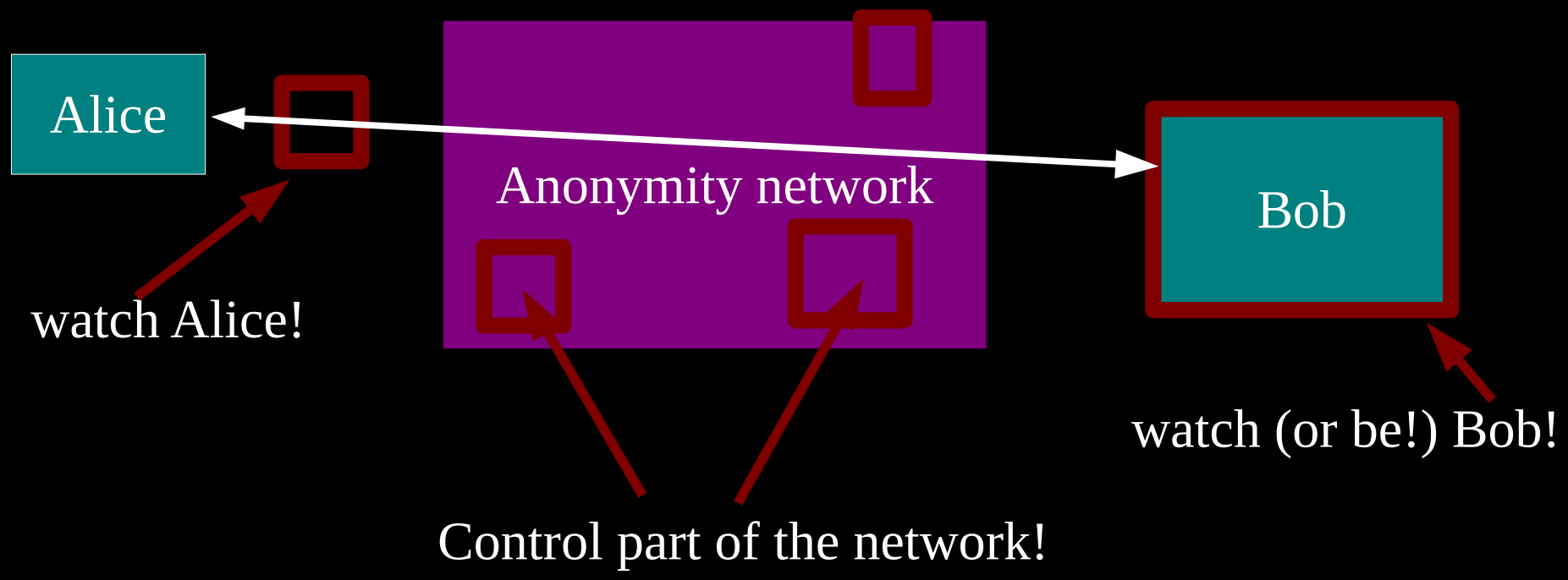
The Tor Project

Our mission is to be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.

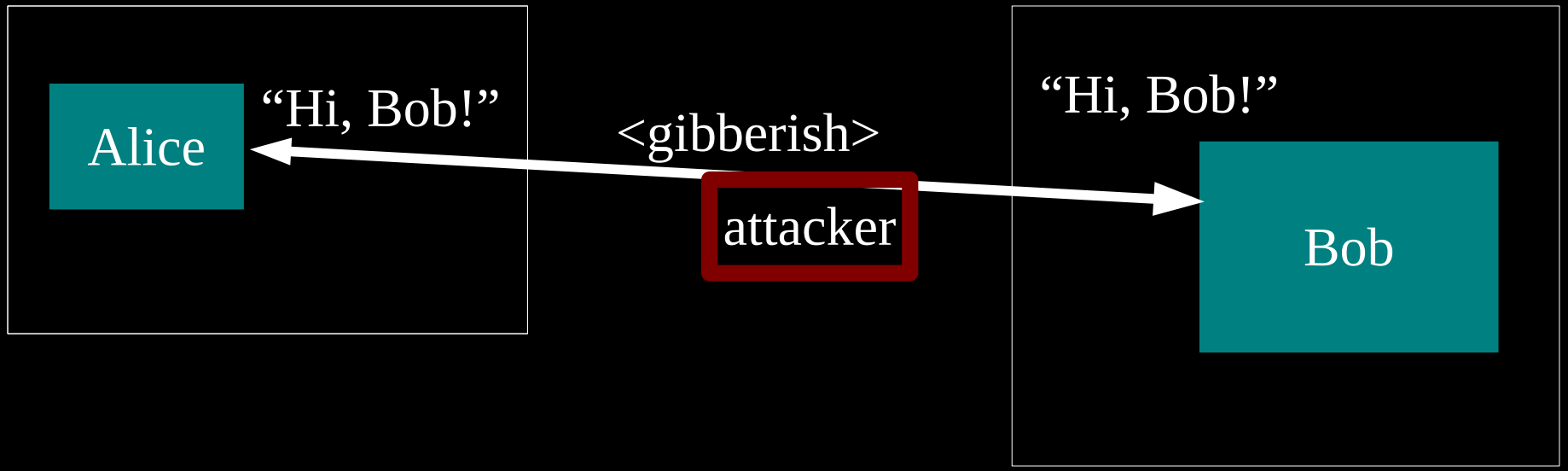
- Online Anonymity
  - Open Source
  - Open Network
- Community of researchers, developers, users and relay operators.
- U.S. 501(c)(3) non-profit organization


Estimated 2,000,000+
daily Tor users

Threat model: what can the attacker do?



Anonymity isn't encryption: Encryption just protects contents.



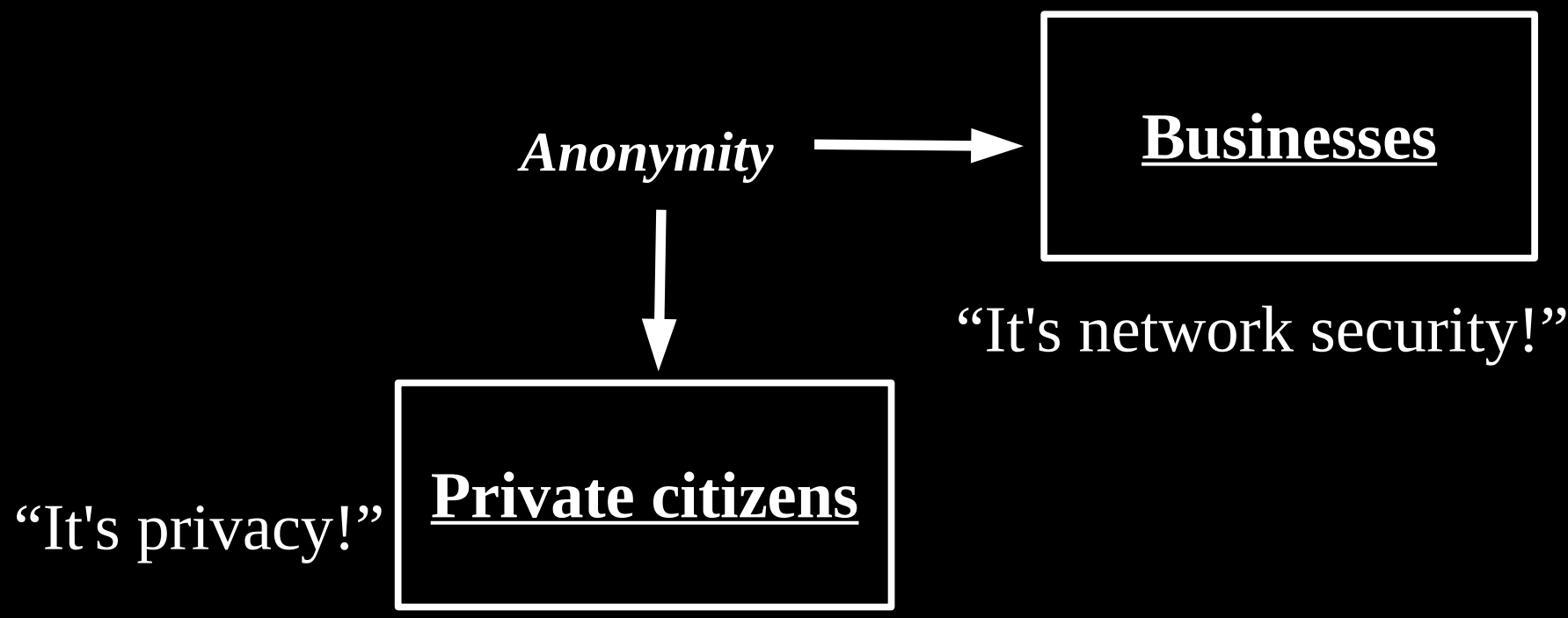
Anonymity serves different interests for different user groups.

Anonymity

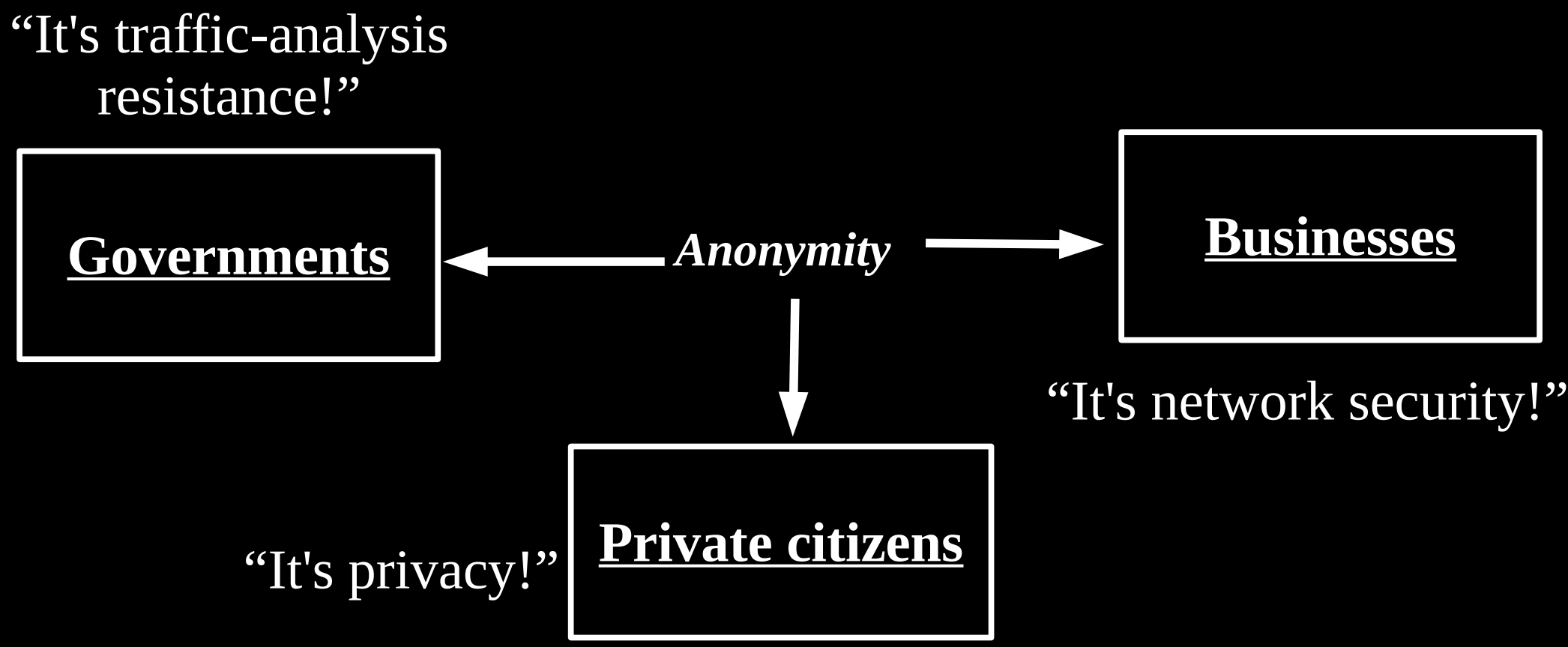
“It's privacy!”

