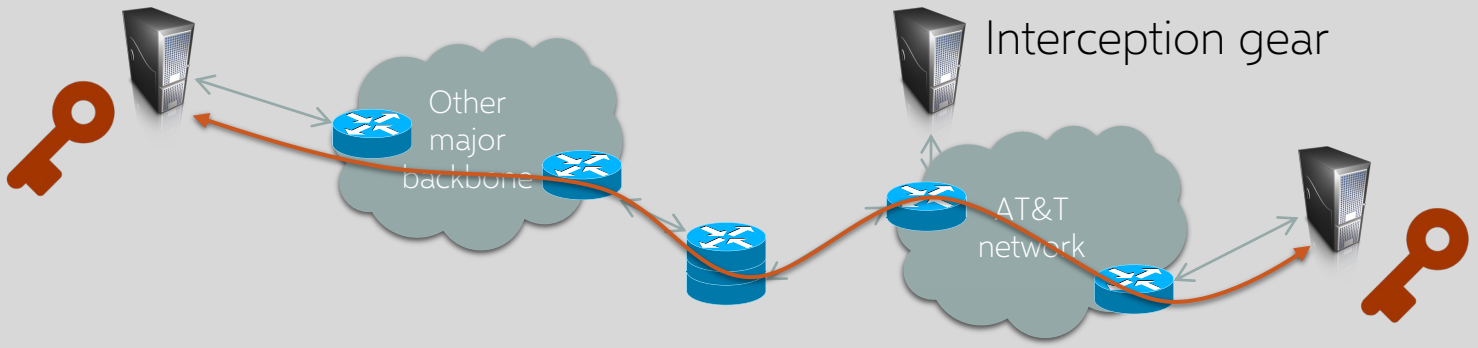
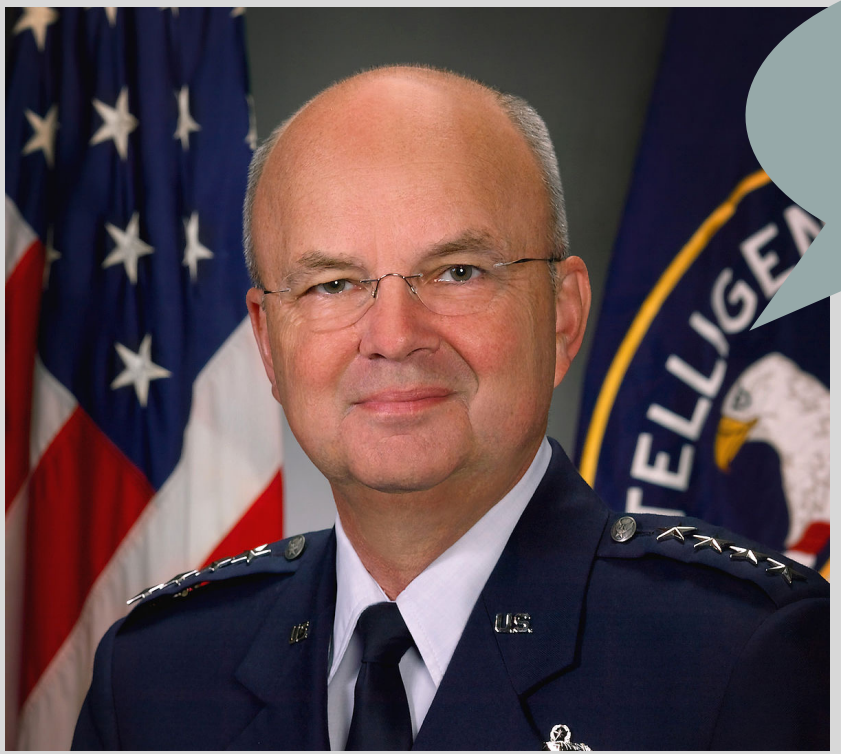
ONION ROUTING
CENSORSHIP RESISTANCE

VITALY SHMATIKOV

Privacy on Public Networks

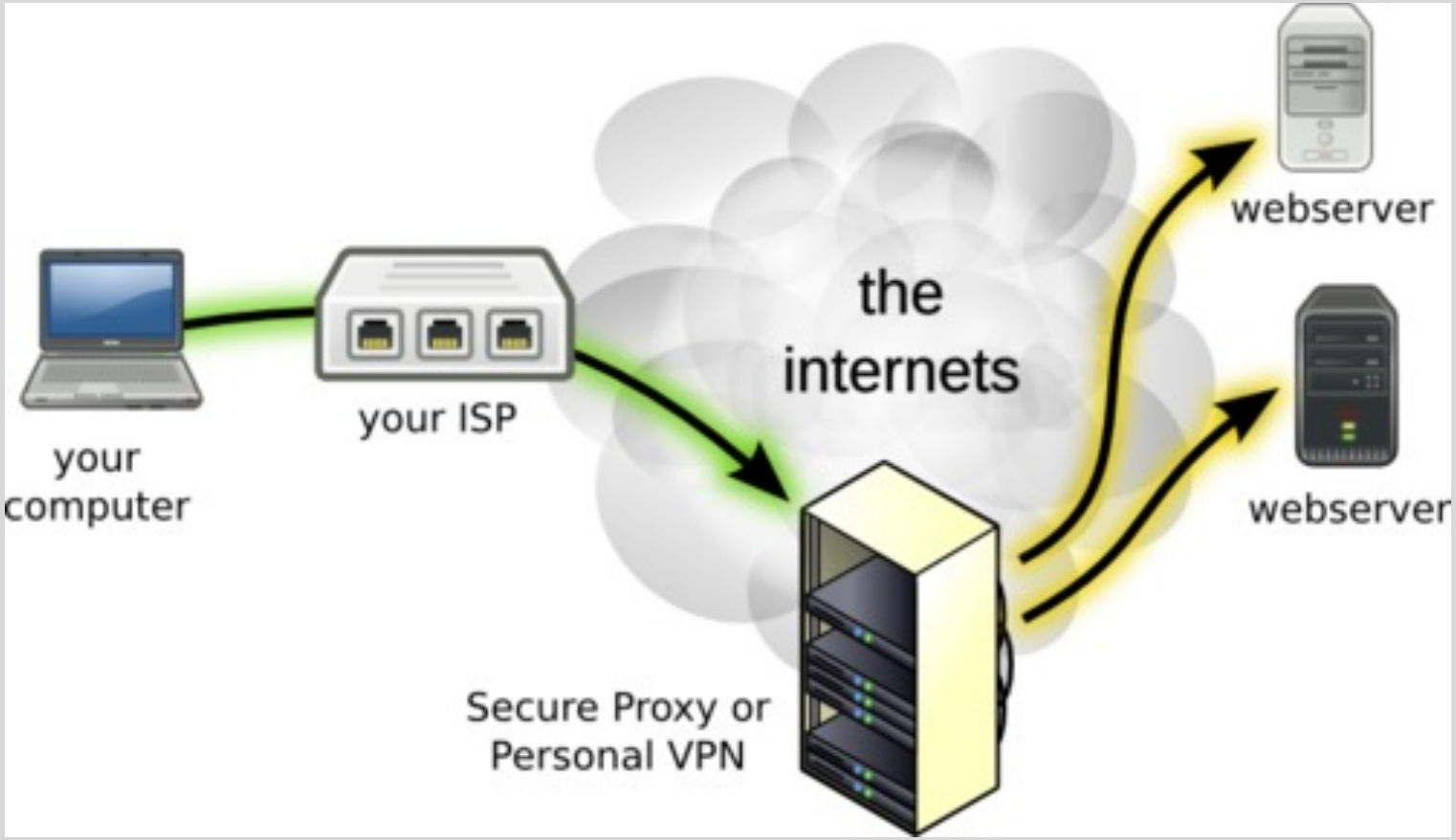
- Internet is designed as a public network, routing information is public
  - IP packet headers identify source and destination
- End-to-end encryption hides payload but does not hide metadata
  - Who is talking to whom
  - When communication is taking place
  - Size of messages





Michael Hayden
Former Director,
National Security Agency

VPN?


webserver
the
internets
your ISP
your
computer
webserver
Secure Proxy or
Personal VPN

VPN Technical Issues

- VPNs generally not designed for anonymity
  - Typical application: work remotely, connect to corporate network
- Even a single leaked DNS request or TCP SYN can identify user
- Can’t use the same browser for both anonymous and non-anonymous browsing
  - Example: shared cookies
- Browser fingerprinting can uniquely identify user

VPN Non-Technical Issues

- Must trust the VPN completely
- Single point of failure with full visibility into your metadata (and content, unless using E2EE with the destination)

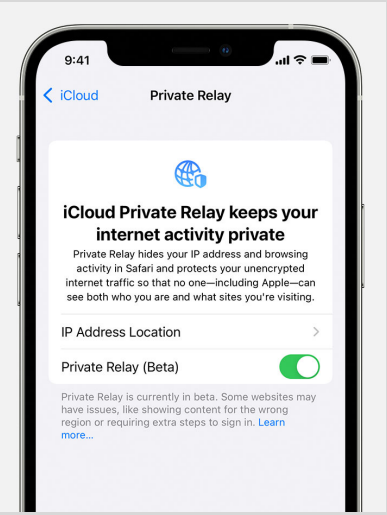
Supposedly Non-Existent VPN Logs Help FBI Catch Internet Stalker

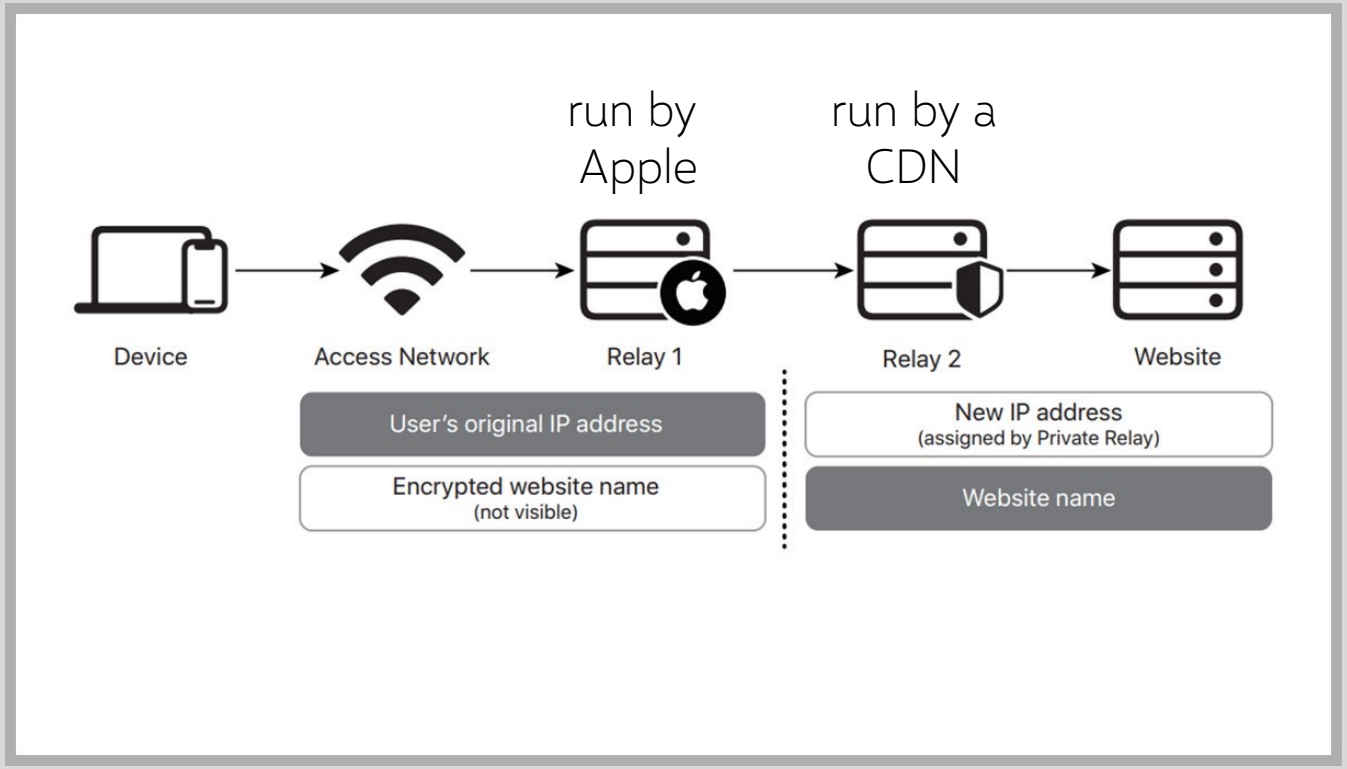
"Zero logs" VPN exposes millions of logs including user passwords, claims data is anonymous

