Prep for Class

- Please pick another student *randomly* from the participants list, pick a word X from the list below that resonates with you (or choose your own), and send them a *private* chat message saying “i’m X”
  - Grumpy/Dopey/Happy/Bashful/Sleepy/Sneezy/Bored/Confident/Loving/Joyful/Anxious/ Peaceful/Determined/Lost/Disinterested/Lonely/Thriving/Dedicated/Frazzled/Alive
- If someone sends you a private chat message “i’m X”, use copy-paste to send them back a *private* chat saying “hi X”
- If you can successfully copy-paste and send private chat messages, vote “yes” in the participants window. If not, vote “no”.
- Think of a positive memory from your time at Cal. Maybe something inspiring, or meaningful to you, or that you’re grateful for, or that captures your time here. Nothing inappropriate or embarrassing, please. Don’t share it (yet).

Lecture 36: Anonymous Communications

https://cs161.org

Announcements

- Homework 3B - due Friday 4/25, 11:59pm
- Project 3 Part 2 - due Sunday 5/3, 11:59pm

Demo

- Think of a positive memory from your time at Cal. Maybe something inspiring, or meaningful to you, or that you're grateful for, or that captures your time here.
  - Nothing inappropriate or embarrassing, please.
- Don't share it! (yet)

Demo

- Puzzle: I'd love for you all to share your memory in chat, but without your name attached. How could we use private chat to achieve that?

Demo

- Step 1: Randomly choose another student on the participants list. Send them a private message with your memory. (Don’t post anything in public chat yet!)
- Step 2: Copy-paste whatever private message(s) you received into a new chat message, and mark it visible to Everyone… but don’t send yet.
- Step 3: Hit send now!

Anonymity

- Anonymity: Concealing your identity

- In the context of the Internet, we may want anonymous communications
  - **Communications where the identity of the source and/or destination are concealed**

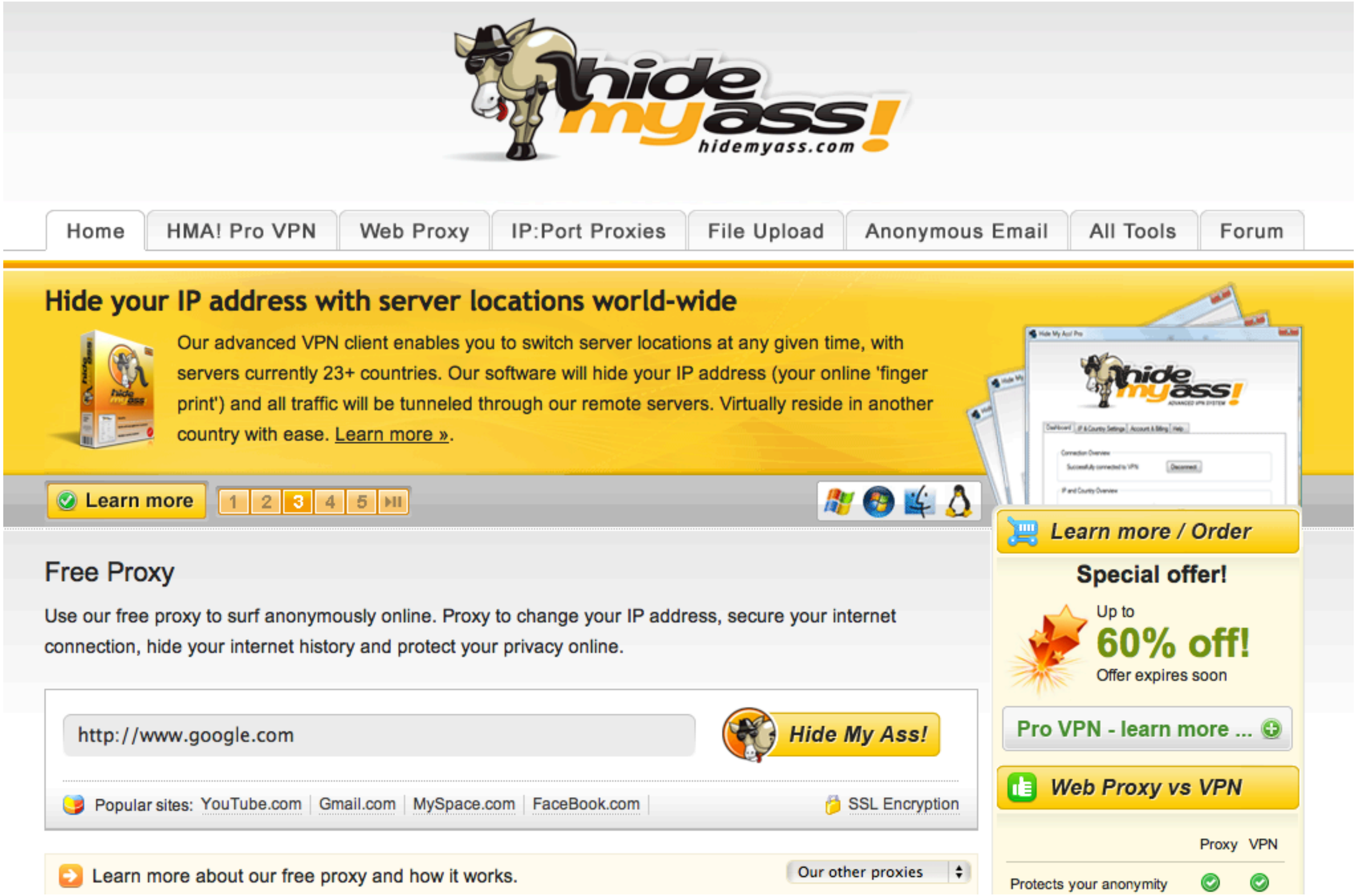
- Not to be confused with confidentiality
  - Confidentiality is about contents, anonymity is about identities

