Anonymous Communication and Internet Freedom

CS 161: Computer Security

Prof. David Wagner

April 29, 2016

Announcements

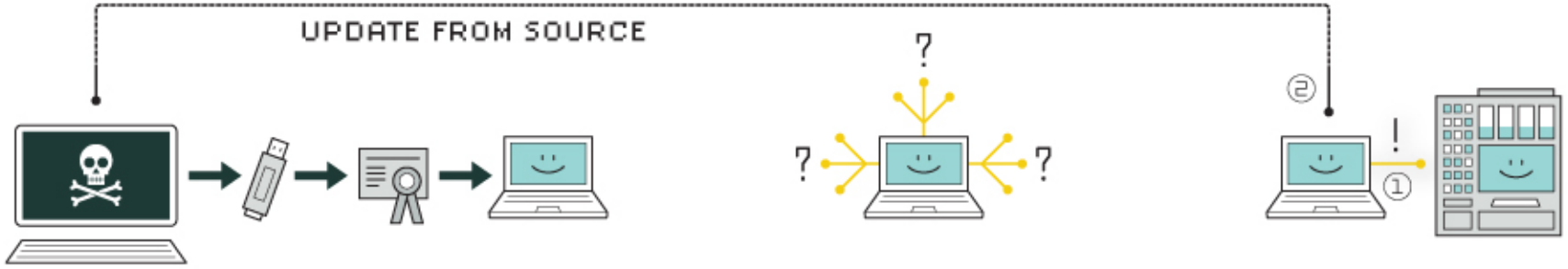
- Final exam in RSF Fieldhouse, 5/10, arrive by 7PM
- HW4 due Monday, 5/2, 11:59pm
- Review sessions next MWF 11am-12 here, with TAs
  - Monday 5/2: Software security and web security
  - Wednesday 5/4: Cryptography
  - Friday 5/6: Network security

Goals For Today

- State-sponsored adversaries
- Anonymous communication
- Internet censorship

State-Sponsored Adversaries

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Anonymous Communication

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

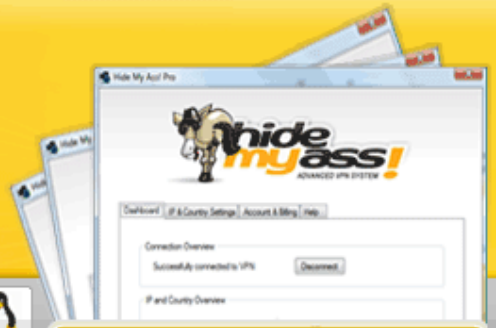
- Internet anonymity is *hard**
  - Difficult if not impossible to achieve on your own
  - Right there in every packet is the source and destination IP address
  - * But it's easy for bad guys. Why?
- You generally need help
- State of the art technique: **Ask someone else to send it for you**
  - (Ok,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

