Genuine onion: Simple, Fast, Flexible, and Cheap Website Authentication

Paul Syverson

U.S. Naval Research Laboratory

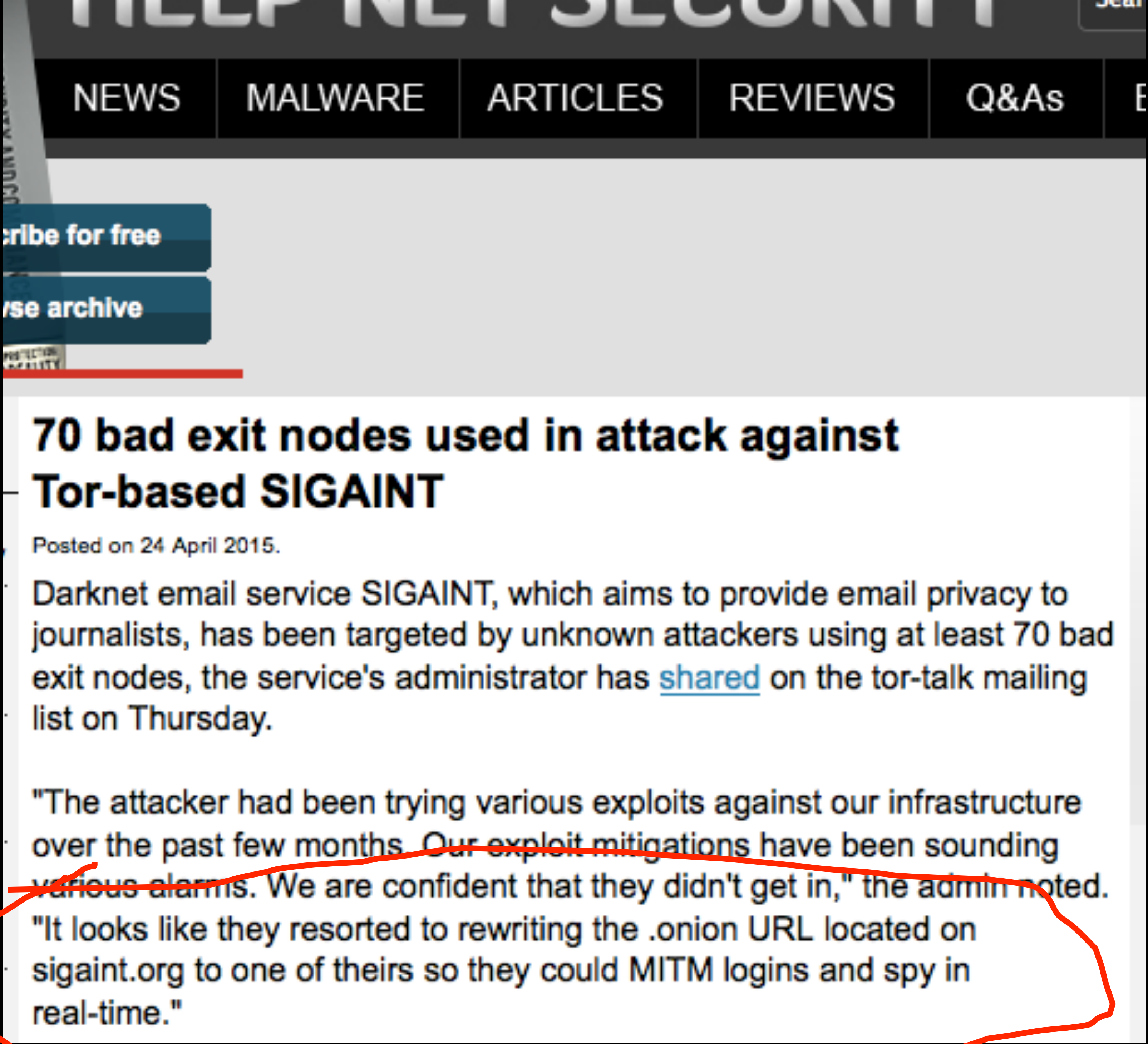
joint work with

Griffin Boyce *Open Internet Tools Project*

IEEE Web 2.0 Security and Privacy Workshop
May 21, 2015

Onionsites: Not just for confidentiality of server network location

- Also useful for site integrity and authentication



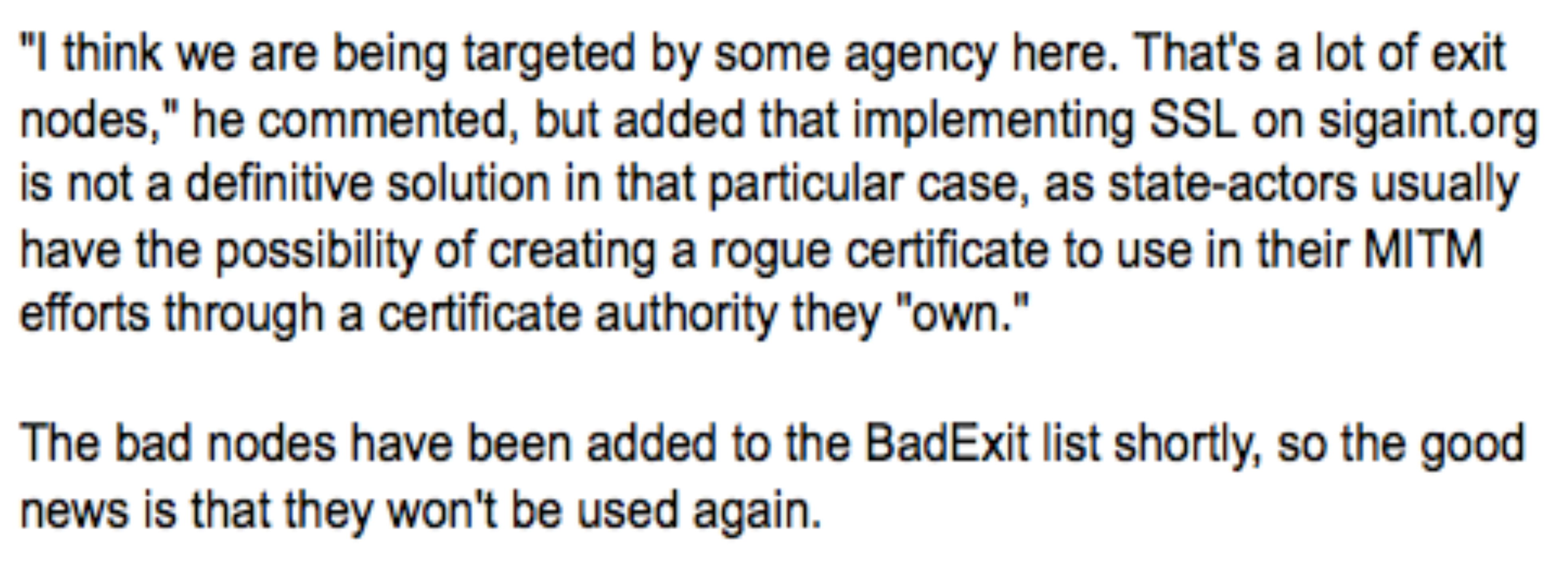
70 bad exit nodes used in attack against Tor-based SIGAINT

Posted on 24 April 2015.

Darknet email service SIGAINT, which aims to provide email privacy to journalists, has been targeted by unknown attackers using at least 70 bad exit nodes, the service's administrator has shared on the tor-talk mailing list on Thursday.

"The attacker had been trying various exploits against our infrastructure over the past few months. Our exploit mitigations have been sounding various alarms. We are confident that they didn't get in," the admin noted. "It looks like they resorted to rewriting the .onion URL located on sigaint.org to one of theirs so they could MITM logins and spy in real-time."

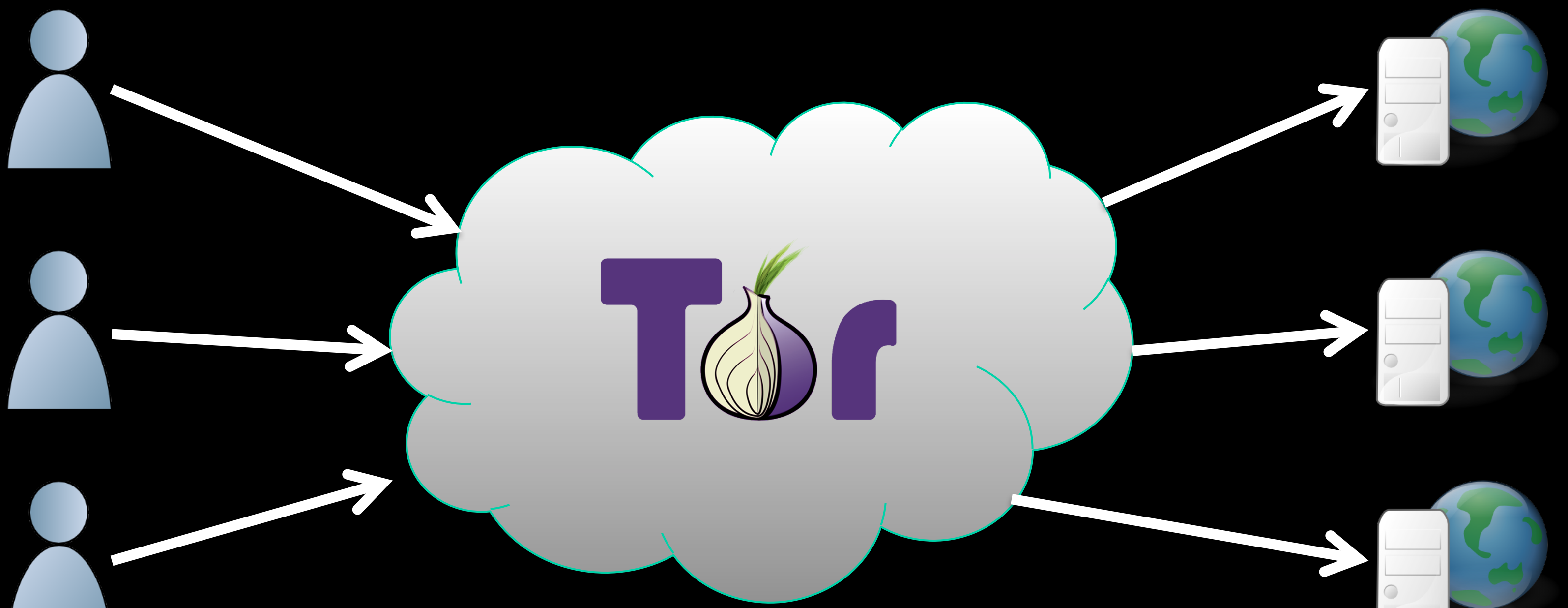
Why didn’t they use SSL Certs?



