

Network Security V

CSE 565: Fall 2024
Computer Security

Xiangyu Guo (xiangyug@buffalo.edu)

University at Buffalo

Disclaimer

- We don't claim any originality of the slides. The content is developed heavily based on
 - Slides from Prof. Dan Boneh and Prof. Zakir Durumeric's lecture on Computer Security (<https://cs155.stanford.edu/syllabus.html>)
 - Slides from Prof Nick McKeown's lecture on Computer Network (<https://vixbob.github.io/cs144-web-page/>)
 - Slides from Prof Ziming Zhao's past offering of CSE565 (<https://zzm7000.github.io/teaching/2023springcse410565/index.html>)
 - Slides from Prof Hongxin Hu's past offering of CSE565

Announcement

- HW3 and Project3 **due Tue, Nov 12, 23:59 pm.**

Review of Last Week

- DDoS Attack
 - Two major types: Amplification & Flooding
 - Defense: Rate limiting; Anycast network (IP multiplexing); Reverse Proxy.
- Network Defense
 - IPSec: securing the Network Layer. Default in IPv6
 - AH (Integrity of the whole packet) , ESP (Confidentiality & Integrity of the payload), & IKE (secure session establishment).
 - VPN: Secure tunneling protocols.
 - TLS: Securing the Transport Layer.
 - The go-to solution for implementing secure channel: HTTPS, QUIC, VPNs
- Firewall / IDS
 - Packet filtering

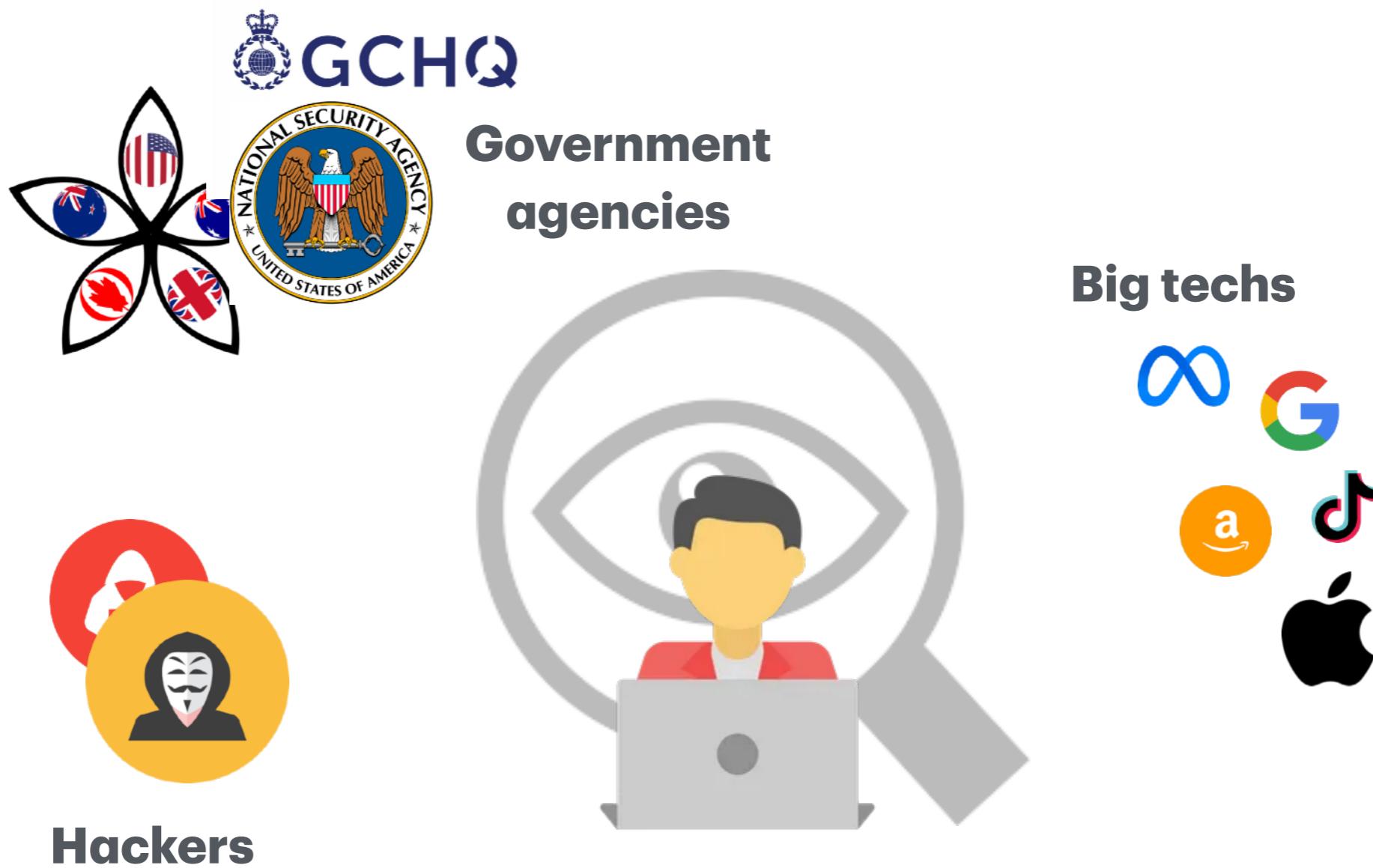
Today's topic

- Privacy in web browsing
 - Tracking and how to stop it
- Anonymity
 - Hide your identity (and/or your actions)
- Secure messaging

Privacy

(Not only) Big brother is watching you

- Individual's data are constantly being collected (legally or illegally) by all kinds of parties.



(Not only) Big brother is watching you

- Individual's data are constantly being collected (legally or illegally) by all kinds of parties.
- What for?
 - **Advertising**: primary reason why Google/Meta/Amazon ... want your data. (E.g. to train ad recommendation models)
 - **National Security** (or not?): thanks to Edward Snowden, we now know the extent of surveillance.
 - **Money**
 - There are simply too many (illegal) ways to exploit people's data

Third Party Tracking

≡ COSMOPOLITAN LOVE | CELEBS | BEAUTY & STYLE | FITNESS SEARCH

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

f SHARE 12.2K
t TWEET 46
p PIN 6

MOST READ

THE BEDROOM BLOG

Does Seafood Make Guys Horny?

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

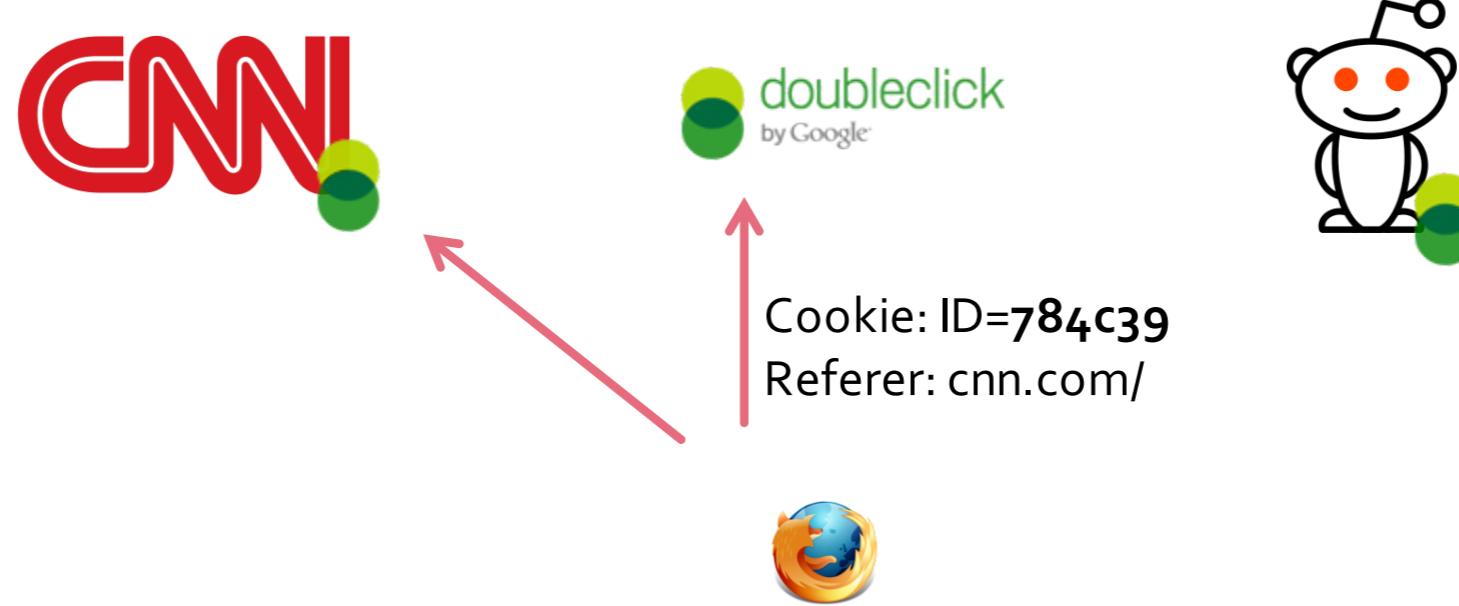


1. First of all, define "cat lady." Does one cat = cat lady? Two cats = cat lady? Does joking about being a cat lady à la sparkling, outgoing multimillionaire Taylor Swift automatically make one a cat lady? It is my personal belief that most female cat owners below the age of 40 fall into the "not a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



A **third-party cookie** is a cookie set by a website **other than the one** you are currently visiting.

Third-Party Web Tracking

Cookies and Code

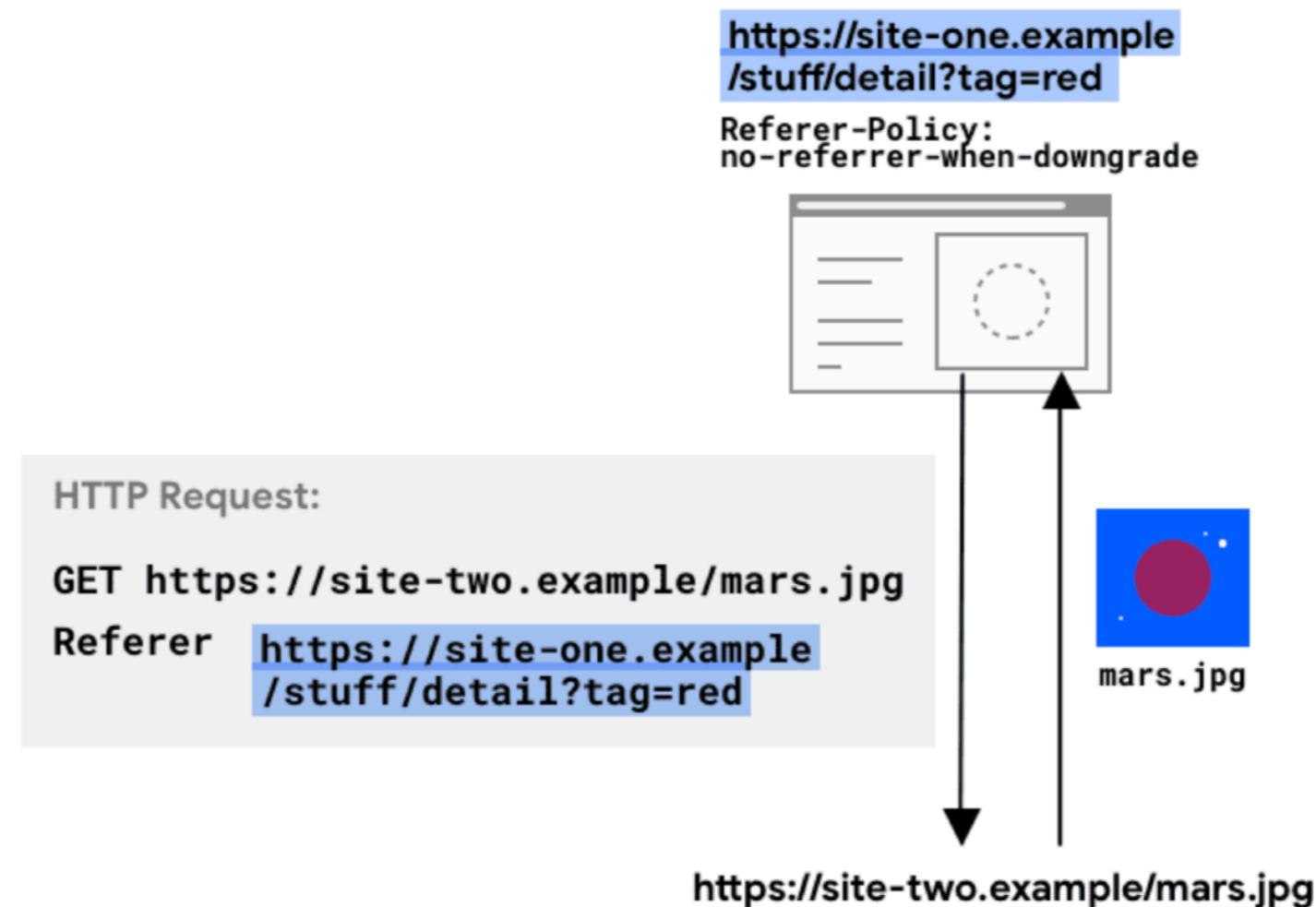


- With this request, companies can link your cookie to your browsing data (e.g., through **Referer** header, **Host** headers, **Origin**, or just **JavaScript**)

Third-Party Web Tracking

Cookies and Code

- What exactly is sent in the referer?



cnn.com

ELECTION DAY

Voters across the US will make their voices heard. Watch CNN

Live Updates: 2024 presidential election | Trending: Joe Rogan endorsement |

★ ★ ELECTION DAY

Americans head

FOR SUBSCRIBERS

It takes at least 270 electoral votes to win the presidency. Experiment with the paths to victory

cnn.com

Ghost icon

Pause on this site 1 hour

Observed activities

Advertising 6

- Nativo 1
- OneTag 1
- Google 2
- Outbrain 1
- DoubleClick 1
- Adobe Audience Manager 3

Site Analytics 4

Georgia voter: I made sure I w

CNN.COM



OBSERVED ACTIVITIES (87)

- This chart shows the total unique trackers seen on this website. Rather than an exact count per page, it shows the diversity of trackers seen over multiple visits.

