CS 253 Cyber Security
Network Defense and More

ShanghaiTech University

PART ONE

01

Network Defenses

Local Network Services

Review: Popular TCP and UDP services live on standardized ports. HTTPS servers listen on TCP/443. SSH on TCP/22.

Some services you don’t want listening on the public Internet.

Recursive DNS Resolvers: allows attackers to mount DDoS attacks

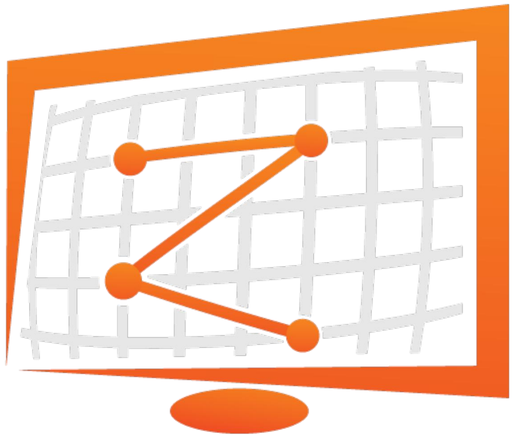
Windows File Sharing: historically full of vulnerabilities. What if a local machine doesn’t have a secure password on it?

Port Scanning

Send a SYN or application-specific UDP packet to a port to see if any service is listening

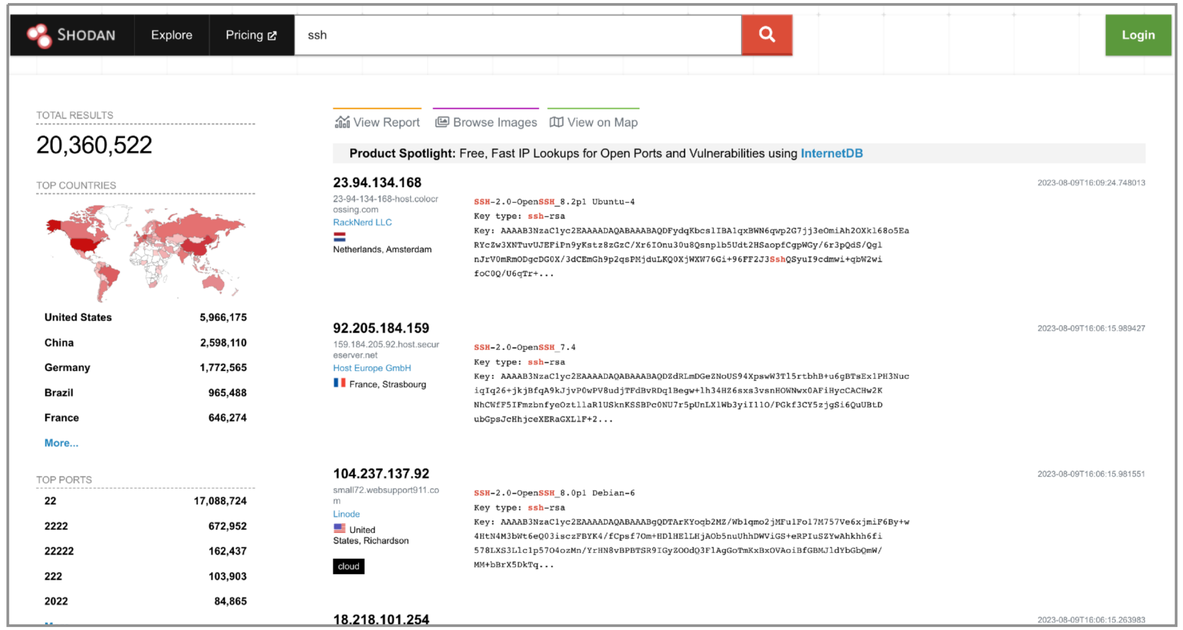
Vertical Scan: Try large number of ports on a single host. Typically use Nmap.

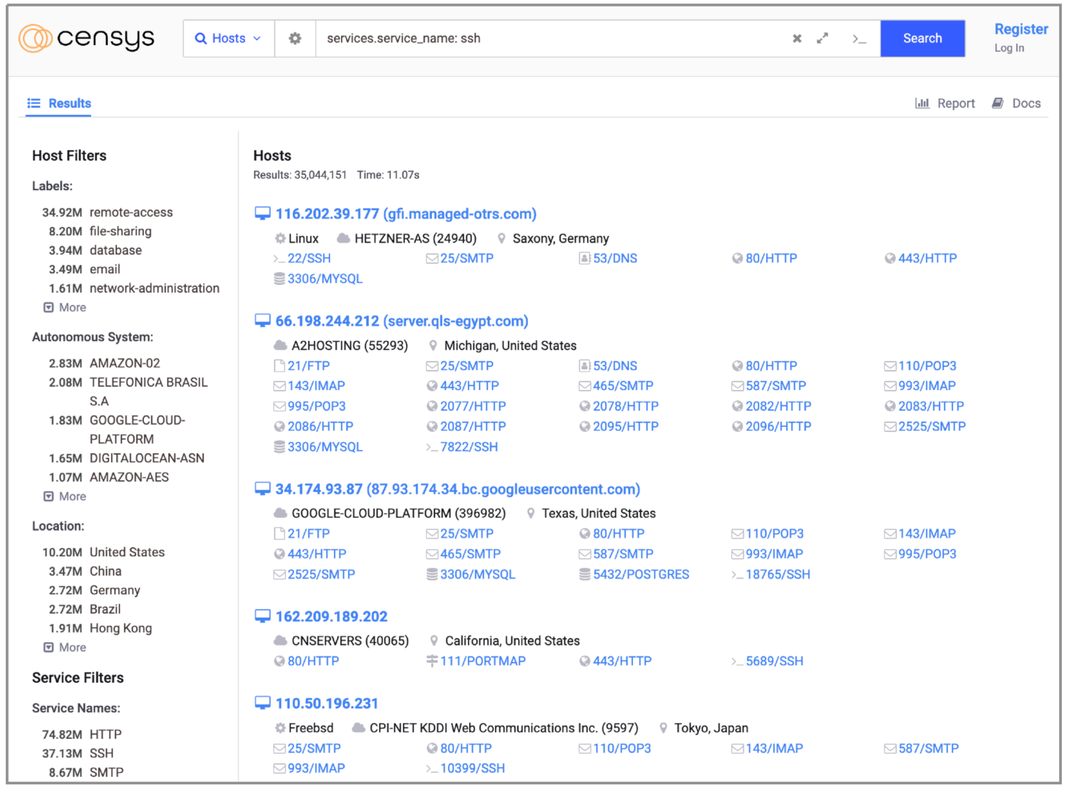
Horizontal Scan: Try a single port on a large number of hosts. Typically ZMap.



Service Search Engines

Public services like Shodan and Censys index all of the publicly available services on the Internet





Attacks Against Internet Services

MOVEit is a piece of software that allows file transfer between organizations

Vulnerable to multiple login-field SQL injection vulnerabilities

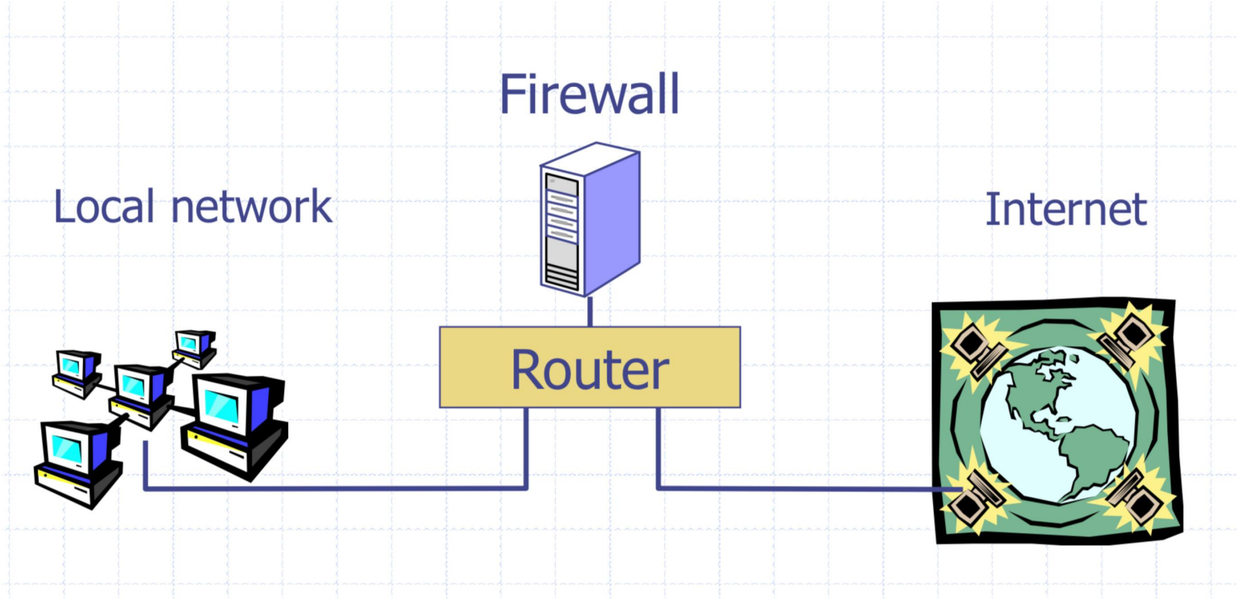
Ransomware'd/Extorted Companies based on the data on their Internet MOVEit Servers

Progress®
MOVEit®

Firewalls

Separate local area network (LAN) from the Internet. Only allow some traffic to transit.

Sometimes rules on a router. Sometimes a standalone device.



Basic Packet Filtering

Uses transport and IP layer information only

- IP Source Address, Destination Address
- Protocol (TCP, UDP, ICMP, etc.)
- TCP and UDP source and destination ports

Examples:

- “Do not allow external hosts to connect to Windows File Sharing”
  -> DROP ALL INBOUND PACKETS TO TCP PORT 445

What's the rule?

What if you have a network with lots of servers but only want outsiders to be able to access a web server?

DROP ALL INBOUND PACKETS IF DEST PORT != 80

All outbound connections also have a source port! Their responses will blocked!

IANA Port Numbering

System or Well-Known Ports [1,1023]:

Common services, e.g., HTTP -> 80, SSH -> 22

User or registered ports [1024, 49151]

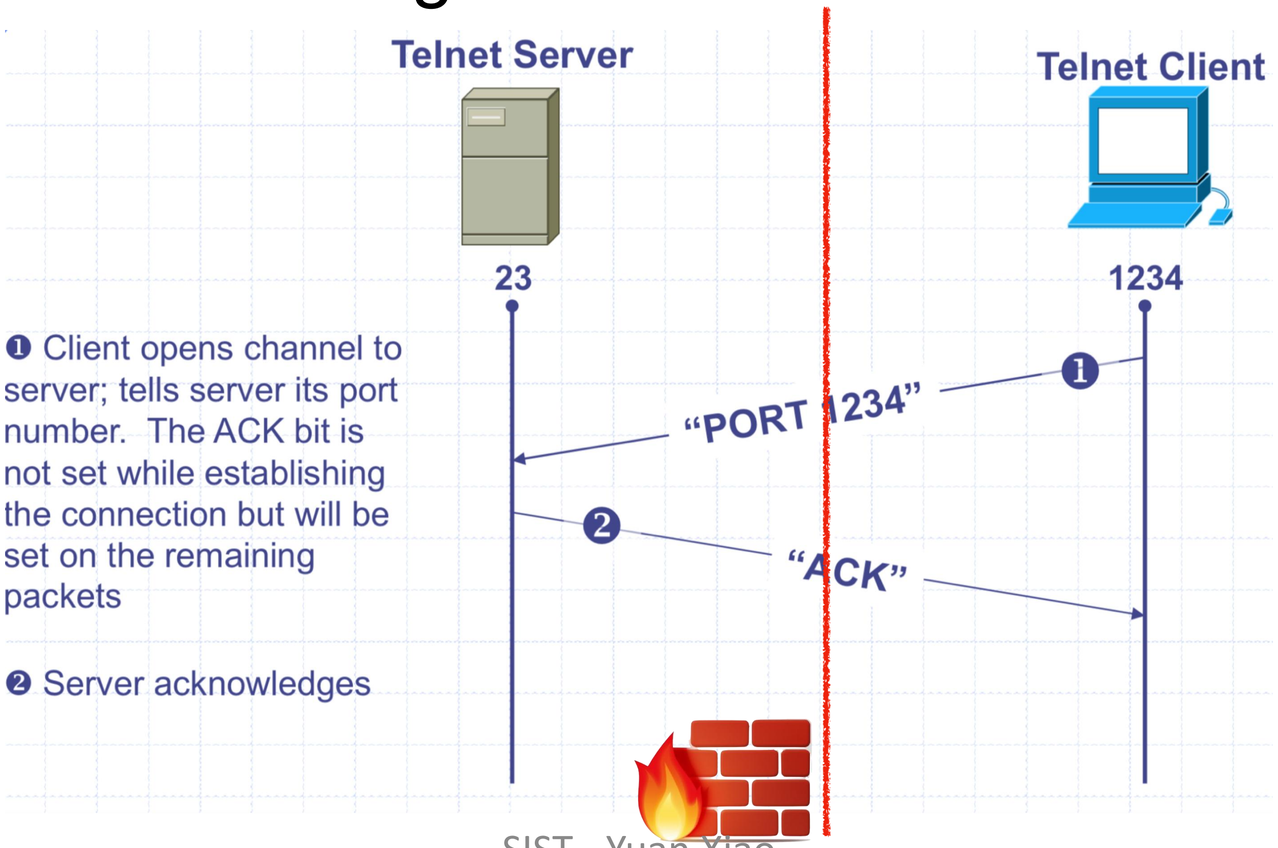
Less well-known services

Ephemeral/Dynamic/Private Ports [49152, 65535]

Short lived connections

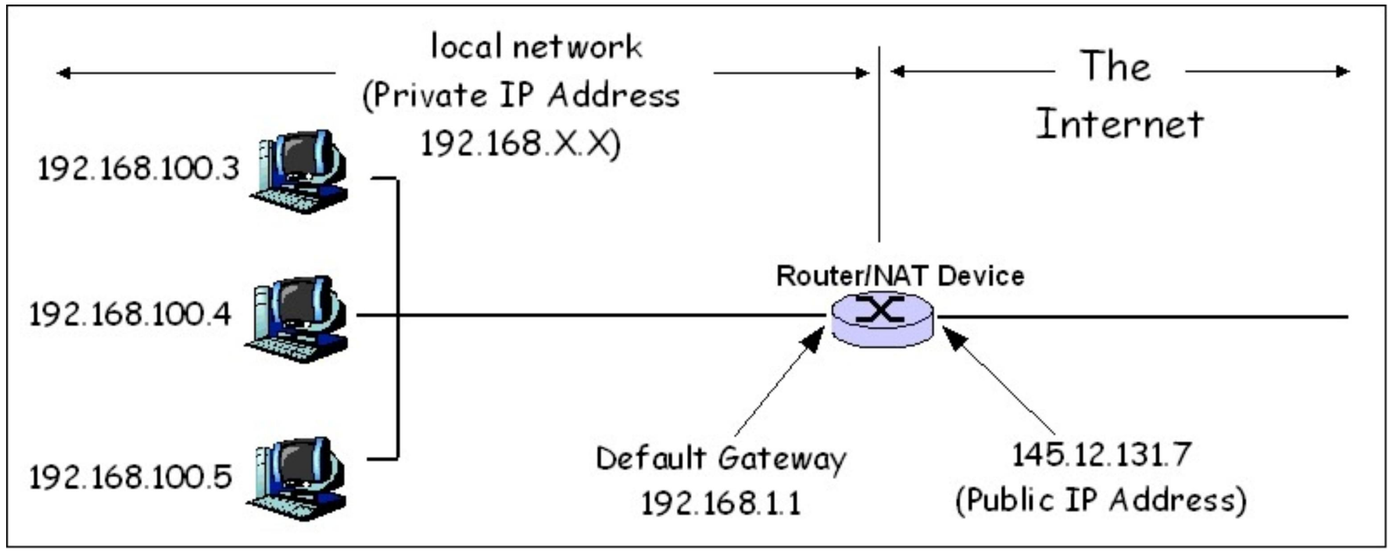
Stateful Filtering

Firewall tracks outgoing connections and allows associated inbound traffic back through



Network Address Translation (NAT)

NATs map between two different address spaces. Most home routers are NATs and firewalls.



Private Subnets

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Local vs. Network Firewall

Firewalls we've discussed so far have all been network firewalls.
Most have lived at the edge of the organization.

Firewalls also run on individual hosts. Linux servers use **iptables**.

