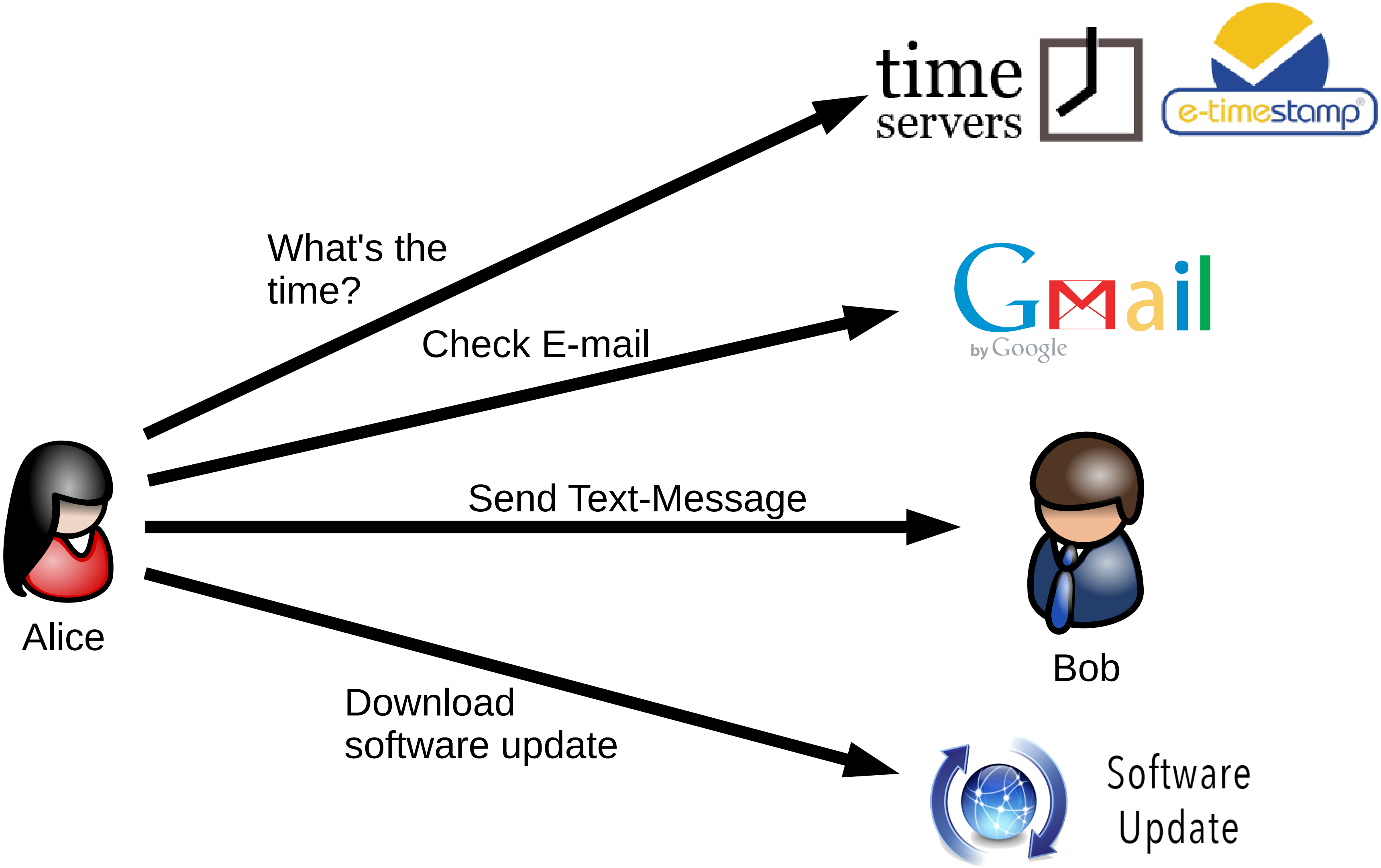
Decentralizing Authorities (such as time services)

http://datatracker.ietf.org/doc/draft-ford-trans-witness/
http://arxiv.org/abs/1503.08768
https://github.com/DeDiS/cothority

Ewa Syta, Iulia Tamas, Dylan Visher, David Wolinsky – **Yale University**
Bryan Ford, Linus Gasser, Nicolas Gailly – **Swiss Federal Institute of Technology (EPFL)**

IETF – November 2, 2015

The Internet needs authorities



What's the time?

