TOR – The Onion Router

St. Louis Unix User's Group
11 May 2022
Lee Lammert
Omnitec Corporation

Brief History of TOR

- Mid 90’s US Naval Research Lab idea of “onion routing” to protect intelligence communications online
- 1997 assigned to DARPA
- Alpha release 20 September 2002
- Second generation released 13 Aug 2004
- 2006 Founding of the TOR project a 501(c)(3) foundation. Funding from the EFF and others
- US Government is the primary sponsor now: www.whoishostingthis.com/blog/2014/11/17/who-funded-tor/

Notable TOR Details

- Arguably made possible the efforts of Edward Snowden in 2013
- Lots of details on Wikipedia

  https://en.wikipedia.org/wiki/Tor_(anonymity_network)
- 2013 Detailed Analysis, the Egotistical Giraffe:

  www.eff.org/files/2014/04/09/20131004-guard-egotistical_giraffe.pdf
- Many other applications for human rights, ..

Real world uses for TOR

The Tor network is used by all kinds of people around the world; anyone with a need or desire to protect their online privacy.

Regular Internet users who want to keep their emails private or protect their children from online predators use Tor to retain their anonymity.

Citizens of countries who censor the Internet use Tor to access blocked news or social media sites, or research sensitive information on topics like AIDs or birth control that may not be available elsewhere.

Journalists, bloggers, and human rights activists use Tor to protect themselves from retaliation from governments or employers.

And whistleblowers use Tor to keep safe when reporting corruption.

Issues today

Very current example – Roe v. Wade

- Leaked supreme court opinion reported by Propublica:

  http://propub3r6espa33w.onion/

- Searching for clinics or other information:

  Various tracking software has started ***selling*** data
  about user searches to troll for suit candidates using the new
  Texas laws!

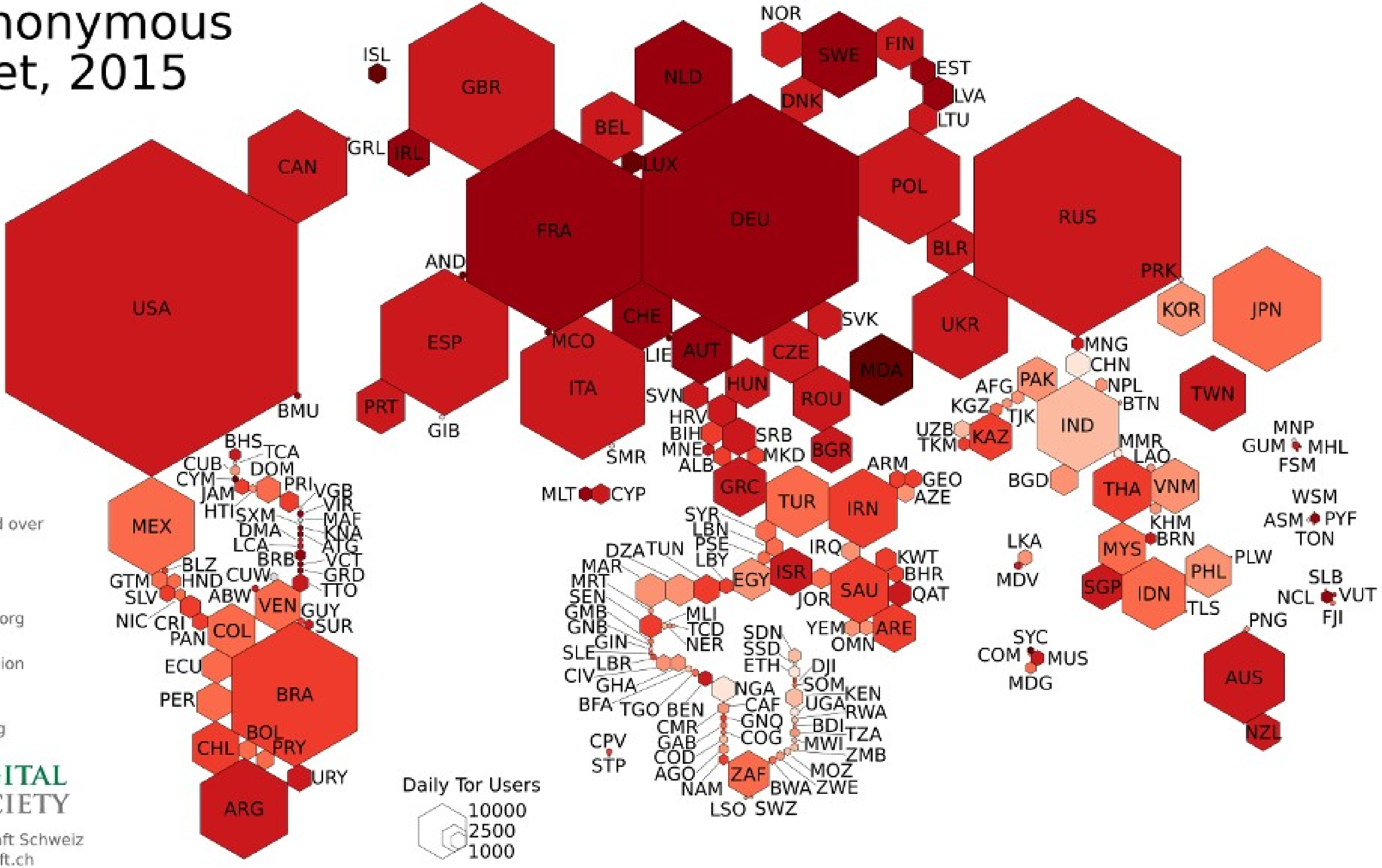
Solution:

