Internet Freedom

CS161: Computer Security

Guest Lecturer: Paul Pearce

Instructor: Vern Paxson
TAs: Jethro Beekman, Mobin Javed
Antonio Lupher, Me,
& Matthias Vallentin

http://www.icir.org/vern/cs161-sp13/

April 23, 2013

Today's Lecture

- What is "Internet Freedom?"
  - Buzzword encompassing:
    - Anonymity
    - Internet Censorship
    - Network Neutrality

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**
  - Concealed from whom?
    - Typically, the other party we are communicating with
    - What about the network itself?

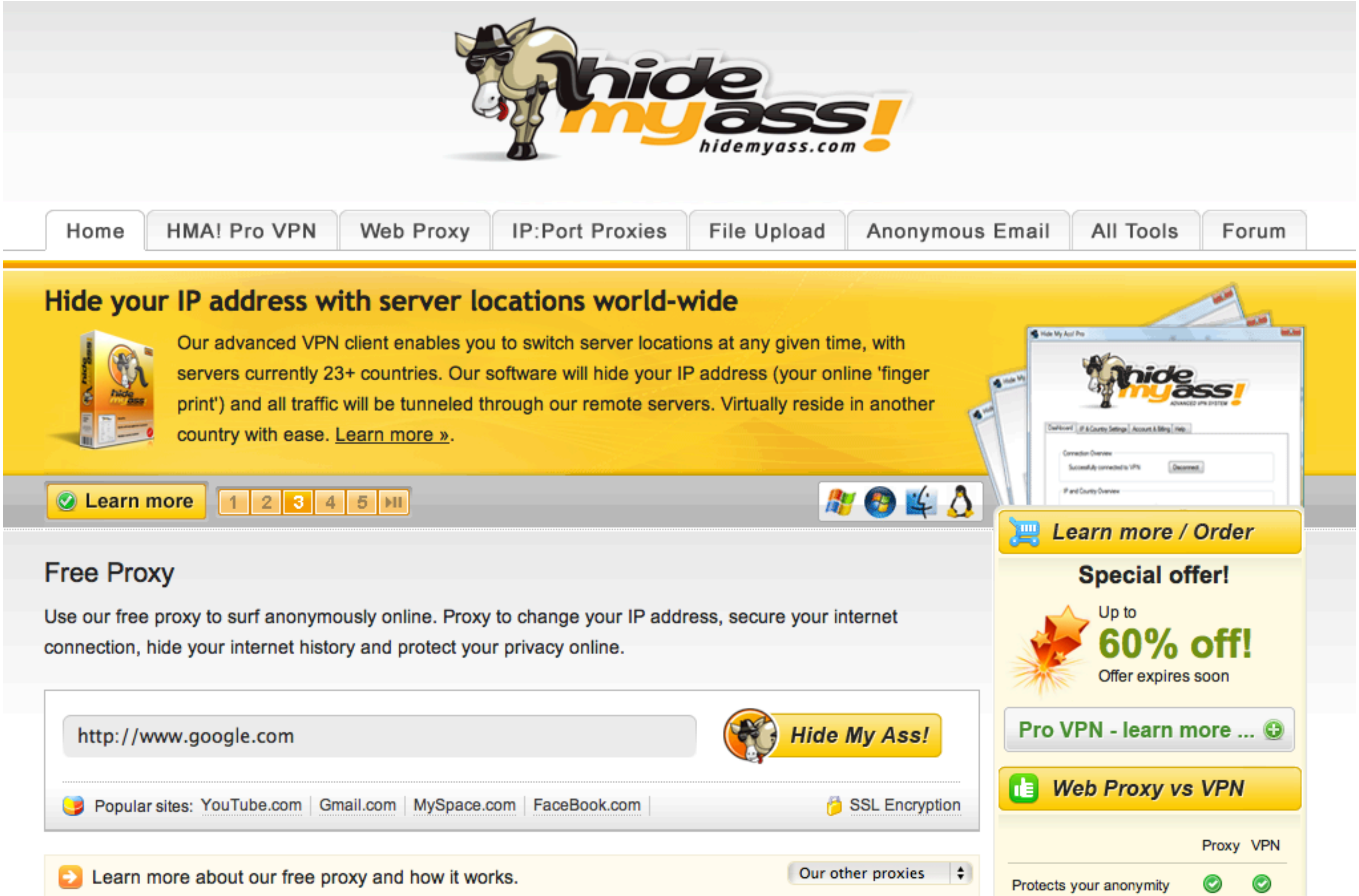
- Not to be confused with confidentiality
  - Confidentiality is about contents, anonymity is about identities

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 ».

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

Popular sites: YouTube.com | Gmail.com | MySpace.com | FaceBook.com | SSL Encryption

Learn more about our free proxy and how it works.

Proxies

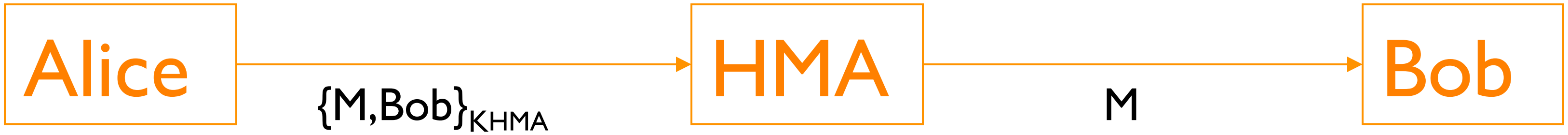
- Proxy: Intermediary that relays our traffic
- Trusted 3rd party, e.g. … hidemyass.com
  - You set up an encrypted VPN to their site
  - All of your traffic goes through them
  - Why easy for bad guys? Compromised machines as proxies.

Alice wants to send a message M to Bob …

… but ensuring that Eve can’t determine that she’s indeed communicating with Bob.

Alice wants to send a message M to Bob …

… but ensuring that Eve can’t determine that she’s indeed communicating with Bob.



Alice

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

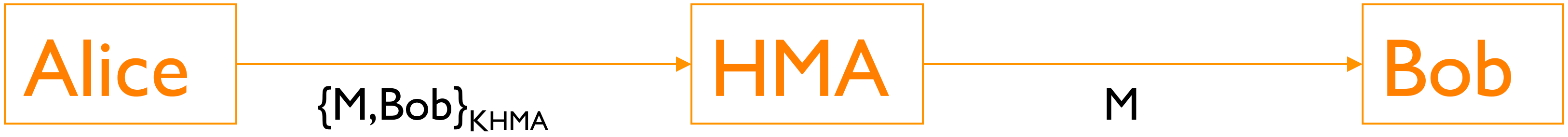
HMA

M

Bob

Alice wants to send a message M to Bob …

… but ensuring that Eve can’t determine that she’s indeed communicating with Bob.



Alice

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

HMA

M

Bob

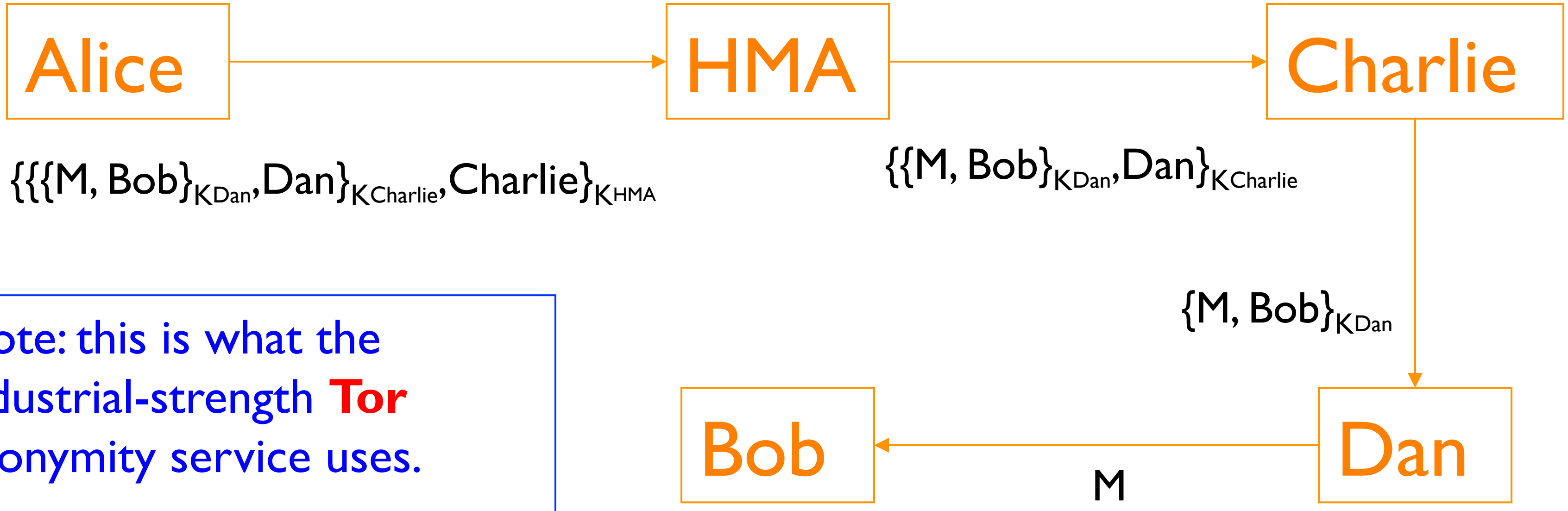
HMA accepts messages encrypted for it.
Extracts destination and forwards.

