

CNT 5412, SPRING 2025

INTRODUCTION

VIET TUNG HOANG

Some slides are based on material from Prof. Stefano Tessaro
(University of Washington) and Prof. Dan Boneh (Stanford)

Agenda

1. The Internet & Its Problems

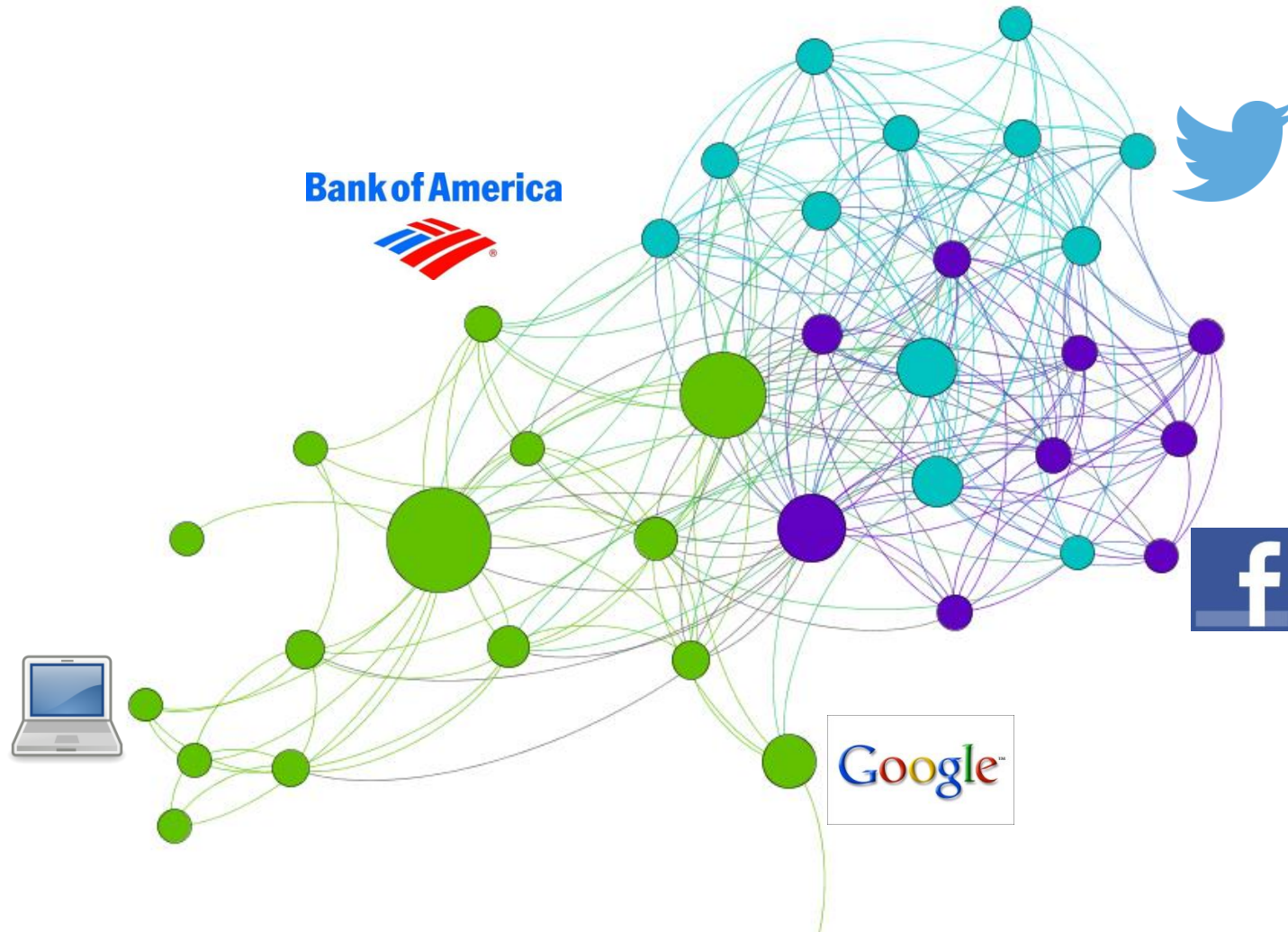
2. HTTP Issues

3. IP Issues

4. Privacy Issue

The Internet

Global network that provides **best-effort delivery** of packets between connected hosts



OSI Layer Model

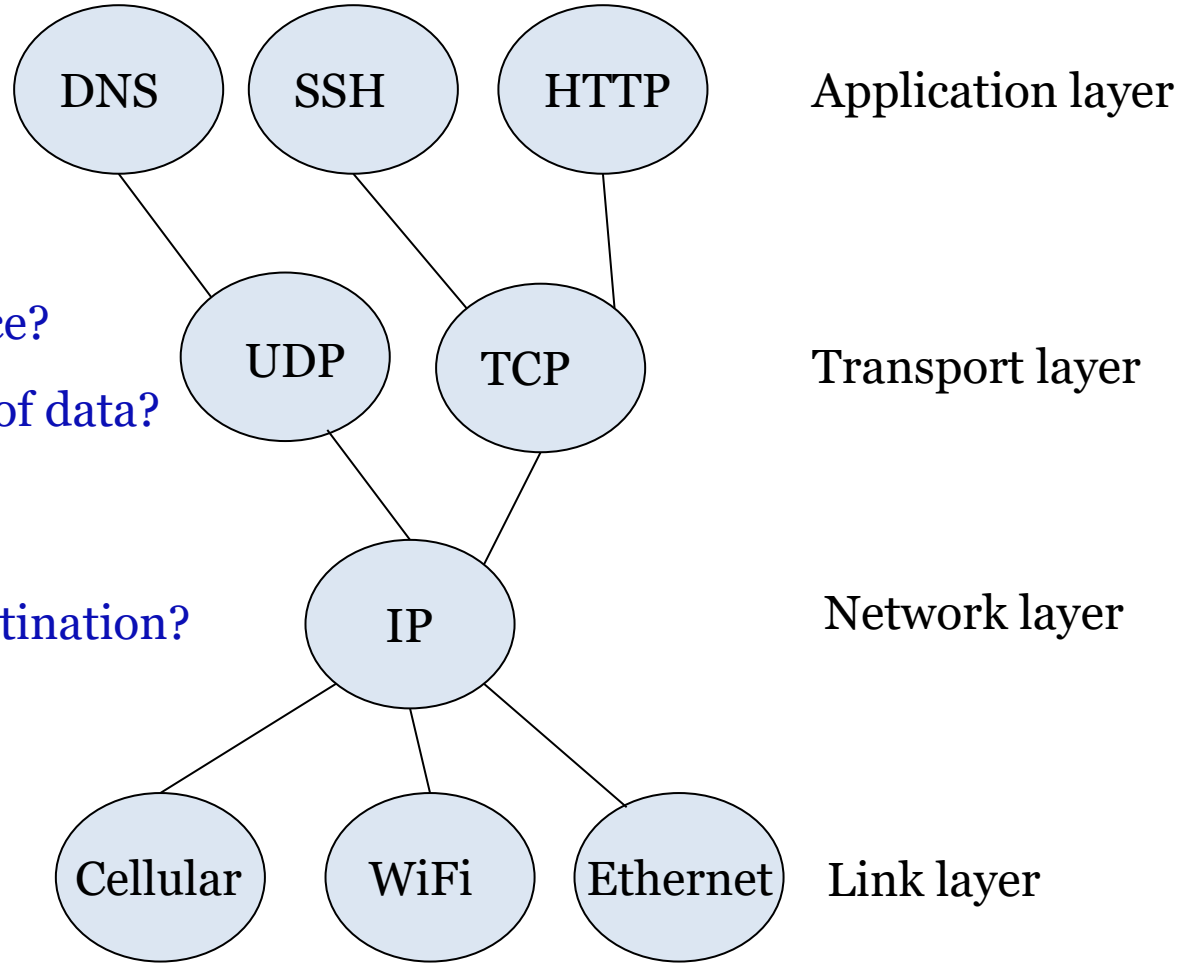
How does Application structure data?

How do I get to the right service?

How to have a reliable stream of data?

How a packet get to a final destination?

How to get to the next hop?



IT'S BACK —

Linux has a serious security problem that once again enables DNS cache poisoning

DNS bug

Bizarre behavior overlooked in Linux for more than a decade revives scary attack scenario.