Check E-mail

Send Text-Message

Download software update

The Internet needs authorities

Respect my Authoritah!

?

Alice

What is:

- The current time?
- Gmail's SSL public key?
- Bob's IM public key?
- Latest version of App?

time servers

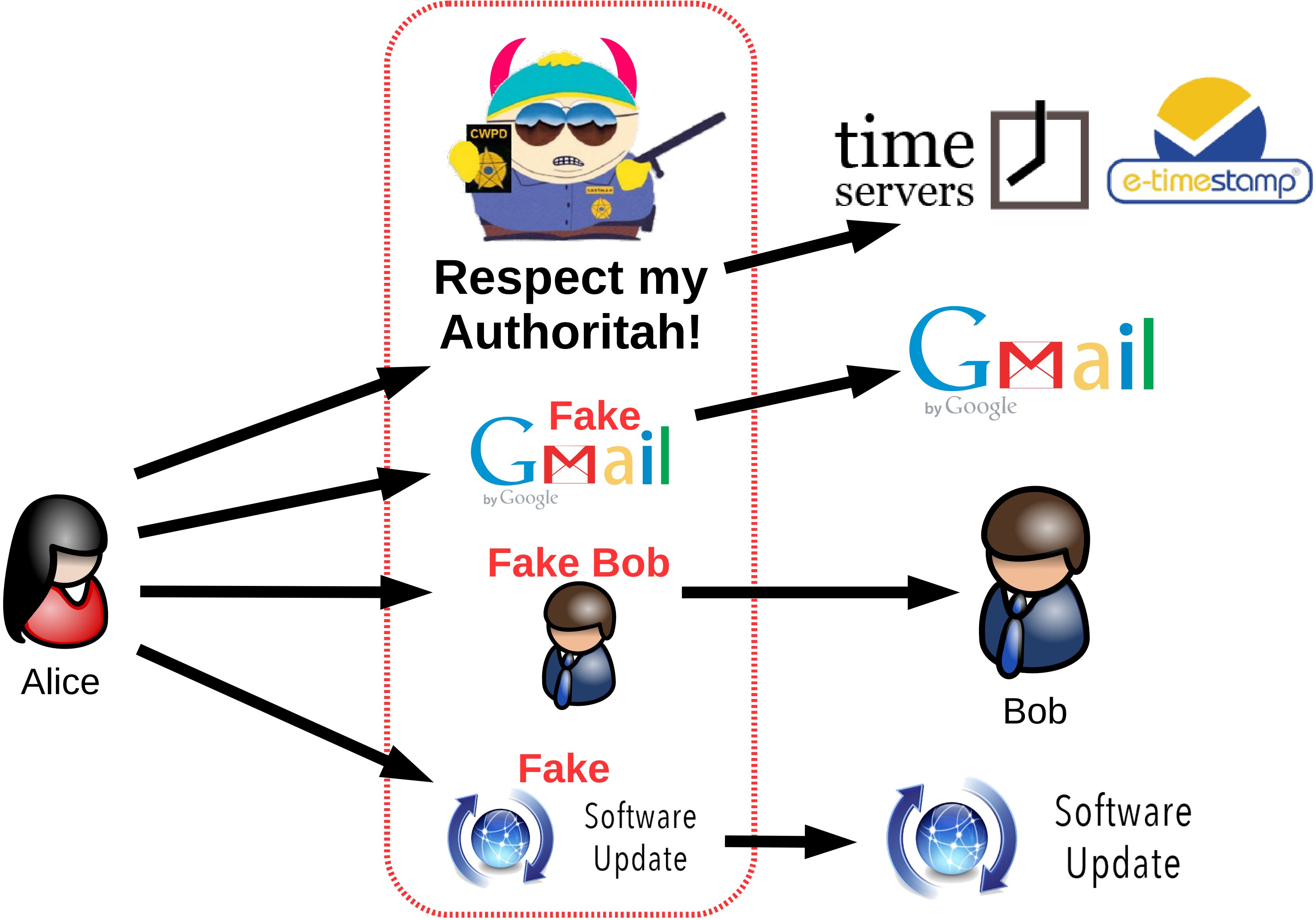
e-timestamp

Gmail by Google

Bob

Software Update

Authorities can be compromised



Respect my Authoritah!

