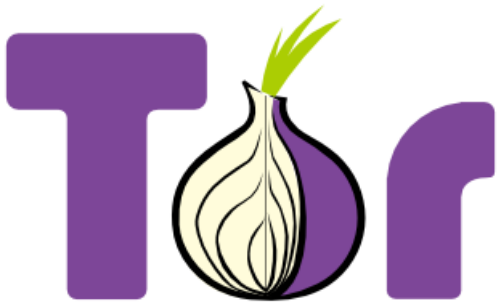
BBC Tor Overview

Andrew Lewman
andrew@torproject.org

March 7, 2011



What are we talking about?

- Crash course on anonymous communications
- Quick overview of Tor
- Quick overview of Tor Hidden Services
- Future directions

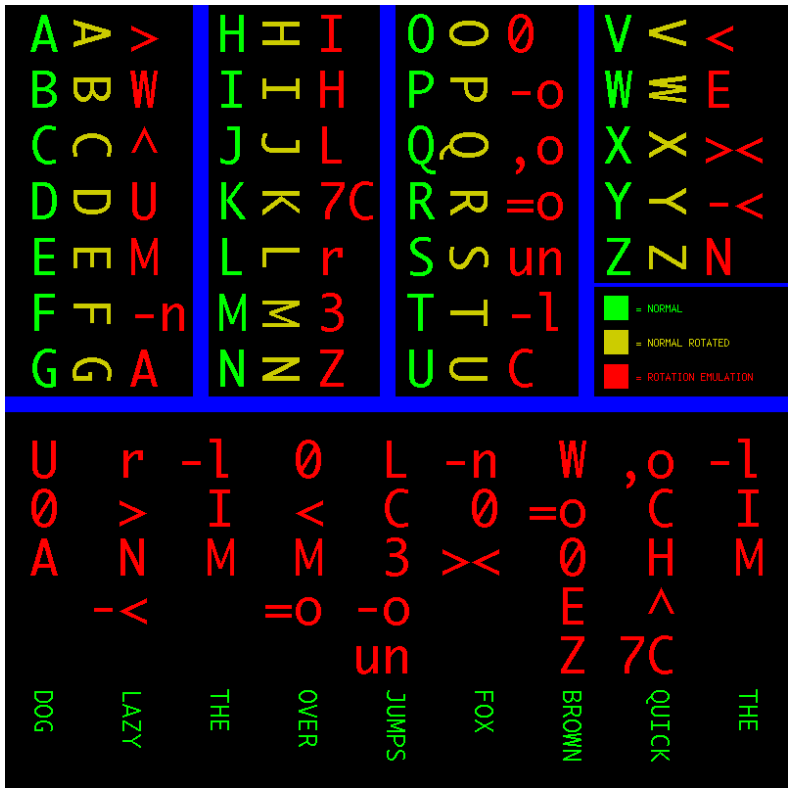
The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy

What is anonymity?

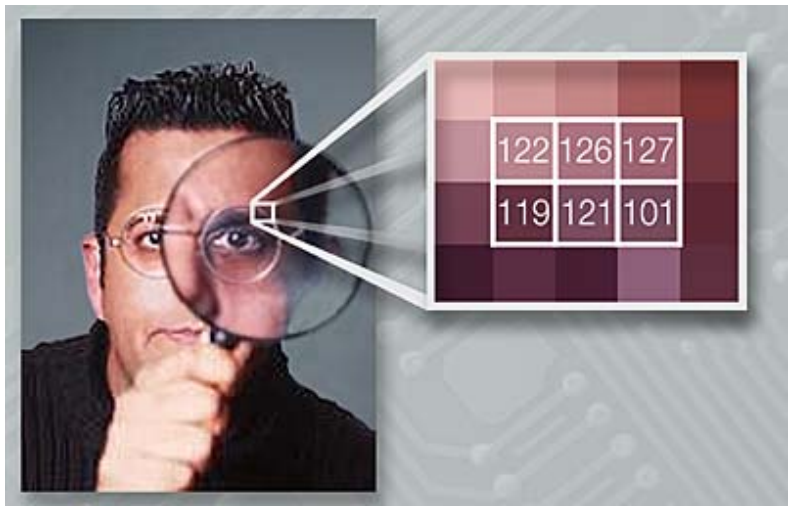
Anonymity isn't cryptography

- Cryptography protects the contents in transit
- You still know who is talking to whom, how often, and how much data is sent.



Anonymity isn't steganography

Attacker can tell Alice is talking to someone, how often, and how much data is sent.



Anonymity isn't just wishful thinking...

- "You can't prove it was me!"

Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"

Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"

Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"
- "Promise you won't tell"

Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"
- "Promise you won't tell"
- "I didn't write my name on it!"

Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"
- "Promise you won't tell"
- "I didn't write my name on it!"
- "Isn't the Internet already anonymous?"

..since "weak" isn't anonymity.

- *"You can't prove it was me!"* Proof is a very **strong** word. Statistical analysis allows suspicion to become certainty.

..since "weak" isn't anonymity.

- *"You can't prove it was me!"* Proof is a very **strong** word. Statistical analysis allows suspicion to become certainty.
- *"Promise you won't look/remember/tell"* Will other parties have the abilities and incentives to keep these promises?

..since "weak" isn't anonymity.

- *"You can't prove it was me!"* Proof is a very **strong** word. Statistical analysis allows suspicion to become certainty.
- *"Promise you won't look/remember/tell"* Will other parties have the abilities and incentives to keep these promises?
- *"I didn't write my name on it!"* Not what we're talking about.

..since "weak" isn't anonymity.

- *"You can't prove it was me!"* Proof is a very **strong** word. Statistical analysis allows suspicion to become certainty.
- *"Promise you won't look/remember/tell"* Will other parties have the abilities and incentives to keep these promises?
- *"I didn't write my name on it!"* Not what we're talking about.
- *"Isn't the Internet already anonymous?"* Nope!

Anonymous communication

- People have to hide in a crowd of other people ("anonymity loves company")
- The goal of the system is to make all users look as similar as possible, to give a bigger crowd
- Hide who is communicating with whom
- Layered encryption and random delays hide correlation between input traffic and output traffic

Low versus High-latency anonymous communication systems

- Tor is not the first system; ZKS, mixmaster, single-hop proxies, Crowds, Java Anon Proxy.
- Low-latency systems are vulnerable to end-to-end correlation attacks.
- High-latency systems are more resistant to end-to-end correlation attacks, but by definition, less interactive.

Low-latency systems are generally more attractive to today's user

- Interactive apps: web, instant messaging, VOIP, ssh, X11, cifs/nfs, video streaming (millions of users)
- Multi-hour delays: email, nntp, blog posting? (tens of thousands of users?)

Low-latency systems are generally more attractive to today's user

- Interactive apps: web, instant messaging, VOIP, ssh, X11, cifs/nfs, video streaming (millions of users)
- Multi-hour delays: email, nntp, blog posting? (tens of thousands of users?)
    - And if anonymity loves company...

What is Tor?

- online anonymity software and network

What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)