DAN GOODIN - 11/17/2021, 8:36 AM

Oct 13, 2020

MICROSOFT FIXES PING OF DEATH FLAW IN WINDOWS

TCP/IP bug

By Dennis Fisher

2010
REPORT TO CONGRESS
of the
U.S.-CHINA ECONOMIC AND
SECURITY REVIEW COMMISSION



Interception of Internet Traffic

For a brief period in April 2010, a state-owned Chinese telecommunications firm “hijacked” massive volumes of Internet traffic.*¹¹⁴ Evidence related to this incident does not clearly indicate whether it was perpetrated by the firm. However, computer security vulnerabilities could enable se

The New York Times



The Lede

The New York Times News Blog

Pakistan Blamed for Worldwide YouTube Break

By MIKE NIZZA FEBRUARY 25, 2008 9:34 AM

If all had gone according to plan, Pakistan would have been the latest government taking part in an unsettling trend [from Brazil to Thailand](#): YouTube blocking. Unlike its predecessors, though, Pakistan also affected thousands of people beyond its borders

Routing bugs

Crypto bugs

ars TECHNICA

[BIZ & IT](#) [TECH](#) [SCIENCE](#) [POLICY](#) [CARS](#) [GAMING & CULTURE](#) [STORE](#) [FORUMS](#)

BIZ & IT —

Meaner POODLE bug that bypasses TLS crypto bites 10 percent of websites

Some of the world's leading sites are vulnerable to an easier, more simplified attack.

DAN GOODIN - 12/8/2014, 7:01 PM

ROBERT MCMILLAN

BUSINESS APR 11, 2014 6:30 AM

How Heartbleed Broke the Internet — And Why It Can Happen Again

It's no surprise that a small bug could cause such huge problems. What's amazing, however, is that the code that contained this bug was overseen by only one full-time paid employee.

PCWorld

[NEWS](#) [BEST PICKS](#) [REVIEWS](#) [HOW-TO](#) [DEALS](#) [LAPTOPS](#) [WINDOWS](#) [SECURITY](#)

UPDATED

KRACK Wi-Fi attack threatens all networks: How to stay safe and what you need to know

Update all the things.

By Brad Chacos and Michael Simon

PCWorld | NOV 8, 2017 7:27 AM PST

Agenda

1. The Internet & Its Problems

2. HTTP Issues

3. IP Issues

4. Privacy Issues

HTTP Issues

Was not designed with security



Privacy issue: Adversary can read Alice's emails

HTTP Issues

Was not designed with security



You have a raise



You're fired



Authenticity issue: Adversary can modify Alice's emails

HTTP Issues

Was not designed with security



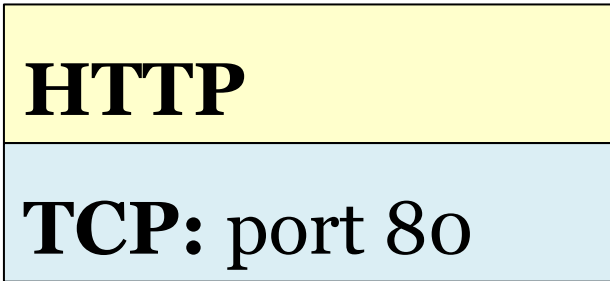
I'm Gmail



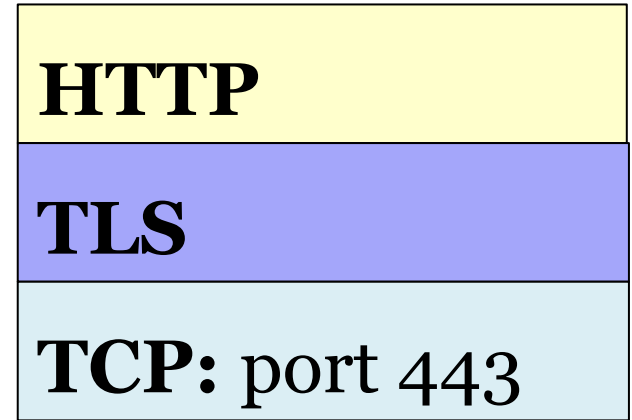
Impersonation: Adversary can pretend to be Gmail