Filter the list by category to view subset tracker types.

All  Advertising  Site Analytics  Consent Management  Hosting  Customer Interaction

 Audio/Video Player  Misc  Social Media

Sorted by frequency of appearance on domain subpages

- | | | | |
|---|--|---|---|
| 1. ChartBeat
87.64% · CHARTBEAT · SITE ANALYTICS | 2. OneTag
85.86% · ONETAG · ADVERTISING | 3. Optimizely
85.23% · OPTIMIZELY · SITE ANALYTICS | 4. Datadog
80.84% · DATADOG · MISC |
| 5. DoubleClick
76.98% · GOOGLE · ADVERTISING | 6. Google
71.27% · GOOGLE · ADVERTISING | 7. videoplayerhub.com
68.67% · MISC | 8. Warner Media
67.28% · AT&T · SITE ANALYTICS |
| 9. Outbrain
66.84% · OUTBRAIN · ADVERTISING | 10. Nativo
65.37% · NATIVO · ADVERTISING | 11. Amazon Advertising
63.14% · AMAZON · ADVERTISING | 12. FreeWheel
61.98% · COMCAST · ADVERTISING |
| 13. Integral Ad Science
60.16% · INTEGRAL AD SCIENCE · ADVERTISING | 14. ComScore, Inc.
60.15% · COMSCORE, INC. · SITE ANALYTICS | 15. Index Exchange
54.09% · INDEX EXCHANGE, INC. · ADVERTISING | 16. PubMatic
50.44% · PUBMATIC, INC. · ADVERTISING |
| 17. Tremor Video
50.23% · TREMOR VIDEO · AUDIO | 18. Rubicon
49.58% · THE RUBICON PROJECT · ADVERTISING | 19. AppNexus
46.21% · MICROSOFT · ADVERTISING | 20. Cloudflare
43.85% · CLOUDFLARE · HOSTING |

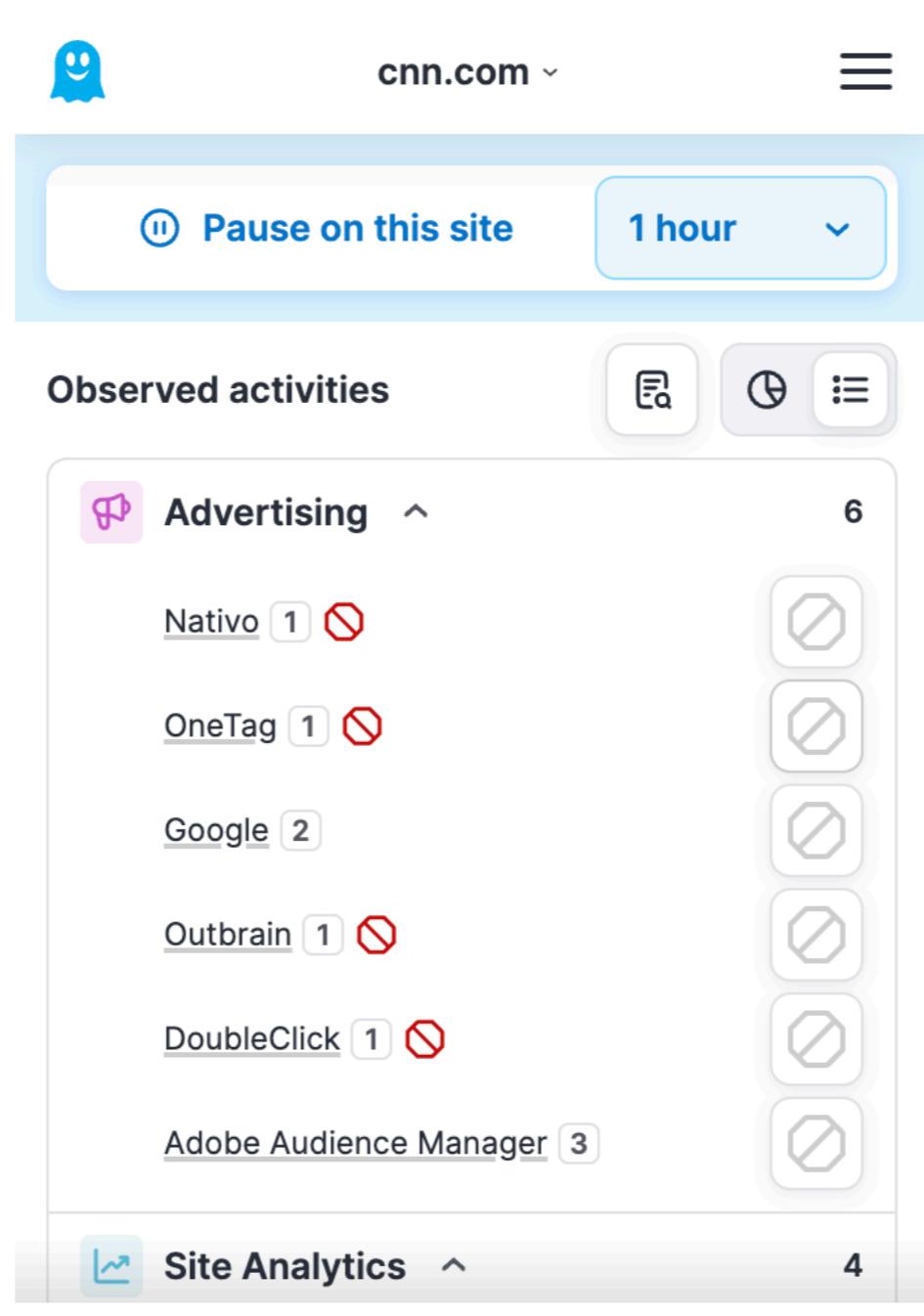
Third Party Cookies

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

Browser extension to prevent tracking



Do Not Track (DNT)

Browser settings to prevent tracking

The screenshot shows the Google Chrome settings page at `chrome://settings/cookies`. The left sidebar lists various settings categories. The 'Privacy and security' category is selected and highlighted in blue. The main content area is titled 'Manage the types of information sites can use to track you as you browse.' It contains three options:

- Allow third-party cookies
- Block third-party cookies in Incognito mode
- Block third-party cookies

The 'Block third-party cookies' option is currently selected. Below it, there are two descriptive paragraphs and a toggle switch:

- A paragraph explaining that sites can use cookies to improve the browsing experience, such as keeping users signed in or remembering items in a shopping cart.
- A paragraph explaining that sites cannot use cookies to track activity across different sites, which prevents personalized ads and ensures some site features work correctly.

Below this section, another toggle switch is shown, labeled 'Allow related sites to see your activity in the group'. A red box highlights the 'Advanced' section at the bottom right, which contains a toggle switch for sending a 'Do Not Track' request with browsing traffic. This section is described as follows:

Send a "Do Not Track" request with your browsing traffic
Sites use their discretion when responding to this request

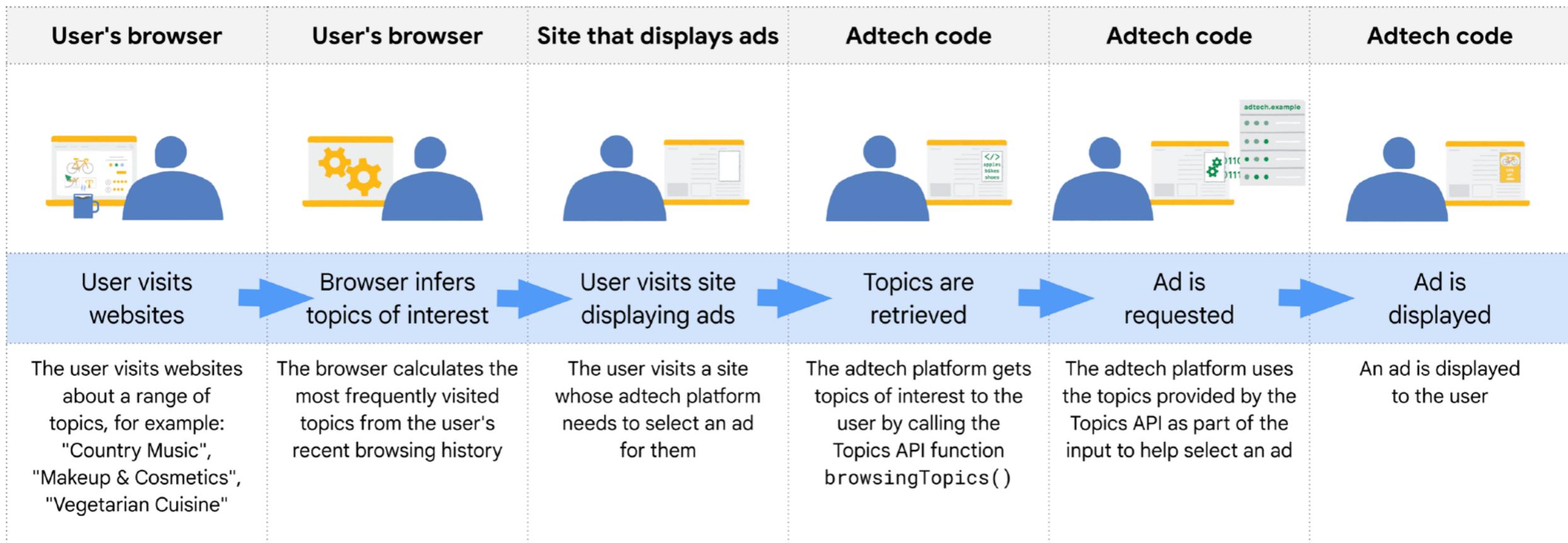
At the very bottom, a link says 'See all site data and permissions'.

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** (*anyone still use this?*): 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

Privacy-preserving Advertising



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).