Proxies

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

Hide 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

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

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	✓	✓

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

M

HMA

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

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

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

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

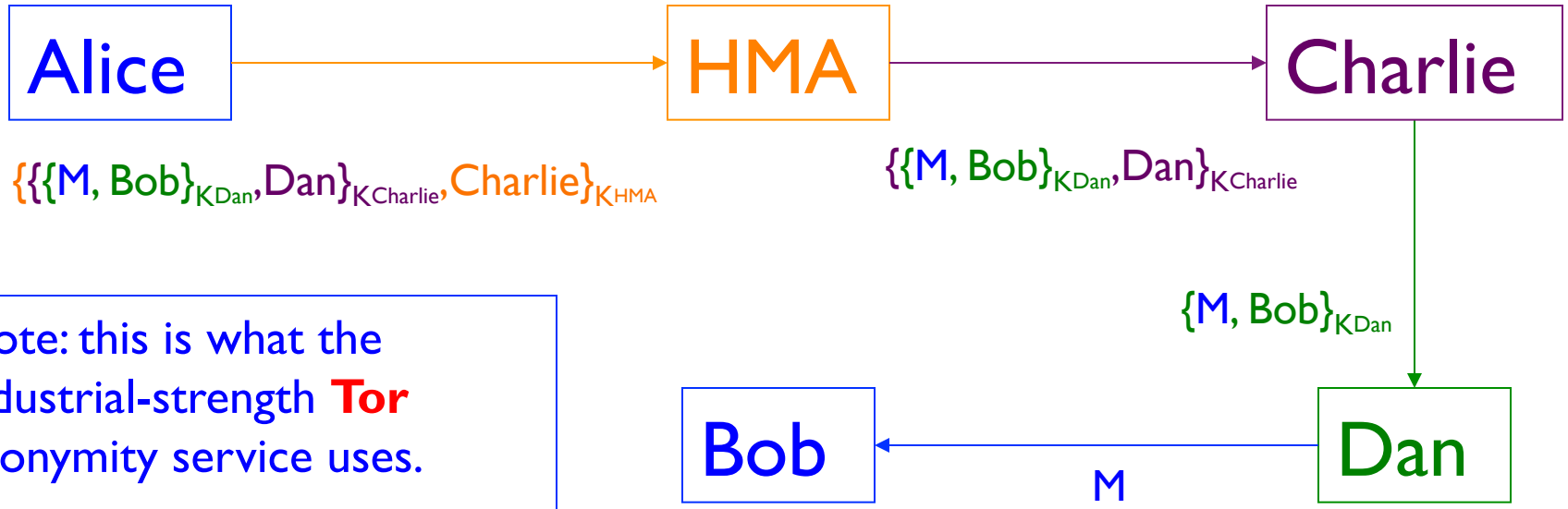
Onion Routing

- 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!

Demo

- Four volunteers, please

Demo

- Look under your seat –

Demo

- Look under your seat – if you find an envelope and index card, you're in!
  - What's your fondest memory of your time at Berkeley? Write it on the index card. Put it in the small envelope. Address the small envelope to a random Tor mix (2nd hop), and put it in the large envelope, addressed to another Tor mix (1st hop).
- Tor mixes: **Byung (front left), Jerry (front right), Apoorva (back right), Abraar (back left)**
  - When you receive an envelope, open it. If it's an envelope, pass on its contents to the next hop. If it's an index card, pass it to a TA.
- Everyone else: you're an Internet router. Help pass envelopes on to their destination.

