

# ECE458/ECE750T27: Computer Security

## 2 Attack Cases

Dr. Kami Vania,  
Electrical and Computer Engineering  
[kami.vania@uwaterloo.ca](mailto:kami.vania@uwaterloo.ca)



UNIVERSITY OF  
**WATERLOO**

FACULTY OF  
ENGINEERING



# First, the news...

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
  1. Some students show up late for various good reasons
  2. Reward students who show up on time
  3. Important to see real world examples

Verizon MITMed traffic and added “supercookies” to all connections so that advertisers could track better and link data to demographics Verizon provided.

arsTECHNICA

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

BIZ & IT

Verizon’s zombie cookie gets new life

Verizon's tracking supercookie joins up with AOL's ad tracking network.

JULIA ANGIN AND JEFF LARSON, PROPUBLICA - 10/7/2015, 8:00 AM

65

Verizon is giving a new mission to its controversial hidden identifier that tracks users of mobile devices. Verizon said in a little-noticed announcement that it will soon begin sharing the profiles with AOL's ad network, which in turn monitors users across a large swath of the Internet.

**FURTHER READING**  
Verizon will now let users kill previously indestructible tracking code

That means AOL's ad network will be able to match millions of Internet users to their real-world details gathered by Verizon, including "your gender, age range and interests." AOL's network is on 40 percent of websites, including on ProPublica.

AOL will also be able to use data from Verizon's identifier to track the apps that mobile users open, what sites they visit, and for how long. Verizon purchased AOL earlier this year.

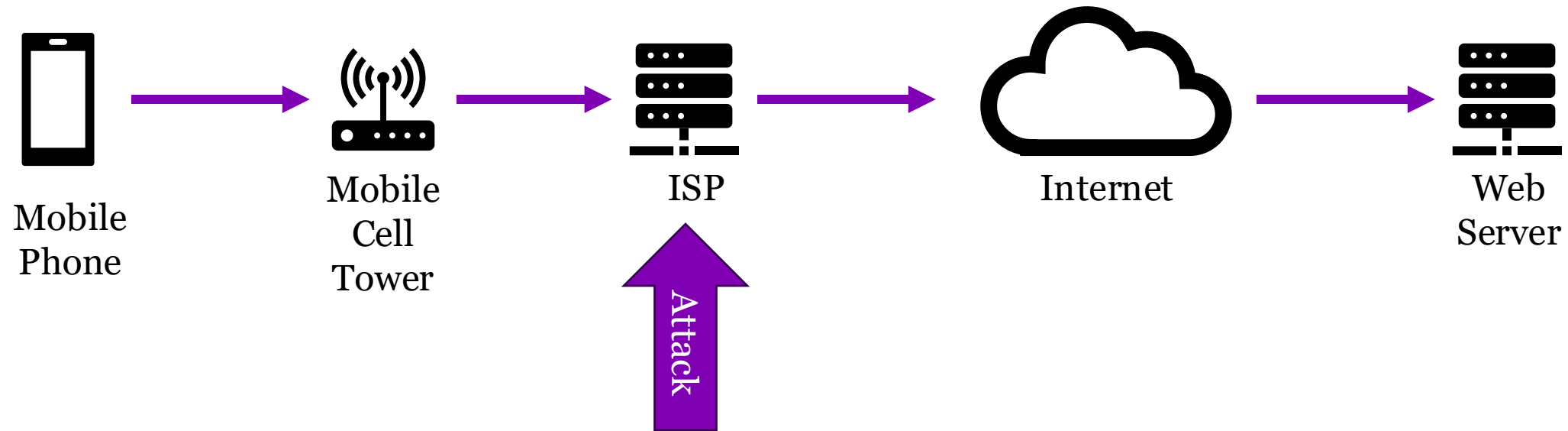
# Verizon MITM to add a “perma-cookie”

- Verizon smartphone customer traffic was modified by Verizon to add a header with a unique identifier
- “Verizon Wireless does not use the [cookie] to track where customers go on the web.” @kennwhite (Verizon)
- Opt-out option was provided to customers two years after the header started being used.
  - “If a customer has not opted out [...] ad serving partners will receive demographic and third-party interest based segments” @kennwhite (Verizon)

# **This attack touches on:**

- Networking
- Cookies
- Web design
- Privacy
- Law

# Verizon Man-in-the-Middle



This is me visiting  
<http://vaniea.com>

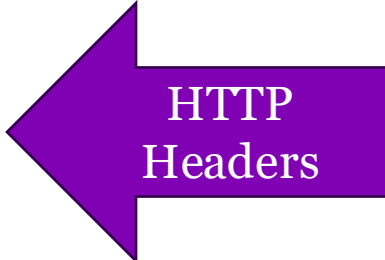
Look at the  
headers, they are  
just text...