"I think we are being targeted by some agency here. That's a lot of exit nodes," he commented, but added that implementing SSL on sigaint.org is not a definitive solution in that particular case, as state-actors usually have the possibility of creating a rogue certificate to use in their MITM efforts through a certificate authority they "own."

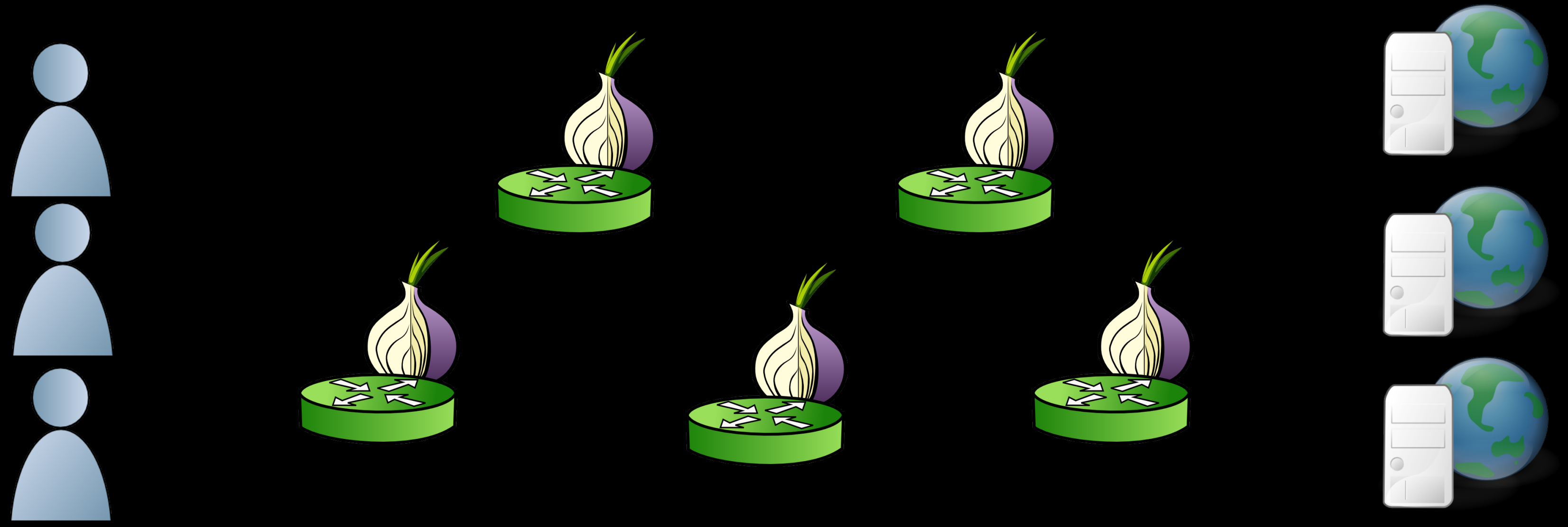
The bad nodes have been added to the BadExit list shortly, so the good news is that they won't be used again.

What is Tor?



Tor is a system for traffic-secure communication.