The Fix: HTTPS

Standard HTTP



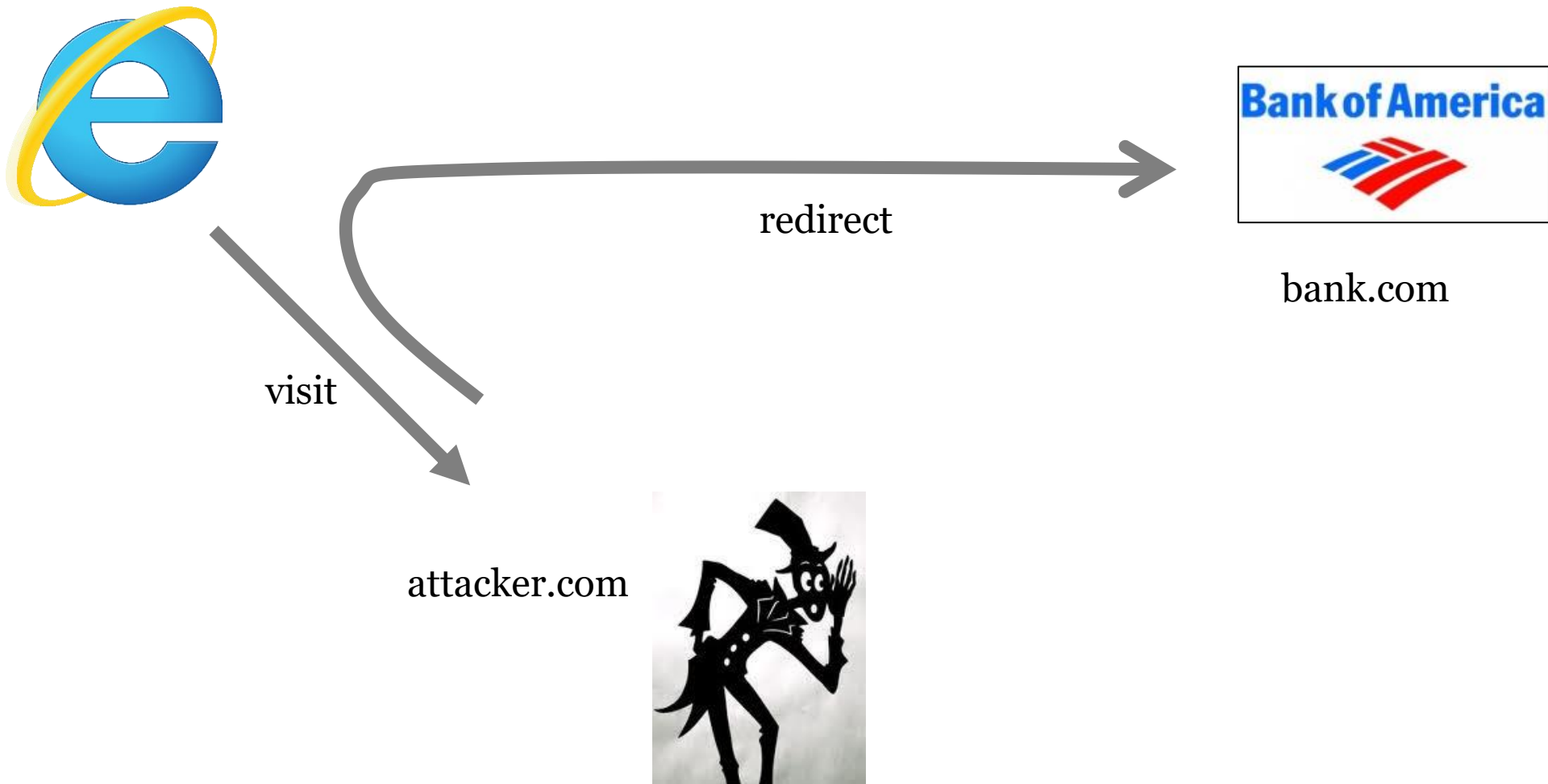
HTTPS



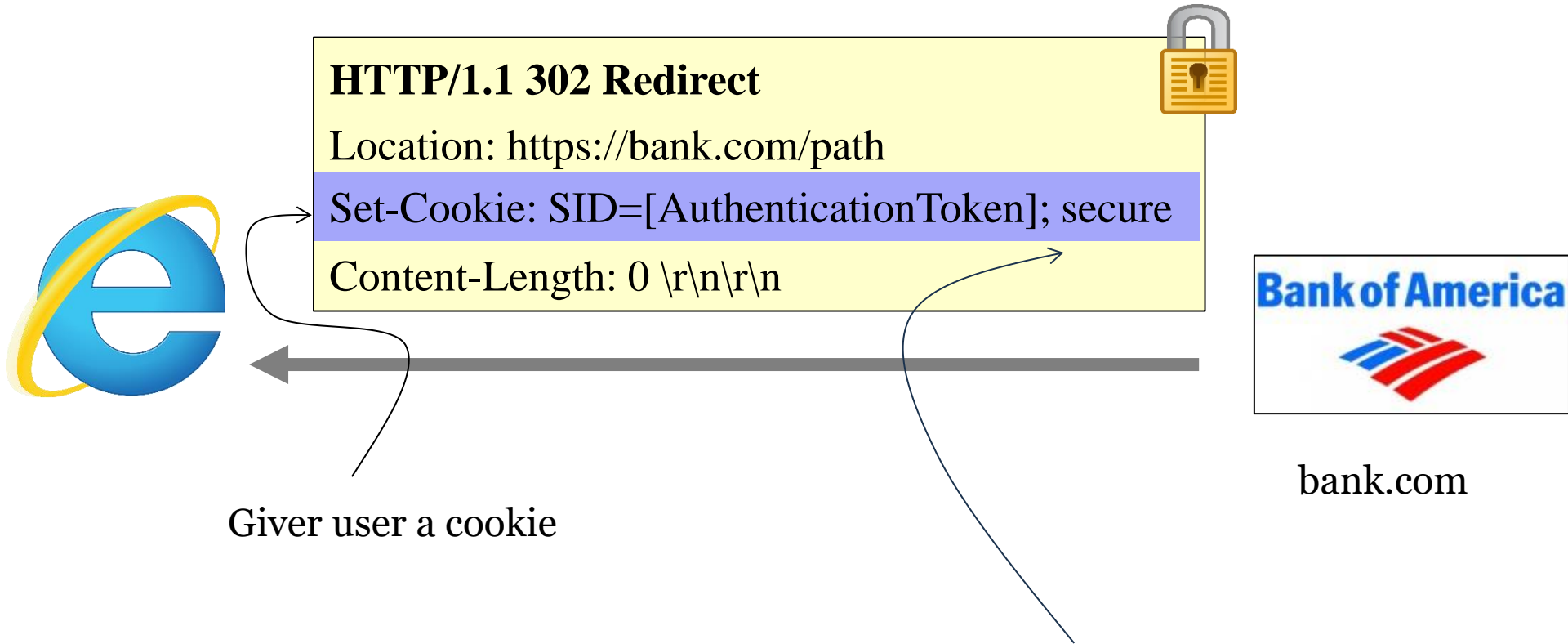
TLS encrypts and authenticates HTTP data

No change to HTTP itself

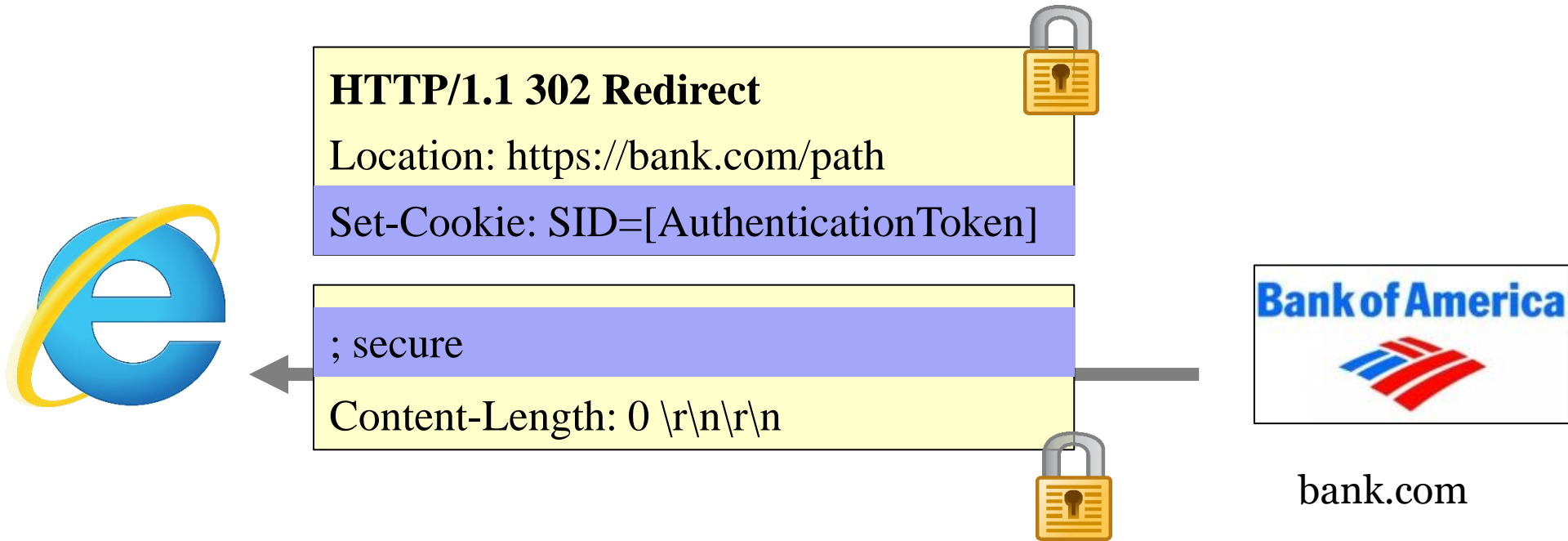
Cookie Cutter Attack on TLS



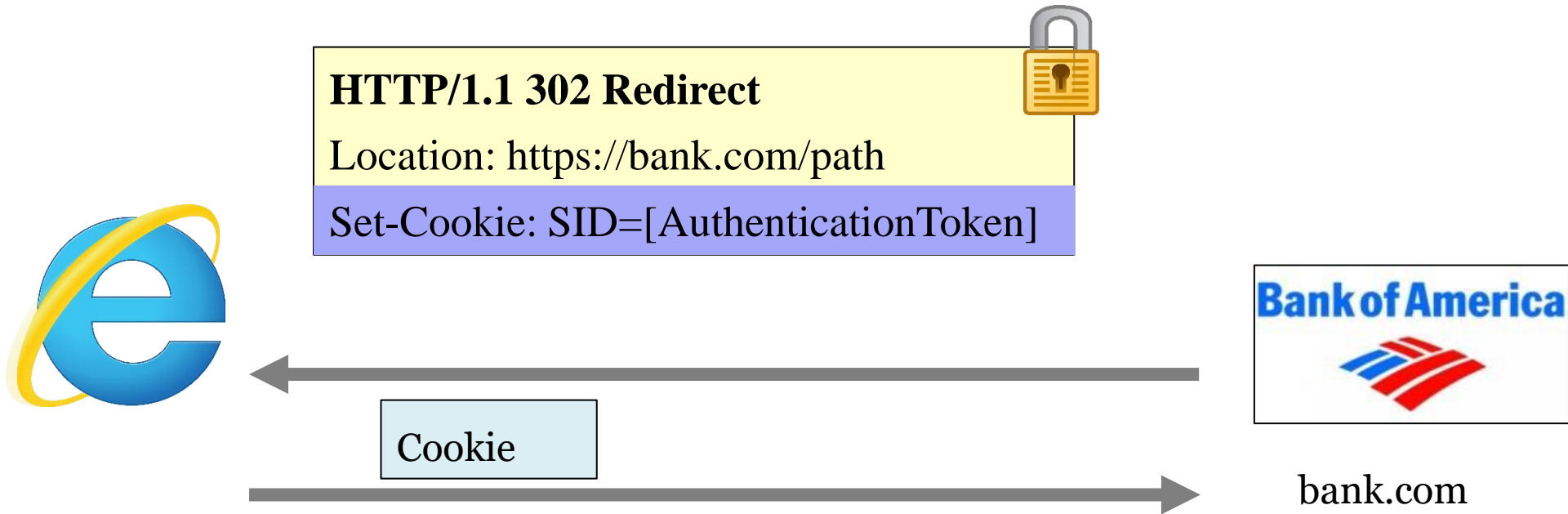
Cookie Cutter Attack on TLS



Message Is Split If URL Path Is Too Long



What Happens If Second Frame Is Blocked?