UFO VPN exposed millions of log files about users of its service, including their account passwords and IP addresses, despite claiming that it keeps no logs.

iCloud+ Private Relay

Safari on mobile
Apps (only unencrypted)





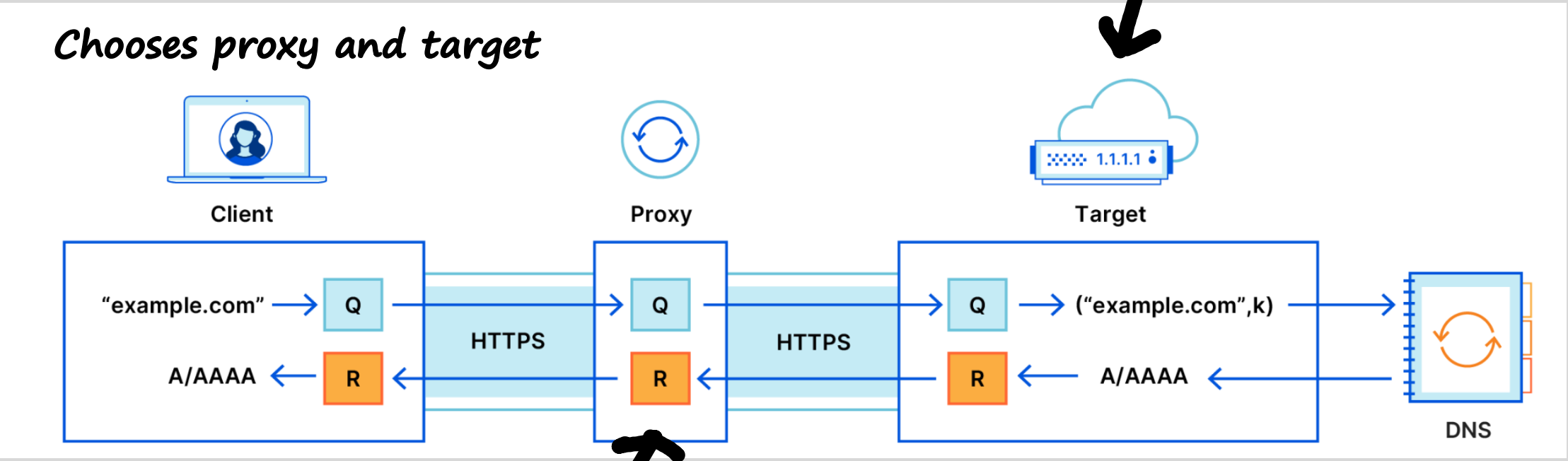
IP addresses assigned by second relay are rotated over time

DNS lookups use Oblivious DNS over HTTPS

Unlike VPN, cannot change country and time zone

Oblivious DNS over HTTPS

Answers DNS queries but does not see who asked them



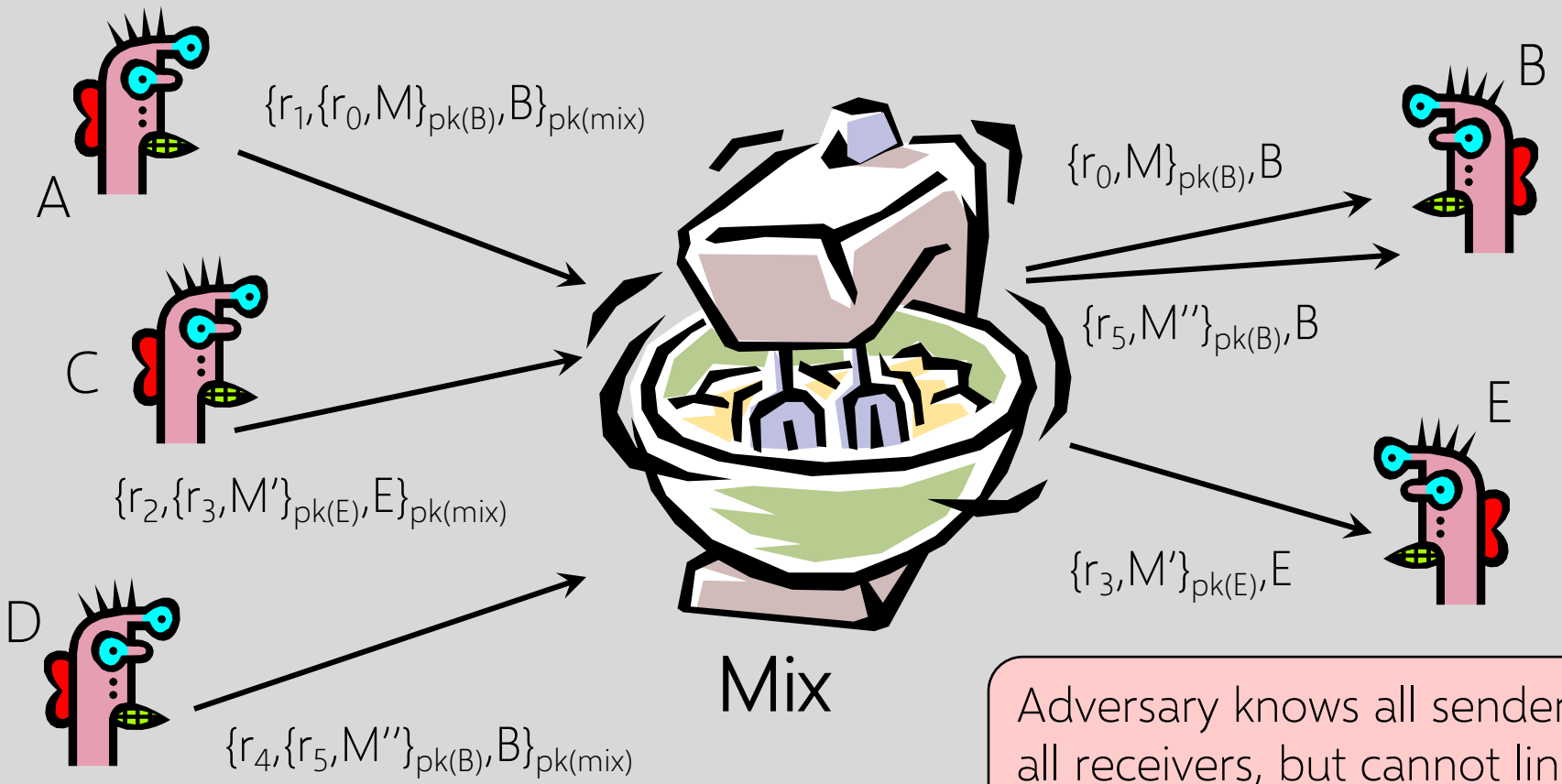
Does not see DNS queries or answers, only forwards them

https://blog.cloudflare.com/oblivious-dns/

Chaum's Mix

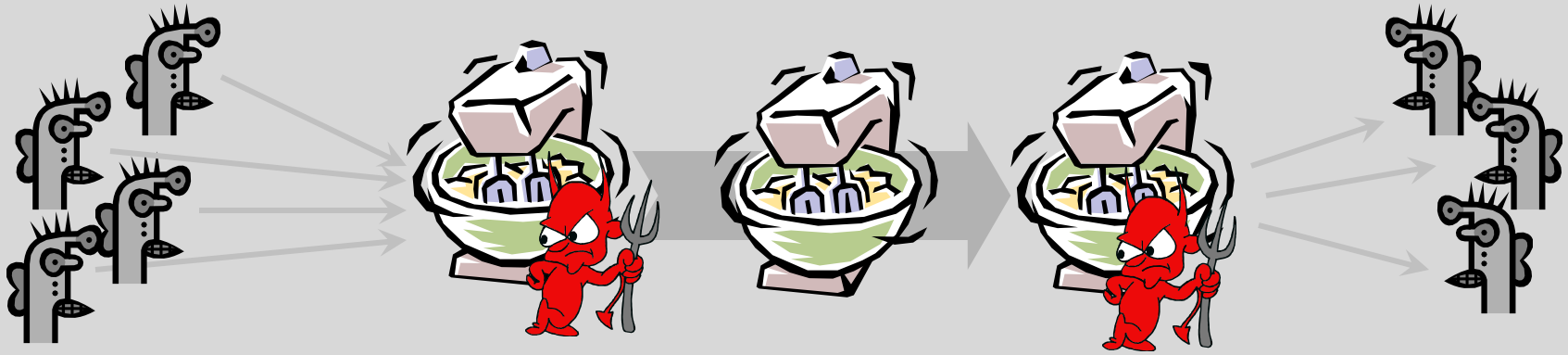
- Early proposal for anonymous email
  - David Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". Communications of the ACM, February 1981.
- Public-key crypto + trusted re-mailer (Mix)
  - Untrusted communication medium
  - Public keys used as persistent pseudonyms
- Modern anonymity systems use Mix as the basic building block

Basic Mix Design



Adversary knows all senders and all receivers, but cannot link a sent message with a received message

Mix Cascades and Mixnets



- Messages are sent through a sequence of mixes
  - Can also form an arbitrary network of mixes ("mixnet")
- Some of the mixes may be controlled by attacker, but even a single good mix ensures anonymity
- Pad and buffer traffic to foil correlation attacks

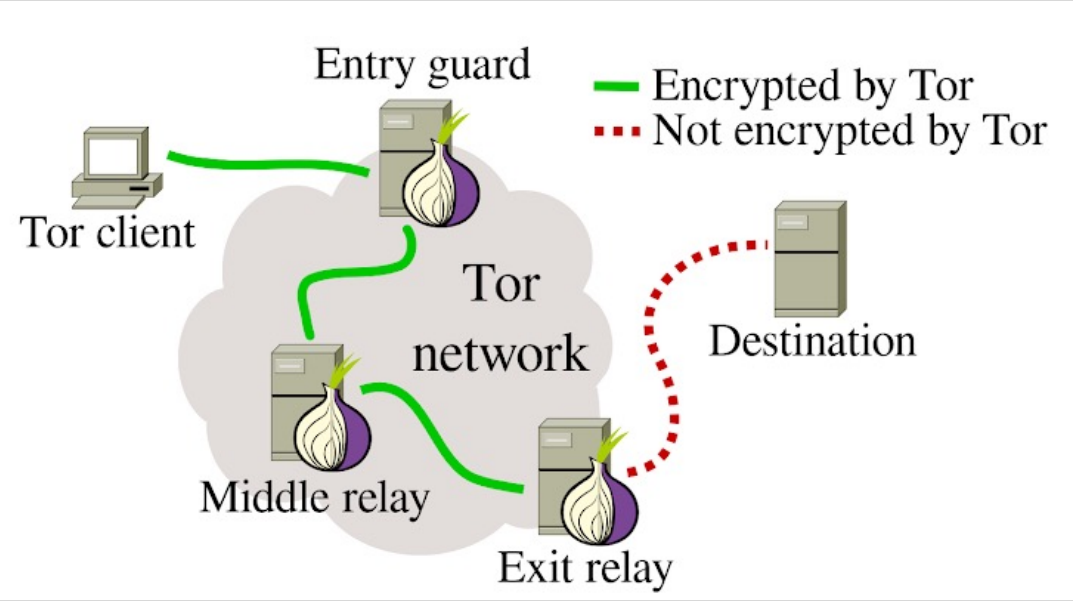
Problem:
high latency ☹

Roger Dingledine

- Second-generation onion routing network
  - http://tor.eff.org
  - Specifically designed for low-latency anonymous Internet communications (e.g., Web browsing)
  - Running since October 2003
- Hundreds of nodes on all continents
- Over 2,500,000 users
- “Easy-to-use” client + Web browser

Tor (The Onion Router)