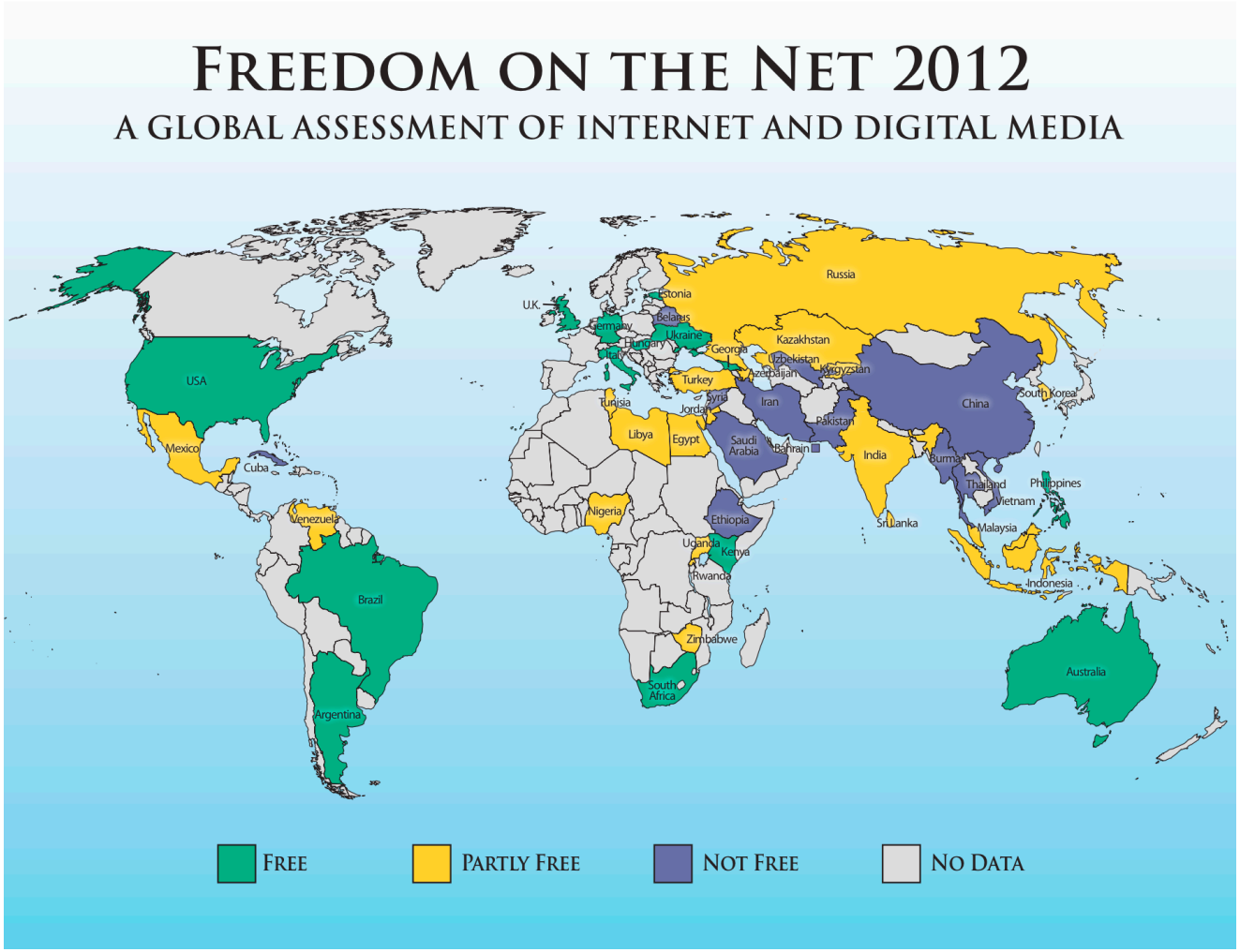
Onion Routing Issues/Attacks?