Cookie is sent in the clear via standard HTTP



Agenda

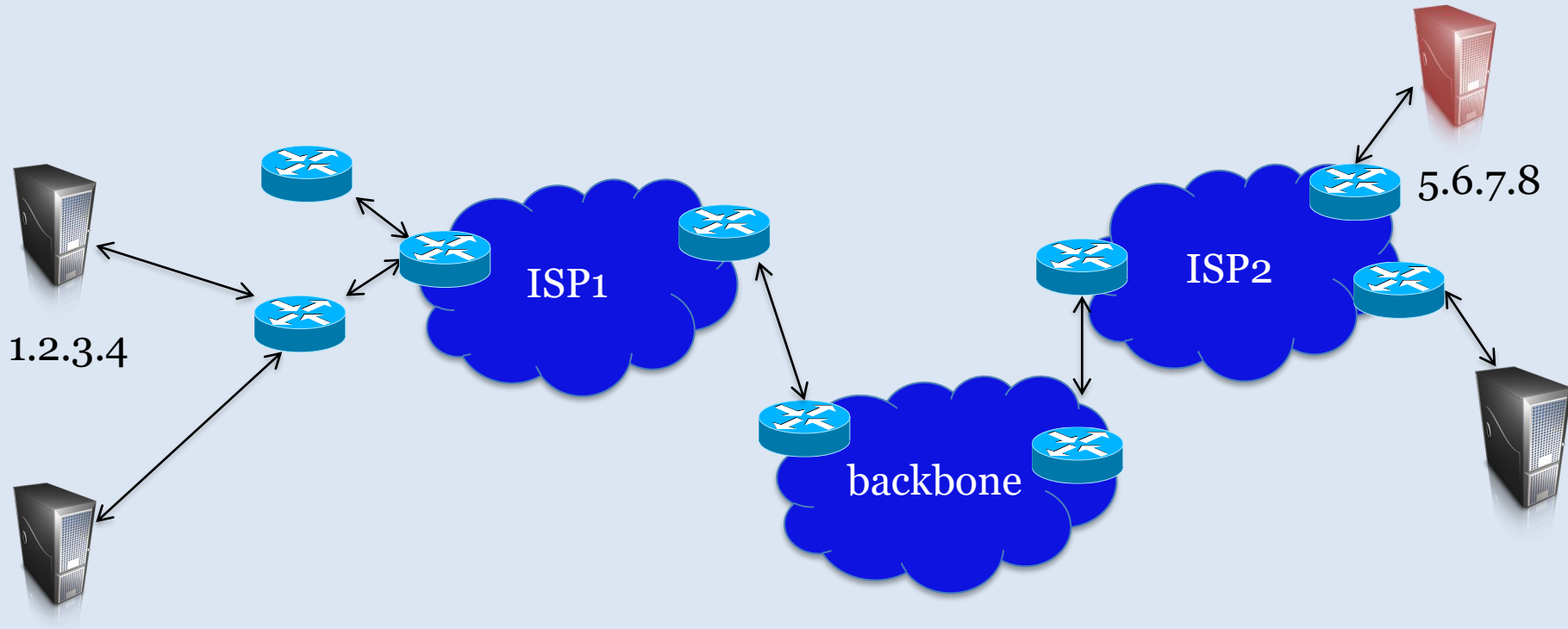
1. The Internet & Its Problems

2. HTTP Issues

3. IP Issues

4. Privacy Issues

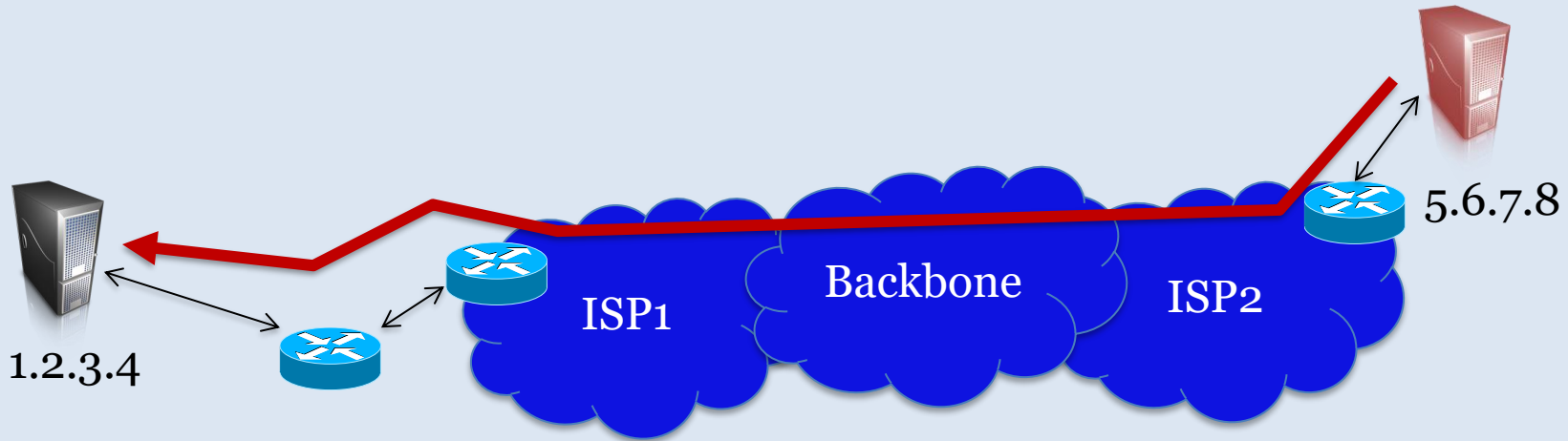
Security Issues with IP



Anyone can talk to any one

No source address authentication in general (spoofing)

Denial of Service (DoS) Attacks



Goal: prevent legitimate users from accessing victim (1.2.3.4)

Example: ICMP ping flood

ICMP = Internet Control Message Protocol, used to relay control/error/ diagnostic message, on top of IP

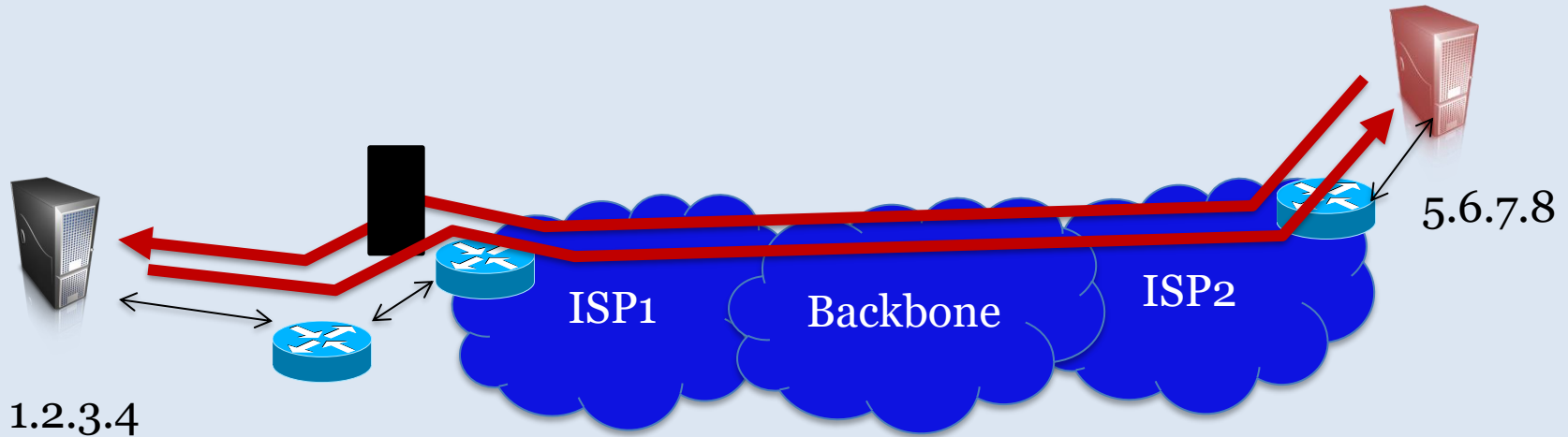
```
$ ping www.example.com
PING www.example.com (93.184.216.119): 56 data bytes
64 bytes from 93.184.216.119: icmp_seq=0 ttl=56 time=11.632 ms
64 bytes from 93.184.216.119: icmp_seq=1 ttl=56 time=11.726 ms
64 bytes from 93.184.216.119: icmp_seq=2 ttl=56 time=10.683 ms
64 bytes from 93.184.216.119: icmp_seq=3 ttl=56 time=9.674 ms

--- www.example.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 9.674/10.929/11.726/0.831 ms
```

Send ICMP “ping” message

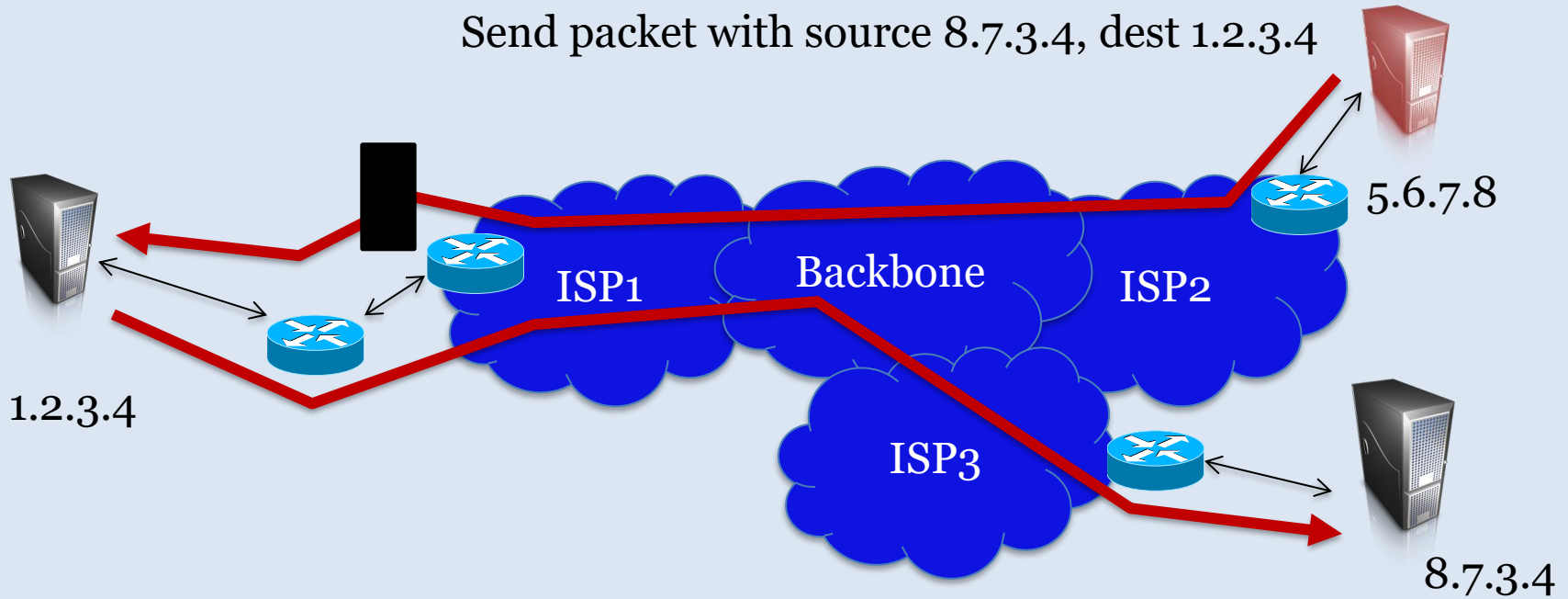
- Host must respond to all ping requests with a pong reply containing the exact data received in the request message.