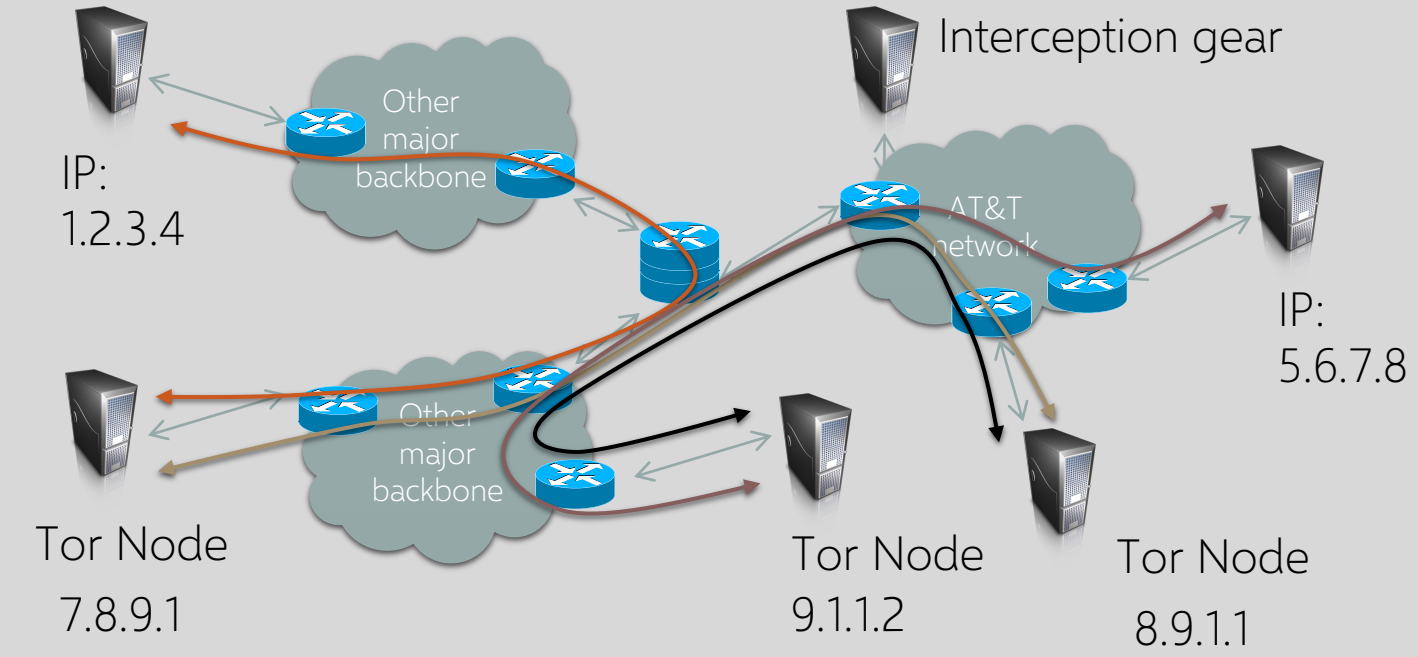
Main idea: tunnel traffic through multiple relays (aka "onion routers") using public key cryptography



Many TCP connections can be "multiplexed" over one Tor circuit

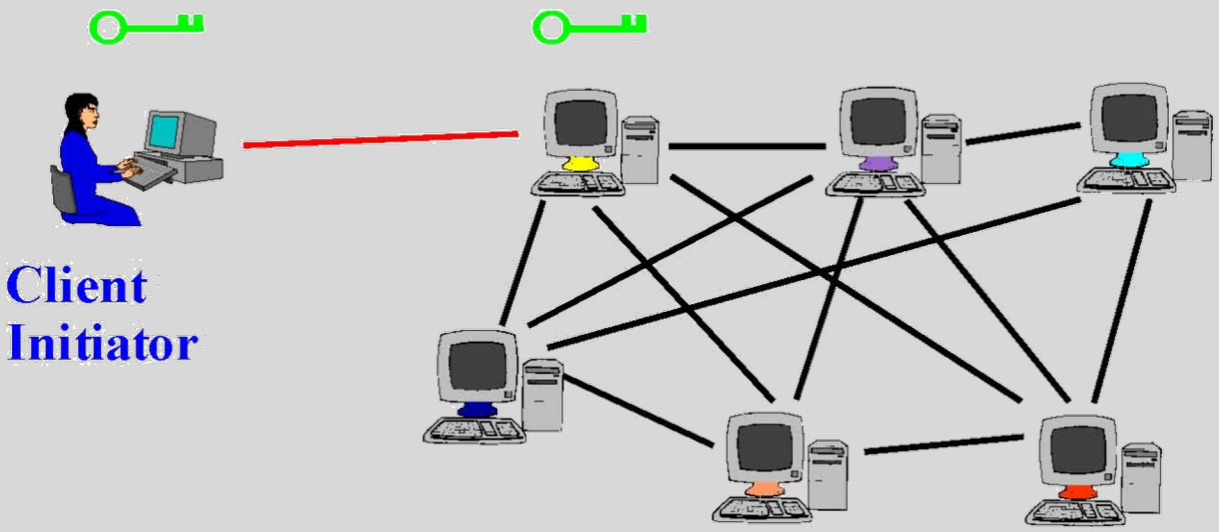
Key concept: an overlay chain of several Tor routers that can be repeatedly used by the client

Tor Circuit Setup: Overview



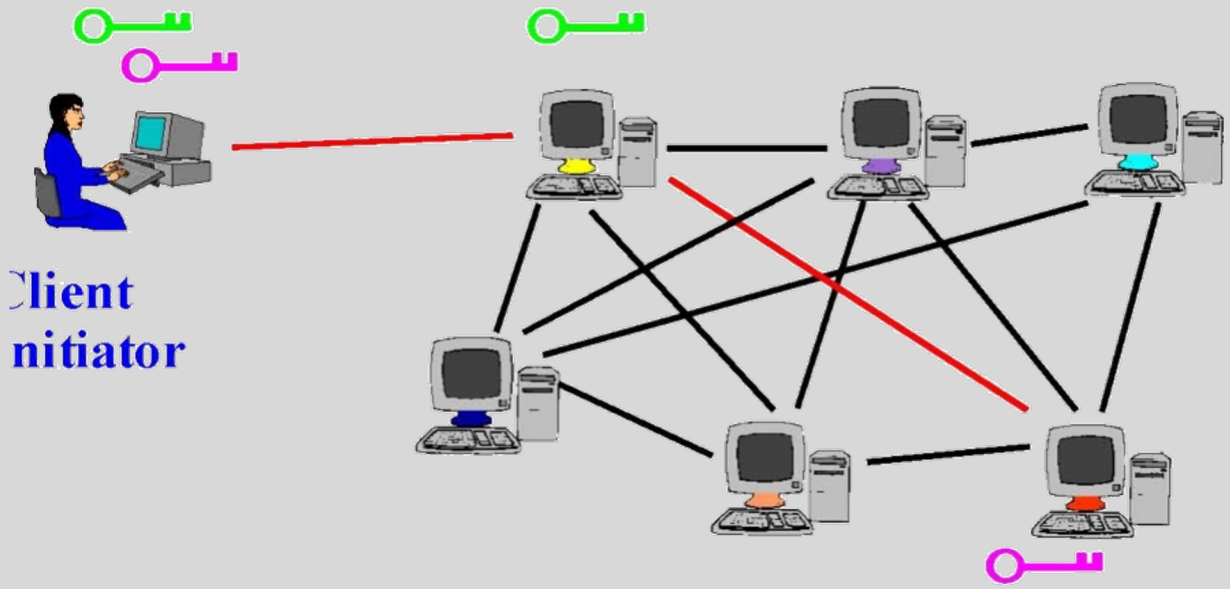
Tor Circuit Setup (1)

Client proxy establishes a symmetric key and circuit with Onion Router #1



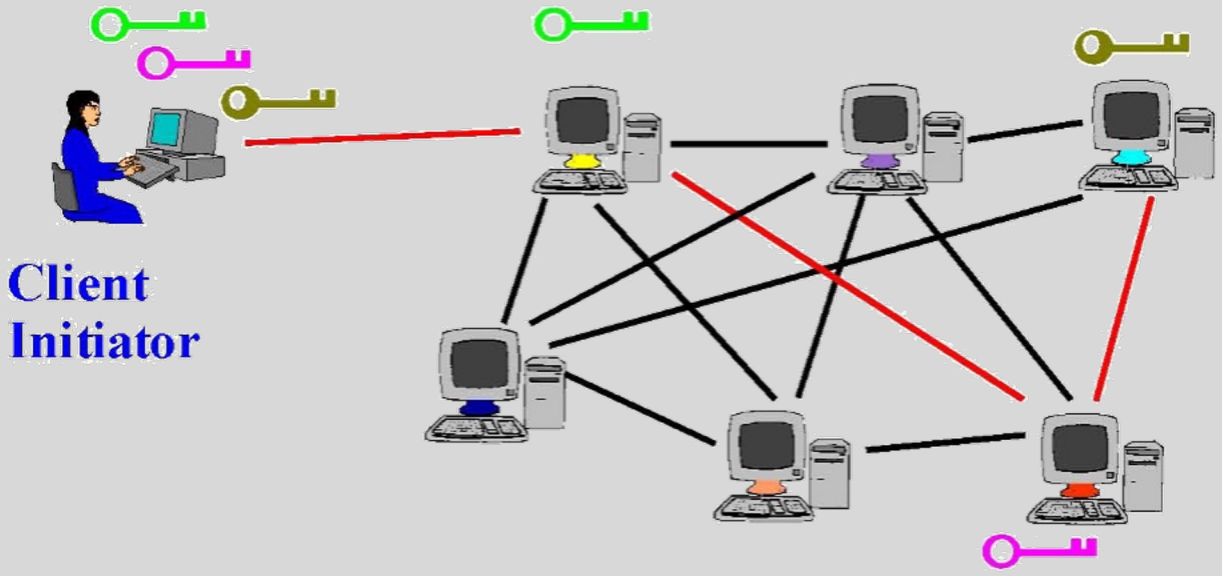
Tor Circuit Setup (2)

Client proxy extends the circuit by tunneling through Onion Router #1 and establishes a symmetric key with Onion Router #2



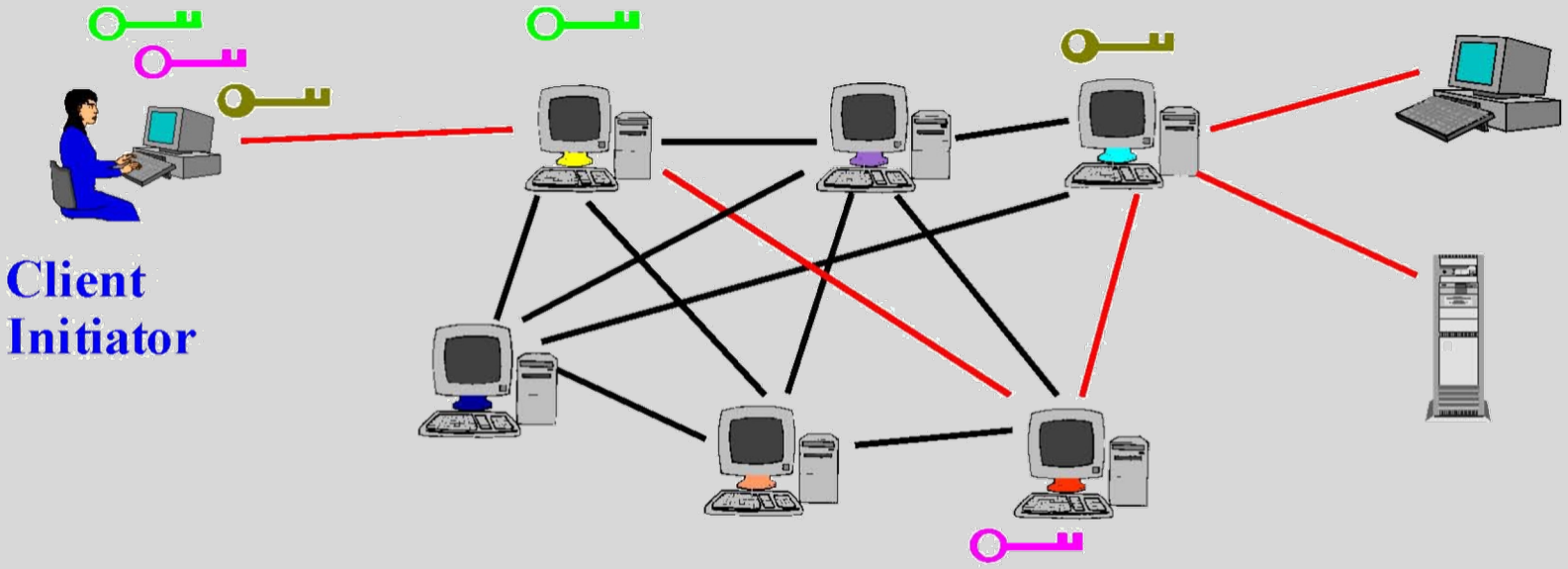
Tor Circuit Setup (3)

Client proxy extends the circuit by tunneling through Onion Routers #1 and #2 and establishes a symmetric key with Onion Router #3