Anonymity

- Internet anonymity is *hard**
  - Difficult if not impossible to achieve on your own
  - Right there in every packet is the source and destination IP address
  - * But it's easy for bad guys. Why?
- You generally need help
- State of the art technique: **Ask someone else to send it for you**
  - (Ok, it's a bit more sophisticated than that…)

Proxies

- Proxy: Intermediary that relays our traffic
- Trusted 3rd party, e.g. …


hide my ass!
hidemyass.com
Home
HMA! Pro VPN
Web Proxy
IP:Port Proxies
File Upload
Anonymous Email
All Tools
Forum
Hide your IP address with server locations world-wide
Our advanced VPN client enables you to switch server locations at any given time, with servers currently 23+ countries. Our software will hide your IP address (your online 'finger print') and all traffic will be tunneled through our remote servers. Virtually reside in another country with ease. Learn more ».
Learn more
1 2 3 4 5
Learn more / Order
Special offer!
Up to
60% off!
Offer expires soon
Pro VPN - learn more ...
Web Proxy vs VPN
Proxy VPN
Protects your anonymity
Free Proxy
Use our free proxy to surf anonymously online. Proxy to change your IP address, secure your internet connection, hide your internet history and protect your privacy online.
http://www.google.com
Hide My Ass!
Popular sites: YouTube.com | Gmail.com | MySpace.com | FaceBook.com
SSL Encryption
Learn more about our free proxy and how it works.
Our other proxies

Proxies

- Proxy: Intermediary that relays our traffic
- Trusted 3rd party, e.g. … hidemyass.com
  - You set up an encrypted VPN to their site
  - All of your traffic goes through them
- Why easy for bad guys? Compromised machines as proxies.

Alice wants to send a message M to Bob …

… but ensuring that
- Bob doesn't know M is from Alice, and/or
- Eve can't determine that Alice is indeed communicating with Bob.

