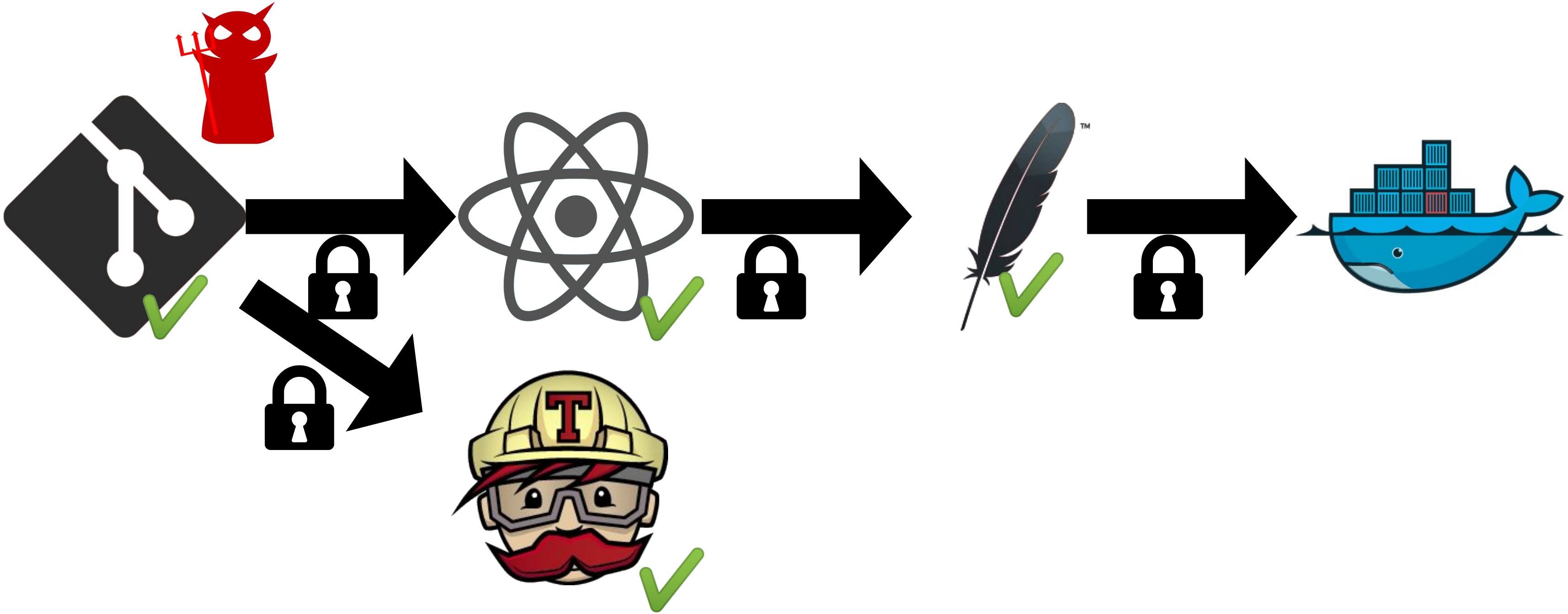
downloaded code after February to check that code against a listing of known good MD5 sums

service Heroku.

HACKERS WHO BREACHED Google and othe

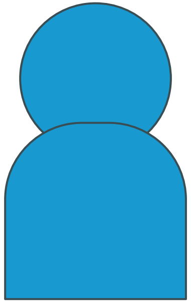


Introducing in-toto

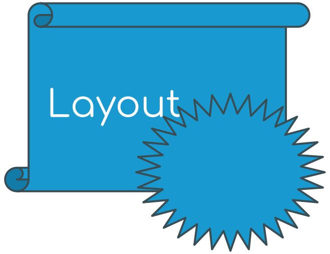


Much like TUF in-toto uses...

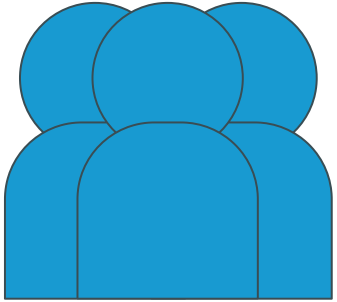
Project owner



Defines what needs to be done

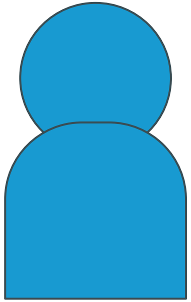


Functionaries

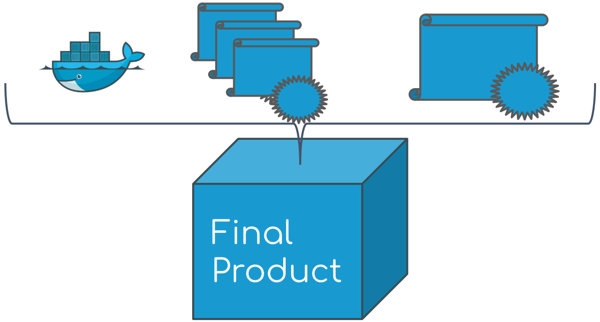


Perform steps, provide evidence

End User



Verify



Conclusion

- Securing software distribution, etc. is hard
  - Use TUF -- standardized, widely used, security audited…
- Docker Content Trust provides strong guarantees for Docker images
- in-toto will further improve security

TUF Standardization (TAPs)

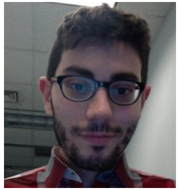
- TAP 3 -- multi-role signatures
    - Lets one have ‘unequal’ quorums
- TAP 4 -- pinning repository keys
    - Control the root of trust for parts of the namespace
    - Root role compromise != game over
- TAP 5 -- specify URLs in root files
    - Makes it easy to change the repo location
- TAP 6 -- version numbers in root metadata
- TAP 7 -- TUF conformance testing

Discuss with us, then submit (TAP 1/2)

Thank you!

KubeCon | CloudNativeCon

Europe 2019



https://theupdateframework.com

https://in-toto.io