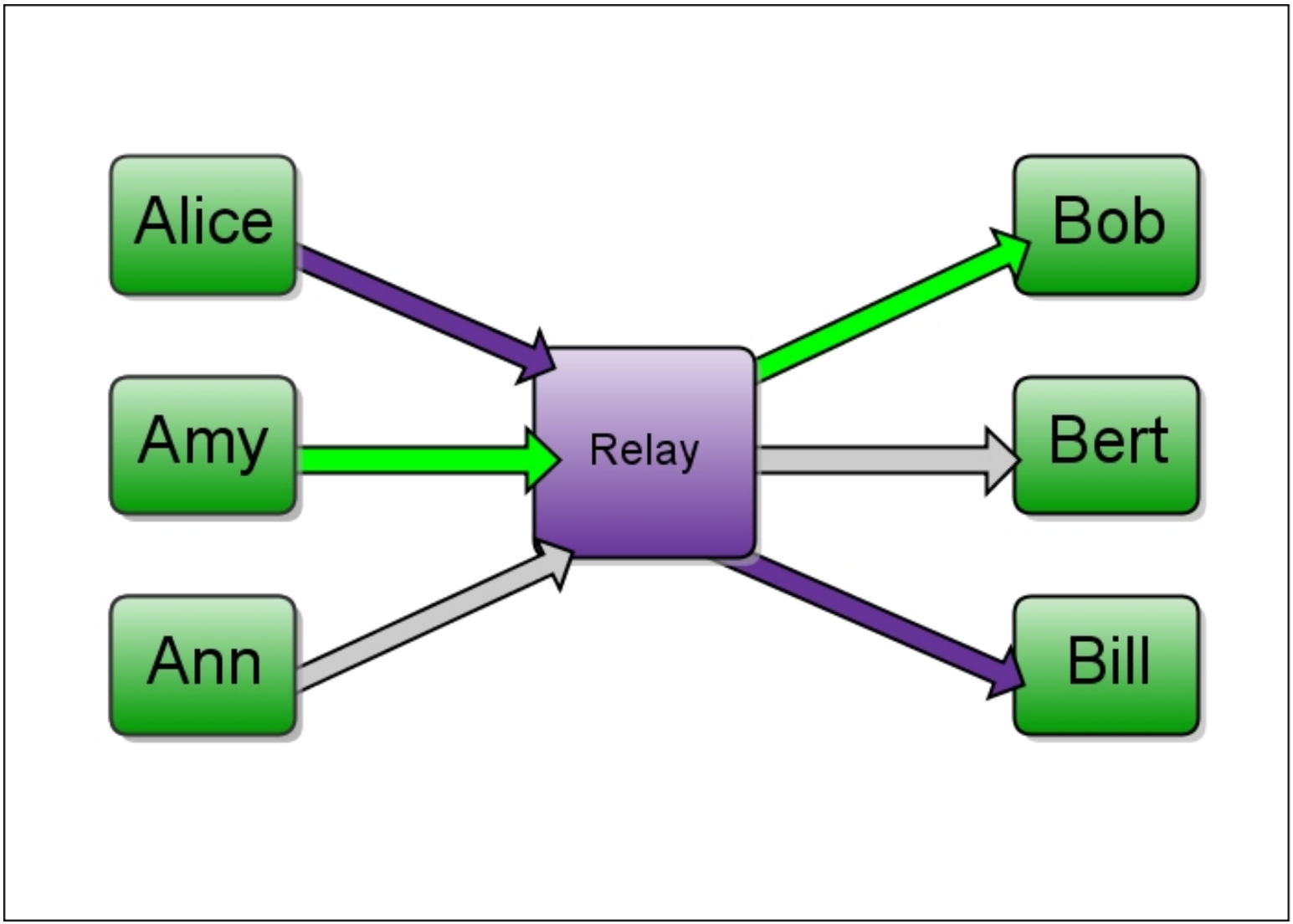
What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech

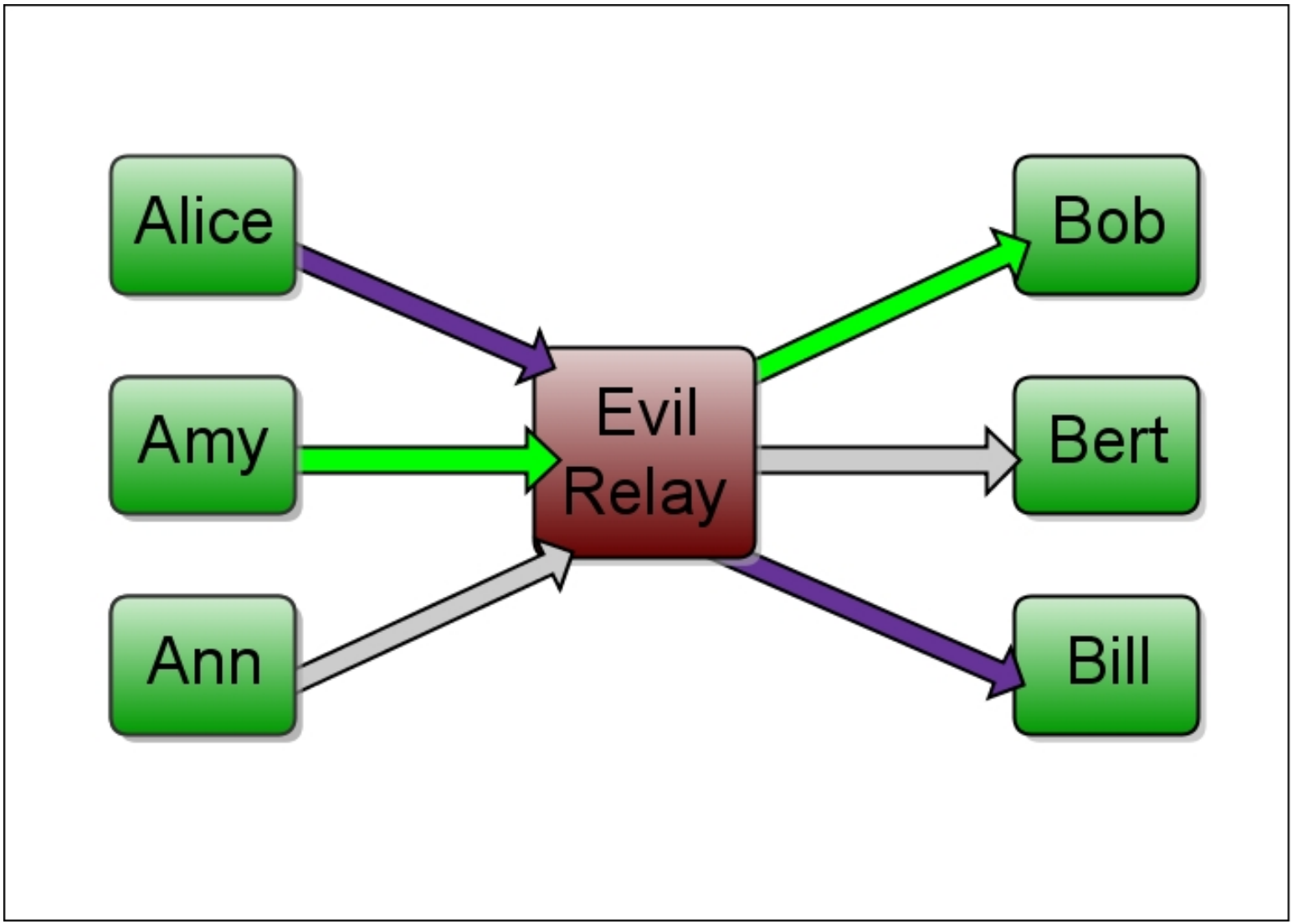
What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech
- increasingly diverse toolset:
  Tor, Torbutton, Tor Browser Bundle, TA(I)LS LiveCD, Tor Weather, Tor auto-responder, Secure Updater, Orbot, Torora, Tor Check, Arm, Nymble, Tor Control, Tor Wall, TorVM

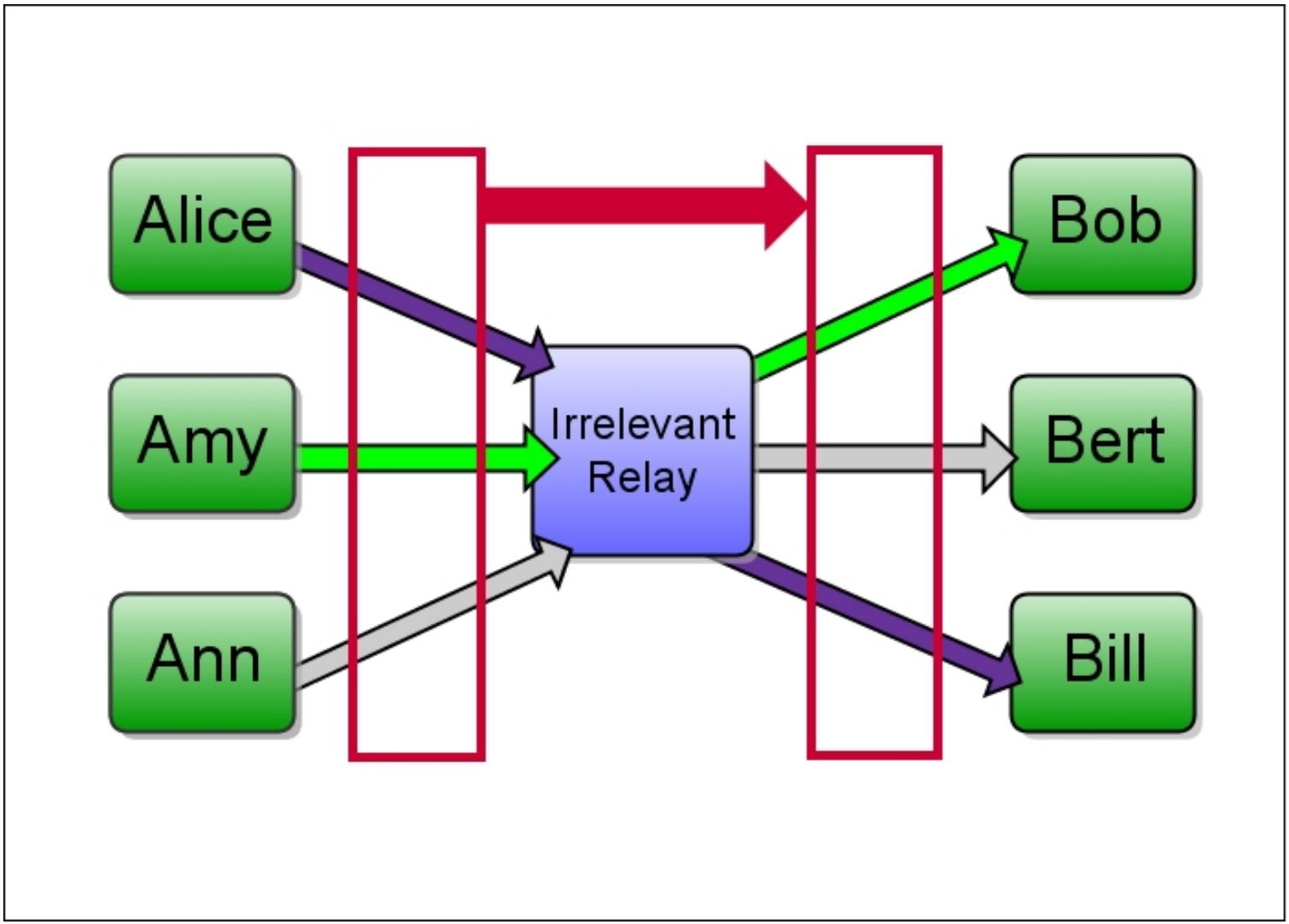
How is Tor different from other systems?