Private citizens

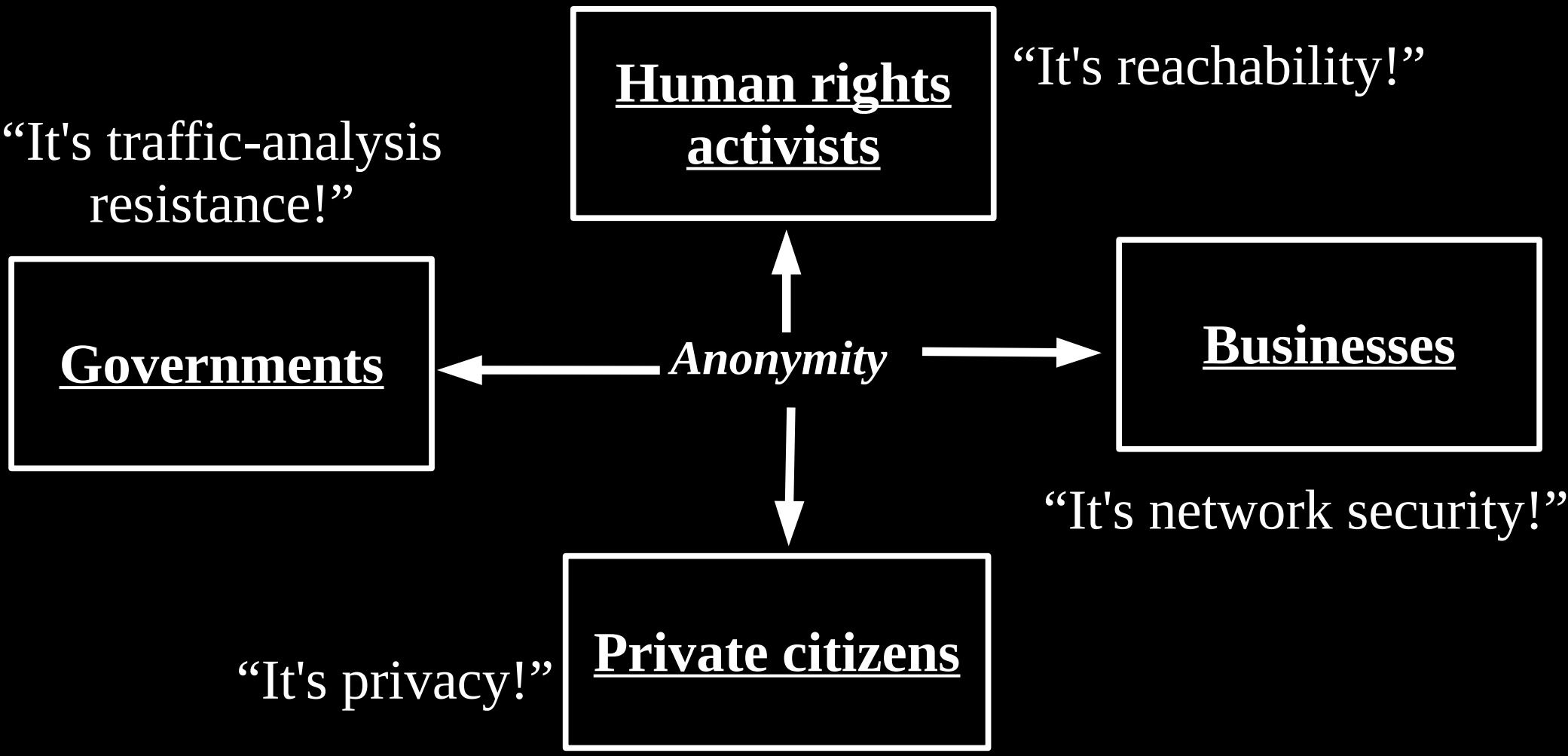
Anonymity serves different interests for different user groups.



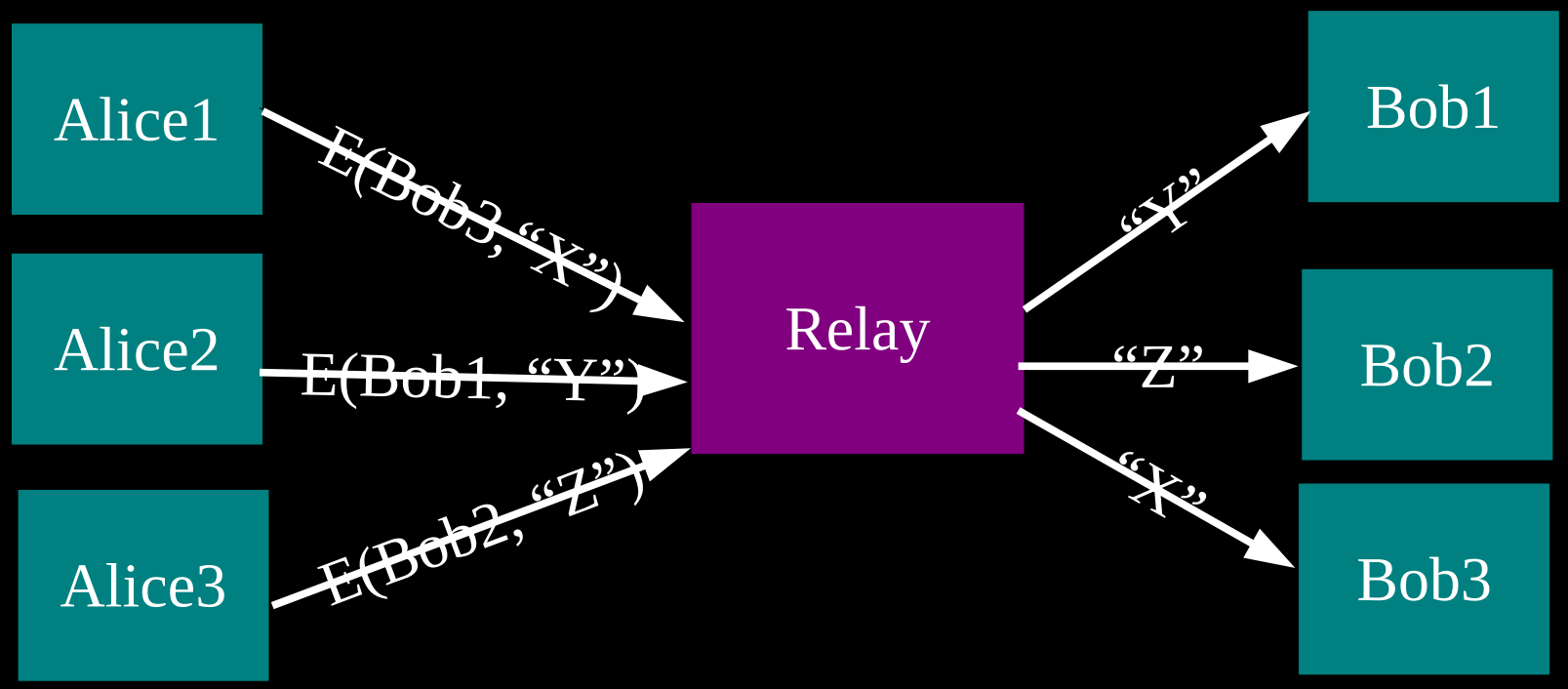
Anonymity serves different interests for different user groups.



Anonymity serves different interests for different user groups.

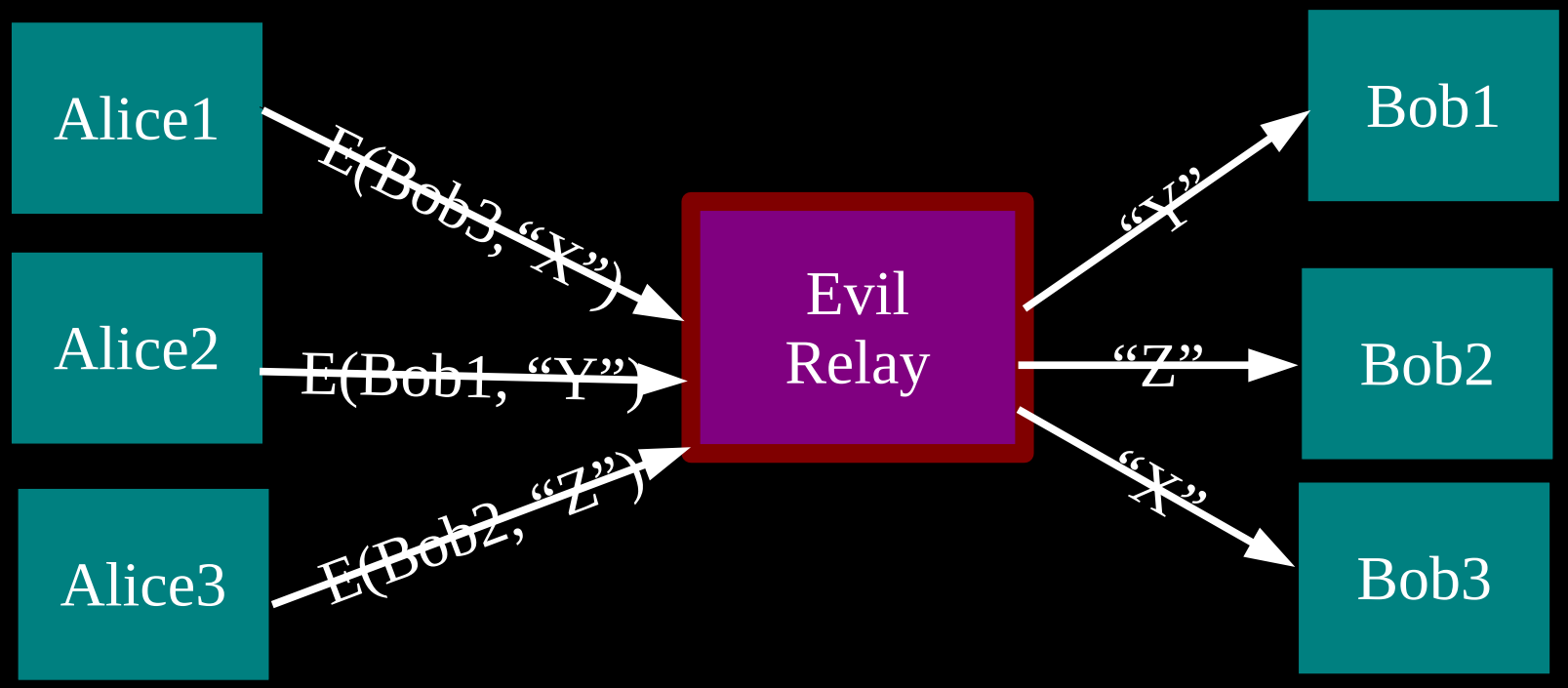


The simplest designs use a single relay to hide connections.