Alice wants to send a message M to Bob …

… but ensuring that
- Bob doesn't know M is from Alice, and/or
- Eve can't determine that Alice is indeed communicating with Bob.

Alice wants to send a message M to Bob …

… but ensuring that
- Bob doesn't know M is from Alice, and/or
- Eve can't determine that Alice is indeed communicating with Bob.

Alice wants to send a message M to Bob …

… but ensuring that
- Bob doesn't know M is from Alice, and/or
- Eve can't determine that Alice is indeed communicating with Bob.

Alice wants to send a message M to Bob …

… but ensuring that
- Bob doesn't know M is from Alice, and/or
- Eve can't determine that Alice is indeed communicating with Bob.

Alice wants to send a message M to Bob …

… but ensuring that
- Bob doesn't know M is from Alice, and/or
- Eve can't determine that Alice is indeed communicating with Bob.

HMA accepts messages encrypted for it.
Extracts destination and forwards.

Proxies

- Proxy: Intermediary that relays our traffic
- Trusted 3rd party, e.g. … hidemyass.com
  - You set up an encrypted VPN to their site
  - All of your traffic goes through them
  - Why easy for bad guys? Compromised machines as proxies.
- Issues?
  - Performance
  - $80-$200/year
  - "Trusted 3rd Party"
  - **rubber hose cryptanalysis**
    - Government comes a "calling" (Or worse)
    - HMA knows Alice and Bob are communicating
- Can we do better?

Onion Routing

Onion Routing

- This approach generalizes to an arbitrary number of intermediaries (“mixes”)

Onion Routing

- This approach generalizes to an arbitrary number of intermediaries (“mixes”)
- Alice ultimately wants to talk to Bob, with the help of HMA, Dan, and Charlie

Onion Routing

- This approach generalizes to an arbitrary number of intermediaries (“mixes”)
- Alice ultimately wants to talk to Bob, with the help of HMA, Dan, and Charlie

Alice

M

Onion Routing

- This approach generalizes to an arbitrary number of intermediaries (“mixes”)
- Alice ultimately wants to talk to Bob, with the help of HMA, Dan, and Charlie

Alice

$\{M, Bob\}_{KDan}$

Onion Routing

- This approach generalizes to an arbitrary number of intermediaries (“mixes”)
- Alice ultimately wants to talk to Bob, with the help of HMA, Dan, and Charlie

Alice

$\{\{M, Bob\}_{K_{Dan}}, Dan\}_{K_{Charlie}}$

Onion Routing

- This approach generalizes to an arbitrary number of intermediaries (“mixes”)
- Alice ultimately wants to talk to Bob, with the help of HMA, Dan, and Charlie