How is Tor different from other systems?



How is Tor different from other systems?



Twitter in Iran: Good.

Iran Protests: Twitter, the Medium of the Movement

By **LEV GROSSMAN** Wednesday, Jun. 17, 2009

Related

Photos

Behind the Scenes with Mousavi

Stories

- In Iran, Rival Regime Factions Play a High-Stakes Game of Chicken
- Latest Tweets on Fallout from Iran's

MORE

Share The U.S. State Department doesn't usually take an interest in the maintenance schedules of dotcom start-ups. But over the weekend, officials there reached out to Twitter and asked them to delay a network upgrade that was scheduled for Monday night. The reason? To protect the interests of

From http://www.time.com/time/world/article/0,8599,1905125,00.html

Twitter in USA: Bad.

FBI Raids Queens Home in G20 Protest Twitter Crackdown

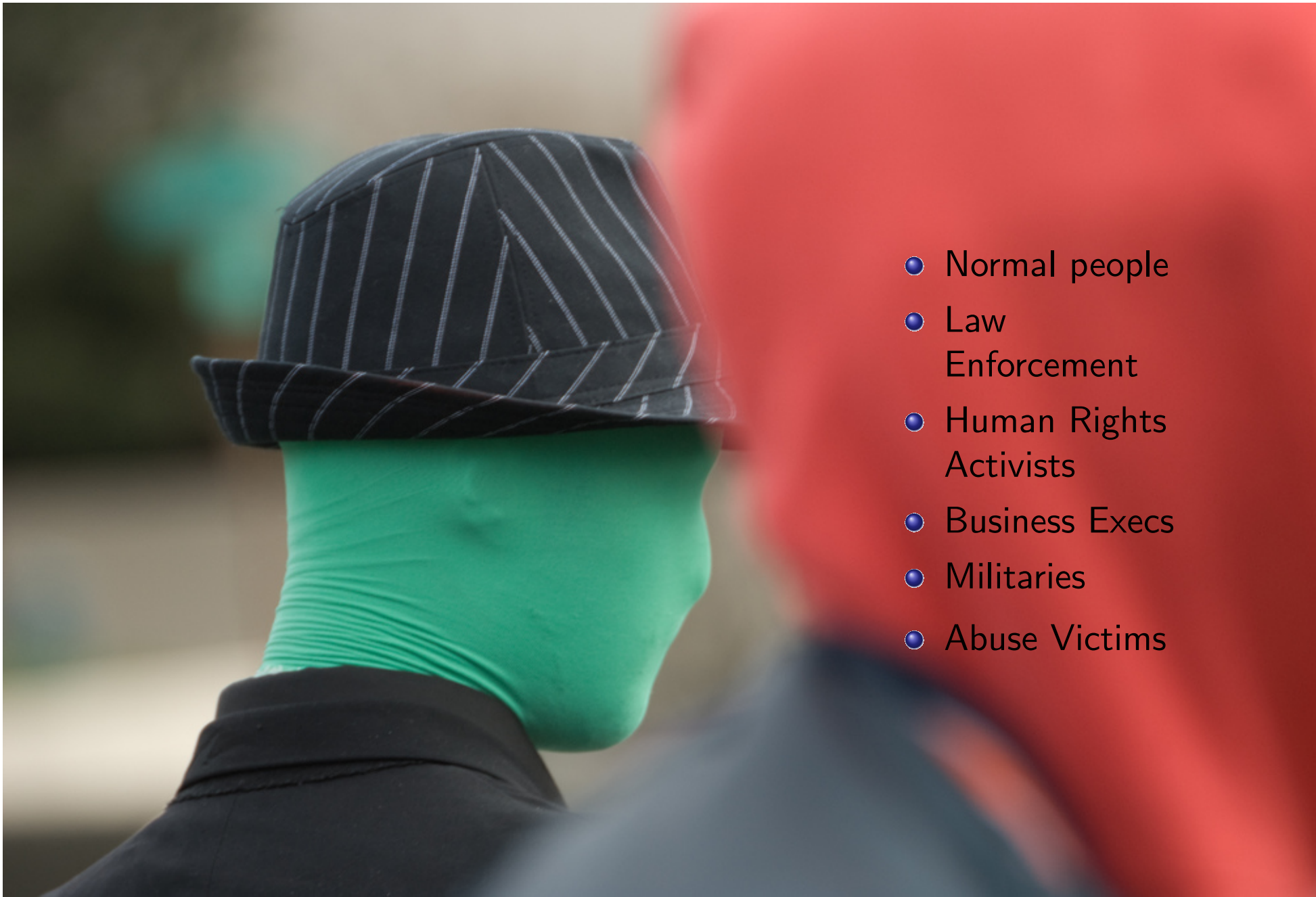
AP Photo/Matt Rourke

That's right, a Twitter crackdown. A lawyer for Jackson Heights social worker Elliot Madison, 41, says that the feds searched his client's house for 16 hours on Thursday after Madison was arrested on September 24th at a Pittsburgh hotel room with another man. What were they up to? Sitting at laptops sending Twitter messages advising G20 demonstrators about riot police activity in the streets. And yet *real* Twitter threats like Lindsay Lohan and Courtney Love remain at large.

Madison, a self-described anarchist, was in Pittsburgh volunteering for the Tin Can Comms Collective, a group that uses Twitter to send mass text messages during protests describing events observed on the streets or over police scanners; stuff like "SWAT teams rolling down 5th Ave." Tin Can was active during the St. Paul RNC protests, and the authorities are now on to them. Madison was charged with hindering apprehension or prosecution, criminal use of a communication facility and possession of instruments of crime; he's currently out on bail.

from http://gothamist.com/2009/10/05/fbi_raids_queens_home_in_g20_protes.php

Who uses Tor?



- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims

estimated 300k to 800k daily users

Tor hides communication patterns by relaying data through volunteer servers

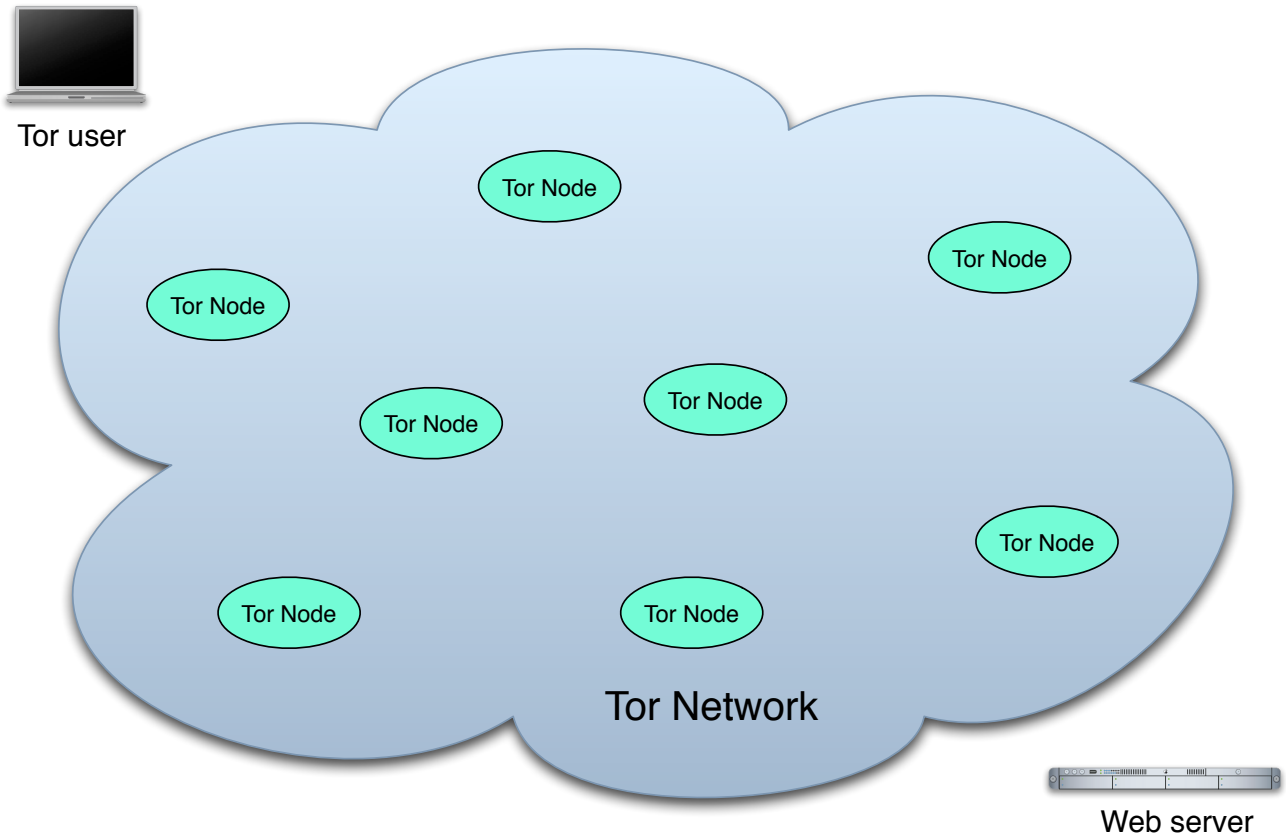


Diagram: Robert Watson

Tor hides communication patterns by relaying data through volunteer servers

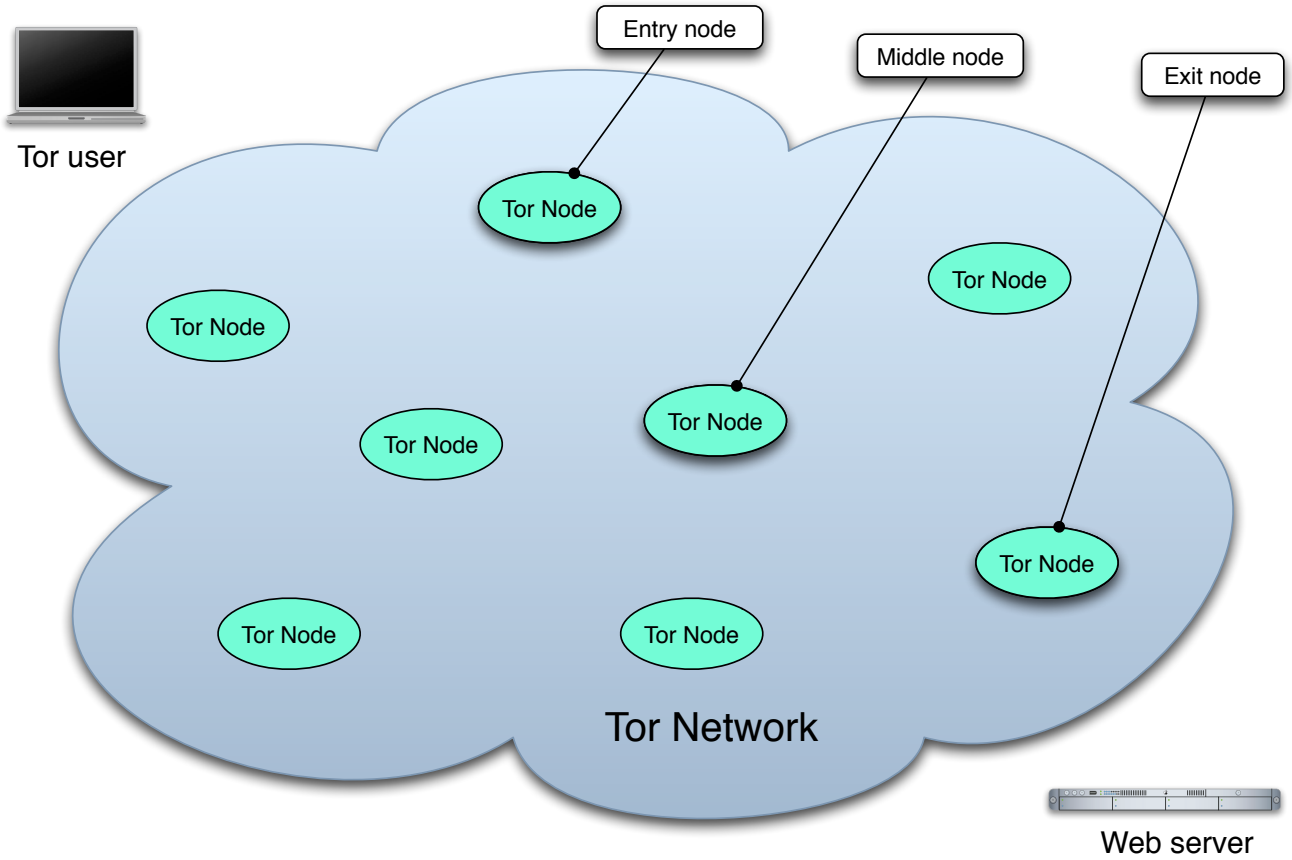