Fake Gmail

Fake Bob

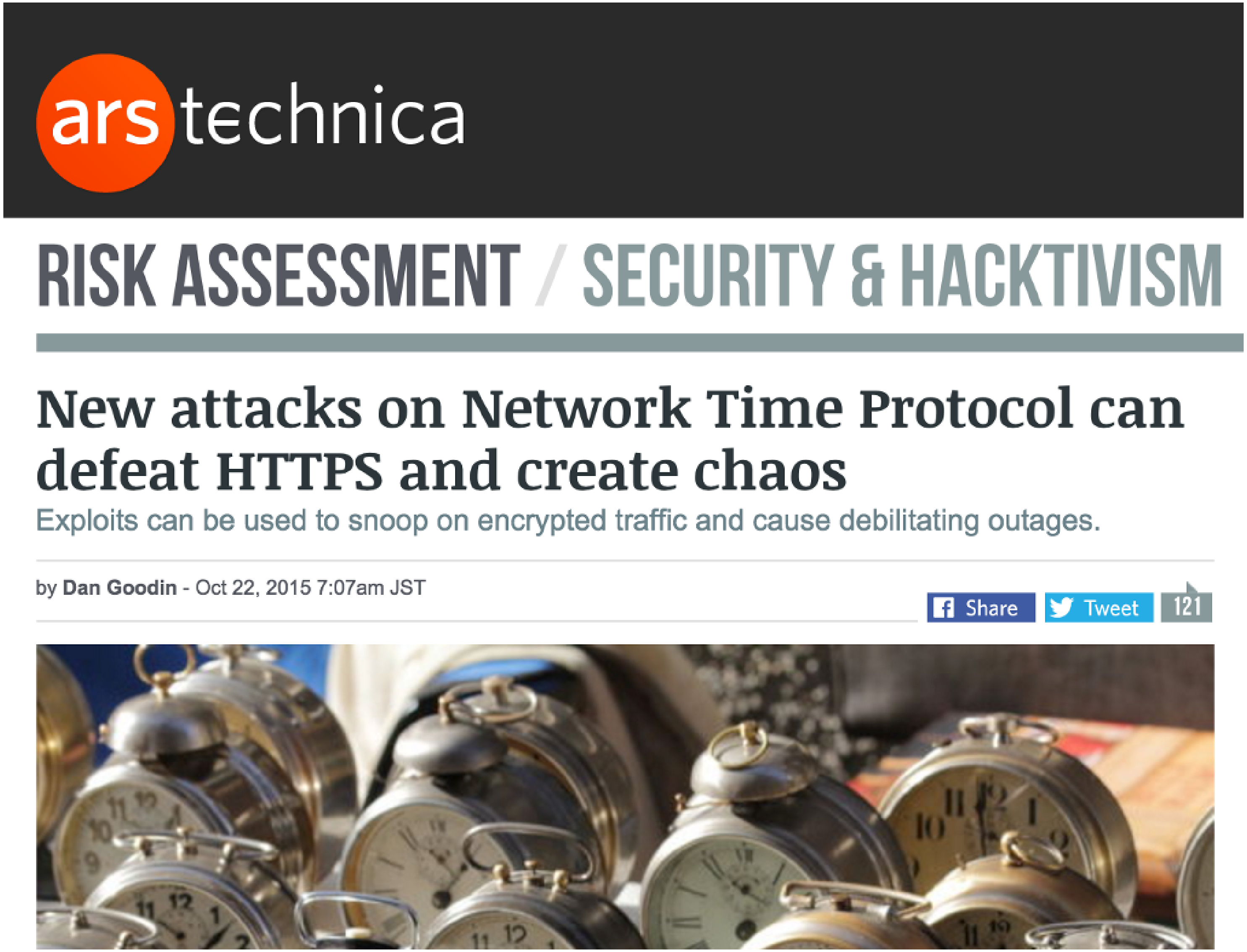
Fake Software Update

Alice

Bob

Software Update

Including time servers



ars technica

RISK ASSESSMENT / SECURITY & HACKTIVISM

New attacks on Network Time Protocol can defeat HTTPS and create chaos

