CS 5435

Surveillance
Anonymity Networks
Censorship Resistance

Vitaly Shmatikov

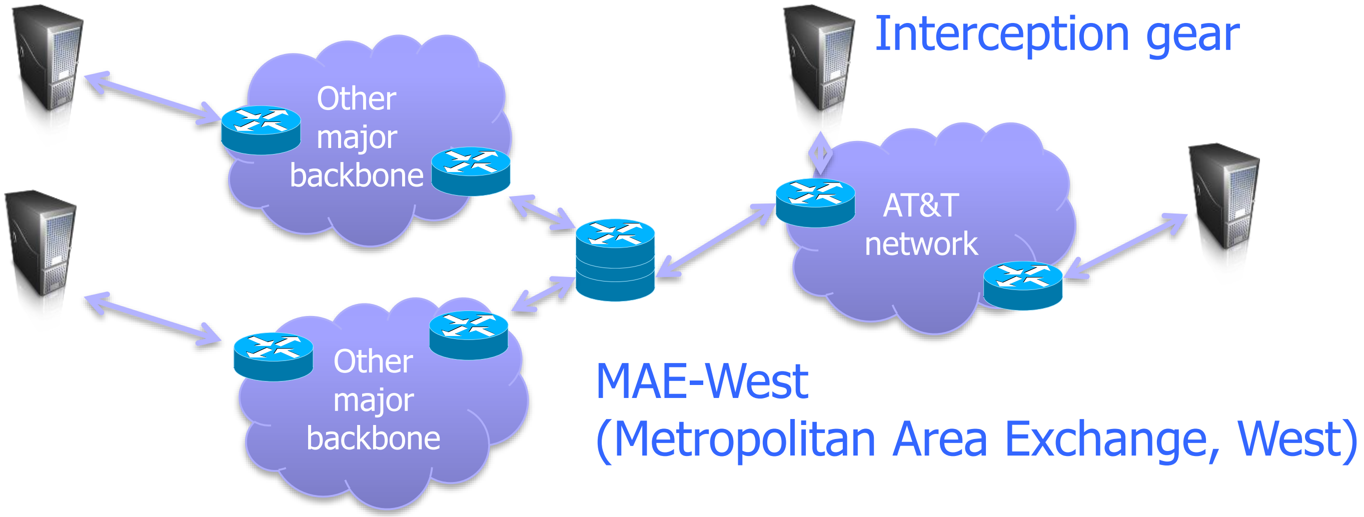
AT&T Wiretap Case

Mark Klein discloses potential wiretapping activities by NSA at San Francisco AT&T office in 2006

Fiber optic splitter on major trunk line for Internet communications

- Electronic voice and data communications copied to "secret room"
- Narus STA 6400 device

Wiretap Surveillance



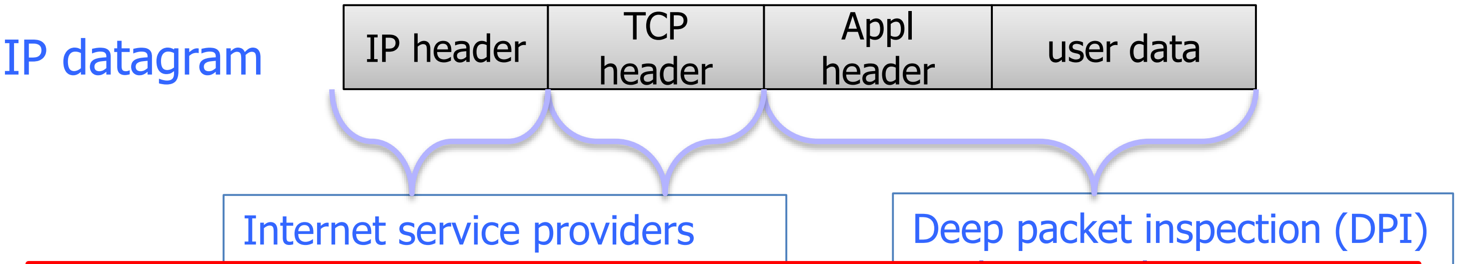
Large amounts of Internet traffic cross relatively few key points

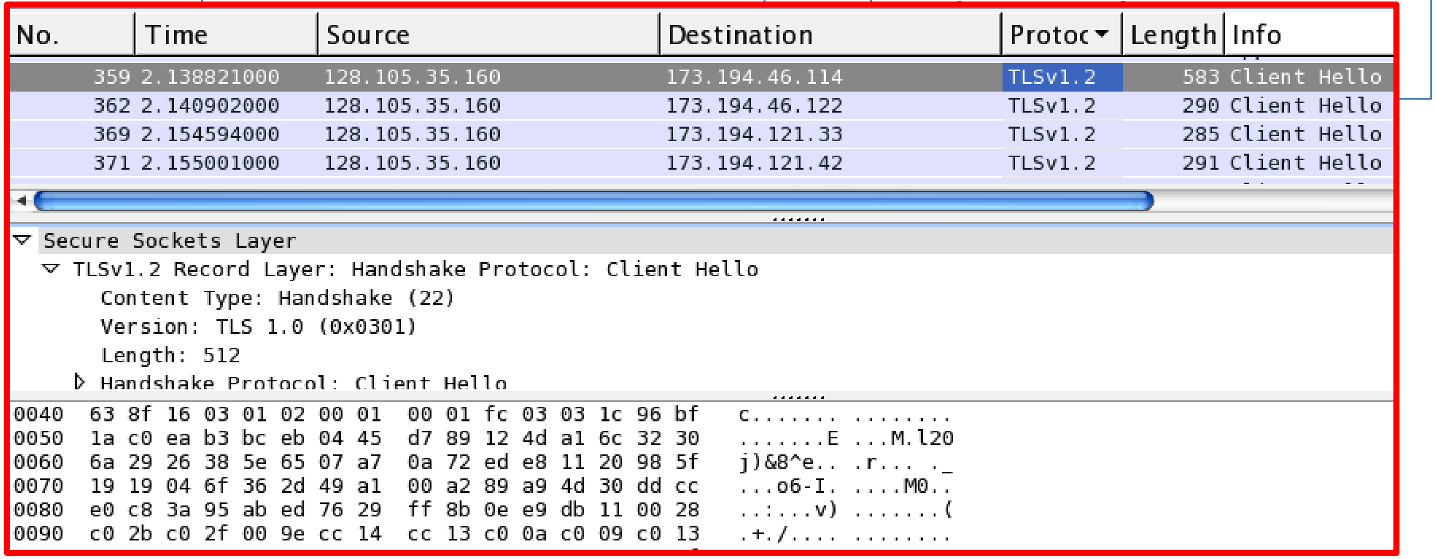
Interception Technology

From Narus' website

- "Target by phone number, URI, email account, user name, keyword, protocol, application and more"
- "Service- and network agnostic"
- "IPV 6 ready"
- Collects at wire speeds beyond 10 Gbps

Types of Packet Inspection





```
No.   Time         Source            Destination       Protoc  Length Info
  359 2.138821000  128.105.35.160    173.194.46.114    TLSv1.2    583 Client Hello
  362 2.140902000  128.105.35.160    173.194.46.122    TLSv1.2    290 Client Hello
  369 2.154594000  128.105.35.160    173.194.121.33    TLSv1.2    285 Client Hello
  371 2.155001000  128.105.35.160    173.194.121.42    TLSv1.2    291 Client Hello
```

```
▽ Secure Sockets Layer
  ▽ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    ▷ Handshake Protocol: Client Hello
```

```
0040  63 8f 16 03 01 02 00 01  00 01 fc 03 03 1c 96 bf   c....... ........
0050  1a c0 ea b3 bc eb 04 45  d7 89 12 4d a1 6c 32 30   .......E ...M.l20
0060  6a 29 26 38 5e 65 07 a7  0a 72 ed e8 11 20 98 5f   j)&8^e.. .r... ._
0070  19 19 04 6f 36 2d 49 a1  00 a2 89 a9 4d 30 dd cc   ...o6-I. ....M0..
0080  e0 c8 3a 95 ab ed 76 29  ff 8b 0e e9 db 11 00 28   ..:...v) .......(
0090  c0 2b c0 2f 00 9e cc 14  cc 13 c0 0a c0 09 c0 13   .+./.... ........
```

Lawful Intercept in the United States

CALEA: Communications Assistance for Law Enforcement Act (1995)

FISA: Foreign Intelligence Surveillance Act (1978)

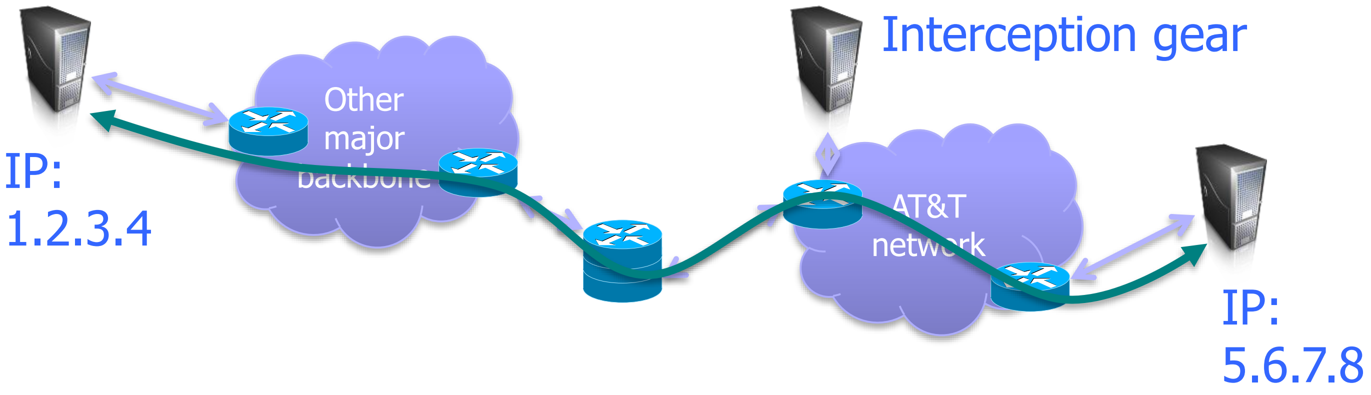
- Separates domestic vs. foreign intelligence gathering
- Foreign Intelligence Surveillance Court (FISC) provides warrant oversight – efficacy sometimes criticized

Also applies to data hosted by services (Gmail, …)

Most (almost all?) national governments mandate some kind of lawful intercept capabilities

Preventing Intercept

End-to-end encryption (TLS, SSH)



What does this protect? What does it leak?

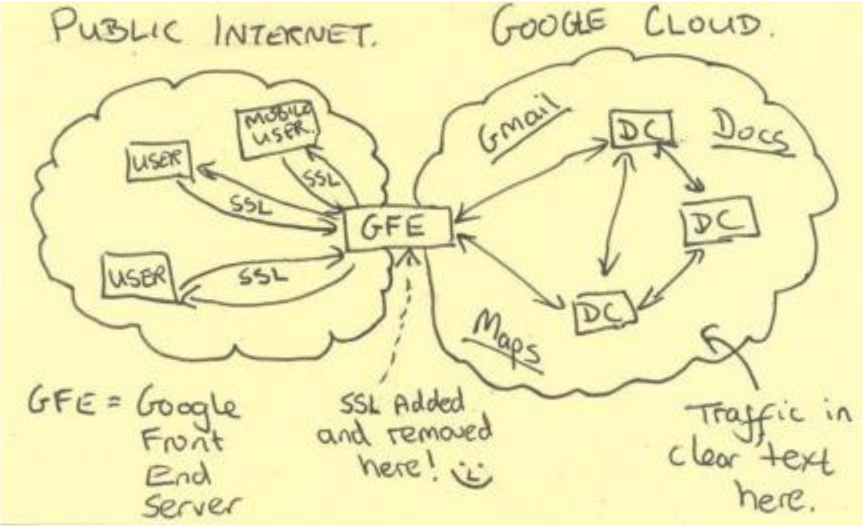
What can go wrong?

End-run Around HTTPS

HTTPS terminated at edge of Google networks

Internal data center-to-data center communications on privately leased lines

- No encryption up until summer 2013


PUBLIC INTERNET.
GOOGLE CLOUD.
USER
MOBILE USER.
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

We kill people based on metadata

Michael Hayden
Former Director,
National Security Agency

Privacy on Public Networks

Internet is designed as a public network

Routing information is public

- IP packet headers identify source and destination
- Even a passive observer can easily figure out who is talking to whom

Encryption does not hide identities

- Encryption hides payload, but not routing headers
- Even IP-level encryption (VPNs, tunnel-mode IPsec) reveals IP addresses of gateways

Chaum’s Mix

Early proposal for anonymous email

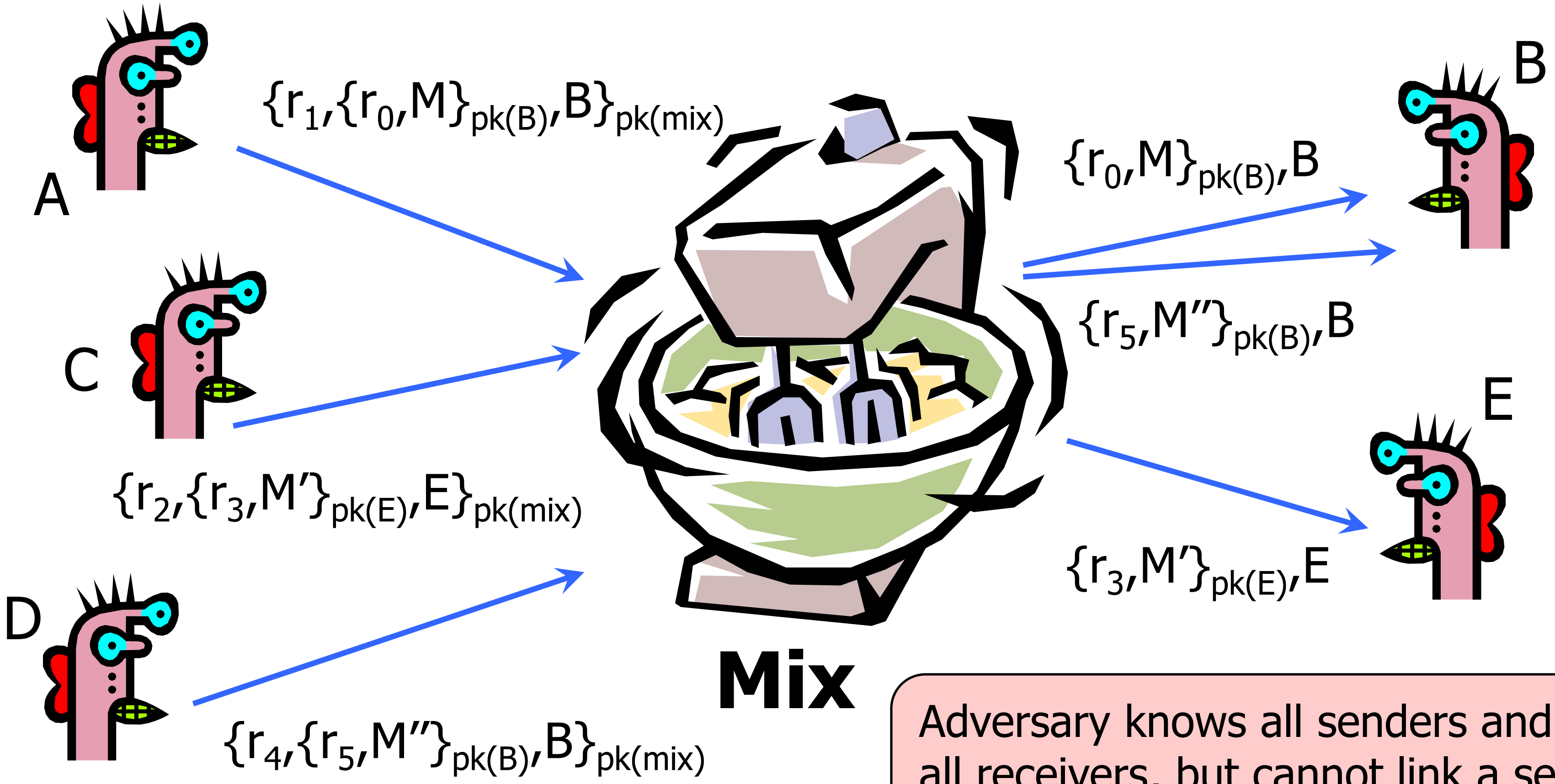
- David Chaum. “Untraceable electronic mail, return addresses, and digital pseudonyms”. Communications of the ACM, February 1981.