Alice

$\{\{\{M, Bob\}_{K_{Dan}}, Dan\}_{K_{Charlie}}, Charlie\}_{K_{HMA}}$

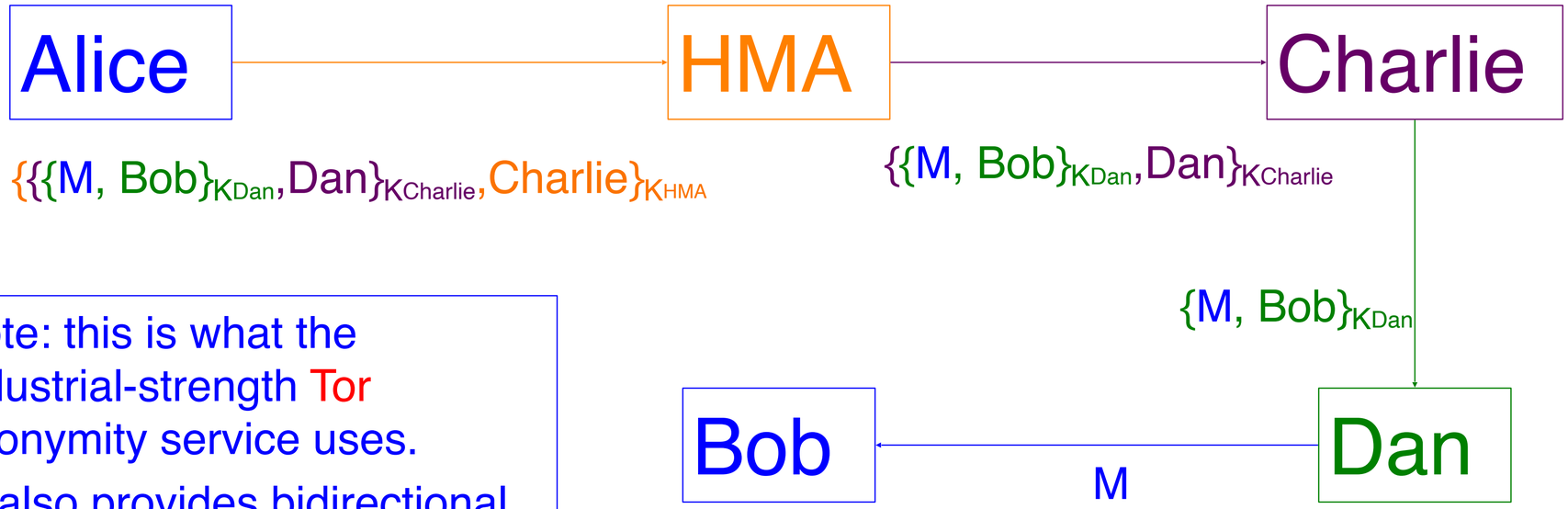
Onion Routing

- This approach generalizes to an arbitrary number of intermediaries (“mixes”)
- Alice ultimately wants to talk to Bob, with the help of HMA, Dan, and Charlie

$\{\{\{M, Bob\}_{K_{Dan}}, Dan\}_{K_{Charlie}}, Charlie\}_{K_{HMA}}$

Onion Routing

- This approach generalizes to an arbitrary number of intermediaries (“mixes”)
- Alice ultimately wants to talk to Bob, with the help of HMA, Dan, and Charlie
- As long as any of the mixes is honest, no one can link Alice with Bob



Note: this is what the industrial-strength Tor anonymity service uses.

(It also provides bidirectional communication)

Key concept: No one relay knows both you and the destination!