Background: Onion Routing

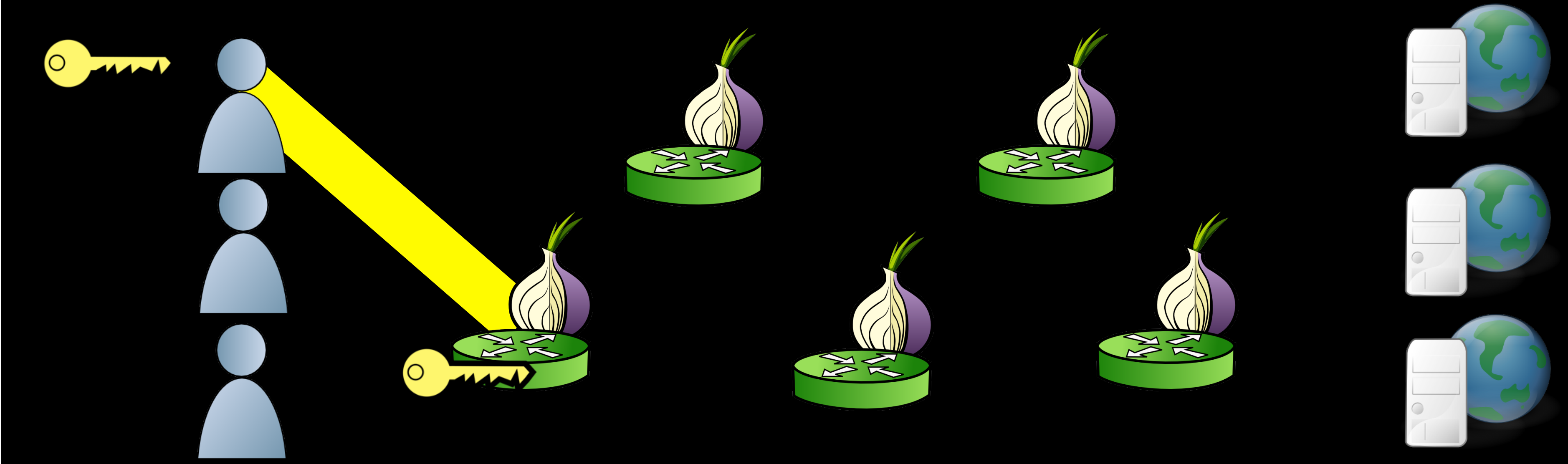


Users

Onion Routers

Destinations

Background: Onion Routing

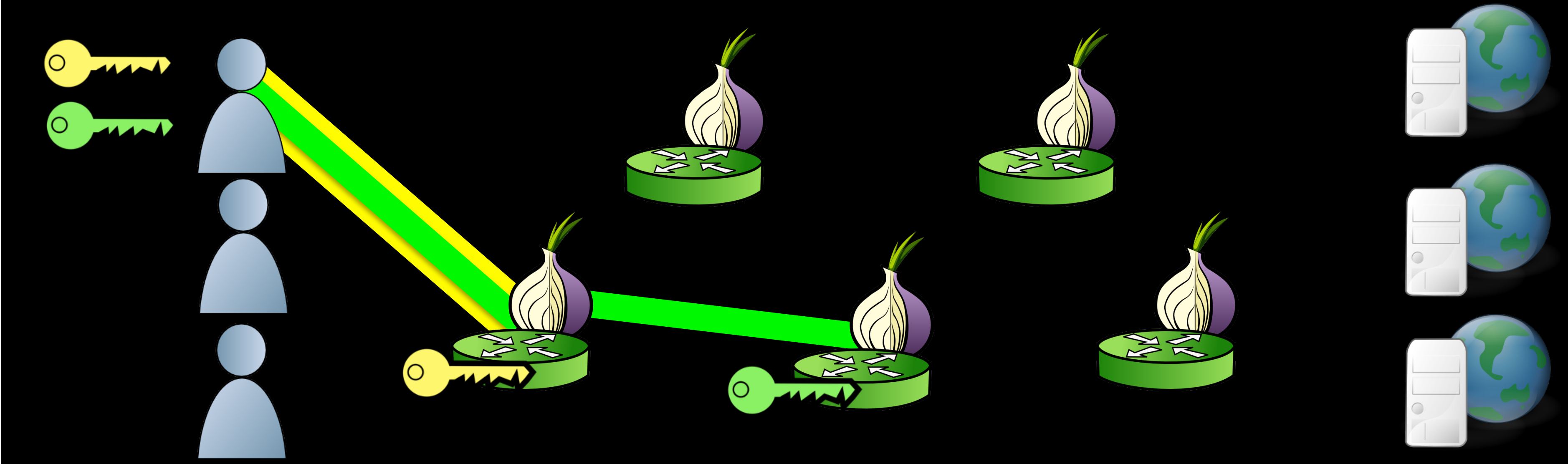


Users

Onion Routers

Destinations

Tor Background: Onion Routing

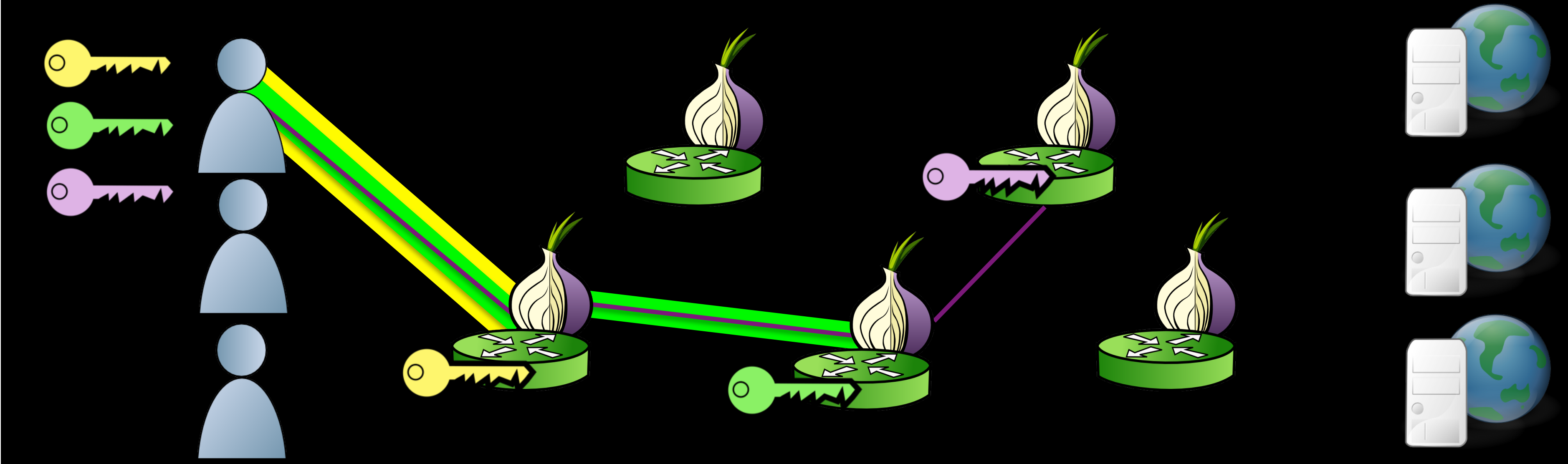


Users

Onion Routers

Destinations

Background: Onion Routing

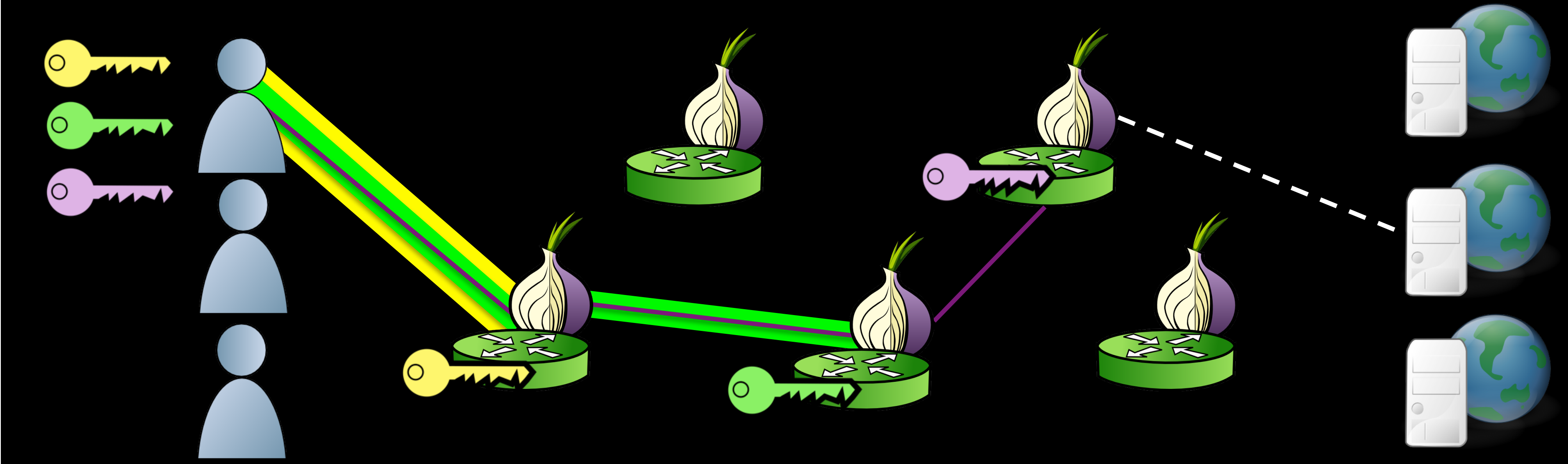


Users

Onion Routers

Destinations

Background: Onion Routing



Users

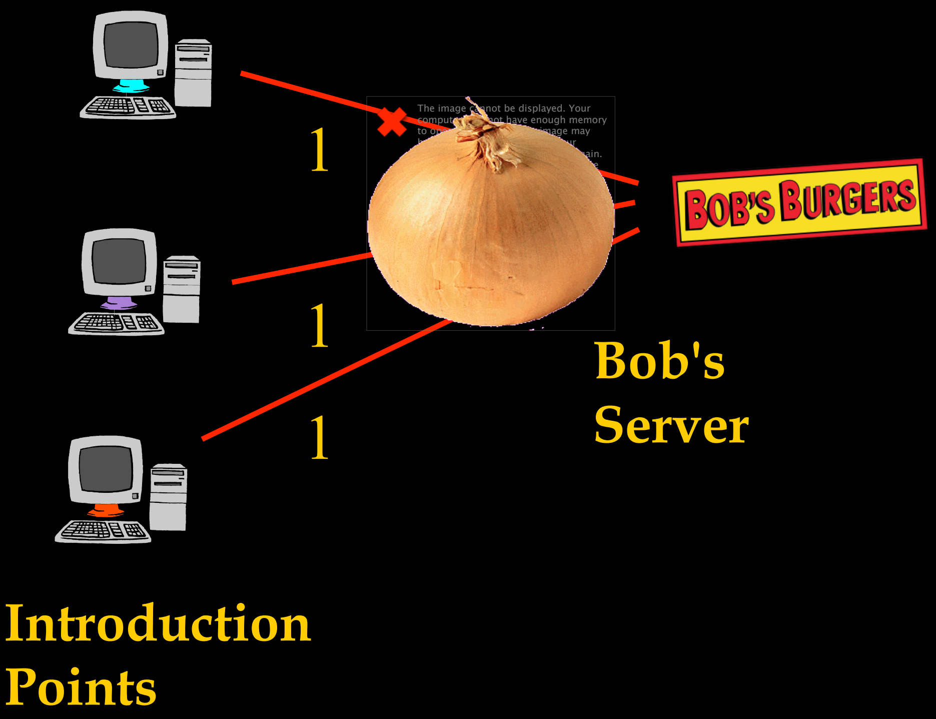
Onion Routers

Destinations

Onionsites

1. Server Bob creates onion routes to Introduction Points (IP)

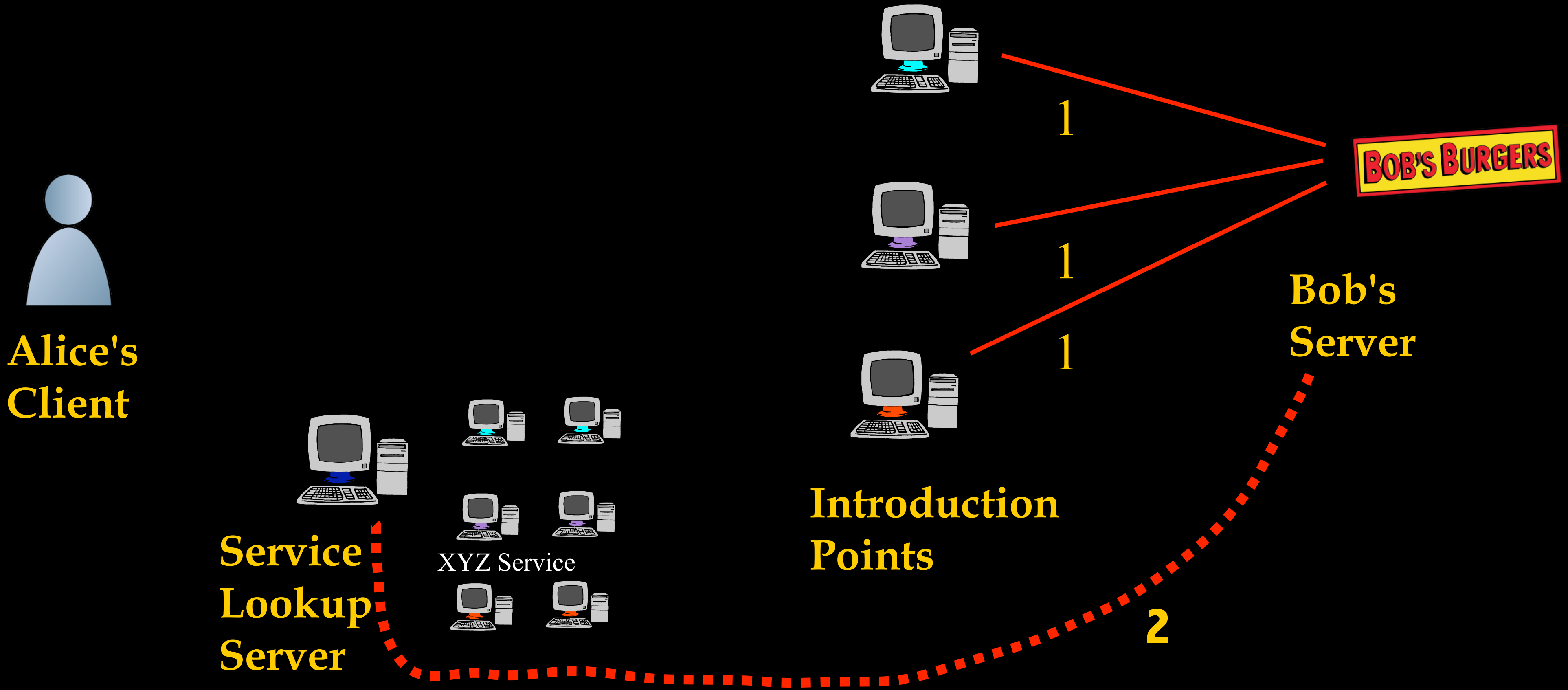
(All routes in these pictures are onion routed through Tor)