Using a Tor Circuit

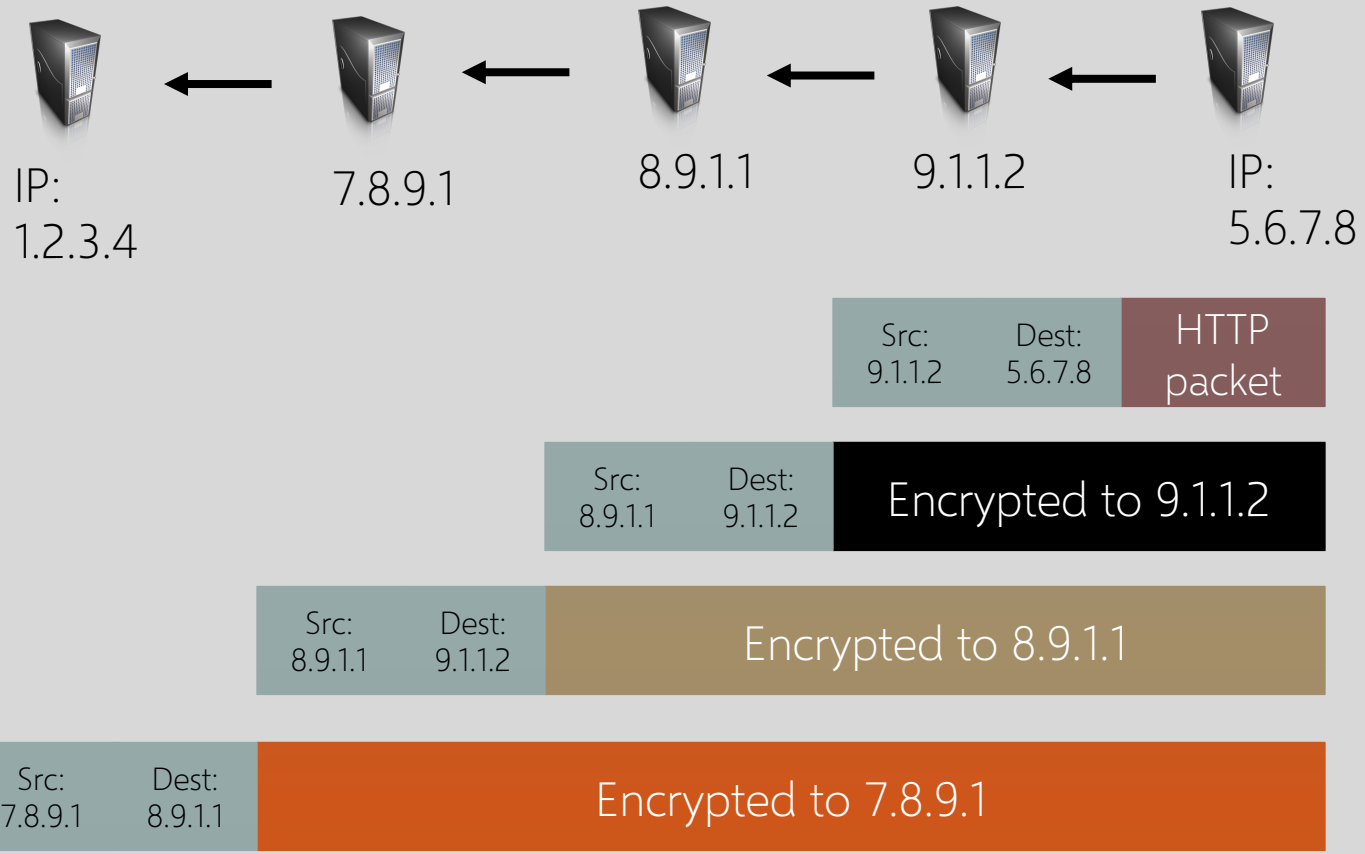
Client applications communicate over the established circuit



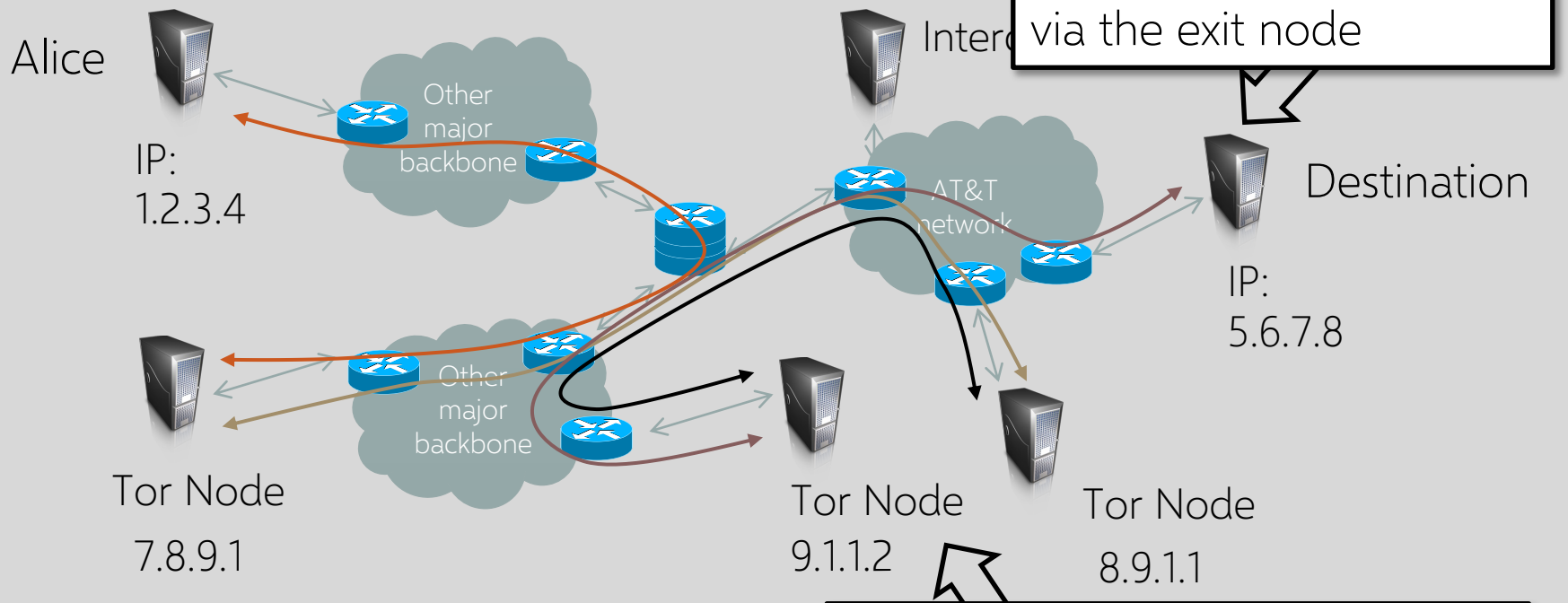
Datagrams decrypted and re-encrypted at each node of the router chain

Tor implements a more complex version of this basic idea

Onion Routing: Example



Who Knows What?



Destination: knows a Tor user is connecting to it via the exit node

Entry node: knows Alice is using Tor + identity of middle relay, but not destination

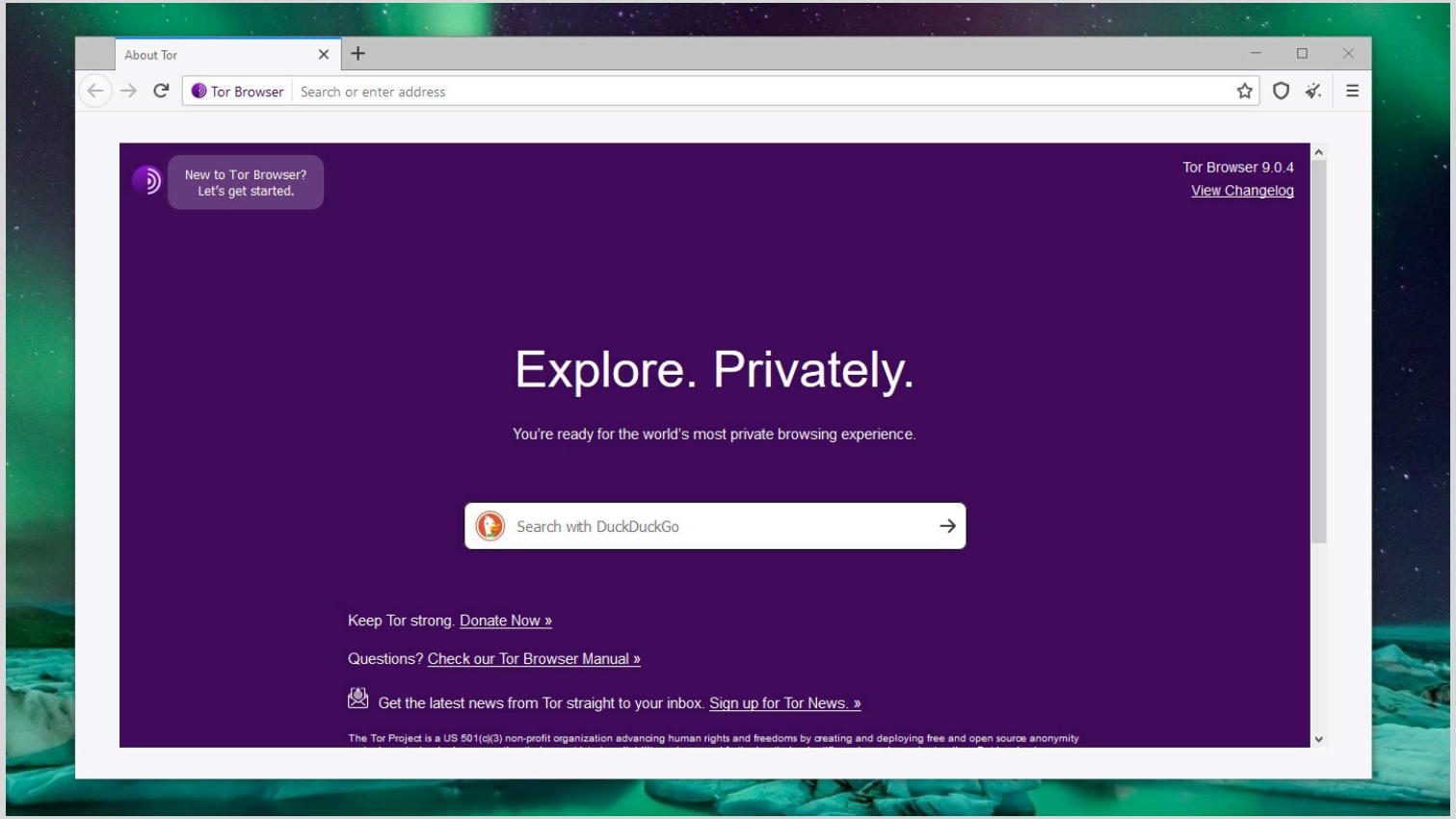
Exit node: knows some Tor user is connecting to destination, but not which user

Hiding From the Destination

- There's no long-term identifier for a Tor user
- If a website gets a connection from Tor today, and another one tomorrow, it cannot tell whether those are from the same user or not
- But two connections in quick succession from the same Tor node are more likely to in fact be from the same user

Hiding from the destination requires application-level protections

Tor Browser



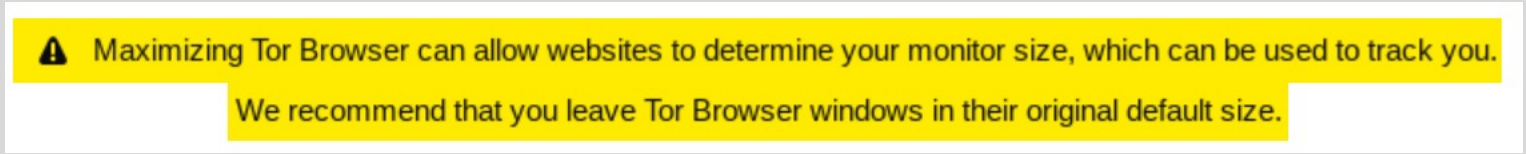
Protections from browser fingerprinting and other threats

https://blog.torproject.org/browser-fingerprinting-introduction-and-challenges-ahead

Fingerprinting Tor Browser

Goal: all Tor users should have the same fingerprint

user-agent: `Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0`



Default fallback fonts

WebGL and Canvas API blocked by default

Access to high-resolution timing blocked

"First Party Isolation": every source of browser identification keyed to the domain in the URL bar (to prevent cross-site tracking)

Choosing Tor Relays

- Tor publishes a directory of of active relays
  - Their locations, current public keys, etc.
  - Public keys of directory servers ship with Tor code
- Must control how relays join
  - Attackers try to create many Tor relays, have their relays selected by users
- Algorithm for path selection preferences high-capacity, long-lived relays… can also choose manually