TOR Browser

The Anonymous Internet, 2015

Daily Tor users per 100'000 Internet users

■	> 300
■	200-300
■	100-200
■	50-100
■	25-50
■	10-25
■	5-10
□	< 5
■	no info



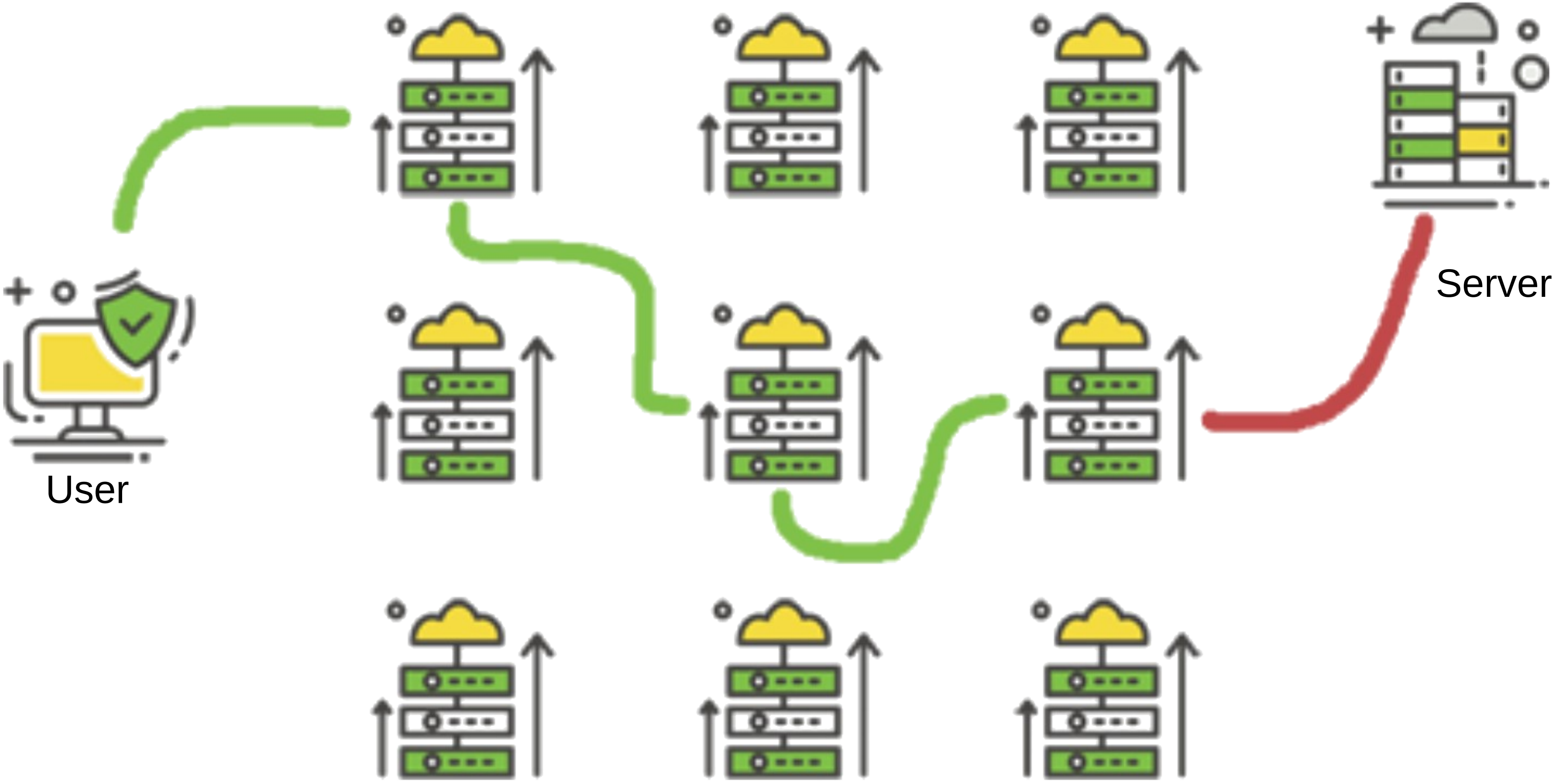
Tor users averaged over the year 2015.