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



A

$\{r_1,\{r_0,M\}_{pk(B)},B\}_{pk(mix)}$

C

$\{r_2,\{r_3,M'\}_{pk(E)},E\}_{pk(mix)}$

D

$\{r_4,\{r_5,M''\}_{pk(B)},B\}_{pk(mix)}$

Mix

B

$\{r_0,M\}_{pk(B)},B$

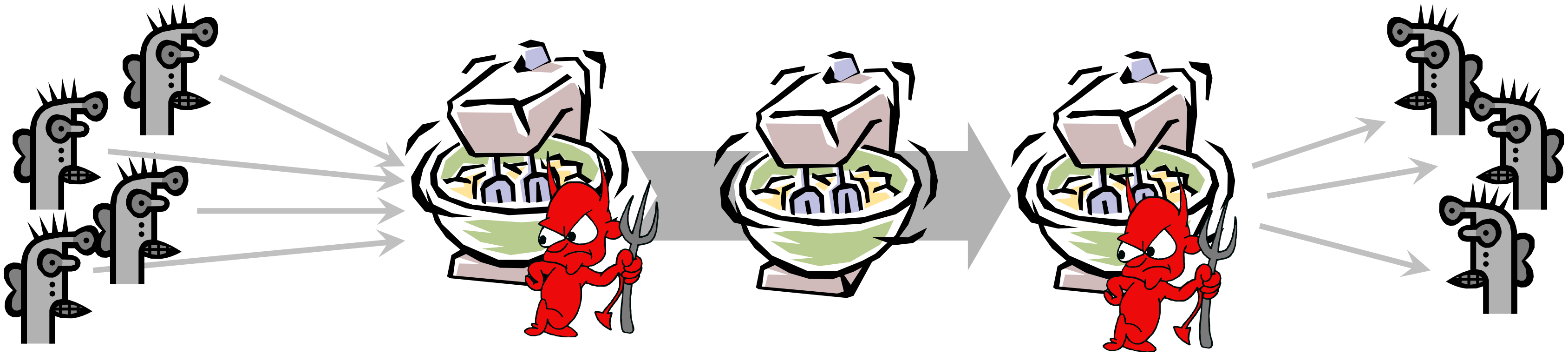
$\{r_5,M''\}_{pk(B)},B$

E

$\{r_3,M'\}_{pk(E)},E$

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

Disadvantages of Basic Mixnets

Public-key encryption and decryption at each mix are computationally expensive

Basic mixnets have high latency

- Ok for email, but not for Web browsing

Challenge: low-latency anonymity network

- Use public-key crypto to establish a “circuit” with pairwise symmetric keys between hops
- Then use symmetric decryption and re-encryption to move data along the established circuits

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

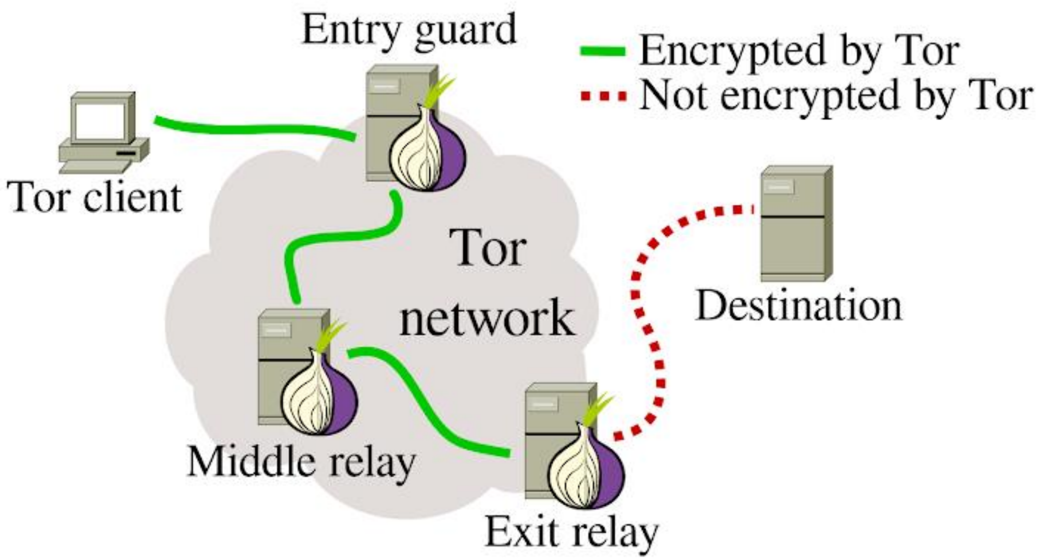
Over 2,500,000 users

“Easy-to-use” client

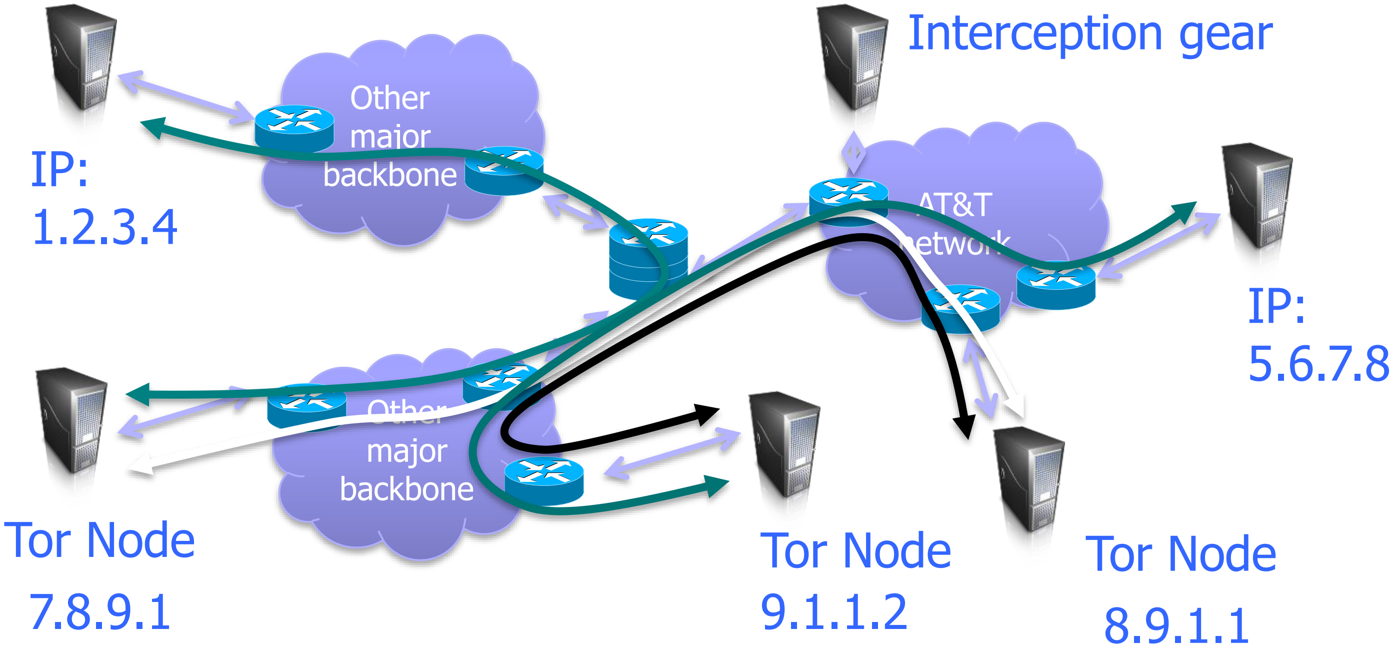
- Freely available, can use it for anonymous browsing

Tor (The Onion Router)

Main idea: tunnel traffic through multiple “onion routers” using public key cryptography

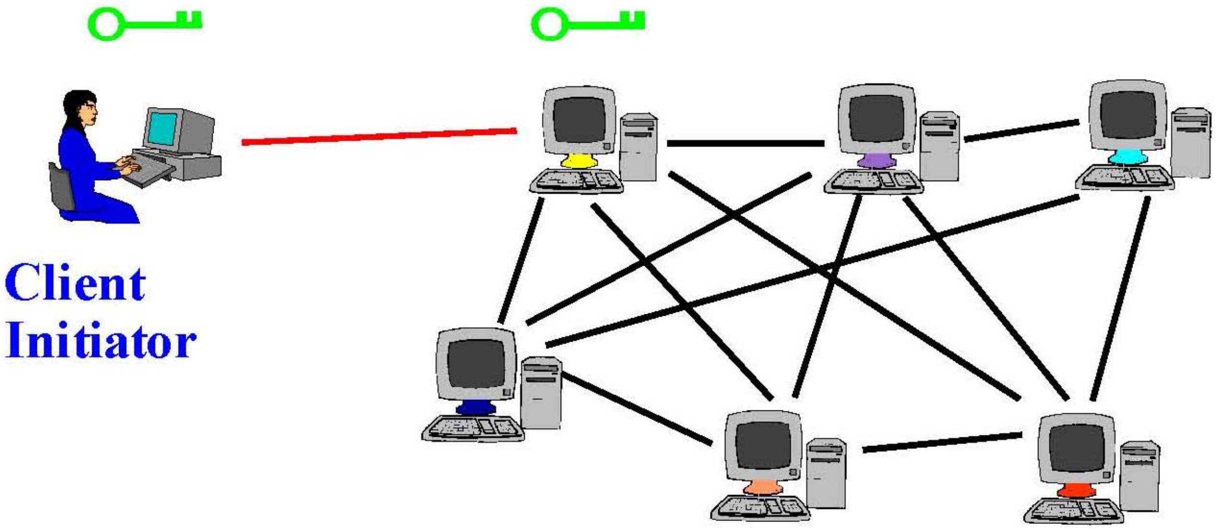


Tor Operation



Tor Circuit Setup (1)

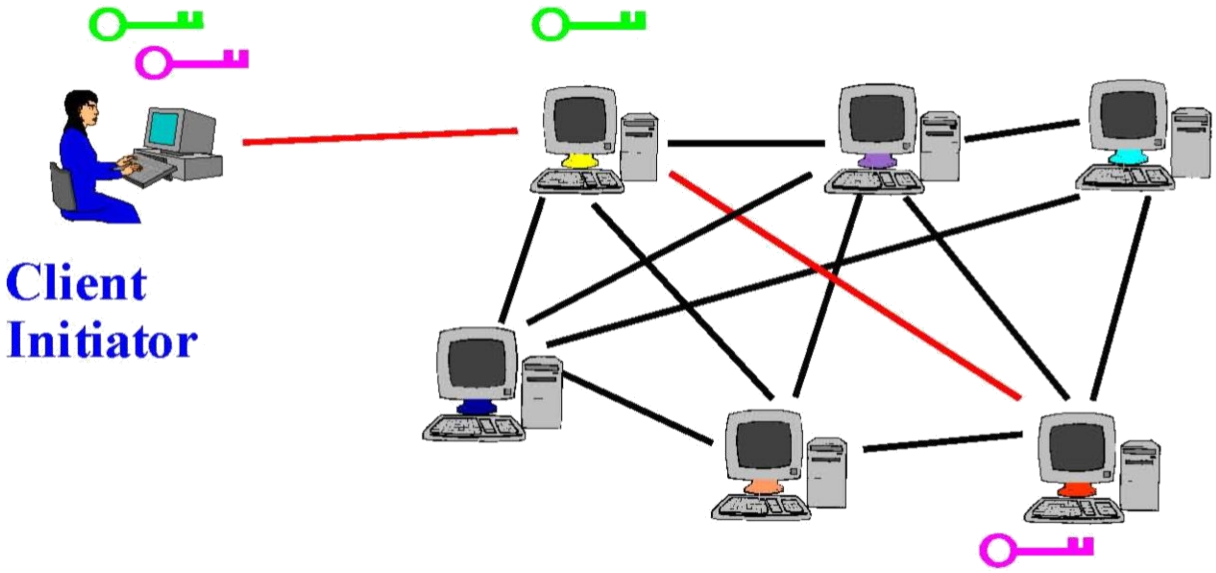
Client proxy establishes a symmetric session key and circuit with Onion Router #1



Tor Circuit Setup (2)

Client proxy extends the circuit by establishing a symmetric session key with Onion Router #2

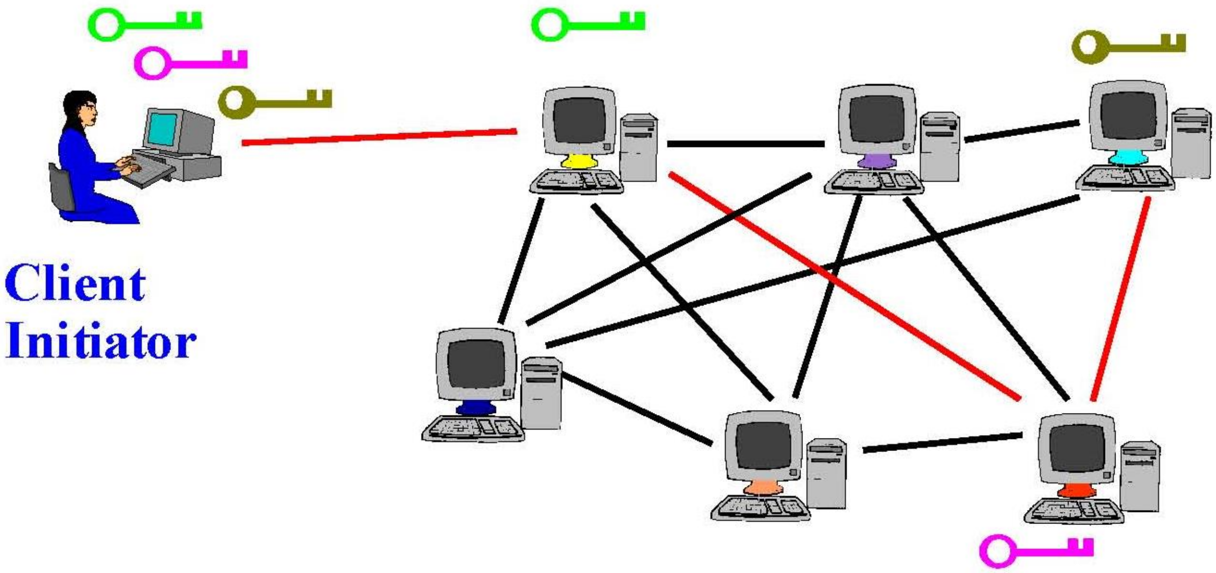
- Tunnel through Onion Router #1



Tor Circuit Setup (3)