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

- This approach generalizes to an arbitrary number of intermediaries (“mixes”)
- As long as any of the mixes is honest, no one can link Alice with Bob


Alice
HMA
Charlie
$\{\{\{M, Bob\}_{KDan}, Dan\}_{KCharlie}, Charlie\}_{KHMA}$
$\{\{M, Bob\}_{KDan}, Dan\}_{KCharlie}$
$\{M, Bob\}_{KDan}$
Bob
Dan
M

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
- Key management: the usual headaches
- 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 "confirmation" attack
  - Defenses: pad messages, introduce significant delays
    - Tor does the former, but notes that it' s not enough for defense

Onion Routing Attacks, con't

- 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 Attacks, con’t

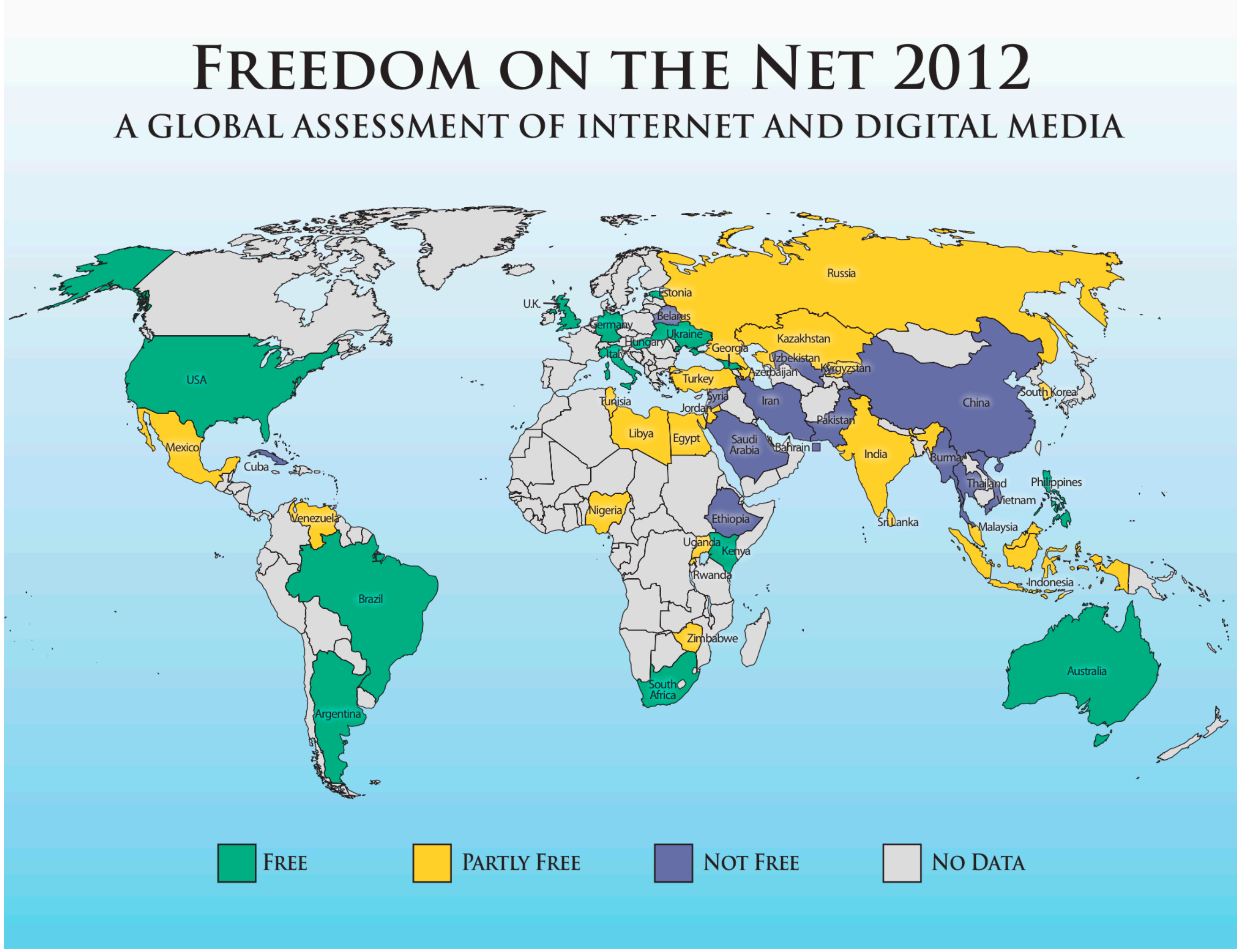
- Issue: **application leakage**
- Suppose you want to send all your BitTorrent traffic over Tor to hide your IP…
  - (Public service announcement: Please don’t do this)
- Problem:
  - BitTorrent includes your computer’s actual IP address in the application protocol messages
- What about tracking cookies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

Onion Routing Attacks, 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.

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

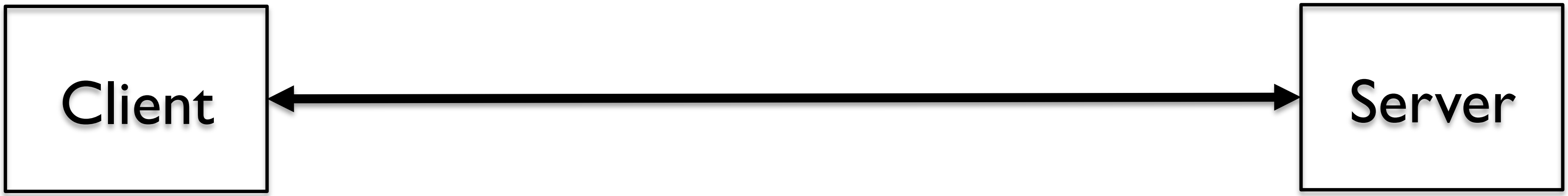
Source: http://www.freedomhouse.org/sites/default/files/FOTN%202012%20summary%20of%20findings.pdf

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

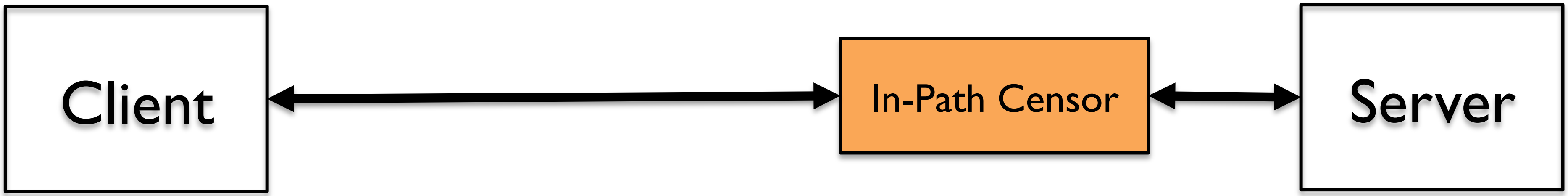
HOWTO: Censorship

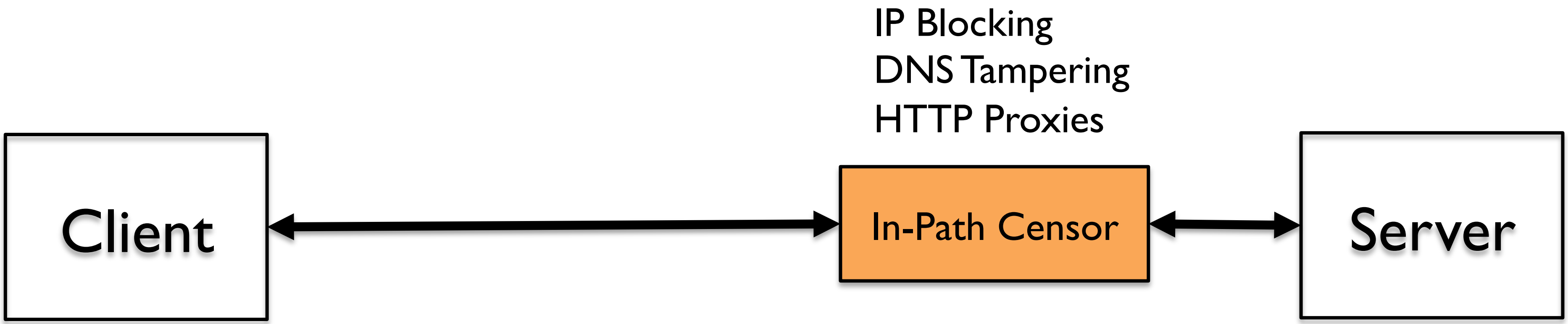
- Approach #1: Blacklist IP addresses
  - Block all communication to a given set of IP addresses
  - **Pros:** Easy to do, low overhead
  - **Cons:** Brittle (must maintain black list), easy to evade (switch IPs), potential collateral damage
- Approach #2: DNS blacklisting and tampering
  - Ask for a banned domain via DNS? Send back bad response
  - Similar pros and cons as #1, better if you want to block domains instead of IPs
- How do we implement?
  - **In-Path censor**