Data sources:
Tor Metrics Portal
metrics.torproject.org
International Telecommunication Union
itu.org
World Bank
data.worldbank.org

DIGITAL SOCIETY

Digitale Gesellschaft Schweiz
digitale-gesellschaft.ch

How does TOR work?



Tor provides

- Connection similar to a VPN, but anonymous
  - No fixed entry endpoint
  - Routing is random and unpredictable
  - No traffic *profiling*
- Downside?
  - Performance (significant degradation)
  - Any IP-based authentication is invalid
  - If using a browser, it must be securable (i.e. no Chrome!)
  - No JS or script allowed

Browser or Service

- Tor Browser for ad-hoc connections
  - Firefox + TOR Client = Tor Browser
  - Significant privacy tool for public connections
  - Works even inside restrictive countries
- *Onion Services* to create a TOR *endpoint*
  - Users can connect to your endpoint with a high degree of anonymity and privacy
  - Traffic is encrypted, and the contents are also likely encrypted (e.g. SSL/TLS)

Installing a TOR Browser

- Package (SuSE):

```
S | Name                         | Summary                                            | Type
--+------------------------------+----------------------------------------------------+--------
  | torbrowser-apparmor-profile | Apparmor profile for Tor Browser                   | package
  | torbrowser-launcher          | Tool for launching and easy-updates of Tor Browser | package
  | torbrowser-launcher-lang     | Translations for package torbrowser-launcher       | package
```

- Download:

https://www.torproject.org/download/

- Container:

https://hub.docker.com/search?q=torbrowser&type=image

Tor Browser

- Demo

TOR Browser Issues

- TOR → Browsing the public Internet DOES create a issue
  - An *Exit Node* is required
  - Once discovered, exiting traffic ***can*** be profiled
  - By comparing profiles across multiple exit nodes, it ***is*** possible to learn more about the traffic
  - More details available on Wikipedia
- Be sure to update on a regular basis
- Many public websites/services have issues with anonymous users, so YMMV