Diagram: Robert Watson

Tor hides communication patterns by relaying data through volunteer servers

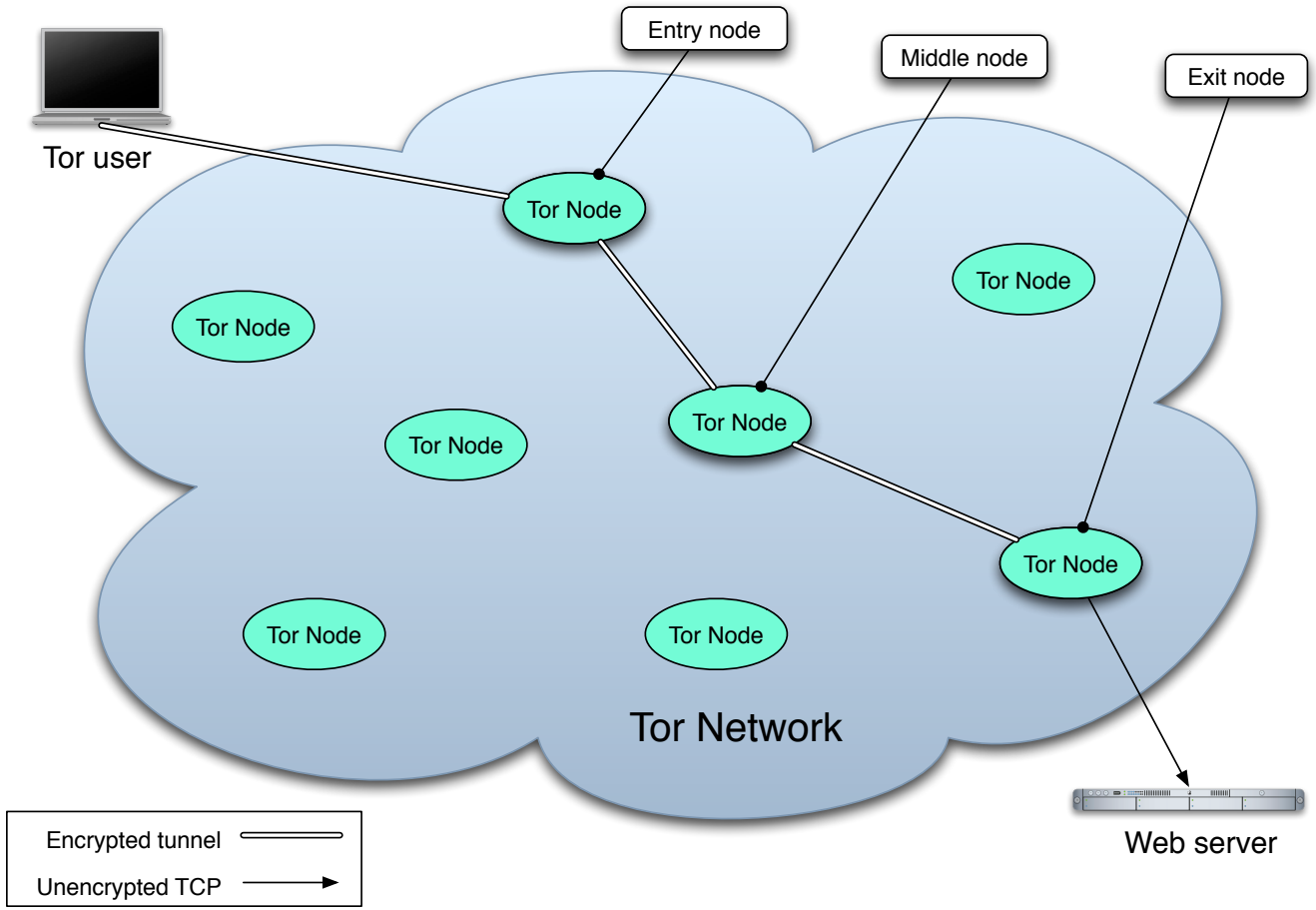


Diagram: Robert Watson

Tor hides communication patterns by relaying data through volunteer servers

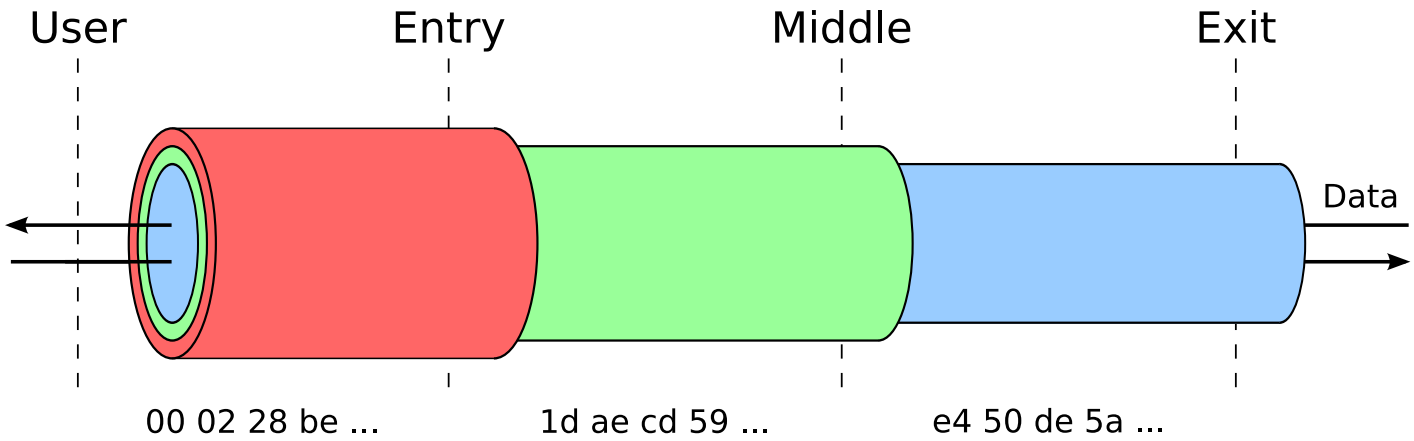
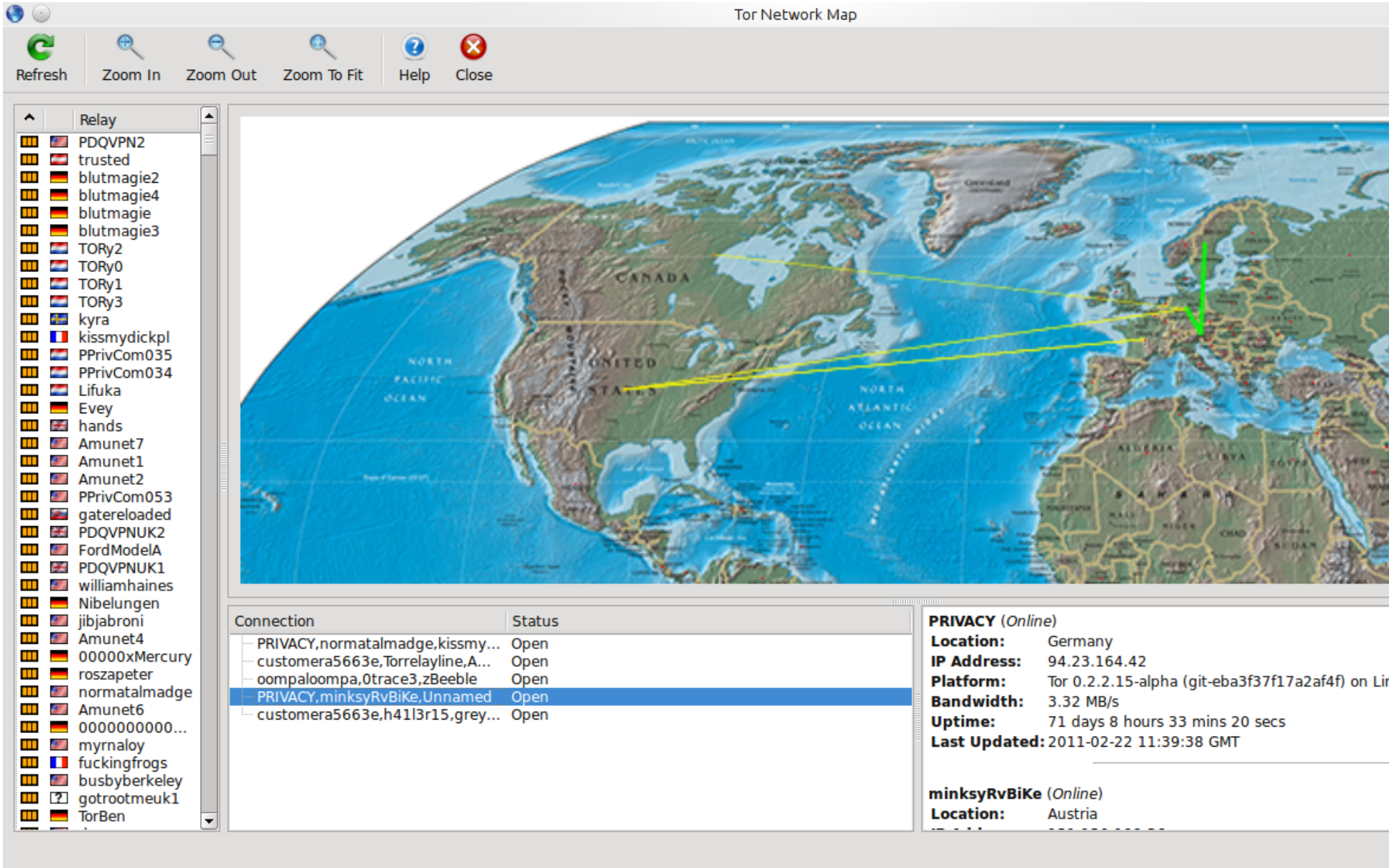