Client

Server


Client
In-Path Censor
Server



IP Blocking
DNS Tampering
HTTP Proxies

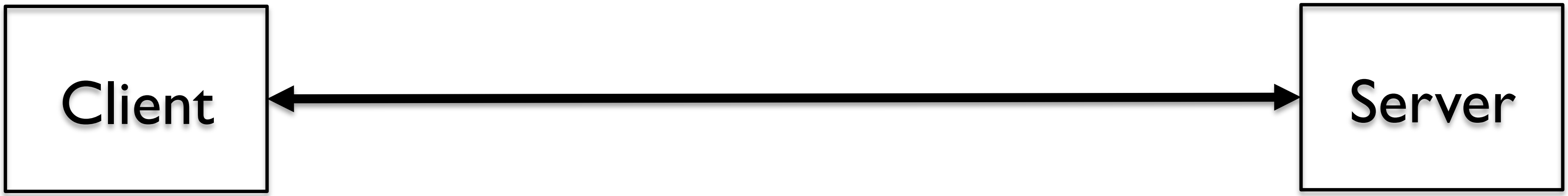
Client

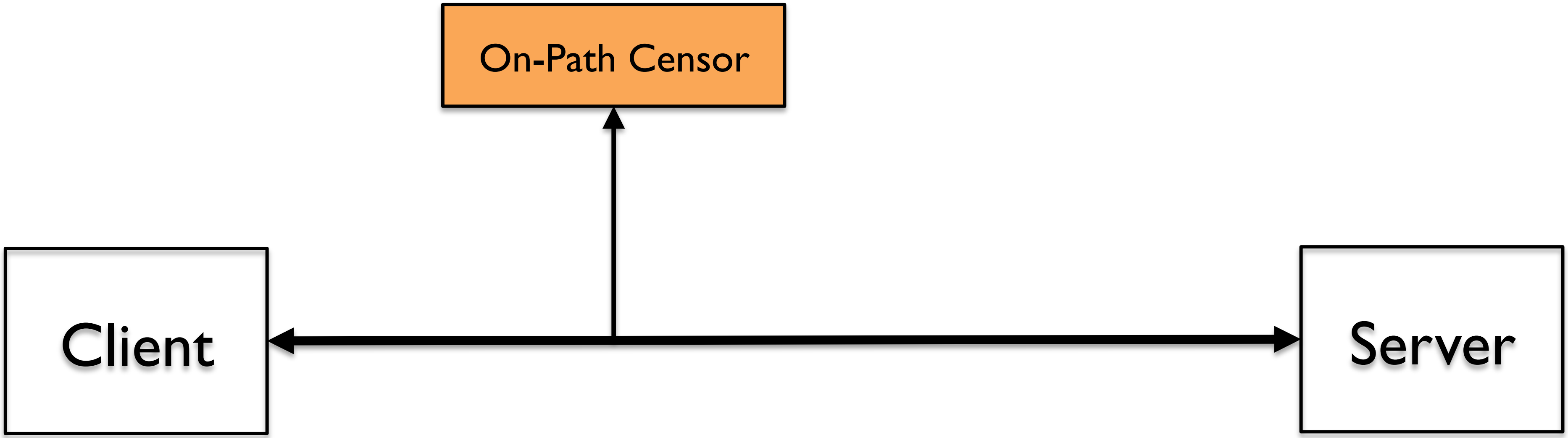
In-Path Censor

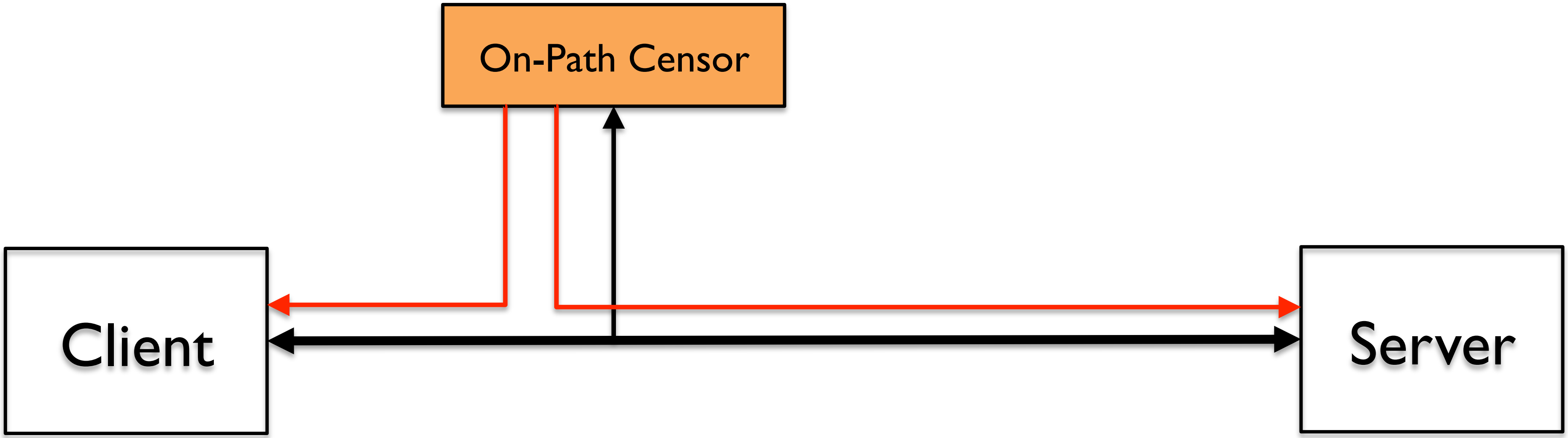
Server

HOWTO: Censorship

- What if we know **what** (keywords) we want to censor, but not **who**?
- Approach #3: Look for censored keywords inside of packets
  - **Pro**: Far more flexible than IP/domain blacklists
  - **Cons**: Packet fragmentation can evade, **slow**
- Approach #4: Deep packet inspect
  - Reassemble TCP streams, understand application protocols
  - **Pro**: Harder to evade
  - **Cons**: Evasion still possible, **Even slower**
- How slow are these approaches? We need a new censorship architecture
  - **On-path censor**