Onion Services

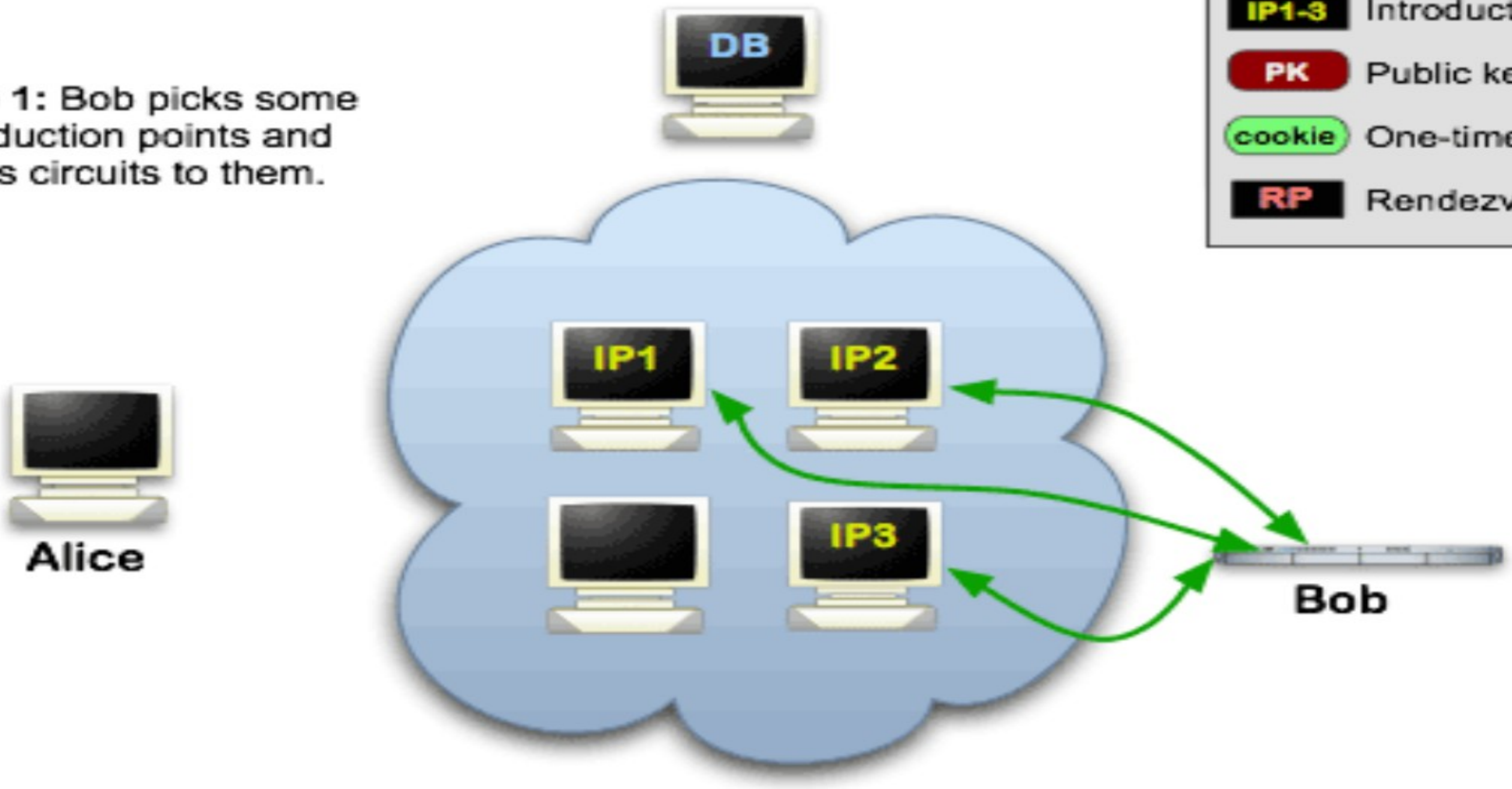
- Provides secure connection between ***any*** TOR ***nodes***
- Uses TOR Onion Services for transport
- All traffic internal to the TOR network
- Does ***<u>NOT</u>*** require an exit node, so very secure
- Many tools to use: torify with a normal program (e.g. ssh); torsocks to communicate directly over the TOR network

Who uses Onion Services?

- The New York Times https://www.nytimes3xbfgragh.onion/
- The Guardian's secure drop: 33y6fjyhs3phzfjj.onion
- Propublica: http://propub3r6espa33w.onion/
- Facebook: https://facebookcorewwwi.onion/
- Protonmail: https://protonirockerxow.onion/
- Riseup: vww6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd.onion