Onionsites

1. Server Bob creates onion routes to Introduction Points (IPo)

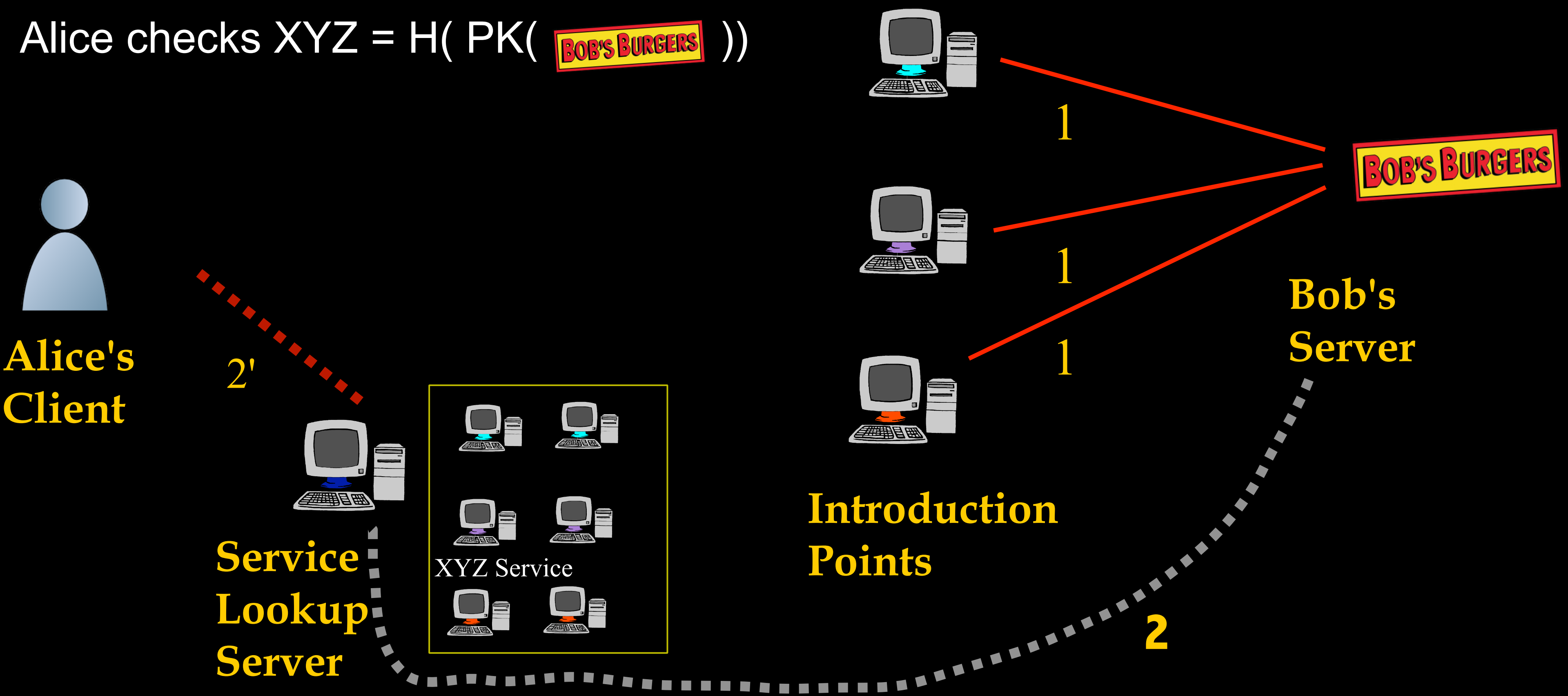
2. Bob publishes his xyz.onion address and puts Service Descriptor incl. Intro Pt. and public key listed under xyz.onion



Onionsites

2'. Alice uses xyz.onion to get Service Descriptor (including Intro Pt. address and Publlic Key) at Lookup Server

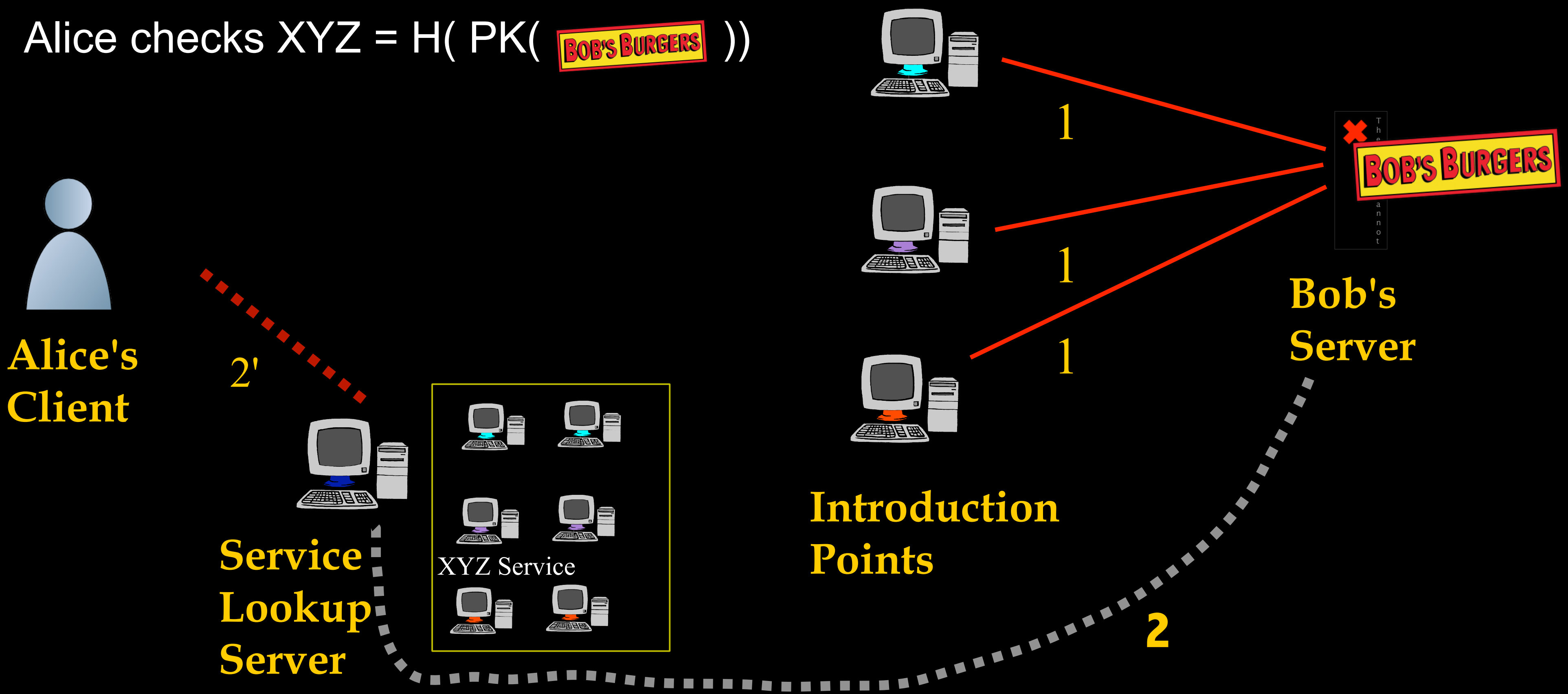
Alice checks XYZ = H(PK(BOB'S BURGERS))



.onions are Self-Authenticating

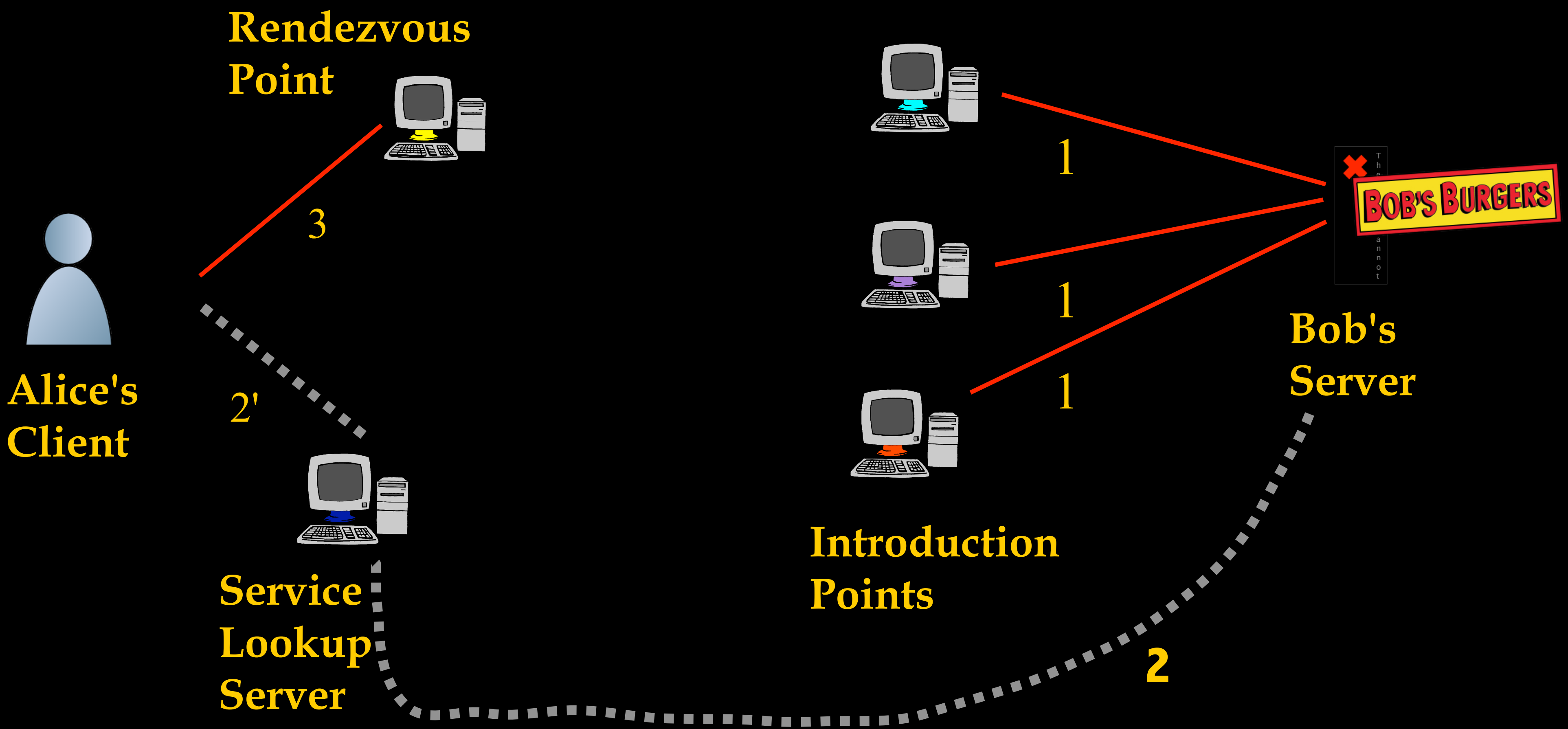
2'. Alice uses xyz.onion to get Service Descriptor (including Intro Pt. address and Publlic Key) at Lookup Server