Client proxy extends the circuit by establishing a symmetric session key with Onion Router #3

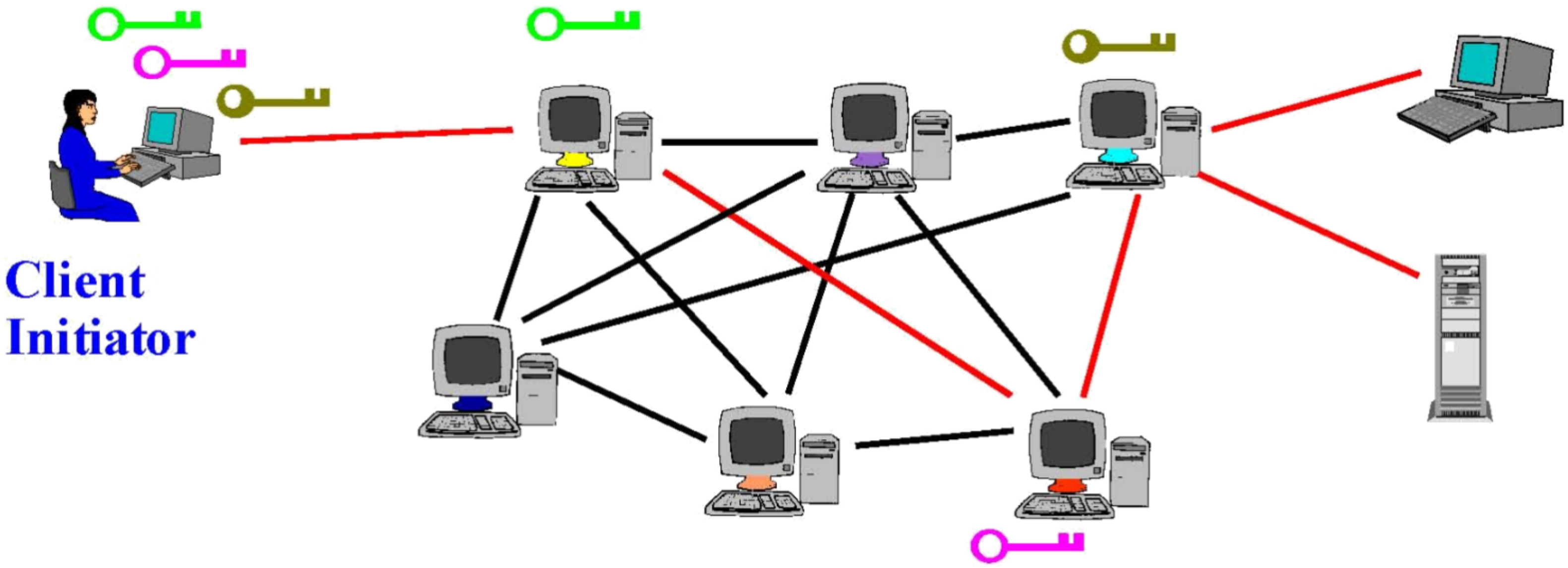
- Tunnel through Onion Routers #1 and #2



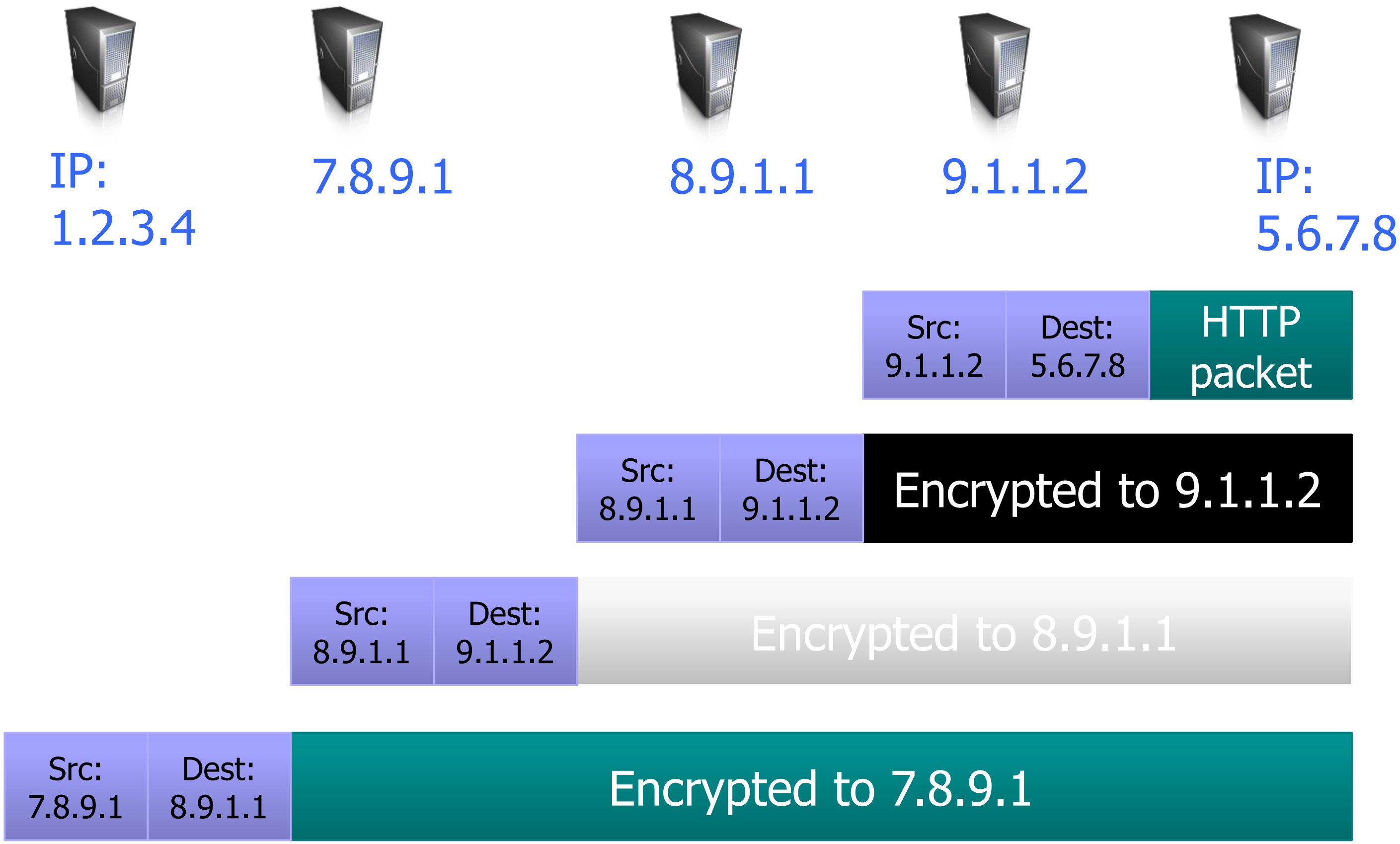
Using a Tor Circuit

Client applications connect and communicate over the established Tor circuit

- Datagrams decrypted and re-encrypted at each link



Onion Routing (Basic Idea)



IP: 1.2.3.4

7.8.9.1

8.9.1.1

9.1.1.2

IP: 5.6.7.8

Src: 9.1.1.2 | Dest: 5.6.7.8 | HTTP packet

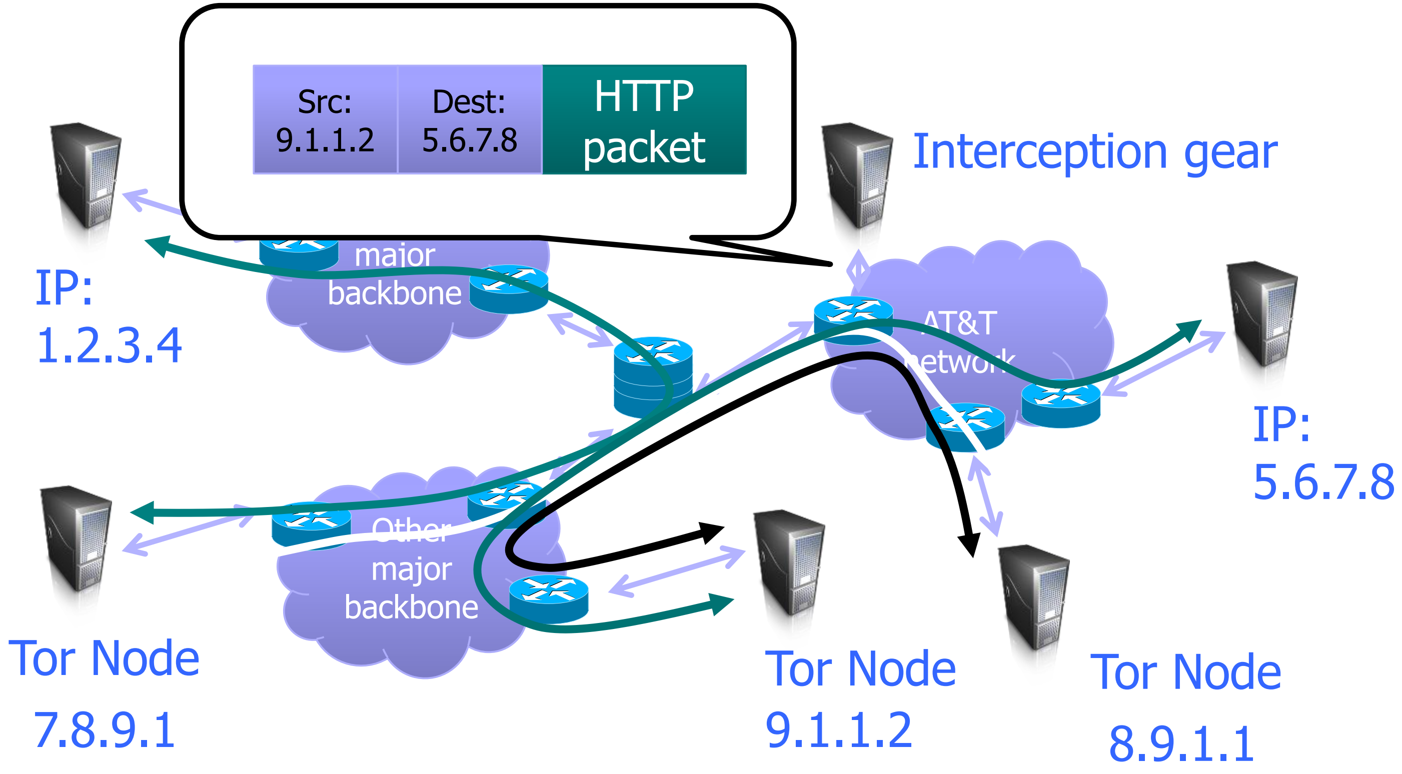
Src: 8.9.1.1 | Dest: 9.1.1.2 | Encrypted to 9.1.1.2

Src: 8.9.1.1 | Dest: 9.1.1.2 | Encrypted to 8.9.1.1

Src: 7.8.9.1 | Dest: 8.9.1.1 | Encrypted to 7.8.9.1

Tor implements more complex version of this basic idea

What Does Adversary See?



Src: 9.1.1.2	Dest: 5.6.7.8	HTTP packet

Tor obfuscates who talked to whom, need end-to-end encryption (e.g., HTTPS) to protect payload

Who Knows What?

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

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

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

Tor does not provide encryption between exit and destination (use HTTPS!)

Tor Anonymity Properties

Goal: anonymity in TCP connections over the Internet, both unlinkably (long-term) and linkably (short-term)

What does this mean?

- There’s no long-term identifier for a Tor user
- If a web server gets a connection from Tor today, and another one tomorrow, it won’t be able to tell whether those are from the same person
- But two connections in quick succession from the same Tor node are more likely to in fact be from the same person

Tor Management Issues

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

Directory servers

- Lists of active onion routers, their locations, current public keys, etc.
- Control how new routers join the network
  - "Sybil attack": attacker creates a large number of routers
- Directory servers' keys ship with Tor code