A Possible DoS Attack: ICMP Ping Flood



- Attacker sends ICMP pings as fast as possible to victim
- When will this work as a DoS? **Attacker resources > victim's**
- How can this be prevented? **Ingress filtering near victim**

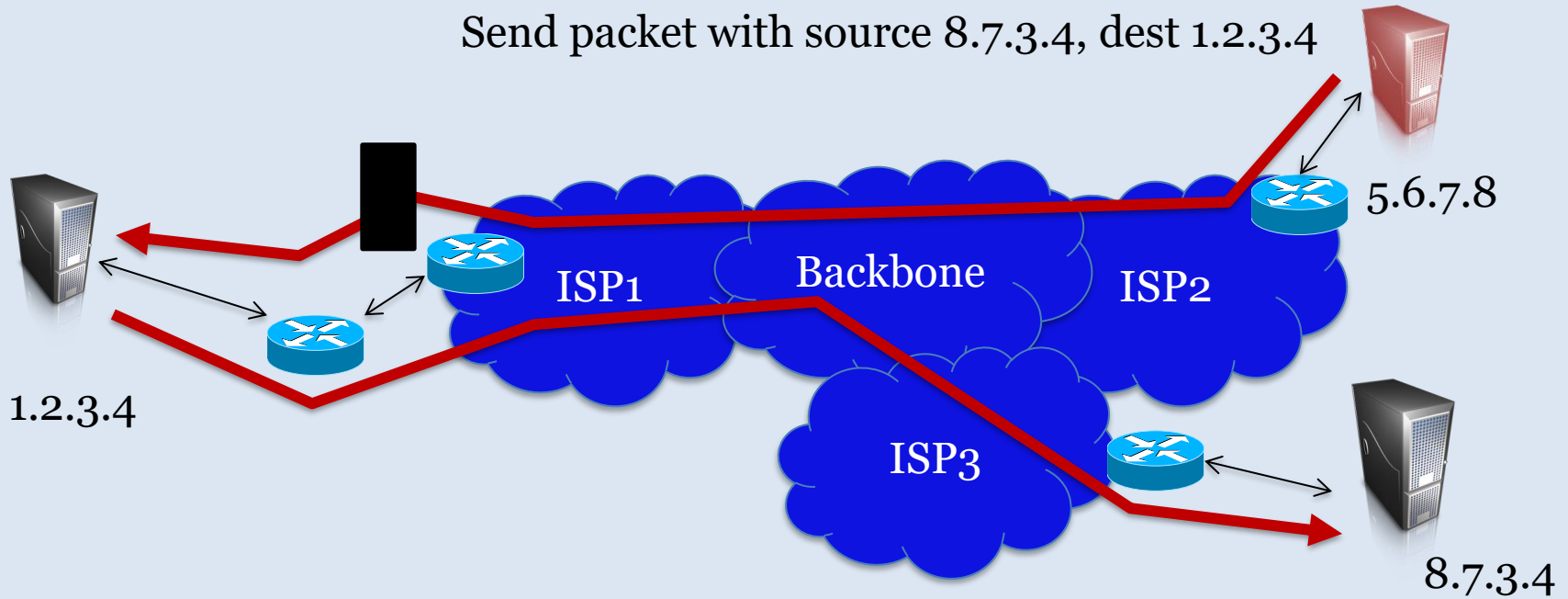
How Can Attacker Avoid Ingress Filtering?



Send packet with fake source IP

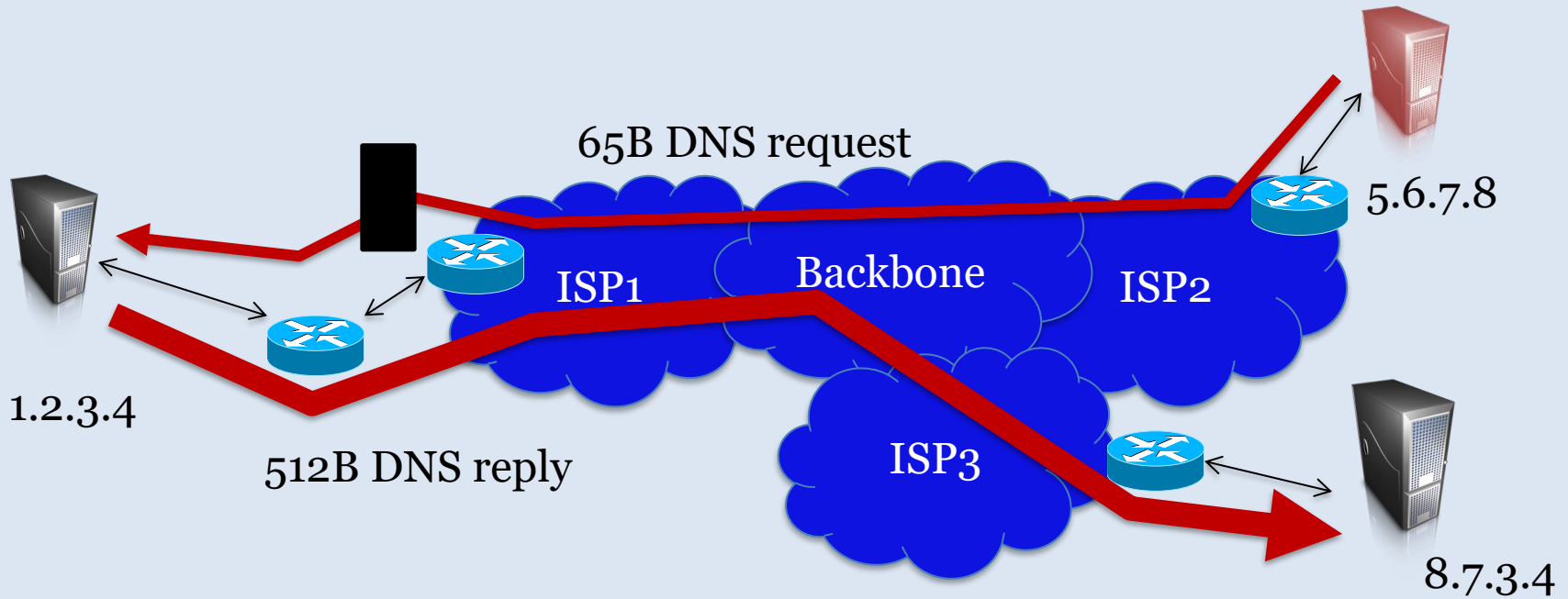
Packet will get routed correctly, but replies will not

DoS Reflection Attacks



Attacker can attack 8.7.3.4 by bouncing packets from 1.2.3.4
“Frame” 1.2.3.4

DoS Amplification Attacks



DNS works better if attacker spends much less resource than the victim

Another Issue of IP



IP packets are sent in the clear, leading to privacy and authenticity issues

A Solution: IPSec

Alice's gateway
1.2.3.4



Bob's gateway
5.6.7.8



Source: Alice

Dest: Bob

Payload

IP packet



A Solution: IPSec

Alice's gateway
1.2.3.4



Bob's gateway
5.6.7.8



Source: 1.2.3.4

Dest: 5.6.7.8

IPSec header

Encrypted IP packet



A Solution: IPSec

Alice's gateway
1.2.3.4



In Hw4 you'll break IPSec (for some configuration choice)



Bob's gateway
5.6.7.8



Source: Alice
Dest: Bob

Payload



Agenda

1. The Internet & Its Problems

2. HTTP Issues

3. IP Issues

4. Privacy Issues

The End Of Privacy

FORBES > TECH

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill Former Staff

Welcome to The Not-So Private Par

ASIA & PACIFIC

China's scary lesson to the world: Censoring the Internet works



By [Simon Denyer](#)