- 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

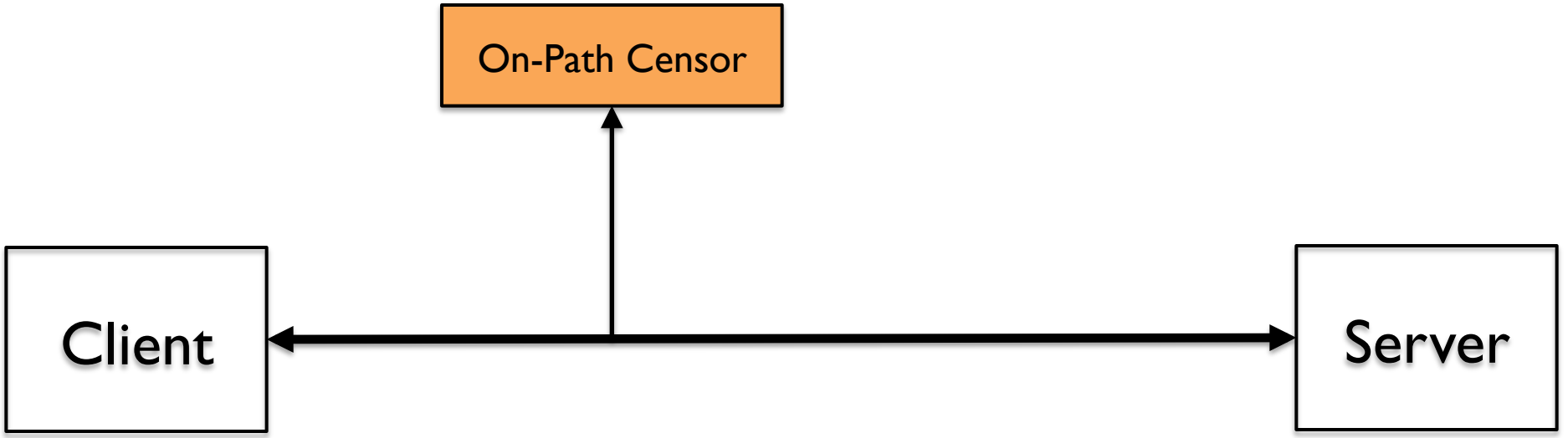


Take these labels with a grain of salt. Read the report for yourself

Source: http://www.freedomhouse.org/sites/default/files/FOTN%202012%20summary%20of%20findings.pdf