Exploits can be used to snoop on encrypted traffic and cause debilitating outages.

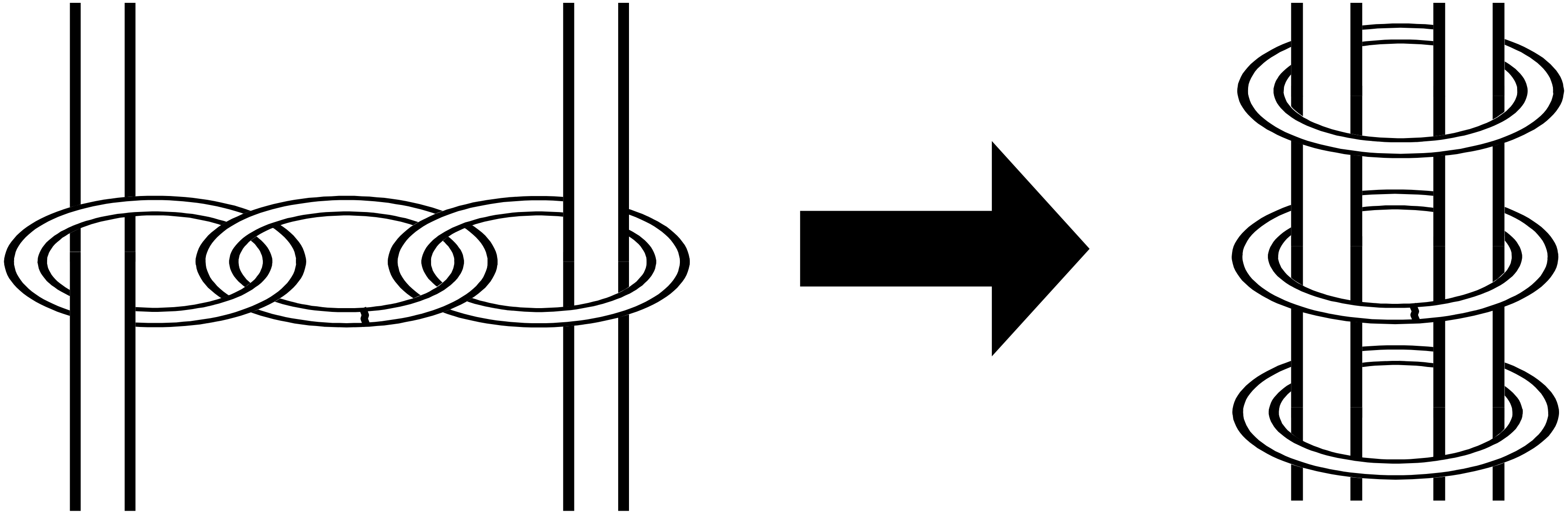
by **Dan Goodin** - Oct 22, 2015 7:07am JST

Challenge: Decentralize Authorities

Split important authority functions across multiple participants (preferably independent)