May 23, 2016 at 3:01 p.m. EDT

Associated Press

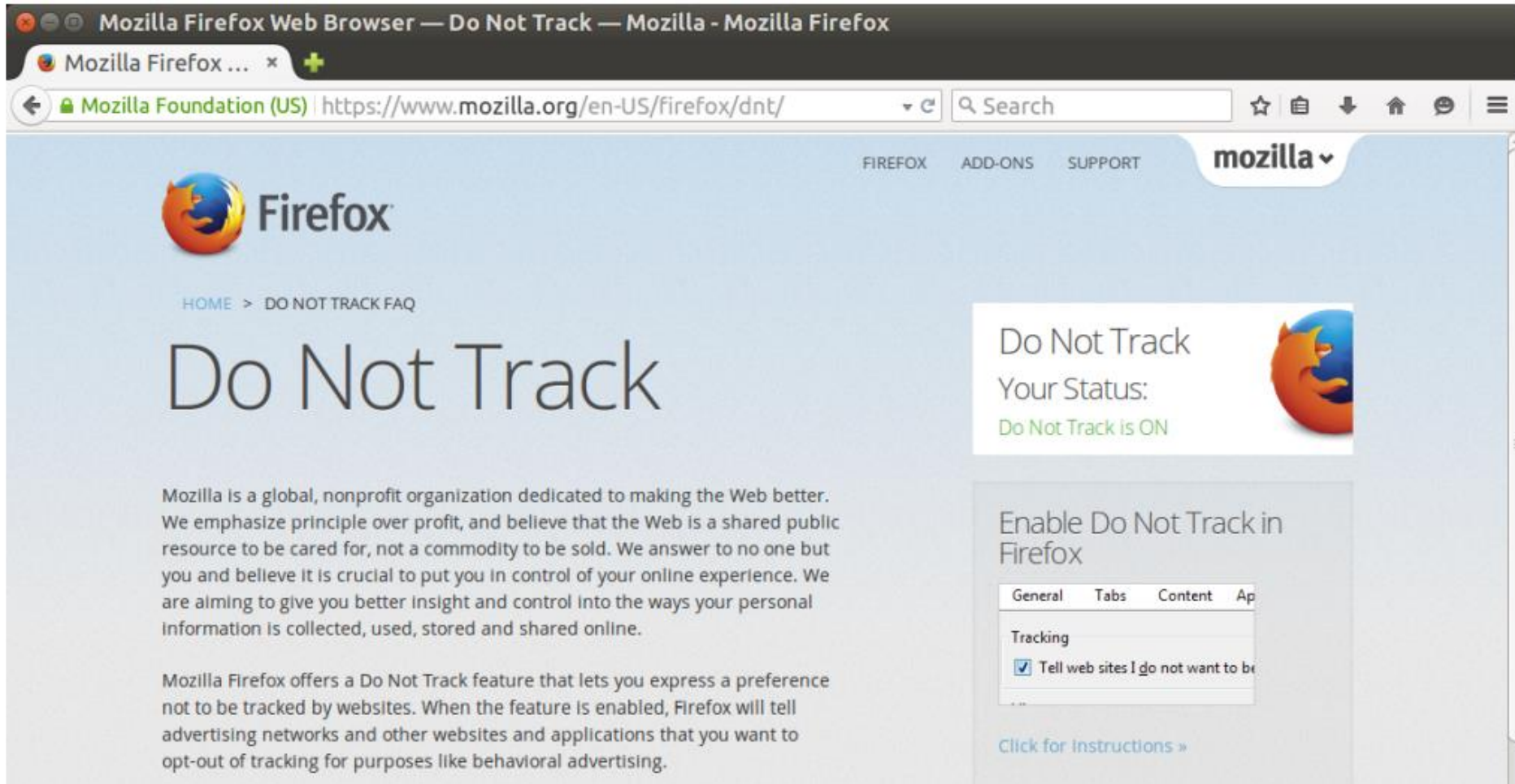
Sat 3 May 2014 01:27 EDT

**The
Guardian**
News website of the year

Everyone is under surveillance now, says whistleblower Edward Snowden

People's privacy is violated without any suspicion of wrongdoing, former National Security Agency contractor claims

Stop Third-Party Tracking




The screenshot shows the Mozilla Firefox Web Browser interface. The address bar displays the URL <https://www.mozilla.org/en-US/firefox/dnt/>. The page title is "Do Not Track". The main content area features the Firefox logo and the heading "Do Not Track". Below the heading, there is a paragraph explaining Mozilla's commitment to privacy and a section titled "Enable Do Not Track in Firefox" with a checkbox for "Tell web sites I do not want to be tracked" which is checked.

Mozilla Firefox Web Browser — Do Not Track — Mozilla - Mozilla Firefox

Mozilla Firefox ... x +

← Mozilla Foundation (US) | <https://www.mozilla.org/en-US/firefox/dnt/> 🔍 Search ☆ 📄 ⬇️ 🏠 🗨️ ☰

FIREFOX ADD-ONS SUPPORT mozilla ▾

 **Firefox**

HOME > DO NOT TRACK FAQ


Do Not Track

Mozilla is a global, nonprofit organization dedicated to making the Web better. We emphasize principle over profit, and believe that the Web is a shared public resource to be cared for, not a commodity to be sold. We answer to no one but you and believe it is crucial to put you in control of your online experience. We are aiming to give you better insight and control into the ways your personal information is collected, used, stored and shared online.

Mozilla Firefox offers a Do Not Track feature that lets you express a preference not to be tracked by websites. When the feature is enabled, Firefox will tell advertising networks and other websites and applications that you want to opt-out of tracking for purposes like behavioral advertising.

Do Not Track

Your Status:
Do Not Track is ON



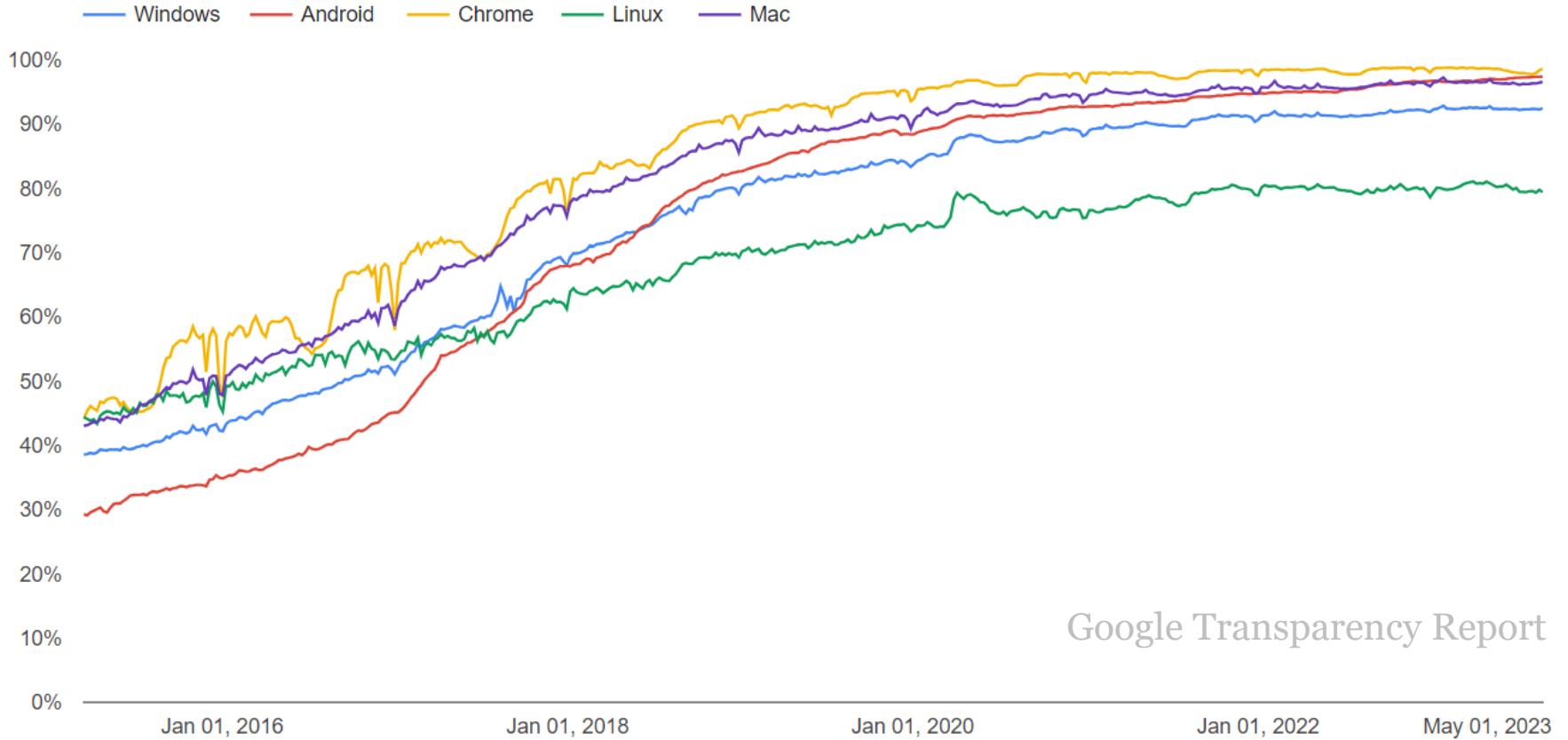
Enable Do Not Track in Firefox

General	Tabs	Content	Ap
Tracking			
<input checked="" type="checkbox"/> Tell web sites I do not want to be			