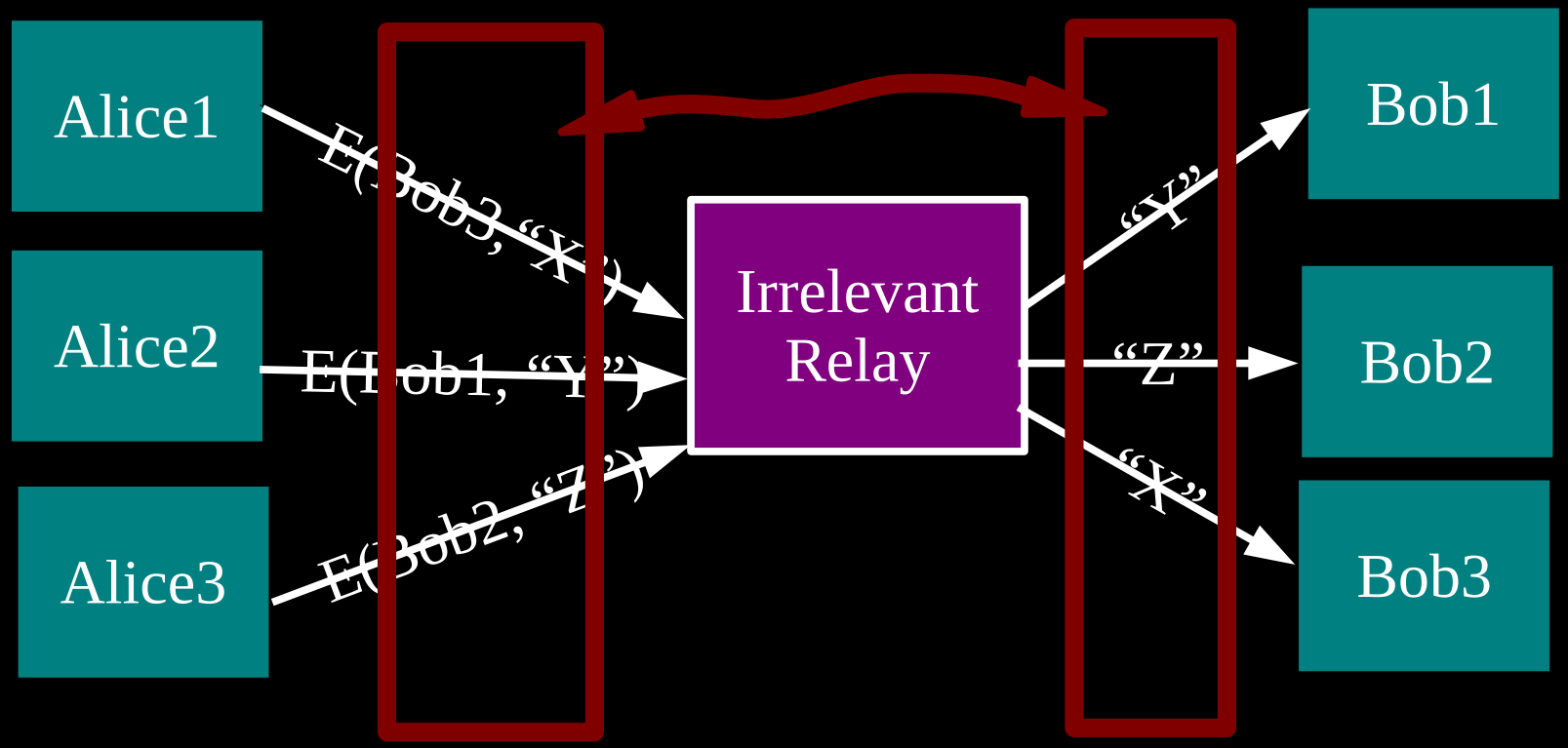


(example: some commercial proxy providers)

But a central relay is a single point of failure.

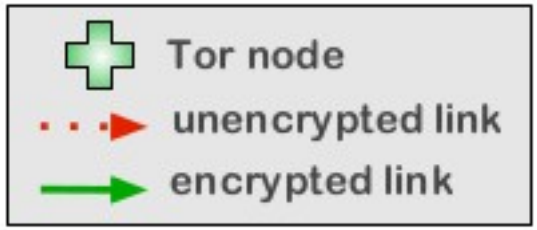


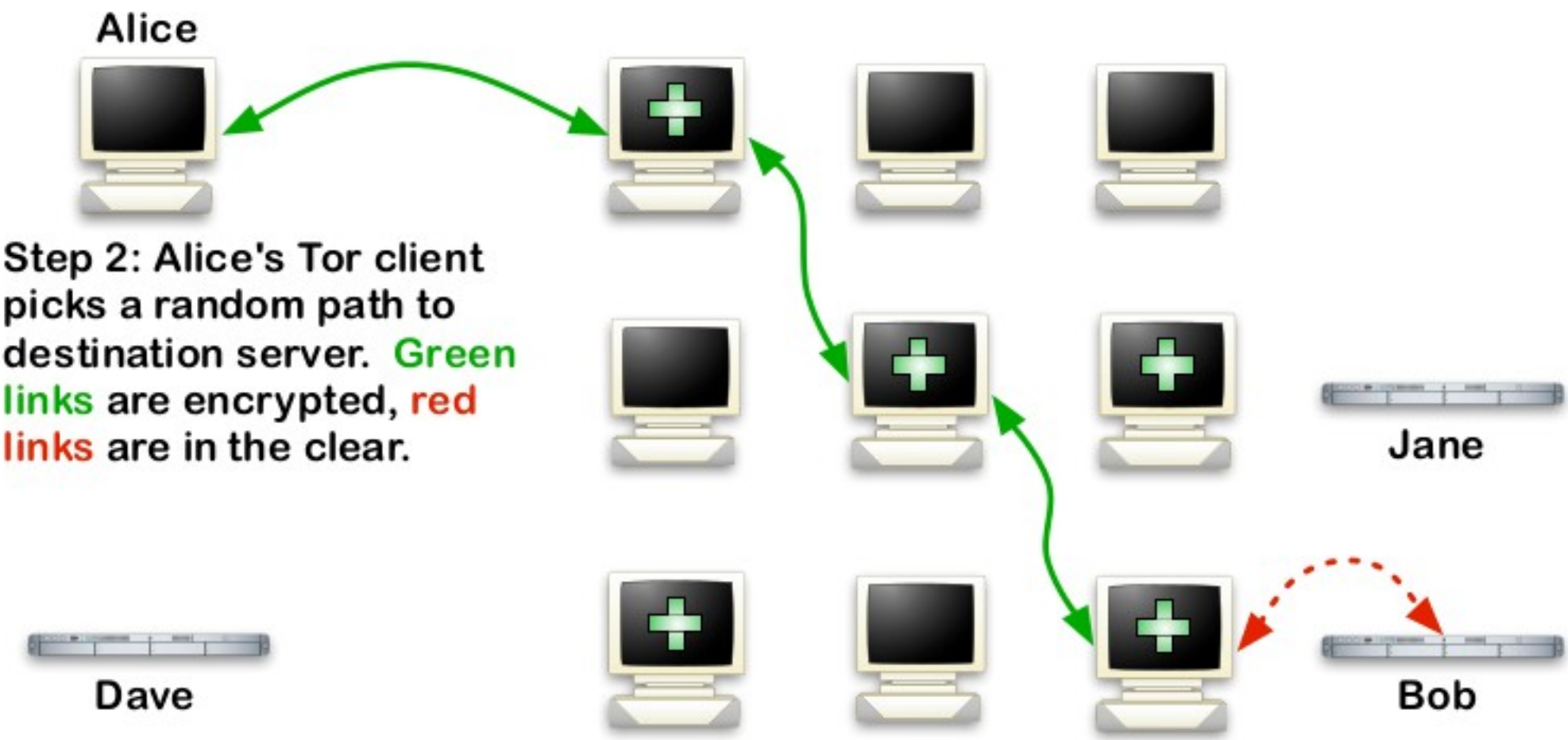
... or a single point of bypass.



Timing analysis bridges all connections through relay ⇒ An attractive fat target

How Tor Works: 2





Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

About Tor – Tor Browser

File Edit View History Bookmarks Tools Help

About Tor | Atlas | Facebook

about:tor

Startpage

- New Identity
- Cookie Protections
- Preferences...
- About Torbutton...
- Open Network Settings...