Alice checks XYZ = H(PK(BOB'S BURGERS))



Onionsites

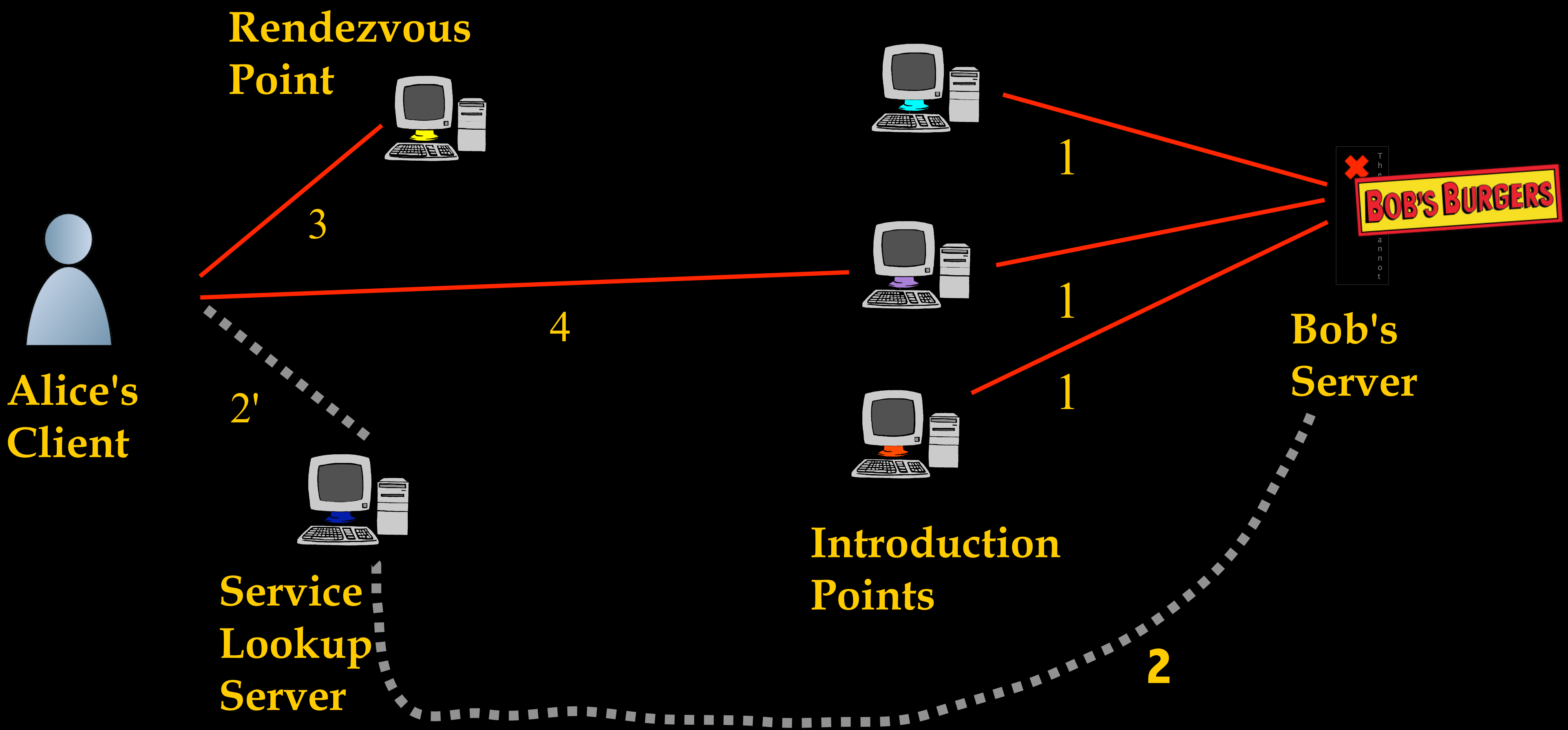
3. Client Alice creates onion route to Rendezvous Point (RP)



Onionsites

3. Client Alice creates onion route to Rendezvous Point (RP)

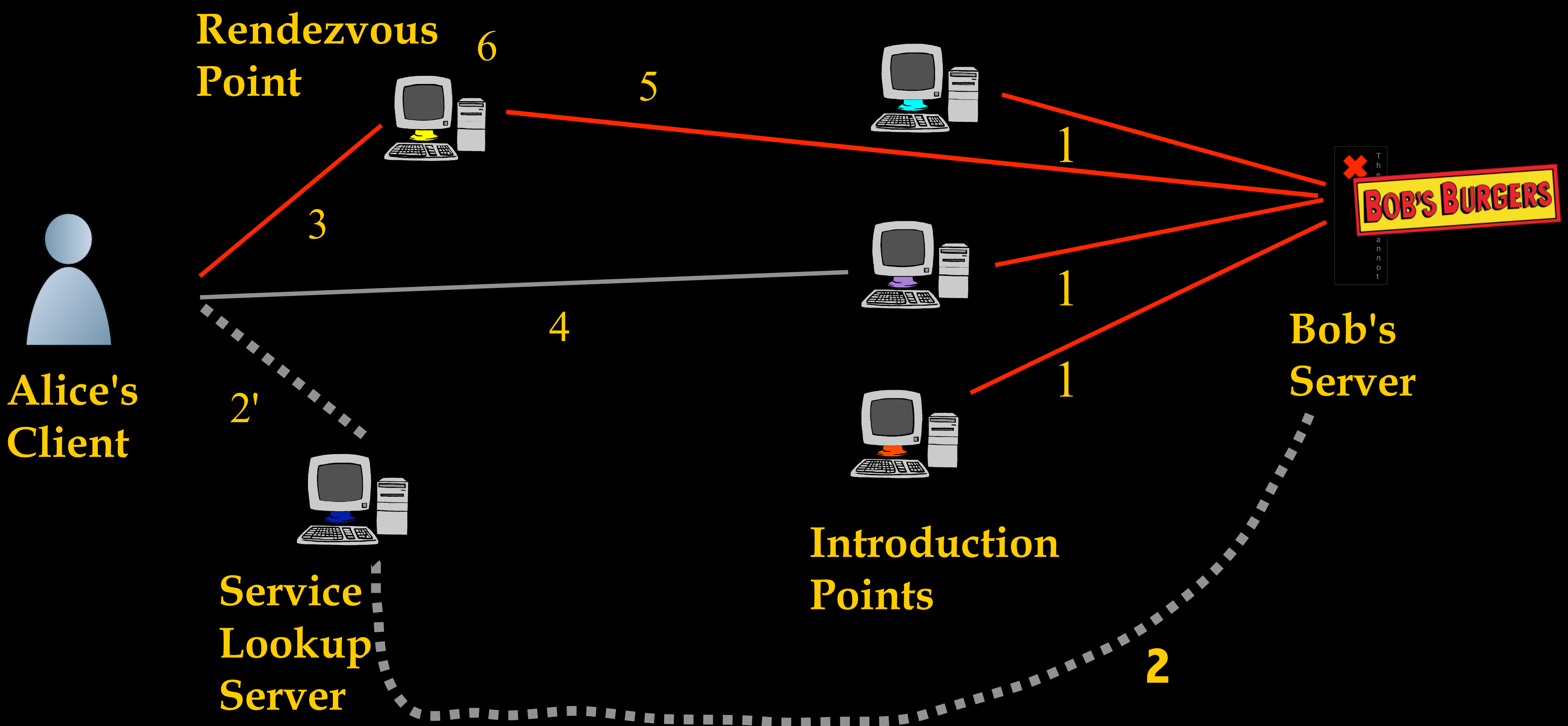
4. Alice sends RP address and any authorization through IPo to Bob