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 censorship

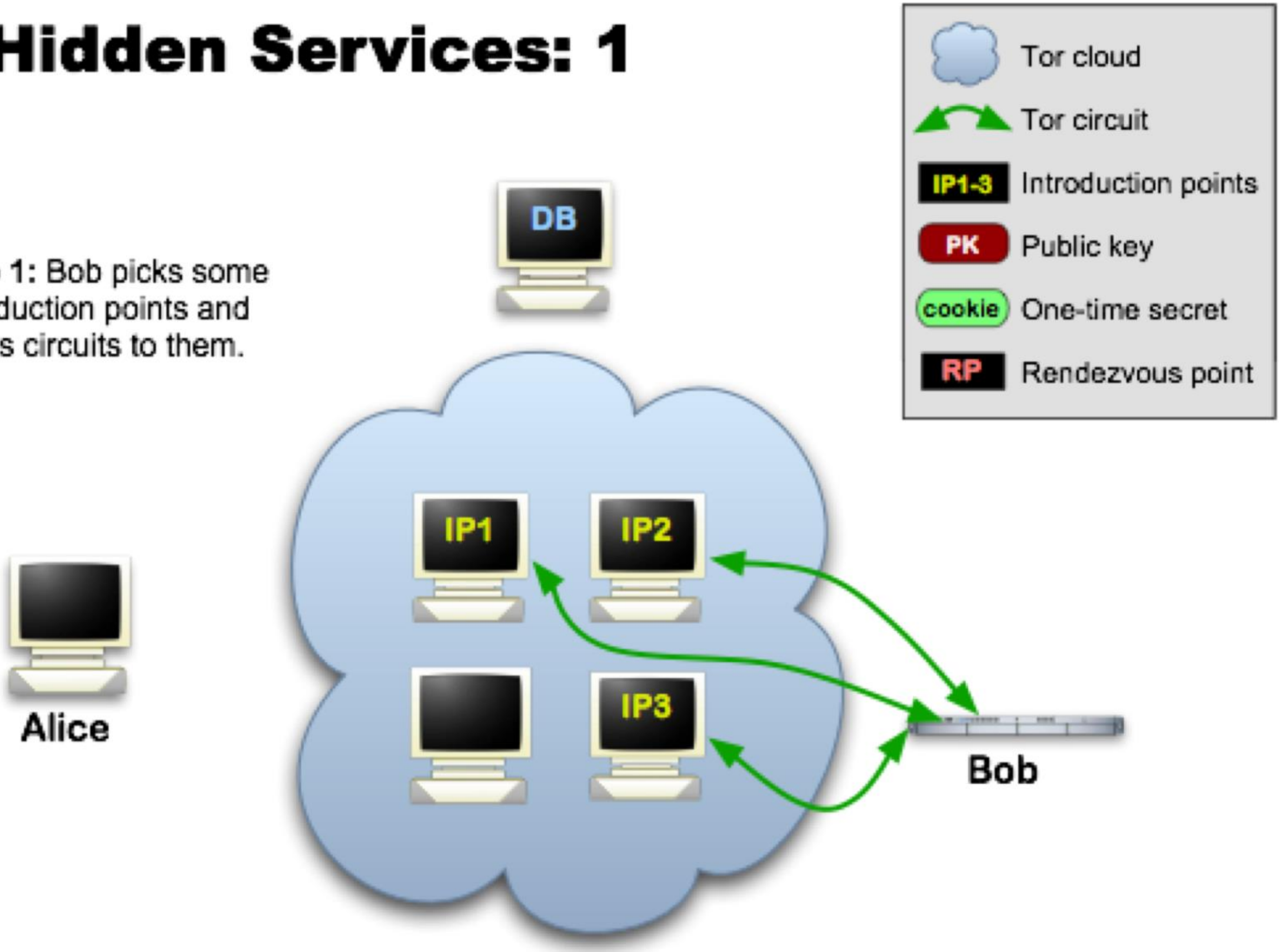
Can survive a full-blown DoS attack

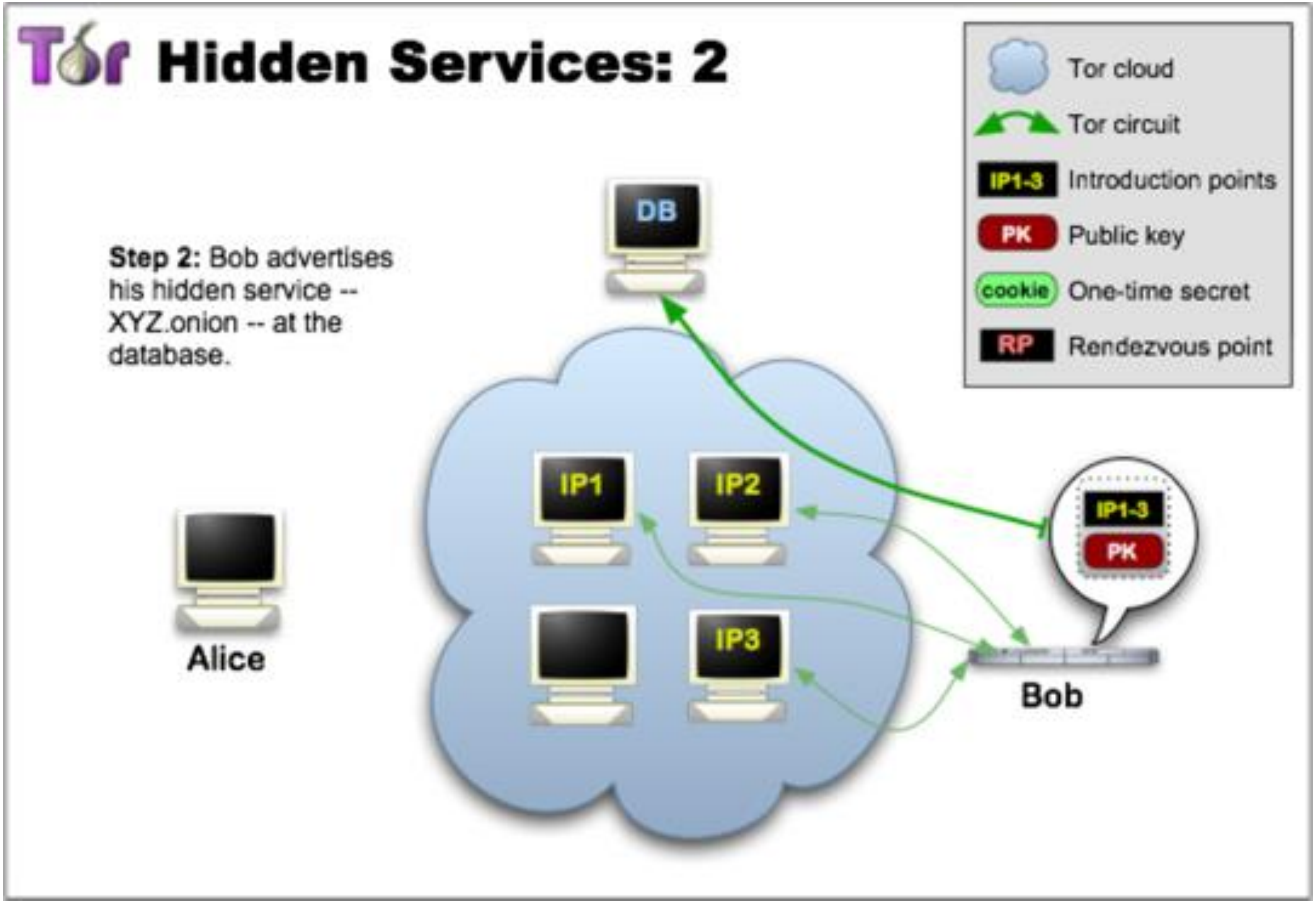
Resistant to physical attack

- Can't find the physical server!

Tor Hidden Services: 1

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





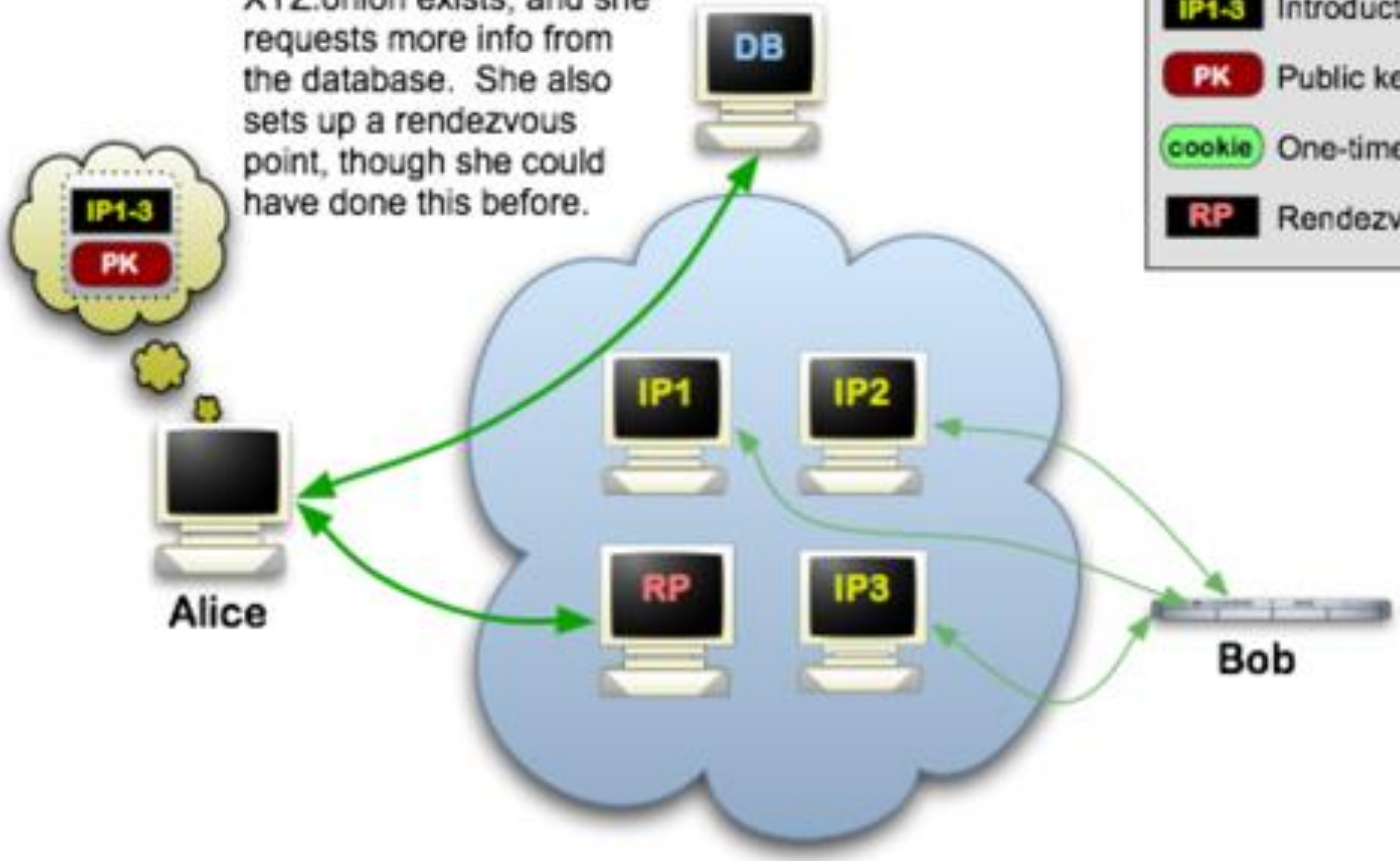
Tor Hidden Services: 2

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

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

Tor Hidden Services: 3

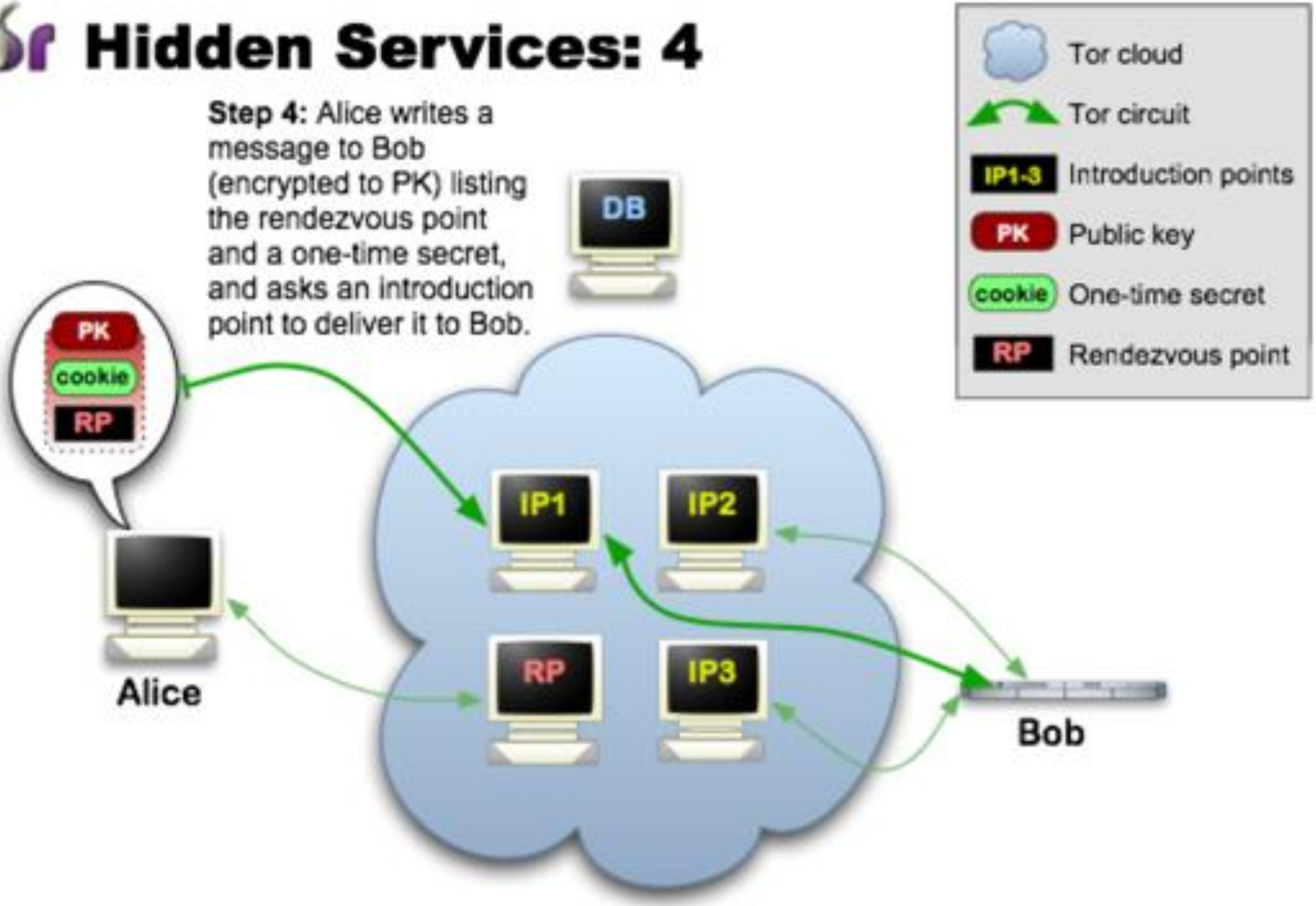
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

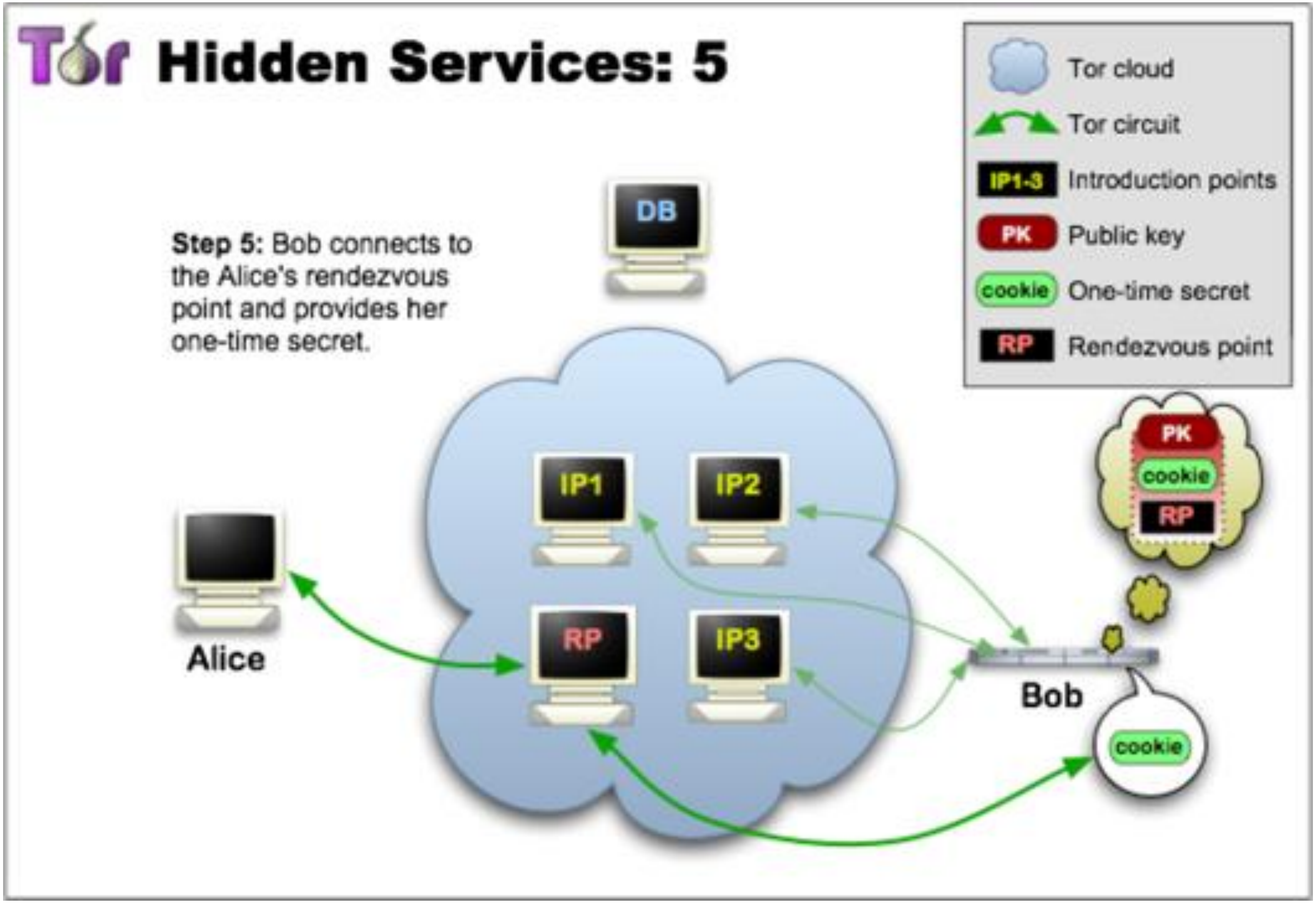


☁	Tor cloud
⇄	Tor circuit
IP1-3	Introduction points
PK	Public key
cookie	One-time secret
RP	Rendezvous point

Tor 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.