Typically have a combination of network and host firewalls

```
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

Local vs. Network Firewall

Organizations typically have a combination of network and host firewalls

- Border (Network) Firewall will block malicious traffic from the outside and limit inbound traffic to accessing only servers intended to be accessed by the public
- Host Firewalls protect hosts from other hosts (e.g., protect against internal compromise and malicious insiders)

Think of firewall rules in terms of “Defense in Depth"

Next Generation Firewalls (NGFW)

So far, firewalls operate by allowing access to a specific host or protocol — but what about malicious application traffic?

Next Generation Firewalls (Industry term for Application-Layer firewall)s protect for attacks *within* L7 traffic

For Example:

- Virus scanning for SMTP
  - Need to understand protocol, MIME encoding, ZIP files, etc
- Look for SQL injection attacks in HTTP POSTs
- Look for a large number of authentication attempts or malformed requests

Intrusion Detection Systems (IDS)

Software/device to monitor network traffic for attacks or policy violations

Violations are reported to a central security information and event management (SIEM) system where analysts can later investigate

Signature Detection: maintains long list of traffic patterns (rules) associated with attacks

Anomaly Detection: attempts to learn normal behavior and report deviations

Open Source IDS

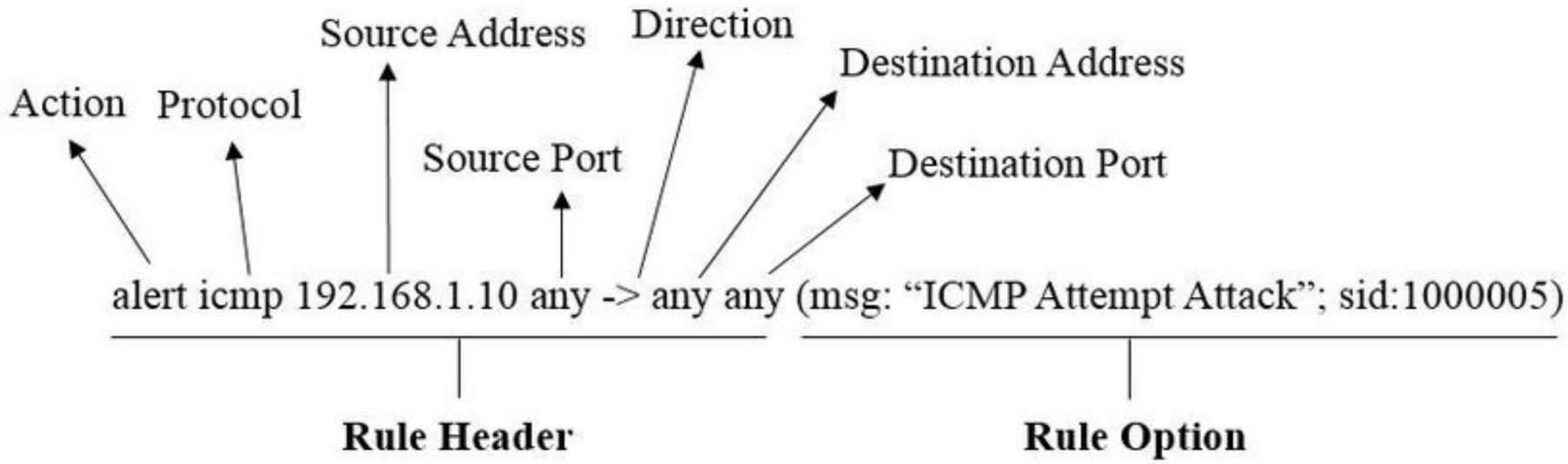
Three Major Open Source IDS (and a *tremendous* number of commercial products)

Snort

~~Bro~~ Zeek

Suricata

Example Snort Rule



Outbound Too!

Organizations will often inspect outbound traffic as well

- Block access to sites with known malicious behavior
- Prevent exfiltrating data
- Block services like bit torrent

Be careful on enterprise networks! Sometimes companies will even install their own root certificates on employee workstations to monitor TLS traffic.

PART TWO

02

Remote Access

Virtual Private Networks (VPNs)

Problem: How do you provide secure communication for non-TLS protocols across the public Internet?

VPNs create a fake shared network on which traffic is encrypted

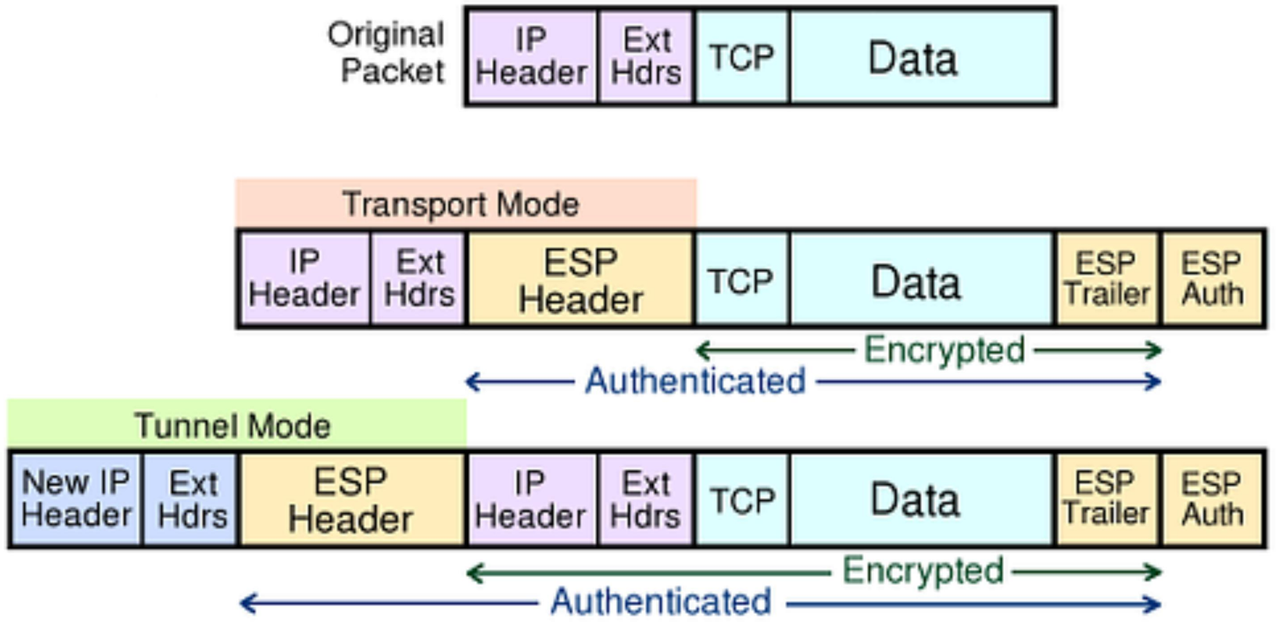
Two Broad Types:

- Remote client (e.g., traveler with laptop) to corporate network
- Connect two remote networks across Internet

IPSec

Several VPN protocols exist (PPTP, L2TP, IPsec, OpenVPN)

Most popular is IPsec. OpenVPN is open source.



Wireguard

Recently introduced VPN that has gained significant following in the past 5 years over options like OpenVPN:

- Simpler protocol and much more performant than OpenVPN.
  Relatively few configuration options reduces opportunity for error
- Utilizes modern cryptographic primitives like Noise protocol framework, Curve25519, ChaCha20, Poly1305,

Cisco AnyConnect

Stanford and many other organizations use Cisco AnyConnect

Encapsulates traffic in TLS! Initial handshake uses normal TCP-based TLS for initial handshake and then DTLS (UDP-based TLS) to transport data

Gooey Middle

VPNs support the idea of having a secure internal network and untrusted public Internet. Unfortunately, attacker has a ton of access once the network perimeter is breached.

Unfortunately, internal networks aren't *that* secure. Computers are compromised all the time and attackers have free rein.

Zero Trust Security (BeyondCorp)

Google: assume internal network is *also* out to get you. Remove privileged intranet and put all corporate applications on the Internet.

Access depends solely on device and user credentials, regardless of a user's network location

Protect applications, not the network

PART THREE

03

Privacy

Direct Sharing

The Incredible Story Of How Target Exposed A Teen Girl's Pregnancy

GUS LUBIN
FEB. 16, 2012, 10:27 AM

Target broke through to a new level of customer tracking with the help of statistical genius Andrew Pole, according to a New York Times Magazine cover story by Charles Duhigg.

Pole identified 25 products that when purchased together indicate a women is likely pregnant. The value of this information was that Target could send coupons to the pregnant woman at an expensive and habit-forming period of her life.

Plugged into Target's customer tracking technology, Pole's formula was a beast. Once it even exposed a teen girl's pregnancy:

Roll over image to zoom in

First Response Early Result Pregnancy Test, 3 tests, Packaging May Vary

by First Response

4.5 out of 5 stars ▾ 486 customer reviews | 17 answered questions

#1 Best Seller in Pregnancy Tests

amazon student 47 Amazon Students rated this highly ▾

4.5 out of 5 stars

List Price: ~~$19.57~~

Price: $12.98 Prime & Free Returns. Details

You Save: $6.59 (34%)

Note: Available at a lower price from other sellers, potentially without free Prime shipping.

In Stock.

Ships from and sold by Amazon.com. Gift-wrap available.

Want it Tuesday, March 24? Order within **29 hrs 56 mins** and choose **One-Day Shipping** at checkout. Details

Package Quantity: **1**

1	2	3
$12.98 Prime	$41.00 Prime	$57.99

Customers Who Bought This Item Also Bought

Page 6 of 14 | Start over

Vitafusion Prenatal DHA and Folic Acid Gummy Vitamins, 180 Count

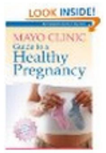
4.0 out of 5 stars 140

$20.25 Prime

One A Day Women's Prenatal One Pill, 30 Count

4.0 out of 5 stars 18

$13.48 Prime



Mayo Clinic Guide to a Healthy Pregnancy:... the pregnancy experts...

4.5 out of 5 stars 804

#1 Best Seller in Motherhood

Summer's Eve Cleansing Wash, Morning Paradise, 15 Ounce

4.5 out of 5 stars 44

$3.99

Nexcare 524560 Basal Digital Thermometer

3.5 out of 5 stars 19

$14.06 Prime

Nature Made Prenatal Multi Vitamin Value Size, Tablets, 250-Count

4.5 out of 5 stars 213

$16.79 Prime

Trojan Condom Pleasure Pack Lubricated, 40 Count

4.5 out of 5 stars 126

$18.12 Prime

Third Party Tracking

COSMOPOLITAN LOVE | CELEBS | BEAUTY & STYLE | FITNESS

18 Things You Should Know Before Dating a Cat Lady

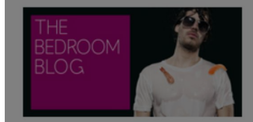
She knows the difference between a guy who's allergic to cats and a guy who's "allergic to cats."

By Anna Breslaw

12.3k
Shares

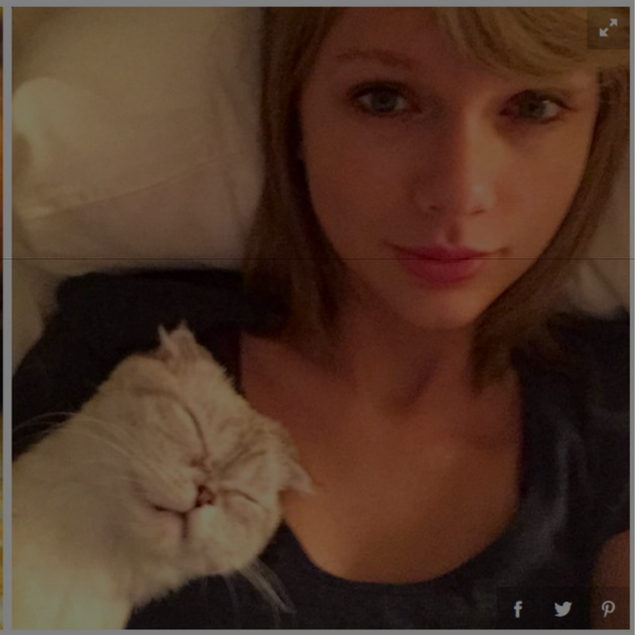
SHARE 12.2K
TWEET 46
PIN 6

MOST READ



Does Seafood Make Guys Horny?

13 Things You Should Know Before Dating Someone Wh...

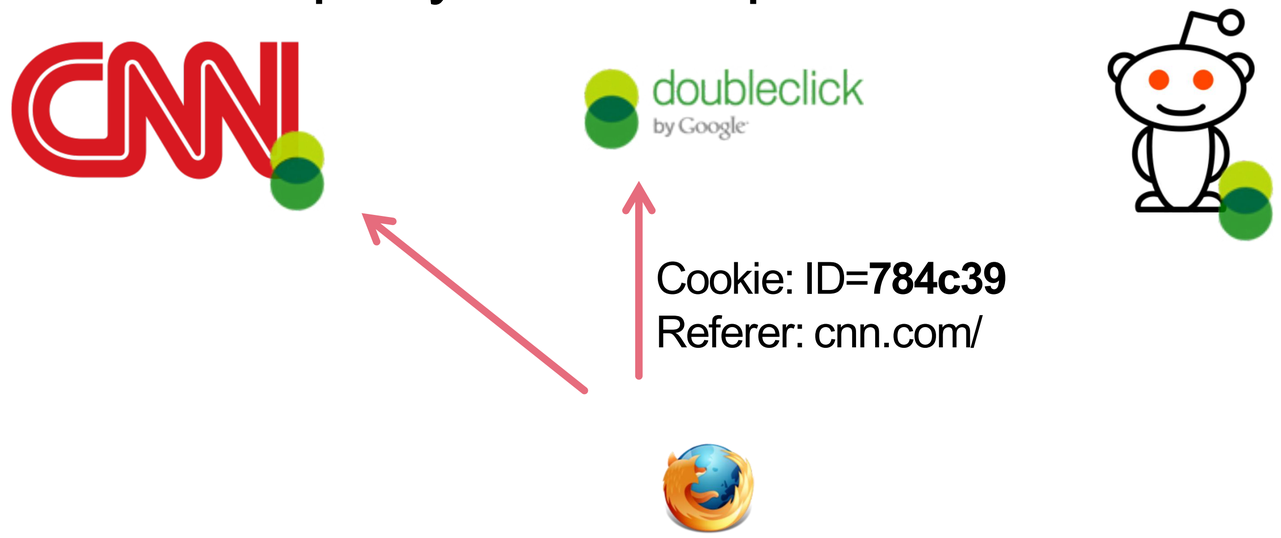


1. First of all, define "cat lady." Does one cat = cat lady? Two cats = cat lady? Does joking about being a cat lady à la sparkling, outgoing multimillionaire Taylor Swift automatically make one a cat lady? It is my personal belief that most female cat owners below the age of 40 fall into the "not a cat girl, not yet a cat lady" category.