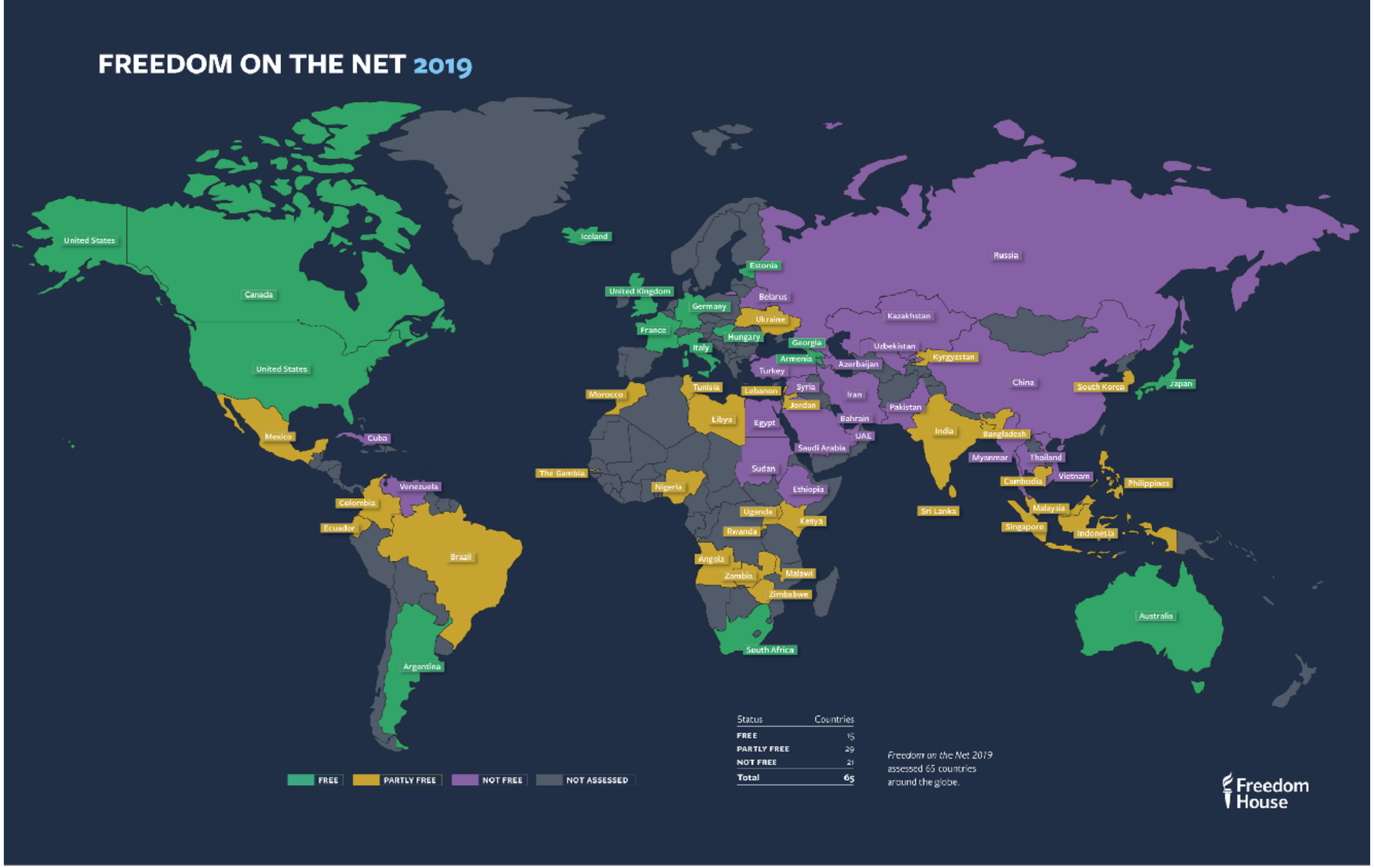
Onion Routing Issues/Attacks?

- Performance: message bounces around a lot
- Attack: rubber-hose cryptanalysis of mix operators
  - Defense: use mix servers in different countries
    - Though this makes performance worse :-(
- Attack: adversary operates all of the mixes
  - Defense: have lots of mix servers (Tor today: ~2,000)
- 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

Internet Censorship

Internet Censorship

- The suppression of Internet communication that may be considered “objectionable,” by a government or network entity
- This is frequently (but not exclusively) related to authoritarian regimes
- We’re going to skip the politics (sorry), and go to the technical meat