Onion Services: Step 1

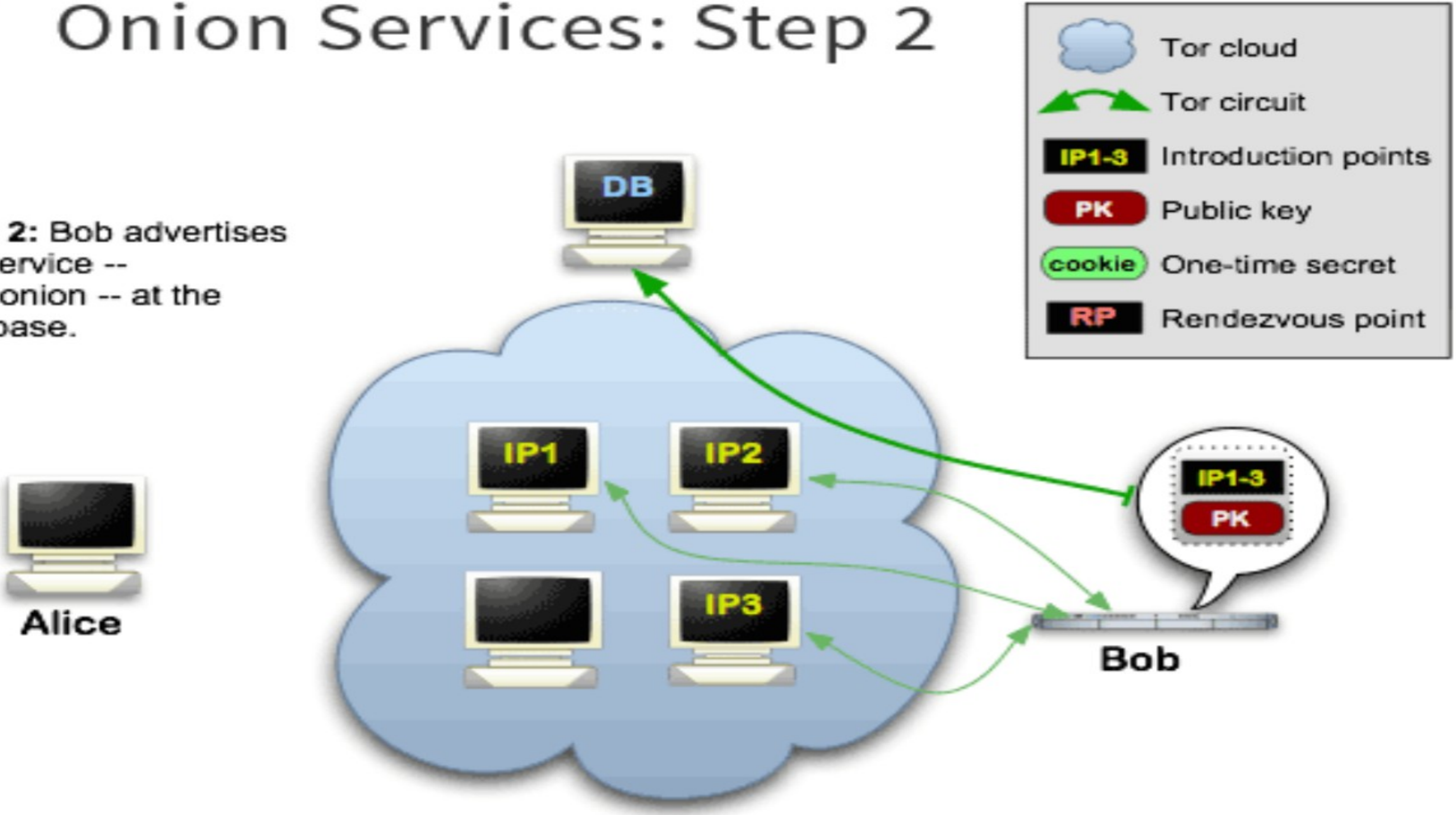
Step 1: Bob picks some introduction points and builds circuits to them.