- So authority isn't compromised unless multiple participants compromised

From **weakest-link** to **strongest-link** security

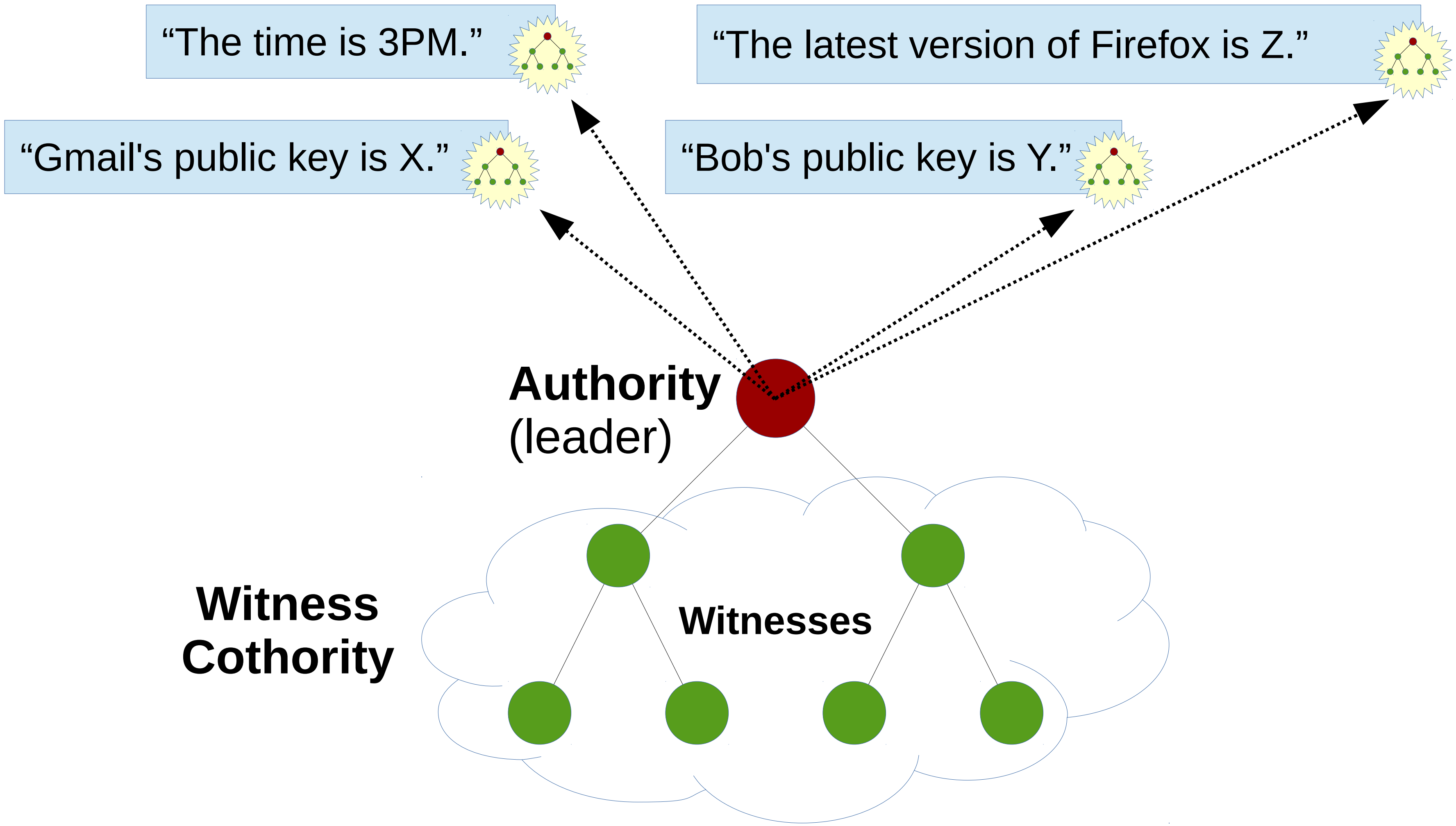


Goal: Secure Time Bootstrap

Enable freshly-booted devices to get a secure, **coarse-grained** notion of current time on start

- Protect against "retrograde time" attacks
  - Even by powerful MITM-capable adversaries
  - Even if adversary has control of one or a few NTP servers' private keys
- Need not be ms-accurate, just guarantee time is not "way off"
  - e.g., not hours or days wrong
- Prevent replay-based "upgrade" of a device to old software version with now-known exploit

CoSi: Scalable Collective Signing



“The time is 3PM.”