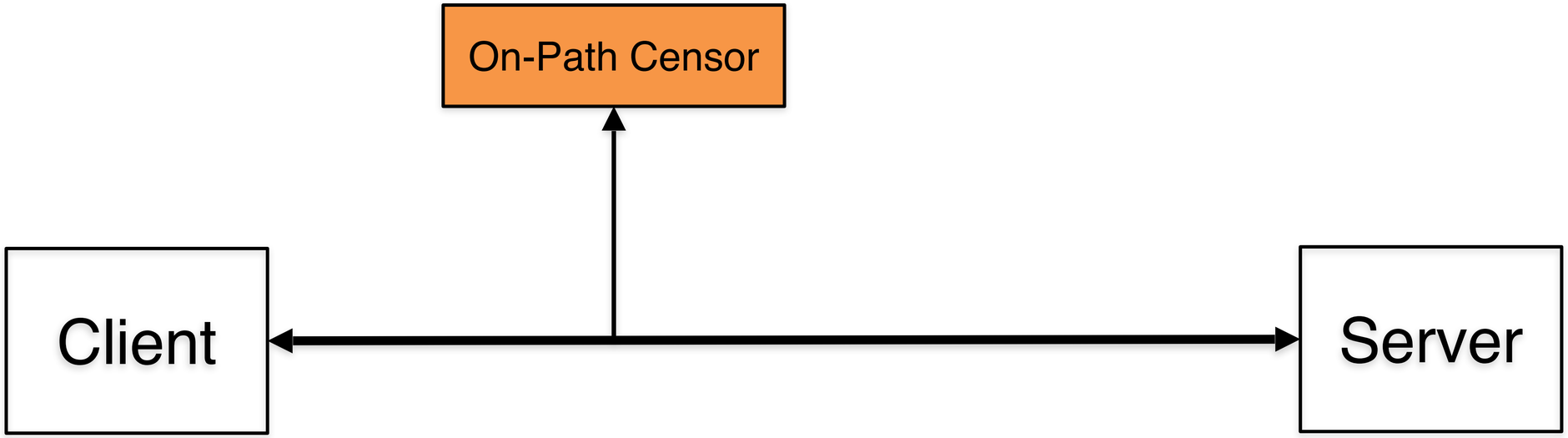


Take these labels with a grain of salt. Read the report for yourself

Source: https://freedomhouse.org/report/freedom-net/2019/crisis-social-media

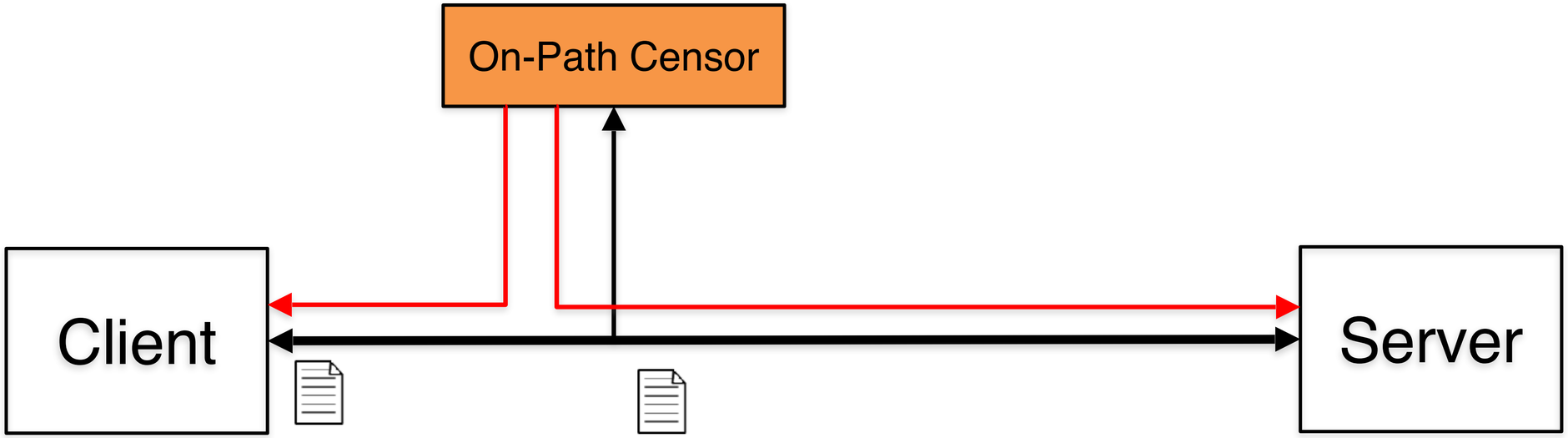
HOWTO: Censorship

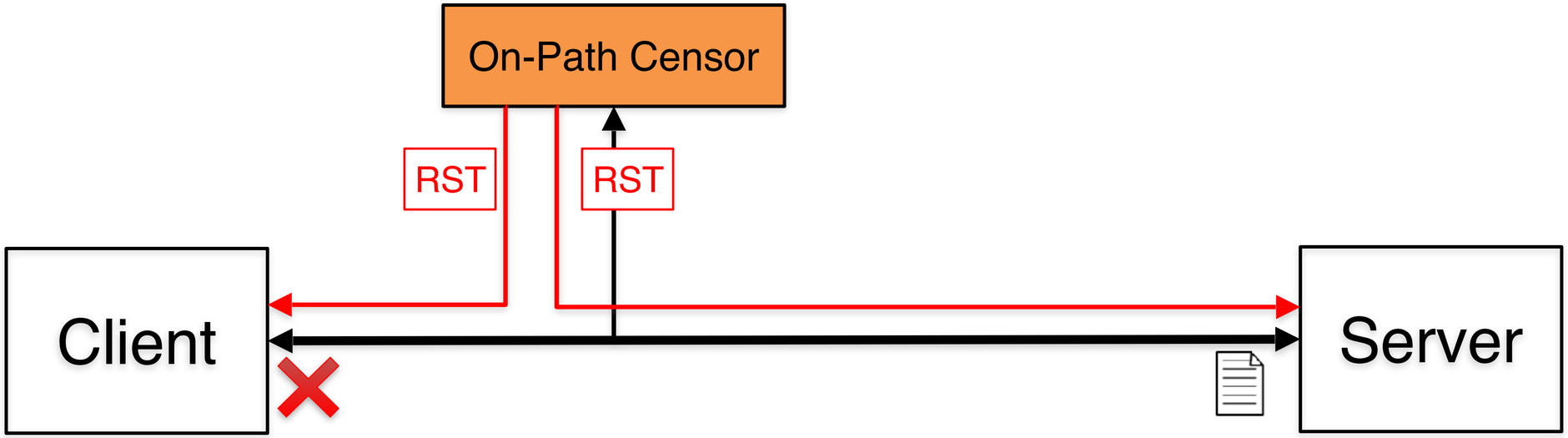
- Requirements:
  - Operate in real time inside of your network
  - Examine large amounts of network traffic
  - Be able to block traffic based on black lists, signatures, or behaviors
- Sounds a lot like a NIDS…
  - Spoiler alert: These systems *are* basically NIDS


On-Path Censor
Client
Server

On-Path Censors

- On-Path device gets a copy of every packet
  - Packets are forwarded on before the on-path device can act (Wait, what?)
- What can we do if we've already forwarded the packet?


On-Path Censor
Client
Server



This is how the elements of the

Great Firewall of China

operate

Evasion

- Evading keyword filters
  - NIDS evasion techniques: TTLs, overlapping segments, etc.
  - Or, simpler: Encryption!
- So that's it right? We'll just encrypt everything, they can't stop that ri…


Iran reportedly blocking en
arstechnica.com/tech-policy/2012/02/iran-reportedly-blocking-encrypted-internet-traffic/
ars technica
MAIN MENU
MY STORIES: 8
FORUMS
SUBSCRIBE
VIDEO
SEARCH
LOG IN
LAW & DISORDER / CIVILIZATION & DISCONTENTS
Iran reportedly blocking encrypted Internet traffic
The Iranian government is reportedly blocking access to websites that use the …
by Jon Brodkin - Feb 10 2012, 8:14am PST
60
The Iranian government is reportedly blocking access to websites that use the HTTPS security protocol, and preventing the use of software residents use to bypass the state-run firewall.
From post on Hacker News today, apparently written by an Iranian resident:
Since Thursday Iranian government has shutted [sic] down the https protocol which has caused almost all google services (gmail, and google.com itself) to become inaccessible. Almost all websites that reply on Google APIs (like wolfram alpha) won't work. Accessing to any website that replies on https (just imaging how many websites use this protocol, from Arch Wiki to bank websites). Also accessing many proxies is also impossible.
Several Hacker News users confirmed the original post's statement that Iran is blocking encrypted Internet traffic. "I live in Iran. The fact about the shut down is correct," one person wrote. Another said "They drop all encrypted connections. This means no https, no IMAP over TLS and no SSH connections. (Im in Iran)."
TOP FEATURE STORY
FEATURE STORY (2 PAGES)
It just works: Dell XPS 13 Developer Edition Linux Ultrabook review
Dell's substantial investment in making a functional Linux Ultrabook pays off.
149
STAY IN THE KNOW WITH