2. Cat ladies mostly look like ... normal ladies. You know. Like regular women. Not like the old hag who sits in front of your local Shop Rite with aluminum foil on her head.

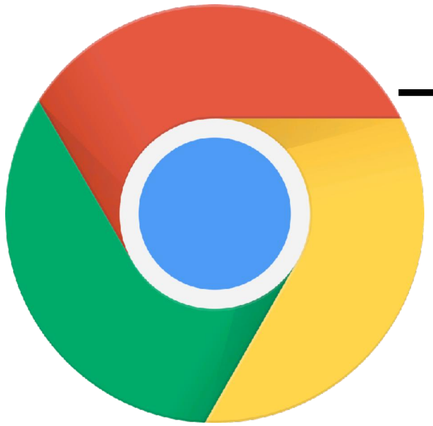
Third Party Cookies

- Site A's page requests a third-party resource (image, script, iframe)
  - Normally, browser sends cookie associated with that third-party in that request



Third-Party Web Tracking

Cookies and Code



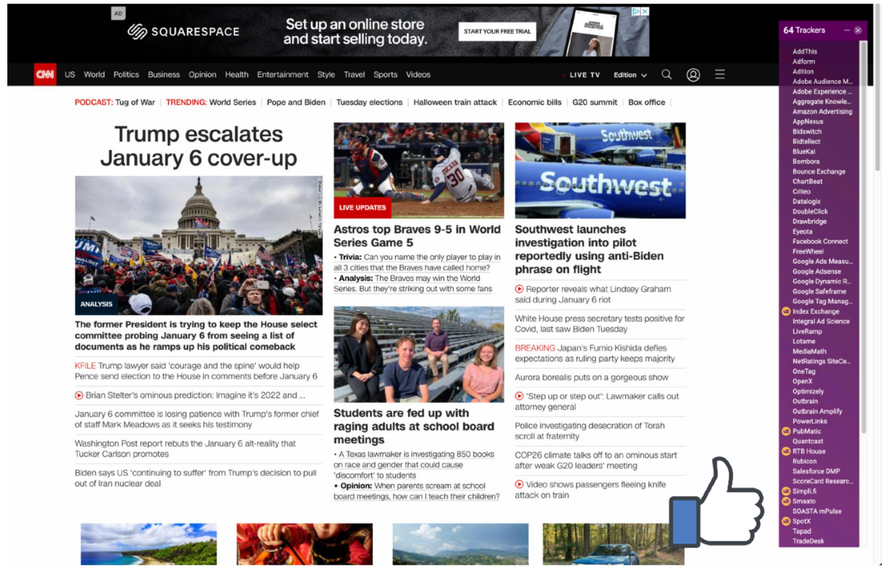
(CNN)

GET / HTTP/3

GET /facebook-like.js HTTP/3

Cookie: User=Deepak, **Referer**=cnn.com

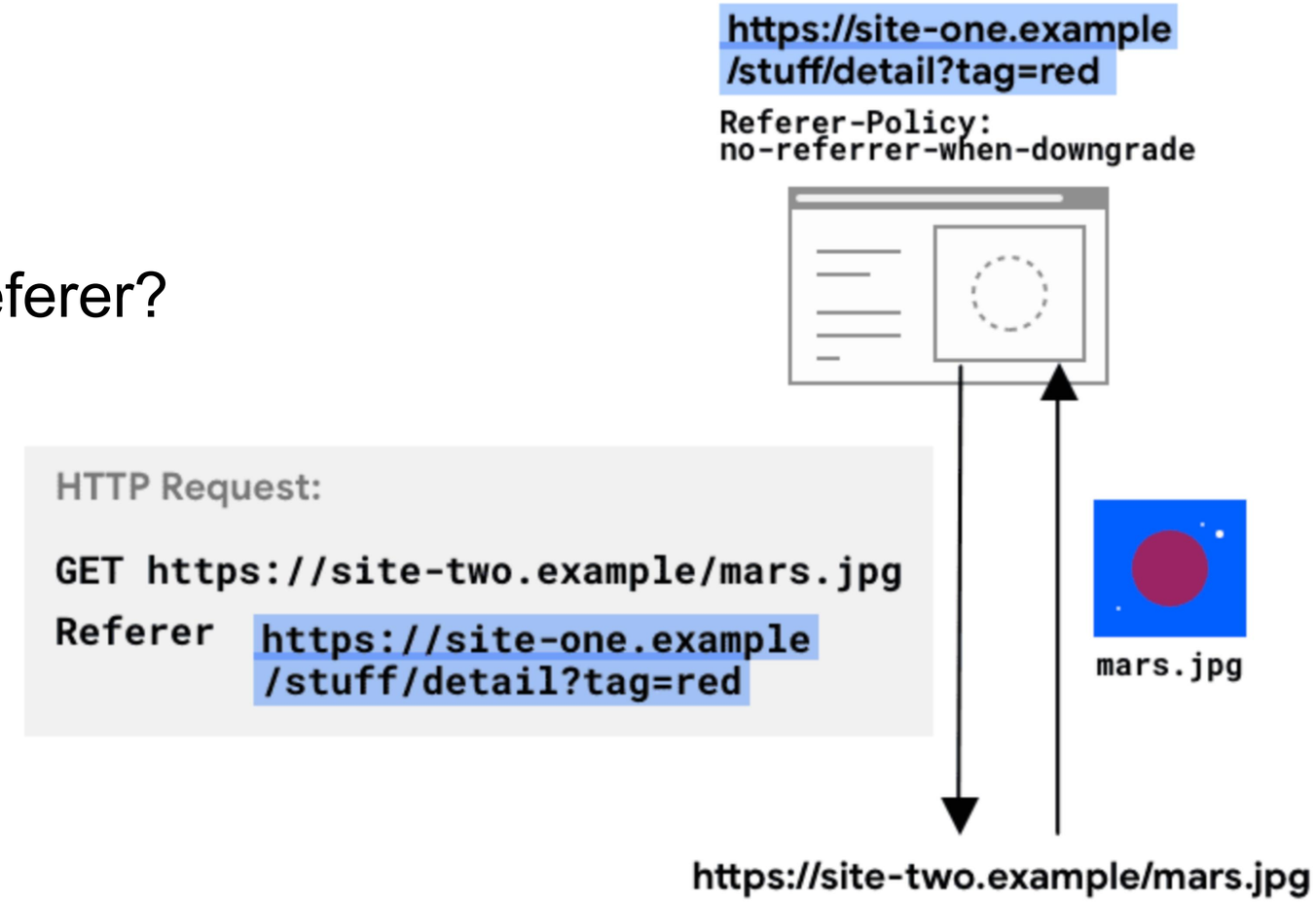
(Facebook)



- With this request, companies can link your cookie to your browsing data (e.g., through Referer header, Host headers, Origin, or just JavaScript)

Web Tracking
Cookies and Code

- What exactly is sent in the referer?



Trump escalates January 6 cover-up

The former President is trying to keep the House select committee probing January 6 from seeing a list of documents as he ramps up his political comeback

KFILE Trump lawyer said 'courage and the spine' would help Pence send election to the House in comments before January 6

Brian Stelter's ominous prediction: Imagine it's 2022 and ...

January 6 committee is losing patience with Trump's former chief of staff Mark Meadows as it seeks his testimony

Washington Post report rebuts the January 6 alt-reality that Tucker Carlson promotes

Biden says US 'continuing to suffer' from Trump's decision to pull out of Iran nuclear deal

Astros top Braves 9-5 in World Series Game 5

• **Trivia:** Can you name the only player to play in all 3 cities that the Braves have called home?
• **Analysis:** The Braves may win the World Series. But they're striking out with some fans

Students are fed up with raging adults at school board meetings

• A Texas lawmaker is investigating 850 books on race and gender that could cause 'discomfort' to students
• **Opinion:** When parents scream at school board meetings, how can I teach their children?

Southwest launches investigation into pilot reportedly using anti-Biden phrase on flight

Reporter reveals what Lindsey Graham said during January 6 riot

White House press secretary tests positive for Covid, last saw Biden Tuesday

BREAKING Japan's Fumio Kishida defies expectations as ruling party keeps majority

Aurora borealis puts on a gorgeous show

'Step up or step out': Lawmaker calls out attorney general

Police investigating desecration of Torah scroll at fraternity

COP26 climate talks off to an ominous start after weak G20 leaders' meeting

Video shows passengers fleeing knife attack on train

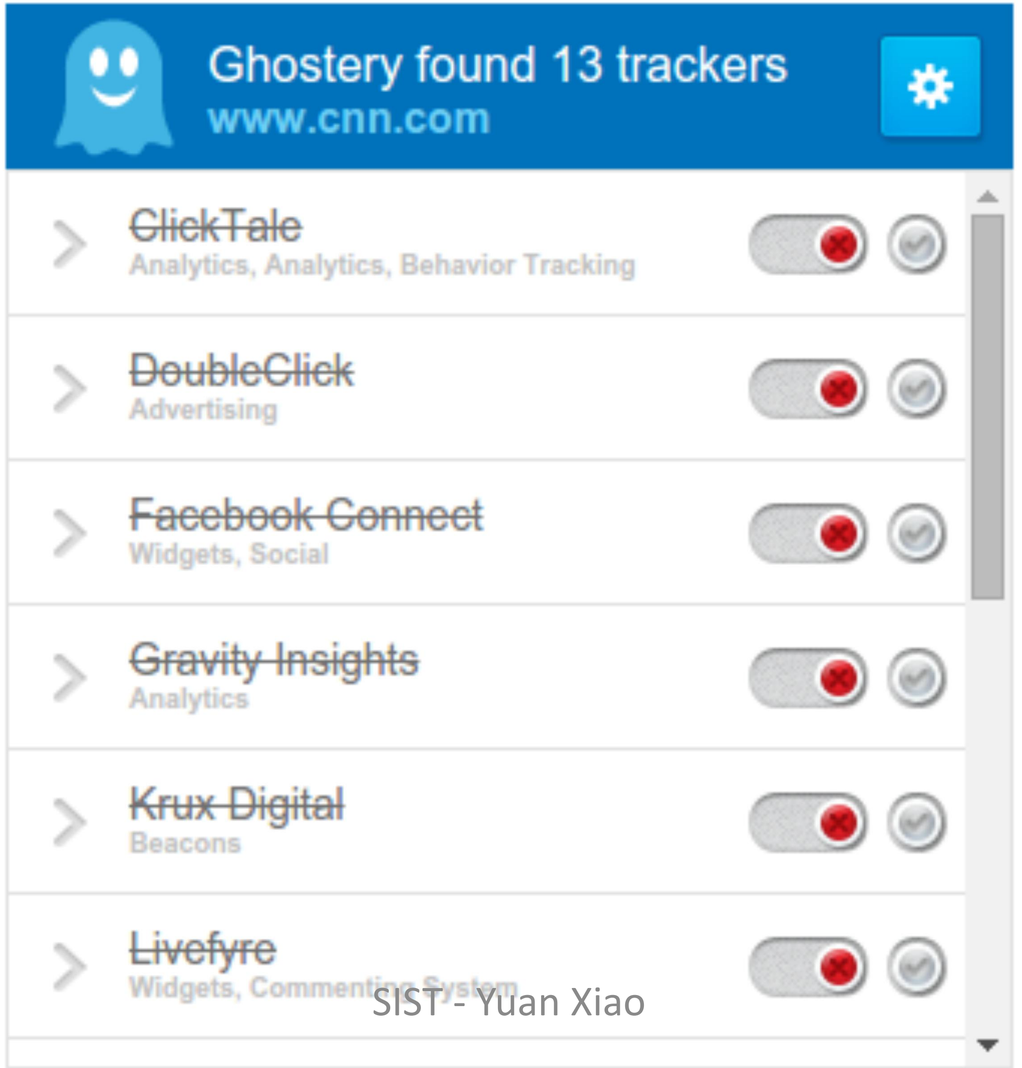



Third Party Cookies

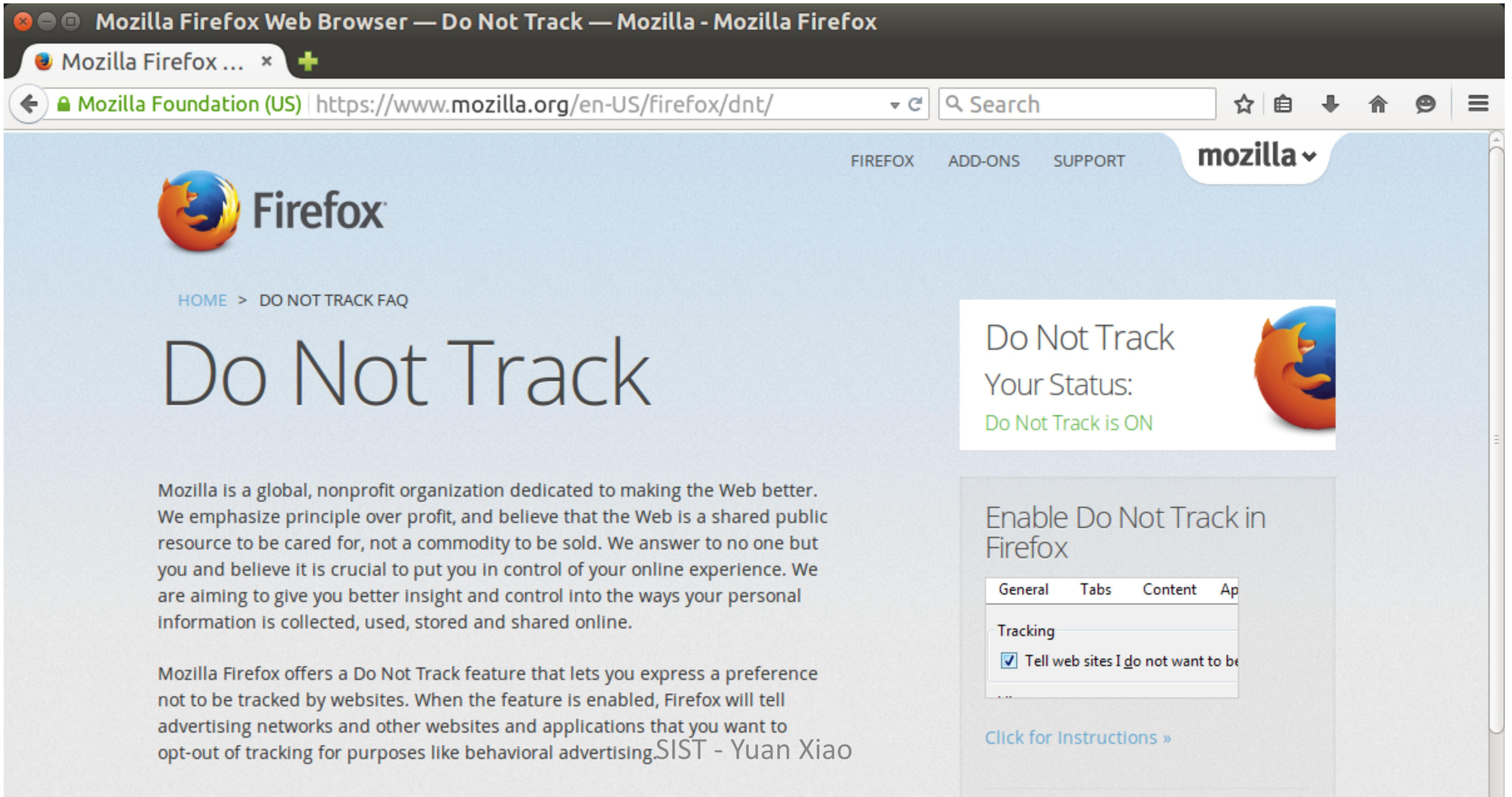
Facebook, DoubleClick, etc. know much more about you than actual website does because they can track you across websites.

Domain	Top 1M	Domain	Top 1M
google-analytics.com	67.8%	ajax.googleapis.com	23.1%
gstatic.com	50.1%	googlesyndication.com	19.6%
fonts.googleapis.com	42.8%	googleadservices.com	14.1%
doubleclick.net	40.5%	twitter.com	12.8%
facebook.com	33.7%	fbcdn.net	10.7%
google.com	33.2%	adnxs.com	10.5%
facebook.net	27.4%		

Ghostery


Ghostery found 13 trackers
www.cnn.com
ClickTale
Analytics, Analytics, Behavior Tracking
DoubleClick
Advertising
Facebook Connect
Widgets, Social
Gravity Insights
Analytics
Krux Digital
Beacons
Livefyre
Widgets, Commenting System

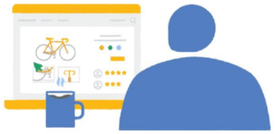
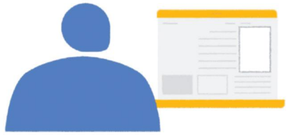
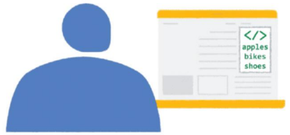
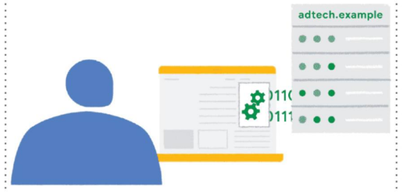
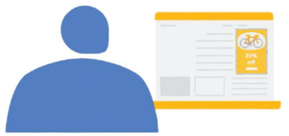
DNT


Mozilla Firefox Web Browser — Do Not Track — Mozilla - Mozilla Firefox
Mozilla Firefox ...
Mozilla Foundation (US) https://www.mozilla.org/en-US/firefox/dnt/
Search
FIREFOX
ADD-ONS
SUPPORT
mozilla
Firefox
HOME > DO NOT TRACK FAQ
Do Not Track
Mozilla is a global, nonprofit organization dedicated to making the Web better. We emphasize principle over profit, and believe that the Web is a shared public resource to be cared for, not a commodity to be sold. We answer to no one but you and believe it is crucial to put you in control of your online experience. We are aiming to give you better insight and control into the ways your personal information is collected, used, stored and shared online.
Mozilla Firefox offers a Do Not Track feature that lets you express a preference not to be tracked by websites. When the feature is enabled, Firefox will tell advertising networks and other websites and applications that you want to opt-out of tracking for purposes like behavioral advertising.
Do Not Track
Your Status:
Do Not Track is ON
Enable Do Not Track in Firefox
General
Tabs
Content
Tracking
Tell web sites I do not want to be
Click for Instructions »

2024 — The Year of the End of Third Party Cookies?

- Firefox:
  - Third-Party Cookies from known trackers are dropped
  - Third-party cookies use separate cookie jar per site, so they can't be used to track users across sites
- Safari: Blocks third-party cookies
- IE: blocks some third-party cookies based on baked-in blacklist
- Edge does not block third-party cookies by default
- Chrome announced that they will drop support for third party cookies by the end of 2024

Google Topics

User's browser	User's browser	Site that displays ads	Adtech code	Adtech code	Adtech code
					
User visits websites	Browser infers topics of interest	User visits site displaying ads	Topics are retrieved	Ad is requested	Ad is displayed
The user visits websites about a range of topics, for example: "Country Music", "Makeup & Cosmetics", "Vegetarian Cuisine"	The browser calculates the most frequently visited topics from the user's recent browsing history	The user visits a site whose adtech platform needs to select an ad for them	The adtech platform gets topics of interest to the user by calling the Topics API function `browsingTopics()`	The adtech platform uses the topics provided by the Topics API as part of the input to help select an ad	An ad is displayed to the user

Topics are selected from a taxonomy consisting of hierarchical categories such as /Arts & Entertainment/Music & Audio/Soul & R&B and /Business & Industrial/Agriculture & Forestry.

The (maximum) three topics returned for a user are chosen at random from the top five for the past three epochs (with a 5% chance of getting a random topic).

Web Tracking
Browser Fingerprinting

- Websites can also fingerprint you effectively with *browser fingerprinting*, which is a technique that leverages all your settings to identify you, and stores this in a cookie on your browser
  - https://amiunique.org/
- So long as JavaScript can run (by third-parties), you run the risk of being "followed" on the web