Diagram: Robert Watson

Vidalia Network Map

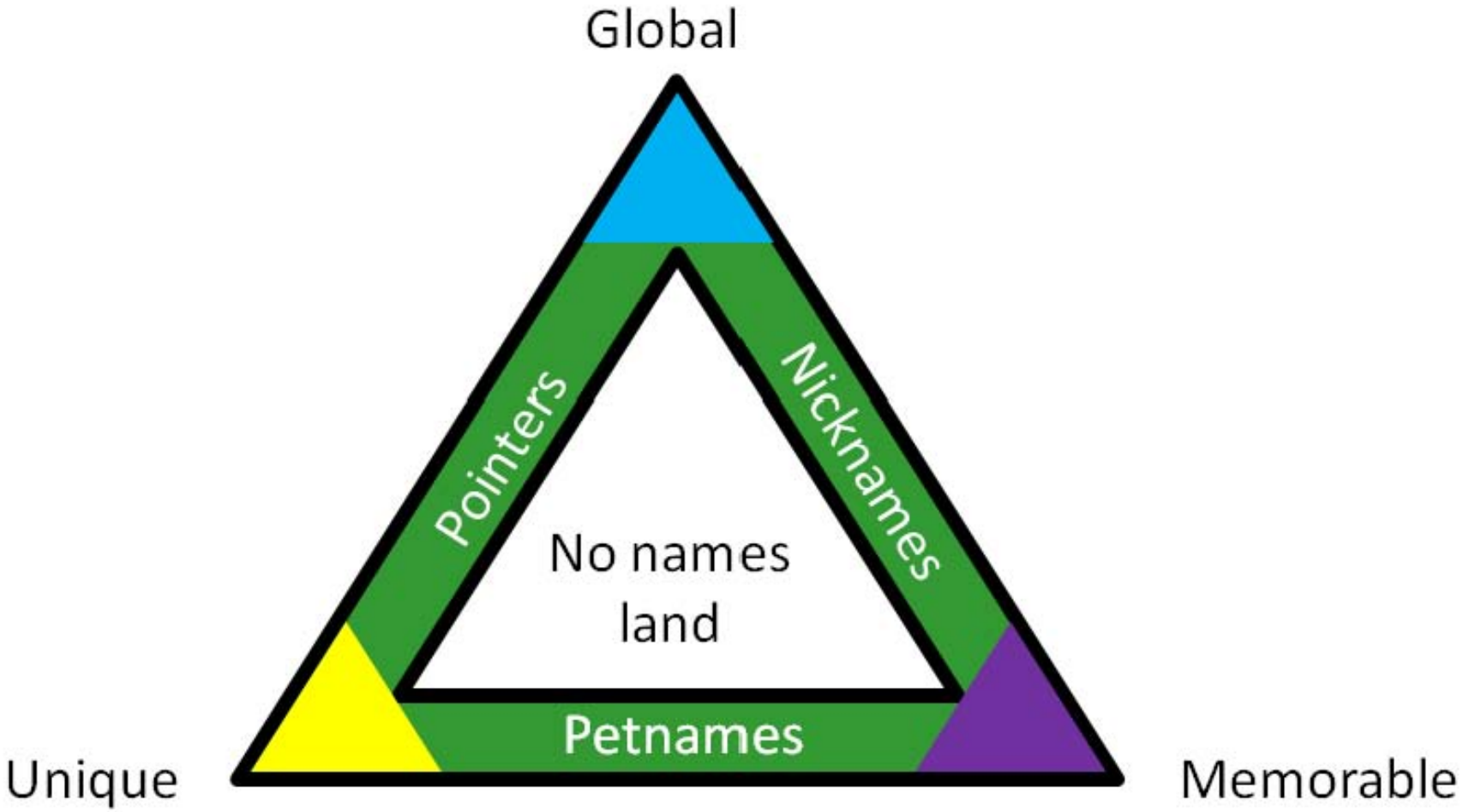


Metrics

- Measuring metrics anonymously
- NSF grant to find out
- Archive of hourly consensus, ExoneraTor, VisiTor
- Metrics portal:
  `https://metrics.torproject.org/`

Tor hidden services allow privacy enhanced hosting of services

dot onion you say?



Hidden services, in text

- Distributed Hash Table (DHT) Directory

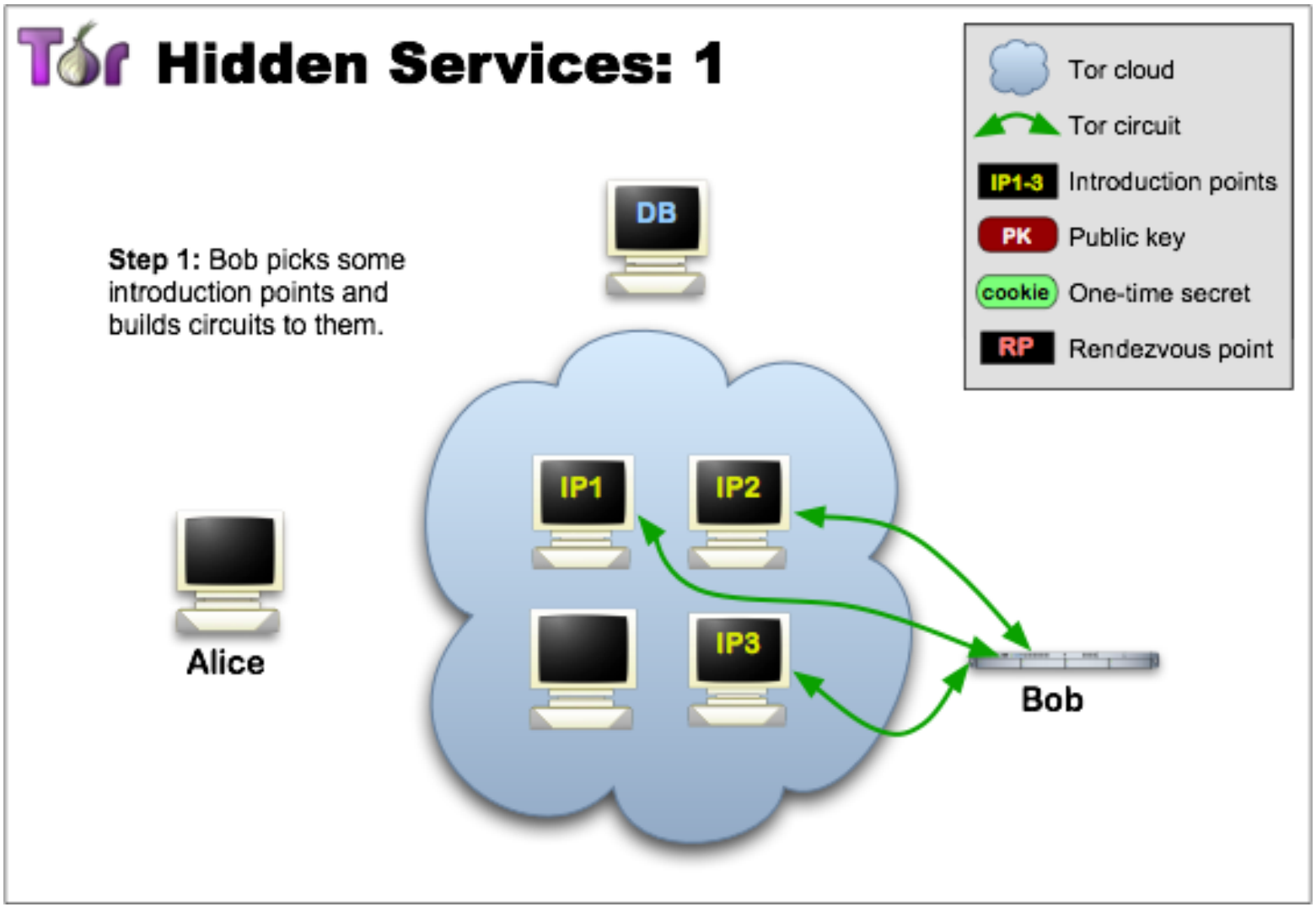
Hidden services, in text

- Distributed Hash Table (DHT) Directory
- Rendezvous points

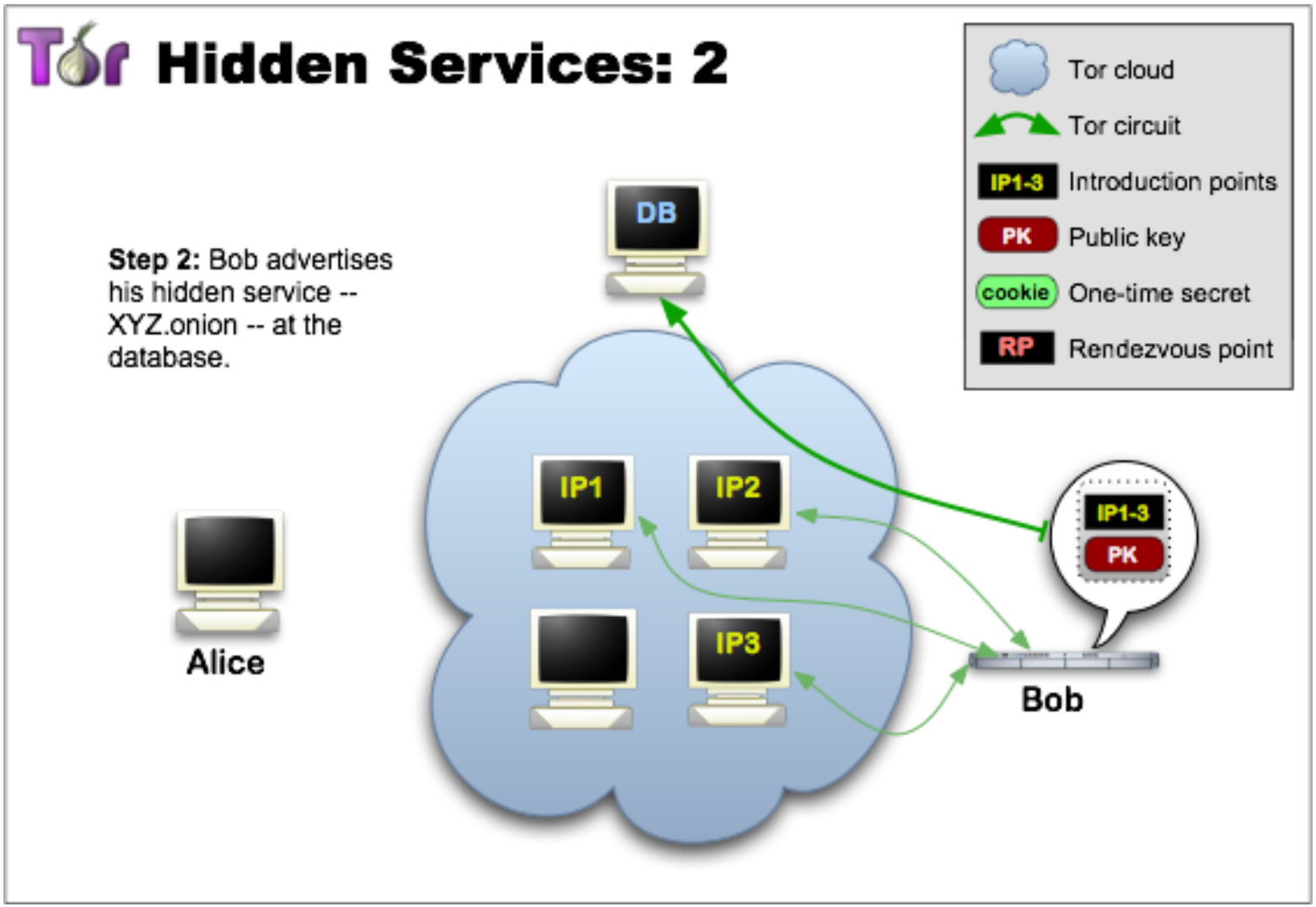
Hidden services, in text

- Distributed Hash Table (DHT) Directory
- Rendezvous points
- Anonymity for both the server and client