Pakistan to ban encryption software

Internet service providers will be required to inform authorities if customers use virtual private networks in government crackdown

Share

Email

Josh Halliday and **Saeed Shah** in Lahore
The Guardian, Tuesday 30 August 2011 14.26 EDT

Internet users in Pakistan will no longer be able to access the web through virtual private networks following the government ban. Photograph: M. Sajjad/AP

Millions of internet users in Pakistan will be unable to send emails and messages without fear of government snooping after authorities banned the use of encryption software.

A legal notice sent to all internet providers (ISPs) by the Pakistan Telecommunications Authority, seen by the Guardian, orders the ISPs to inform authorities if any of their customers are using virtual private networks (VPNs) to browse the web.

Article history

World news
Pakistan · South and Central Asia

Technology
Internet · Facebook · BlackBerry · Mobile phones

Media
Social networking

More news

Related

19 Apr 2013
How Pervez Musharraf's story has gone from Facebook fantasy to farce

16 Apr 2013
Eric Schmidt denies claims Google plans to block Facebook Home

15 Apr 2013
Facebook's Sheryl Sandberg defends mobile advertising plans

13 Apr 2013
Cash is on the line when

Our correspondents on Twitter

Follow all the top stories of the day on Twitter with the Guardian's world news team

john_hooper: As part of the plan for rejuvenating Italian politics, Giorgio Napolitano, aged 87, has agreed to remain president #news #Italy
about 14 hours, 36 minutes ago

john_hooper: All the talk in #Italy this morning is of getting Napolitano to stay on for another 7-year term as president. He is 87. #news
about 19 hours, 2 minutes ago

john_hooper: #Italy presidential vote: #Prodi just pulled out after humiliating failure to secure a 50% majority #news
about 1 day, 9 hours ago

• Follow all our correspondents on a Twitter list

Today's best video

The Guardian Film Show
Our critics review Olympus Has Fallen, Love is all You Need (above), Evil Dead and Fuck for Forest

Evasion

- Evading keyword filters
  - NIDS evasion techniques: TTLs, overlapping segments, etc.
  - Or, simpler: Encryption!
- So that's it right? We'll just encrypt everything, they can't stop that ~~right~~ wrong
- This is called an arms race

Evasion

- Evading both keyword and IP/Domain blacklists
  - Simple approach: Use a VPN
    - If encryption is not banned this is a great solution
    - Con: Easy to ban the VPN IP, especially if it's public
  - More robust approach
    - Use an onion router like Tor
      - Despite being built for anonymity, it has good censorship resistance properties
      - **Tor is the defacto standard for censorship resistance**

China Cracks Down on Tor Anonymity Network

A leading anonymity technology is targeted by the Chinese government for the first time.

By David Talbot

Constant arms race between Tor and censoring governments

For the first time, the Chinese governmen
for surfing the Internet anonymously. The
the days leading up to the 60th anniversary of China's "national day" on October 1. It is part of a growing trend in which repressive nations orchestrate massive clampdowns during politically sensitive periods, in addition to trying to maintain Internet firewalls year-round.

"It was the first time the Chinese government has ever even included Tor in any sort of censorship circumvention effort," says Andrew Lewman, the executive director of Tor Project, the nonprofit that maintains the Tor software and network. "They were so worried about October 1, they went to anything that could possibly circumvent their firewall and blocked it."

Tor is one of several systems that route data through intermediate computers called proxies, thereby circumventing government filters. To anyone watching Internet connections, the traffic then seems to be