Exploited by the CERT / DHS attack on Tor during Operation Onymous

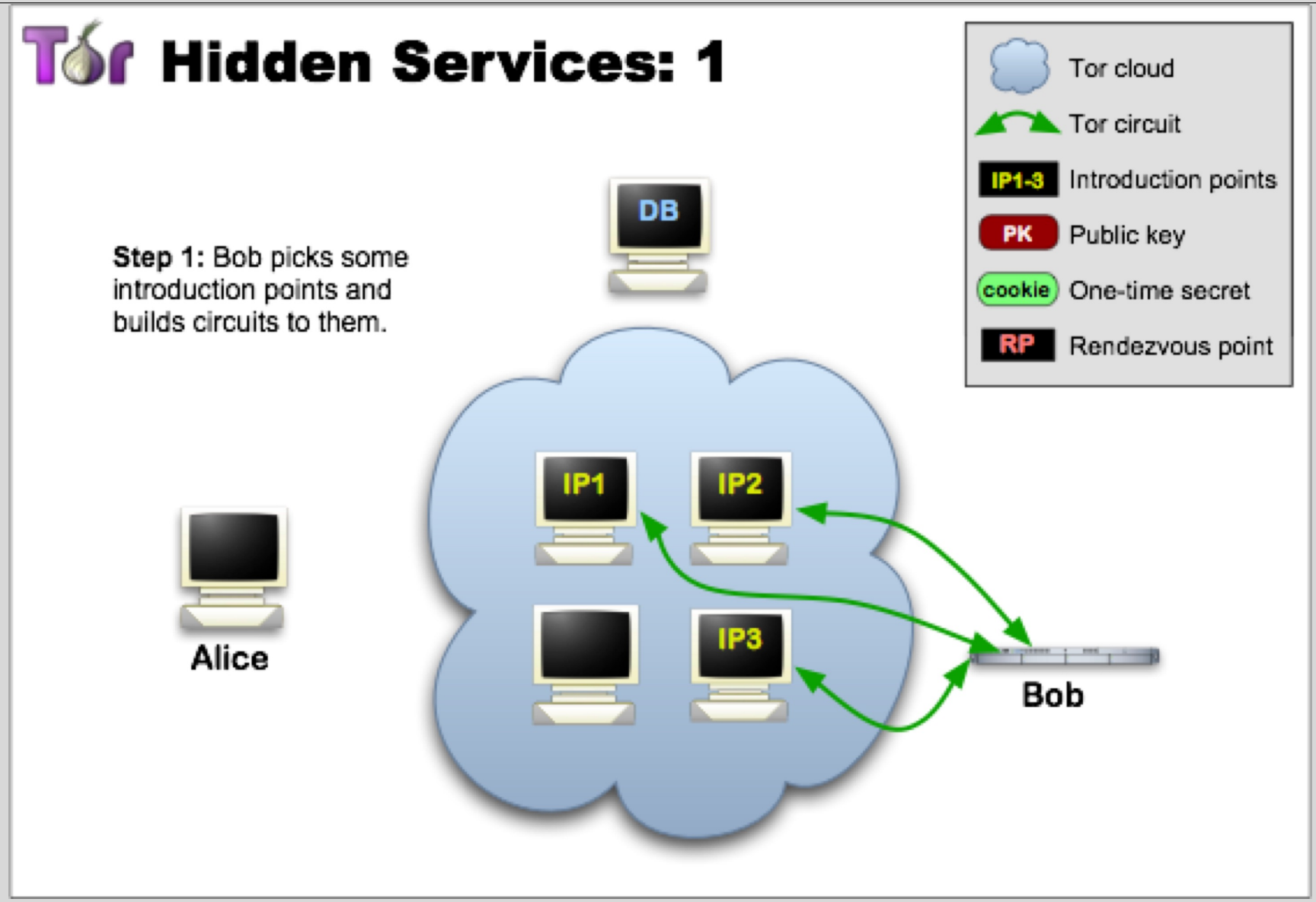
Onion Services (aka Hidden Services)

Goal: deploy a server on the Internet that anyone can connect to without knowing where it is or who runs it