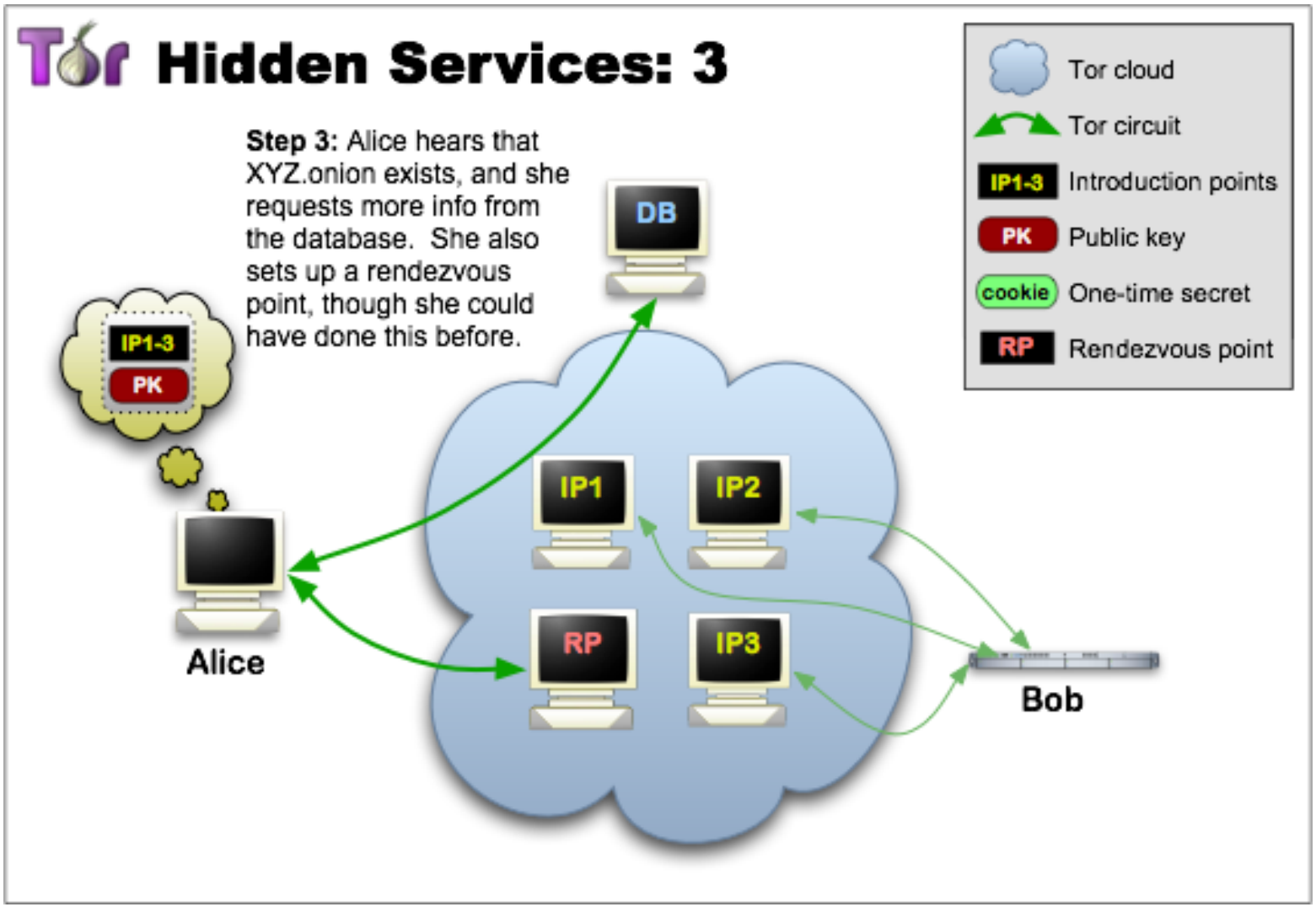
Hidden Services, in graphics



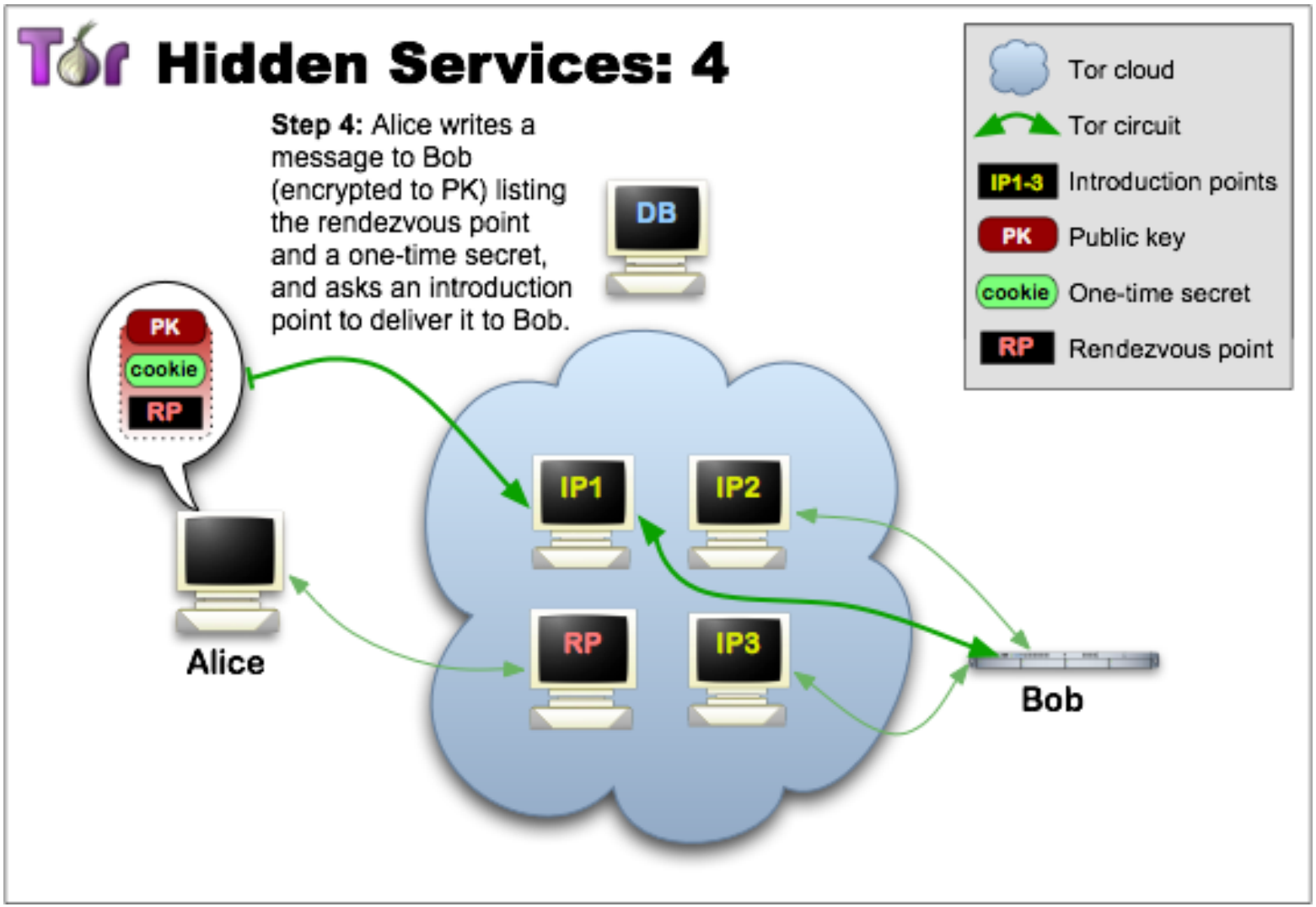
Hidden Services, in graphics



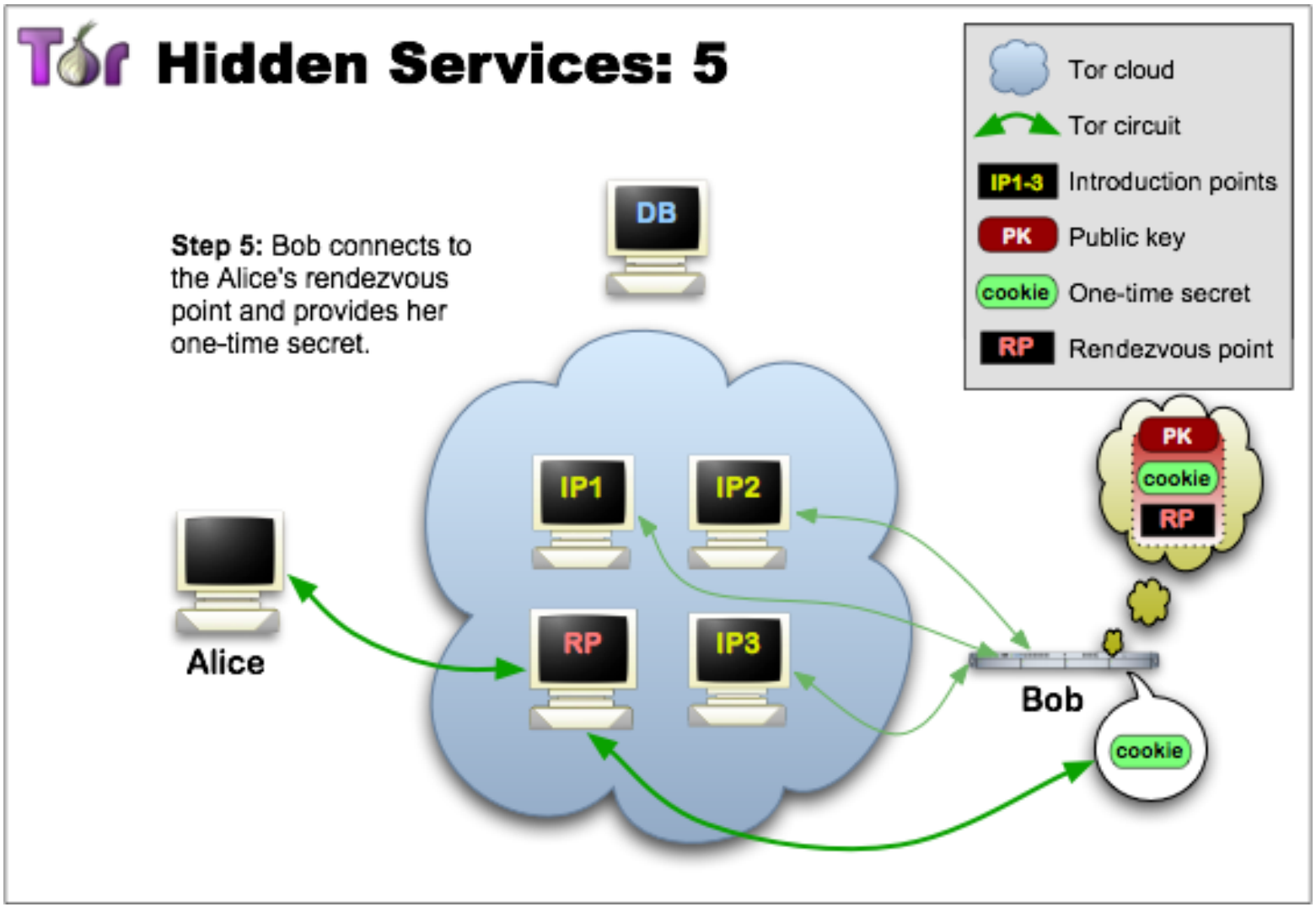
Hidden Services, in graphics



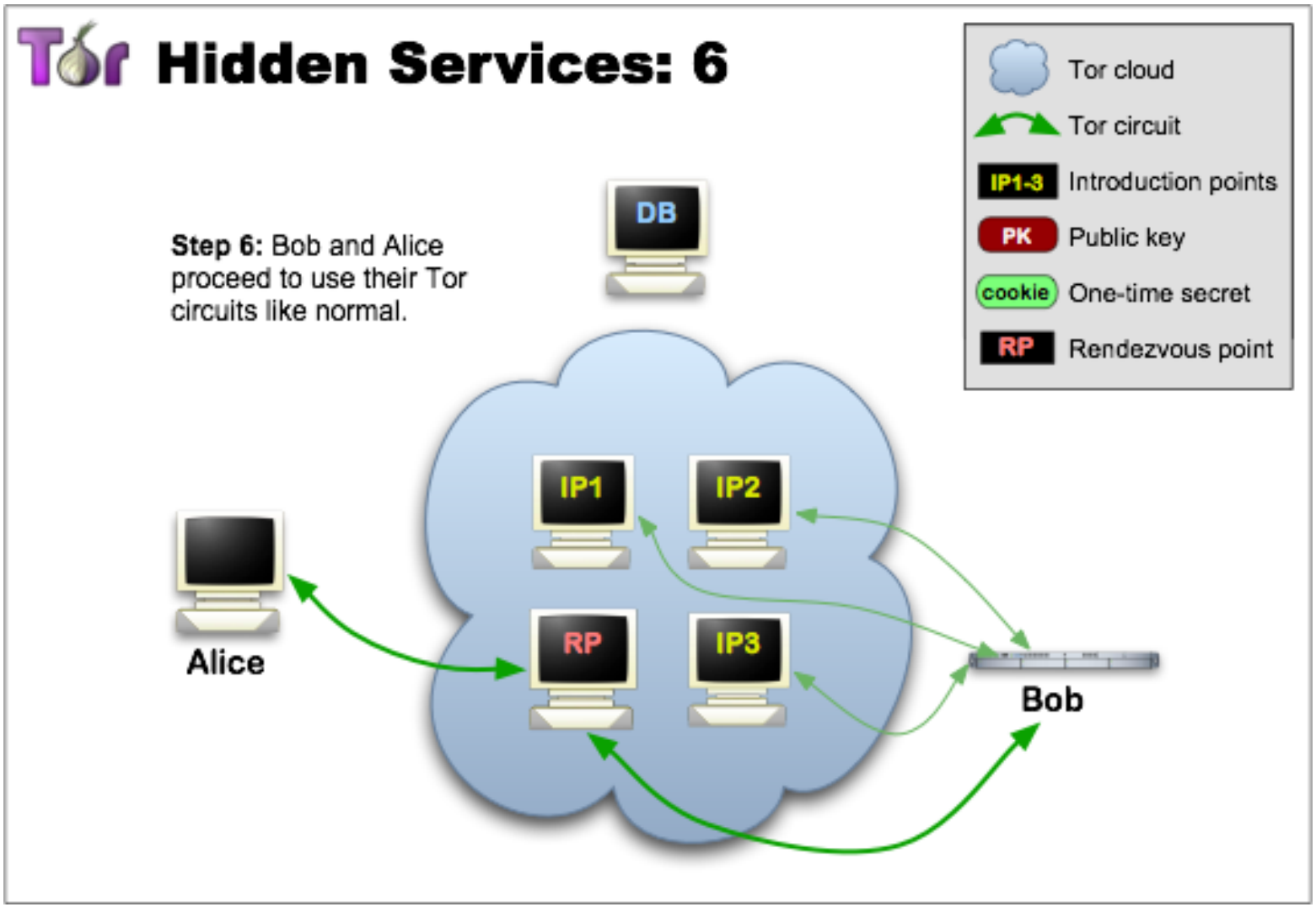
Hidden Services, in graphics



Hidden Services, in graphics



Hidden Services, in graphics



Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my....

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"
- Did you know Microsoft Word and OpenOffice Writer are browsers?

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"
- Did you know Microsoft Word and OpenOffice Writer are browsers?
- `www.decloak.net` is a fine test

Mobile Operating Systems

- Entirely new set of challenges for something designed to know where you are at all times.
- Orbot: Tor on Android. `https://guardianproject.info/apps/`
- Tor on iphone, maemo/meego, symbian, etc
- Tor on Windows CE, `http://www.gsmk.de` as an example.
- Guardian Project, `https://guardianproject.info/`

Next steps

Visit `https://www.torproject.org/` for more information, links, and ideas.

Credits & Thanks

- who uses tor? `http://www.flickr.com/photos/mattw/2336507468/siz`, Matt Westervelt, CC-BY-SA.
- danger!, `http://flickr.com/photos/hmvh/58185411/sizes/o/`, hmvh, CC-BY-SA.
- 500k, `http://www.flickr.com/photos/lukaskracic/334850378/sizes/l/`, Luka Skracic, used with permission.