Onionsites

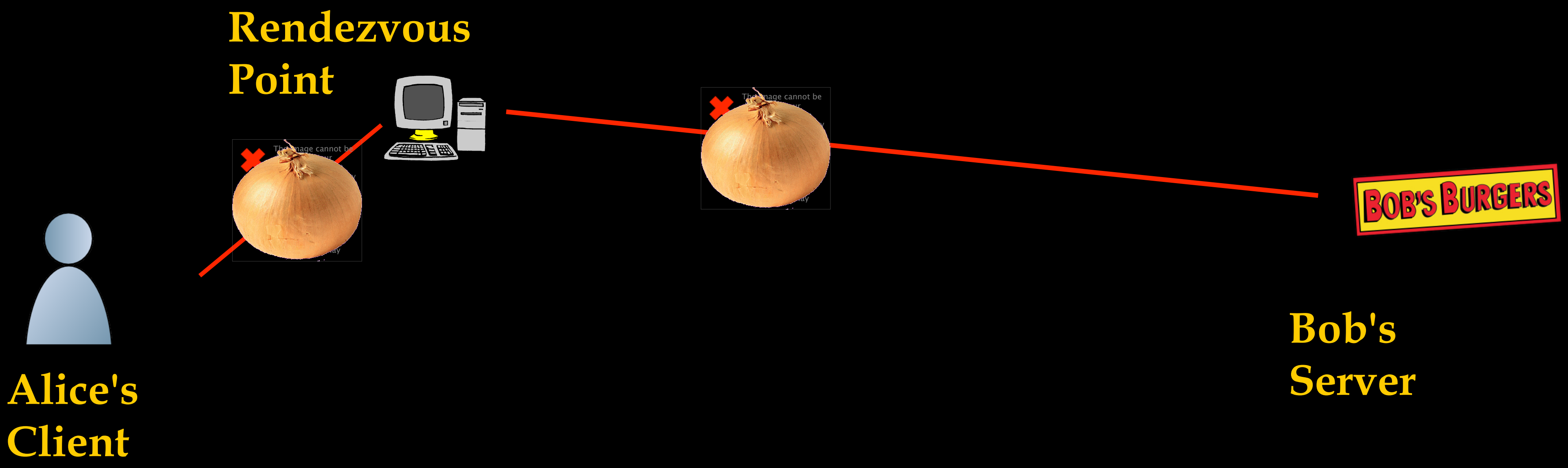
5. If Bob chooses to talk to Alice, connects to Rendezvous Point