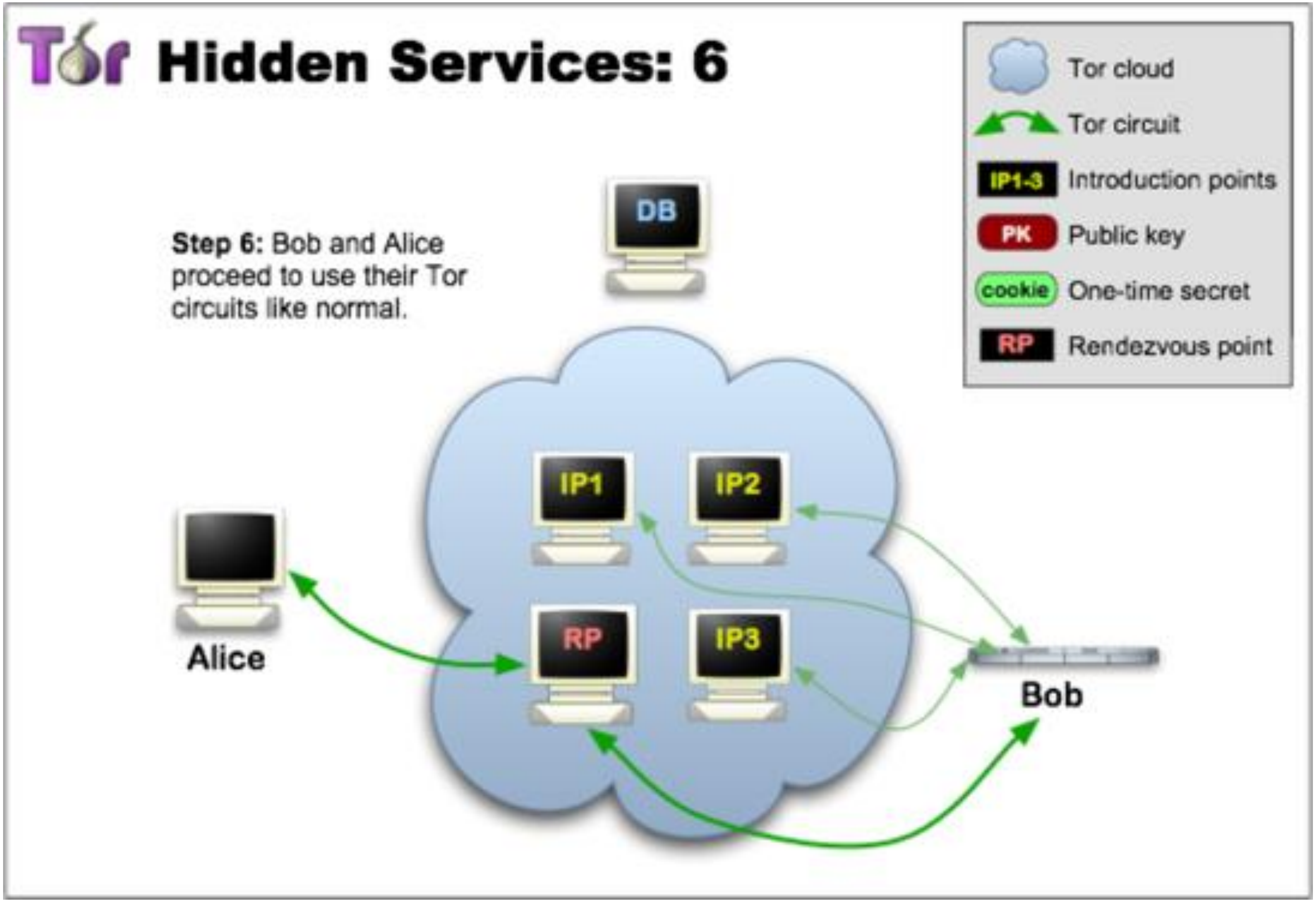




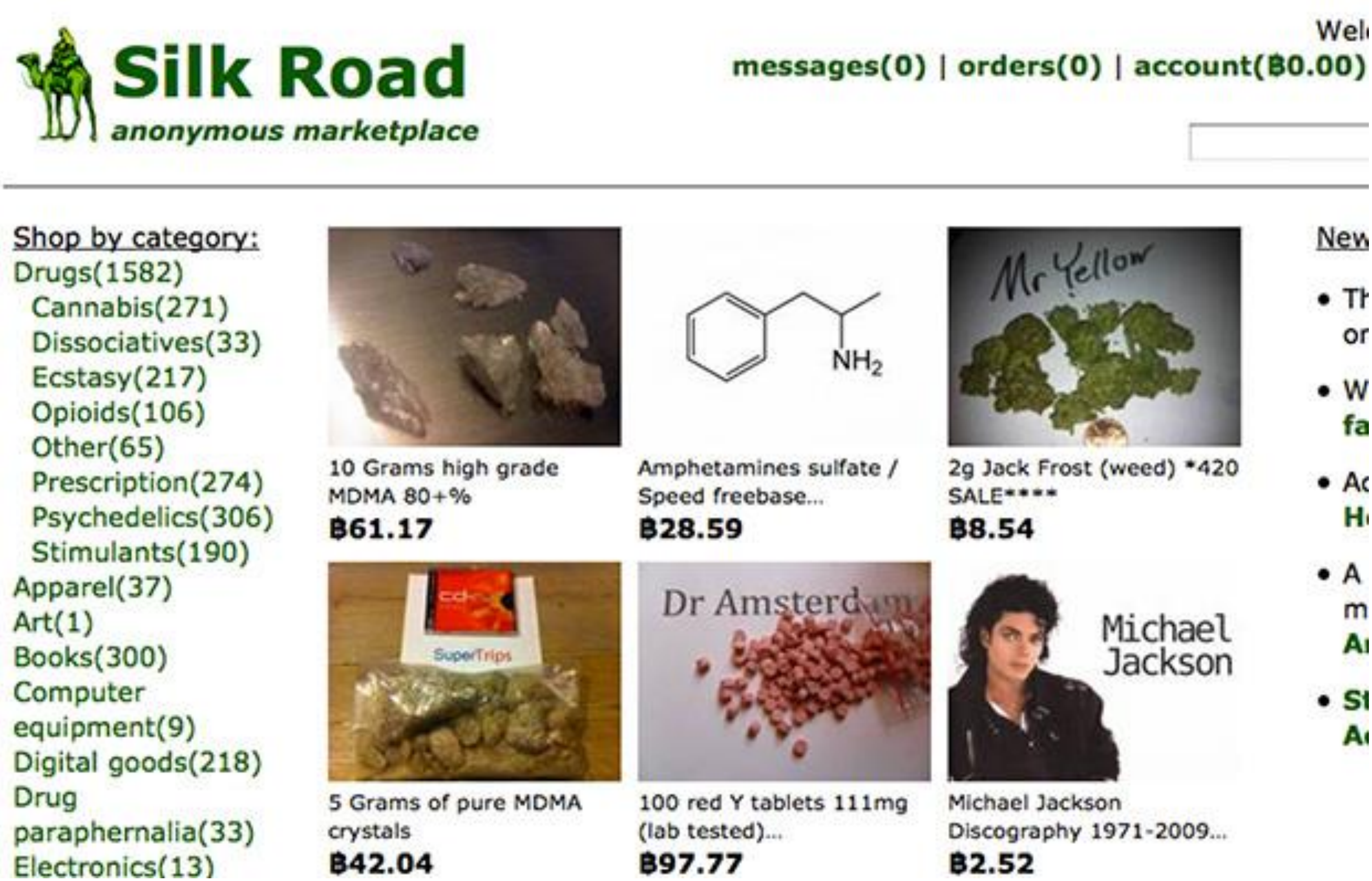
Tor Hidden Services: 5

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

Tor Hidden Services: 6



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



Wel

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

Silk Road

anonymous marketplace

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

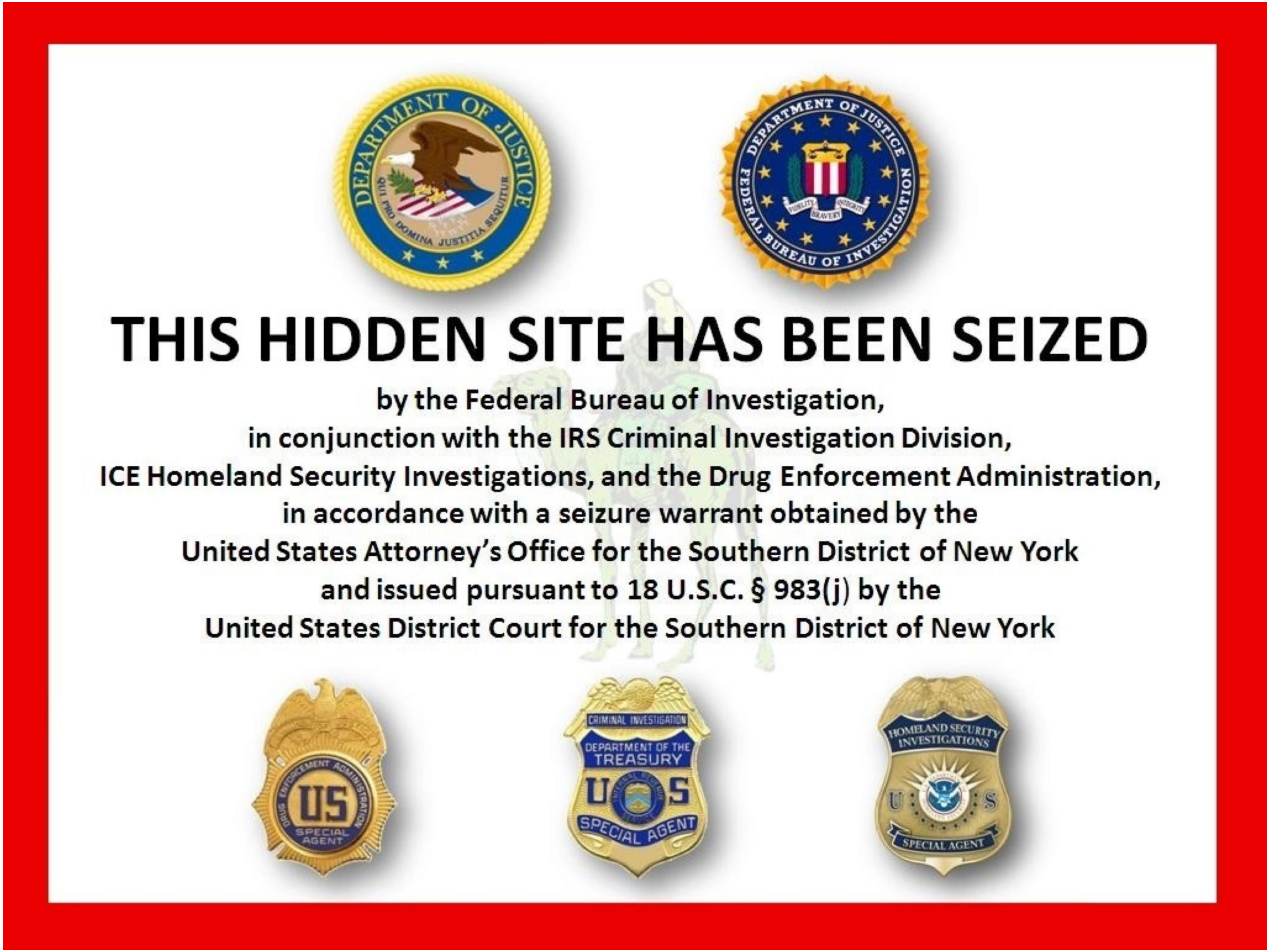
5 Grams of pure MDMA crystals
฿42.04

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
Ar
- **St**
Ac

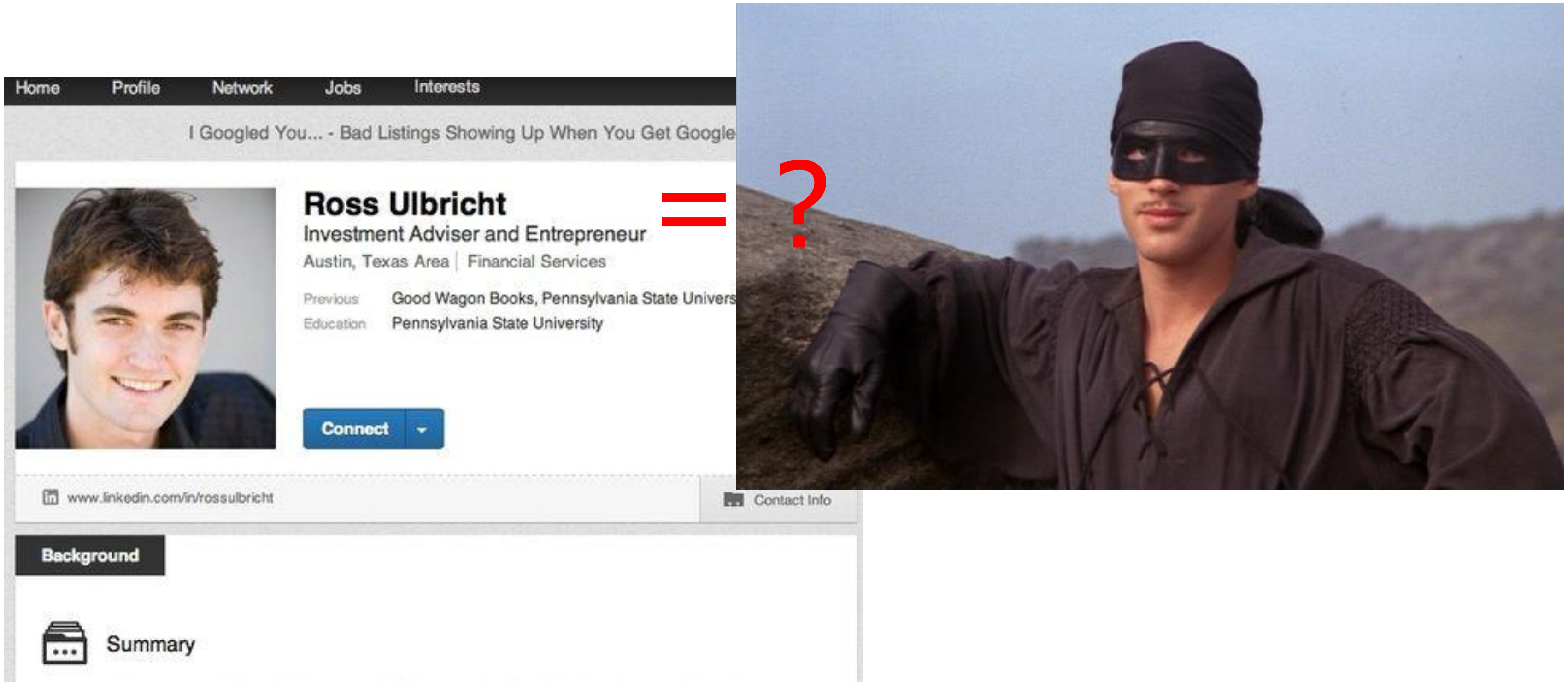


THIS HIDDEN SITE HAS BEEN SEIZED

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, alleged operator of the Silk Road Marketplace, arrested by the FBI on Oct 1, 2013



I Googled You... - Bad Listings Showing Up When You Get Google

Ross Ulbricht

Investment Adviser and Entrepreneur

Austin, Texas Area | Financial Services

Previous Good Wagon Books, Pennsylvania State Univers

Education Pennsylvania State University

Silk Road Shutdown Theories

A package of fake IDs from Canada traced to an apartment to San Francisco?