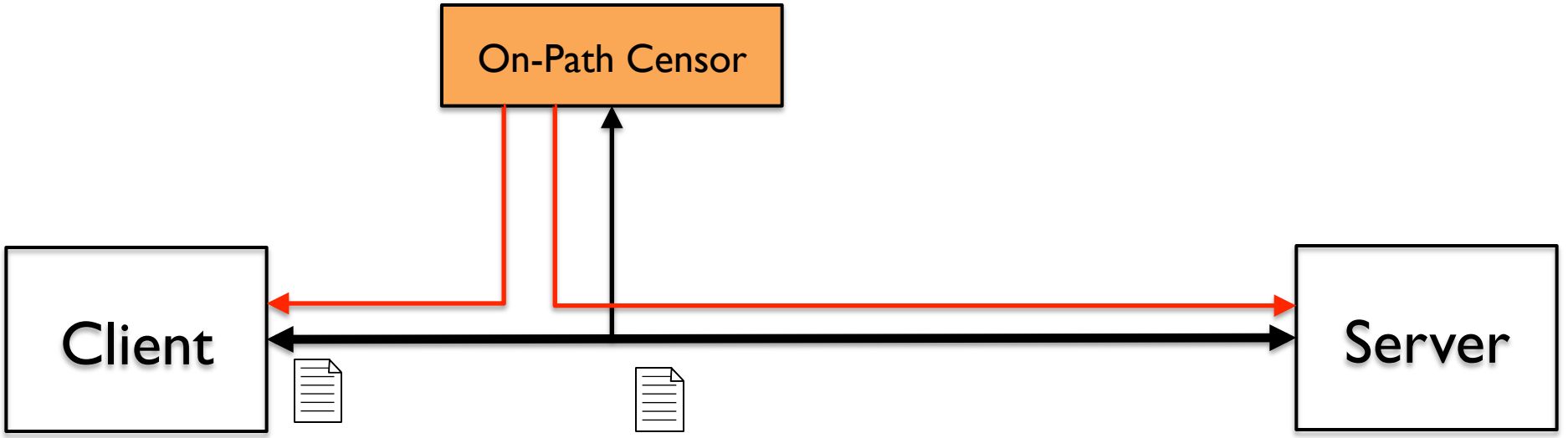
HOWTO: Censorship

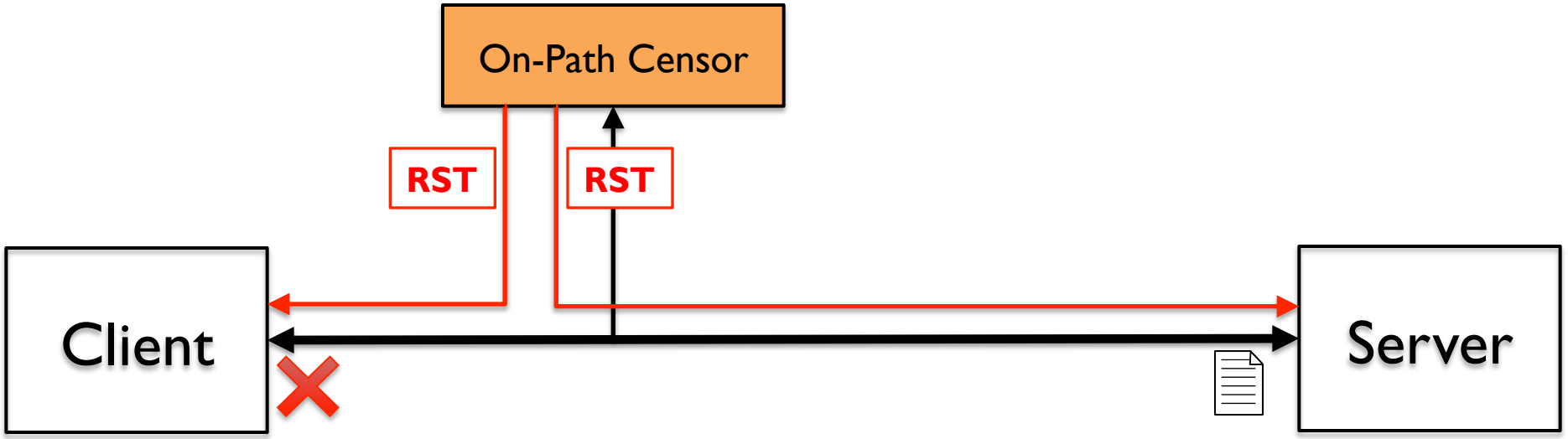
- Requirements:
  - Operate in real time inside of your network
  - Examine large amounts of network traffic
  - Be able to block traffic based on black lists, signatures, or behaviors
- Sounds a lot like a NIDS…
  - Spoiler alert: These systems *are* basically NIDS


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. (see lecture 3/10)
  - Or, simpler: Encryption!
- So that's it right? We'll just encrypt everything, they can't stop that ri…

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)."

Pakistan to ban encryption software

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

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

Article history

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.

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

Evasion

- Evading keyword filters
  - NIDS evasion techniques: TTLs, overlapping segments, etc. (see lecture 3/10)
  - 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 government has attacked one of the best, most secure tools for surfing the Internet anonymously. The clampdown against the tool, called Tor, came in 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."

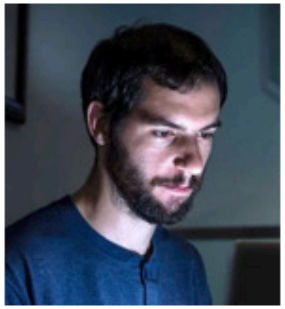
Tor is one of several systems that route data through intermediate computers called proxies, thereby circumventing government filters. To anyone watching Internet connections, the traffic then seems to be

Takeaways from this course

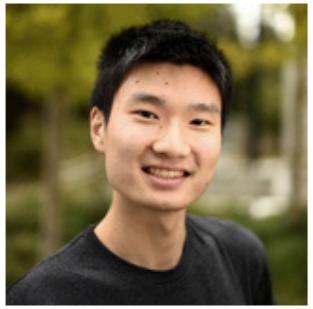
- I hope you've learned: how to recognize when you might face an adversary; what defenses might be available; and their strengths and limitations.

- If you want to learn more:
  - www.schneier.com (Bruce Schneier's blog)
  - blog.cryptographyengineering.com (Matt Green's blog)
  - Security Engineering (book by Ross Anderson)
  - security.stackexchange.com, crypto.stackexchange.com

Jethro Beekman



Nicholas Carlini

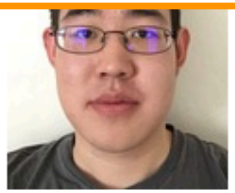


Austin Chen

Michael Chen (Head GSI)

Please thank your hard-working TAs!