[Click for instructions »](#)

Protect Content Of Your Web Surfing: HTTPS

Chrome Page Loads over HTTPS



But HTTPS Doesn't Protect Metadata



Big Brother knows Alice sent an encrypted message to Human Rights Watch

Naïve Approach To Protect Metadata: VPN



Naïve Approach To Protect Metadata: VPN

Newsletters

The Atlantic

TECHNOLOGY

LulzSec Hacker Exposed by the Service He Thought Would Hide Him

Hidemyass.com didn't, gave details on hacker to investigators instead

By Adam Martin

The  Register

This article is more than 1 year old

HideMyAss defends role in LulzSec hack arrest

Anons vow to give ass-hiders a hiding

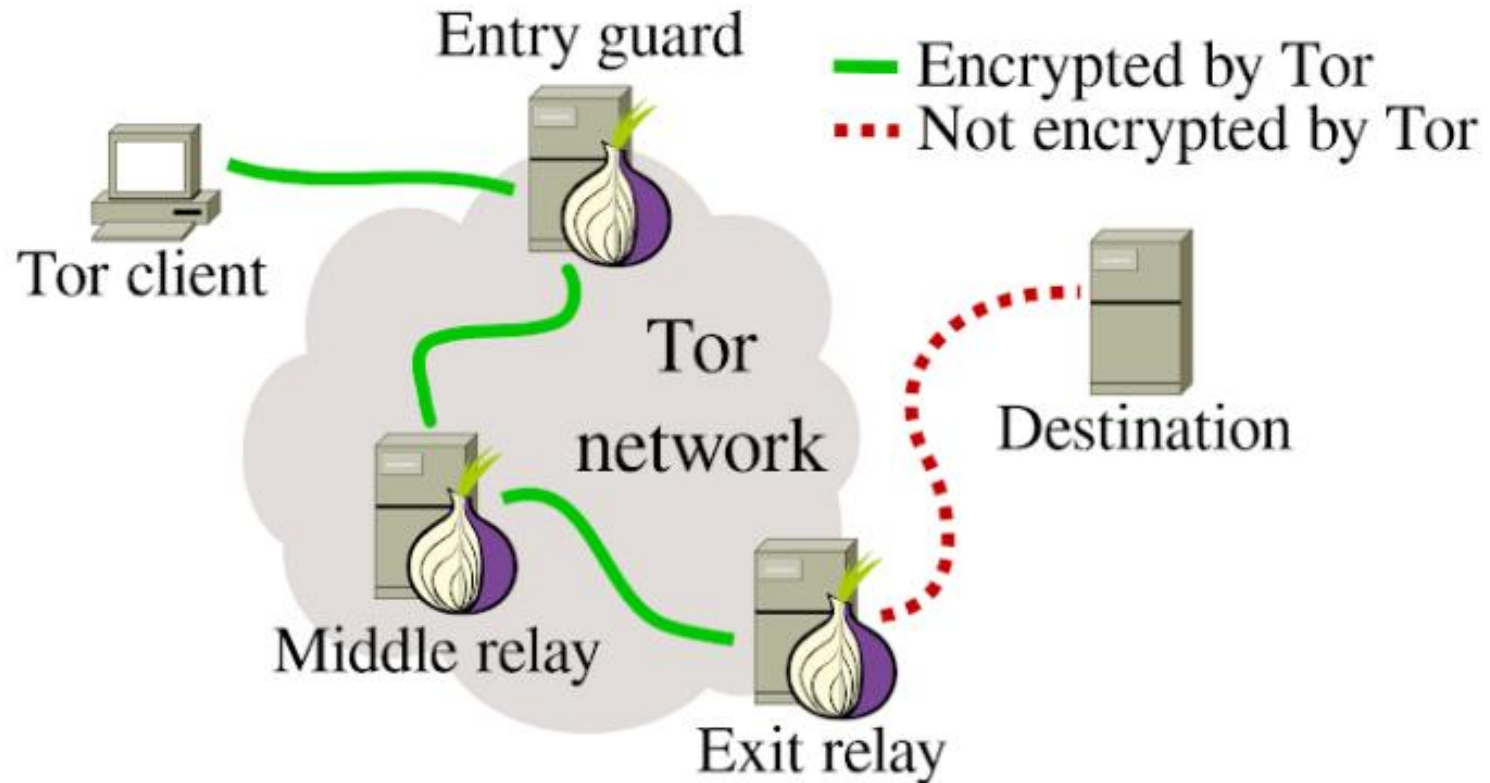
 [John Leyden](#)

Mon 26 Sep 2011 // 13:27 UTC

“As a legitimate company we will cooperate with law enforcement if we receive a court order”

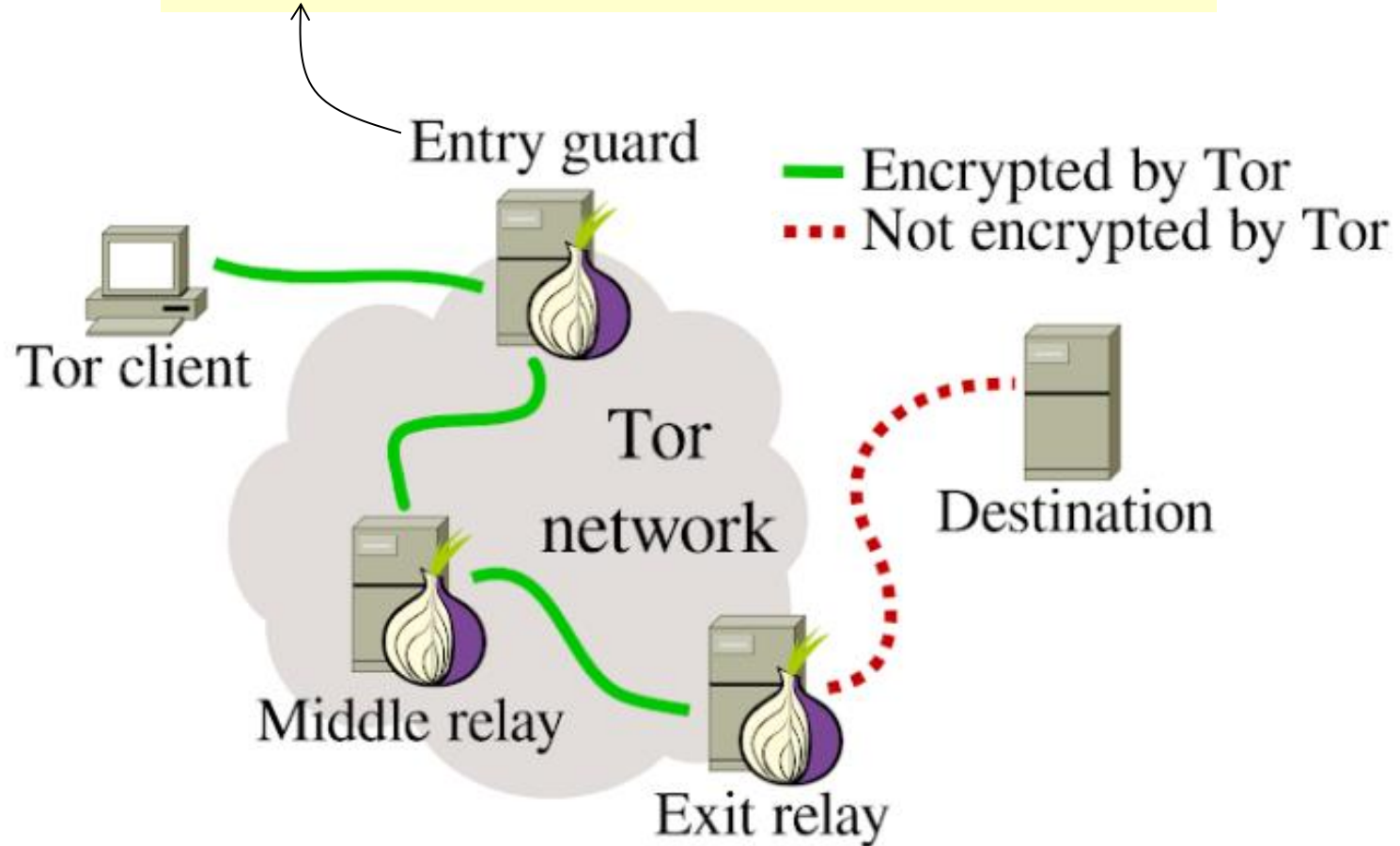
Tor (“The Onion Router”)

Tor operates by tunnelling traffic through three **random** “onion routers”