```
{
 "user-agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:93.0) Gecko/20100101 Firefox/93.0",
 "accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8",
 "accept-encoding": "gzip, deflate, br",
 "accept-language": "en-US,en;q=0.5",
 "upgrade-insecure-requests": "1",
 "referer": "https://amiunique.org/",
 "userAgent-js": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:93.0) Gecko/20100101 Firefox/93.0",
 "platform": "MacIntel",
 "cookies": "yes",
 "timezone": 420,
 "languages-js": "en-US,en",
 "ad": "no",
 "doNotTrack": "NC",
 "navigator_properties": [
  "vibrate",
  "javaEnabled",
  "getGamepads",
  "getVRDisplays",
  "mozGetUserMedia",
  "sendBeacon",
  "requestMediaKeySystemAccess",
  "registerProtocolHandler",
  "taintEnabled",
```

MY BROWSER FINGERPRINT

SEE YOUR BROWSER FINGERPRINT PROPERTIES

ARE YOU UNIQUE ?

DOWNLOAD | TIMELINE

TODAY | 7 DAYS | 15 DAYS | 30 DAYS | 90 DAYS | ALL TIME

Yes! You are unique among the 2382170 fingerprints in our entire dataset.

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users sharing the same elements.

mac os	chrome	en	UTC-08:00
Operating system	Web browser	Language	Timezone
MacOS		en	UTC-08:00
10.11 %	43.12 %	75.07 %	1.88 %

HTTP HEADERS ATTRIBUTES

Search for an attribute

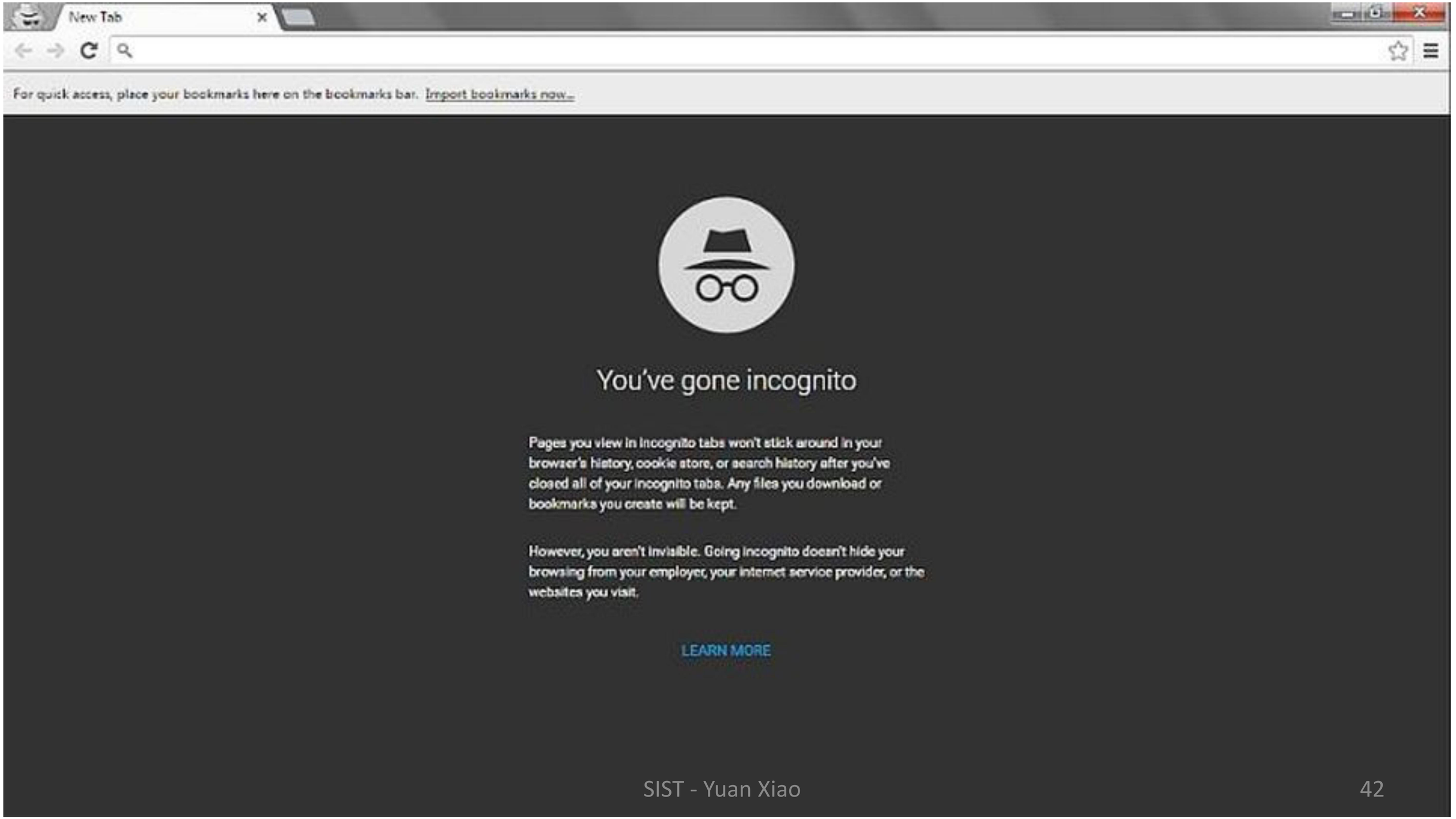
Attribute	Similarity ratio	Value
1 - User agent	0.10 %	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
2 - Accept	12.02 %	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
3 - Content encoding	96.52 %	gzip, deflate, br
4 - Content language	19.94 %	en-US,en;q=0.9
5 - Upgrade Insecure Requests	91.00 %	1

JAVASCRIPT ATTRIBUTES

Search for an attribute

Attribute	Similarity ratio	Value
1 - User agent	0.09 %	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
2 - Platform	10.01 %	MacIntel
3 - Cookies enabled	89.14 %	✓
4 - Timezone	1.88 %	UTC-08:00

		pdf-viewer.
20 - Screen width	4.25 %	2560
21 - Screen height	4.58 %	1440
22 - Screen depth	3.64 %	30
23 - Screen available top	3.32 %	25
24 - Screen available Left	83.26 %	0
25 - Screen available Height	0.01 %	1346
26 - Screen available width	4.07 %	2560
27 - Permissions	6.24 %	**accelerometer** : granted **accessibility** : Not supported **ambient-light-sensor** : Not supported **camera** : prompt **clipboard-read** : prompt **clipboard-write** : granted **geolocation** : prompt **background-sync** : granted **magnetometer** : granted **microphone** : prompt **midi** : granted **notifications** : prompt **payment-handler** : granted **persistent-storage** : prompt **push** : Not supported
28 - WebGL Vendor	1.83 %	Google Inc. (Apple)
29 - WebGL Renderer	0.01 %	ANGLE (Apple, ANGLE Metal Renderer: Apple M2 Max, Unspecified Version)
30 - WebGL Data	0.13 %	
31 - WebGL Parameters	0.03 %	35 different extensions 25 different general parameters analyzed 36 different shaders precisions analyzed


New Tab