Browser Fingerprinting

- Websites can also track 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",  
    "un沉没的"
```

MY BROWSER FINGERPRINT

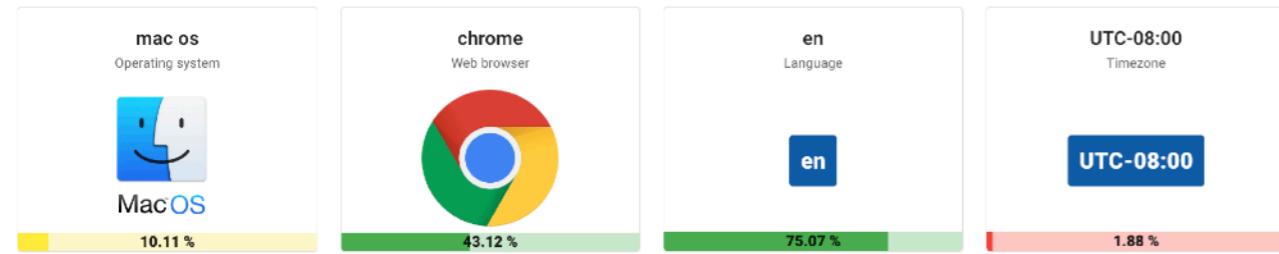
SEE YOUR BROWSER FINGERPRINT PROPERTIES

ARE YOU UNIQUE ?

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.



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

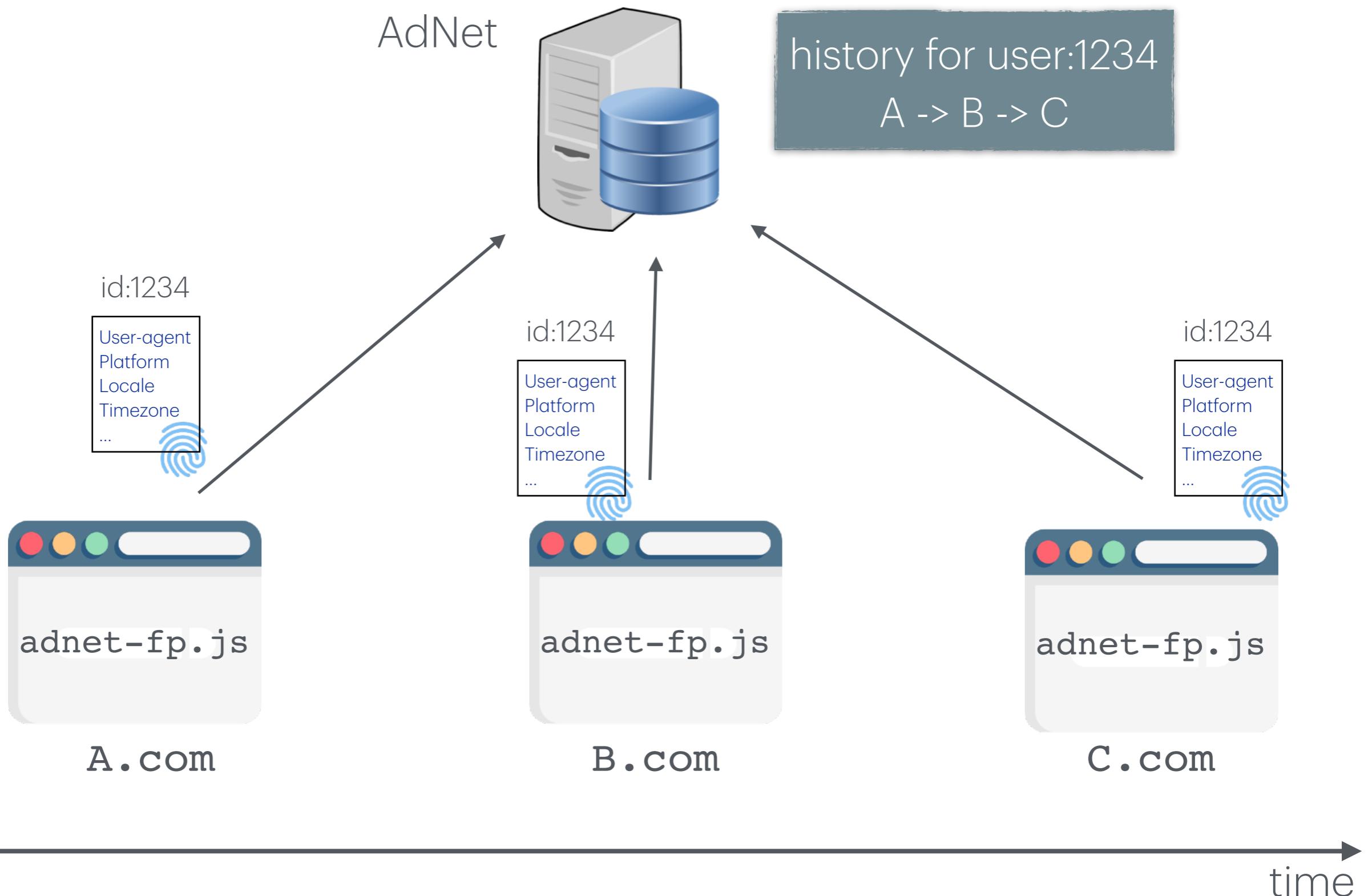
JAVASCRIPT ATTRIBUTES

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

20 - Screen width		4.25 %	2560	pdf-viewer.
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	

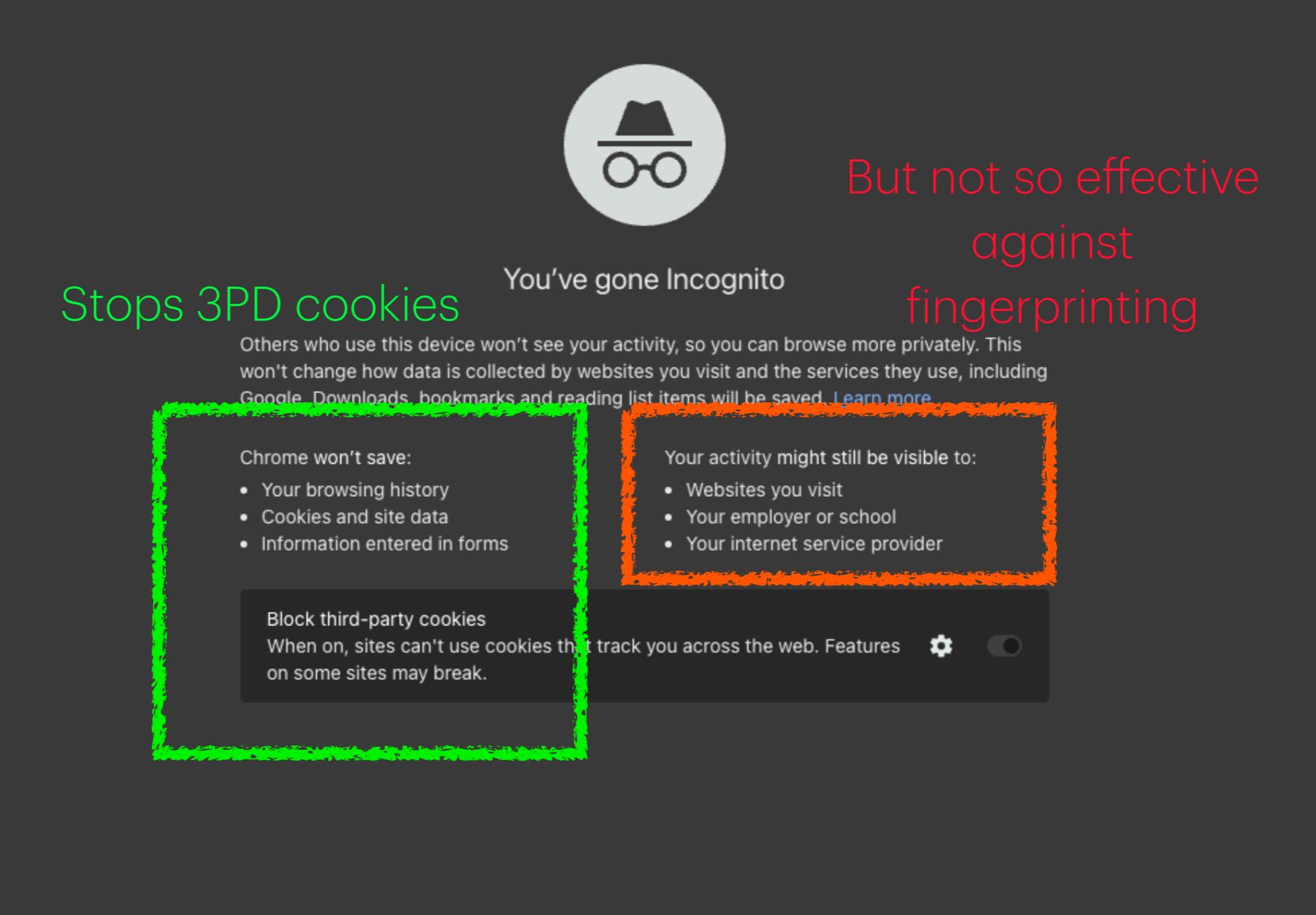
Cross-Site Fingerprinting



Fingerprinting is Hard to Block

- **No dependency on cookies:** does *not store* any data on the user's device, so [cookie-blocking tools](#) do not stop it.
- **Inherent device characteristics:** relies on information that browsers naturally provide (e.g., screen resolution and browser type), which are often needed for the website to function correctly.
- **Consistency across websites:** As long as multiple websites use the same third-party service, the fingerprint identifier will be the same, allowing seamless tracking.

Incognito?



The screenshot shows a dark-themed browser window. At the top center is a circular icon with a silhouette of a person wearing a hat and glasses. To its right, the text "You've gone Incognito" is displayed. Below this, on the left, the text "Stops 3PD cookies" is shown in green. In the center, a paragraph explains that others won't see your activity, but it notes that data collection by websites and services continues. On the right, the text "But not so effective against fingerprinting" is written in red. Two sections are highlighted with hand-drawn style outlines: one in green on the left listing what Chrome won't save (browsing history, cookies, form info), and one in orange on the right listing what might still be visible (websites visited, employer/school, ISP). A "Block third-party cookies" button is at the bottom, with a note that some site features might break if it's turned on. A gear icon and a toggle switch are also present.

Stops 3PD cookies

You've gone Incognito

But not so effective
against
fingerprinting

Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites you visit and the services they use, including Google, Downloads, bookmarks and reading list items will be saved. [Learn more](#)

Chrome won't save:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies

When on, sites can't use cookies that track you across the web. Features on some sites may break.

⚙️

My Fingerprint- Am I Unique? amiunique.org/fingerprint

AM I UNIQUE? MY FINGERPRINT MY EXTENSION GLOBAL STATISTICS SURVEY BLOG USEFUL LINKS LANGUAGE

MY BROWSER FINGERPRINT

SEE YOUR BROWSER FINGERPRINT PROPERTIES

ARE YOU UNIQUE ?