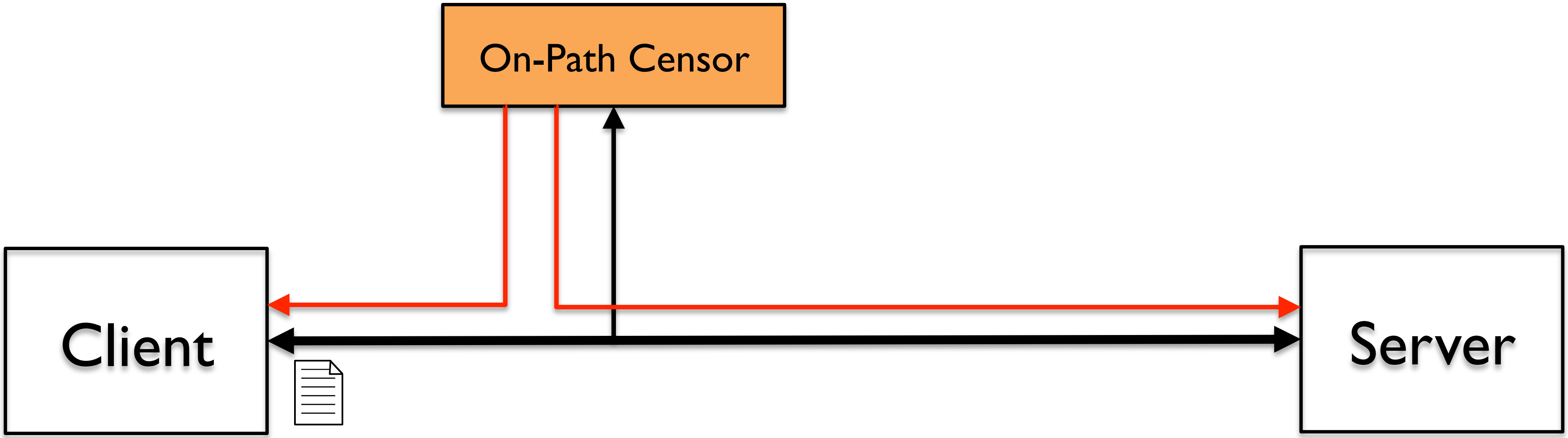

Client
Server

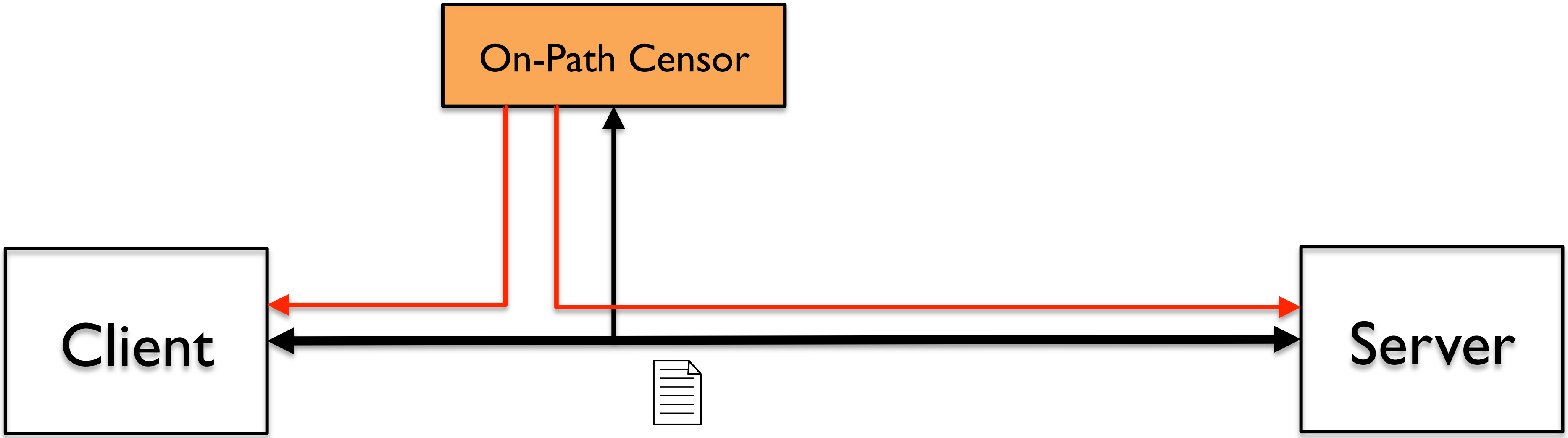

On-Path Censor
Client
Server

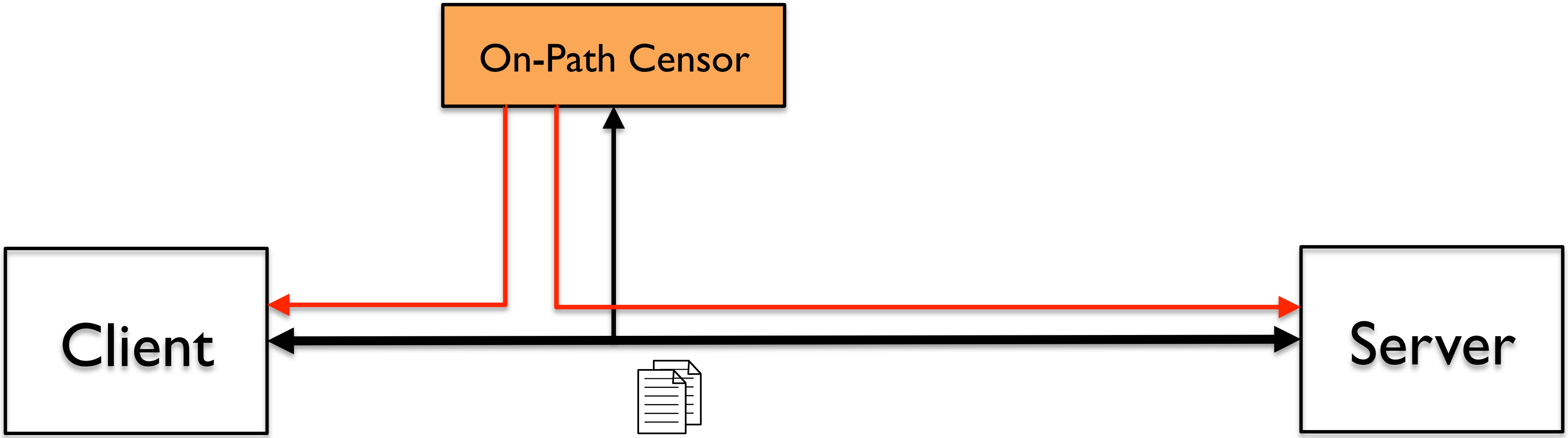

On-Path Censor
Client
Server

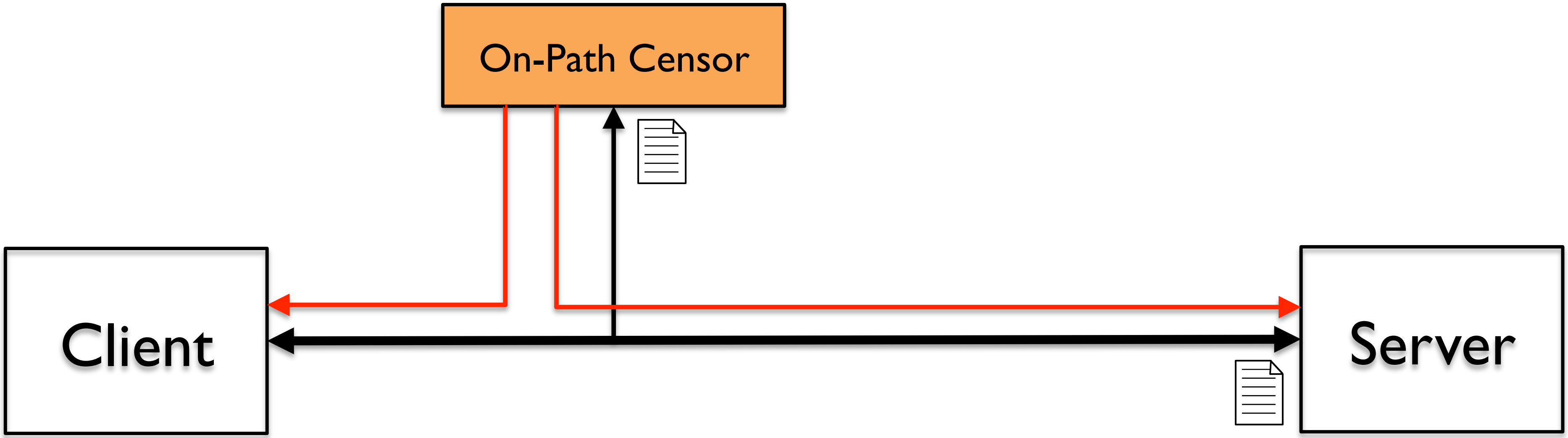
On-Path Censors

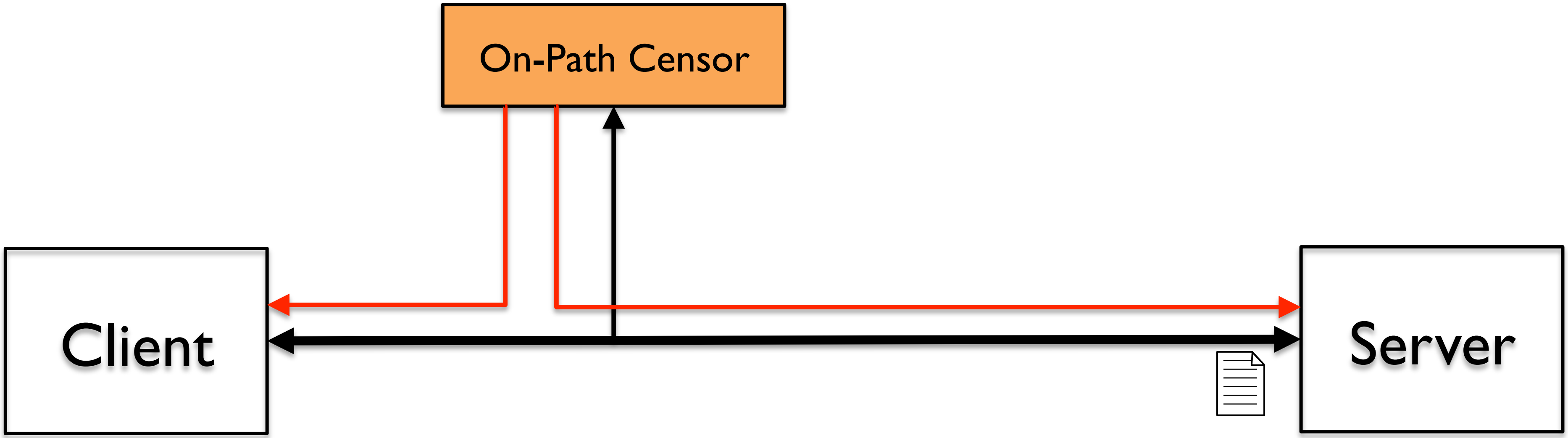
- On-Path device gets a copy of every packet
  - Packets are forwarded on before the on-path device can act (Wait, what?)
- Device can inject packets into the network
- This solves our speed problem
  - Why?
    - **We have a whole Round Trip Time (RTT) to make a decision (order milliseconds)**
    - In-path must make a decision in order microseconds!
- But what can we do if we've already forwarded the packet?