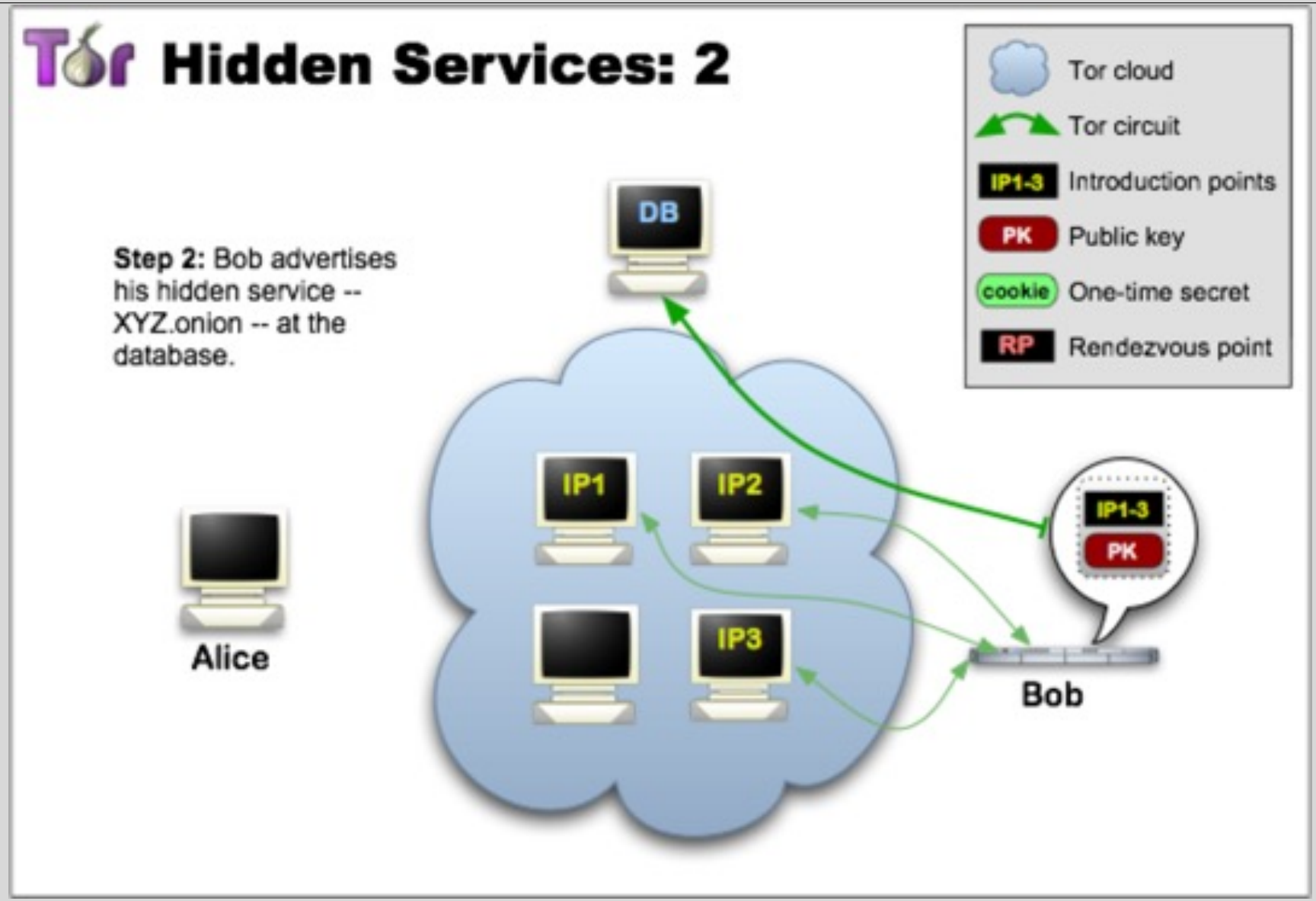
Accessible from anywhere

Resistant to blocking and censorship, denial of service, physical attacks

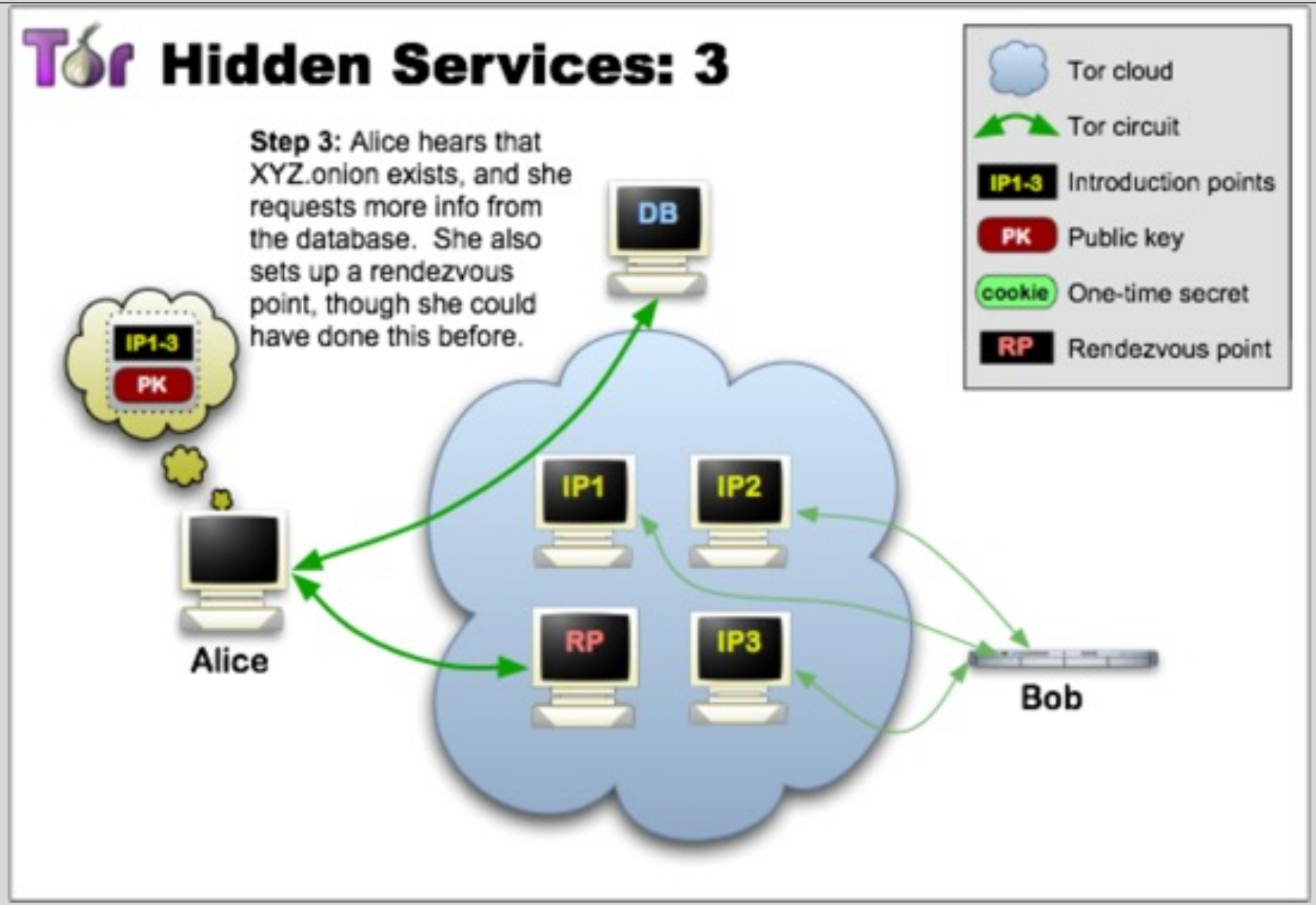
Hidden Services: 1



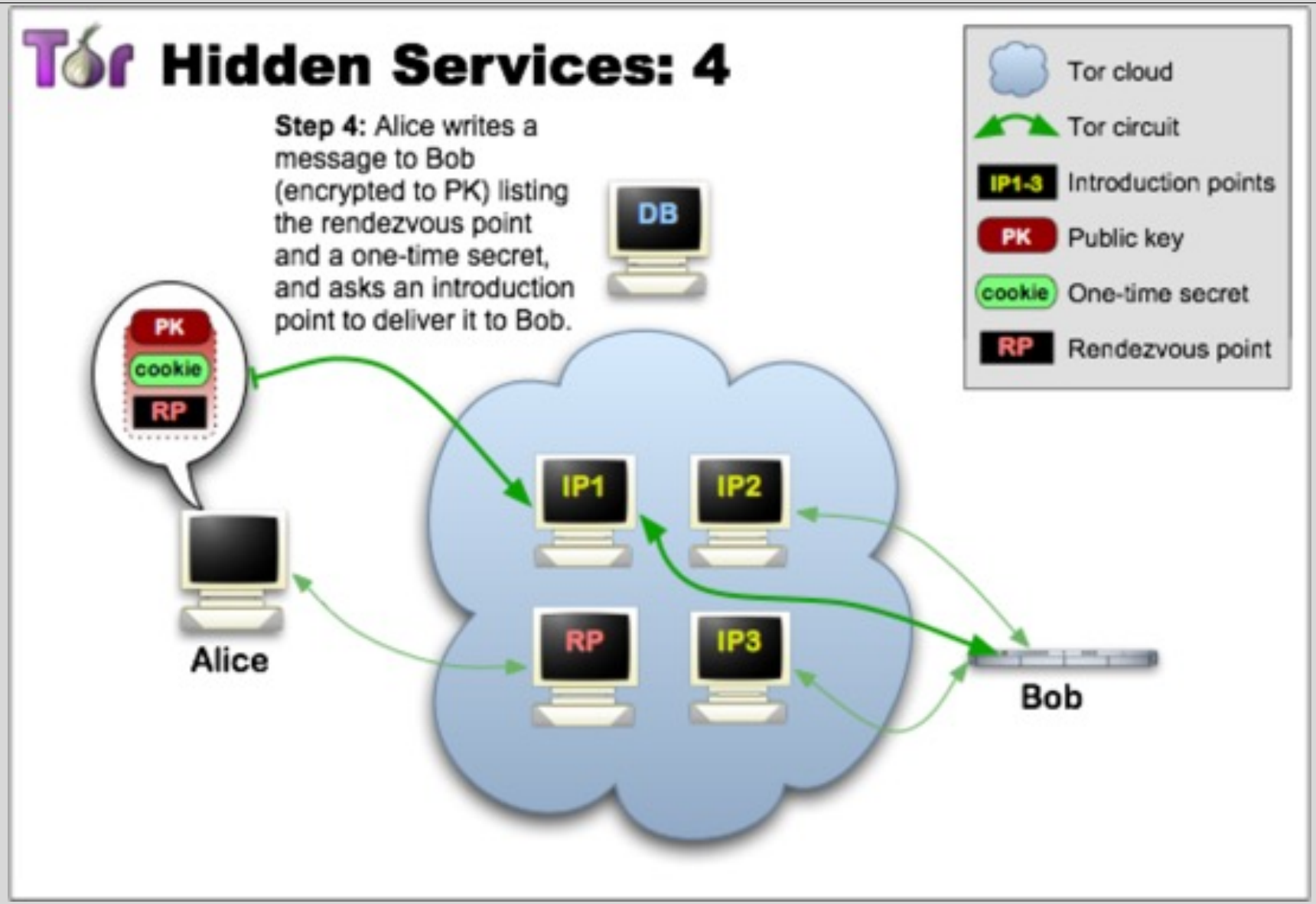
Hidden Services: 2



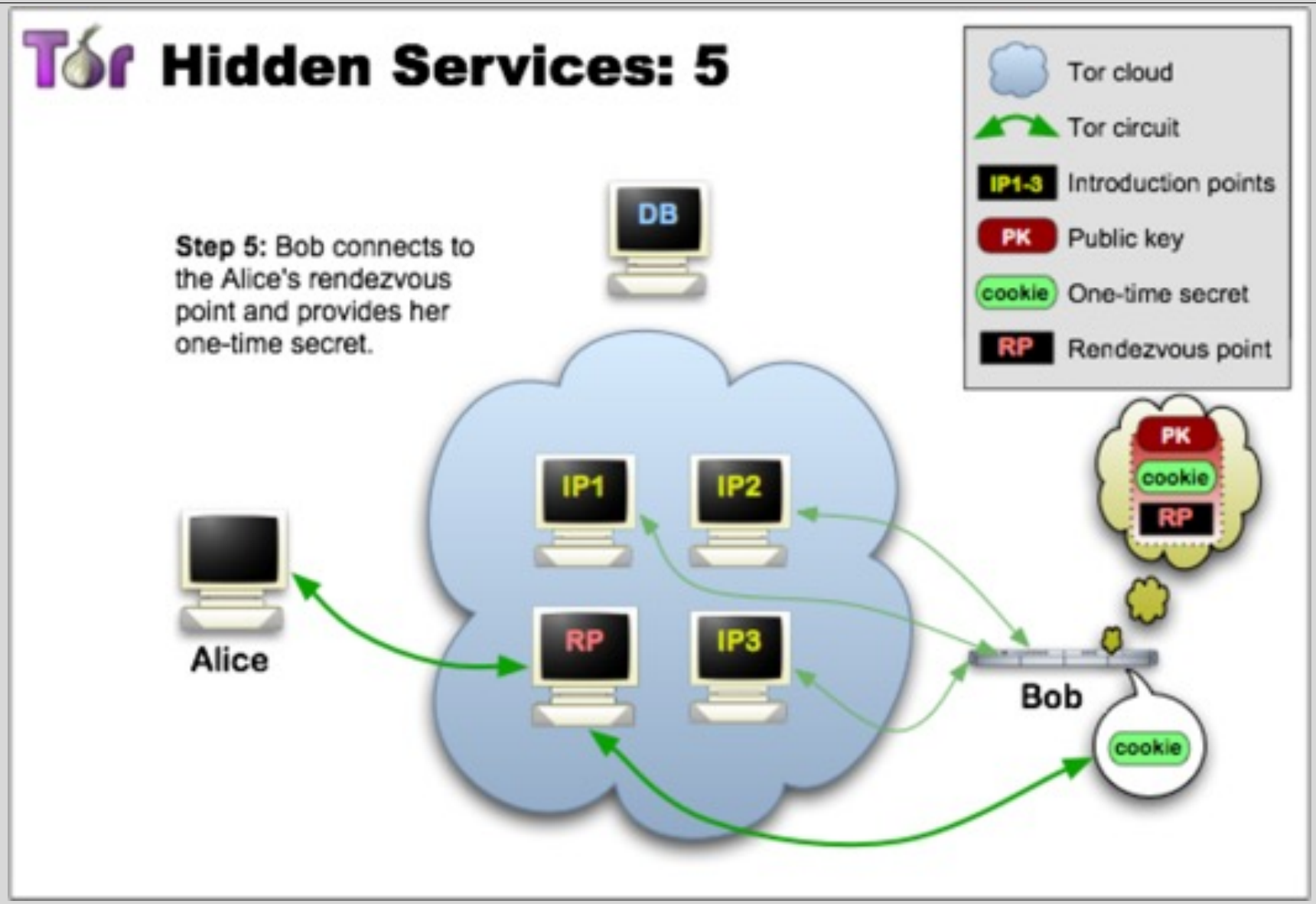
Tor Hidden Services: 3



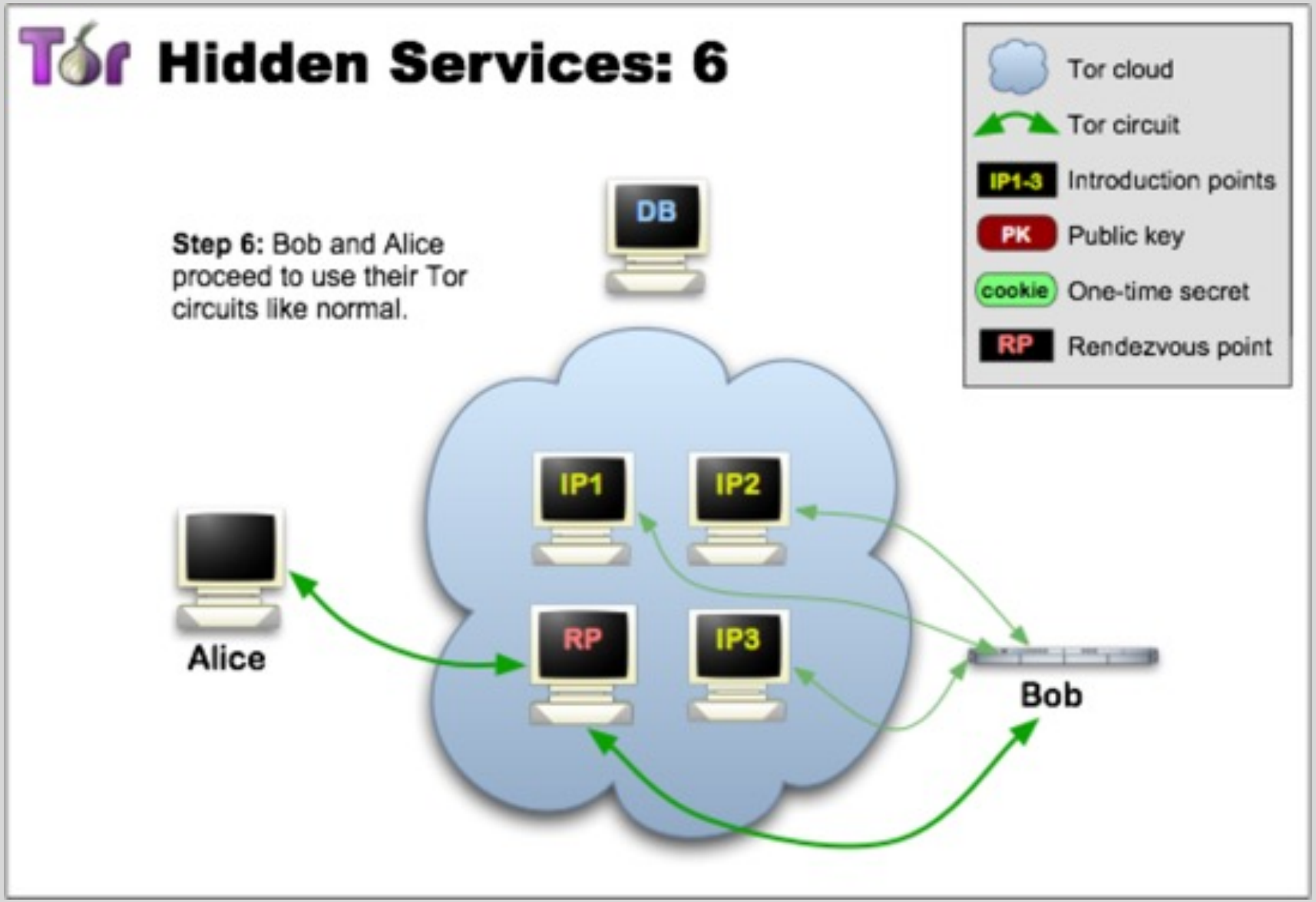
Tor Hidden Services: 4



Tor Hidden Services: 5



Tor Hidden Services: 6



Silk Road

anonymous marketplace

Wel

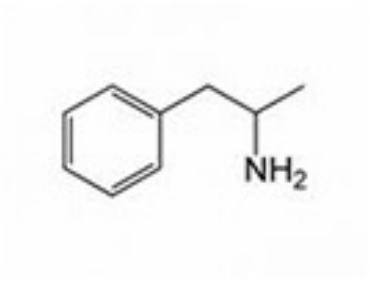
messages(0) | orders(0) | account(฿0.00)

Shop by category:

- Drugs(1582)
  - Cannabis(271)
  - Dissociatives(33)
  - Ecstasy(217)
  - Opioids(106)
  - Other(65)
  - Prescription(274)
  - Psychedelics(306)
  - Stimulants(190)
- Apparel(37)
- Art(1)
- Books(300)
- Computer equipment(9)
- Digital goods(218)
- Drug paraphernalia(33)
- Electronics(13)

10 Grams high grade MDMA 80+%

฿61.17



Amphetamines sulfate / Speed freebase...

฿28.59

2g Jack Frost (weed) *420 SALE****

฿8.54

5 Grams of pure MDMA crystals

฿42.04

100 red Y tablets 111mg (lab tested)...

฿97.77

Michael Jackson Discography 1971-2009...

฿2.52

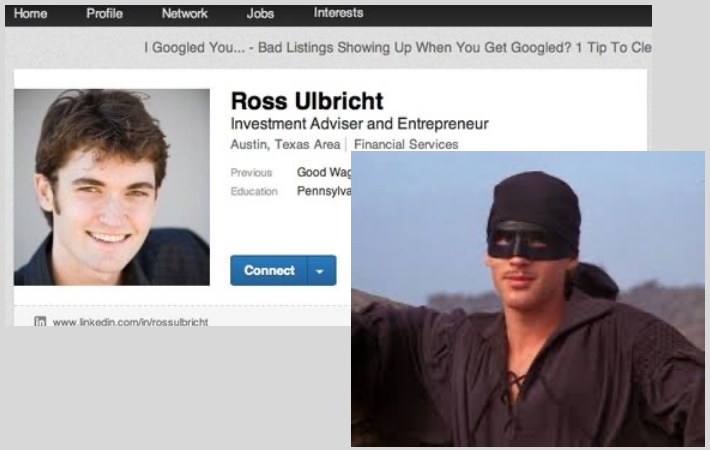
New

- Th
  or
- W
  fa
- Ac
  H
- A
  m
  A
- St
  A

THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Silk Road Shutdown



Ross Ulbricht arrested by the FBI on Oct 1, 2013

In 2015, sentenced to double life + 40 years without the possibility of parole

How was Ulbricht discovered?