Tor Browser
3.5-Linux

Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

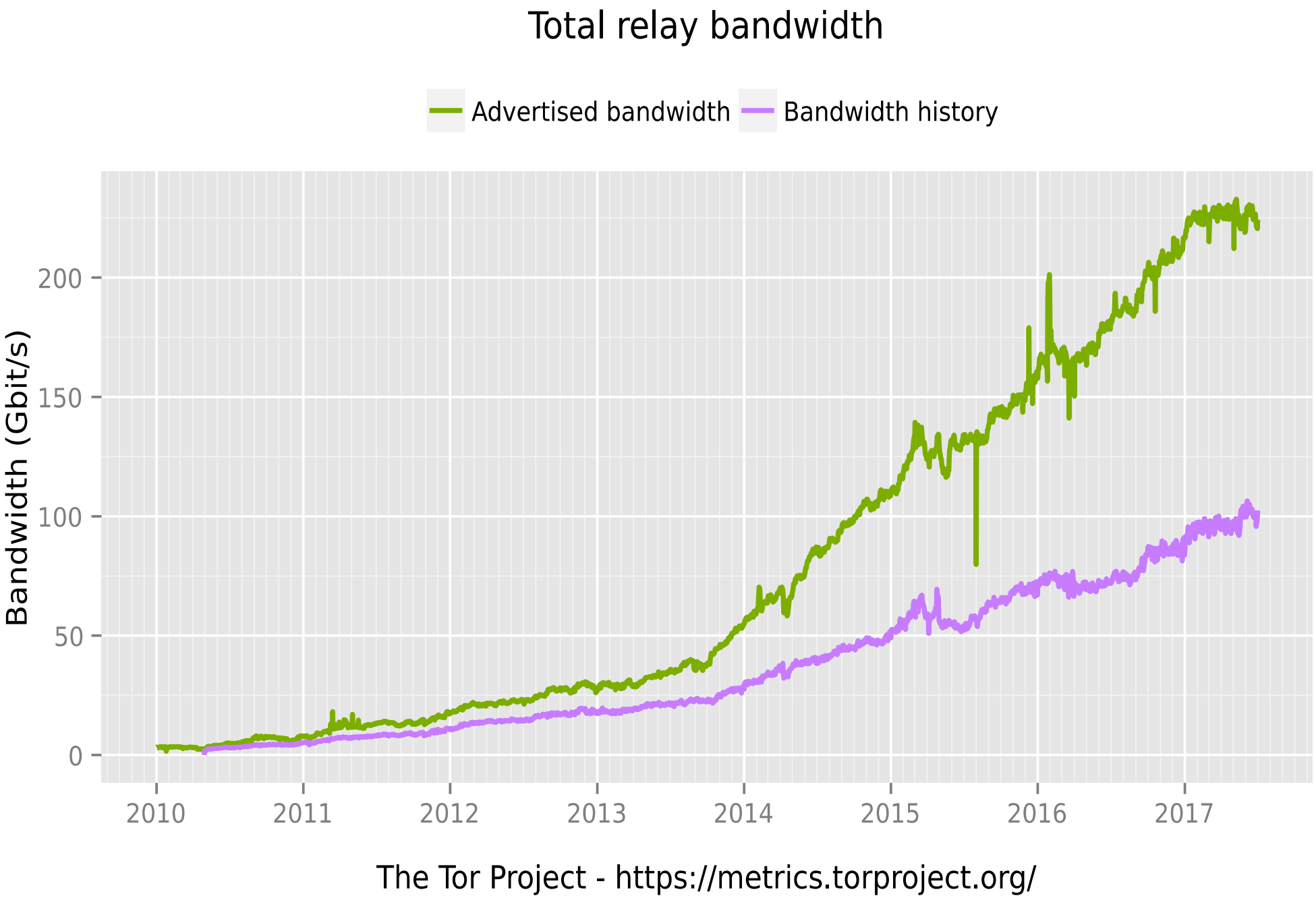
Tips On Staying Anonymous »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »


Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (Gbit/s)
200
150
100
50
0
2010
2011
2012
2013
2014
2015
2016
2017
The Tor Project - https://metrics.torproject.org/

Tor's safety comes from diversity

- #1: Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation. (Research problem: measuring diversity over time)
- #2: Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.

Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers
- Not a contradiction:
  privacy is about choice!

But what about bad people?

- Remember the millions of daily users.
- Still a two-edged sword?
- Good people need Tor much more than bad guys need it.

Myth #1

- “I heard the Navy wrote Tor originally, so how can I trust it?”

Myth #2

- “I heard the NSA runs half the relays.”

Myth #3

- “I heard Tor is slow.”

Myth #4

- “I heard Tor gets most of its money from the US government.”

Myth #5

- “I heard 80% of Tor is bad people.”

Myth #6

- “I shouldn't use Tor, because if I do the NSA will watch me.”

Myth #7

- “I heard Tor is broken.”

riseup.net

cwoiopiifrlzcuos.onion

riseup.net

Welcome to Riseup B

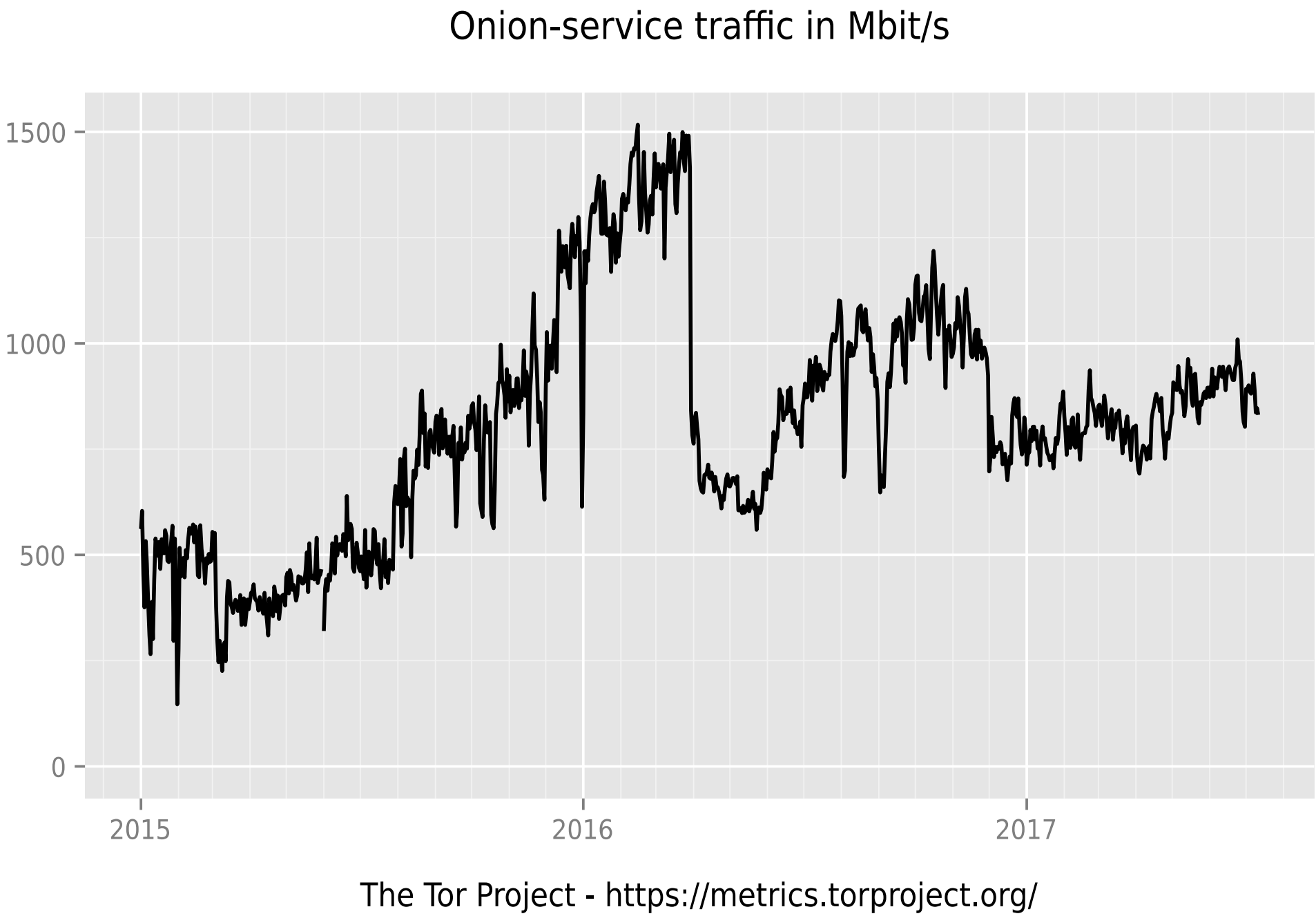
This is the home of the Riseup "Black" services, our new enhan
application.

Important: To avoid possible issues, you will need to create
services. But don't fear, you will be later able to use your cur

D

Onion service properties

- Self authenticated
- End-to-end encrypted
- Built-in NAT punching
- Limit surface area
- No need to “exit” from Tor


Onion-service traffic in Mbit/s
1500
1000
500
0
2015
2016
2017
The Tor Project - https://metrics.torproject.org/

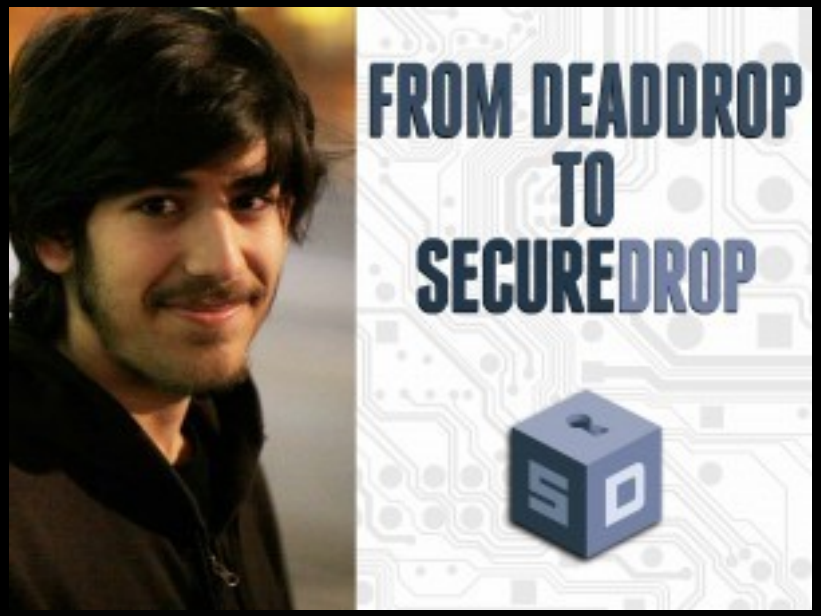
About 3%

- <show graph showing that 1gbit/s is about 3% of Tor's traffic> – onion services are still in the “neat toy” stage
- Terbium labs (and others) found about 7000 useful onion sites