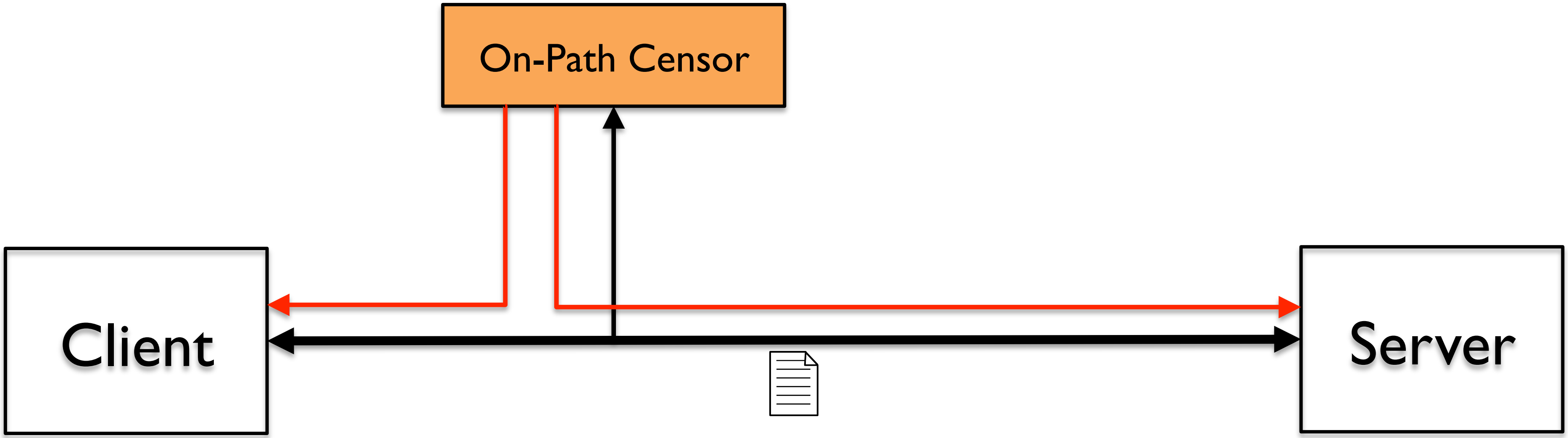

On-Path Censor
Client
Server

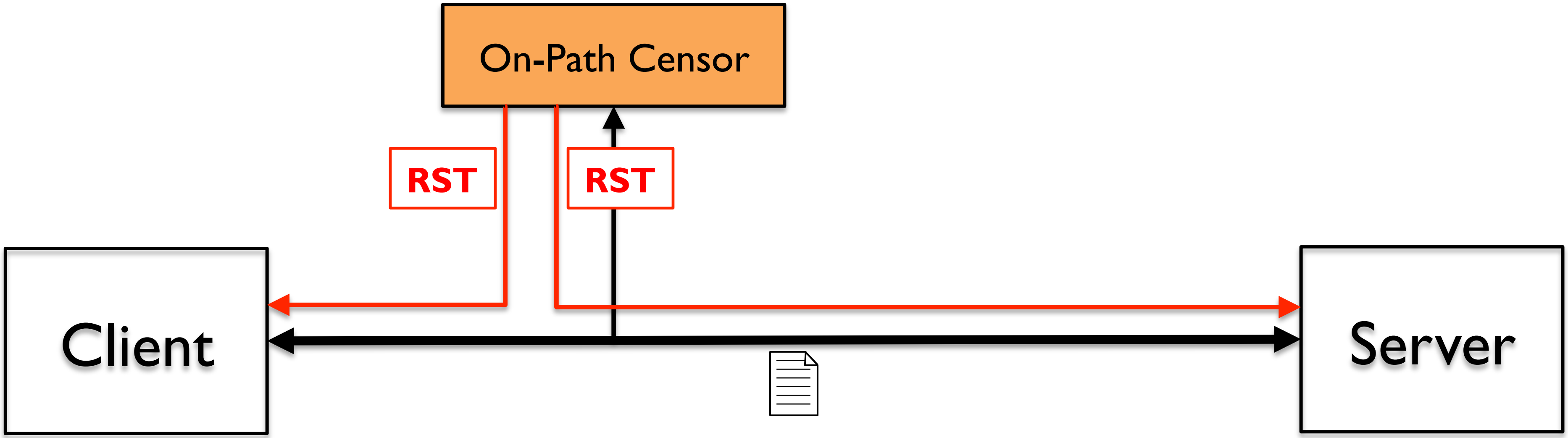

On-Path Censor
Client
Server

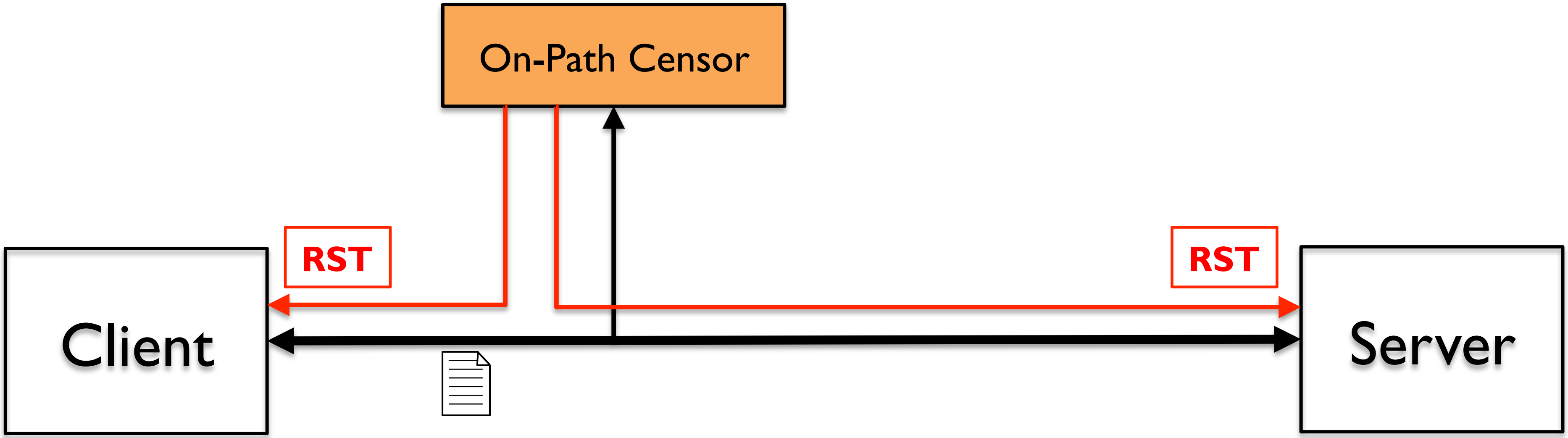

On-Path Censor
Client
Server

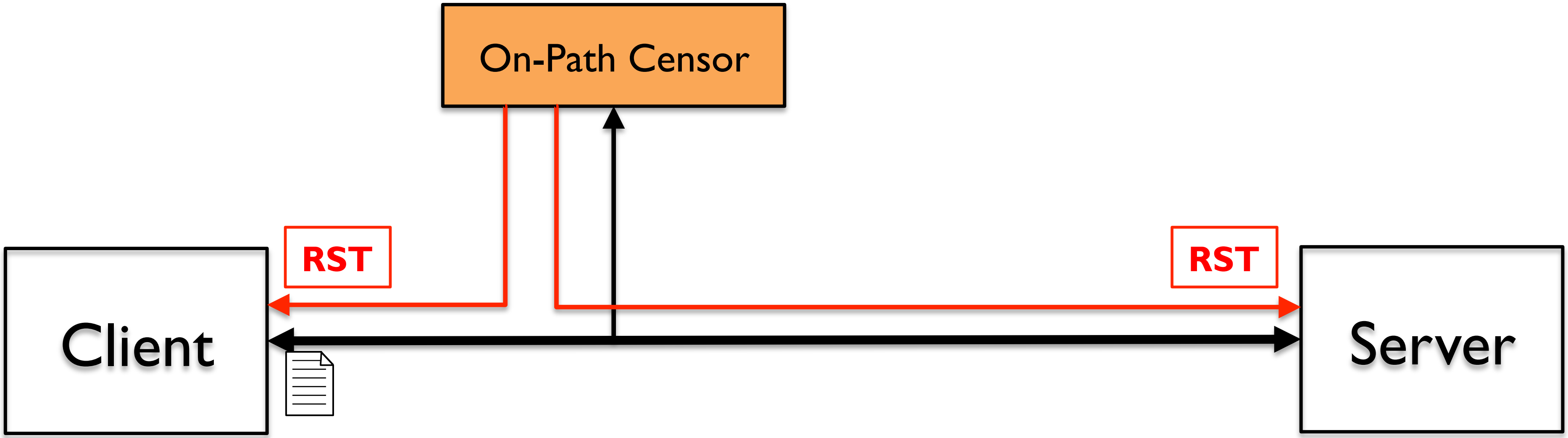

On-Path Censor
Client
Server

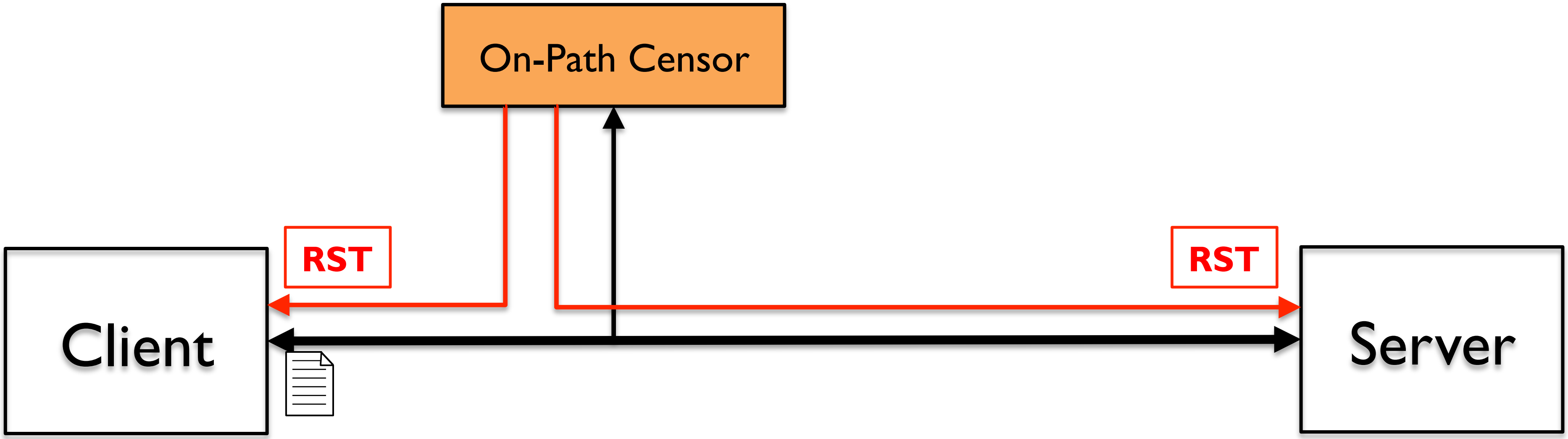

On-Path Censor
Client
Server


On-Path Censor
Client
Server


On-Path Censor
RST
RST
Client
Server


On-Path Censor
RST
RST
Client
Server