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

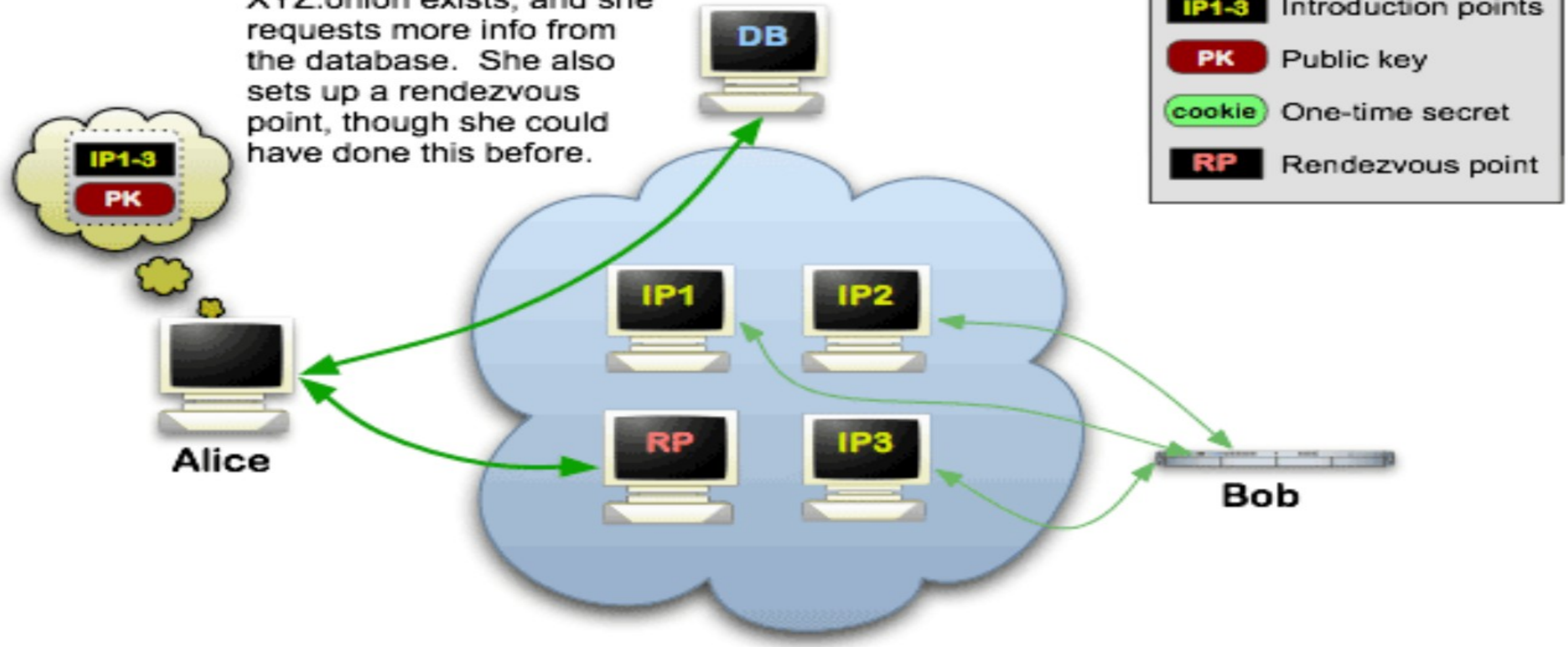
Onion Services: Step 2

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



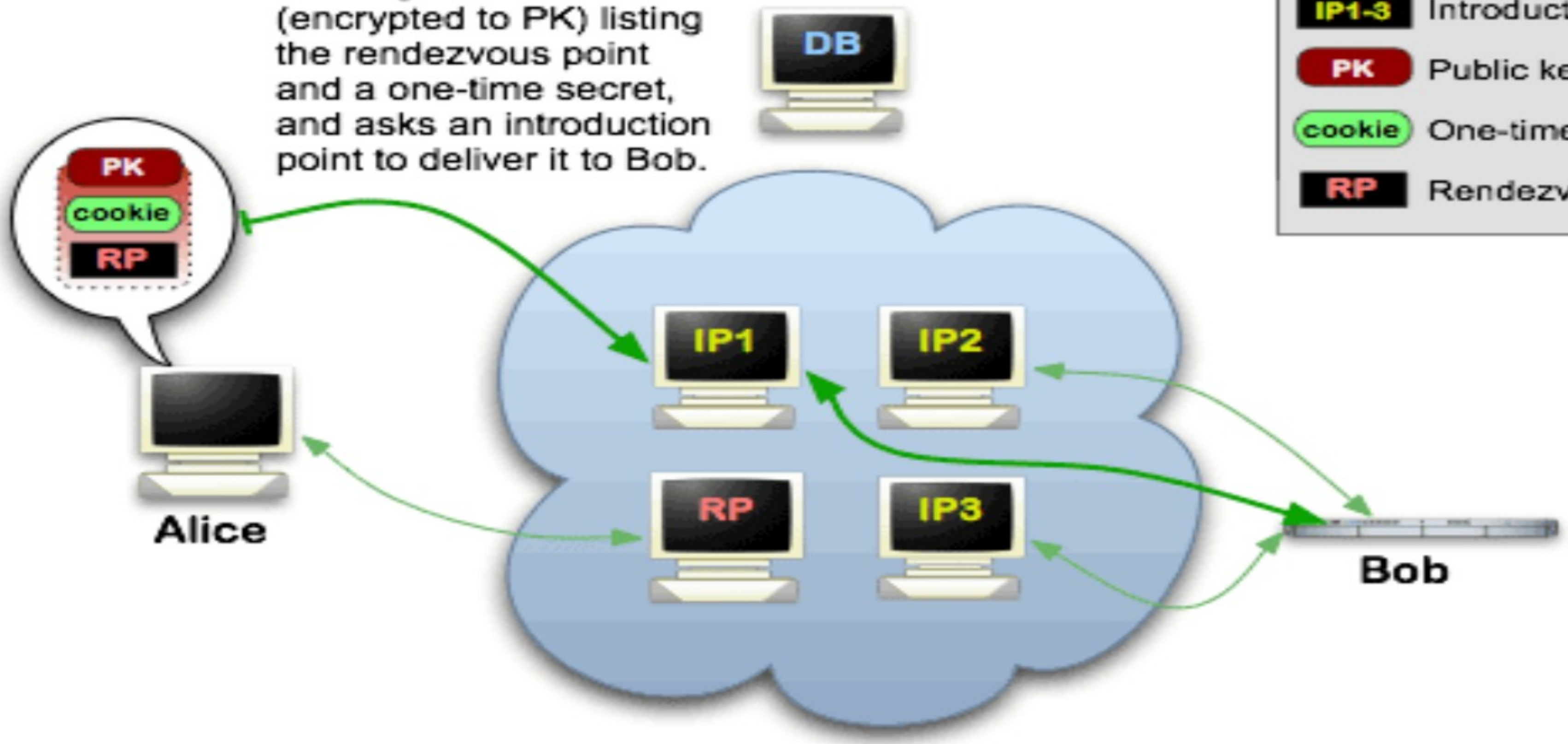
Onion Services: Step 3

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.