World Wide Web
Deep Web
Dark Web

SecureDrop

THE NEW YORKER
STRONGBOX



SECUREDROP

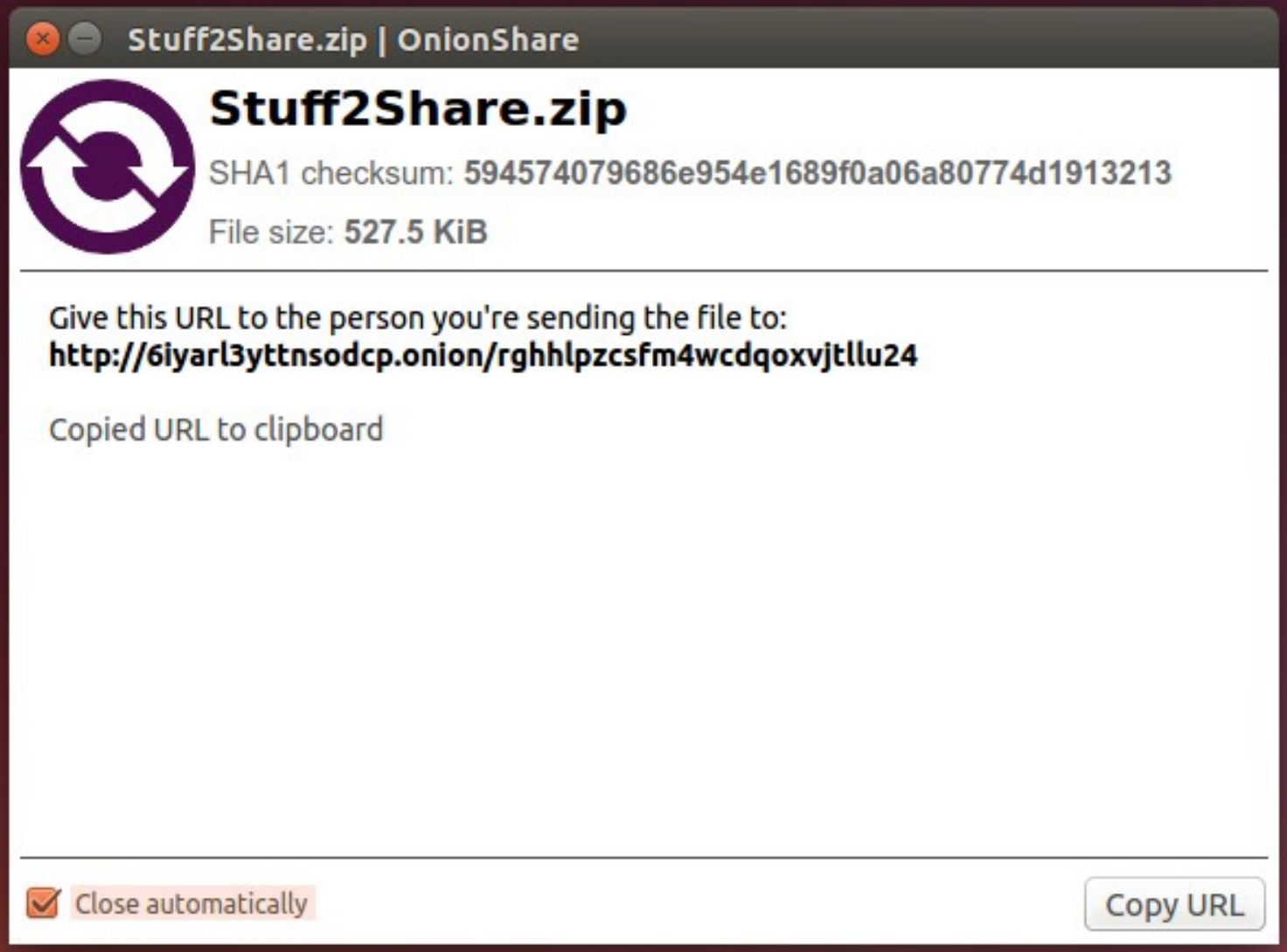
Today, 30+ organizations use SecureDrop

https://securedrop.org/directory

Ricochet


Ricochet
En ligne
CONNECTÉ
Lecteur 1
1
REQUÊTES
John Brooks
Lecteur 1
Lecteur 1
25/05/2015 10:56
Salut !
Salut Korben !
ça fonctionne, c'est cool. A qui ai je l'honneur ?
Oui, c'est cool. Je suis un lecteur de ton site, Paul.
enchanté !
j'ai commenté qu'une fois un article sur Mario64 porté sur plateforme x86

OnionShare


Stuff2Share.zip | OnionShare
Stuff2Share.zip
SHA1 checksum: 594574079686e954e1689f0a06a80774d1913213
File size: 527.5 KiB
Give this URL to the person you're sending the file to:
http://6iyarl3yttnsodcp.onion/rghhlpzcsfm4wcdqoxvjtllu24
Copied URL to clipboard
Close automatically
Copy URL

Services and Tools

All Riseup.net services are available using hidden service

https://help.riseup.net/en/tor#riseups-tor-hidden-services

... and many others

...

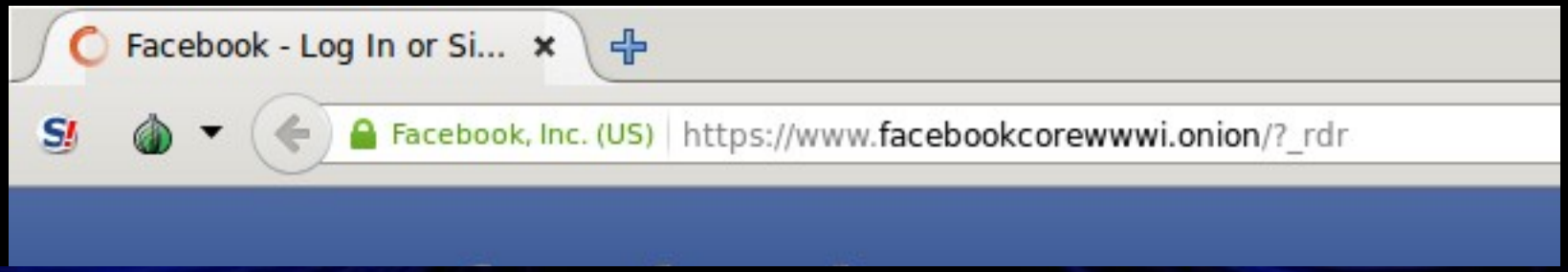
Package repository

`http://vwakviie2ienjx6t.onion/`

```
apt-get install apt-tor-transport
```

Anonymous updates are awesome

- Evil package repository can't target you with a bad update, because they don't know it's you
- Local observer can't learn what you're updating, so they can't target you for being out of date



1 Million People use Facebook over Tor

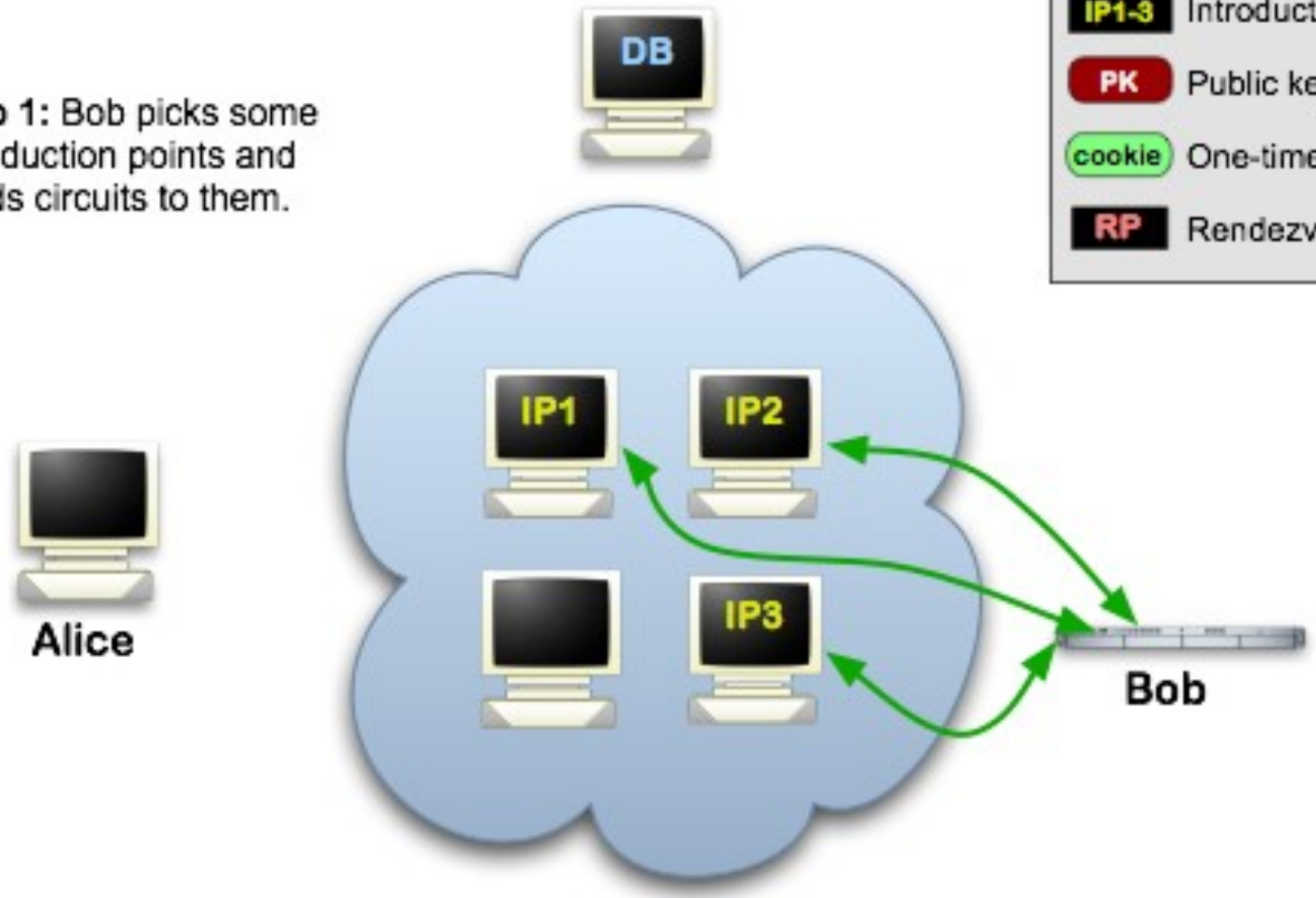
FACEBOOK OVER TOR · FRIDAY, APRIL 22, 2016

People who choose to communicate over Tor do so for a variety of reasons related to privacy, security and safety. As we've written previously it's important to us to provide methods for people to use our services securely – particularly if they lack reliable methods to do so.

This is why in the last two years we built the Facebook onion site and onion-mobile site, helped standardise the ".onion" domain name, and implemented Tor connectivity for our Android mobile app by enabling connections through Orbot.