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
You've gone incognito
Pages you view in Incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your Incognito tabs. Any files you download or bookmarks you create will be kept.
However, you aren't invisible. Going Incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.
LEARN MORE

Services & Forms

- Bankruptcy
- Bankruptcy Basics
- Filing Without an Attorney
- Credit Counseling and Debtor Education
- Trustees and Administrators
- Approved Bankruptcy Notice Providers

Share This Page

Bankruptcy

Bankruptcy helps people who can no longer pay their debts get a fresh start by liquidating assets to pay their debts or by creating a repayment plan. Bankruptcy laws also protect financially troubled businesses. This section explains the bankruptcy process and laws.

About Bankruptcy

Filing bankruptcy can help a person by discarding debt or making a plan to repay debts. A bankruptcy case normally begins when the debtor files a petition with the bankruptcy court. A petition may be filed by an individual, by spouses together, or by a corporation or other entity.

All bankruptcy cases are handled in federal courts under rules outlined in the U.S. Bankruptcy Code.

There are different types of bankruptcies, which are usually referred to by their chapter in the U.S. Bankruptcy Code.

- Individuals may file Chapter 7 or Chapter 13 bankruptcy, depending on the specifics of their situation.
- Municipalities—cities, towns, villages, taxing districts, municipal utilities, and school districts may file under Chapter 9 to reorganize.

Related Links

- Bankruptcy Fees
- Bankruptcy Forms
- Chapter 7 Fee Waiver Procedures & Resources
- Protection of Tax Information Guidance
- Pending Bankruptcy Forms
- Permitted Changes to Official Bankruptcy Forms

Privacy Enhancing Technologies

Methods for protecting personal data

Most Common/Successful? TLS.

Comes with browser. Also used for protecting email. It just works, without you having to configure anything. Protects *contents* of communication from passive eavesdroppers and active MITM attacks.

Tools that provide confidentiality also provide some privacy. You probably don't want your landlord or coffee shop customers to learn things about you.

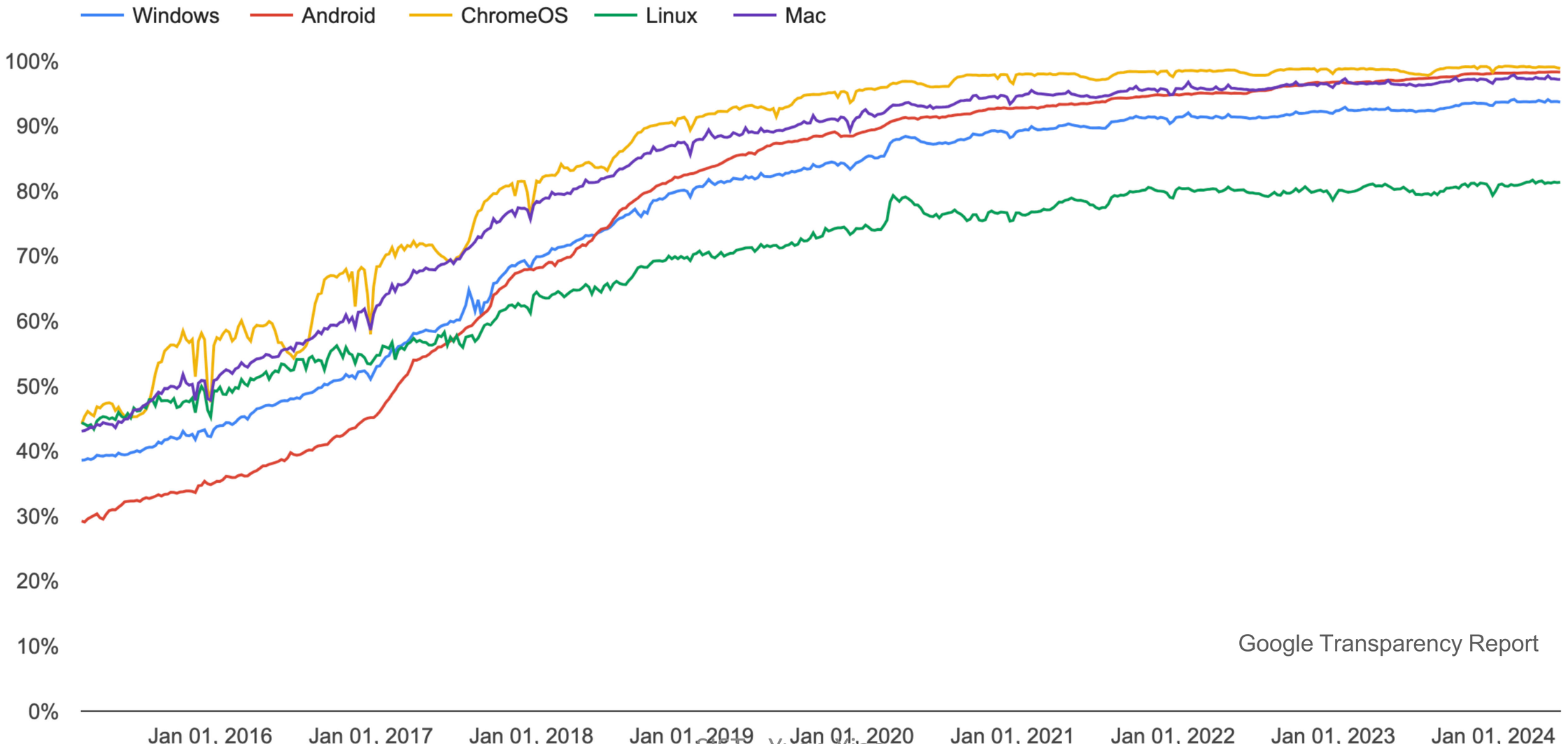
Encouraging HTTPS Adoption

2014: HTTPS used as a page rank indicator

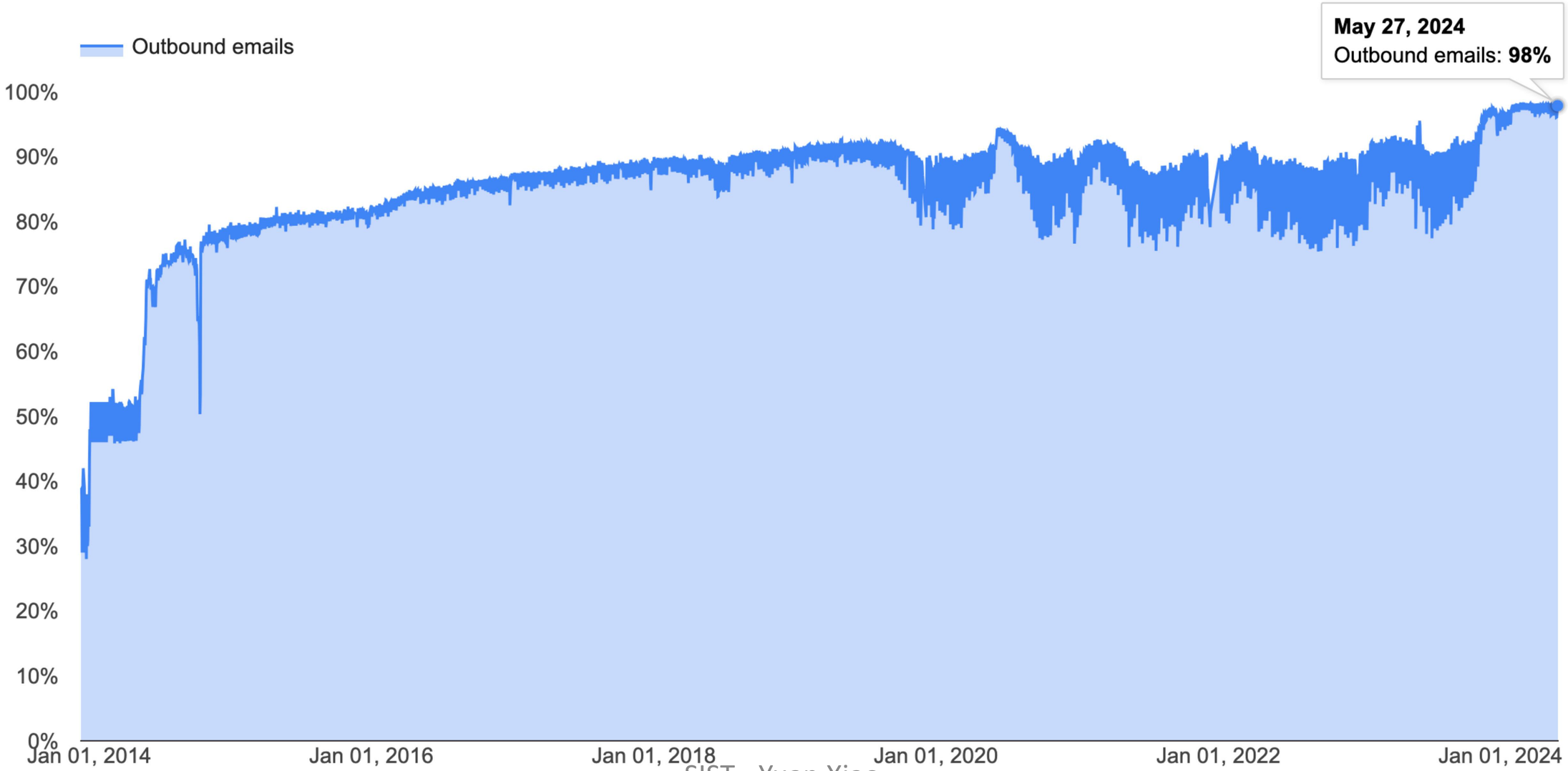
Early 2018: Mozilla announces that new features will require HTTPS

Late 2018: New Chrome HTTPS indicators

Chrome Page Loads over HTTPS



STARTTLS as seen by Gmail



Protecting Metadata

TLS only protects content. What doesn't TLS protect against?

We may want to protect metadata:

- Who is visiting what websites? Who is sending messages to whom?
- Gov't might not like that you're visiting Human Rights Watch website
- Gov't might not be amused that you're sending messages to Human Rights Watch