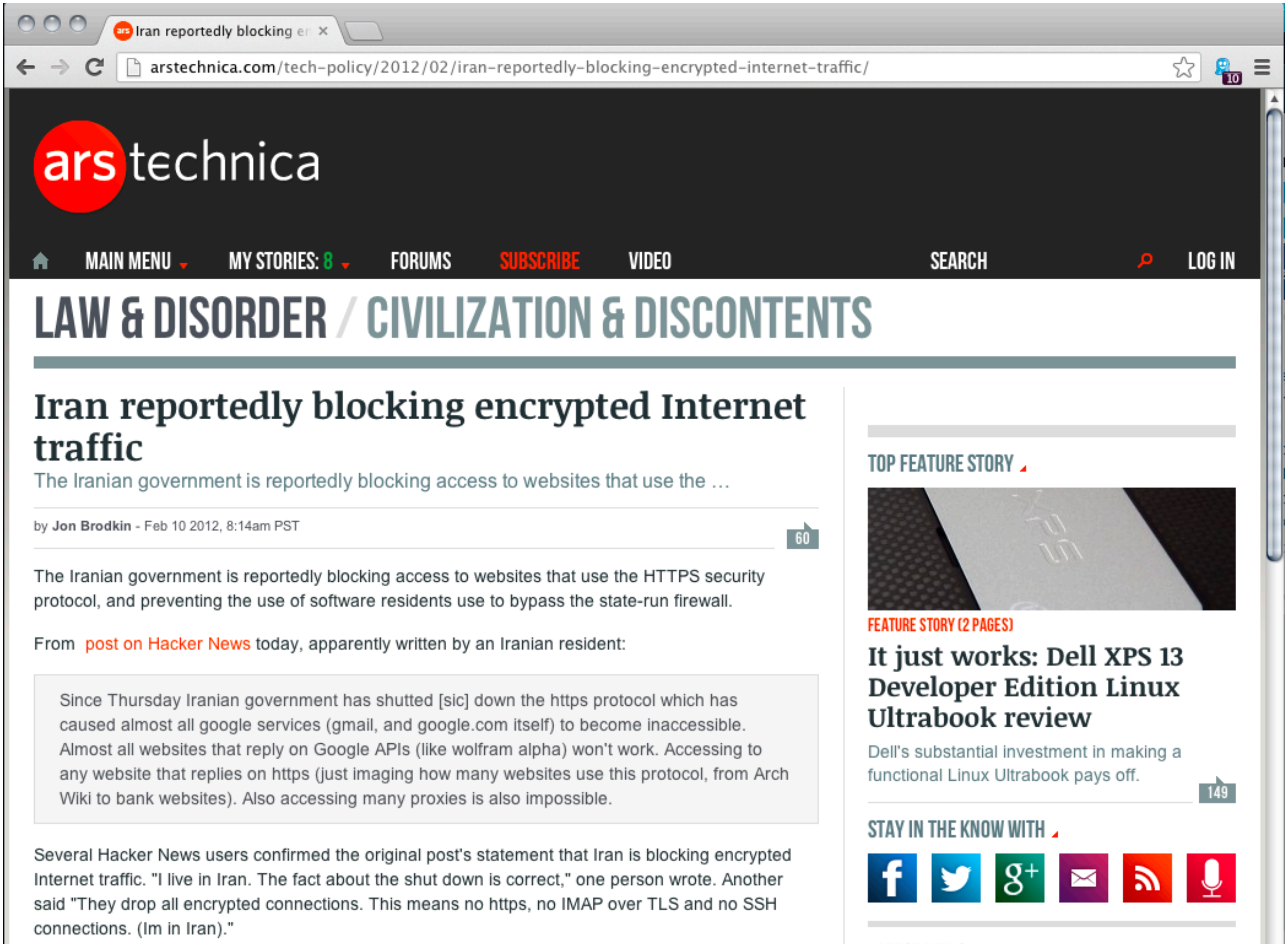

On-Path Censor
RST
RST
Client
Server



This is how the elements of the
Great Firewall of China
operate

Evasion

- Evading keyword filters
  - NIDS evasion techniques: TTLs, overlapping packets, etc (see lecture 4/11)
  - Is there something 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/
10
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

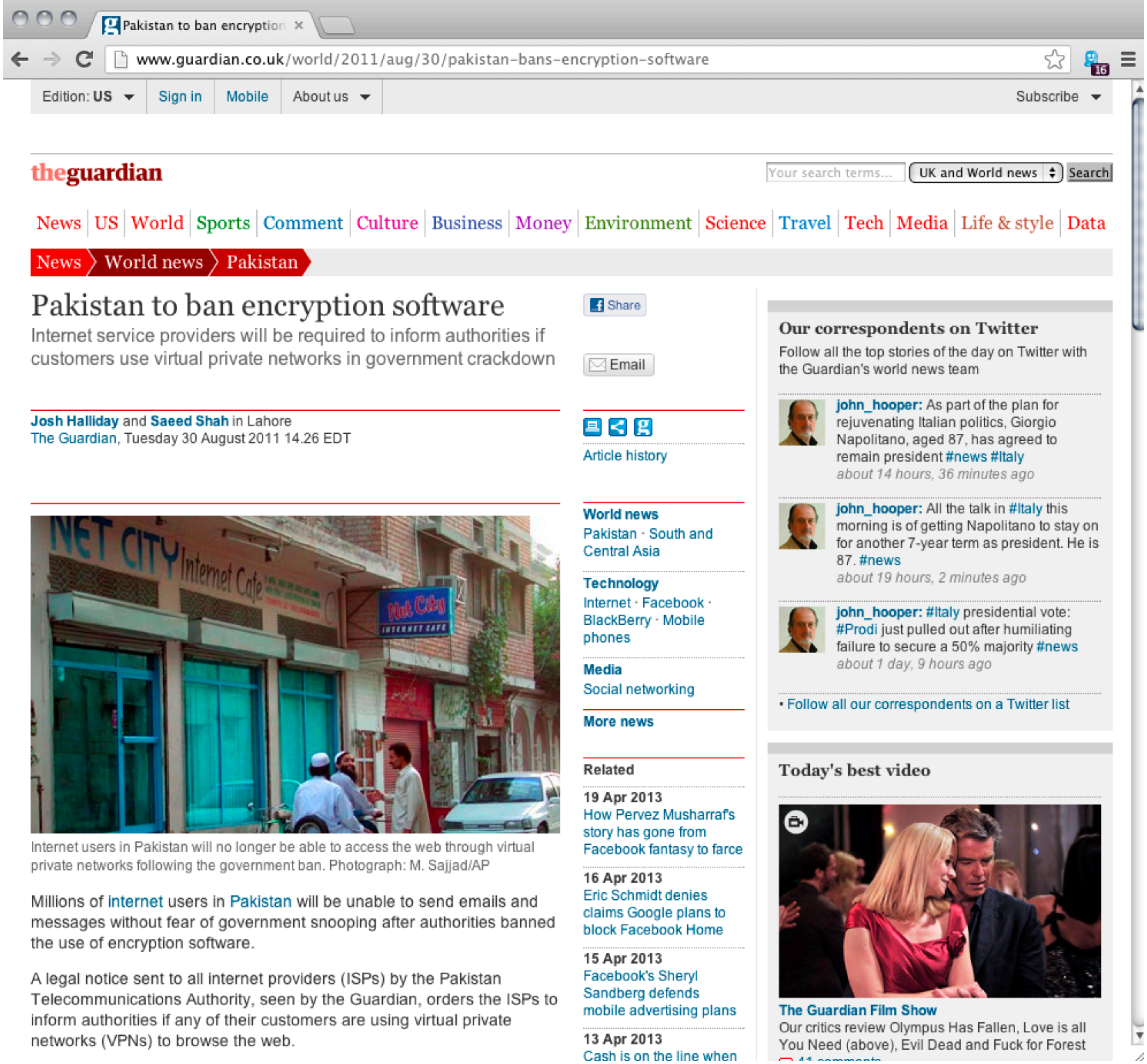
FEATURE STORY (2 PAGES)