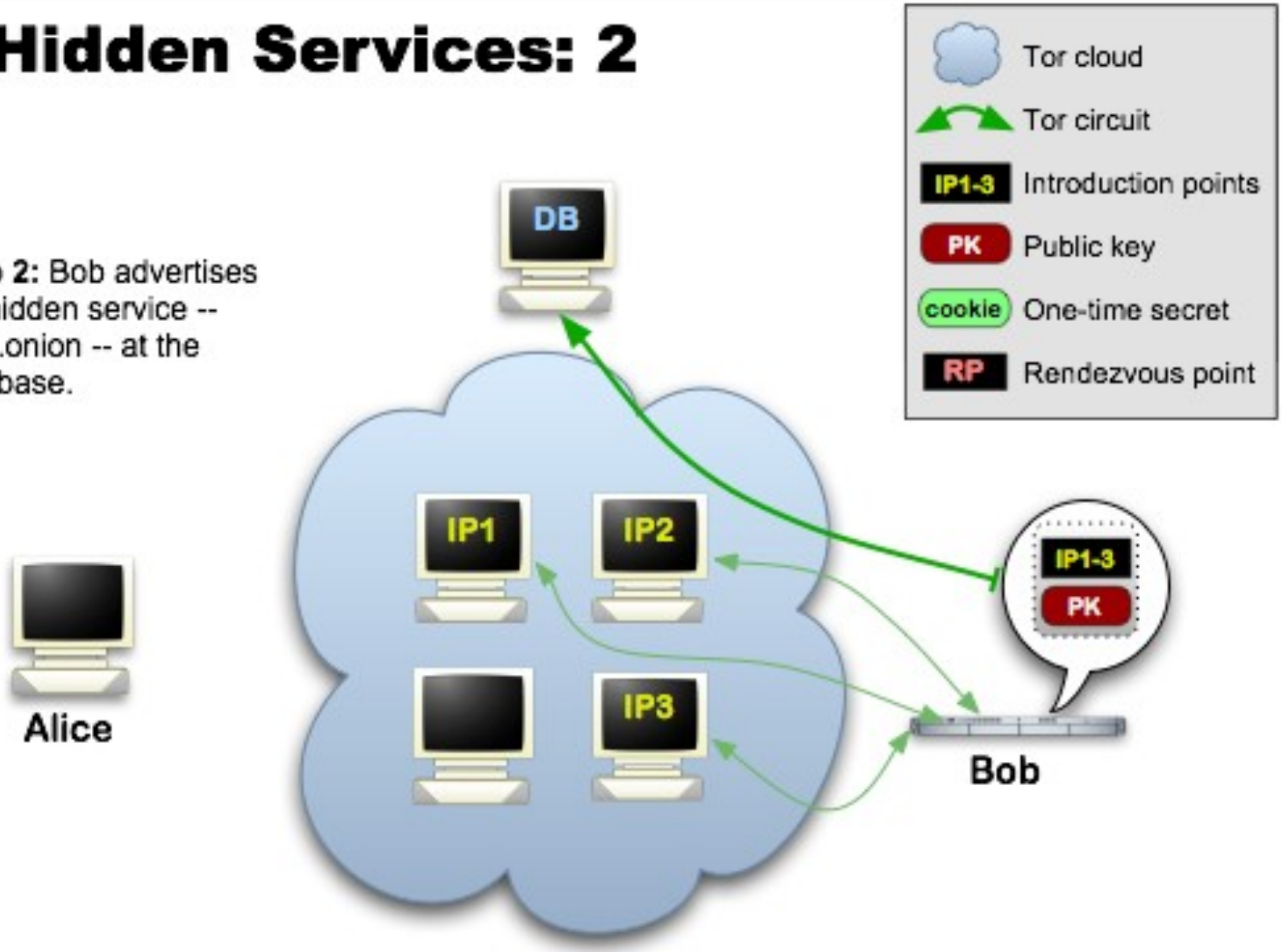
Hidden Services: 1

Step 1: Bob picks some introduction points and builds circuits to them.



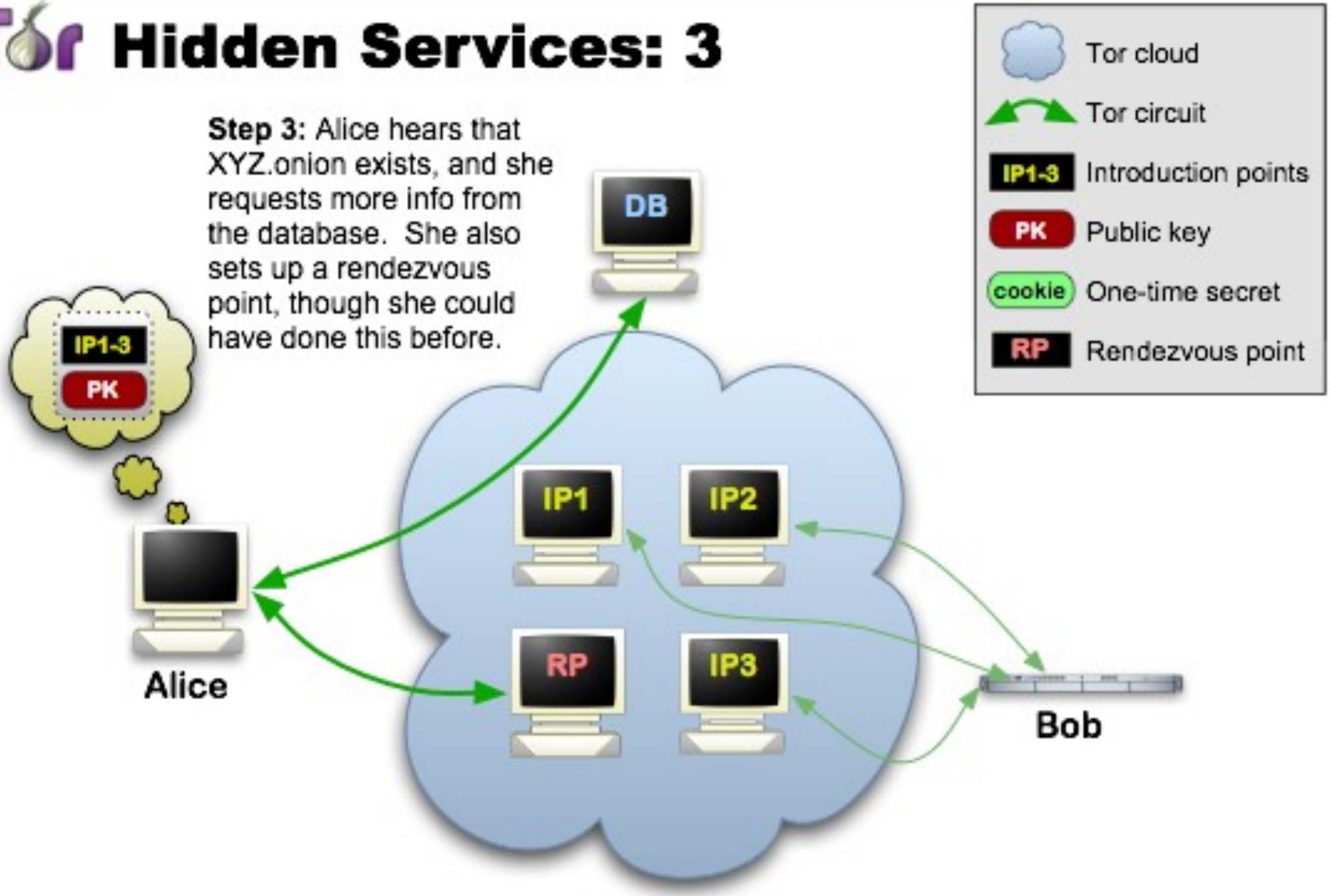
Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.



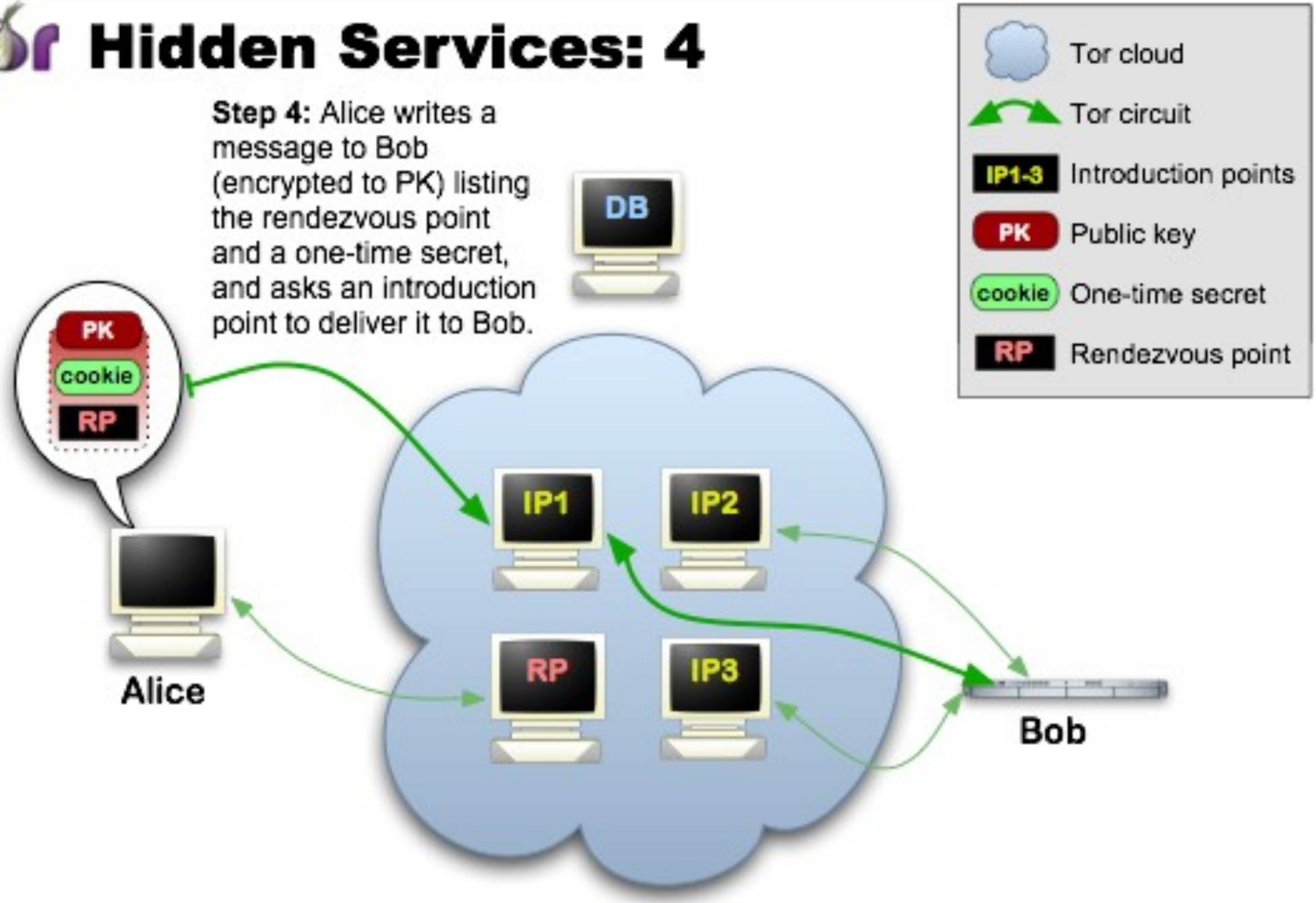
Tor Hidden Services: 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