6. Rendezvous Point mates the circuits from Alice and Bob



Onionsites

Final resulting communication channel



Rendezvous Point

Alice's Client

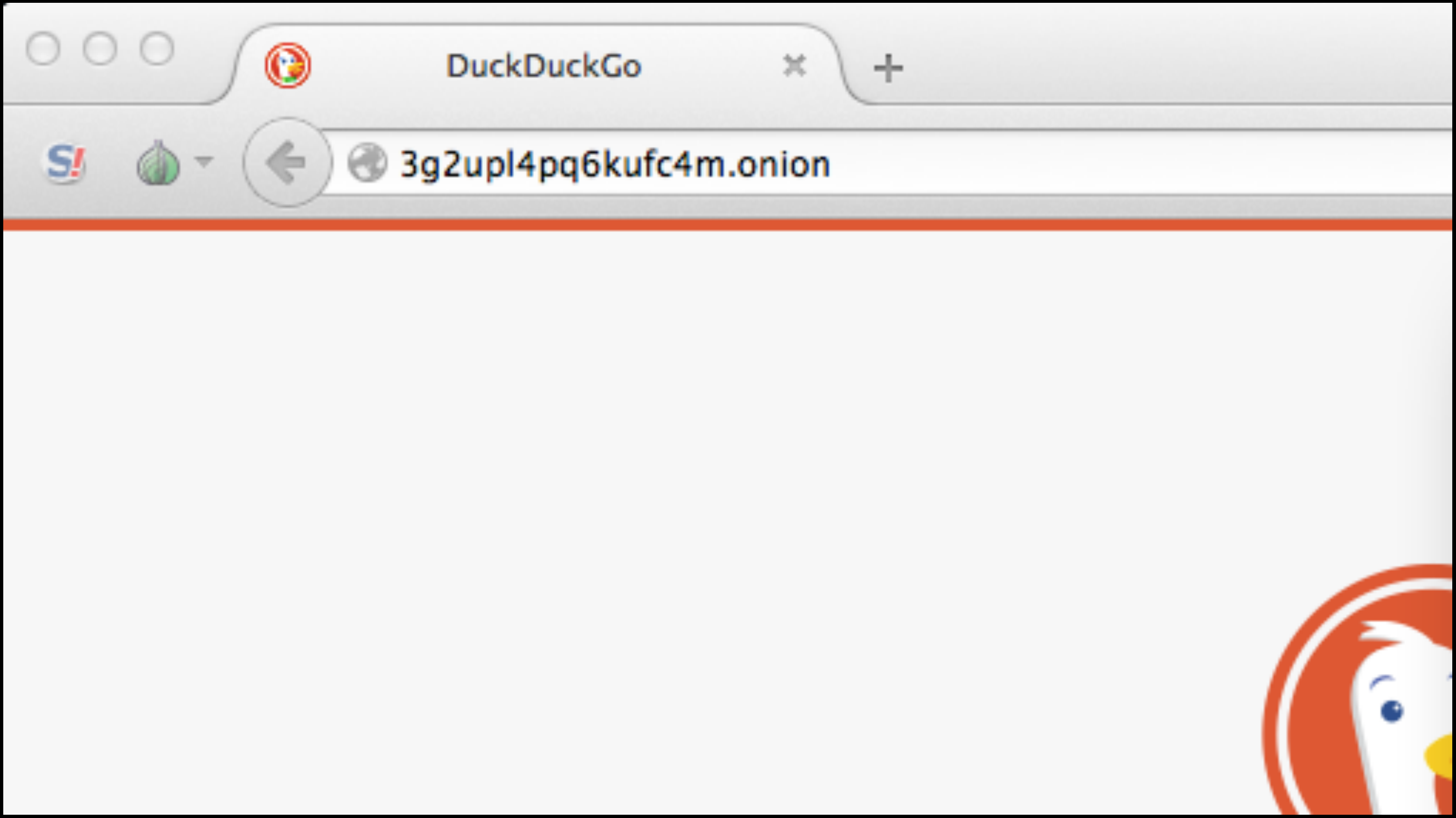
Bob's Server

.onions are not Human Meaningful

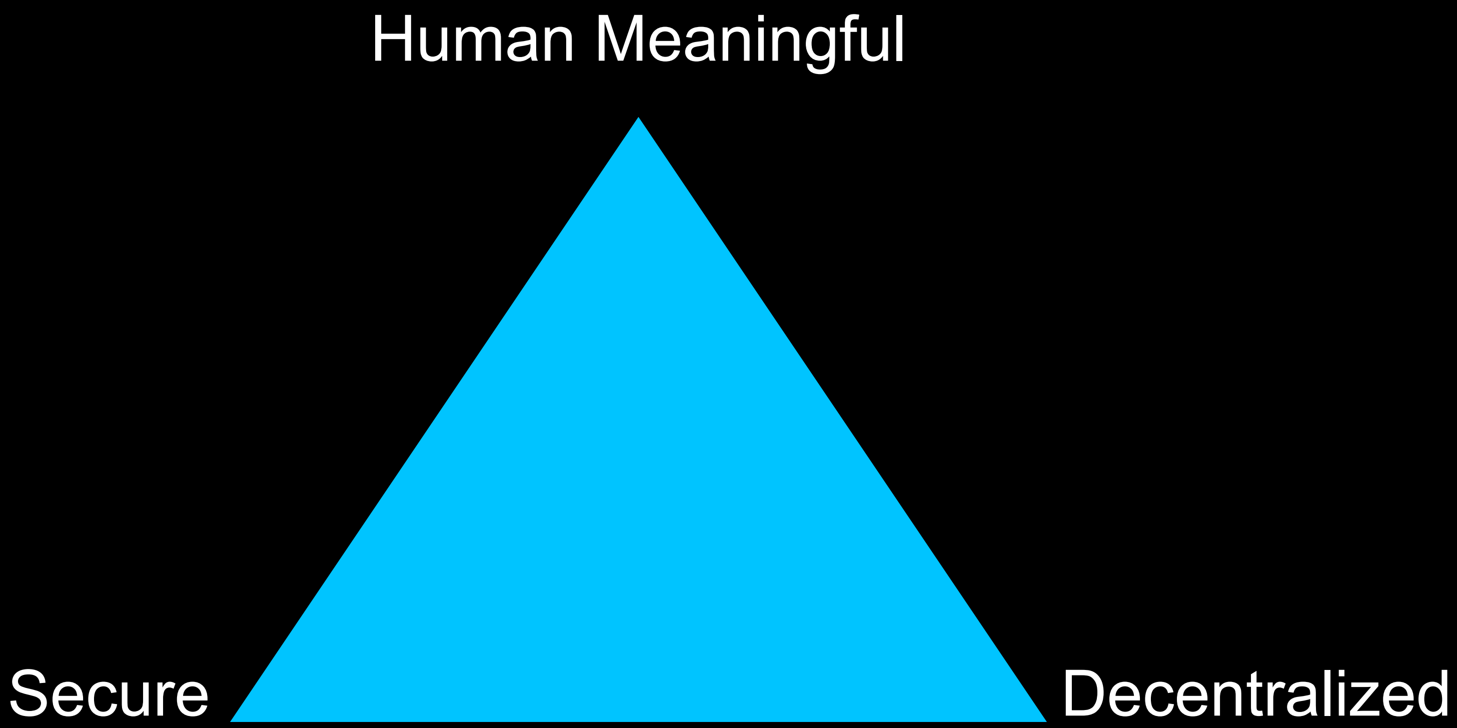
3g2upl4pq6kufc4m.onion

.onions are not Human Meaningful

3g2upl4pq6kufc4m.onion

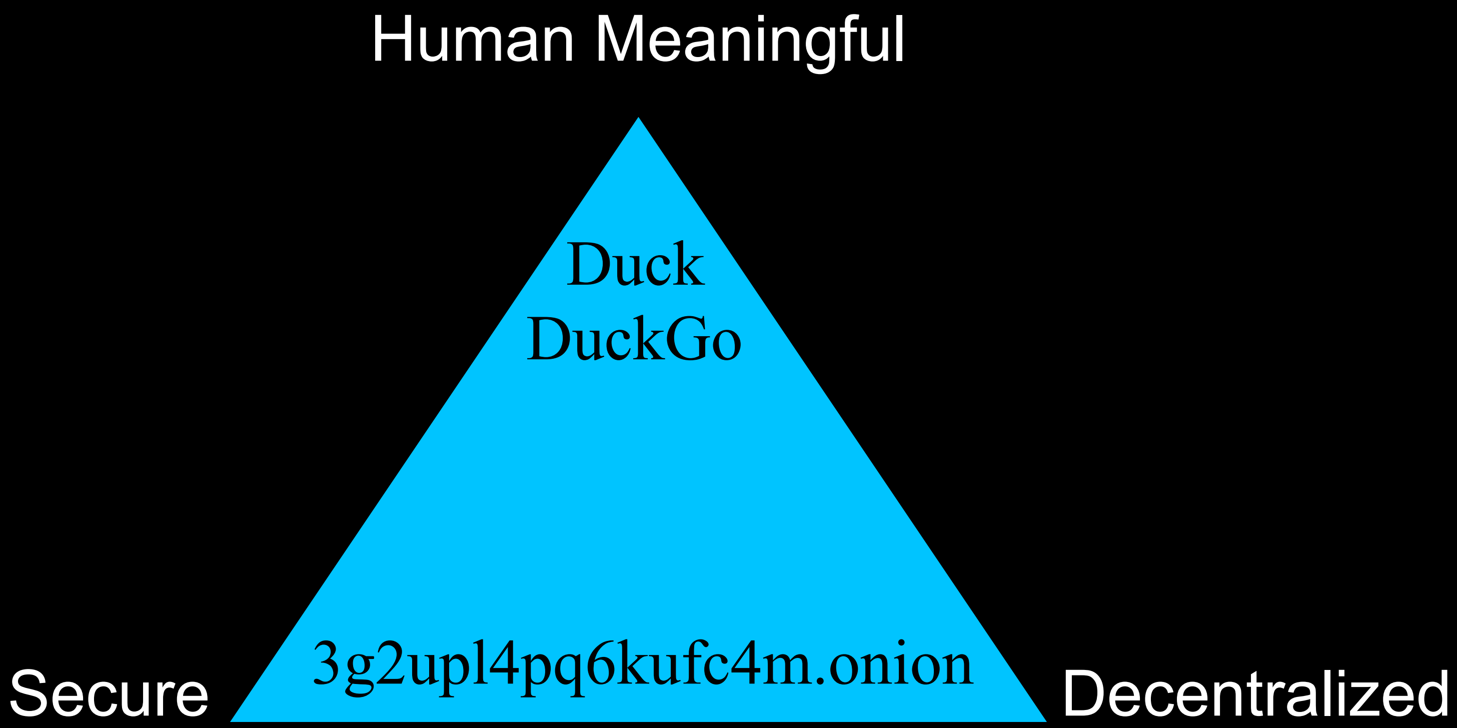


Zooko’s Triangle for Names



- Can generally obtain any two out of three

Zooko’s Triangle for Names



Human Meaningful

Duck DuckGo

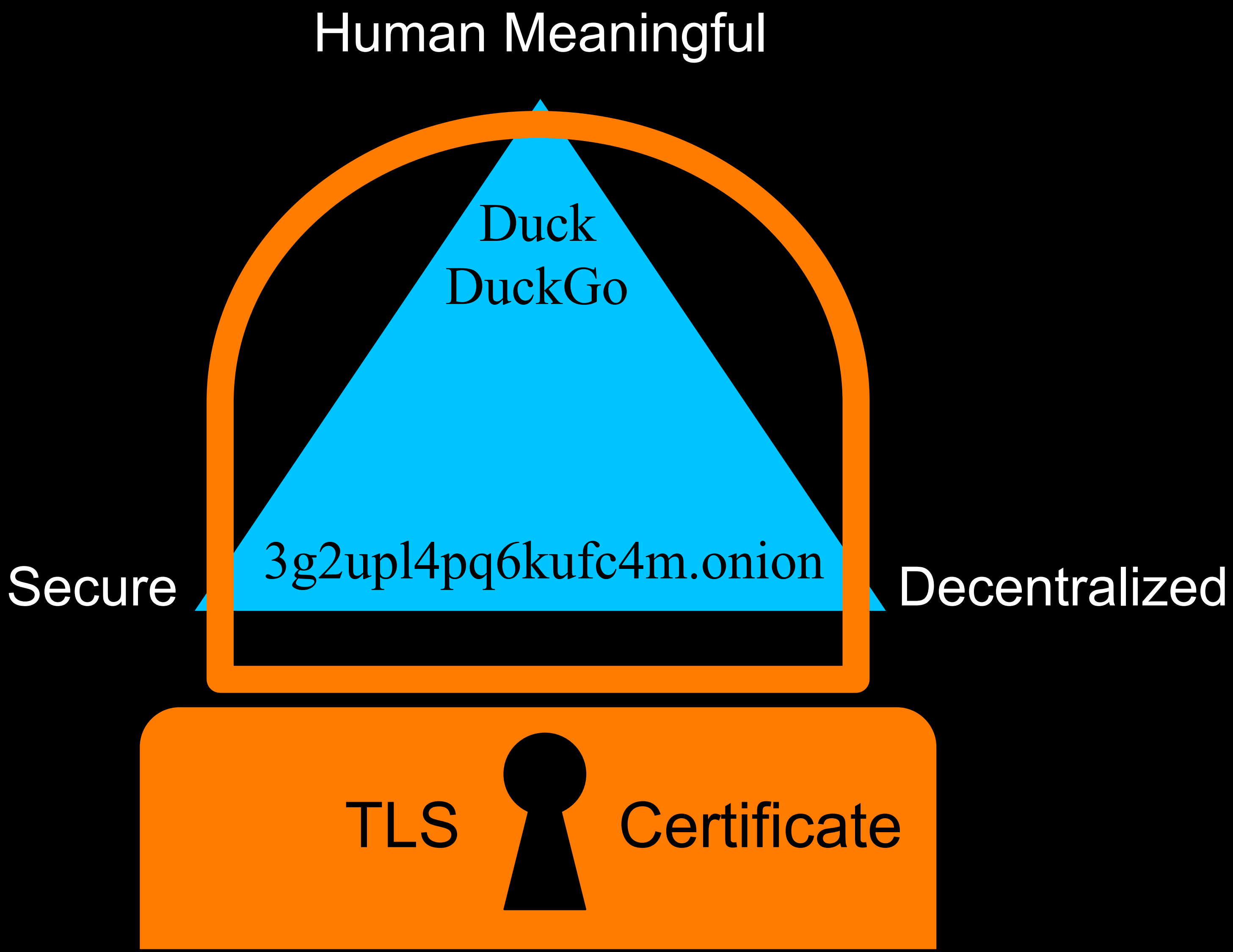
Secure

3g2upl4pq6kufc4m.onion

Decentralized

- Can generally obtain any two out of three

Zooko's Triangle for Names



Problems with TLS Certs

Can be:

- Costly
- Time consuming
- Hard to set up
- Not typically available for .onion (EV only)

Problems with TLS Certs

Can be:

- Costly
- Time consuming
- Hard to set up
- Not typically available for .onion (EV only)

- Let’s Encrypt: Free, Easy, Fast CA w/ backing of Mozilla, EFF, Akamai, Cisco, etc.

Problems with TLS Certs

Can be:

- Costly
- Time consuming
- Hard to set up
- Not typically available for .onion (EV only)

- Let's Encrypt: Free, Easy, Fast CA w/ backing of Mozilla, EFF, Akamai, Cisco, etc.
- Not available for a few months yet