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
www.guardian.co.uk/world/2011/aug/30/pakistan-bans-encryption-software
Edition: US
Sign in
Mobile
About us
Subscribe
theguardian
Your search terms...
UK and World news
Search
News | US | World | Sports | Comment | Culture | Business | Money | Environment | Science | Travel | Tech | Media | Life & style | Data
News
World news
Pakistan
Share
Email

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

NET CITY Internet Cafe
Net City
INTERNET CAFE

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 packets, etc (see lecture 4/11)
  - Is there something 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

THURSDAY, OCTOBER 15, 2009

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."

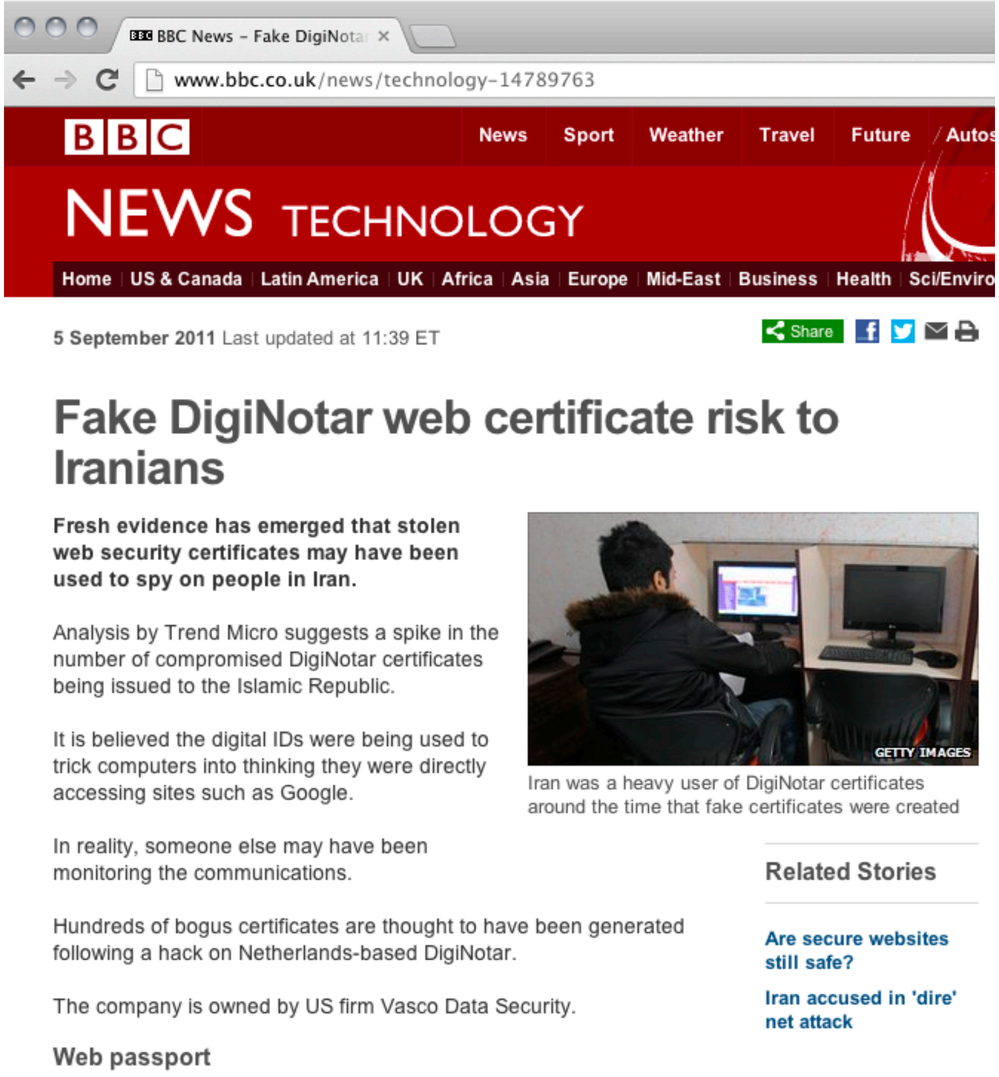
Tor is one of several systems that route data through intermediate computers called proxies, thereby circumventing government filters. To anyone watching Internet connections, the traffic then seems to be

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**
    - Constant arms race between Tor and censoring governments,
      - Great talk: https://www.youtube.com/watch?v=GwMr8XI7JMQ

Related Activity: Intelligence Gathering

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



5 September 2011 Last updated at 11:39 ET

Fake DigiNotar web certificate risk to Iranians

Fresh evidence has emerged that stolen web security certificates may have been used to spy on people in Iran.

Analysis by Trend Micro suggests a spike in the number of compromised DigiNotar certificates being issued to the Islamic Republic.

It is believed the digital IDs were being used to trick computers into thinking they were directly accessing sites such as Google.

In reality, someone else may have been monitoring the communications.

Hundreds of bogus certificates are thought to have been generated following a hack on Netherlands-based DigiNotar.

The company is owned by US firm Vasco Data Security.

Web passport

Iran was a heavy user of DigiNotar certificates around the time that fake certificates were created

Related Stories

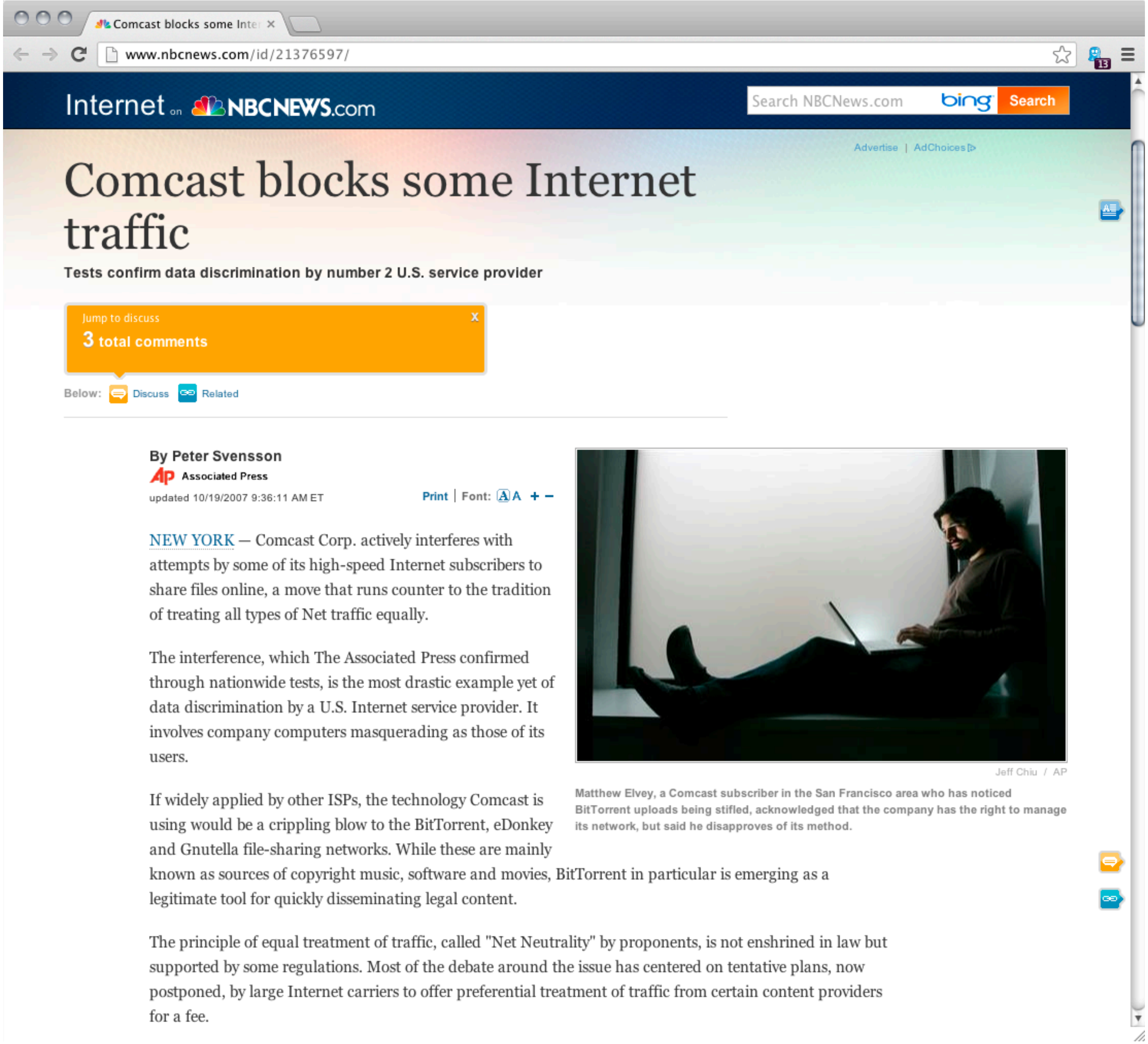
Are secure websites still safe?