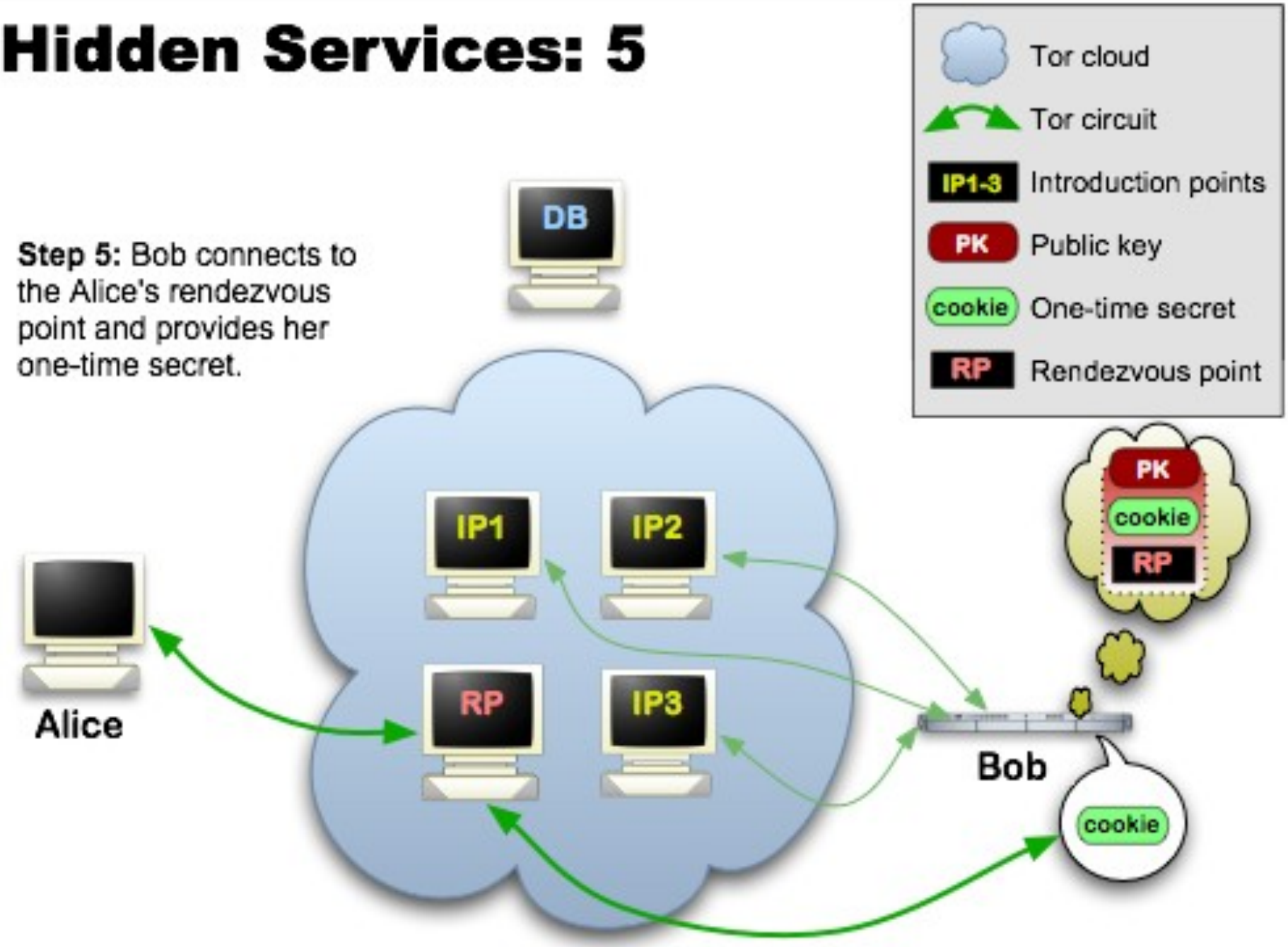
Hidden Services: 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



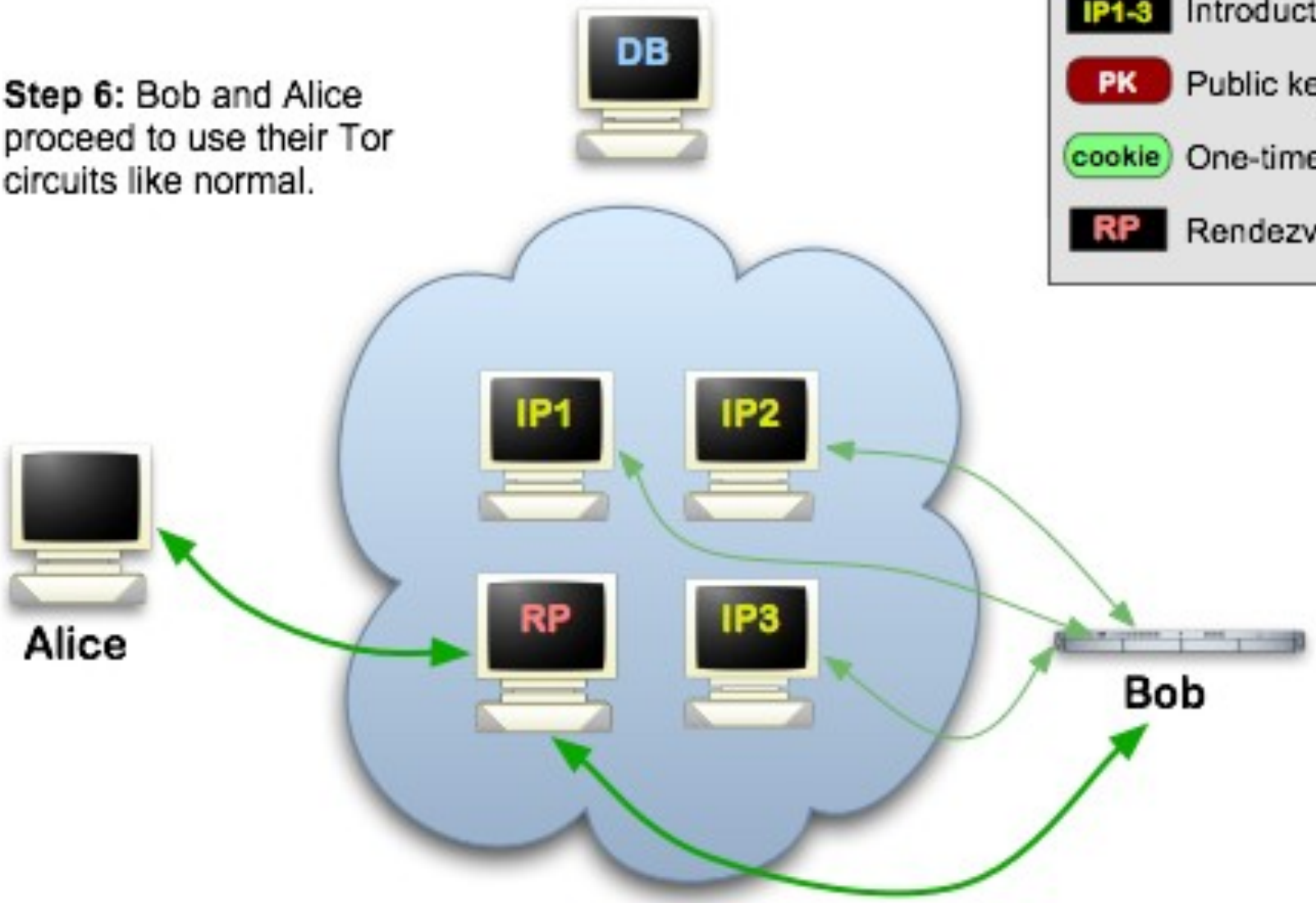
Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



Hidden Services: 6

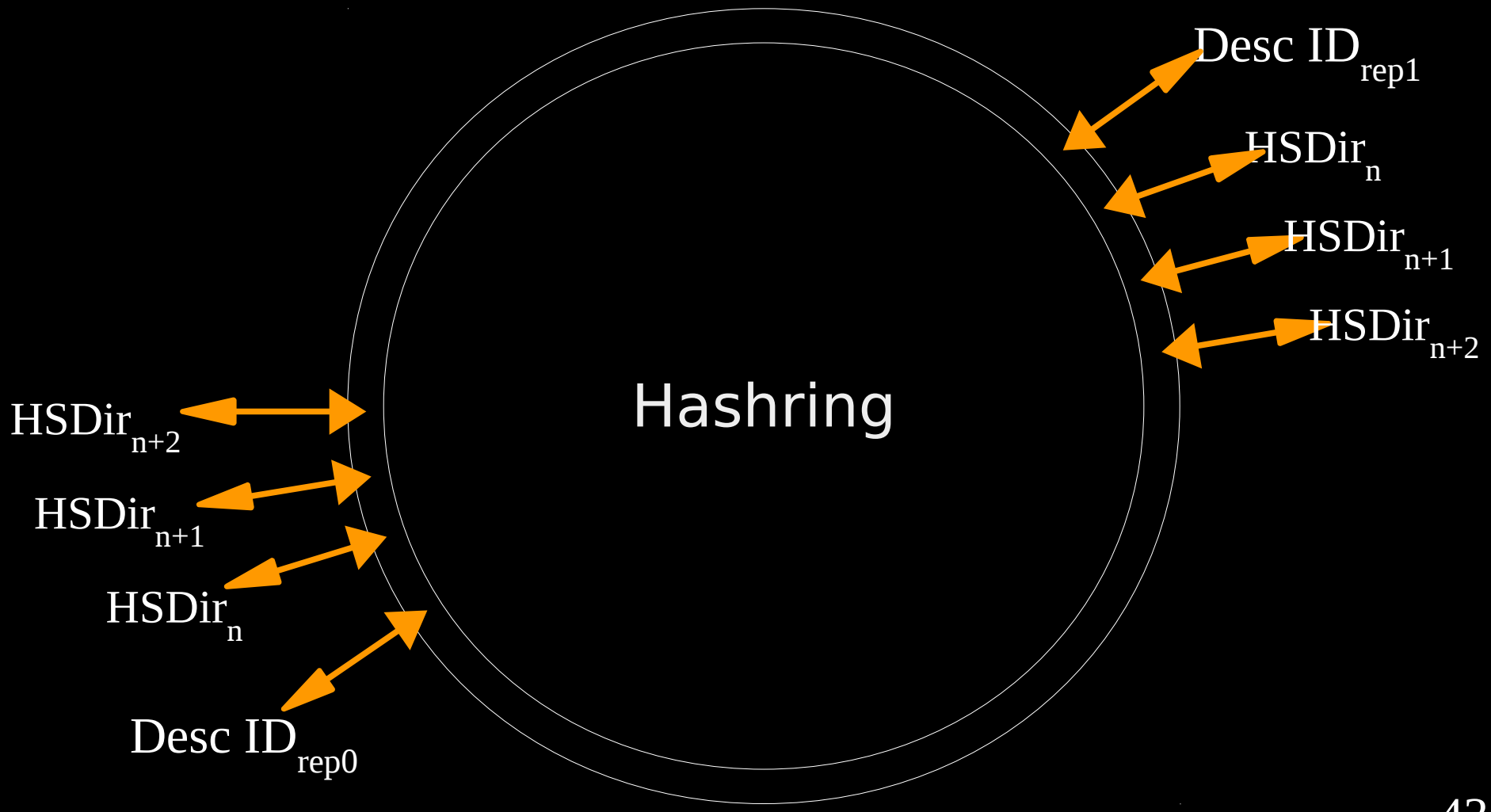
Step 6: Bob and Alice proceed to use their Tor circuits like normal.