- Username “altoid” in an early Silk Road announcement also used by Ulbricht
- A Stack Overflow question accidentally posted by Ulbricht under his real name
  - “How can I connect to a Tor hidden service using curl in php?”
  - … a few seconds later, changed username to “frosty”
  - … the encryption key on the Silk Road server ends with the substring "frosty@frosty"
- A package of fake IDs from Canada traced to an apartment to San Francisco
- A fake murder-for-hire arranged by “Dread Pirate Roberts”, operator of Silk Road

Weaknesses in Tor? Probably Not…

FBI agent Tarbell's testimony:

- Agents examined the headers of IP packets as they interacted with the Silk Road's login screen, noticed an IP address not associated with any Tor nodes
- As they typed this address into the browser, Silk Road's CAPTCHA prompt appeared
- Address led to a rented server in a data center in Iceland

Common problem: misconfigured software does not send all traffic via Tor, leaks IP address

- Is this really what happened with the Silk Road server?

Subsequent Developments

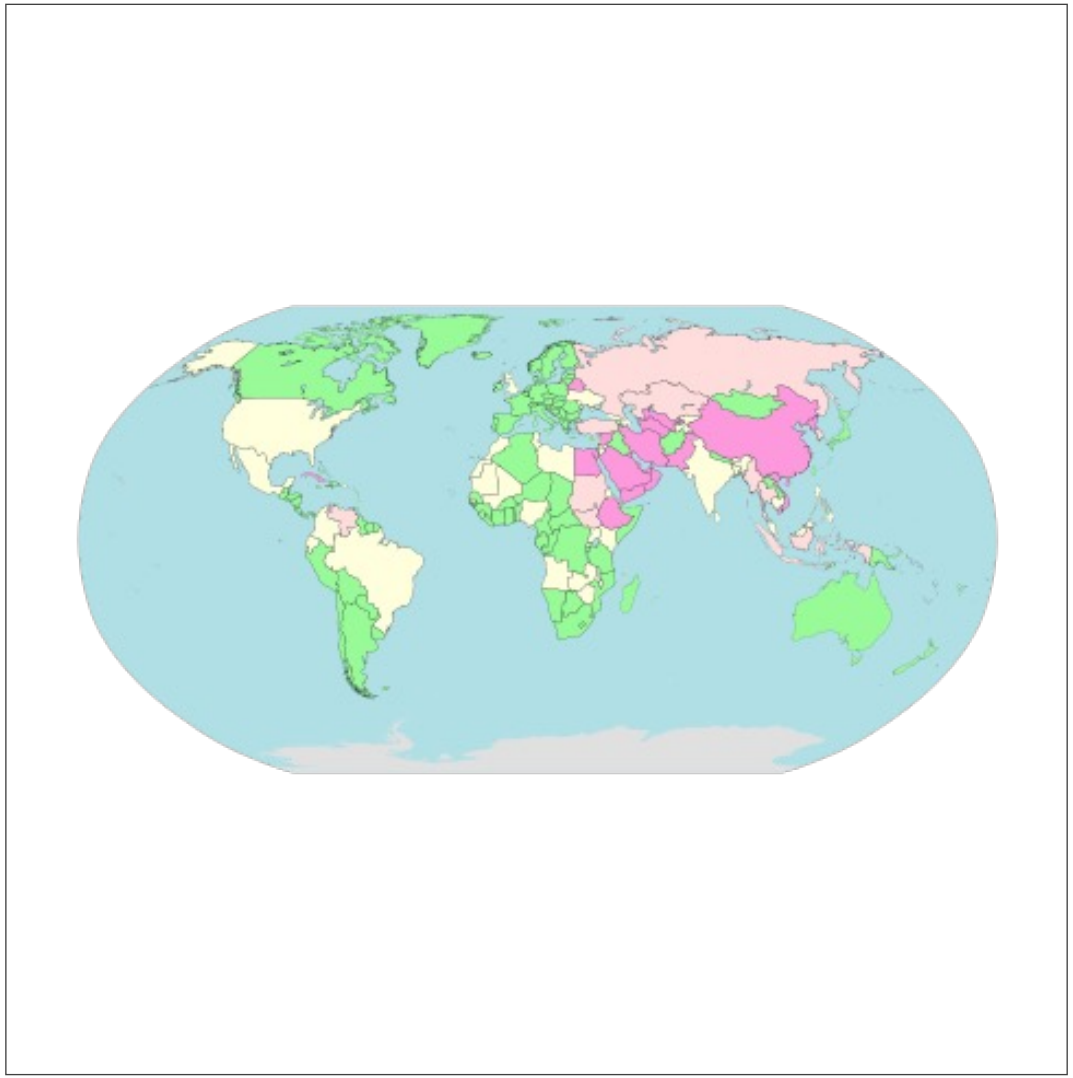
Several DEA and US Secret Service agents convicted of stealing Bitcoin during the Silk Road investigation

Operation Onymous (2014)

- Federal takedown of online drug markets, including Silk Road 2.0
- Facilitated by an attack on the Tor network: multiple relays introduced into the network by a reputable organization (CMU CERT) + a novel exploit of a vulnerability in Tor that enables linkage of entry and exit nodes

Operation DisrupTor (2020)

- Another federal takedown of online drug markets, 179 arrests



Internet Censorship

- Golden Shield Project / Great Firewall of China
- Iran, Syria
- Pakistan (YouTube hijack), Turkey (Twitter ban), Russia
- Singapore, Australia

Filtering Technologies

Censorship mechanism	Circumvention mechanism
IP filtering	Proxies
DNS filter/redirection	DNS proxy (1.1.1.1)
URL filtering	Encryption / Tunneling
Packet filtering (keywords in packets)	Encryption / Tunneling
Protocol filtering (e.g., detect Tor)	Protocol obfuscation

Filtering Devices

- Blue Coat
- NetApp
- SmartFilter software from Secure Computing (bought by McAfee)

Reported use in Syria, Iran, Saudi Arabia

- Embargos prevent direct selling by US companies, but resellers still resell

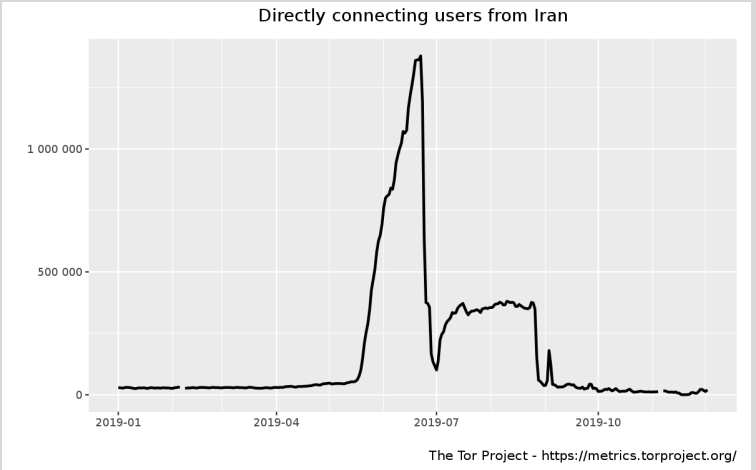
Iran

- Every ISP must run “content-control software”
  - SmartFilter (up until 2009), Nokia Siemens DPI systems
- Filters Facebook, Twitter, YouTube, RapidShare, WordPress, BBC, CNN…
- Occasional widespread filtering of Tor, TLS, other encrypted protocols

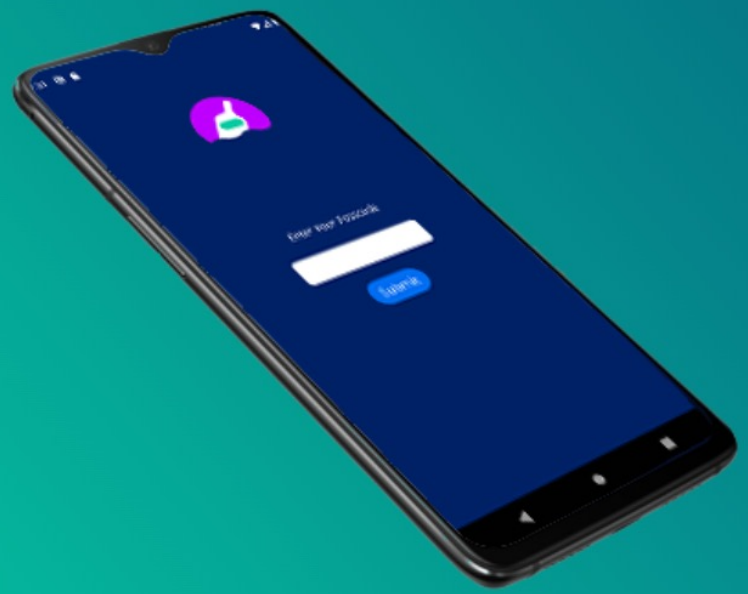
LILY HAY NEWMAN SECURITY 11.17.2019 03:34 PM

How the Iranian Government Shut Off the Internet

After years of centralizing internet control, Iran pulled the plug on connectivity for nearly all of its citizens.



NAHOFT

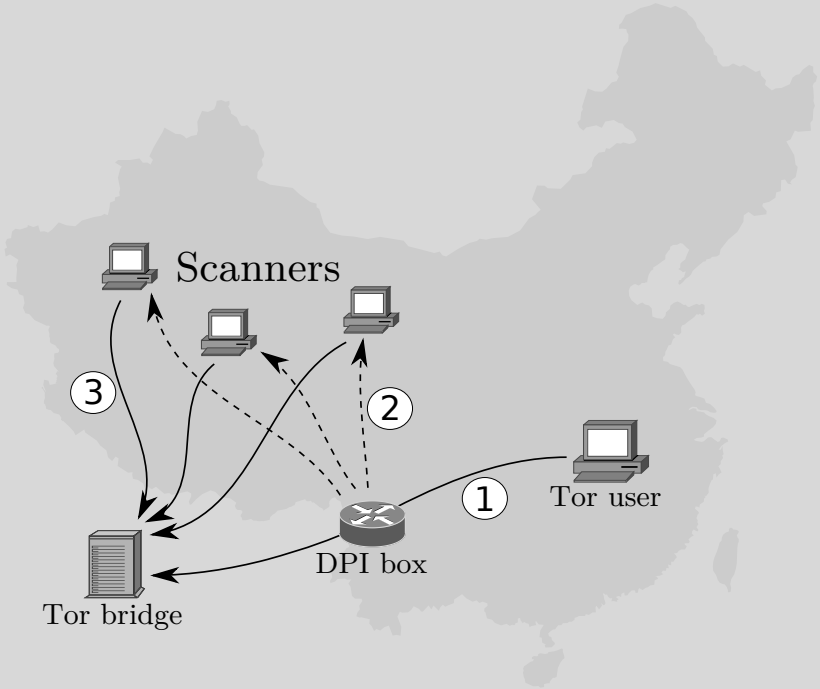


Nahoft is a state-of-the-art encryption app made for Android mobile phones. With Nahoft you can easily encrypt your private message into a string of Persian words or hide your encrypted messages in a photo before sending it safely via any messaging app.

- Does not require Internet
- Sequence of coded words can be sent by letter, read over the phone, or transmitted over a channel where content is scanned
- Recipient uses their app to decode

The Great Firewall of China

- IP filtering
- DNS filtering / redirection
- URL filtering
- Packet filtering
  - Search for keywords in TCP packets, send TCP FIN both ways
- Protocol filtering
  - Tor is mostly shut down



Source: Winter, Lindskog (2012)

Get connected

If you are in a country where Tor is blocked, you can configure Tor to connect to a bridge during the setup process.

Select "Tor is censored in my country."