Iran accused in 'dire' net attack

Net Neutrality

- Net Neutrality: The principle that network providers should treat all traffic equally
  - The corporate cousin of the censorship debate

- But why wouldn’t an ISP want to treat all traffic equally?



Comcast blocks some Internet traffic

Tests confirm data discrimination by number 2 U.S. service provider

By Peter Svensson
Associated Press
updated 10/19/2007 9:36:11 AM ET

NEW YORK — Comcast Corp. actively interferes with attempts by some of its high-speed Internet subscribers to share files online, a move that runs counter to the tradition of treating all types of Net traffic equally.

The interference, which The Associated Press confirmed through nationwide tests, is the most drastic example yet of data discrimination by a U.S. Internet service provider. It involves company computers masquerading as those of its users.

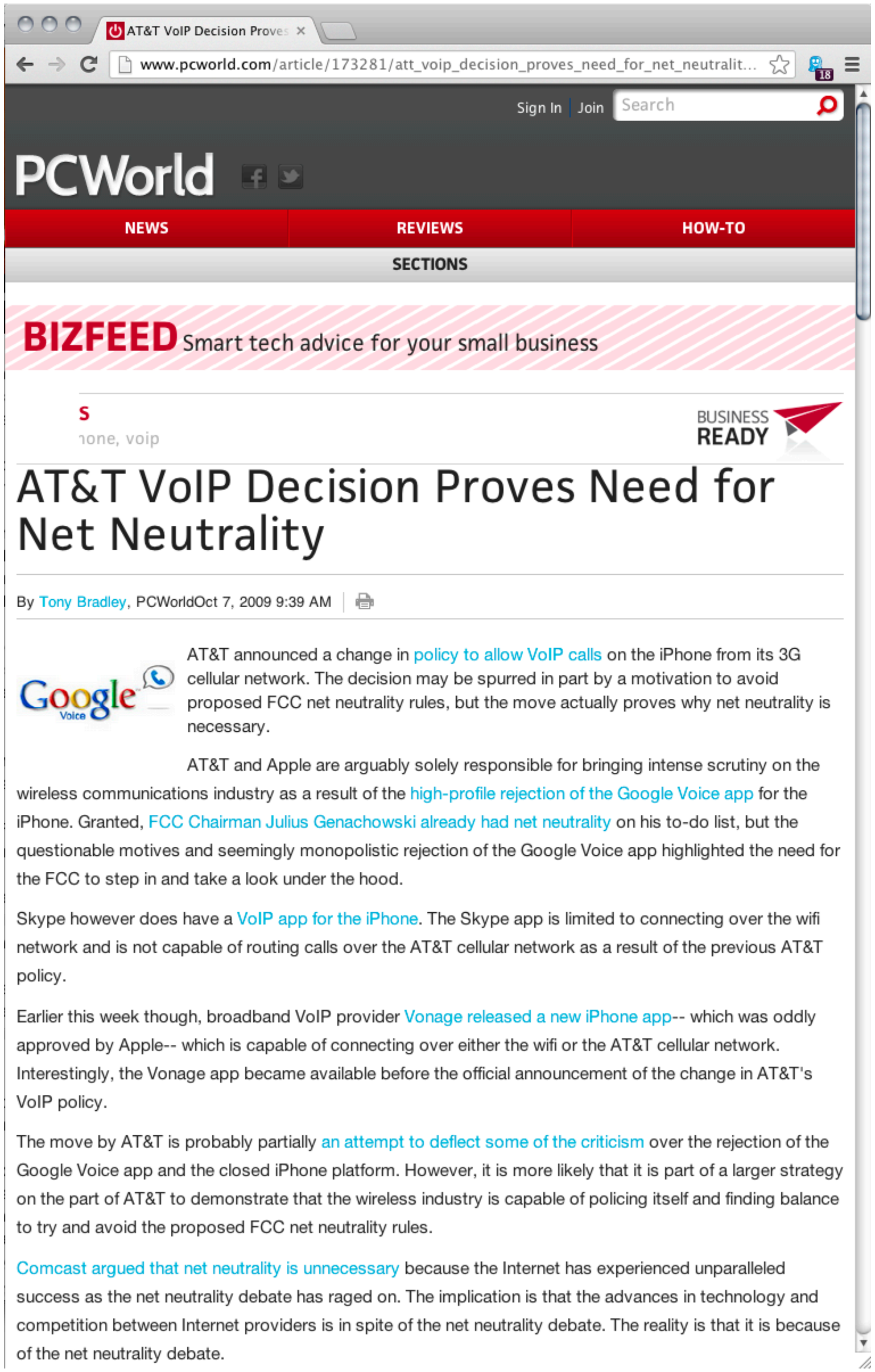
If widely applied by other ISPs, the technology Comcast is using would be a crippling blow to the BitTorrent, eDonkey and Gnutella file-sharing networks. While these are mainly known as sources of copyright music, software and movies, BitTorrent in particular is emerging as a legitimate tool for quickly disseminating legal content.

The principle of equal treatment of traffic, called "Net Neutrality" by proponents, is not enshrined in law but supported by some regulations. Most of the debate around the issue has centered on tentative plans, now postponed, by large Internet carriers to offer preferential treatment of traffic from certain content providers for a fee.

Jeff Chiu / AP

Matthew Elvey, a Comcast subscriber in the San Francisco area who has noticed BitTorrent uploads being stifled, acknowledged that the company has the right to manage its network, but said he disapproves of its method.

Why?


AT&T VoIP Decision Prove
www.pcworld.com/article/173281/att_voip_decision_proves_need_for_net_neutralit...
Sign In
Join
Search
PCWorld
NEWS
REVIEWS
HOW-TO
SECTIONS
BIZFEED Smart tech advice for your small business
S
ıone, voip
BUSINESS READY
Google Voice

AT&T VoIP Decision Proves Need for Net Neutrality

By Tony Bradley, PCWorldOct 7, 2009 9:39 AM

AT&T announced a change in policy to allow VoIP calls on the iPhone from its 3G cellular network. The decision may be spurred in part by a motivation to avoid proposed FCC net neutrality rules, but the move actually proves why net neutrality is necessary.

AT&T and Apple are arguably solely responsible for bringing intense scrutiny on the wireless communications industry as a result of the high-profile rejection of the Google Voice app for the iPhone. Granted, FCC Chairman Julius Genachowski already had net neutrality on his to-do list, but the questionable motives and seemingly monopolistic rejection of the Google Voice app highlighted the need for the FCC to step in and take a look under the hood.

Skype however does have a VoIP app for the iPhone. The Skype app is limited to connecting over the wifi network and is not capable of routing calls over the AT&T cellular network as a result of the previous AT&T policy.

Earlier this week though, broadband VoIP provider Vonage released a new iPhone app-- which was oddly approved by Apple-- which is capable of connecting over either the wifi or the AT&T cellular network. Interestingly, the Vonage app became available before the official announcement of the change in AT&T's VoIP policy.

The move by AT&T is probably partially an attempt to deflect some of the criticism over the rejection of the Google Voice app and the closed iPhone platform. However, it is more likely that it is part of a larger strategy on the part of AT&T to demonstrate that the wireless industry is capable of policing itself and finding balance to try and avoid the proposed FCC net neutrality rules.

Comcast argued that net neutrality is unnecessary because the Internet has experienced unparalleled success as the net neutrality debate has raged on. The implication is that the advances in technology and competition between Internet providers is in spite of the net neutrality debate. The reality is that it is because of the net neutrality debate.

Why?

Net Neutrality

- Core idea: Is an ISP selling you a pipe, or do they get a say in what goes over it?
  - **Network Commoditization**
- Pro:
  - Stifles innovation and competition
  - Preserves existing freedoms
  - End to end principle
- Con:
  - Prevents optimizing network performance
  - Commoditization → worse performance

- **What do you think?**

Reminder:
I have OH right after this, 751
Soda