More problems with TLS Certs

- Subject to hijacking

- HTTPS Observatory, Certificate Transparency, Perspectives, reveal shenanigans

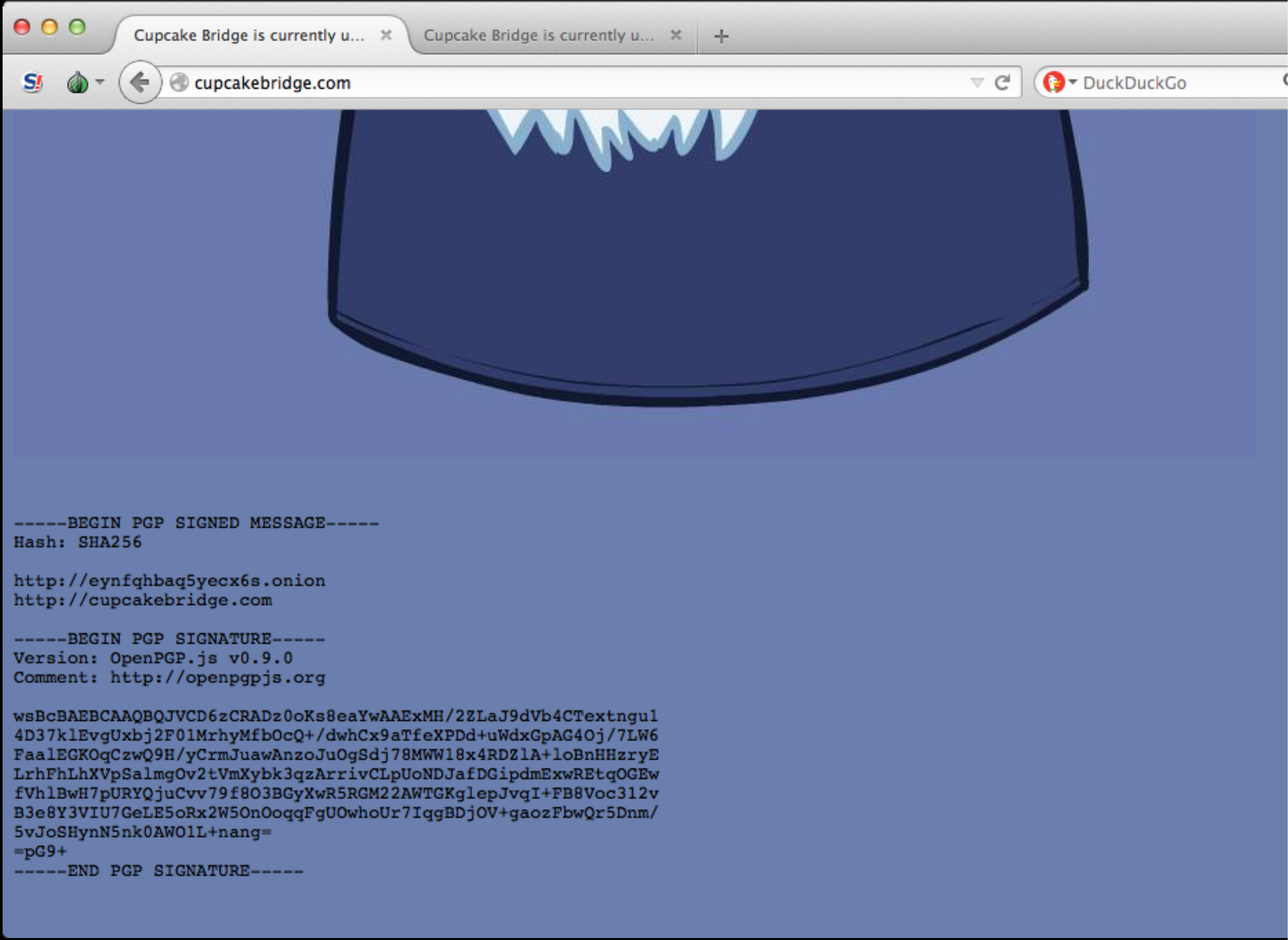
More problems with TLS Certs

- Subject to hijacking
- Trust relations opaque to users

- HTTPS Observatory, Certificate Transparency, Perspectives, reveal shenanigans

Our solution

- Set up onionsite corresponding to clearnet website
  - Might or might not be identical site or even on single web service instance
- Place GPG signature binding onionsite and clearnet website

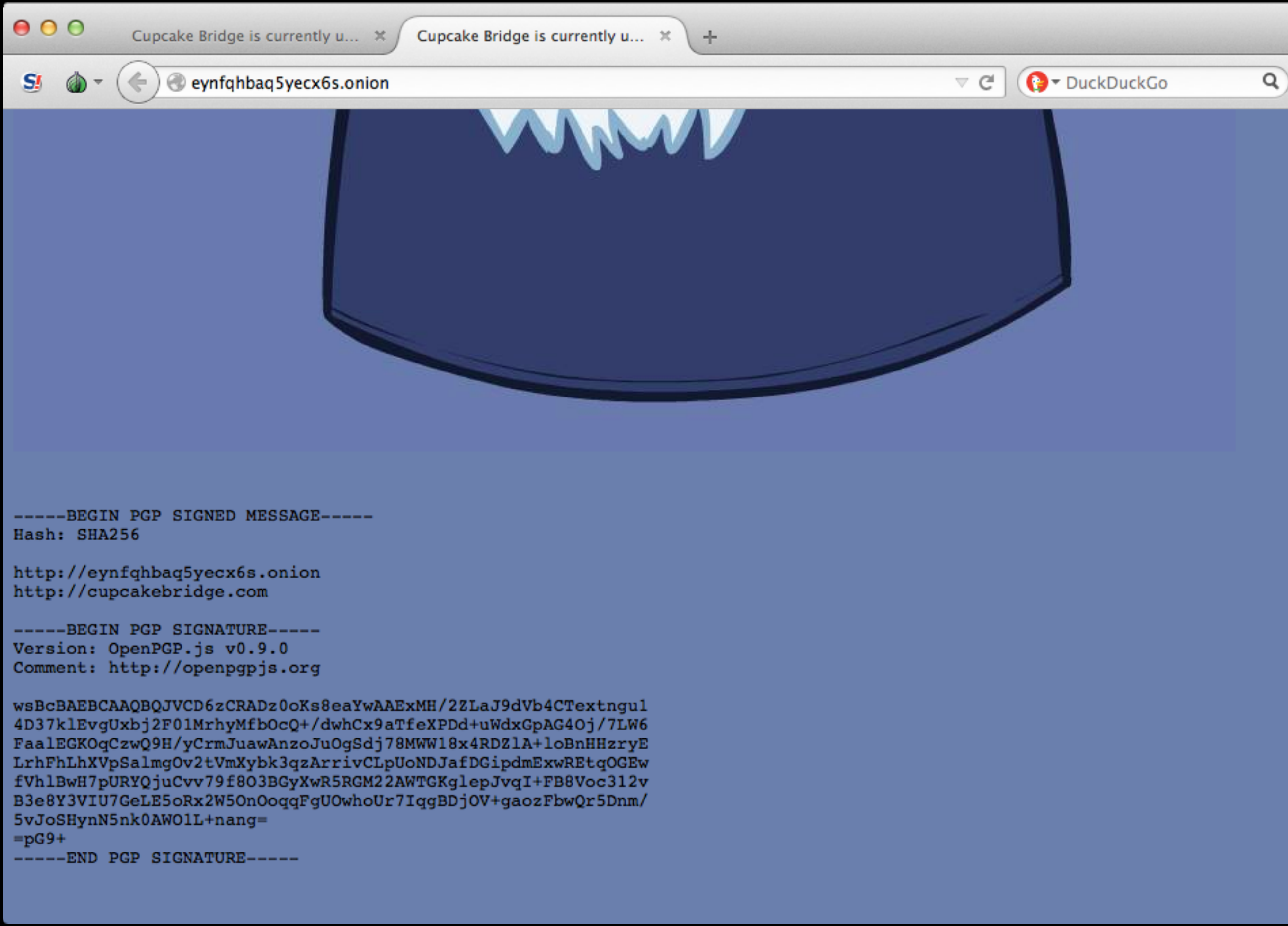

Cupcake Bridge is currently u...
Cupcake Bridge is currently u...
cupcakebridge.com
DuckDuckGo

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

http://eynfqhbaq5yecx6s.onion
http://cupcakebridge.com

-----BEGIN PGP SIGNATURE-----
Version: OpenPGP.js v0.9.0
Comment: http://openpgpjs.org

wsBcBAEBCAAQBQJVCD6zCRADz0oKs8eaYwAAExMH/2ZLaJ9dVb4CTextngul
4D37klEvgUxbj2F01MrhyMfbOcQ+/dwhCx9aTfeXPDd+uWdxGpAG4Oj/7LW6
FaalEGKOqCzwQ9H/yCrmJuawAnzoJuOgSdj78MWW18x4RDZlA+loBnHHzryE
LrhFhLhXVpSalmgOv2tVmXybk3qzArrivCLpUoNDJafDGipdmExwREtqOGEw
fVhlBwH7pURYQjuCvv79f8O3BGyXwR5RGM22AWTGKglepJvqI+FB8Voc312v
B3e8Y3VIU7GeLE5oRx2W5OnOoqqFgUOwhoUr7IqgBDjOV+gaozFbwQr5Dnm/
5vJoSHynN5nk0AWO1L+nang=
=pG9+
-----END PGP SIGNATURE-----
```


Cupcake Bridge is currently u...
Cupcake Bridge is currently u...
eynfqhbaq5yecx6s.onion
DuckDuckGo

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

http://eynfqhbaq5yecx6s.onion
http://cupcakebridge.com

-----BEGIN PGP SIGNATURE-----
Version: OpenPGP.js v0.9.0
Comment: http://openpgpjs.org

wsBcBAEBCAAQBQJVCD6zCRADz0oKs8eaYwAAExMH/2ZLaJ9dVb4CTextngul
4D37klEvgUxbj2F01MrhyMfbOcQ+/dwhCx9aTfeXPDd+uWdxGpAG4Oj/7LW6
FaalEGKOqCzwQ9H/yCrmJuawAnzoJuOgSdj78MWW18x4RDZlA+loBnHHzryE
LrhFhLhXVpSalmgOv2tVmXybk3qzArrivCLpUoNDJafDGipdmExwREtqOGEw
fVhlBwH7pURYQjuCvv79f8O3BGyXwR5RGM22AWTGKglepJvqI+FB8Voc312v
B3e8Y3VIU7GeLE5oRx2W5OnOoqqFgUOwhoUr7IqgBDjOV+gaozFbwQr5Dnm/
5vJoSHynN5nk0AWO1L+nang=
=pG9+
-----END PGP SIGNATURE-----
```

Advantages of PGP/GPG binding of onionsites to ordinary URL sites

- Can be done by anyone right now using existing software
- Site trust is based on known established trust relations (web of trust)
  - Seymour’s Bay Chamber of Commerce signs Bob’s Burgers website cert
- Not subject to MitM or hijacking
- Can be used instead of/until various proposals for web of trust with novel name system or TLS cert infrastructure grow

Current Limitations of PGP/GPG binding of onionsites to ordinary URL sites

- Not currently automated
  - should be straightforward to do so (Monkeysphere)
  - Ahmia (onionsite search engine) suggests providing results linking clearnet to onion sites and signature validation. Simple plugin could check.
- Not as widely familiar as TLS and not integrated with traditional browser TLS encryption and authentication
  - could support both X.509 certs and GPG certs (Monkeysphere)

More advantages of using onionsites for authentication

- Don’t need to register a domain name at all to have recognizable, secure, webpage
  - post signed onion address on Facebook Page, Wordpress Blog, etc.
  - Facebook’s Cert not much use here for personal content assurance
- Route security & server hiding still useful for
  - personal (or minimally shared) cloud services
  - Integrity protection for personal RSS feeds (especially from non-TLS feed sources)

Questions?

Talk Points

- Onionsites are self-authenticating but not human meaningful
- GPG binding of plain domain names and onions permits authentication that is
  - to a meaningful name
  - backed by existing human trust relations
  - avoids problems of existing TLS Cert infrastructure
  - available to use right now
- Readily automatable
- Complements rather than replaces existing mechanisms