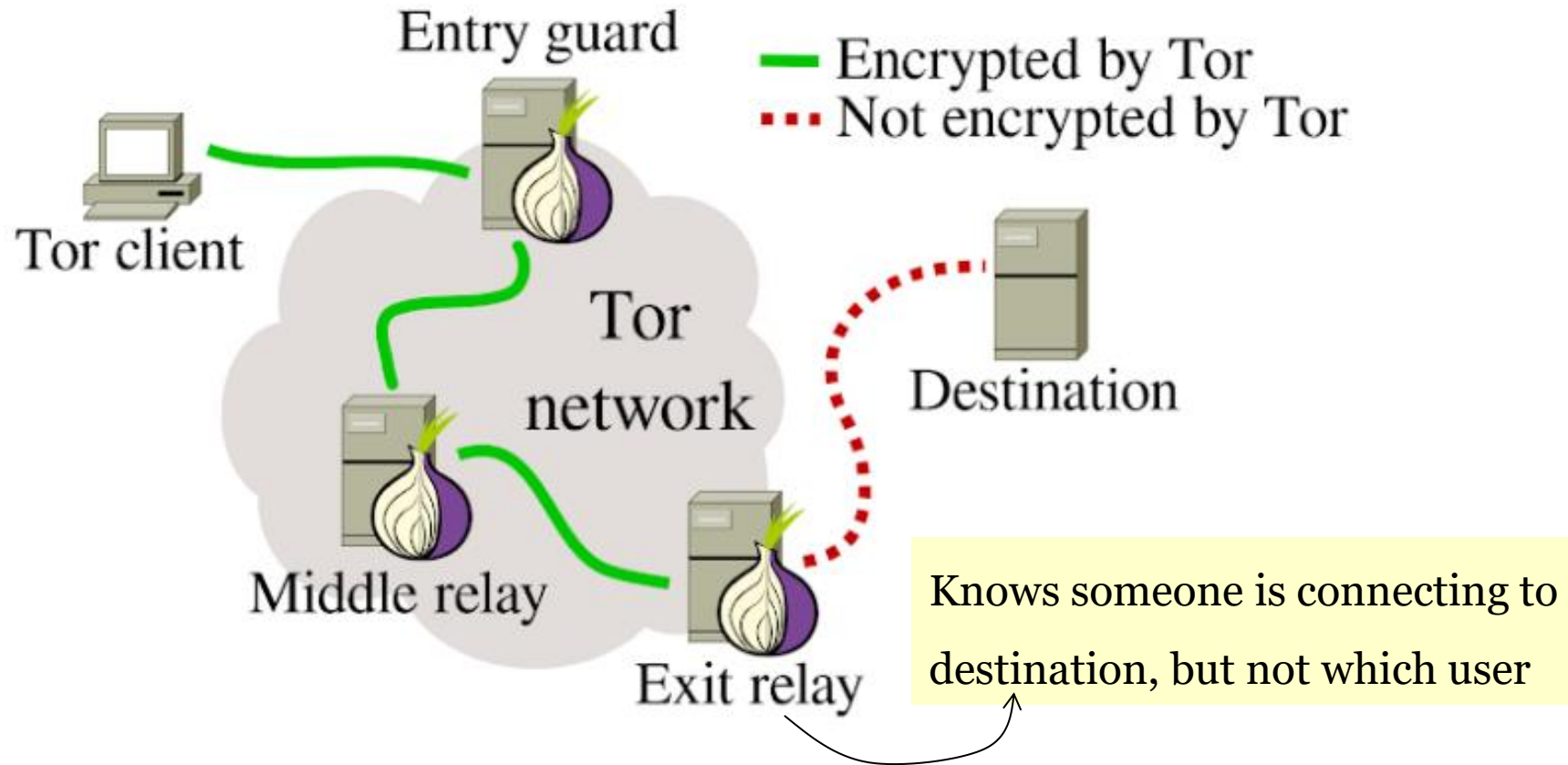


Who Knows What

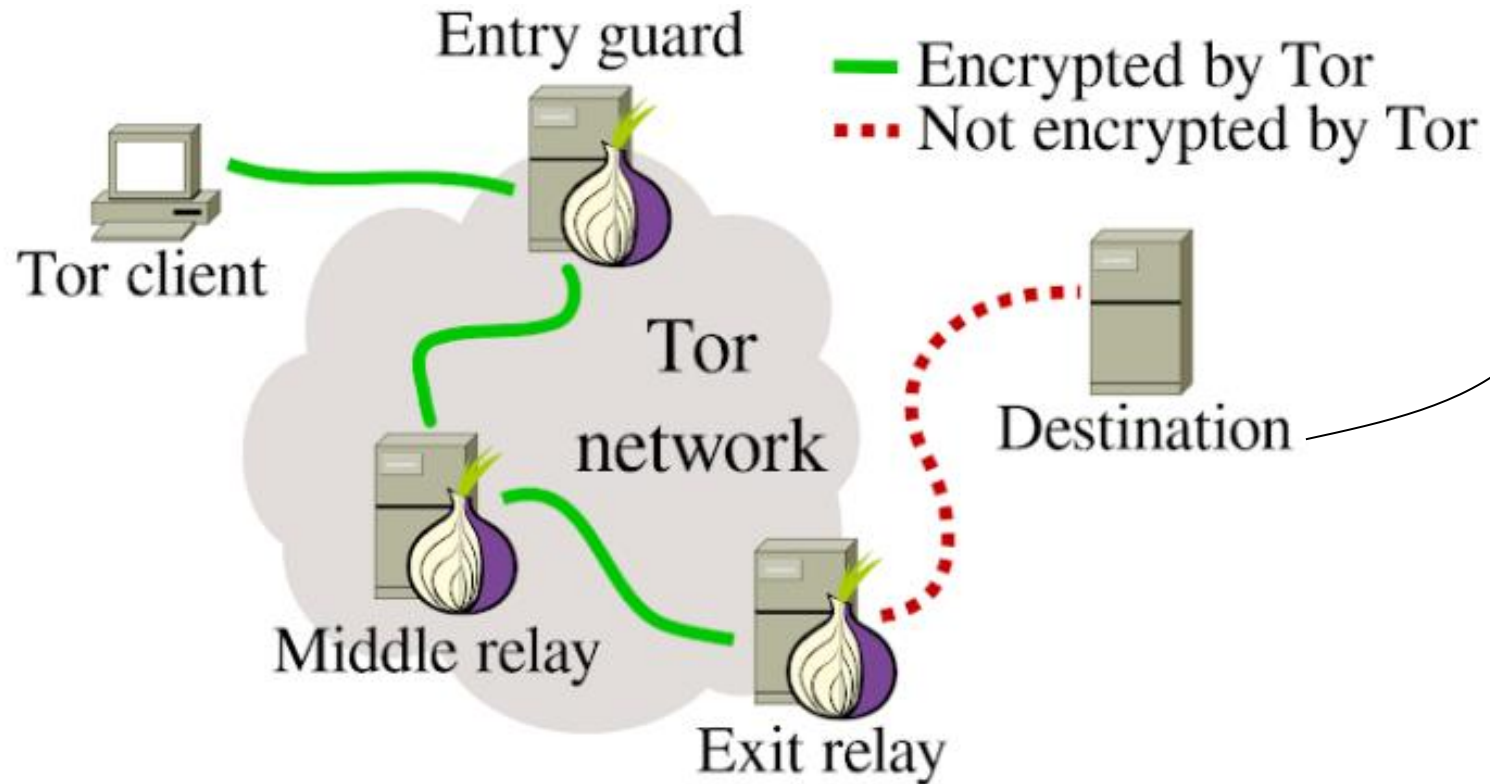
Knows Alice is using Tor and the identity of the middle node, but not the destination



Who Knows What



Who Knows What



Knows a Tor user is connecting to it via the exit node

— Encrypted by Tor
- - - Not encrypted by Tor



1.2.3.4



entry



middle



exit



5.6.7.8



Onion routing

Src: exit	Dest: 5.6.7.8	HTTP packet
--------------	------------------	----------------

Src: middle	Dest: exit	Encrypted with exit's key
----------------	---------------	---------------------------

Src: entry	Dest: middle	Encrypted with middle's key
---------------	-----------------	-----------------------------

Src: 1.2.3.4	Dest: entry	Encrypted with entry's key
-----------------	----------------	----------------------------

Tor implements more complex version of this basic idea

Tor Is Not A Panacea



BUSINESS INSIDER BI INTELLIGENCE EVENTS f t g+

Tech Finance **Politics** Strategy Life Sports Video

LAW & ORDER More: Harvard Bomb scare FBI

Harvard Student Arrested For Bomb Threat Tried And Failed To Hide Identity With Anonymous Browser

 PAMELA ENGEL  
DEC. 18, 2013, 3:03 PM:  57,643

MOTHERBOARD
TECH BY VICE

How the NSA (Or Anyone Else) Can Crack Tor's Anonymity

Researchers identified 81 percent of people using the service with a honeypot scheme and some statistical analysis.



By Jason Koebler