Tor Onion Services: Step 4

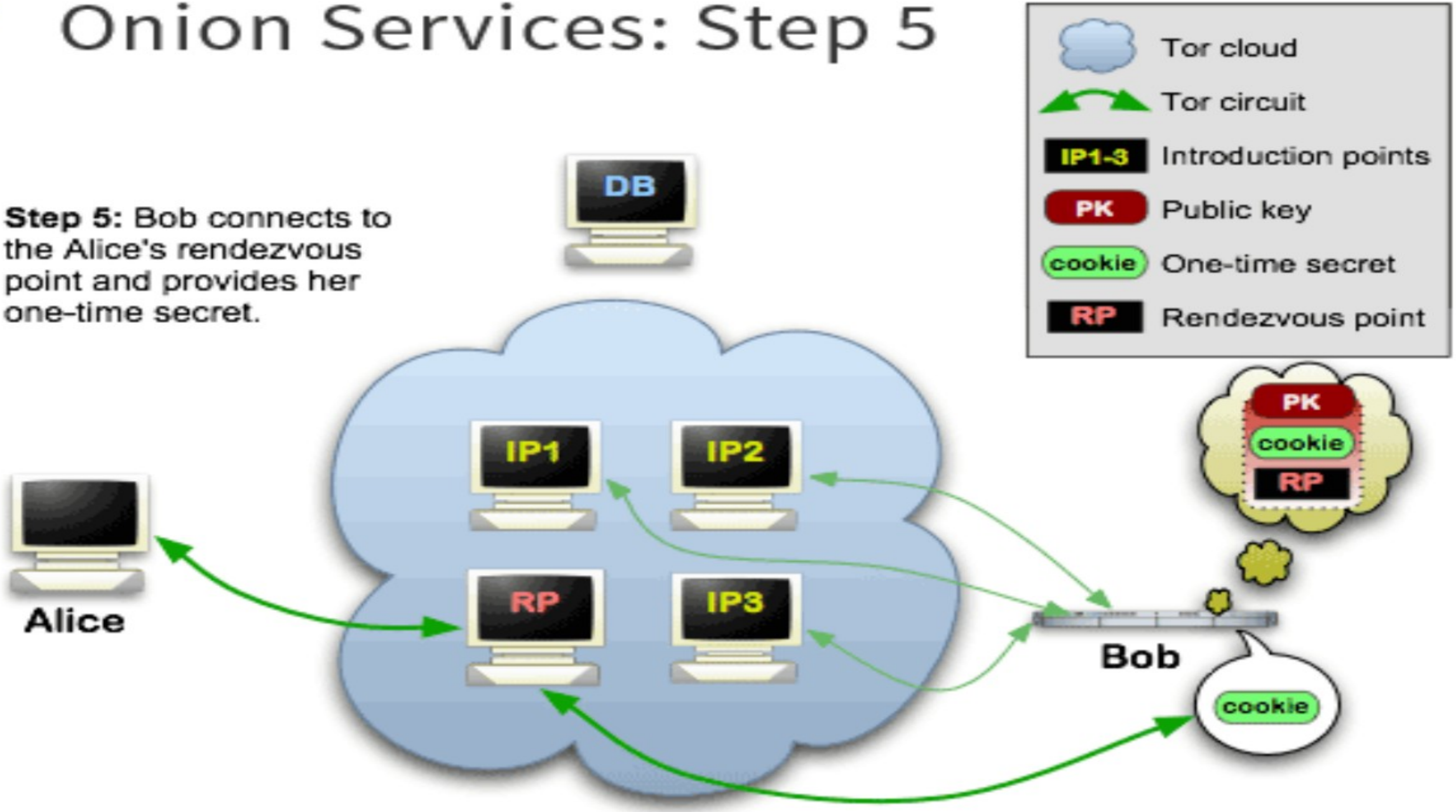
Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