TODAY 7 DAYS 15 DAYS 30 DAYS 90 DAYS ALL TIME

Yes! You are unique among the 2974298 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 Operating system
MacOS 10.70 %

Incognito (3)

AM I UNIQUE? MY FINGERPRINT MY EXTENSION GLOBAL STATISTICS SURVEY BLOG USEFUL LINKS LANGUAGE

MY BROWSER FINGERPRINT

SEE YOUR BROWSER FINGERPRINT PROPERTIES

ARE YOU UNIQUE ?

TODAY 7 DAYS 15 DAYS 30 DAYS 90 DAYS ALL TIME

Yes! You are unique among the 2975612 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 Operating system
MacOS 10.70 %

chrome Web browser
44.08 %

en Language
73.59 %

UTC-05:00 Timezone
UTC-05:00 5.61 %

Evading fingerprinting

- **VPN**: only hide your IP, but *not* browser fingerprints
- **Privacy-enhanced Browsers**
 - [Tor Browser](#) (next section): Hide IP & obfuscate browser attribute
 - Firefox, Brave Browser
- **Browser extensions**: uBlock Origin, NoScript, Privacy Badger
- **Privacy-enhanced OS**: Tails OS
 - Not for everyday use.

Other reasons for privacy?

- Tracked by ad companies: annoying but does not seem to be much harmful ([really?](#))
- Monitored by government:
 - *"I'm just a nobody / I'm not a criminal. What bad could the government do with my data?"*
 - Governments are not always doing good.
- ... but there are more reasons for not being tracked

What if banks know you searched for this?

The screenshot shows the official website of the United States Courts. At the top, there's a navigation bar with links for Email Updates, Federal Court Finder, Careers, News, Listen to this page, and a search bar for uscourts.gov. Below the header is a main menu with categories like About Federal Courts, Judges & Judgeships, Services & Forms, Court Records, Statistics & Reports, and Rules & Policies. On the left, a sidebar titled 'Services & Forms' lists links for Bankruptcy Basics, Filing Without an Attorney, Credit Counseling and Debtor Education, Trustees and Administrators, and Approved Bankruptcy Notice Providers. It also includes social media sharing icons for Facebook, Twitter, Google+, LinkedIn, and Pinterest. The main content area features a large heading 'Bankruptcy' and a descriptive paragraph explaining what bankruptcy is. Below this is a section titled 'About Bankruptcy' with information about filing bankruptcy and different types of cases. A bulleted list at the bottom details specific chapters: Chapter 7, Chapter 13, and Chapter 9. To the right, a 'Related Links' sidebar lists various resources such as Bankruptcy Fees, Forms, Chapter 7 Fee Waiver Procedures, Protection of Tax Information Guidance, Pending Bankruptcy Forms, and Permitted Changes to Official Forms. At the bottom right is a 'Federal Court Finder' box with fields for Location and Court Name, and a large input field for an address.

UNITED STATES COURTS