- We may want to hide the existence of the message (maybe sending an encrypted message at all is going to cause you problems)

What is Anonymity?

Anonymity (“without name’’) means that a person is not identifiable within a set of subjects

Unlinkability of action and identity

- For example, sender and his email are no more related after adversary’s observations than they were before

- Who talks to whom

Unobservability

- Adversary cannot tell whether someone is using a particular system and/or protocol

Why Anonymity?

To protect privacy:

- Avoid tracking by advertising companies
- Viewing sensitive content
    - Information on medical conditions
    - Advice on bankruptcy

Protection from prosecution

- Not every country guarantees free speech

To prevent chilling-effects

- It’s easier to voice unpopular or controversial opinions if you are anonymous

Anonymity is Hard

Internet anonymity is hard…

Right there in every packet is the source and destination IP address

ISPs store communications records

- Law enforcement can subpoena these records

Wireless traffic can be trivially intercepted

Tier 1 ASs and IXPs are compromised — NSA, GCHQ, “Five Eyes”

Anonymity

Difficult if not impossible to achieve on your own

You generally need help.

State of the art technique: Ask someone else to send it for you

Naive approach .... VPNs

Naive approach .... VPNs

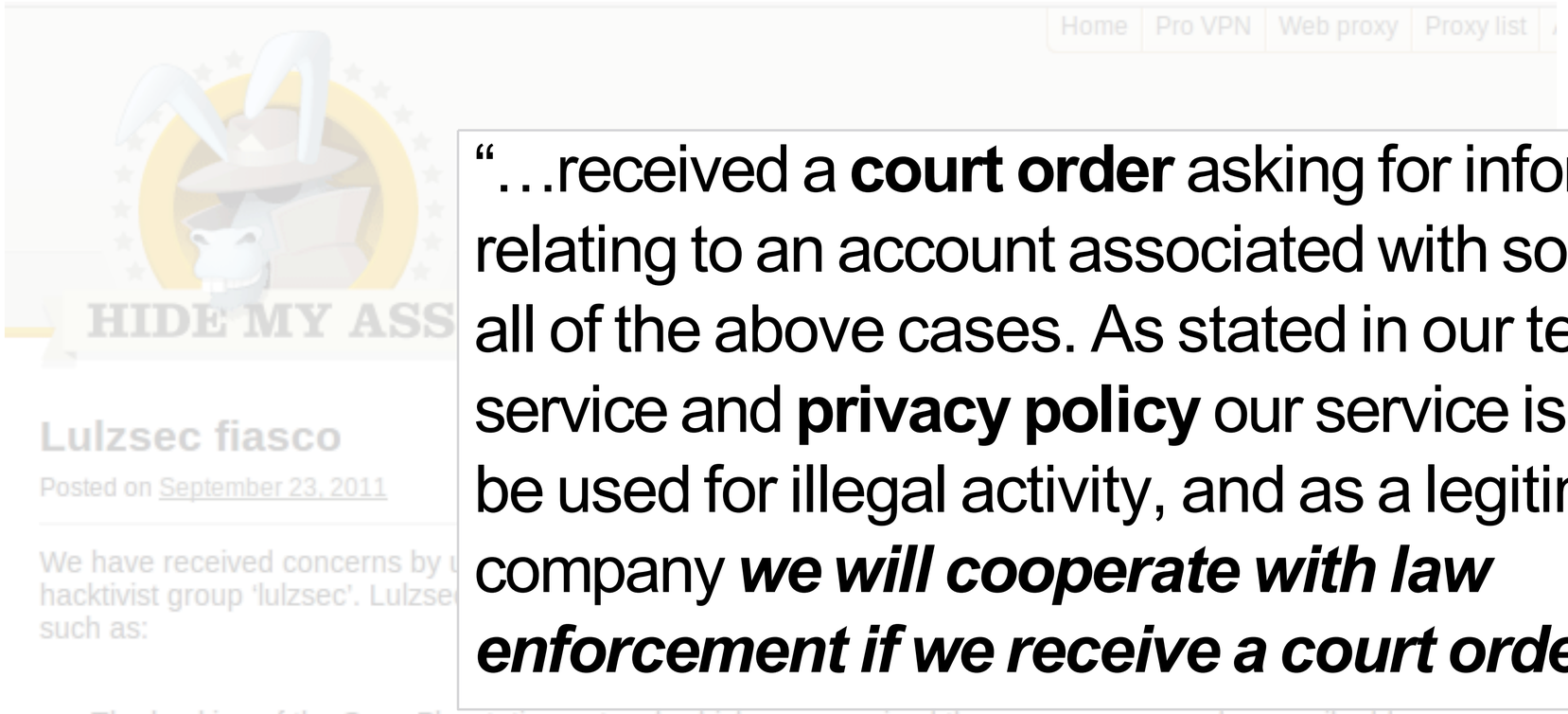
Lulzsec fiasco

Posted on September 23, 2011

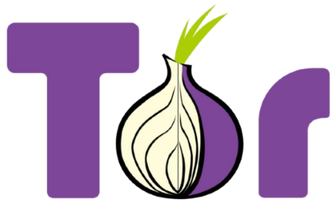
We have received concerns by users that our VPN service was utilized by a member or members of the hacktivist group 'lulzsec'. Lulzsec have been ALLEGEDLY been responsible for a number of high profile cases such as:

- The hacking of the Sony Playstation network which compromised the names, passwords, e-mail addresses, home addresses and dates of birth of thousands of people.
- The DDOS attack which knocked the British governments SOCA (Serious Organised Crime Agency) and other government websites offline.
- The release of various sensitive and confidential information from companies such as AT&T, Viacom, Disney, EMI, NBC Universal, and AOL.
- Gaining access to NATO servers and releasing documents regarding the communication and information services (CIS) in Kosovo.
- The defacement of British newspaper websites The Sun & The Times

Naive approach .... VPNs



"…received a **court order** asking for information relating to an account associated with some or all of the above cases. As stated in our terms of service and **privacy policy** our service is not to be used for illegal activity, and as a legitimate company ***we will cooperate with law enforcement if we receive a court order***"

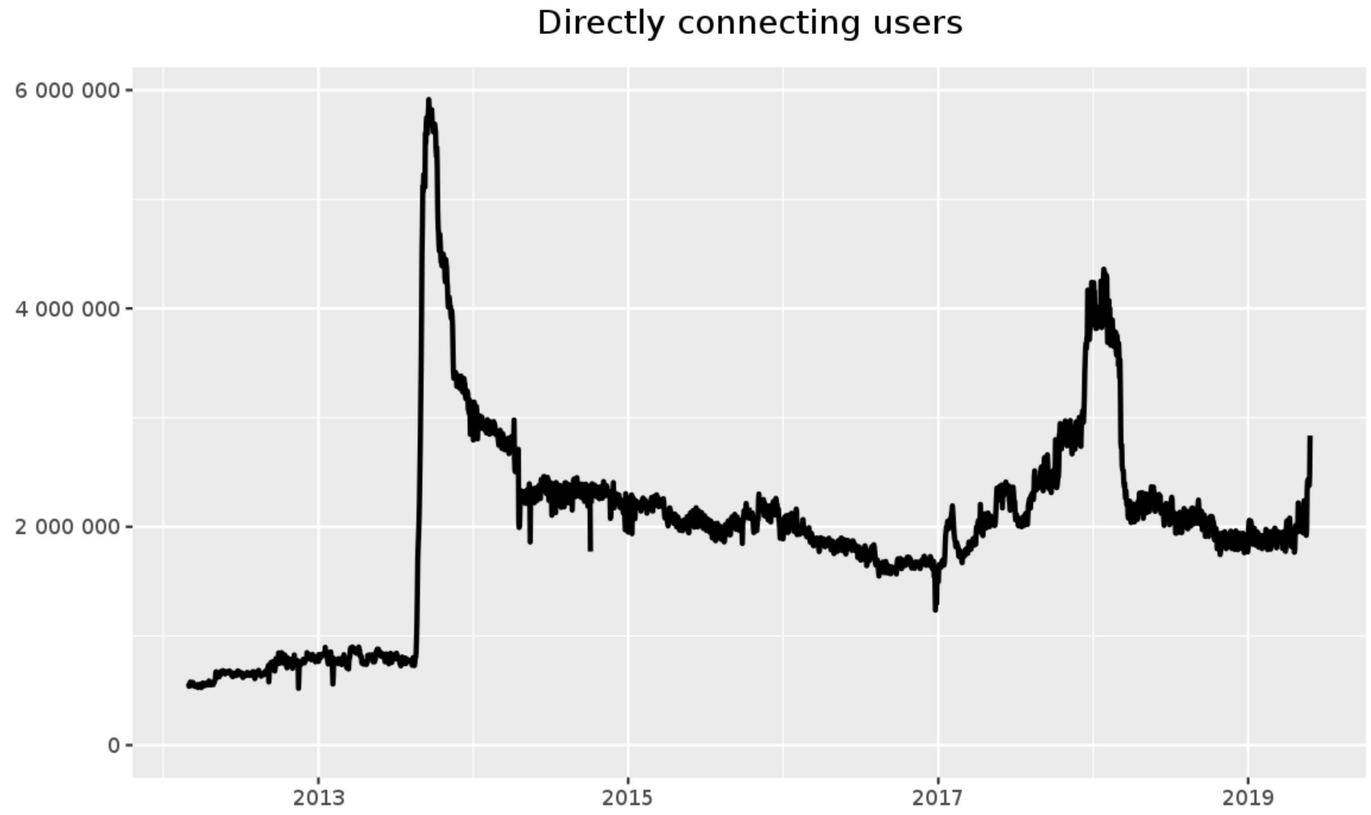


Tor is a successful privacy enhancing technology that works at the transport layer