A fake murder-for-hire arranged by DPR?

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"
- … oh, and the encryption key on the Silk Road server ends with the substring "frosty@frosty"

Probably <u>not</u> weaknesses in Tor

How Was Silk Road Located?

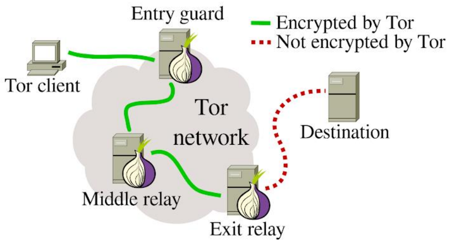
FBI agent Tarbell’s testimony:

- 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 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?

Guard Relays



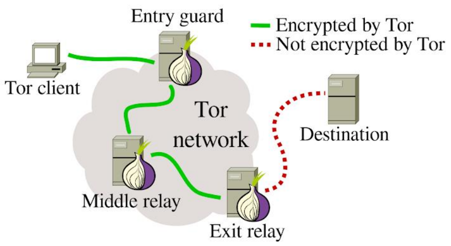
How do you protect against an adversary creating a large number of onion routers and performing timing observation at entrance and exits?

Limit the servers used for initial connection to a subset of trusted nodes:

- Have long and consistent uptimes…
- Have high bandwidth…
- Are manually vetted by the Tor community

Tor client selects 3 guard relays and uses them for 3 months

Exit Nodes

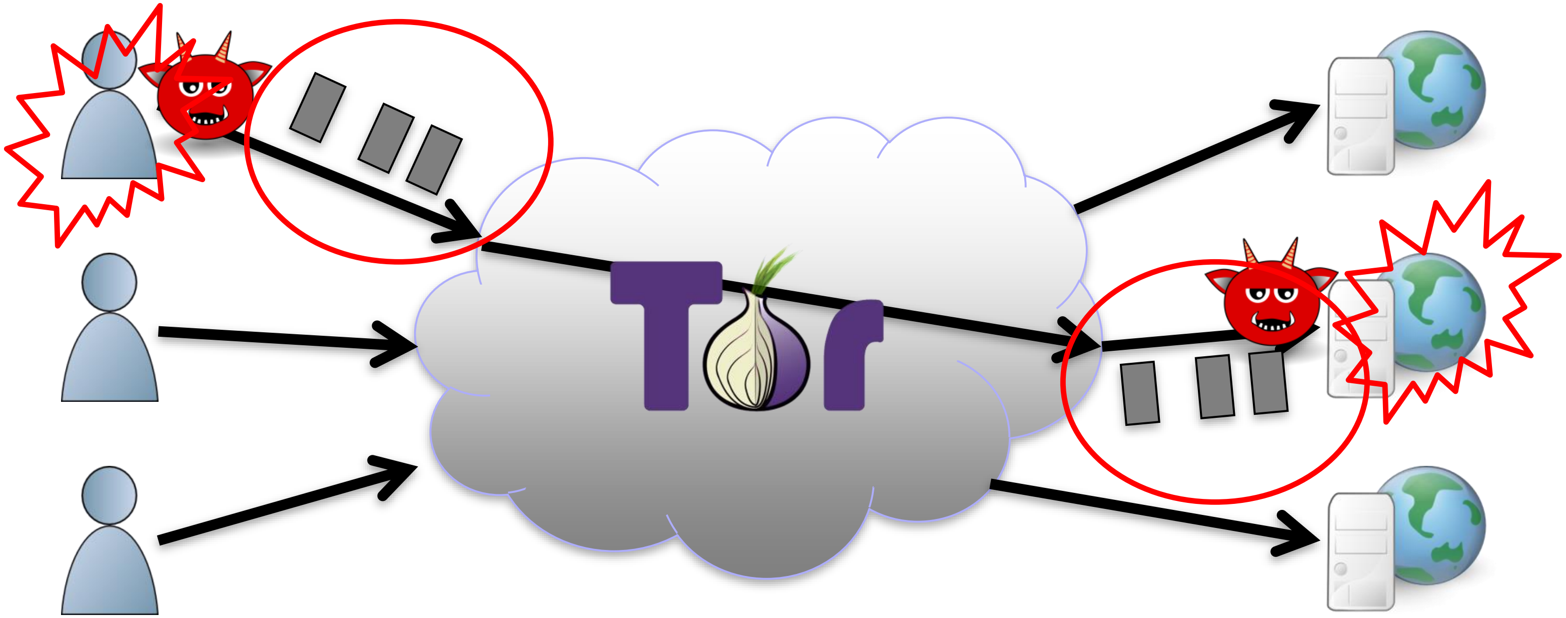


Relays must self-elect to be exit nodes. Why?

- Legal problems

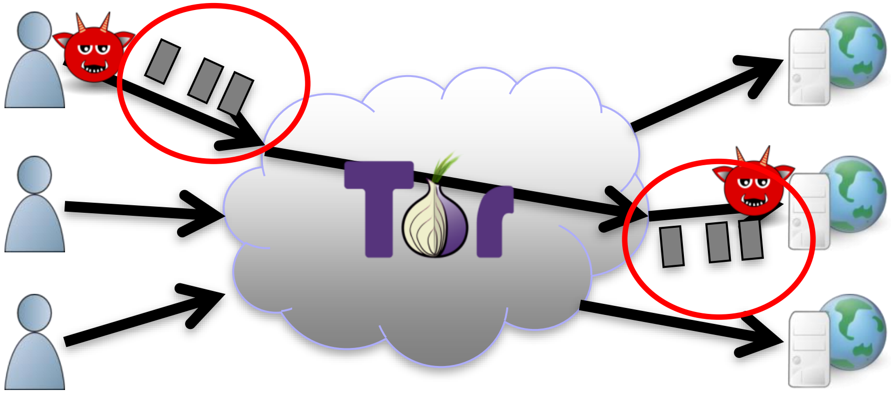
- If someone does something malicious or illegal using Tor and the police trace the traffic, the trace leads to the exit node

Main (?) Tor Problem



Traffic correlation and confirmation

Traffic Confirmation Techniques



Congestion and denial-of-service attacks

- Attack a Tor relay, see if circuit slows down

Throughput attacks

Latency leaks

Website fingerprinting

Not a Theoretical Threat!

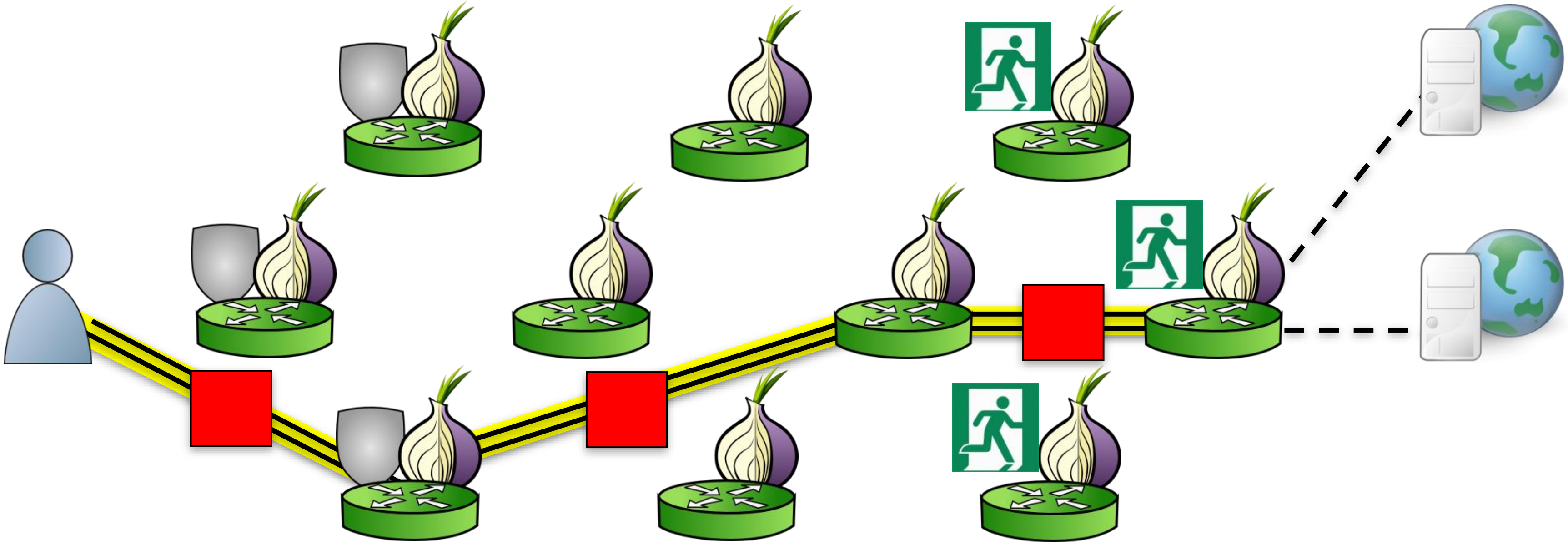
Sybil attack + traffic confirmation

In 2014, two CMU CERT “researchers” added 115 fast relays to the Tor network

- Accounted for about 6.4% of available guards
- Because of Tor’s guard selection algorithm, these relays became entry guards for a significant chunk of users over their five months of operation

The attackers then used these relays to stage a traffic confirmation attack

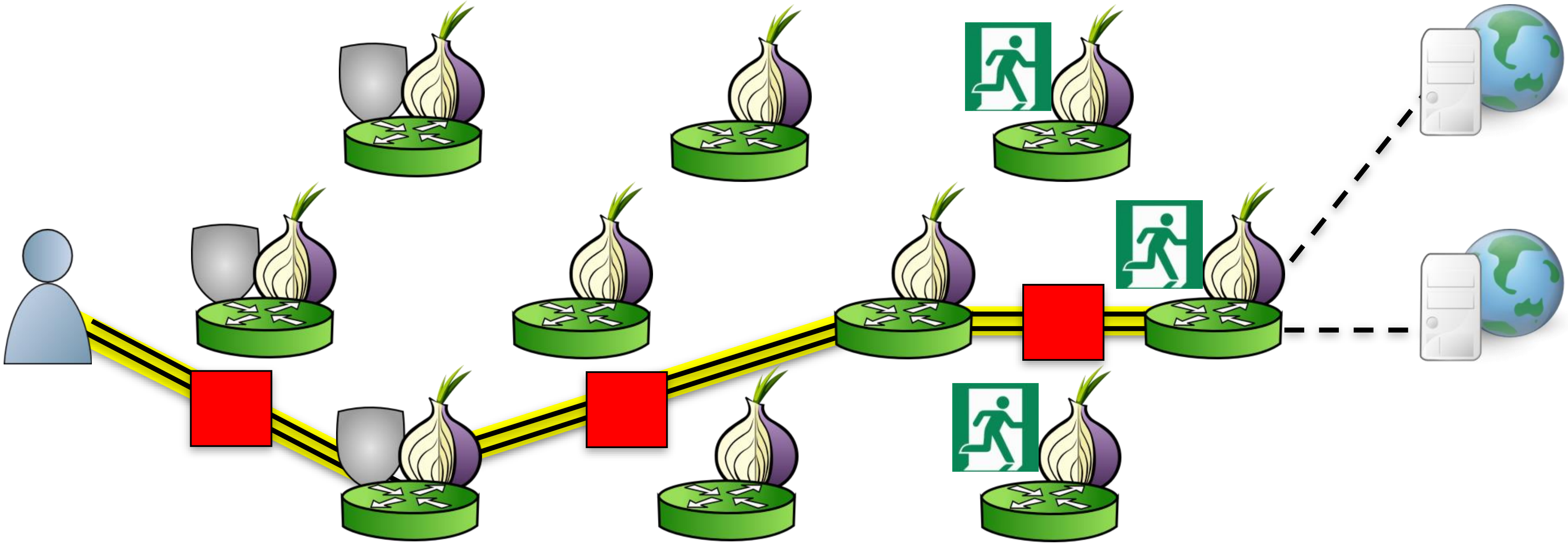
RELAY_EARLY Cell



Goal: prevent building very long Tor paths
(to prevent older DoS attack on Tor relays)

Special control cell sent to the other end of the circuit
-- not just the next hop, like normal cell