Wireshark · Follow TCP Stream (tcp.stream eq 36) · wireshark\_2357B808-9...

```
GET / HTTP/1.1
Host: vaniea.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:49.0) Gecko/20100101
Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Sun, 25 Sep 2016 21:03:35 GMT
Server: Apache
Last-Modified: Mon, 29 Aug 2016 11:39:46 GMT
ETag: "10de-53b34522f89ac"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1831
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Content-Type: text/html

.....Xmo.....3....j+i..7U4tN..7.....0.4E[1$Q#)..?..b.!%[q..n_Z.<..
9.....1.~|..&..IZ)/.....z{=}.....FMI....W_|..oI.....
3.7o....Maj.U.J]O.U.d1.F.~..._E....K]?Ra..z.|W..tP....]....G$}.,.MN.....ld1M..
$Mbj...]6.....OV4..P.o..-r-.z#.6u..wJ.....0..Vn..O...+MD.&.;>.....
7..C.-...].Z...Gw..o.:W_z.w+.z.....I[r..0.....P..
8...b.j..'i.....Xixi....f..-G{...].u...s...Ma..Rh..t]...J..o..y.b]..
6_X.J.....V...1.?7.i.6..`.] .....U15....5[.....c.....c9C...K/yvJ..e.MM...~q}/
q/.cJ2...C...z....c...i..Mq(..x....." {.m.
.C.....s.....a;..4.9. 20...pr@.....+F...y.....WJ.....gRqWI...
4.....6U"E..\DU+...{.....tS          ].4...$.u4h.:.q8.....H..1.O.
5..C.~....."W.....^.....4.!?MX4.....~.@UN  +.t.+|xG.*|./.m%jZ.....S...
```



HTTP Headers

# More companies than Verizon used this trick.

HTTP Header	Operator	Notes
x-nokia-bearer	3 (ID), EE (GB), SFR (FR)	3GPP standard
x-orange-rat	EE (GB)	
x-up-3gpp-rat-type	Vodacom (ZA)	
x-up-bear-type	Movistar (MX)	
x-up-bearer-type	Vodacom (ZA)	
x-operator-domain	EE (GB)	Operator name
x-vfprovider	SFR (FR)	
x-vodafone-roamingind	Vodafone (IE)	MCC, MNC
x-up-3gpp-sgsn-mcc-mnc	Vodacom (ZA)	Operator name
x-orange-roaming	EE (GB)	Roaming state
x-sdp-roaming	Vodafone (TR)	
vf-za-trust	Vodacom (ZA)	Private IP address
x-ee-client-ip	EE (GB)	
x-forwarded-for	AIS (TH), AT&T (US), Bouygues (FR), Etisalat (AE), LMT (LV), Movistar (MX), O2 (GB), Orange (CH), SaskTel (CA), SFR (FR), Singtel (SG), T-Mobile (DE), TOT (TH), Vodacom (ZA), Vodafone (DE)	
x-nokia-ipaddress	EE (GB), SFR (FR)	
x-up-forwarded-for	TIM (IT)	
o2gw-id	O2 (GB)	Gateway ID & location
x-gateway	O2 (GB)	
x-bluecoat-via	3 (IE), Vodafone (QA)	Bluecoat-specific
x-nokia-gateway-id	SFR (FR)	Gateway model
x-nokia-gid	SFR (FR)	
x-proxy-id	LMT (LV)	Proxy unique ID
x-up-sgsn-ip	Vodacom (ZA)	SGSN IP address
proxy-connection	TIM (IT)	Persistent connections
wap-connection	Airtel (IN)	Layer-7 protocol
x-nokia-connection_mode	SFR (FR)	Layer-4 protocol
x-vodafone-3gppdpcontext	Vodafone (IE)	PDP context
wisp-a	Orange (FR)	Wireless provider
x-wisp	Orange (FR)	

Table 3: HTTP headers leaking network-related information added by different operators.



# Questions

1. Would this attack work if visiting a website over https?
2. Attack particularly bad because it could be used to re-create user-deleted cookies (aka “zombie” cookies). Describe how a deleted cookie could be resurrected using this attack.

# Questions: privacy and law

1. Why was the Verizon Supercookie attack illegal? MITM attacks are not necessarily illegal.
2. Give an example of a legal MITM that changes traffic without explicit user consent.

**DRAGNETS**

**Verizon to Pay \$1.35 Million to Settle Zombie Cookie Privacy Charges**

The settlement is the latest sign that the FCC is stepping up privacy enforcement actions.

by Julia Angwin, March 7, 2016, 6 p.m. EST



#### DRAGNETS

Tracking

Censorship and  
Surveillance

Verizon agreed to pay \$1.35 million to settle Federal Communications Commission charges that it violated customers' privacy when it used a [hidden undeletable number](#) to track cellphone users.