Millions of active users.

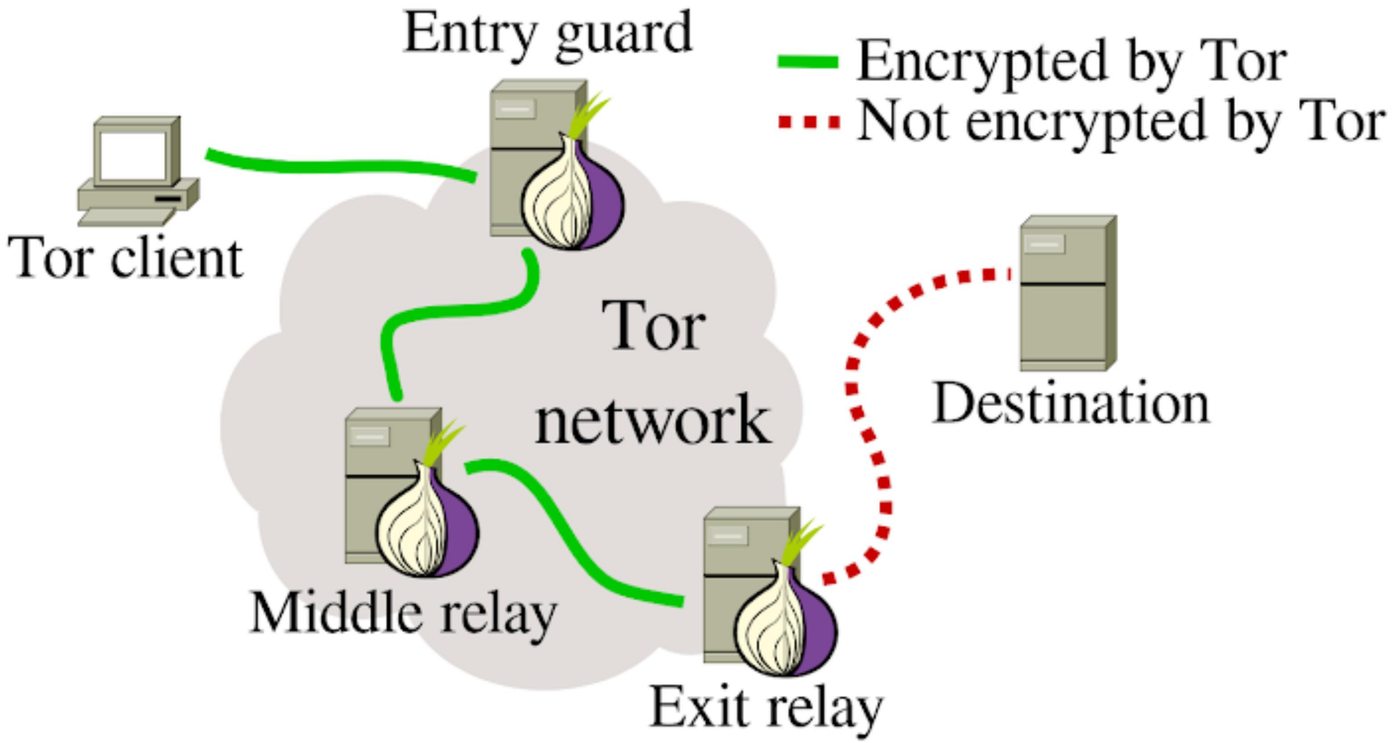
Normally, a TCP connection reveals your IP address

Tor allows TCP connections without revealing your IP



Tor ("The Onion Router")

Tor operates by tunneling traffic through multiple "onion routers" using public key cryptography



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!)

Does Tor Provide Anonymity?

Tor provides for 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 Challenges

Performance: message bounces around a lot (can be slow)

Attack: government can coerce server operates in one country
  Defense: use mix servers in different legal jurisdictions

Attack: adversary operates all of the mixes
  Defense: have lots of mix servers (Tor has ~7,000 onion routers today). Use diverse set.

Attack: adversary observes when Alice sends and when Bob receives, links the two together

A side channel attack – exploits timing information
  Defenses: pad messages, introduce significant delays
    Tor does the former, but notes that it's not enough for defense

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

Tor Hidden Services

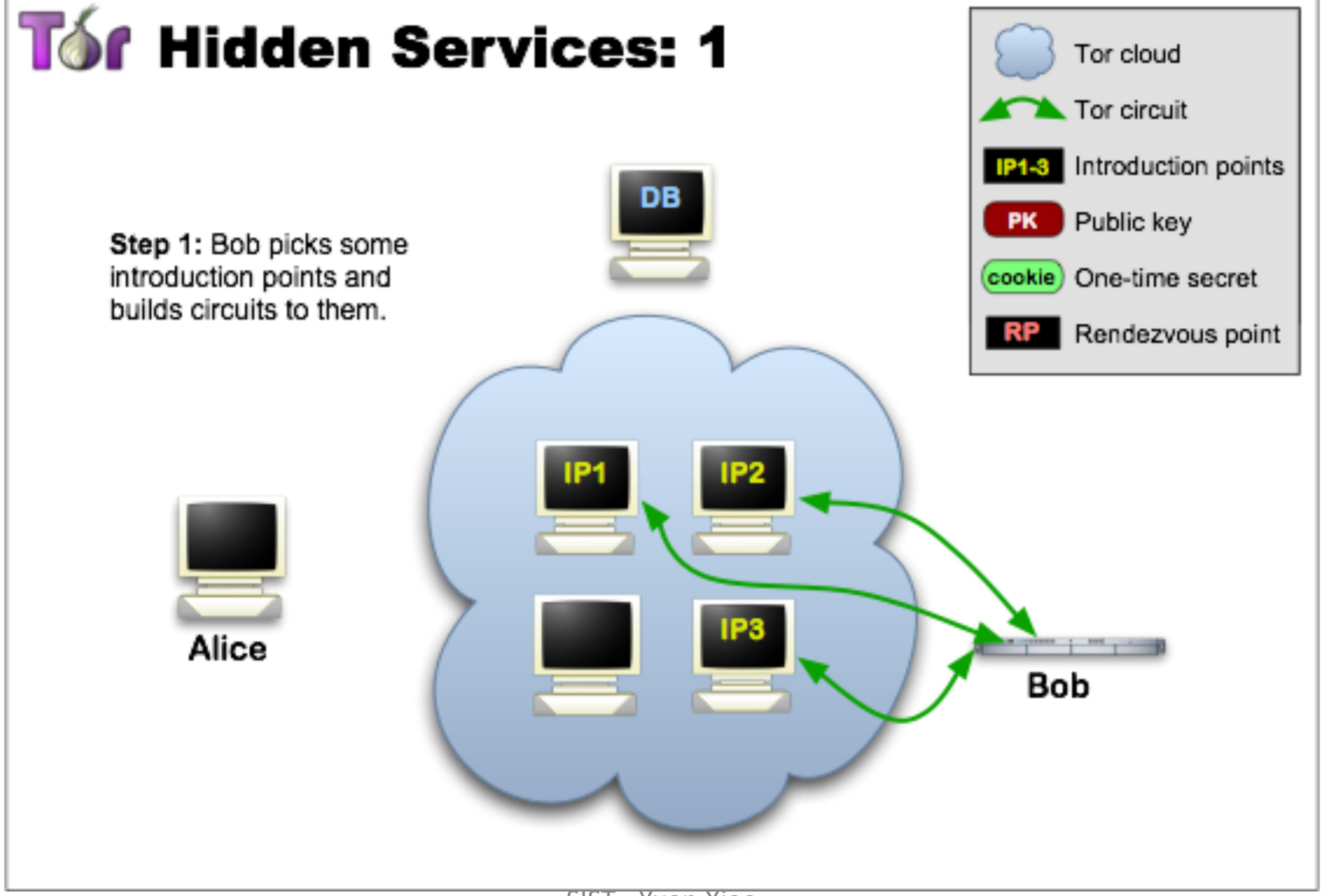
As described, Tor protects the identity of the client, but not the server

What if we want to run an anonymous service?
- a website, where nobody knows the IP address?

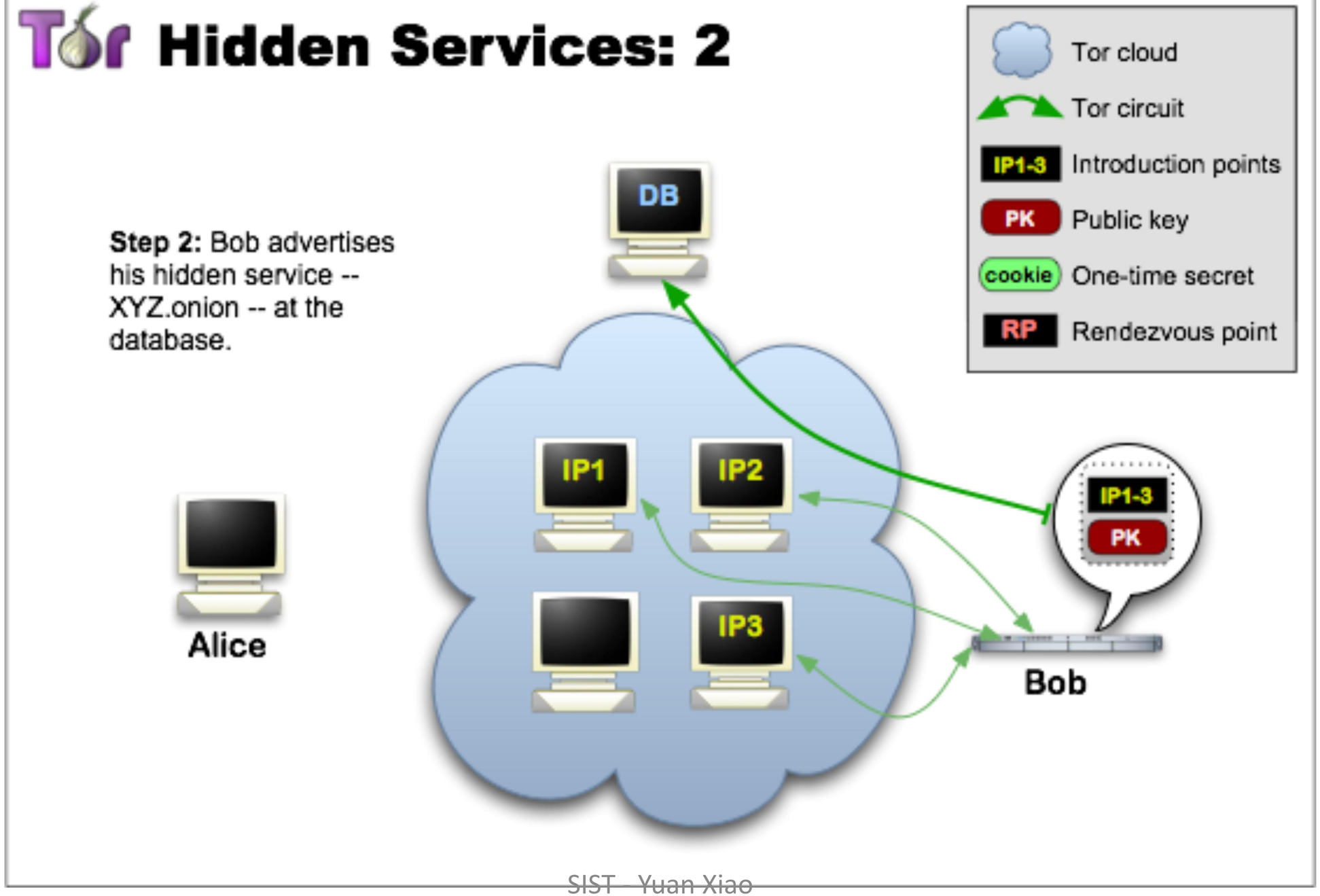
Tor supports Hidden Services…
- Allows you to run a server without disclosing the IP or DNS name

Many hidden services
- Duck Duck Go, Tor Chat, Wikileaks

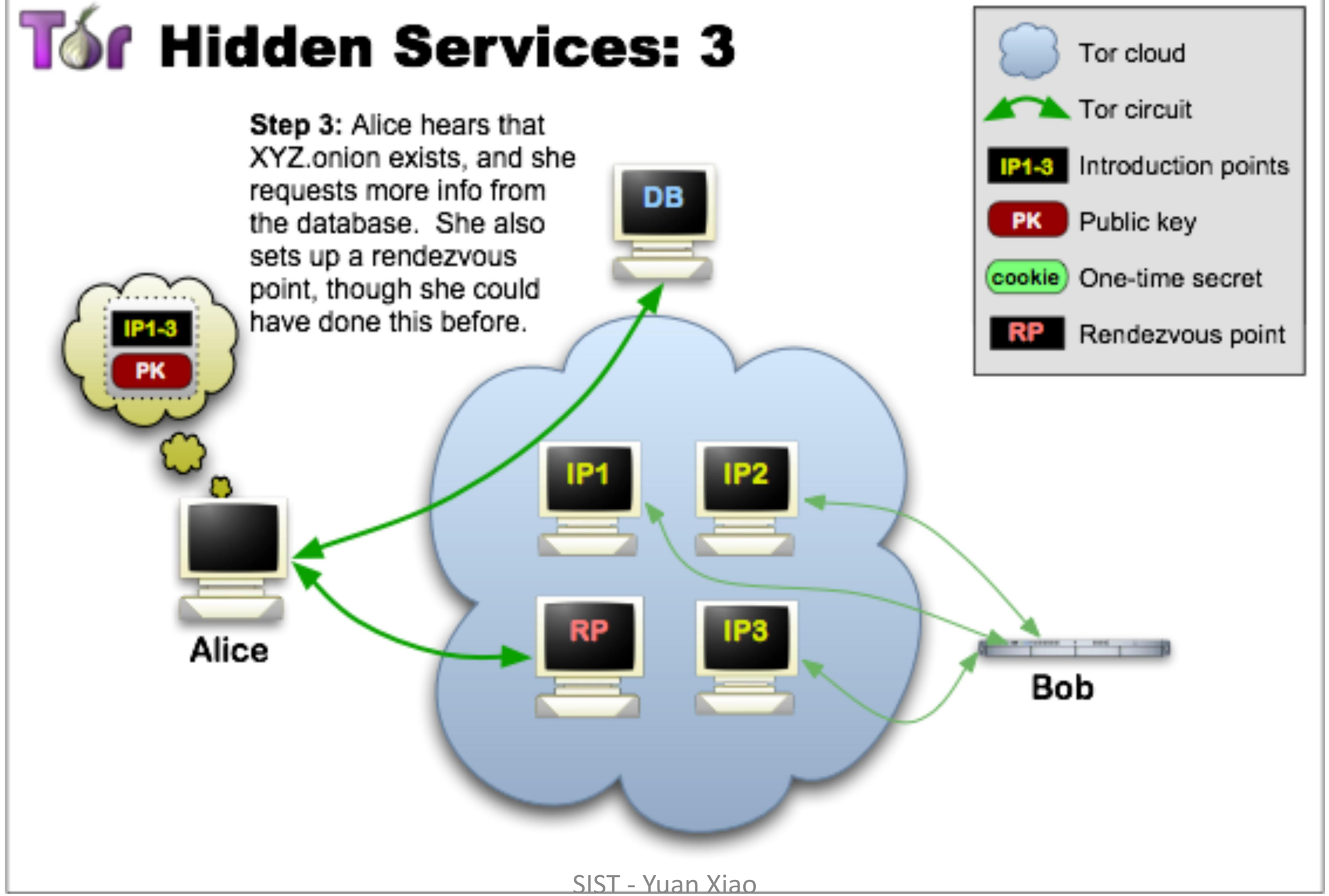
Hidden Services: 1



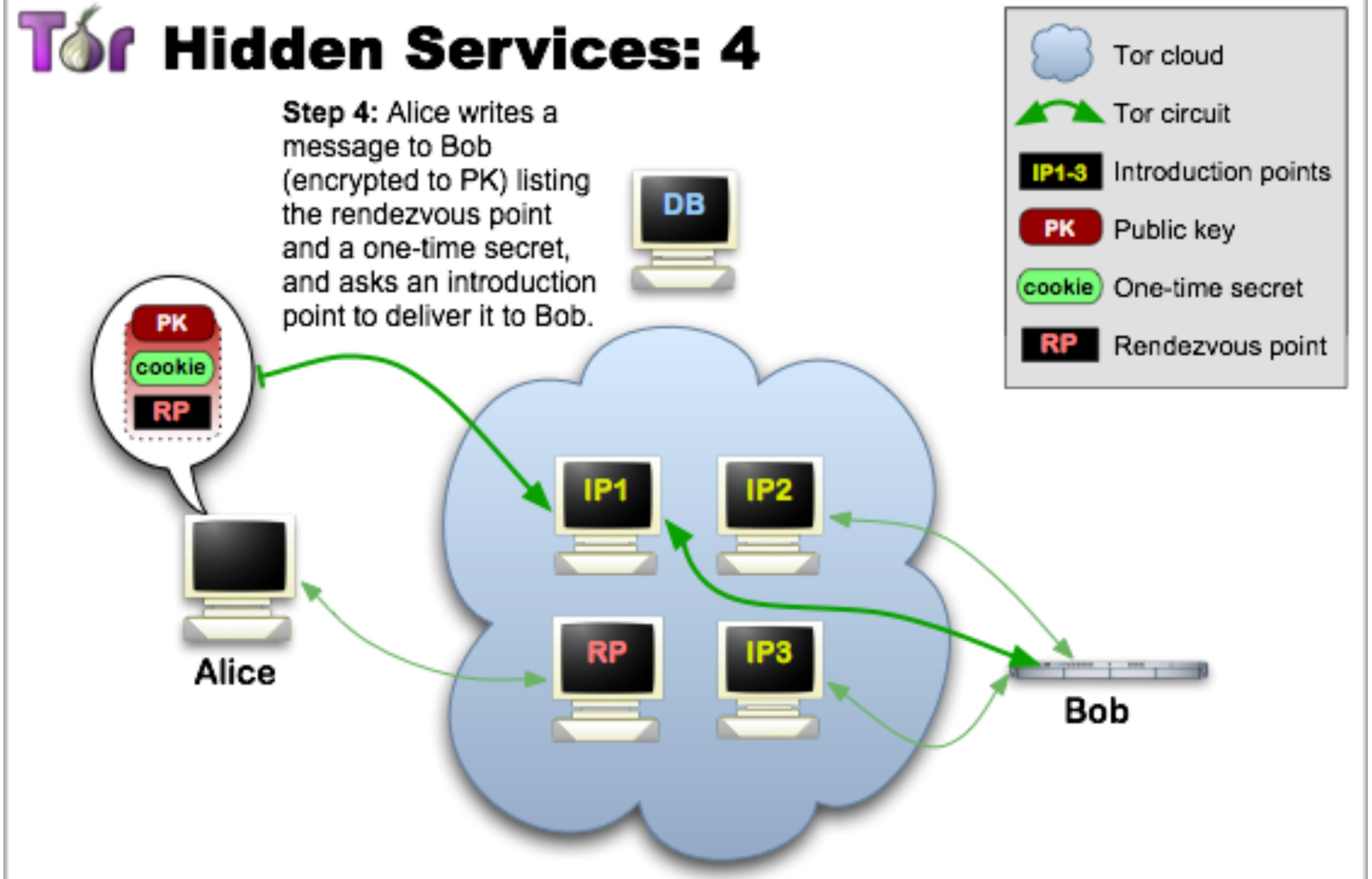
Hidden Services: 2



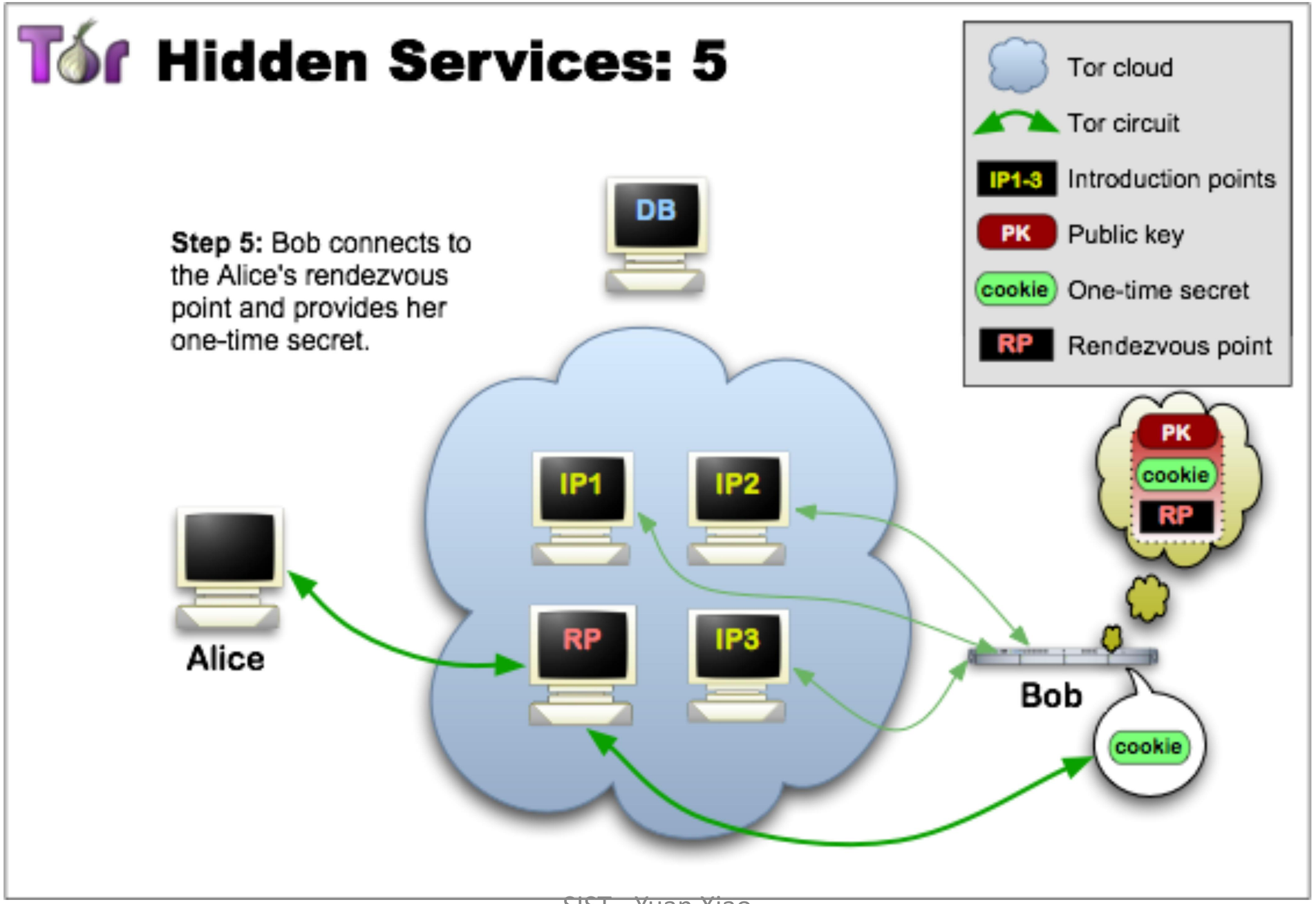
Hidden Services: 3



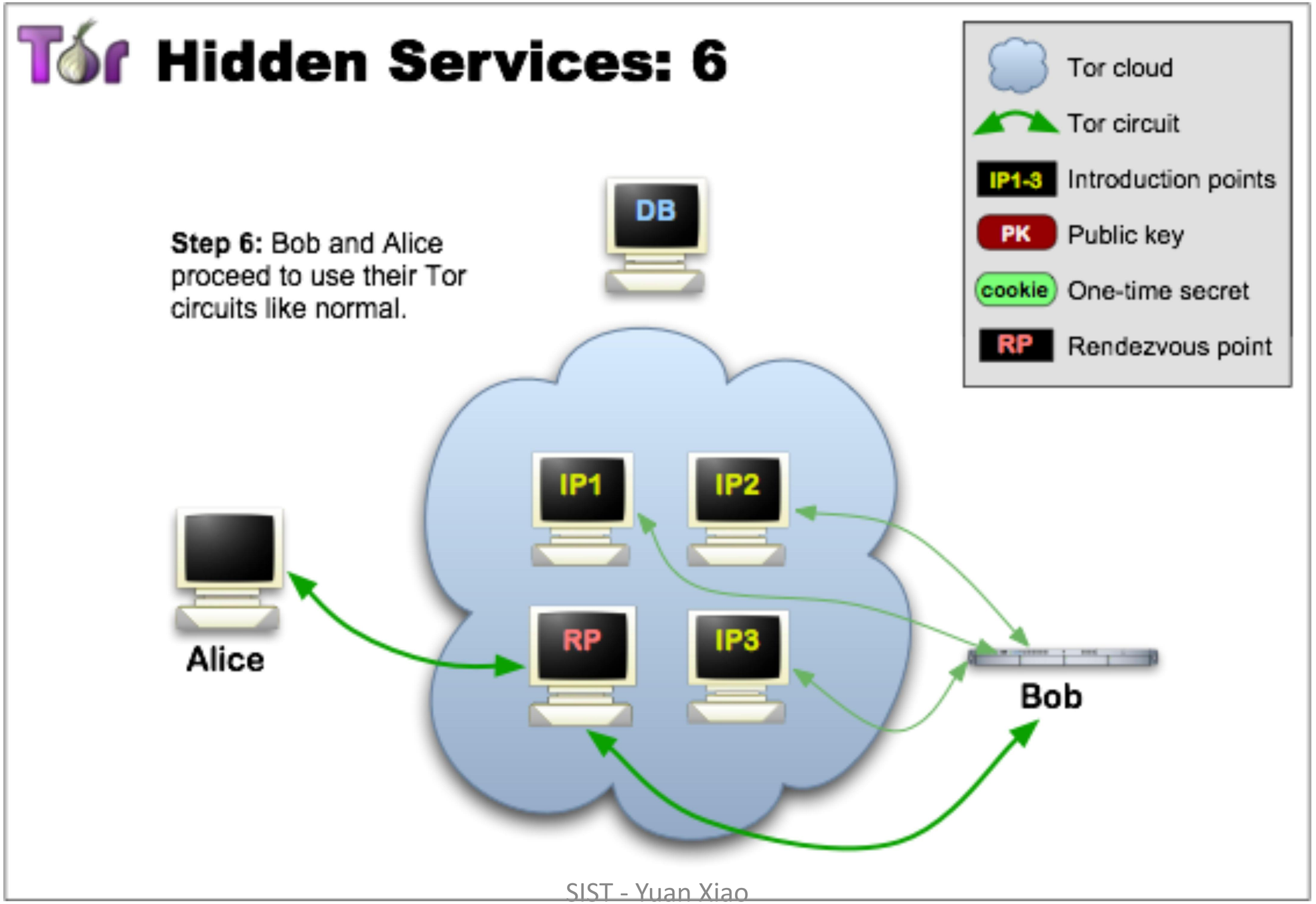
Hidden Services: 4



Hidden Services: 5



Hidden Services: 6



Silk Road

anonymous marketplace

Welcome **now0open**!

messages(0) | **orders(0)** | **account(฿0)** | **settings** | **log out**

search | **(0)**

Shop by category:

- Drugs(752)
  - Cannabis(280)
  - Ecstasy(35)
  - Dissociatives(11)
  - Psychedelics(84)
  - Opioids(62)
  - Stimulants(53)
  - Other(107)
  - Benzos(70)
- Lab Supplies(6)
- Digital goods(98)
- Services(48)
- Money(55)
- Weaponry(15)
- Home & Garden(14)
- Food(4)
- Electronics(5)
- Books(49)
- Drug paraphernalia(28)
- XXX(30)
- Medical(3)
- Computer equipment(4)
- Apparel(4)
- Musical instruments(2)
- Tickets(1)
- Forgeries(13)

5 Marijuana Butter Chocolate Chip...
฿8.53

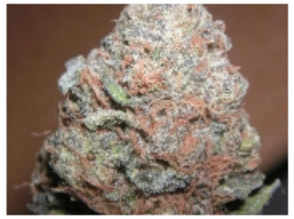
4mg. TIZANIDINE (zanaflex) x25
฿2.09

US customers only Express...
฿2.79

4 x 20MG Original Lily Cialis
฿7.85

(1g) High-grade Crystal Meth
฿11.95

MindFood - Protect your brain!...
฿3.69



to US 1/4 lb (qp) BC Master Kush...
฿121.37

How to Grow Mushrooms
฿0.14

Mushroom Indoor Growing - Easy...
฿0.29

News:

- Escrow hedging **update**