Email Updates Federal Court Finder Careers News Listen to this page Search uscourts.gov

Home About Federal Courts Judges & Judgeships Services & Forms Court Records Statistics & Reports Rules & Policies

Services & Forms

★ Bankruptcy

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

Share This Page

f
t
g+
in
p

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.

Businesses may file bankruptcy under [Chapter 7](#) to liquidate or [Chapter 11](#) 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

Federal Court Finder

Location Court Name

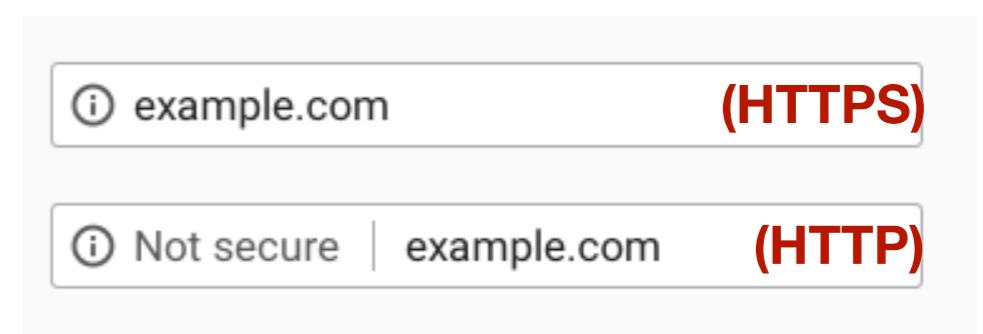
Address, city, state, or ZIP

Privacy Enhancing Technologies

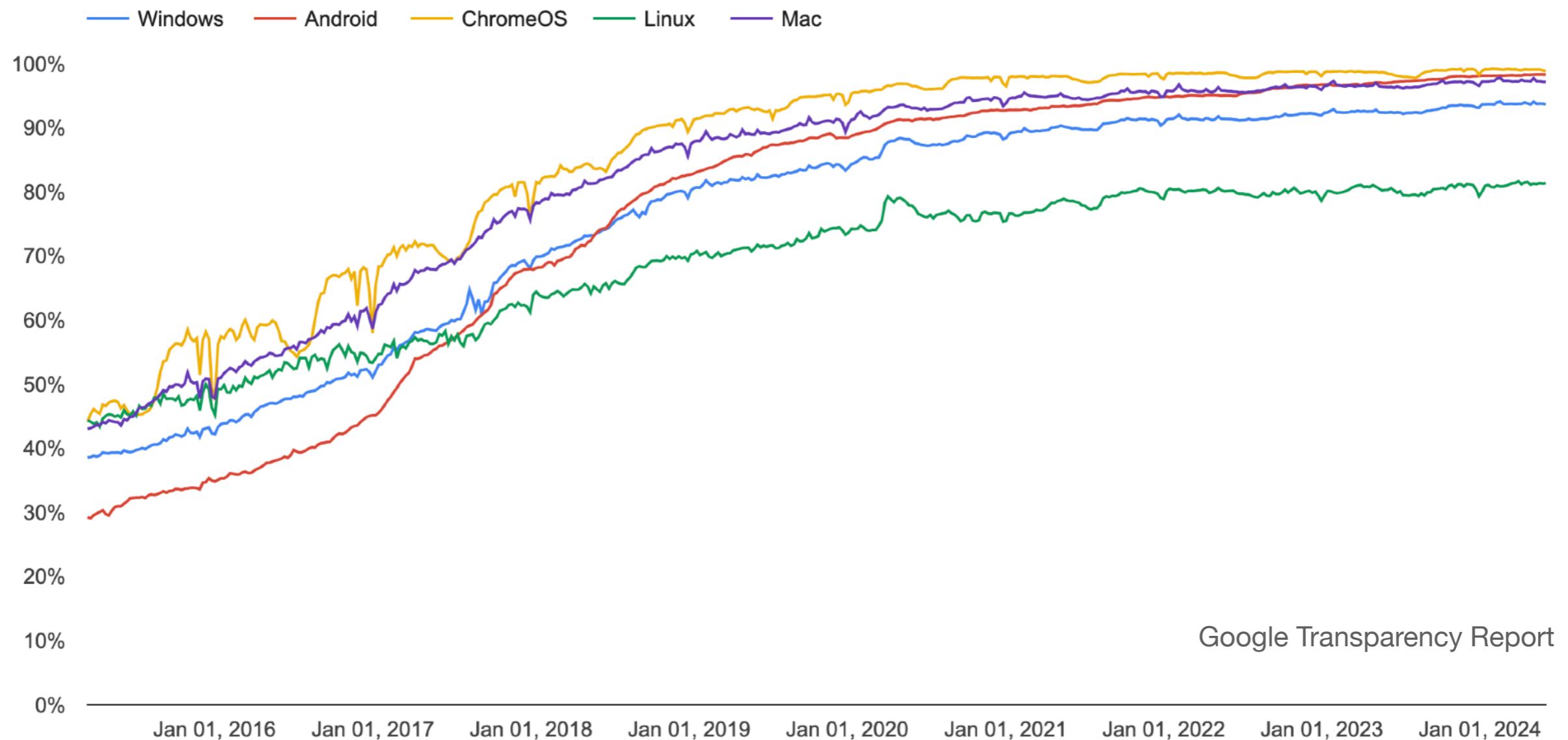
- Methods for protecting personal data
- Most Common/Successful? **TLS**.
- Comes with browser. Also used for protecting email. **It just works, without you having to configure anything.**
 - Protects contents of communication from passive eavesdroppers and active **MITM** attacks.
 - Tools that provide confidentiality also provide some privacy. You probably don't want your landlord or coffee shop customers to learn things about you.

Encouraging HTTPS Adoption

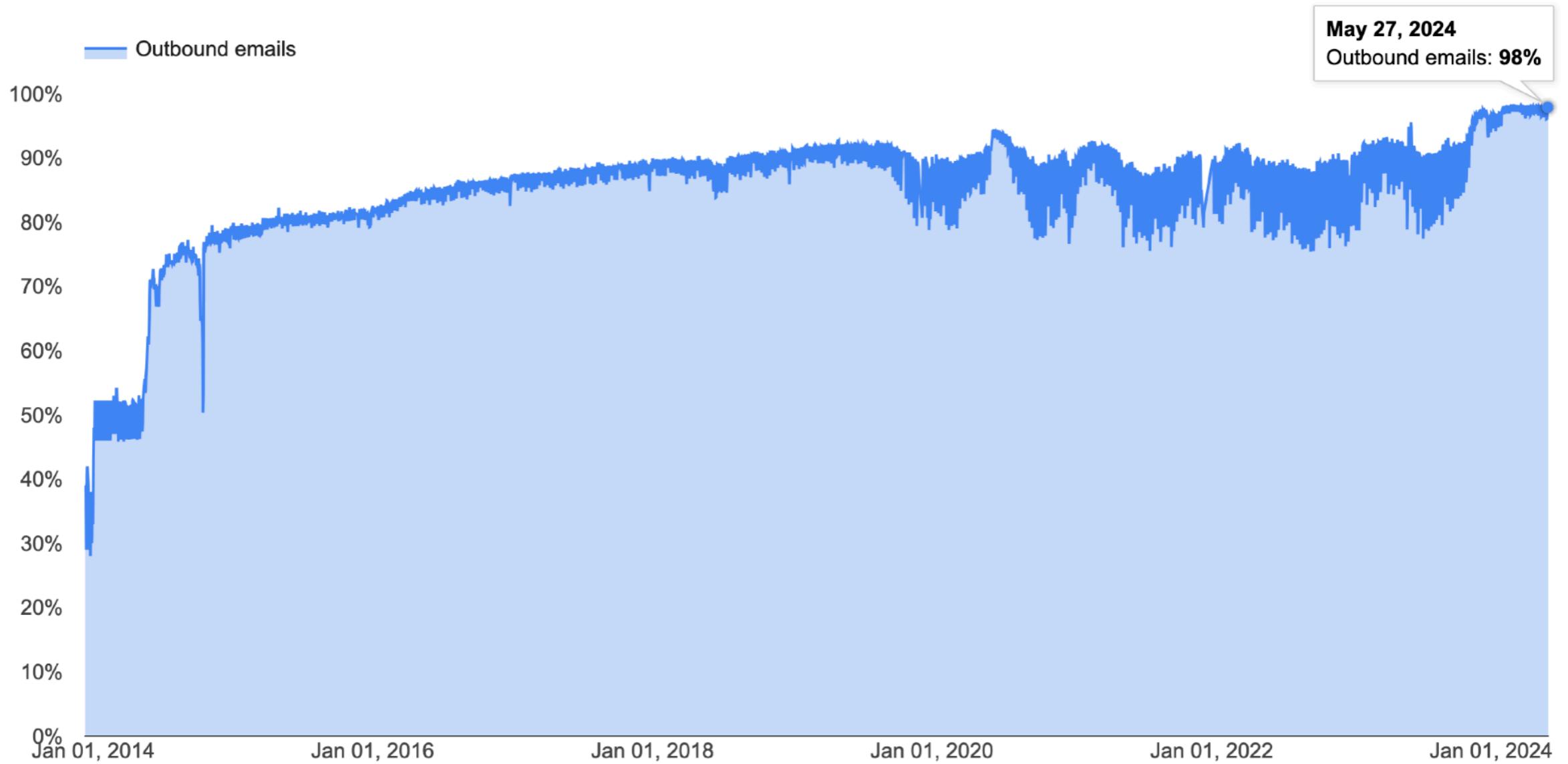
- **2014:** HTTPS used as a page rank indicator
- **Early 2018:** Mozilla announces that new features will require HTTPS
- **Late 2018:** New Chrome HTTPS indicators



Chrome Page Loads over HTTPS



STARTTLS 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)

Anonymity

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 ISPs 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.
- The hacking of 77 law enforcement sheriff websites.

It first came to our attention when leaked IRC chat logs were [released](#), in these logs participants discussed about various VPN services they use, and it became apparent that some members were using our service. No action was taken, after all there was no evidence to suggest wrongdoing and nothing to identify which accounts with us they were using. At a later date it came as no surprise to have received a court order asking for

Naive approach VPNs



Home | Pro VPN | Web proxy | Proxy list |

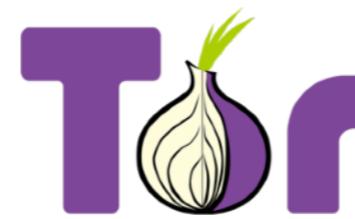
Lulzsec fiasco
Posted on September 23, 2011

We have received concerns by u
hacktivist group 'lulzsec'. Lulzsec
such as:

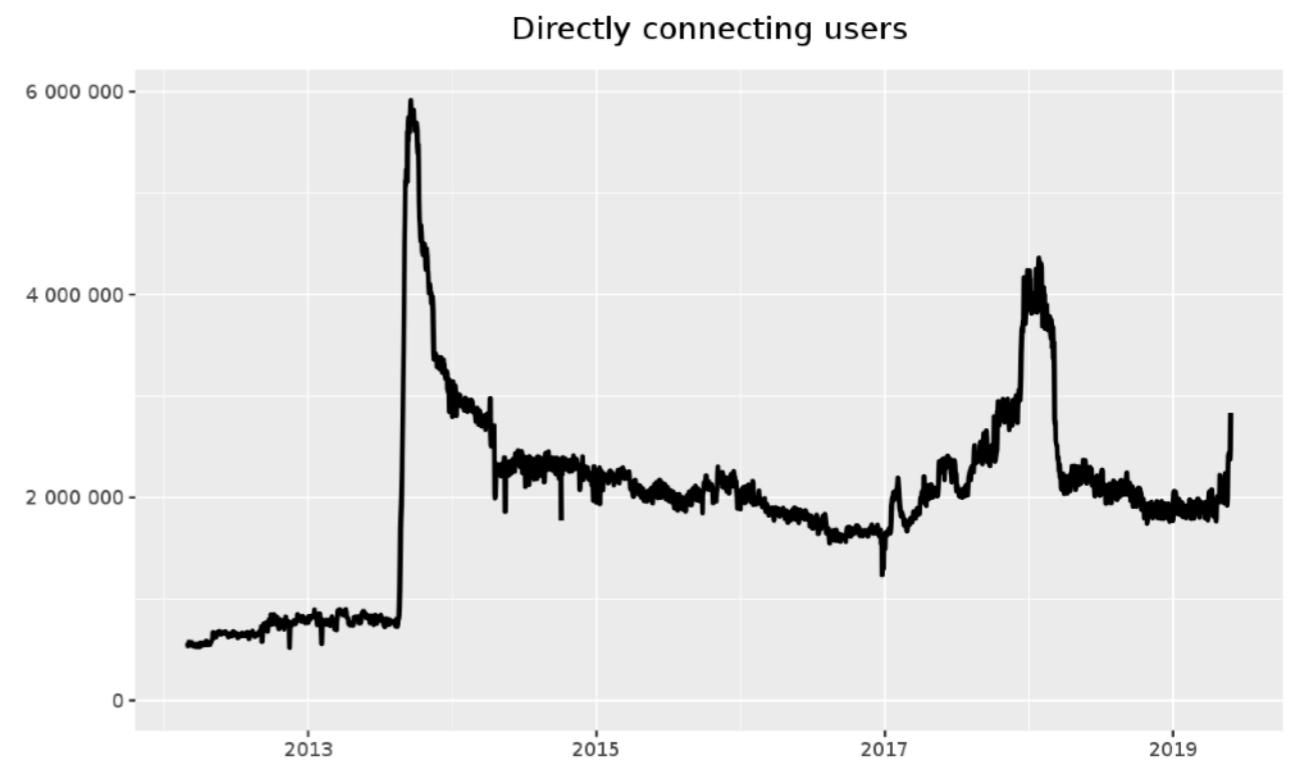
“...received a **court order** asking for information
relating to an account associated with some or
all of the above cases. As stated in our terms of
service and **privacy policy** our service is not to
be used for illegal activity, and as a legitimate
company **we will cooperate with law
enforcement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

- 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.
- The hacking of 77 law enforcement sheriff websites.