“Gmail's public key is X.”

“The latest version of Firefox is Z.”

“Bob's public key is Y.”

Authority
(leader)

Witness Cothority

Witnesses

A Timestamping Cothority

Like classic **digital timestamp** services, only decentralized.

- Each round (e.g., 10 secs):

  1) Each server collects hashes, nonces to timestamp

  2) Each server aggregates hashes into Merkle tree

  3) Servers aggregate local trees into one global tree

  4) Servers collectively sign root of global tree

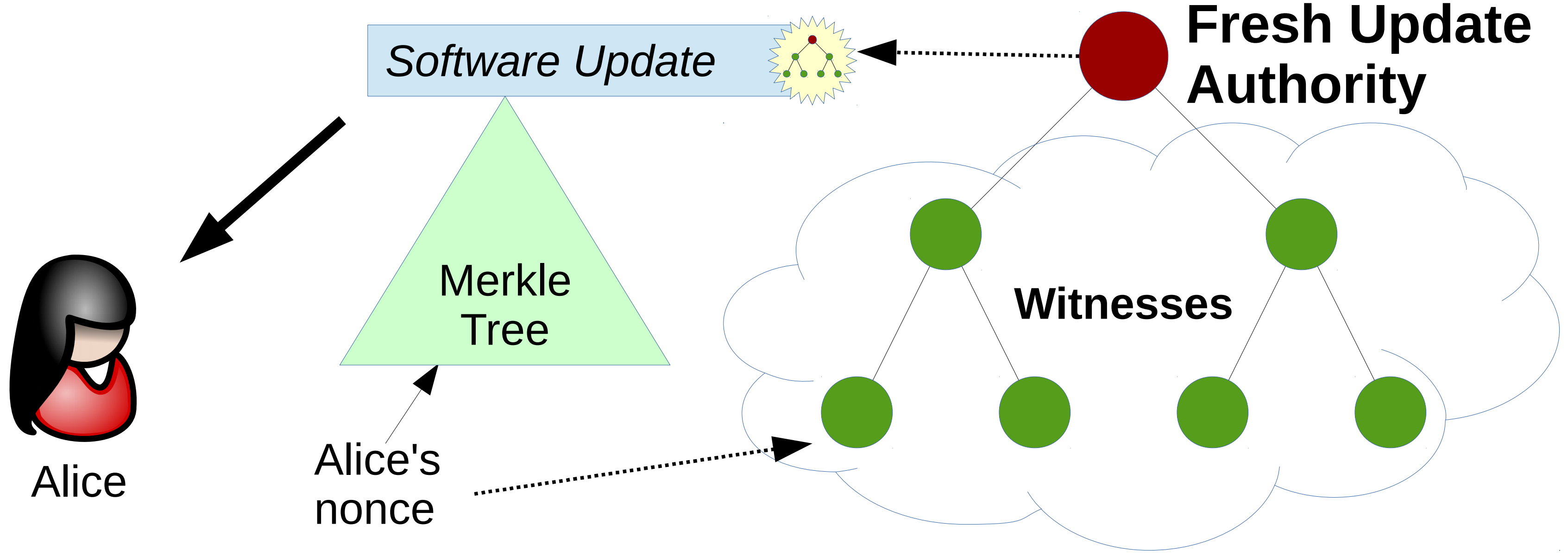
  5) Server give signed root + inclusion proof to clients