Tor Bridges

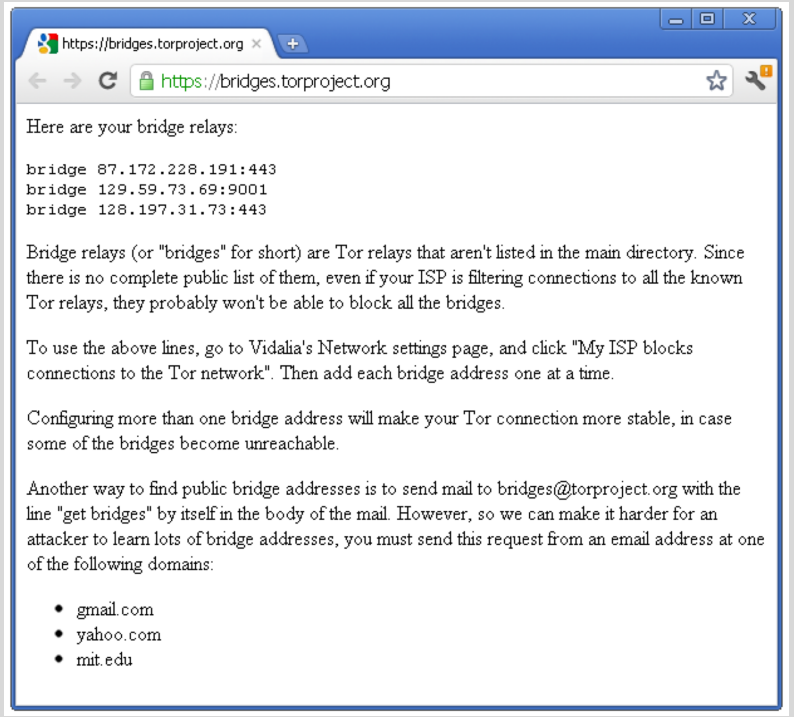
Anyone can look up the IP addresses of Tor relays

- Public information in the consensus file

Many countries block traffic to these IPs

Solution: Tor bridges

- Tor proxies that are not publicly known



Obfuscating Tor Traffic

Bridges alone do not get around all types of censorship

- DPI can be used to locate and drop Tor frames

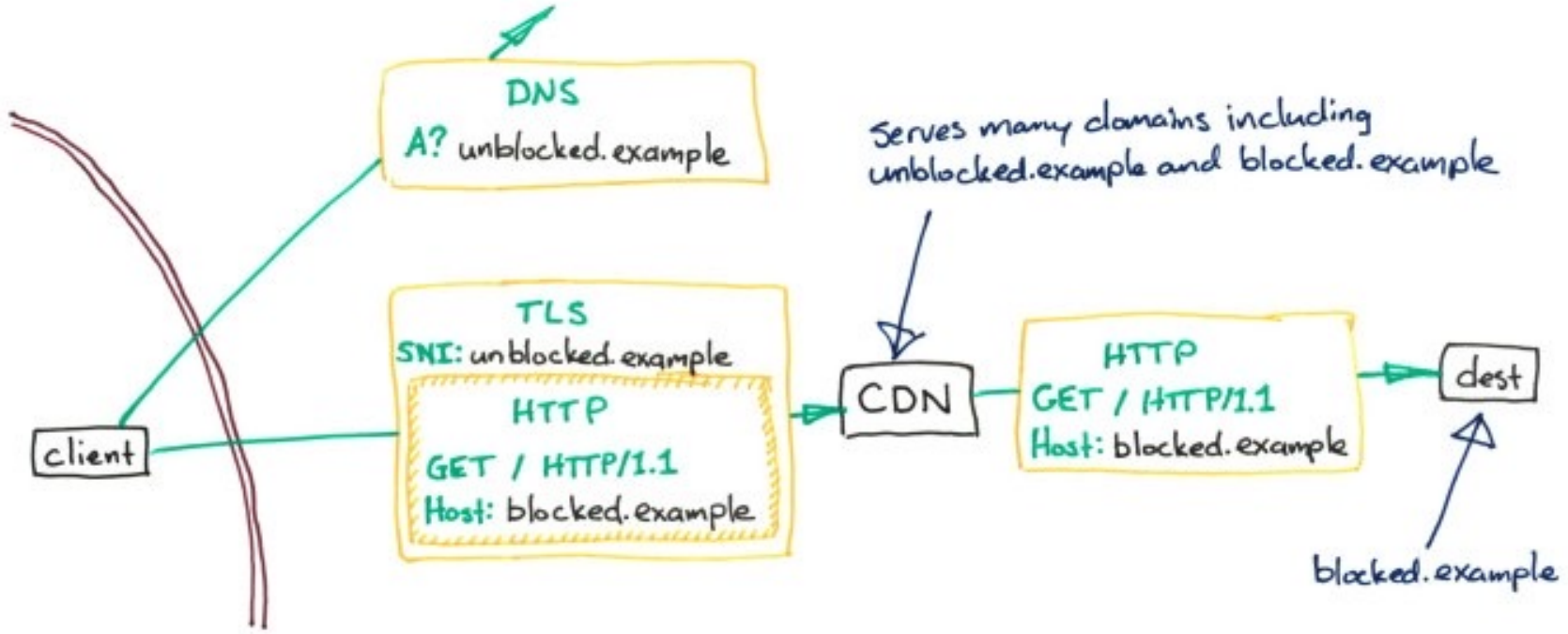
Countries can passively detect and block bridges

- Single-use bridges

Tor adopts a pluggable transport design

- Tor traffic is forwarded to an obfuscation program
- Obfuscator transforms the Tor traffic to look like some other protocol (BitTorrent, Skype, HTTP, streaming audio, ...)

DOMAIN FRONTING

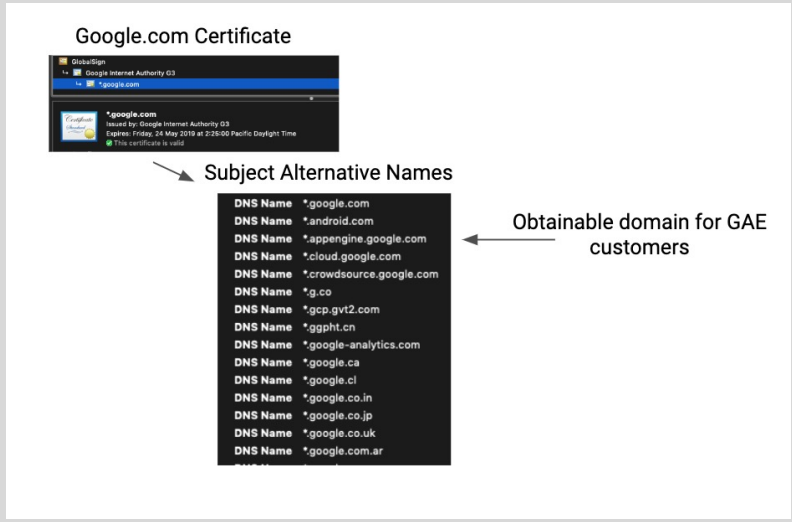


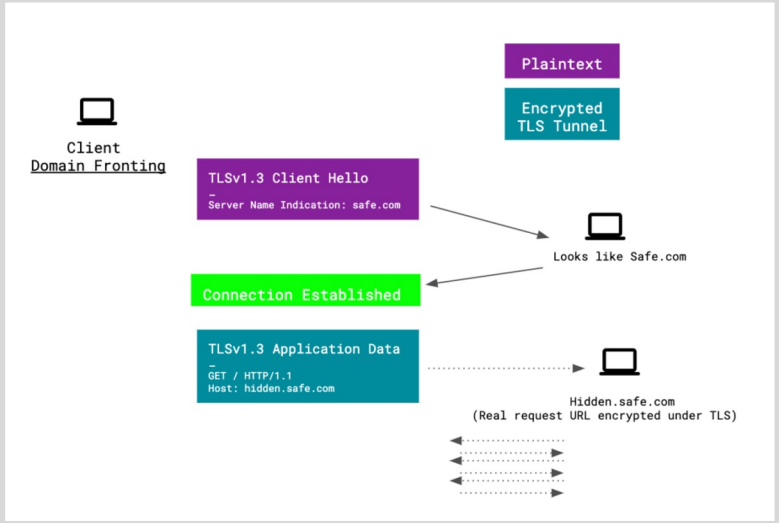
TLS SNI doesn't match HTTP Host header.
The censor sees only the TLS SNI and DNS request.
Intermediary CDN routes according to the Host header.

credit: bamsoftware.com

Domain Fronting in Tor

Tor would place bridges in hidden domains behind standard cloud-service domains: Google App Engine, Amazon CloudFront/EC2, Microsoft Azure





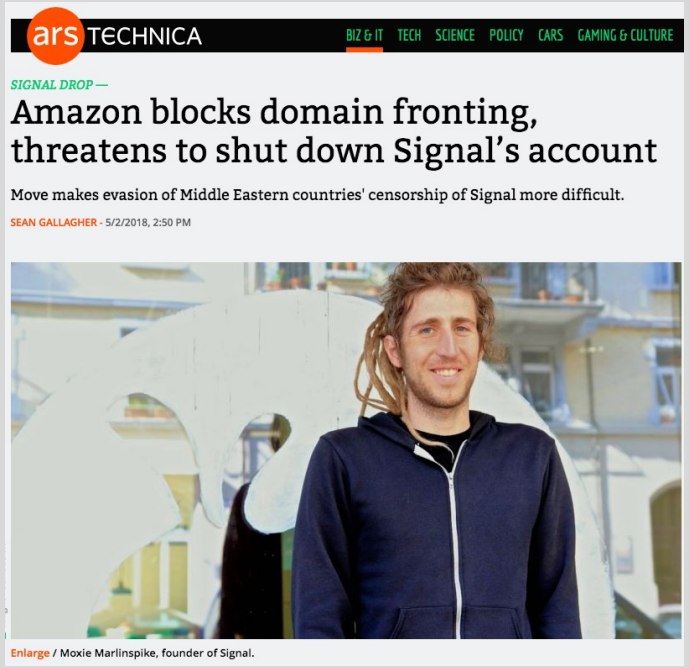
... and use domain fronting to access the bridges

https://www.sentinelone.com/blog/privacy-2019-tor-meek-rise-fall-domain-fronting/

Domain Fronting in Signal

Used by Signal and Telegram to evade blocking in Egypt, UAE, Qatar, Oman…

But:



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

SIGNAL DROP —

Amazon blocks domain fronting, threatens to shut down Signal's account

Move makes evasion of Middle Eastern countries' censorship of Signal more difficult.

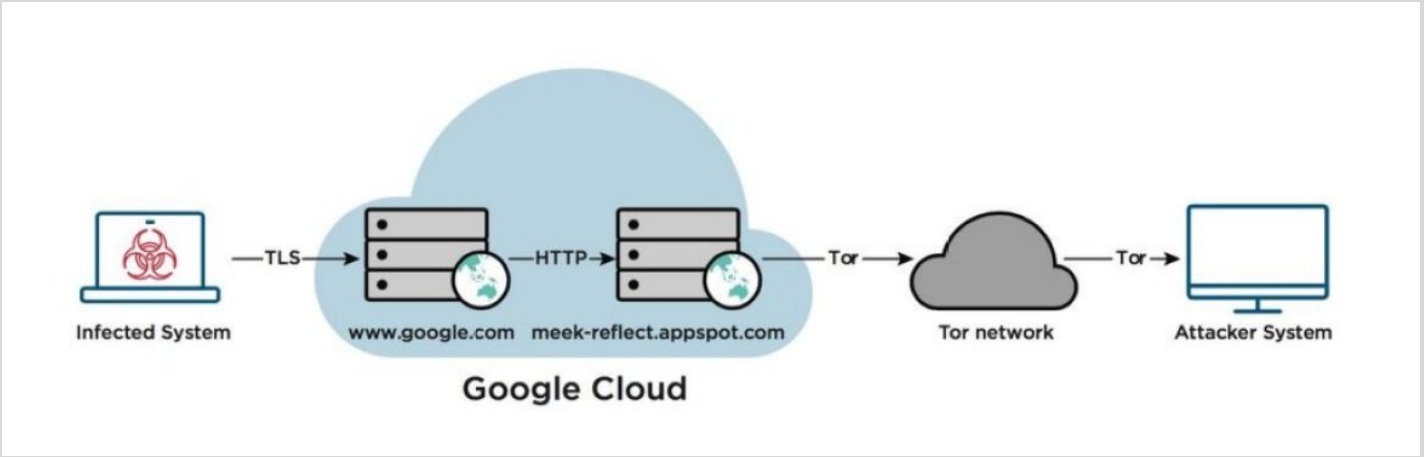
SEAN GALLAGHER - 5/2/2018, 2:50 PM

Enlarge / Moxie Marlinspike, founder of Signal.

APT29 Domain Fronting with Tor

Russian “Cozy Bear” hacker group used domain fronting to access a Tor hidden service from compromised machines

Responsible for many attacks, including the DNC hack in 2016, attempts to steal vaccine data in July 2020…



https://www.fireeye.com/blog/threat-research/2017/03/apt29_domain_frontin.html