It first came to our attention when leaked IRC chat logs were [released](#), in these logs participants discussed about various VPN services they use, and it became apparent that some members were using our service. No action was taken, after all there was no evidence to suggest wrongdoing and nothing to identify which accounts with us they were using. At a later date it came as no surprise to have received a court order asking for

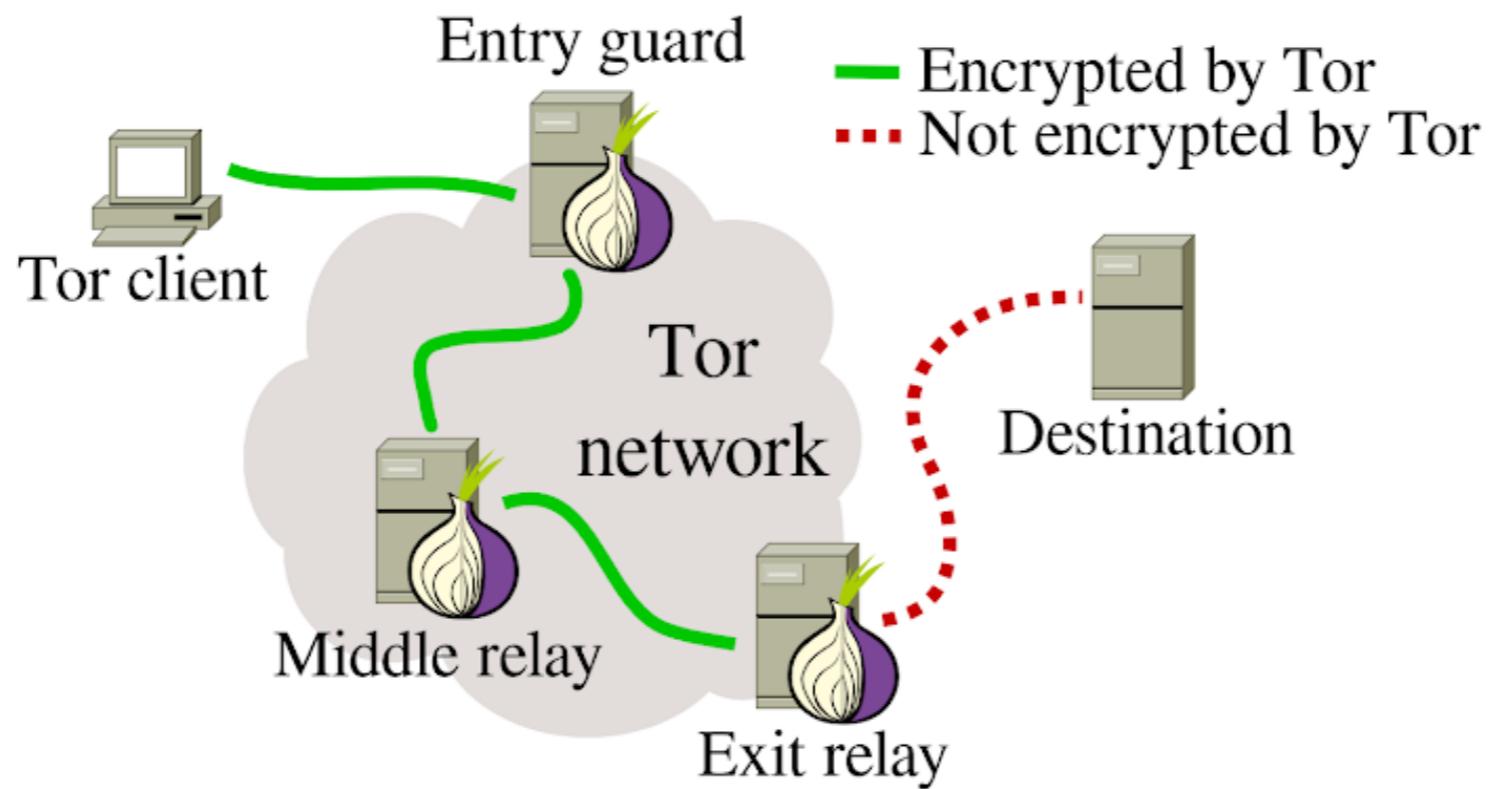


- Tor is a successful privacy enhancing technology that works at the transport layer
- Millions of active users.
- Normally, a TCP connection reveals your IP address
- Tor allows TCP connections without revealing your IP



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

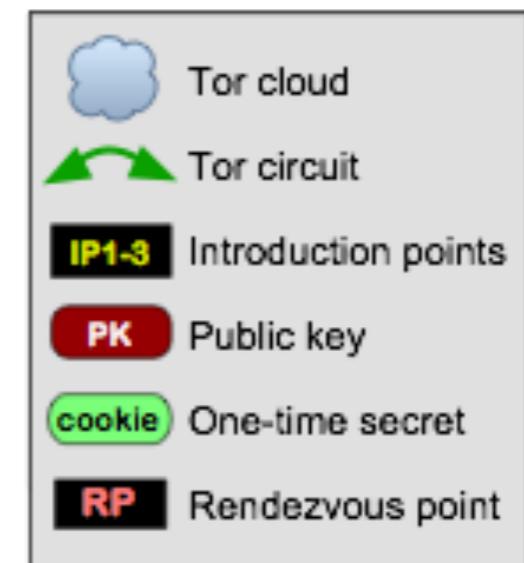
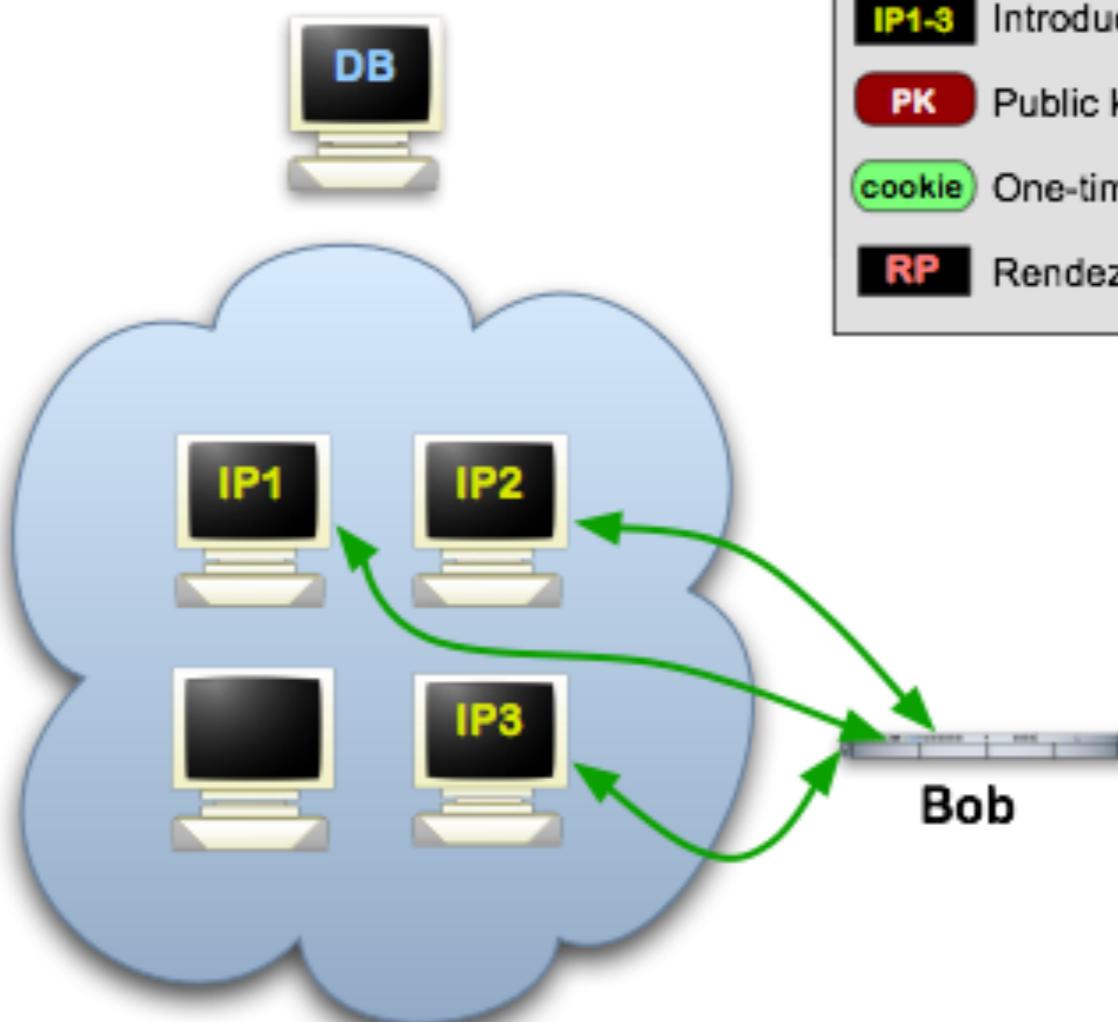
- Relays must *self-elect* to be exit nodes. Why?
 - Legal problems
 - If someone does something malicious or illegal using Tor and the police trace the traffic, [the trace leads to the exit node](#)

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

Tor Hidden Services: 1

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

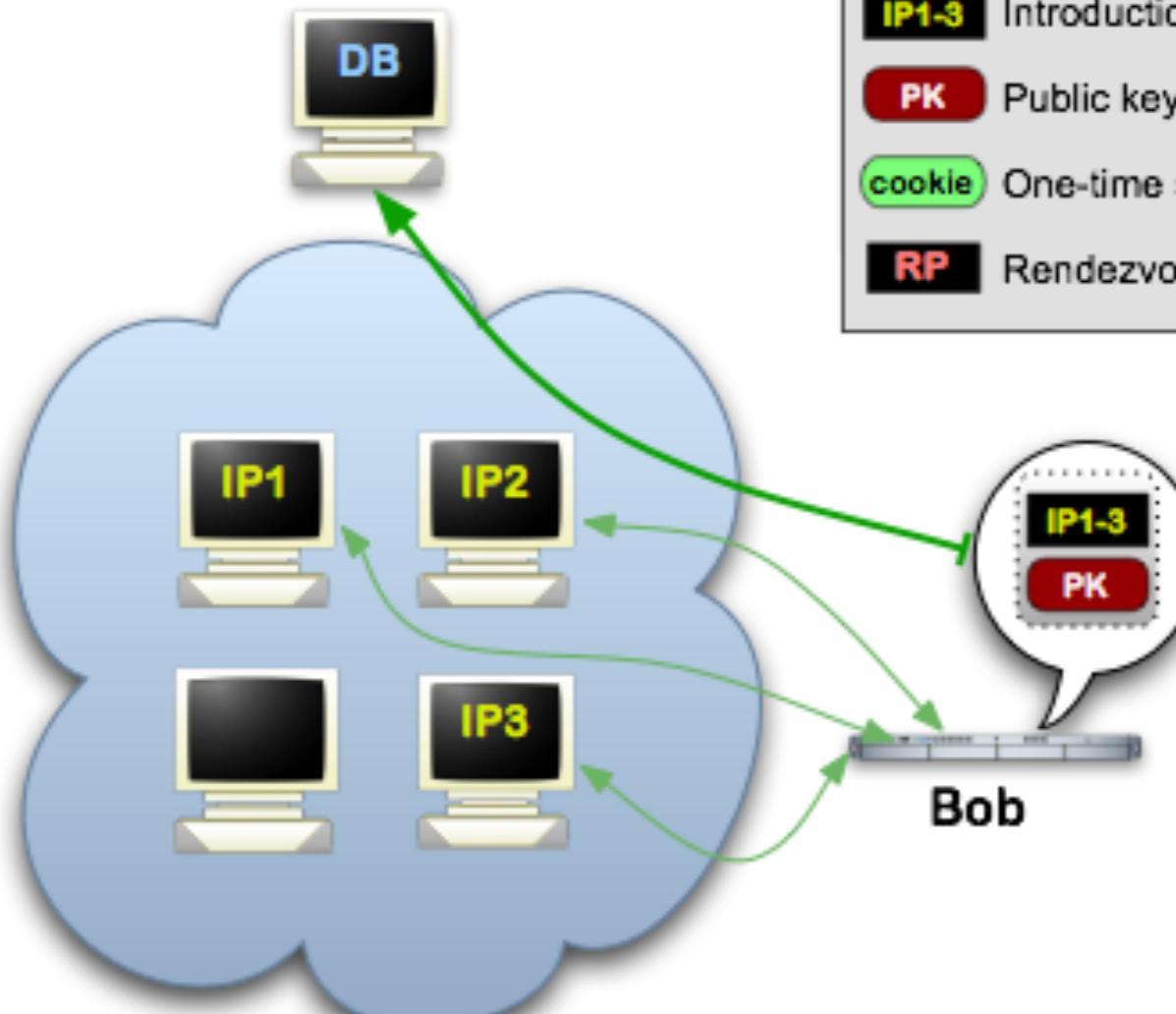


Tor Hidden Services: 2

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

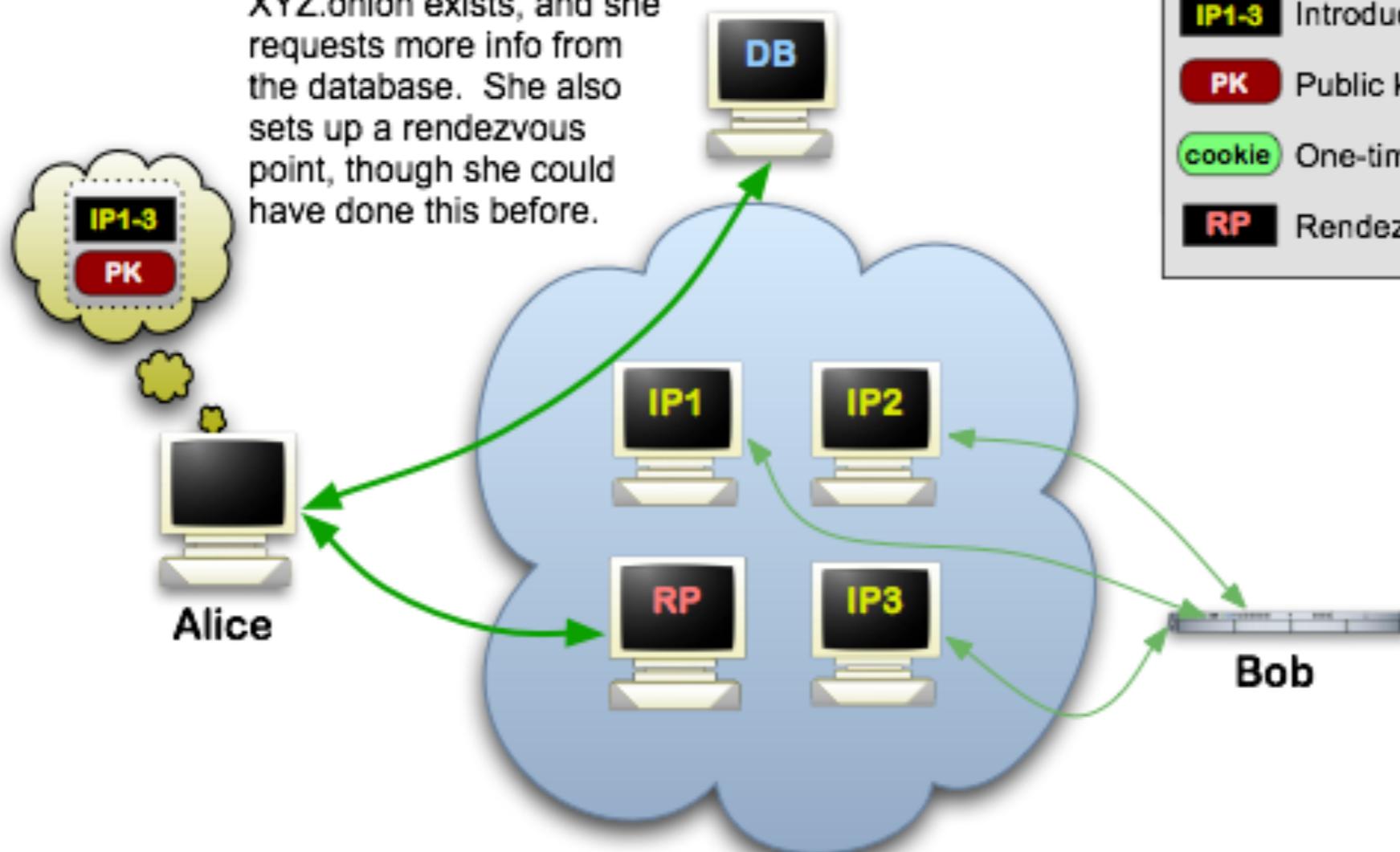


Alice



Tor Hidden Services: 3

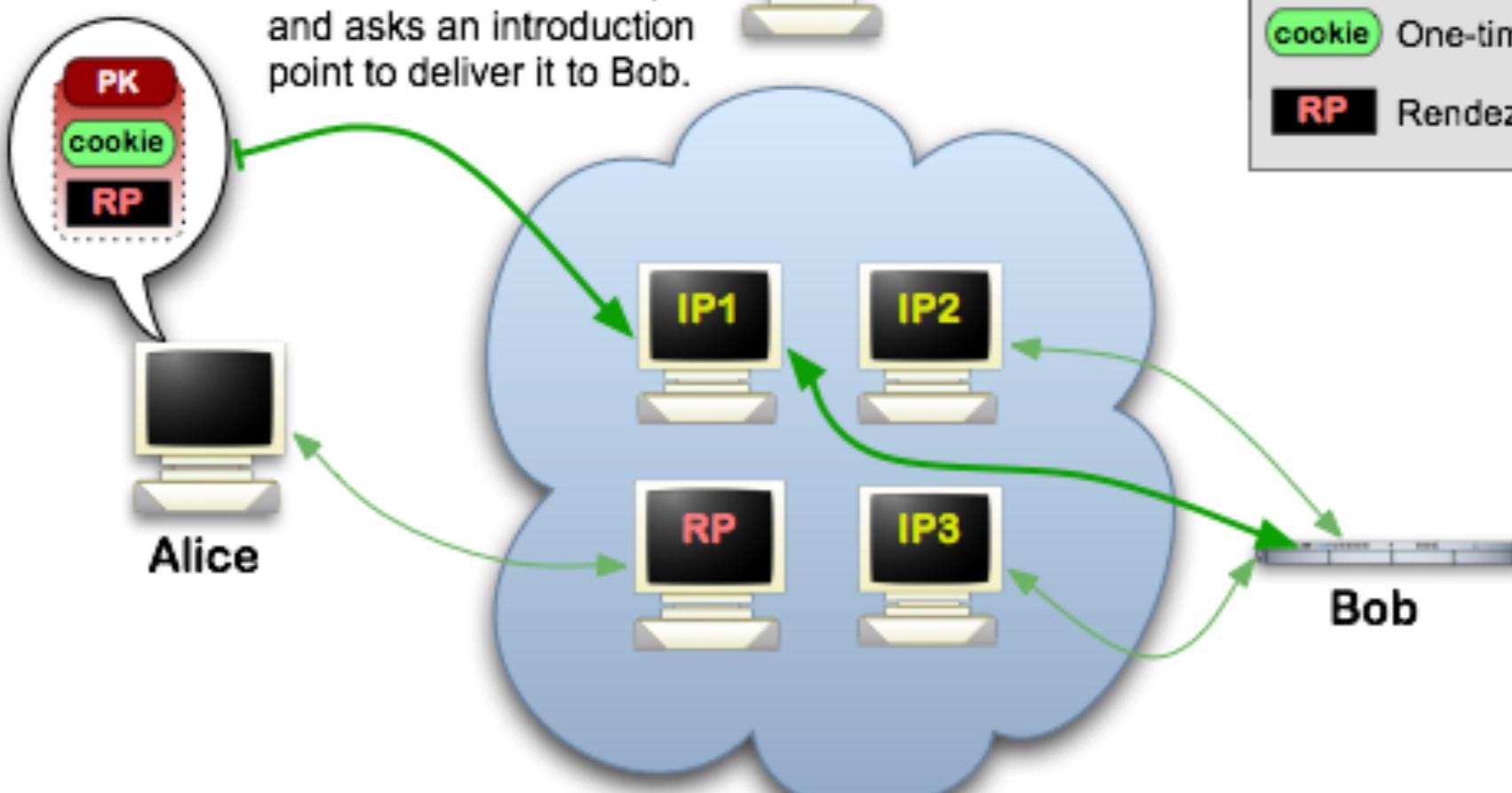
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



	Tor cloud
	Tor circuit
	Introduction points
	Public key
	One-time secret
	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.

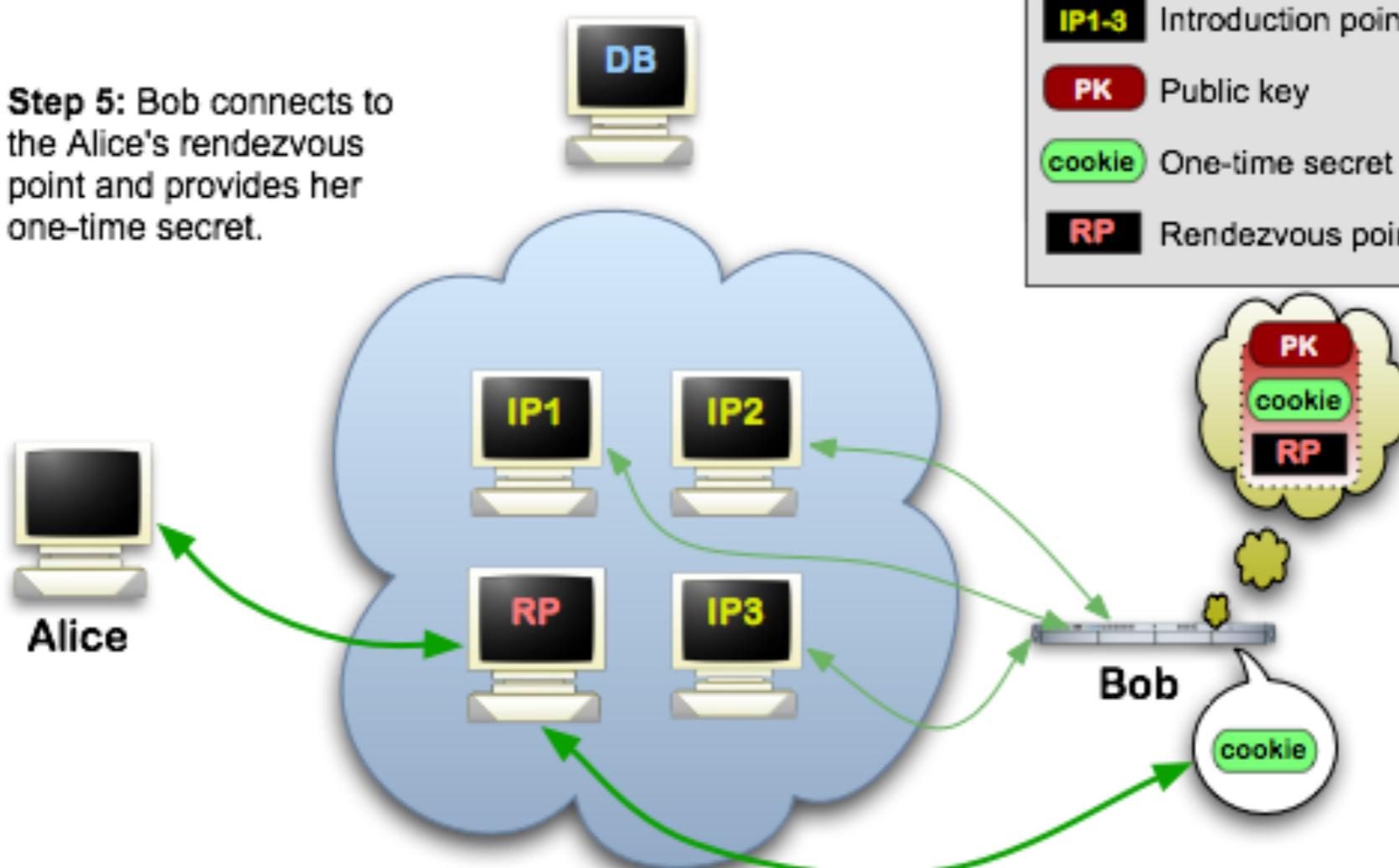


Tor Hidden Services: 5

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



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

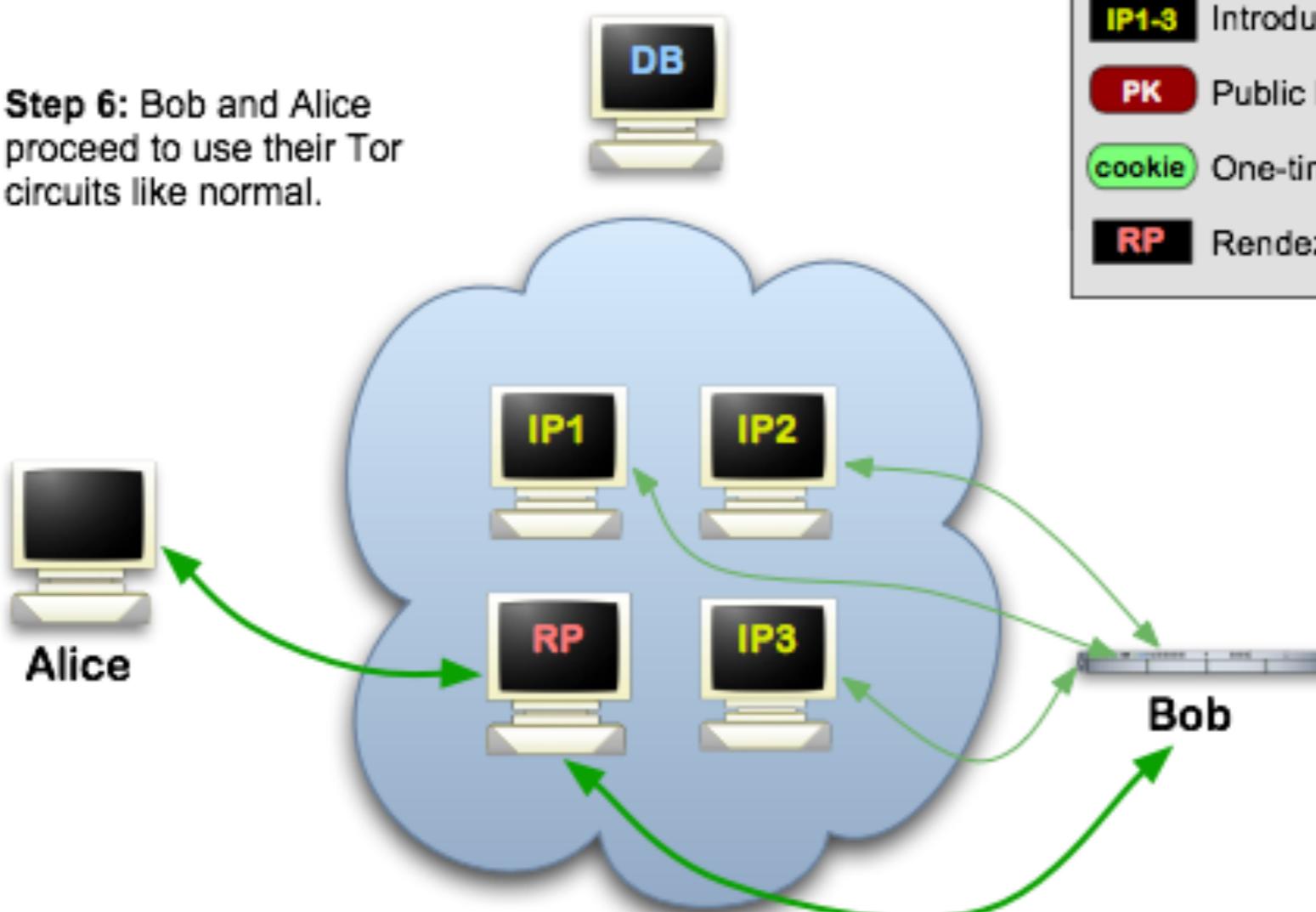


Tor Hidden Services: 6

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

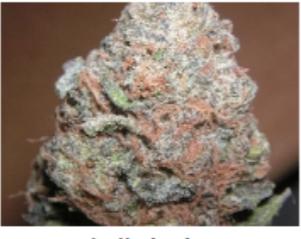


	Tor cloud
	Tor circuit
	Introduction points
	Public key
	One-time secret
	Rendezvous point



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

recent feedback:

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**

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

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

The screenshot shows the homepage of the Tor Bridges website. The header features the Tor logo (a white onion icon) and the word "Tor" in a stylized font. To the right of the logo are buttons for "Donate Now" (yellow), "About", "Support", "Community", "Blog", "Donate", and a "Download Tor Browser" button with a downward arrow. Below the header, the word "Bridges" is centered. The main title "Get Bridges for Tor" is displayed in large, white, sans-serif font. At the bottom left of the main content area, there is a link "BridgeDB / Bridge Info".

Here are your bridge lines:

```
obfs4 98.16.155.208:7001 9E48072D43FFD90D53665C08E68A2FEBEC4F8856  
obfs4 83.219.181.35:9443 E7A080574A671C6346322CEC8AE278B1F1CED7F1
```

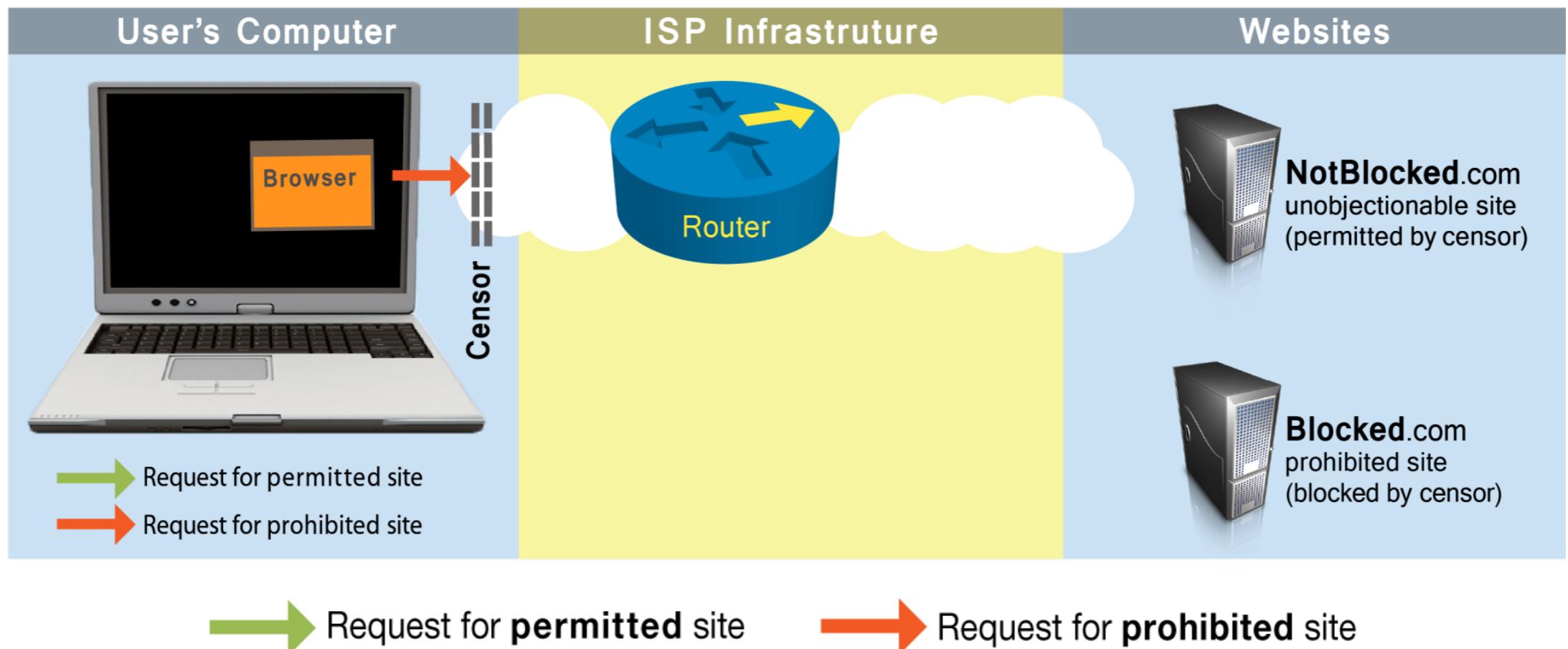
Copy All



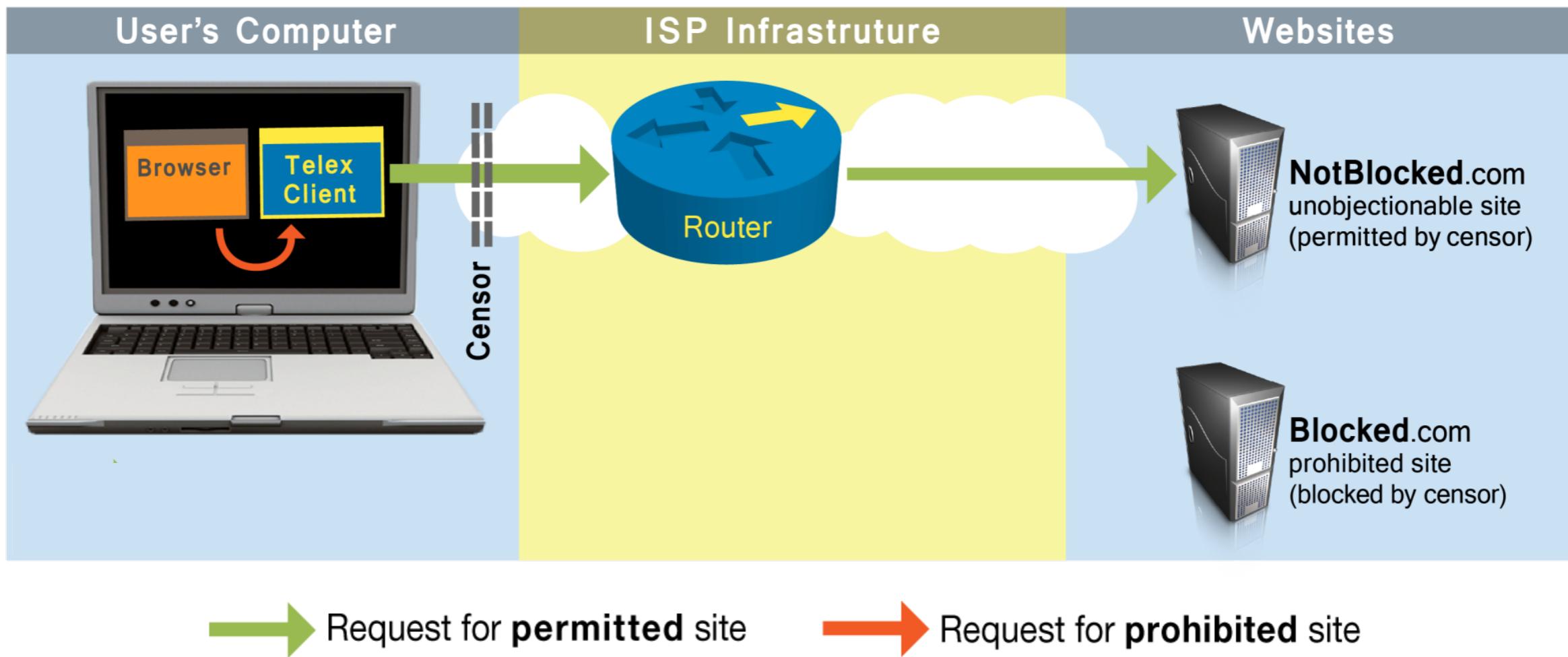
Obfuscating Tor Traffic

- 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.

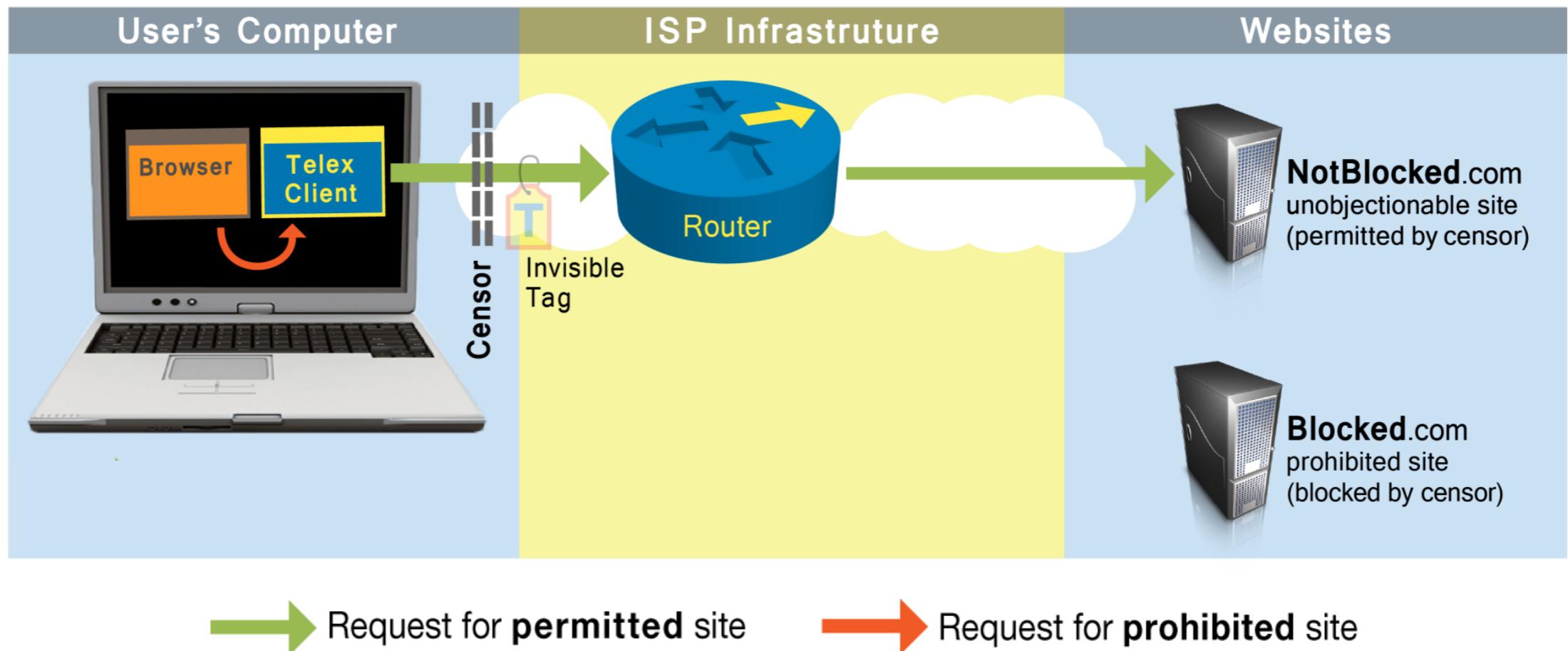
Decoy Routing (Telex)



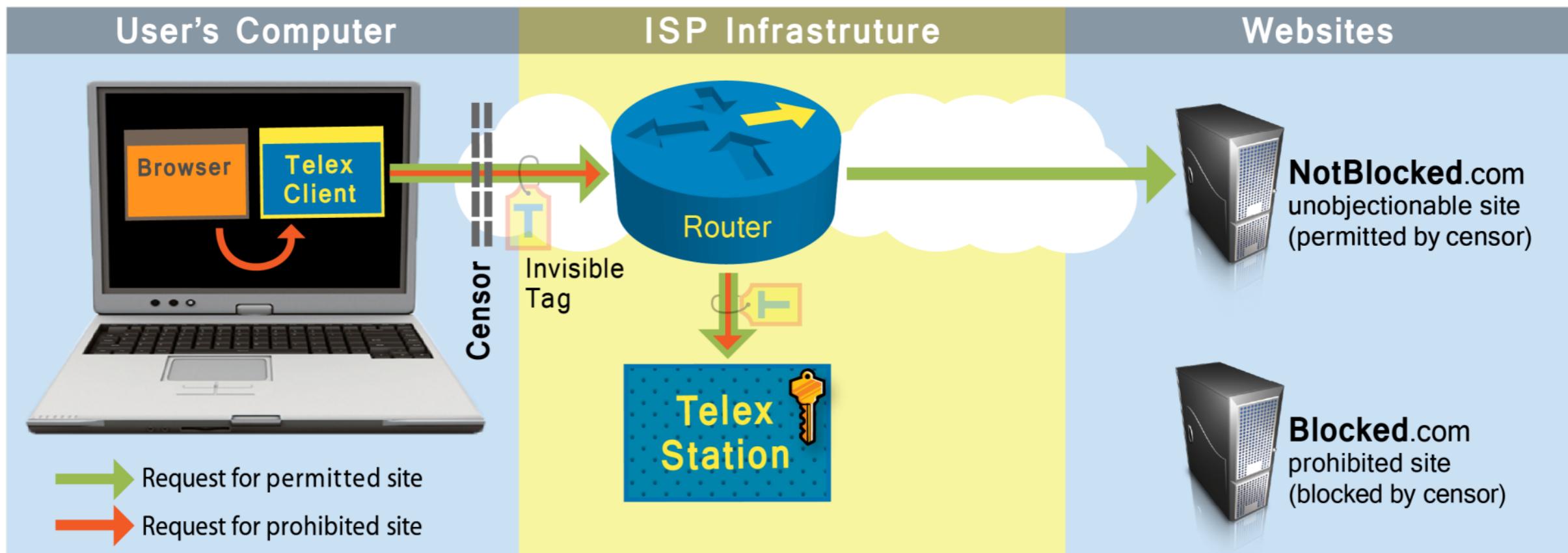
Decoy Routing (Telex)



Decoy Routing (Telex)



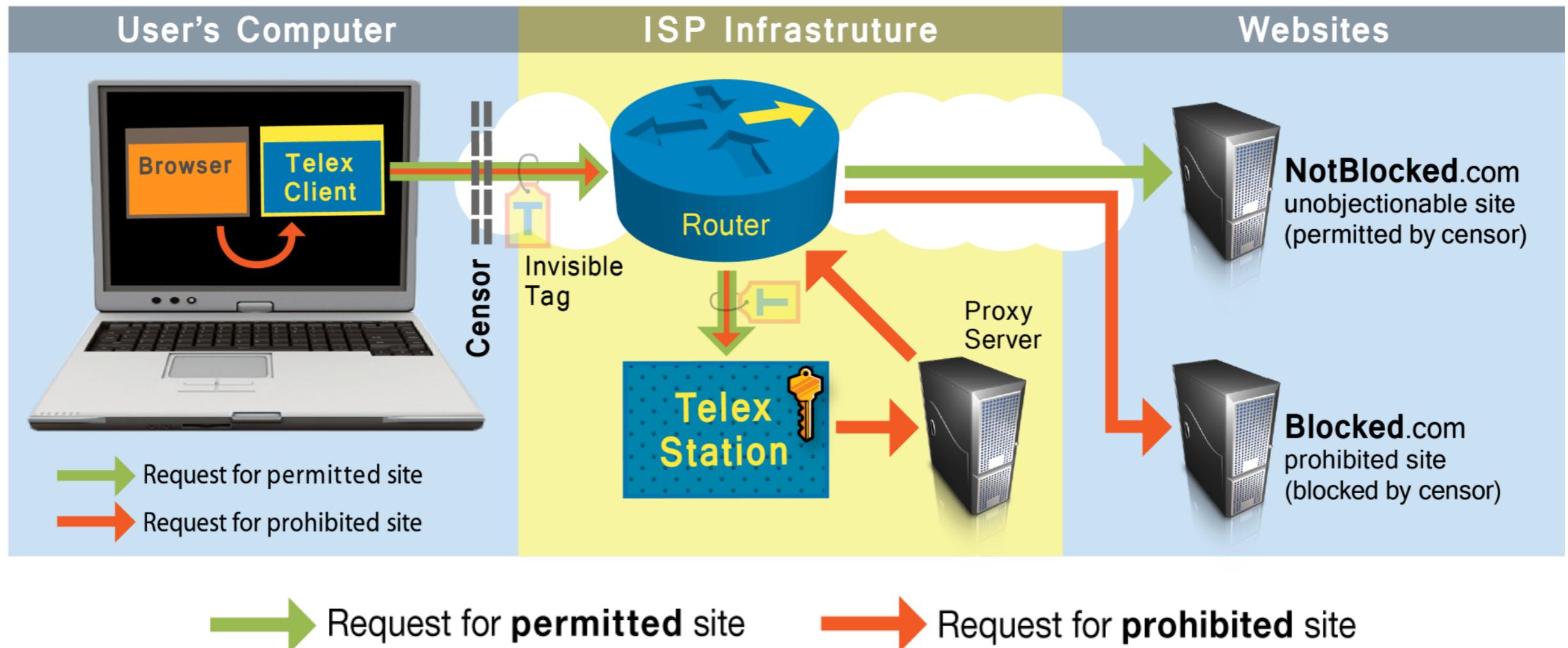
Decoy Routing (Telex)



→ Request for **permitted** site

→ Request for **prohibited** site

Decoy Routing (Telex)



Secure Messaging

Secure Messaging

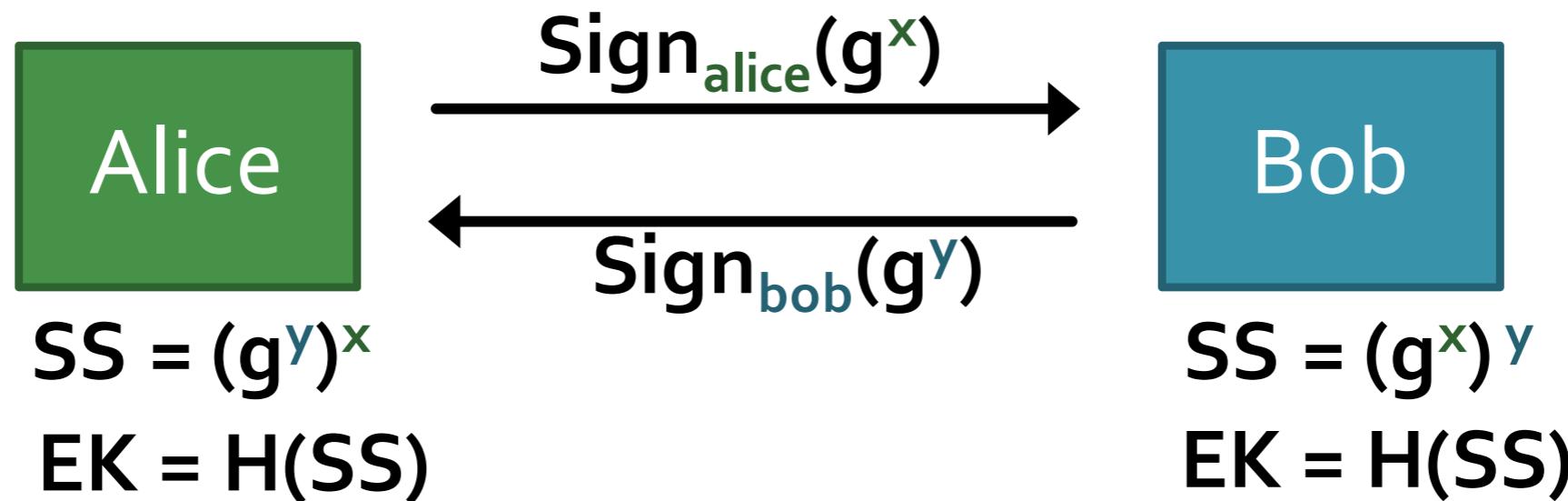
- Most communications today are through some (instant) messaging apps.
- Unique challenges:
 - Chats are highly sensitive, containing lots of personal info.
 - Authenticated (between the two) but Deniable (to any third party)
 - Chats are sporadic in short-term, but can persist in long-term.
 - Forward-secrecy and post-compromise security?
 - Need to establish a secure channel even when the receiver is offline.
 - You really want End-to-End encryption: no one (even the service provider) other than the sender & receiver should be able to read a message.

Deniability

- **Def:** Even if a communication is intercepted or recovered, neither the sender nor the recipient can prove (or be forced to prove) that they sent or received the message
- Opposite to the **non-repudiability** provided by digital signatures
- Crucial for privacy & anonymity
 - Similar to secret verbal conversation
 - Reduce the value of compromised communications
 - Prevents (out-of-context) **misuse** of messages