- Clients verify signature + Merkle inclusion proof

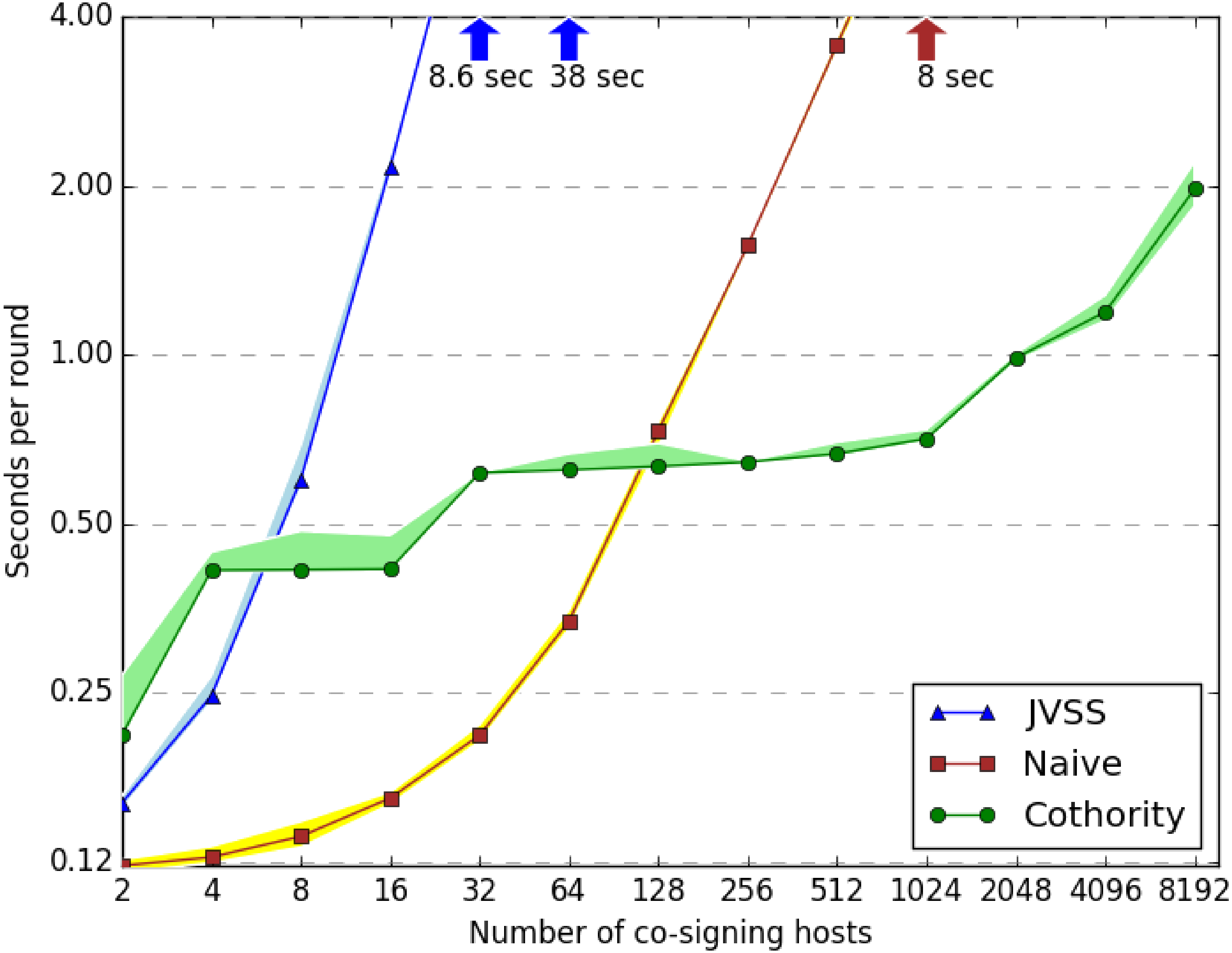
Verifiably Fresh Software Updates

Alice accepts only updates with fresh timestamp:

- Knows update can't be an outdated version: tree contains inclusion proof of *her* nonce
- Knows update can't have targeted backdoor: witness cothority ensures *many* parties saw it



Collective signing performance


Seconds per round
8.6 sec
38 sec
8 sec
Number of co-signing hosts
JVSS
Naive
Cothority