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

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

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. Evidence related to this incident does not clearly indicate whether it was perpetuated by the Chinese government or other actors. However, computer security experts believe that it is likely that a computer virus or malware attack may have been involved. This vulnerability could enable serious consequences.

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.
Crypto bugs

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

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.

Robert McMillan - Business Apr 11, 2014 6:38 AM

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

Authenticity issue: Adversary can modify Alice’s emails
HTTP Issues

Was not designed with security

Impersonation: Adversary can pretend to be Gmail
The Fix: HTTPS

Standard HTTP

<table>
<thead>
<tr>
<th>HTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP: port 80</td>
</tr>
</tbody>
</table>

HTTP
TCP: port 80

HTTPS

<table>
<thead>
<tr>
<th>HTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS</td>
</tr>
<tr>
<td>TCP: port 443</td>
</tr>
</tbody>
</table>

TLS encrypts and authenticates HTTP data
No change to HTTP itself
Cookie Cutter Attack on TLS

Visit

Attacker.com

Redirect

Bank of America

Bank.com
Cookie Cutter Attack on TLS

HTTP/1.1 302 Redirect
Location: https://bank.com/path
Set-Cookie: SID=[AuthenticationToken]; secure
Content-Length: 0

Giver user a cookie

Cookies must be sent via HTTPS
Message Is Split If URL Path Is Too Long

HTTP/1.1 302 Redirect
Location: https://bank.com/path
Set-Cookie: SID=[AuthenticationToken]

; secure
Content-Length: 0

bank.com
What Happens If Second Frame Is Blocked?

HTTP/1.1 302 Redirect
Location: https://bank.com/path
Set-Cookie: SID=[AuthenticationToken]

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
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 source 8.7.3.4, dest 1.2.3.4

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

Bob’s gateway
5.6.7.8

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

Source: Alice
Dest: Bob
Payload
1. The Internet & Its Problems

2. HTTP Issues

3. IP Issues

4. Privacy Issues
The End Of Privacy

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

Kashmir Hill  Former Staff
Welcome to The Not-So Private Parenting Era

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

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

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

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.
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

“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

Knows someone is connecting to destination, but not which user
Who Knows What

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

<table>
<thead>
<tr>
<th>Src: entry</th>
<th>Dest: middle</th>
<th>Encrypted with middle’s key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src: middle</td>
<td>Dest: exit</td>
<td>Encrypted with exit’s key</td>
</tr>
<tr>
<td>Src: exit</td>
<td>Dest: 5.6.7.8</td>
<td>HTTP packet</td>
</tr>
</tbody>
</table>

Tor implements more complex version of this basic idea
Tor Is Not A Panacea

We’ll later learn how to break Tor

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