- Tor cloud
- Tor circuit
- IP1-3 Introduction points
- PK Public key
- cookie One-time secret
- RP Rendezvous point

HS Directory

Desc ID = H(onion-address | H(time-period | descriptor-cookie | replica))



New keys => longer onion addresses

From 16 characters:

nzh3fv6jc6jskki3.onion

... to 52 characters:

a1uik0w1gmfq3i5ievxdm9ceu27e88g6o7pe0rffdw9jmntwkdsd.onion

(ed25519 public key base32 encoded)

Network-wide shared random value

- The six HSDirs for a given onion address are predictable into the future
- So bad guys can run six relays with just the right keys to target a specific future day...to censor it or to measure popularity
- People – we don't know who – were doing this attack in practice

Network-wide shared random value

- The solution: make the HSDir mapping include a communal random value that everybody agrees about but that nobody can predict
- The directory authorities pick this value each day as part of their consensus voting process

HSDirs get to learn onion addresses

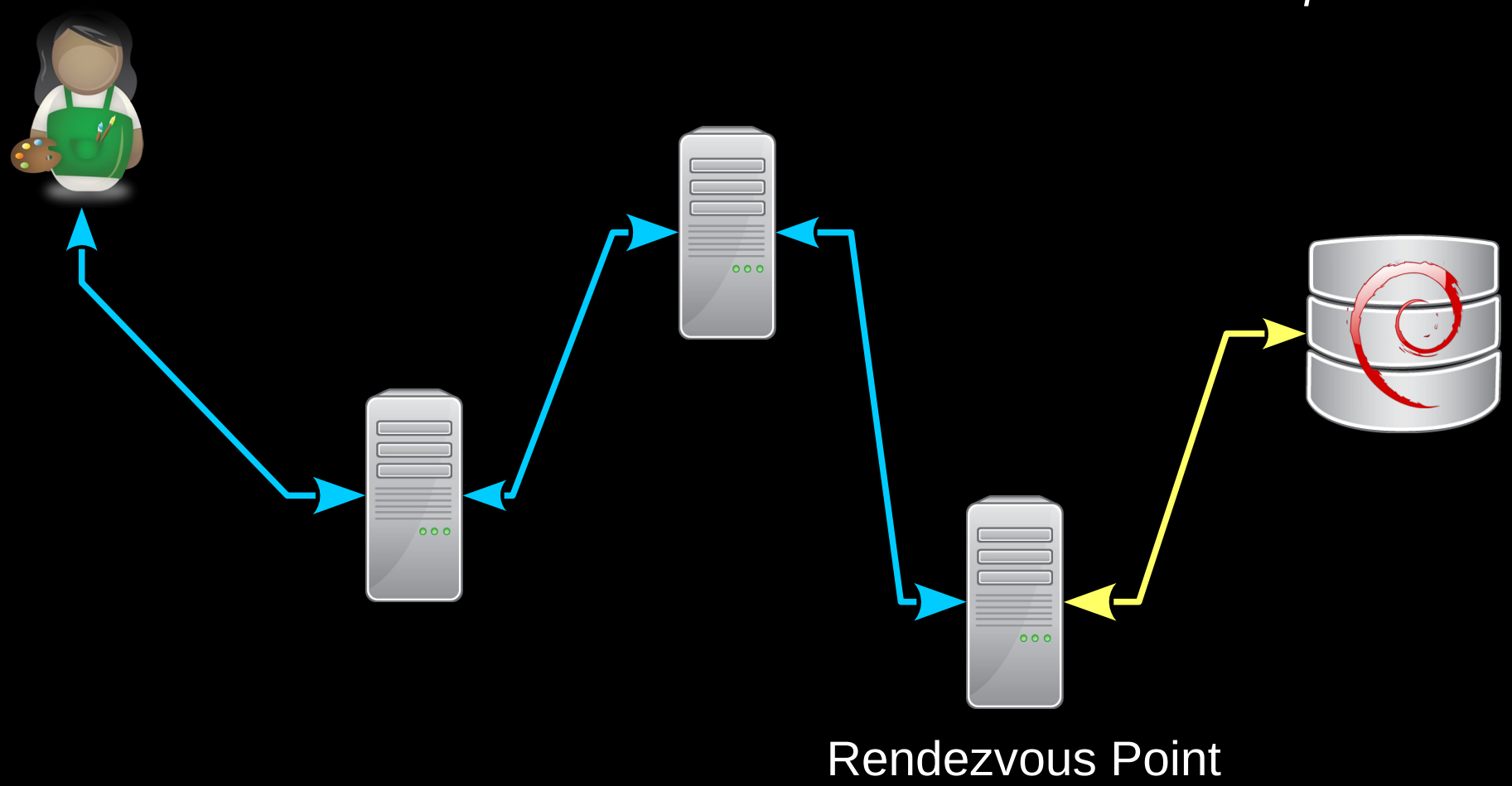
- The onion service descriptor (which gets uploaded to the HSDir) includes the public key for the service (so everybody can check the signature)
- So you can run relays and discover otherwise-unpublished onion addresses
- “Threat intelligence” companies have been trying to do just that

HSDirs get to learn onion addresses

- The solution: the new cryptosystem has a cool feature where you can sign the onion descriptor with a subkey
- So everybody can check the signature but nobody can learn the main key from the subkey
- Should finally kill the arms race with jerks running relays to gather onions

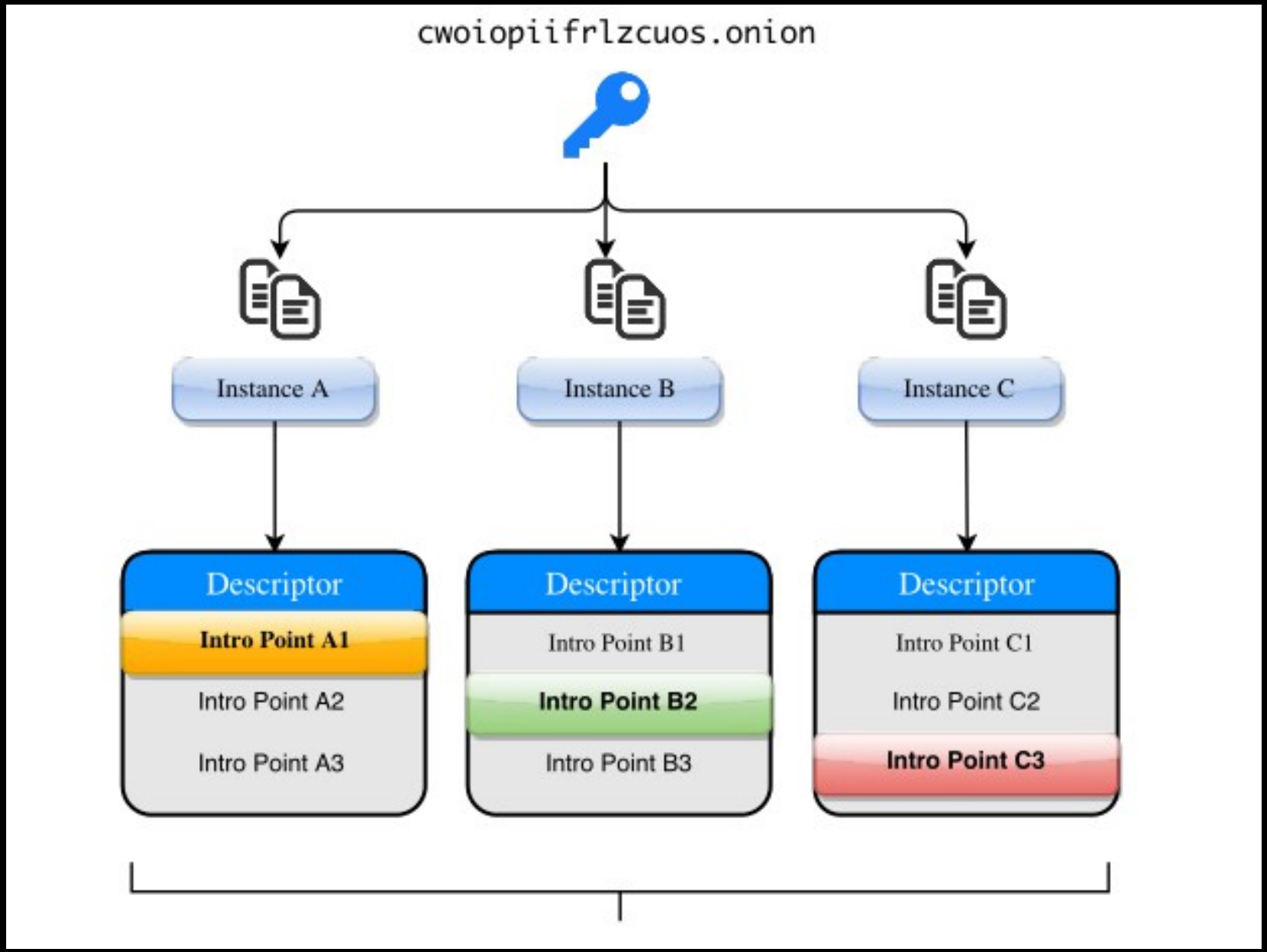
Rendezvous Single Onion Services

Proposal 260



OnionBalance

https://onionbalance.readthedocs.org



Vanguards (Tor proposal 271)

- Tor clients use a single relay (called a Guard) for the first hop in all their paths, to limit exposed surface area
- But there are relatively easy attacks to learn a user's guard, and for onion services that can be especially bad.
- Multiple layers of guards protect better against Sybil+compromise attacks

Deployment timeline

- HSDir side:
- Client side:
- Service side:

Try it at: <git url coming soon>

Tor isn't foolproof

- Opsec mistakes
- Browser metadata fingerprints
- Browser exploits
- Traffic analysis

“Still the King of high secure,
low latency Internet Anonymity”

“There are no contenders for the throne”