Robin Hu

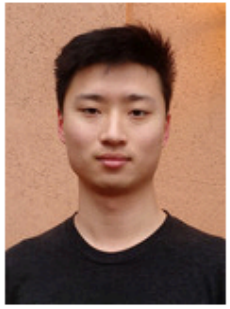


Calvin Li

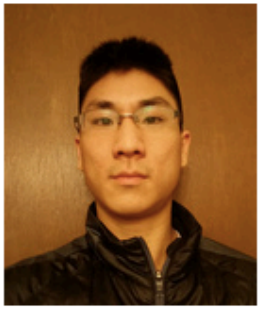
Frank Li

Pratyush Mishra

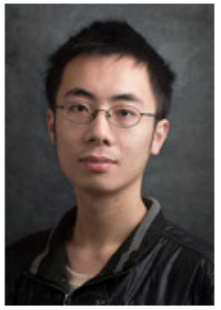
Chris Thompson



William Xu



Bill Yeh



Qi Zhong

Extra Material

Onion Routing Issues, cont.

- Issue: **traffic leakage**
- Suppose all of your HTTP/HTTPS traffic goes through Tor, but the rest of your traffic doesn't
  - Because you don't want it to suffer performance hit
- How might the operator of `sensitive.com` deanonymize your web session to their server?
- Answer: they inspect the logs of their DNS server to see who looked up `sensitive.com` just before your connection to their web server arrived
- **Hard**, general problem: anonymity often at risk when adversary can correlate separate sources of information

Onion Routing Issues, con't

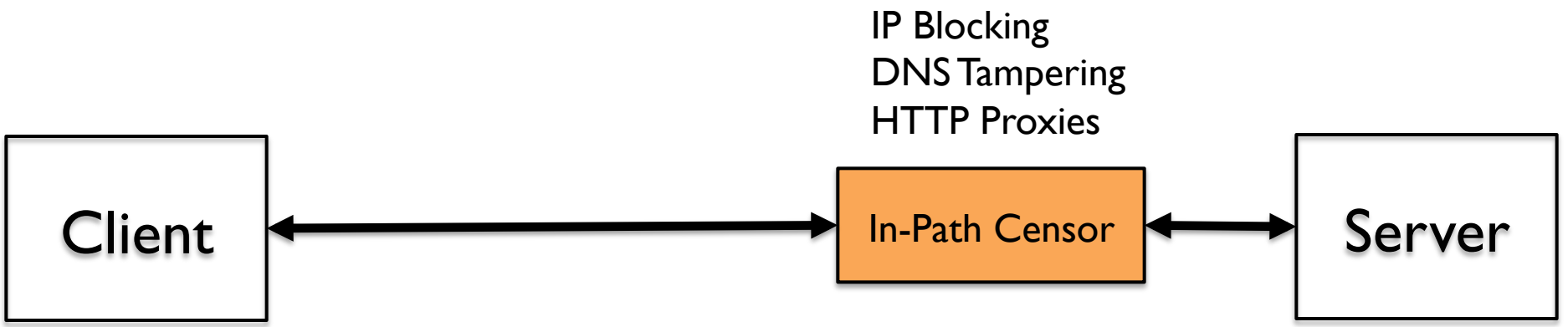
- Issue: **application leakage**
- Suppose you want to send all your BitTorrent traffic over Tor to hide your IP…
  - (Public service announcement: Please don't do this)
- Problem:
  - BitTorrent includes your computer's actual IP address in the application protocol messages
- What about tracking cookies in your web browser?
- Javascript?

Onion Routing Issues, con't

- Issue: **performing deanonymizing actions**
- Suppose you want to anonymously search Google
  - Great. Right after I check my email, paul_pearce_berkeley_cs161_ta@gmail.com
- If you perform some action that intrinsically identifies you, all the technology in the world can't help.

HOWTO: Censorship

- How do we implement censorship?
- Attempt #1: **In-Path censor**
  - Blacklist of IP addresses, domain names, or keywords


IP Blocking
DNS Tampering
HTTP Proxies
Client
In-Path Censor
Server

HOWTO: Censorship

- In-path monitoring is **slow** , particularly if inspecting content.
- We need a new censorship architecture: **On-path censor**

Related Activity: Intelligence Gathering

- Using same infrastructure, redirect users to malicious sites, collect information