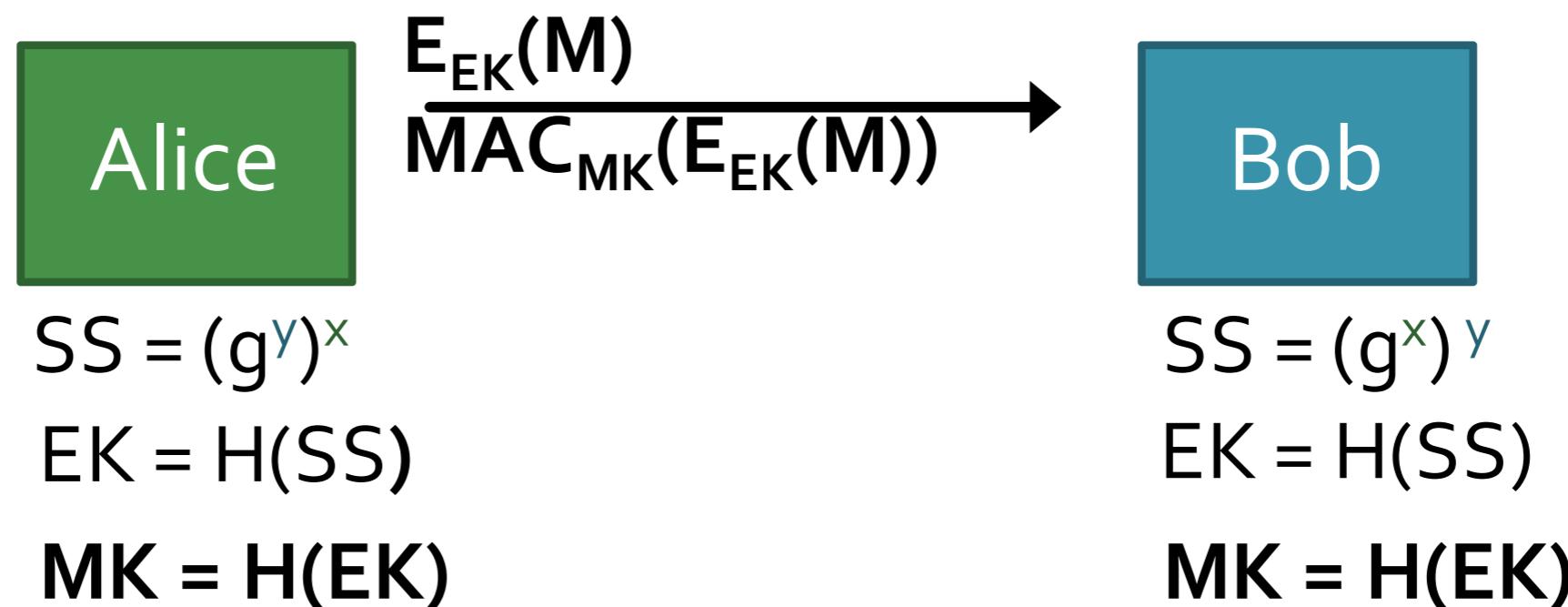
OTR: Off the Record Chat

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



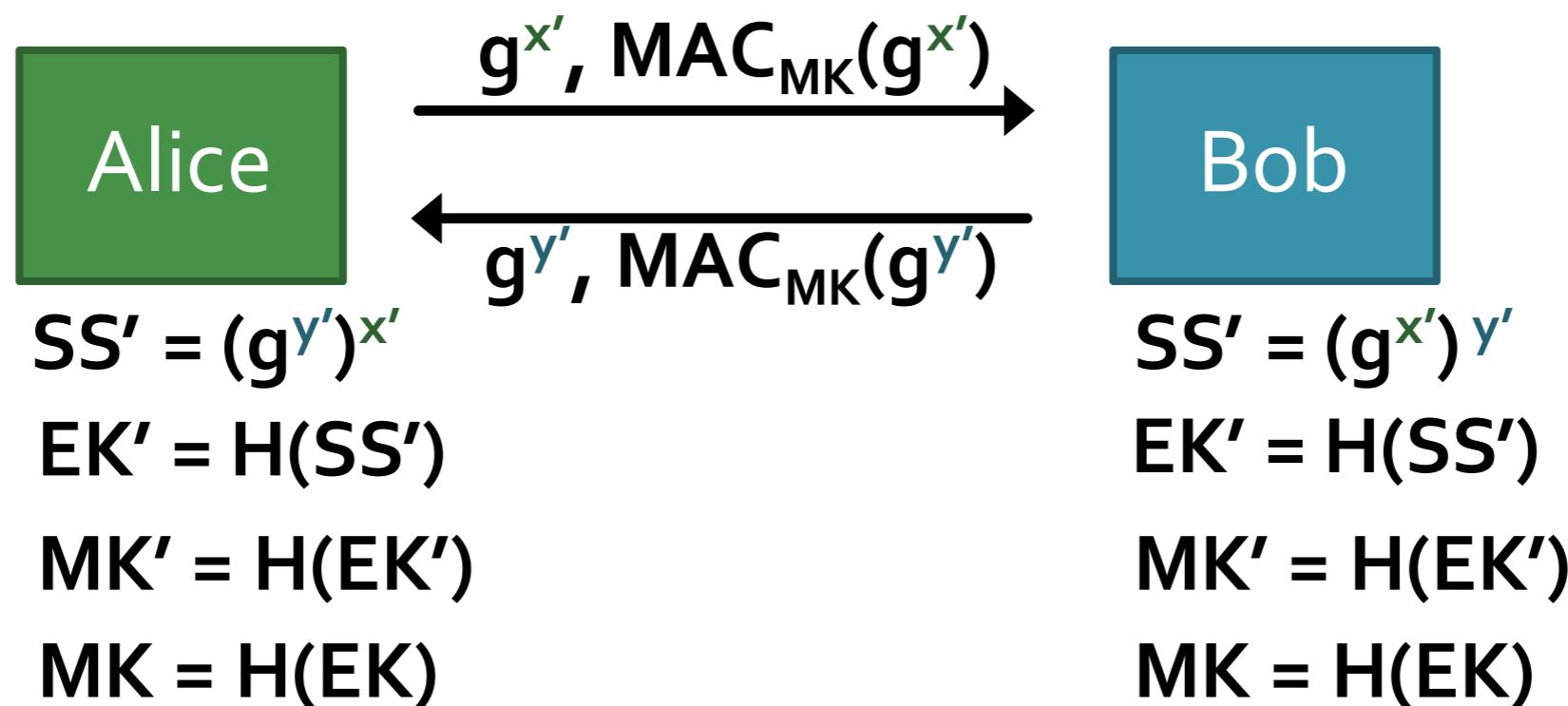
OTR: Off the Record Chat

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



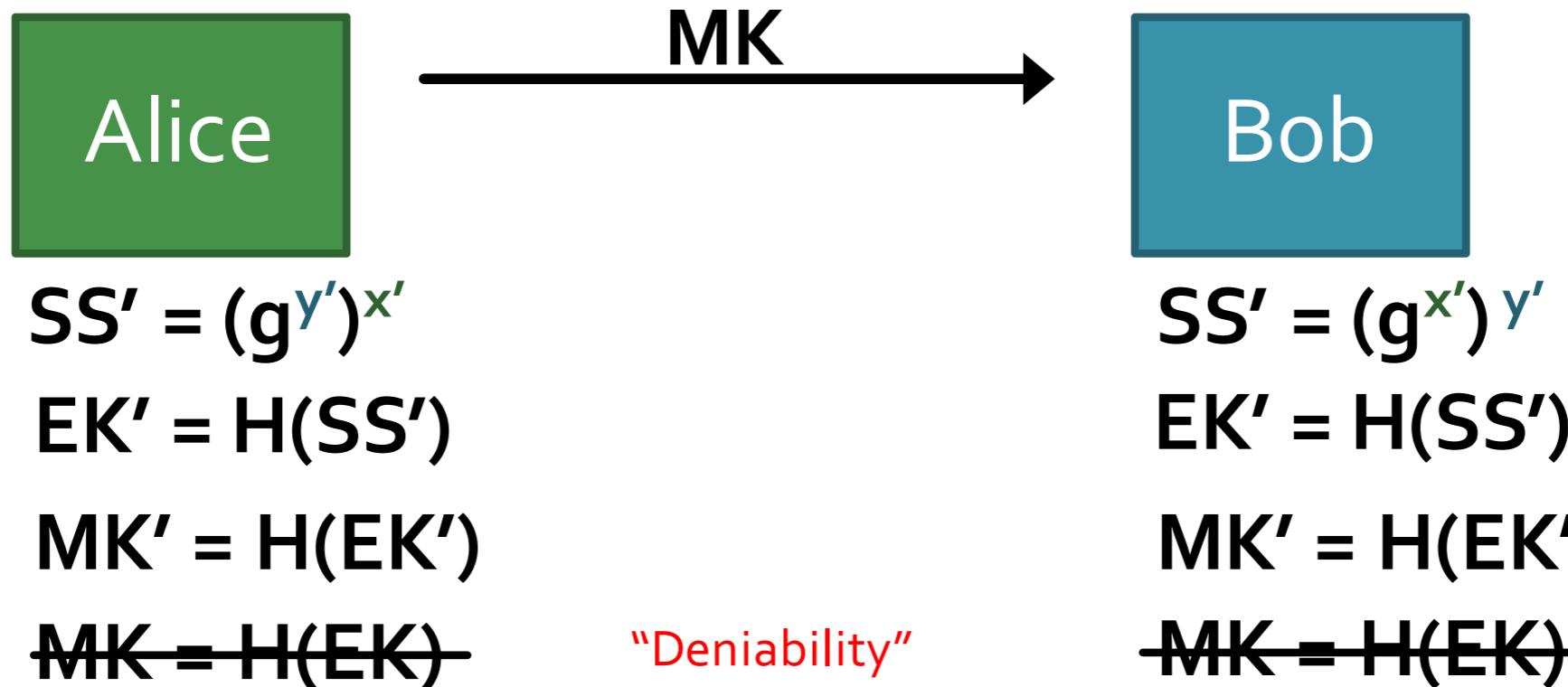
OTR: Off the Record Chat

3. Re-key using Diffie-Hellman



OTR: Off the Record Chat

4. Publish old MK



Signal / WhatsApp

A successor to OTR

- **End-to-End Encryption:**

- Messages are encrypted on the sender's device and only decrypted on the recipient's device. Even Signal's servers can't access message content.

- **Double Ratchet Algorithm:**

- The "ratcheting" process ensures that [each new message has a unique encryption key](#), meaning past and future messages remain secure even if a key is compromised.

- **Asynchronous (Pre-Key) Messaging:**

- [Pre-keys](#) are temporary public keys stored on the server. When Alice sends a message to Bob (*who is offline*), Alice can encrypt it using one of Bob's pre-keys, which is later decrypted by Bob's device.

- **X3DH (Extended Triple Diffie-Hellman) Key Agreement Protocol:**

- Allows authenticated, async key exchange.

Telegram



- **MTProto:** Telegram's proprietary protocol. Hasn't undergone the same level of peer review and scrutiny as the Signal Protocol.
- **Default Chats:** By default, Telegram stores all messages on its servers with standard client-server encryption.
- **Secret Chats:** Implements end-to-end encryption: encrypted on the device level and are not stored on Telegram's servers
- **Group Chats:** No end-to-end encryption for group chats, so all group conversations are stored on Telegram's servers with only client-server encryption.

Questions?