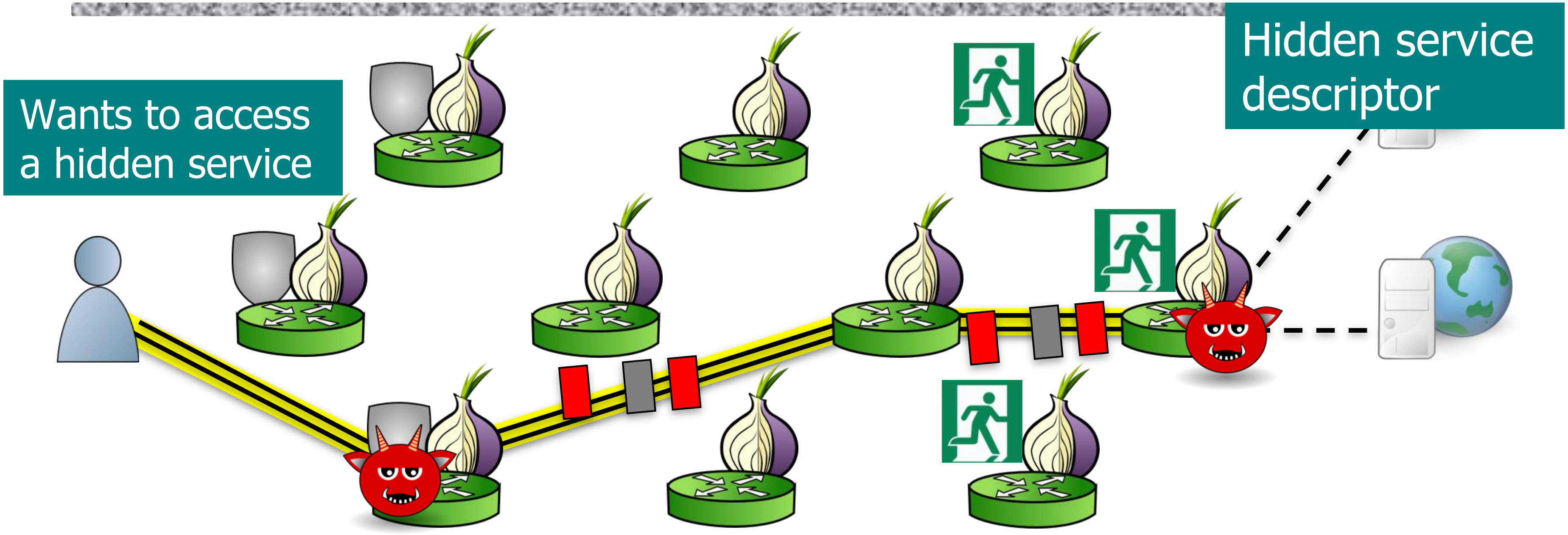
RELAY_EARLY Sent Backward



Any number of RELAY_EARLY cells can be sent backward along the circuit

… no legitimate reason for this, just an oversight

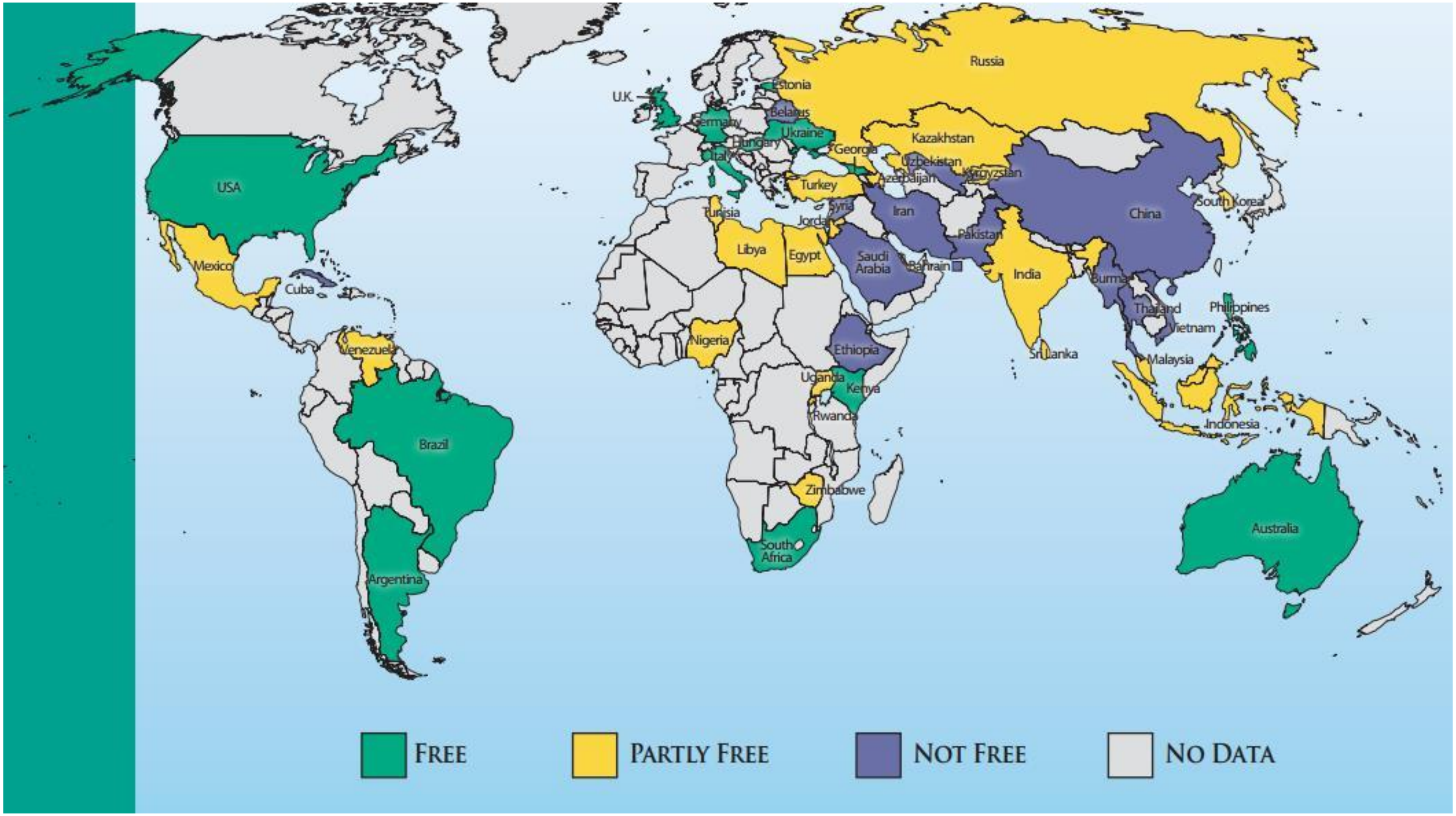
Traffic Confirmation



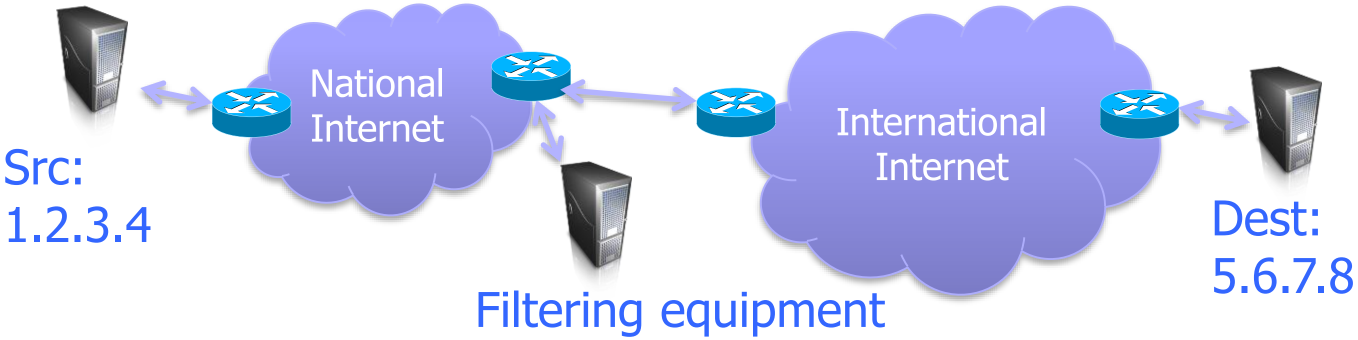
Malicious exit node encodes the name of hidden service in the pattern of relay and padding cells

Malicious guard learns which hidden service the client is accessing

Fighting Internet Censorship



Censorship via Internet filtering



- Golden Shield Project (Great Firewall of China) most famous example
- But many other nations perform filtering as well including
  - Iran, Syria, Pakistan (YouTube anecdote)
  - Turkey (twitter ban)
  - Singapore, Australia (proposed legislation)
  - …

Filtering Technologies

Syria (reported)

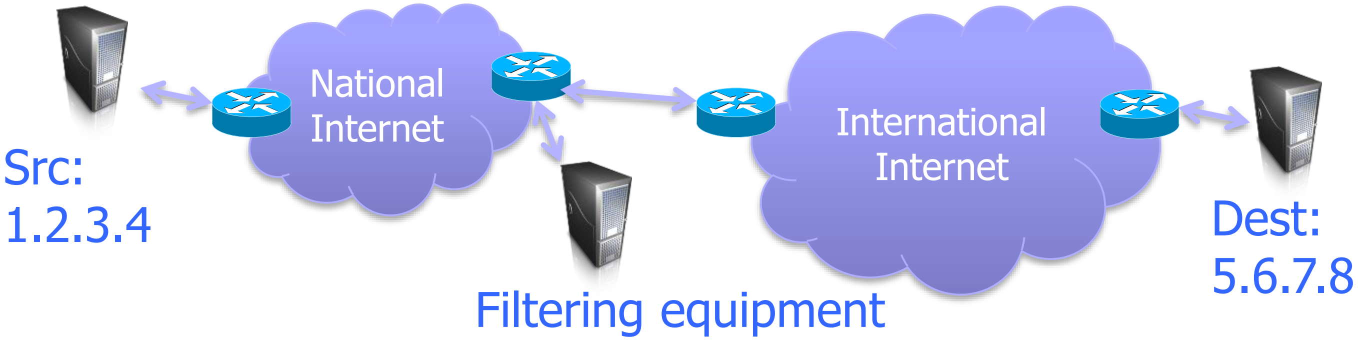
- Blue Coat (http://www.bluecoat.com/)
- NetApp (http://www.netapp.com/)

Iran, Saudi Arabia

- Secure Computing's SmartFilter software
- Secure Computing (bought by McAfee)

Embargos prevent selling directly by US companies, but resellers do

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

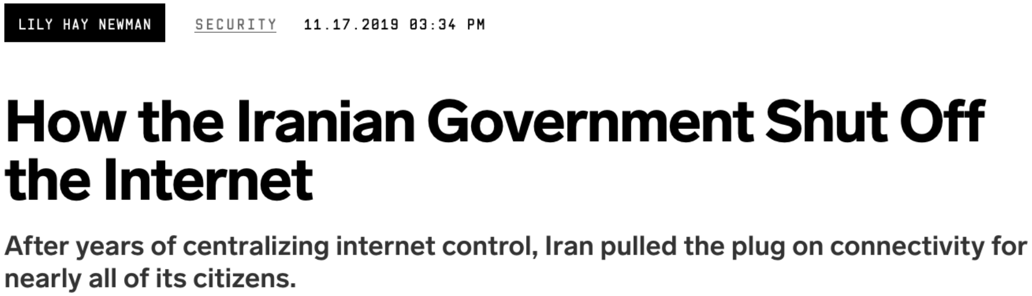
Iran

Every ISP must run “content-control software”

- SmartFilter (up until 2009)
- Nokia Siemens DPI systems

Filters Facebook, Myspace, Twitter, YouTube, RapidShare, WordPress, BBC, CNN…

Occasional widespread filtering of Tor, TLS, other encrypted protocols

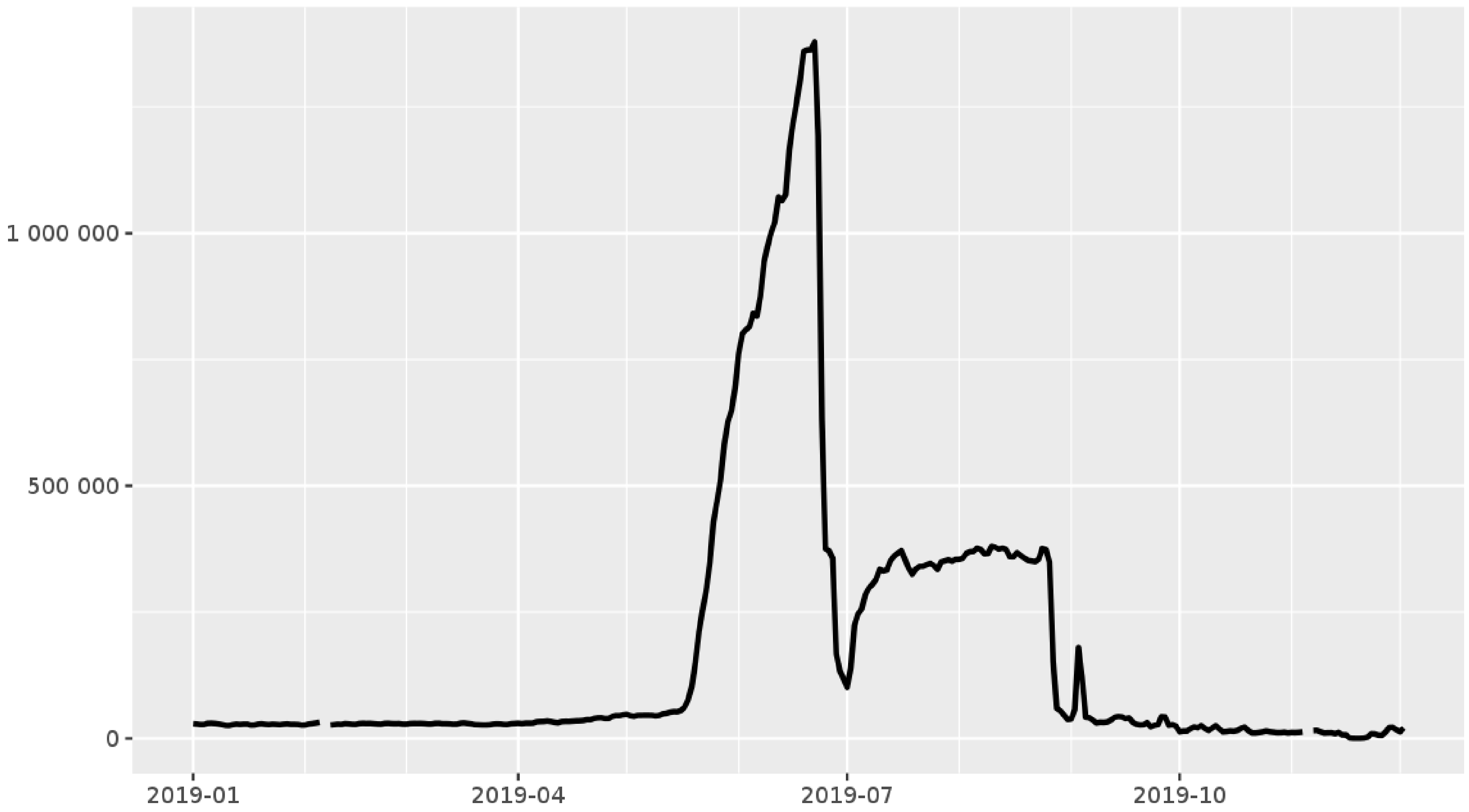


LILY HAY NEWMAN SECURITY 11.17.2019 03:34 PM

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.