In the [settlement](#), Verizon also agreed to make its unkillable "zombie" cookie opt-in, meaning that users are not tracked by default. Previously, users had been tracked by default unless they opted out.

However, the settlement does not apply to Verizon's tracking of its customers who visit the 40 percent of [websites that use AOL's ad network](#). That is because Verizon owns AOL, and therefore it is not considered a third party that requires opt-in.

# On-device MITM Attack

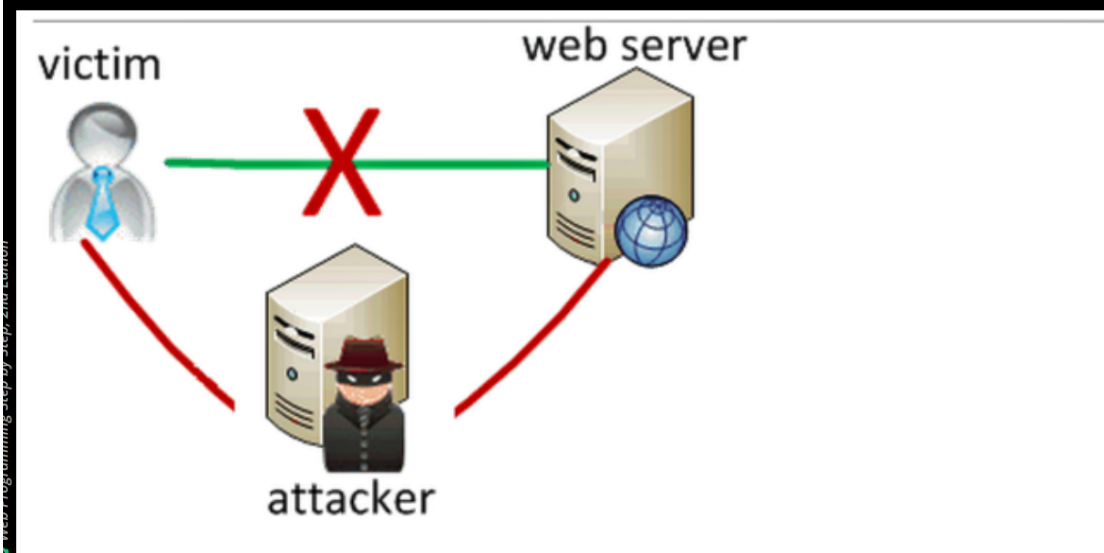
Lenovo shipped computers with software that used MITM to inject ads into all network traffic.

BIZ &amp; IT —

## Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated]

Superfish may make it trivial for attackers to spoof any HTTPS website.

DAN GOODIN - 2/19/2015, 11:36 AM



333

Lenovo is selling computers that come preinstalled with adware that hijacks encrypted Web sessions and may make users vulnerable to HTTPS man-in-the-middle attacks that are trivial for attackers to carry out, security researchers said.

The critical threat is present on Lenovo PCs that have adware from a company called Superfish installed. As unsavory as many people find software that injects ads into Web pages, there's something much more nefarious about the Superfish package. It installs a self-signed root HTTPS certificate that can intercept encrypted traffic for every website a user visits. When a user visits an HTTPS site, the site certificate is signed and controlled by Superfish and falsely represents itself as the official website certificate.

Even worse, the private encryption key accompanying the Superfish-signed Transport Layer Security certificate appears to be the same for every Lenovo machine. Attackers may be able to use the key to certify imposter HTTPS websites that masquerade as Bank of America, Google, or any other secure destination on the Internet. Under such a scenario, PCs that have the Superfish root certificate installed will fail to flag the sites as forgeries—a failure that completely undermines the reason HTTPS protections exist in the first place.

## This attack touches on:

- Man-in-the-middle attacks
  - Cryptography
  - Certificate Authorities
  - Access Control – where is the reference monitor? Who is authorized to change your computer?
  - Trust
  - Law – when is MITM legally acceptable
  - Law – consent
- Security researcher Marc Rogers wrote that it's “quite possibly the single worst thing I have seen a manufacturer do to its customer base. ... I cannot overstate how evil this is.”

# Lenovo, a laptop manufacturer

- Pre-installed Superfish
- Superfish Man-in-the-middle all traffic and added advertising
- Superfish/Lenovo pre-installed a single self-signed root certificate
- They used the same root certificate with a weak 1024-bit RSA key on ALL affected Lenovo PCs (1024-bit depreciated in 2013)

152 3134

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION

Commissioners: Maureen K. Ohlhausen, Acting Chairman  
Terrell McSweeney

In the Matter of

LENOVO (UNITED STATES) INC.  
a corporation.