- New feature to help protect **sellers**
- We are **hiring**! Get paid for a referral, too...
- Reclaim lost coins from **MyBitcoin.com**
- Seller ranking and feedback **overhaul**
- Change your Mt. Gox **password**

recent feedback:

Silk Road Marketplace

Who uses anonymity systems?

“If you’re not doing anything wrong, you shouldn’t have anything to hide.”

- Implies that anonymous communication is for criminals

The truth: who uses Tor?

- Journalists, Law Enforcement, Human Rights Activists, Business Executives, Intelligence/Military, Normal People

Internet Censorship

Government censors

Block websites containing “offensive” content

Commonly employ blacklist approach

Observed techniques

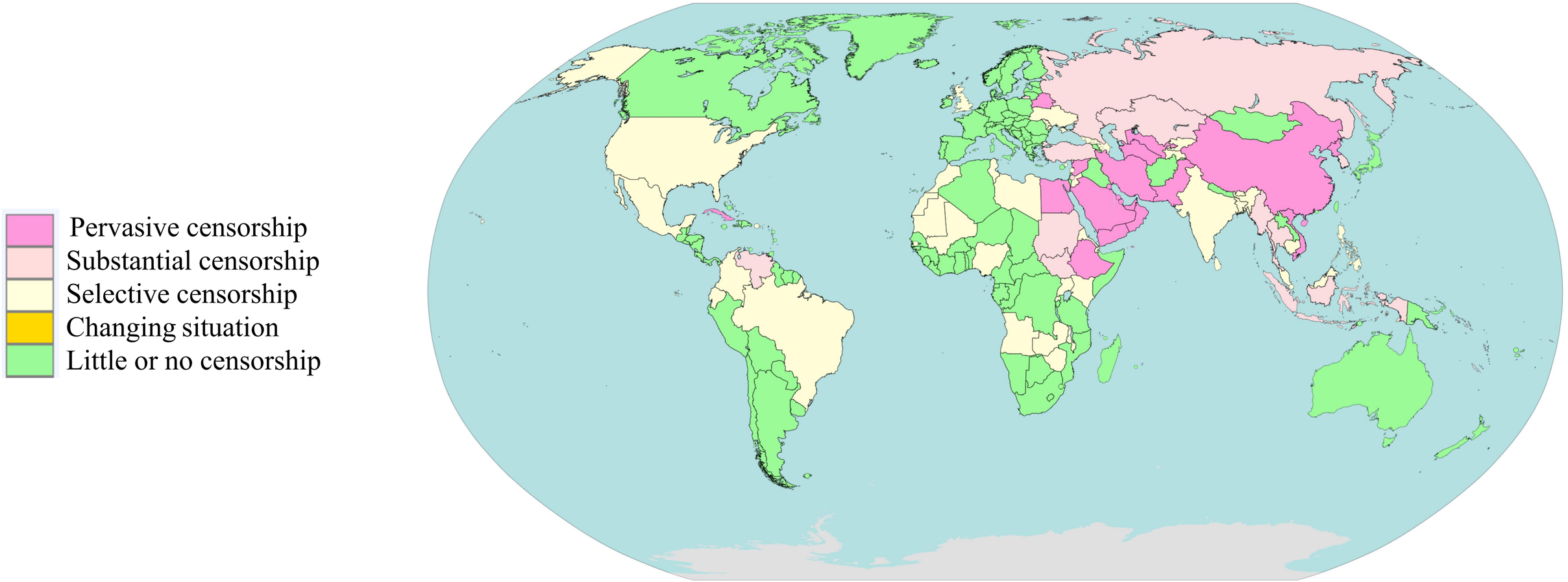
IP blocking, DNS blackholes, forged RST packets

Popular countermeasures

Mostly proxy based — Tor, Freenet, Ultrasurf, …

Problem: Cat-and-mouse game

Internet Censorship



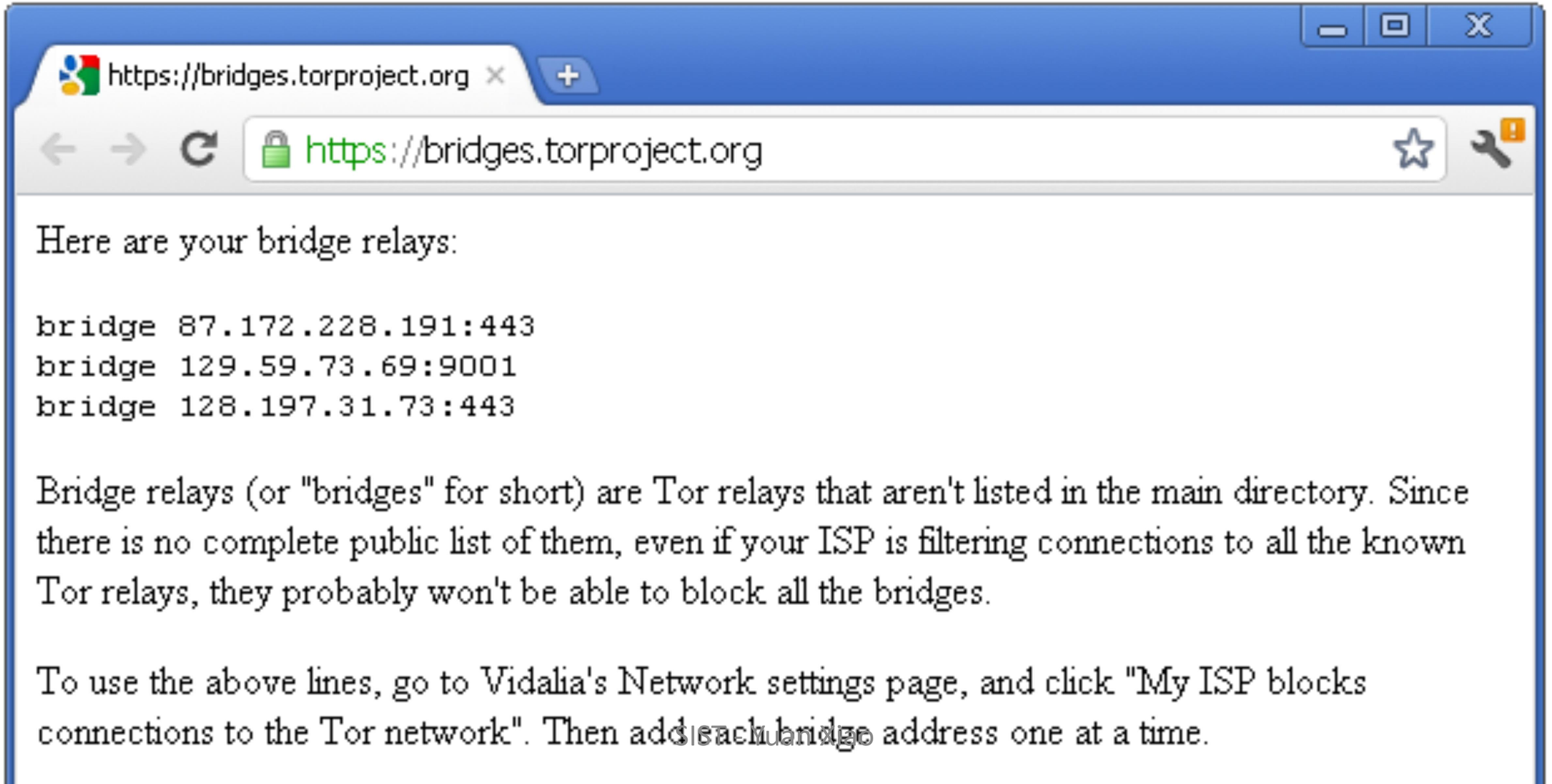
Tor Bridges

Anyone can look up the IP addresses of Tor relays
- Public information in the consensus file

Many countries block traffic to these IPs
- Essentially a denial-of-service against Tor

Solution: Tor Bridges
- Tor proxies that are not publicly known

Tor Bridges


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.

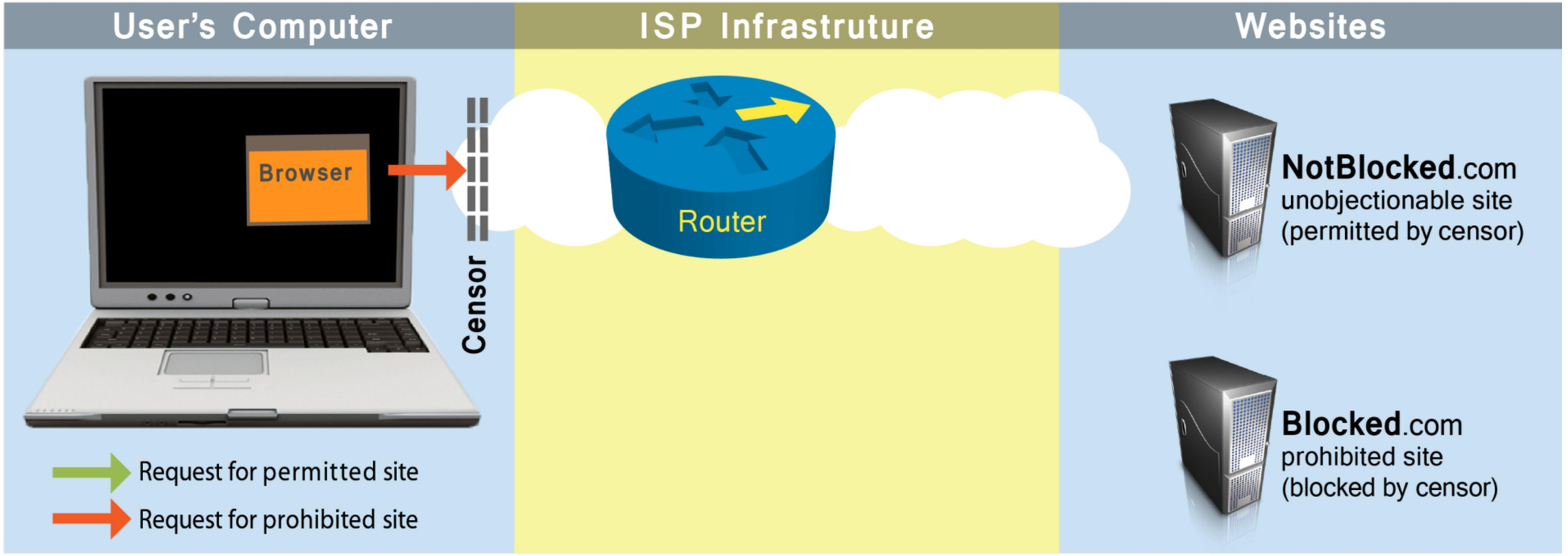
Obfuscating Tor Traffic

Bridges alone may be insufficient to 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

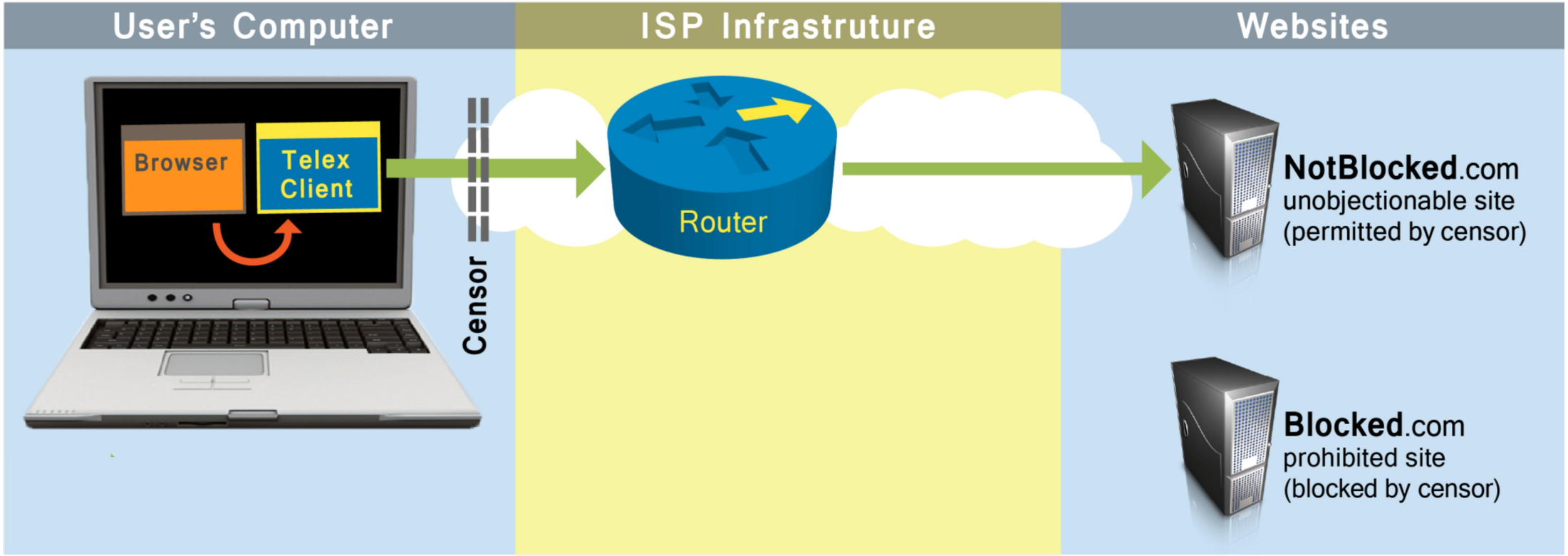
Tor adopts a pluggable transport design
- Tor traffic is forwarded to an obfuscation program
- Obfuscator transforms the Tor traffic to look like some other protocol
  - BitTorrent, Skype, HTTP, streaming audio, etc.

Decoy Routing (Telex)

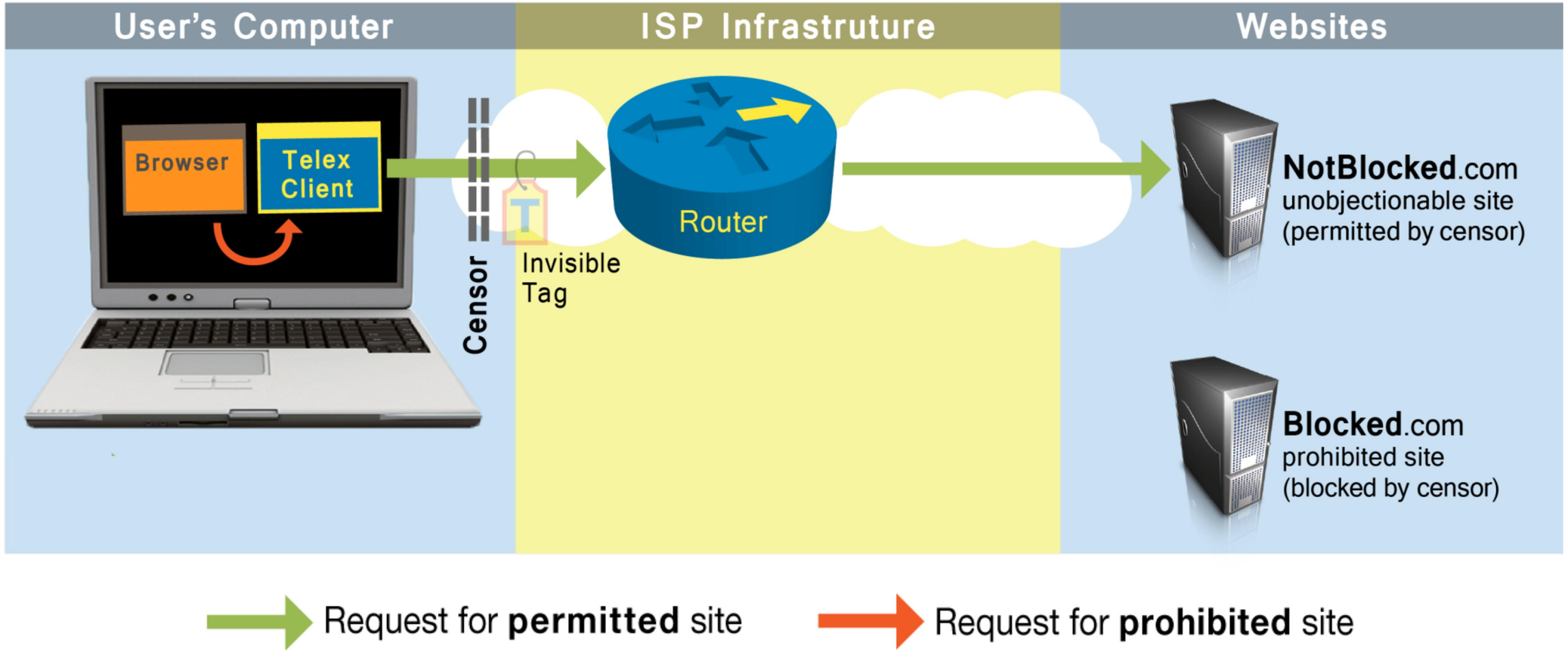


Request for **permitted** site Request for **prohibited** site

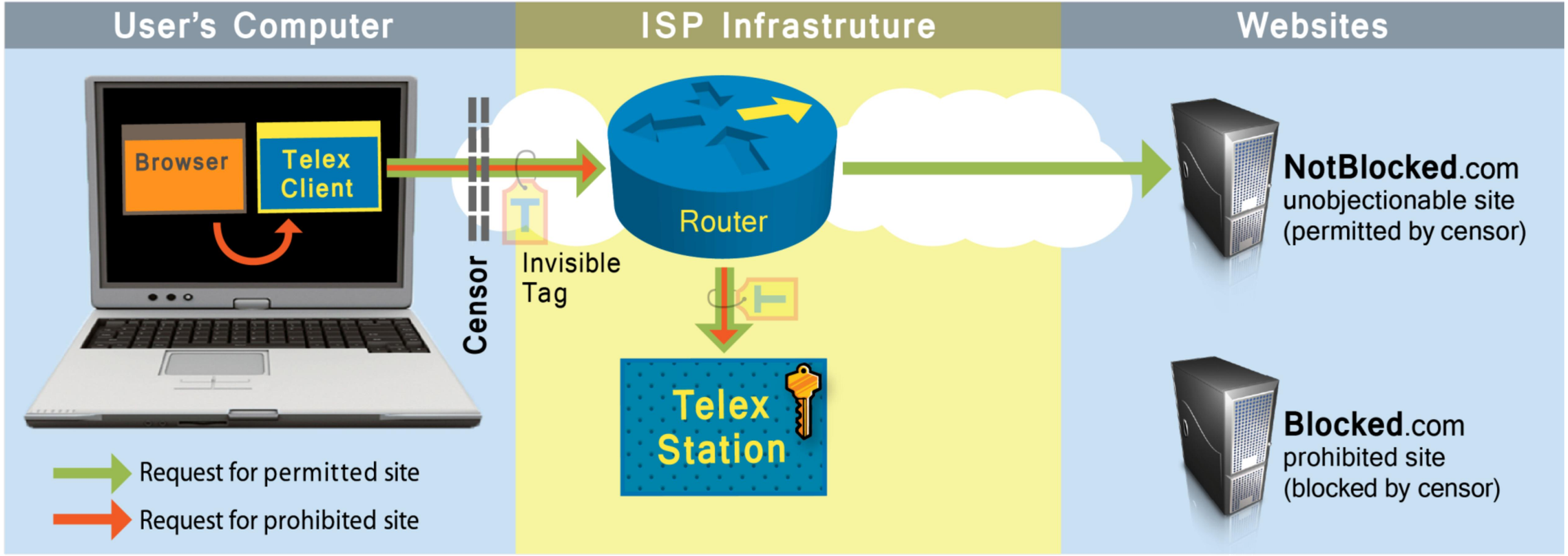
Decoy Routing (Telex)



Decoy Routing (Telex)



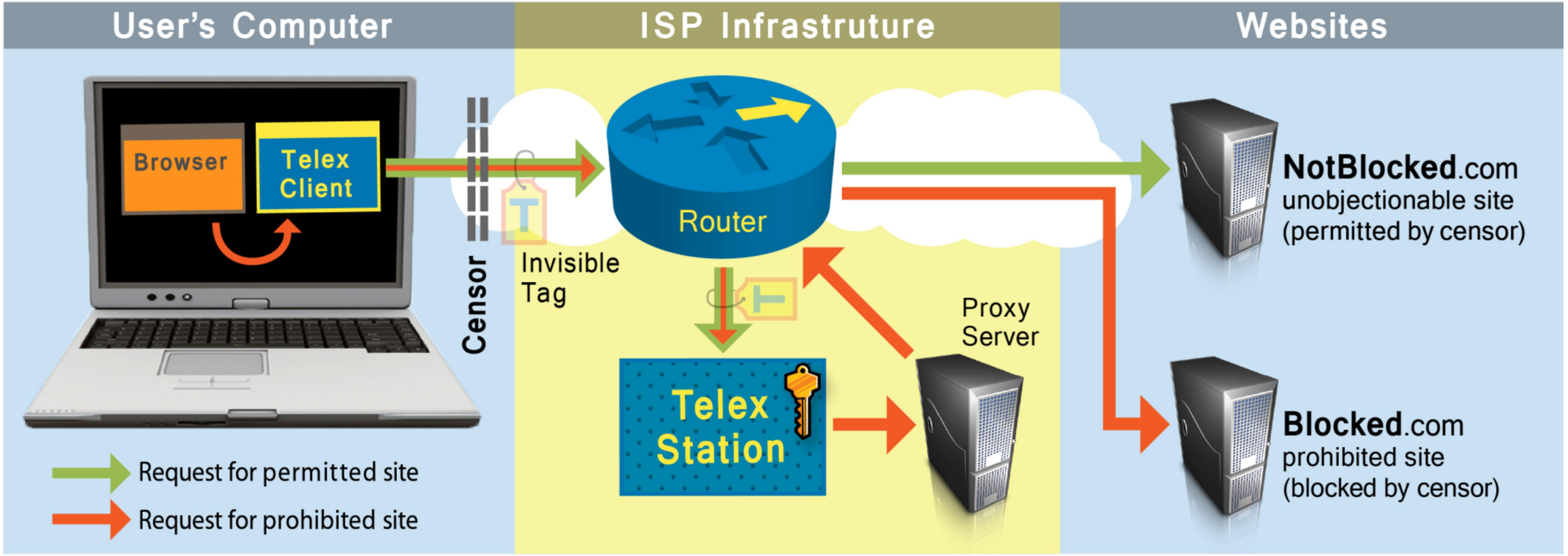
Decoy Routing (Telex)



Request for **permitted** site

Request for **prohibited** site

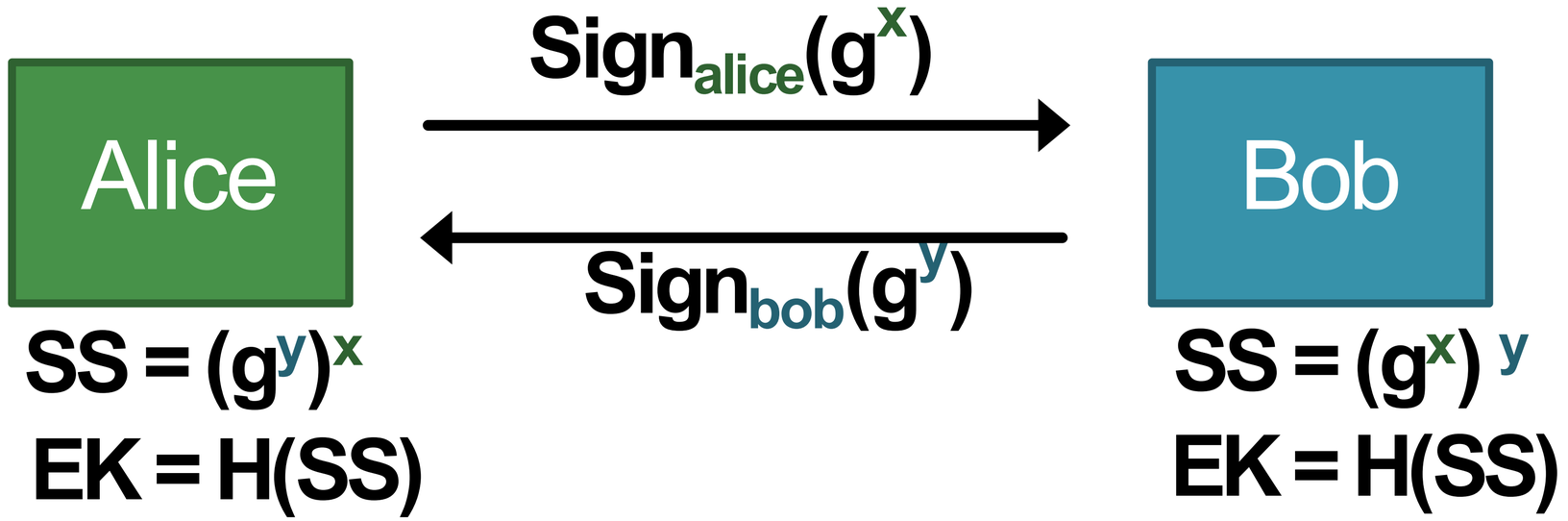
Decoy Routing (Telex)



Request for **permitted** site Request for **prohibited** site

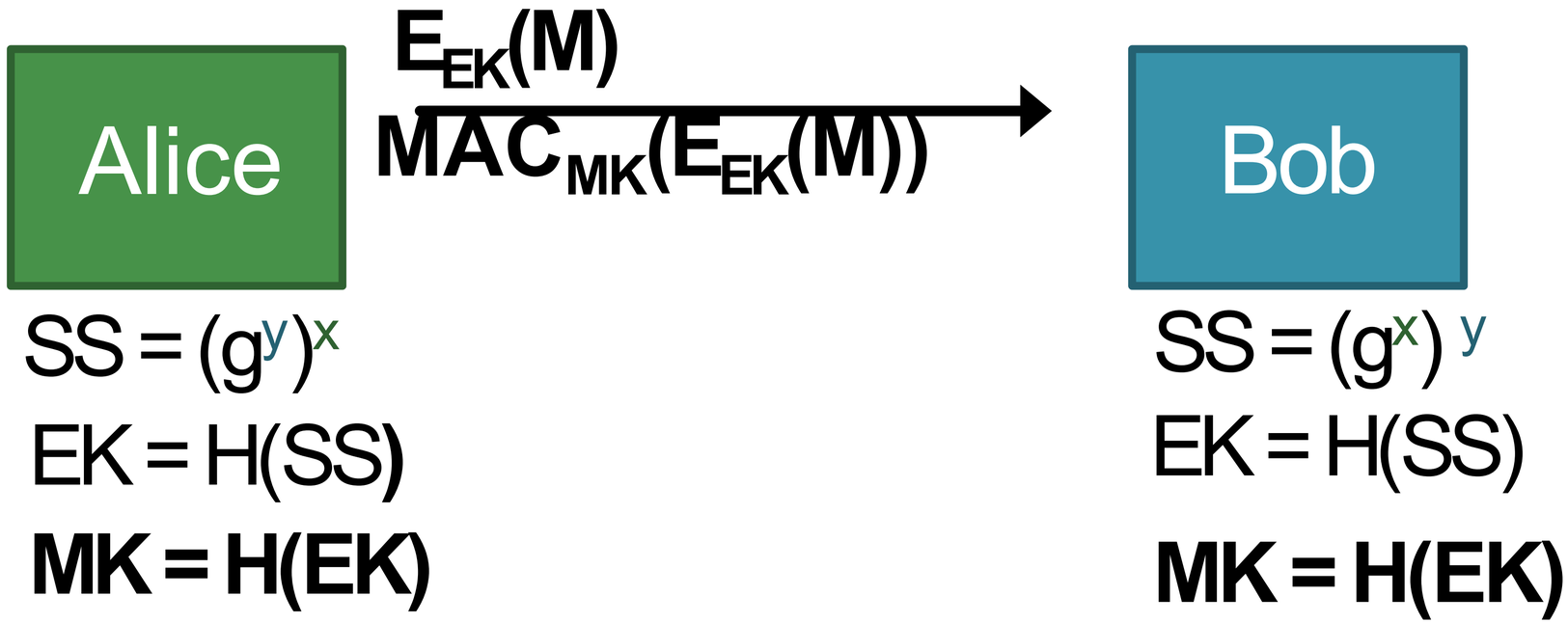
OTR: Off the Record Chat

1. Use authenticated Diffie-Hellman to establish a (short-lived) session key EK



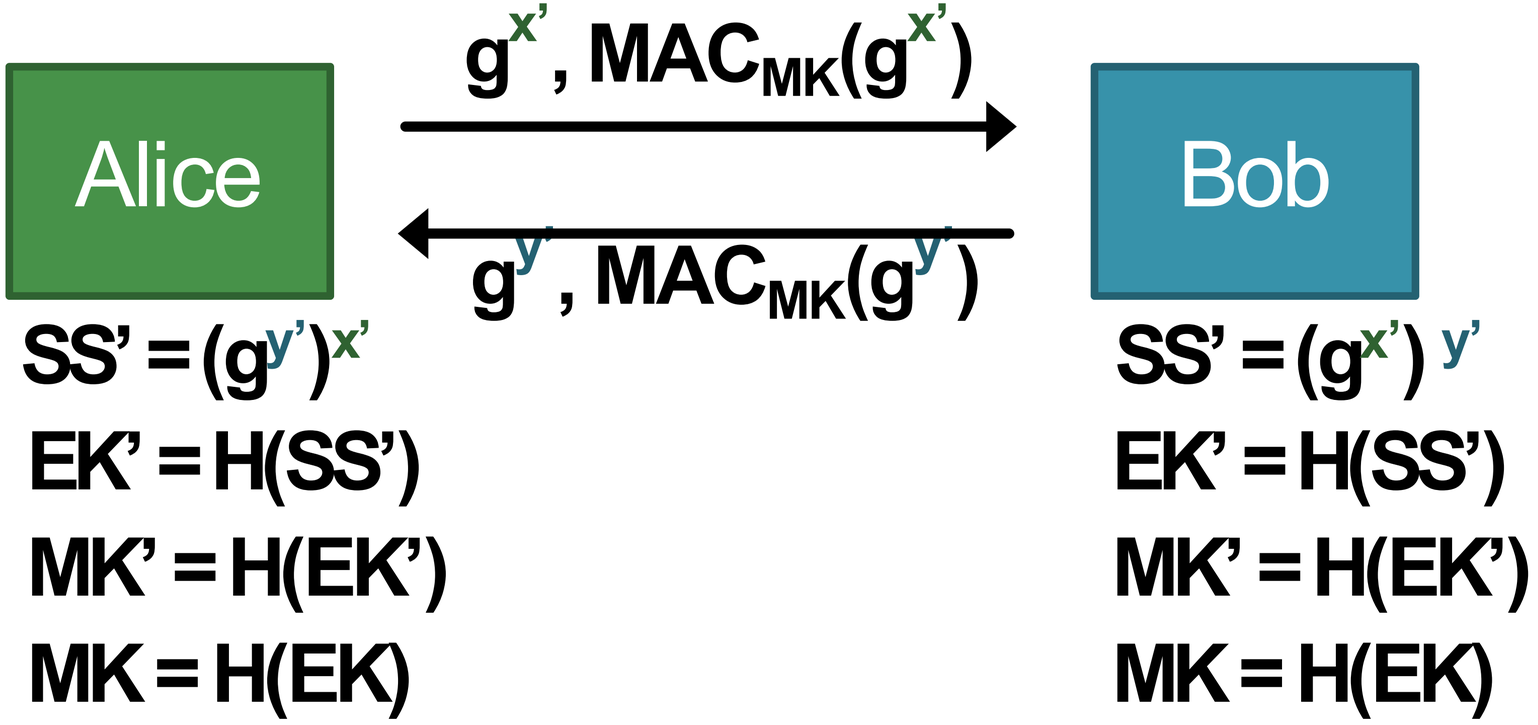
OTR: Off the Record Chat

2. Then use symmetric encryption on message M
... and authenticate using a MAC



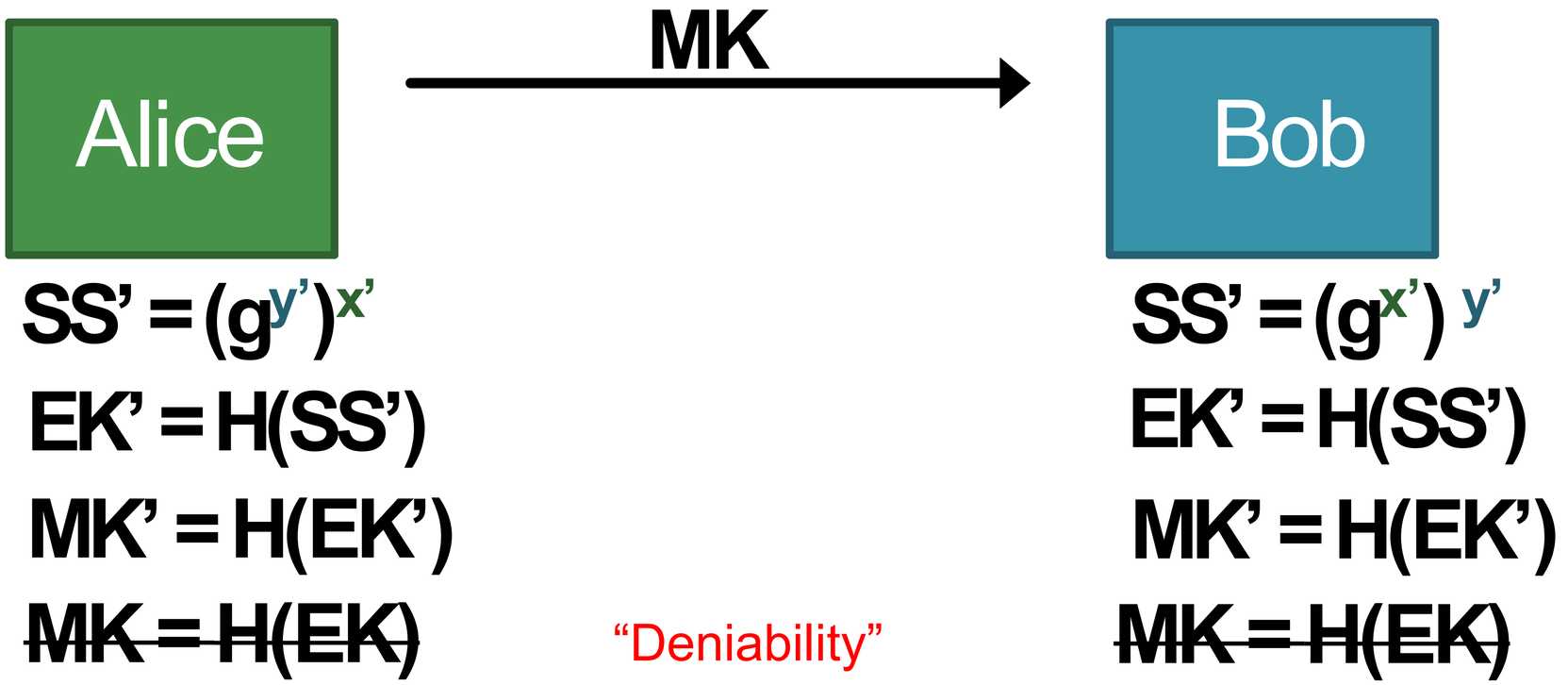
OTR: Off the Record Chat

3. Re-key using Diffie-Hellman



OTR: Off the Record Chat

4. Publish old MK



Signal/Whatsapp

Note this is suited to interactive communication, not so much email.

But, OTR provides
- message confidentiality
- authentication
- perfect forward secrecy
- deniability

OTR has since lost popularity. Signal Protocol now de facto standard.