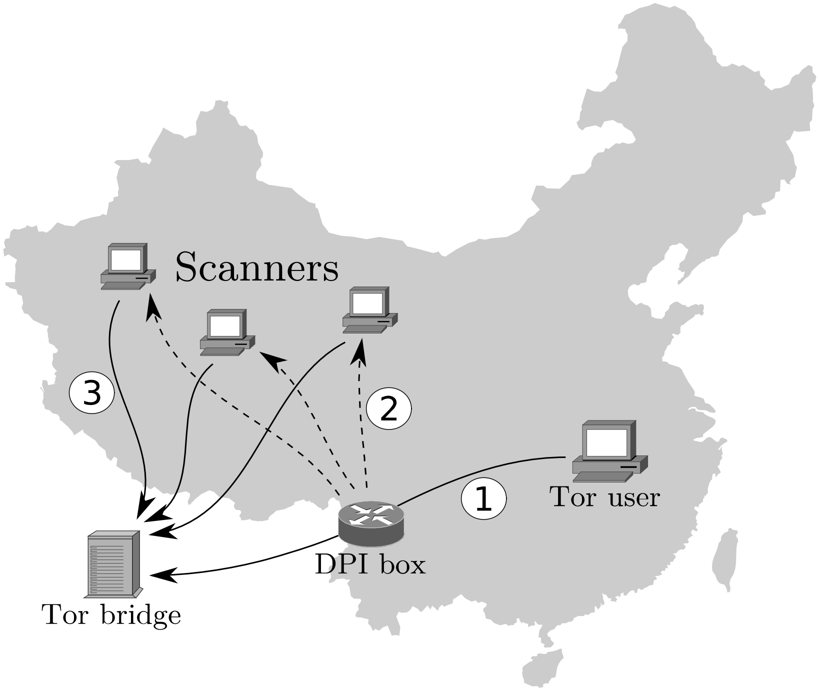
Directly connecting users from Iran



The Tor Project - https://metrics.torproject.org/

Great Firewall of China

- IP filtering
- DNS filtering / redirection
- URL filtering
- Packet filtering (search keywords in TCP packets)
  - Send TCP FIN both ways
- Protocol filtering
  - Tor is mostly shut down



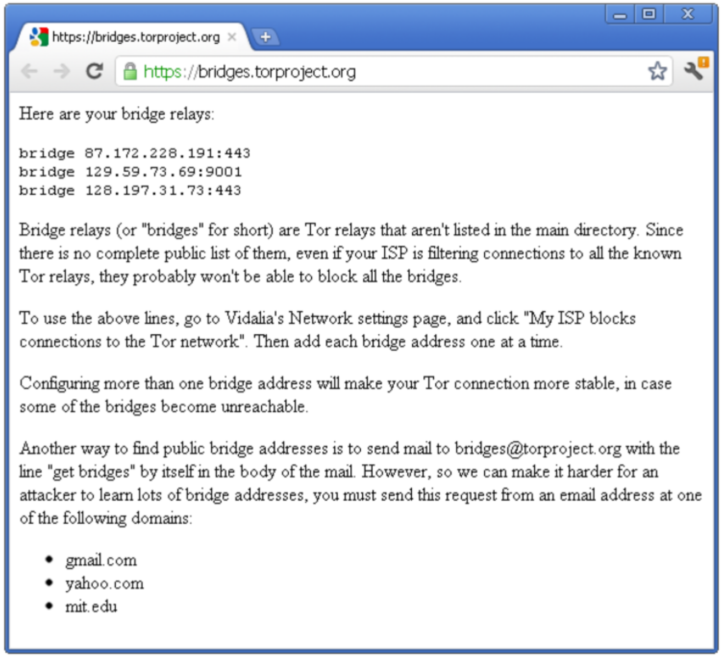
From [Winter, Lindskog 2012]

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


https://bridges.torproject.org
https://bridges.torproject.org

Here are your bridge relays:

```
bridge 87.172.228.191:443
bridge 129.59.73.69:9001
bridge 128.197.31.73:443
```

Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won't be able to block all the bridges.

To use the above lines, go to Vidalia's Network settings page, and click "My ISP blocks connections to the Tor network". Then add each bridge address one at a time.

Configuring more than one bridge address will make your Tor connection more stable, in case some of the bridges become unreachable.

Another way to find public bridge addresses is to send mail to bridges@torproject.org with the line "get bridges" by itself in the body of the mail. However, so we can make it harder for an attacker to learn lots of bridge addresses, you must send this request from an email address at one of the following domains:

- gmail.com
- yahoo.com
- mit.edu

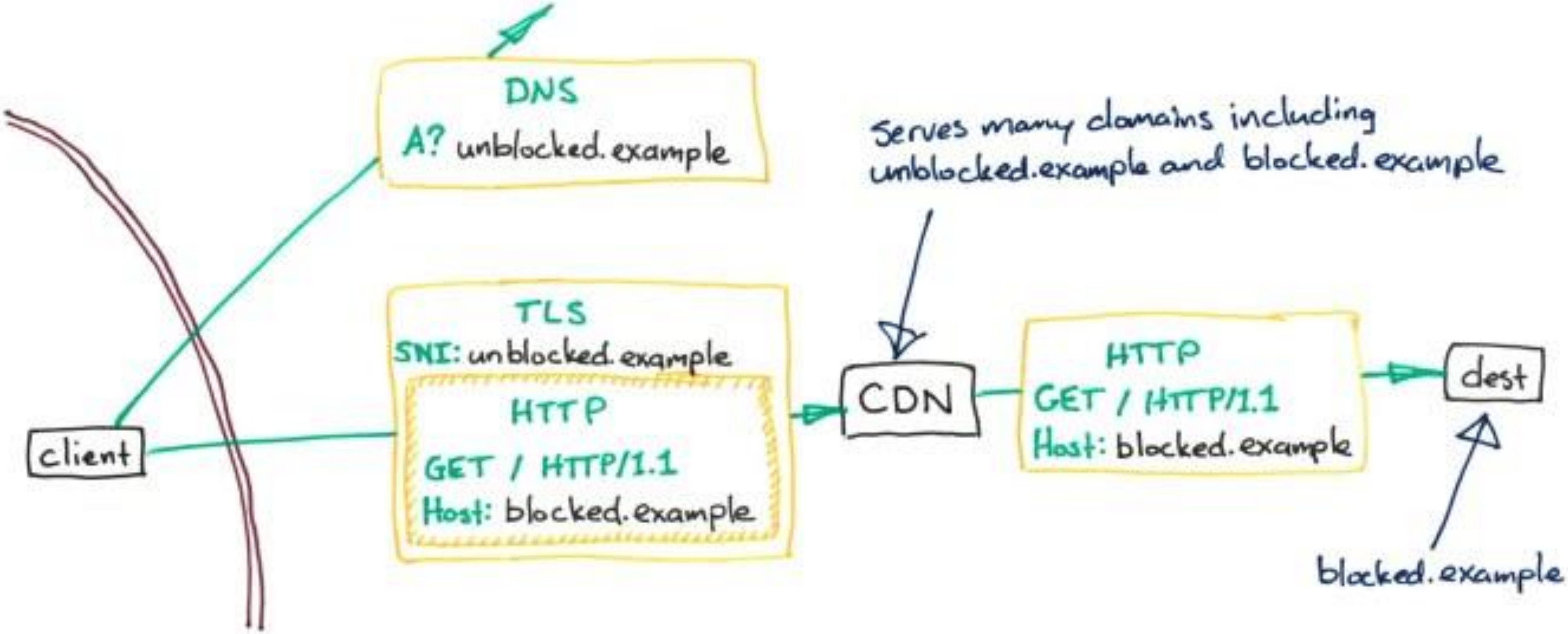
Obfuscating Tor Traffic

Bridges alone do not get around all types of censorship
- DPI can be used to locate and drop Tor frames

Countries would 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.

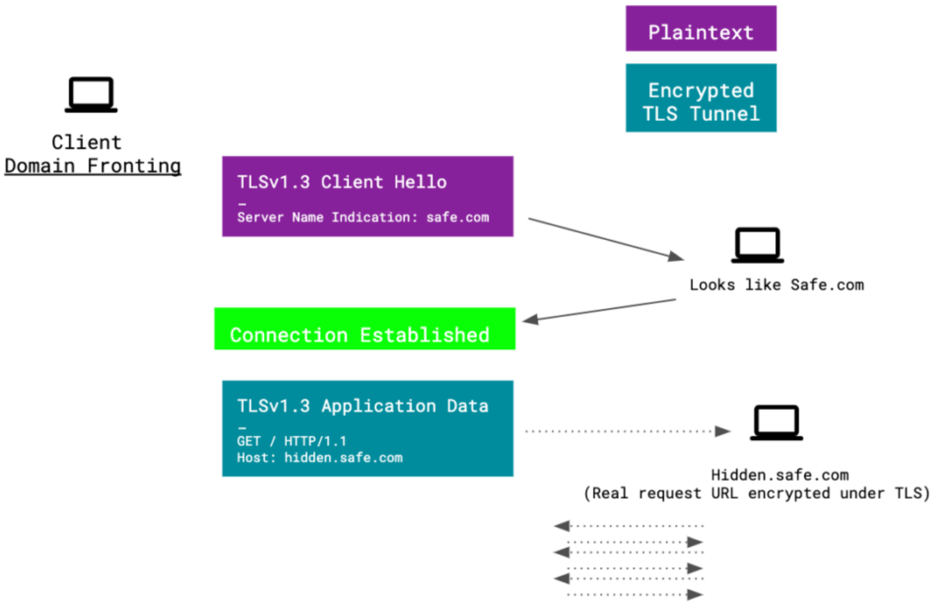
The censor sees only the TLS SNI and DNS request.

Intermediary CDN routes according to the Host header.

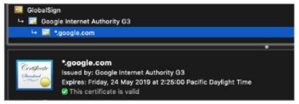
Credits: bamsoftware.com

Domain Fronting in Tor

Tor used domain fronting with Google App Engine, Amazon CloudFront/EC2 and Microsoft Azure to hide Tor bridges

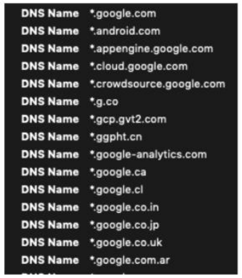


Google.com Certificate


GlobalSign
↳ Google Internet Authority G3
↳ *.google.com

*.google.com
Issued by: Google Internet Authority G3
Expires: Friday, 24 May 2019 at 2:25:00 Pacific Daylight Time
✓ This certificate is valid

Subject Alternative Names



DNS Name	*.google.com
DNS Name	*.android.com
DNS Name	*.appengine.google.com
DNS Name	*.cloud.google.com
DNS Name	*.crowdsource.google.com
DNS Name	*.g.co
DNS Name	*.gcp.gvt2.com
DNS Name	*.ggpht.cn
DNS Name	*.google-analytics.com
DNS Name	*.google.ca
DNS Name	*.google.cl
DNS Name	*.google.co.in
DNS Name	*.google.co.jp
DNS Name	*.google.co.uk
DNS Name	*.google.com.ar

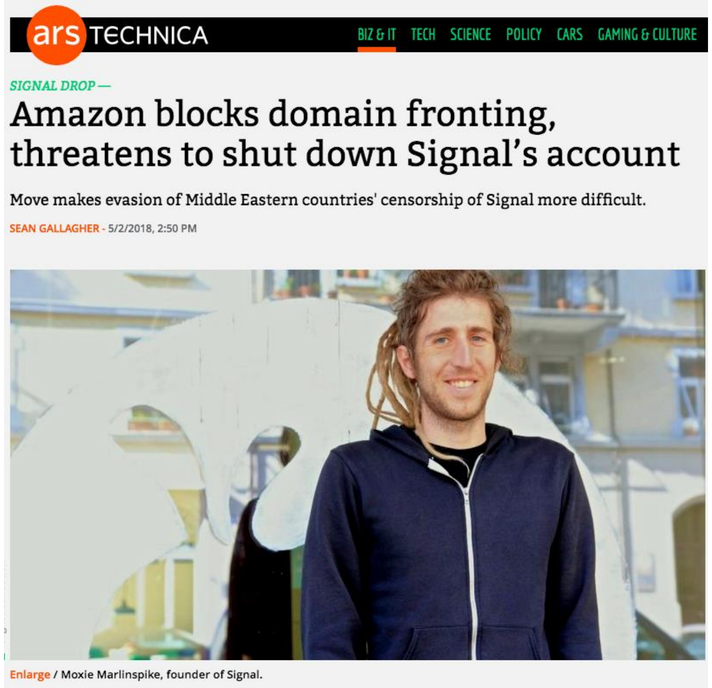
Obtainable domain for GAE customers

Tor bridges lived in hidden domains behind standard cloud-service domains

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…



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.

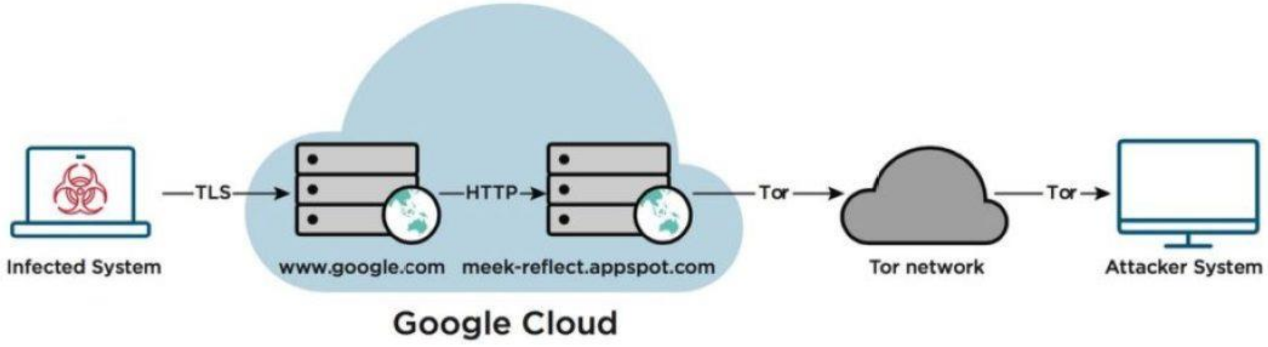
SEAN GALLAGHER - 5/2/2018, 2:50 PM

Enlarge / Moxie Marlinspike, founder of Signal.

APT29 Domain Fronting With TOR

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

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



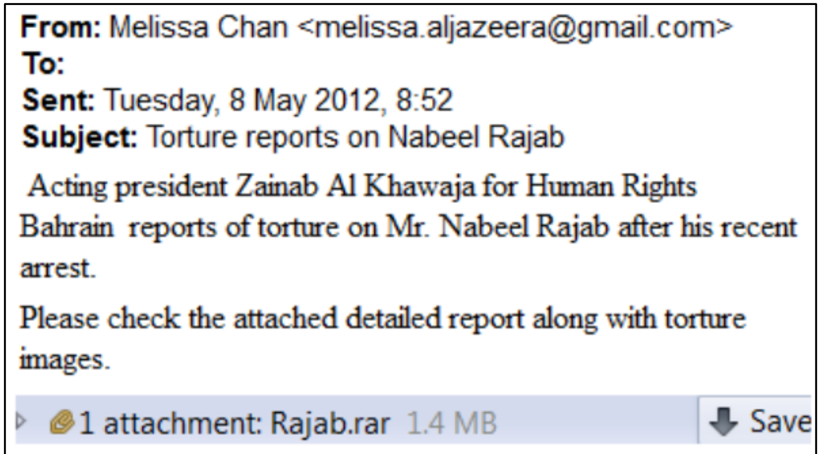
Responsible for many attacks, including DNC hack in 2016, attempts to steal vaccine data in July 2020…

Targeted Attacks

Dissidents, journalists, activists targeted by nation-states

- Phishing attacks, botnet-style C&C servers to collect data
- Remote Access Trojans (RATs)

Small industry of companies providing “lawful access” tools



From: Melissa Chan <melissa.aljazeera@gmail.com>
To:
Sent: Tuesday, 8 May 2012, 8:52
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.

Figure 1: E-mail containing FinSpy.

"Crypto Wars"

"Going dark" debate

- Police and others argue encryption is preventing criminals, terrorists from being caught
- Push for building backdoors into crypto & other systems
- Manhattan DA report about smartphone unlocking

Long history

- 1990s: export controls on cryptography, failed Clipper chip effort

Consensus among cryptographers & security experts: mandated backdoors fundamentally weaken security

- "Keys under doormats" report: https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf

Backdoors

NIST’s Dual EC pseudorandom number generator (PRNG) backdoored

- Mandated public parameters are public key
- Intuitively: TLS ClientHello random nonce is public-key encryption of values sufficient to derive session key

Unauthorized code in Juniper’s NetScreen VPN

- Authentication bypass for remote admin access
- Change to parameters of Dual EC pseudorandom generator that enables passive decryption of VPN traffic