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

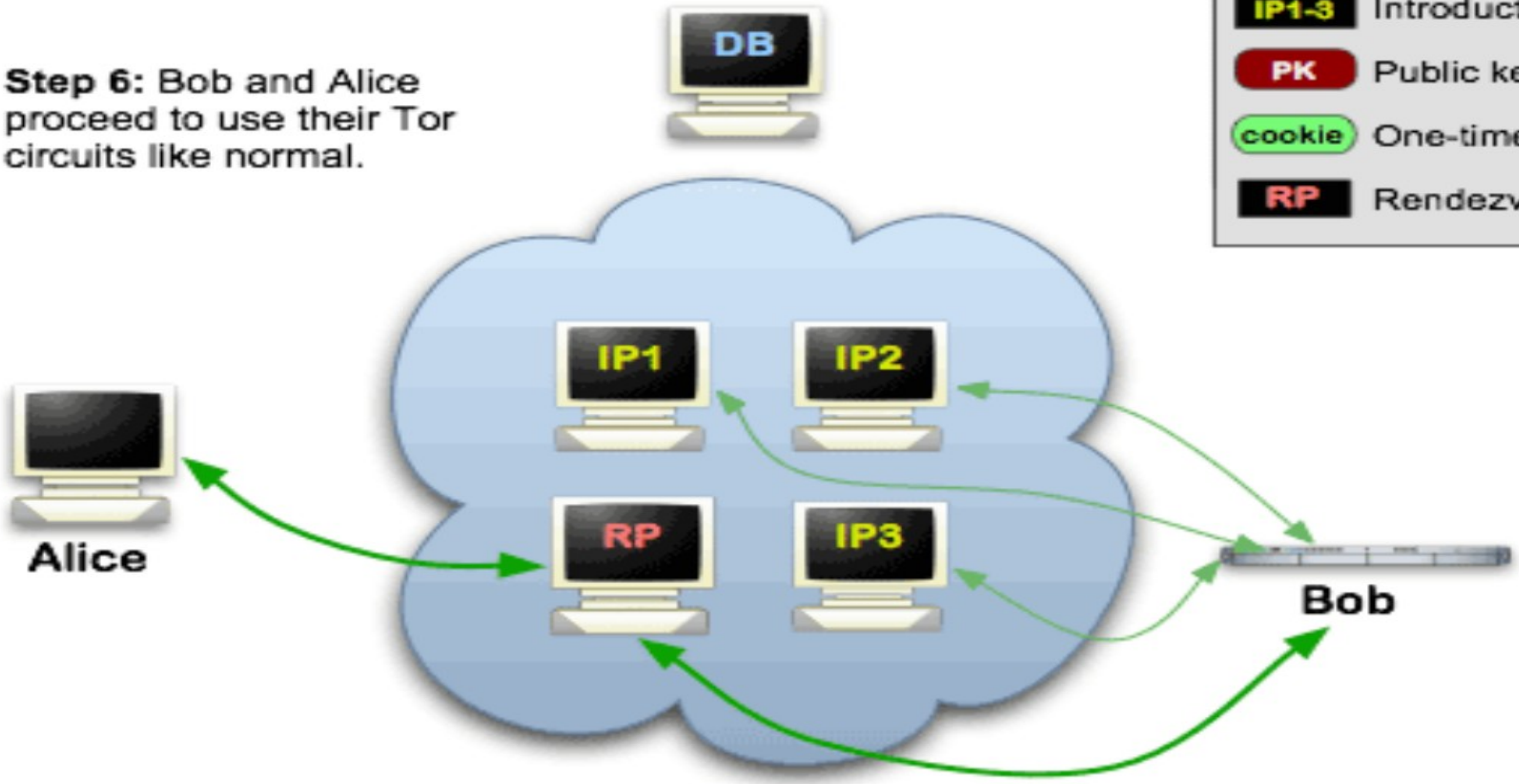
Onion Services: Step 5

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



Onion Services: Step 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

TOR *Onion Services*

- Debian:

  https://www.torproject.org/docs/debian.html.en

- SuSE:
  - zypper in tor
- Default “hidden_service” /etc/tor/torrc:

```
#HiddenServiceDir /var/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80
```

Configure tor

- ssh:

```
HiddenServiceDir /var/lib/tor/tor_hidden_service
HiddenServicePort 2206 127.0.0.1:2206
```

- Start the service:

```
systemctl start tor
```

- What is our Onion hostname?

```
cat /var/lib/tor/hidden_service/hostname
```

Using Onion Services

- Torify; Torification: Generic term, also proxification, socksification or transsocksification
- Simplest use:

```
torify <    application
```

Test!

- torify ssh lvl@___________.onion
- Connected! Anonymously!
- Secure tunnel point-to-point!

Resources

- TOR Project: *https://www.torproject.org/docs/onion-services.html.en* *https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf*
- TOR Onion Services: *https://www.youtube.com/watch?v=wHmxCeLpveA* https://medium.com/@tzhenghao/how-to-ssh-over-tor-onion-service-c6d06194147

Credits

- *Presentation graphics:*

  Andrew Denner,
  Central Iowa Linux Users Group (CIALUG)

Thank you!

OMNITEC Corporation

Lee Lammert *lvl@omnitec.net*