)  
)  
)  
)  
)  
)

Docket No. C-

COMPLAINT

The Federal Trade Commission, having reason to believe that Lenovo (United States) Inc. has violated Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1.

Respondent Lenovo (United States) Inc. (“Lenovo”) is a Delaware corporation with its principal office or place of business located at 1009 Think Place, Morrisville, North Carolina 27560-9002.

2.

The acts and practices of Respondent alleged in the Complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT’S BUSINESS PRACTICES

3.

Respondent is one of the world’s largest manufacturers of personal computers, including desktop computers, laptops, notebooks, and tablets. Respondent employs approximately 7,500 people in the United States.

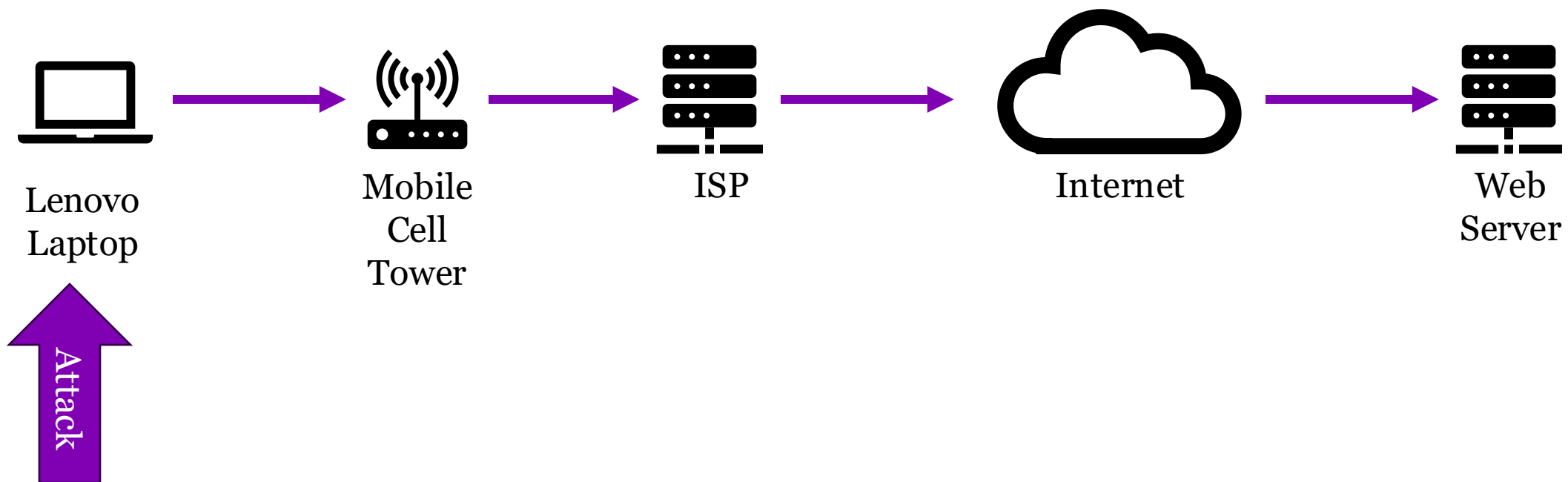
4.

In August 2014, Respondent began selling certain laptop models to U.S. consumers with a preinstalled ad-injecting software (commonly referred to as “adware”), known as VisualDiscovery. VisualDiscovery was developed by Superfish, Inc. , a Delaware corporation with its principal office or place of business located in Palo Alto, California.

5.

VisualDiscovery delivered pop-up ads to consumers of similar-looking products sold by Superfish’s retail partners whenever a consumer’s cursor hovered over the image of a product on a shopping website. For example, if a consumer’s cursor hovered over a product image while the consumer viewed owl pendants on a shopping website like Amazon.com, VisualDiscovery would overlay pop-up ads onto that website of other similar-looking owl pendants sold by Superfish’s retail partners.

# Verizon Man-in-the-Middle



# Browsers use locally-managed root certificates

- The user (or their admin) can install any root-certificate they want to on a computer.
- Most browsers honor locally installed root certificates.



Chromium Blog

News and developments from the open source browser project

## Announcing the Launch of the Chrome Root Program

Monday, September 19, 2022

In 2020, we [announced](#) we were in the early phases of establishing the Chrome Root Program and launching the Chrome Root Store.

The Chrome Root Program ultimately determines which website certificates are trusted by default in Chrome, and enables more consistent and reliable website certificate validation across platforms.

This post shares an update on our progress and how these changes help us better protect Chrome's users.

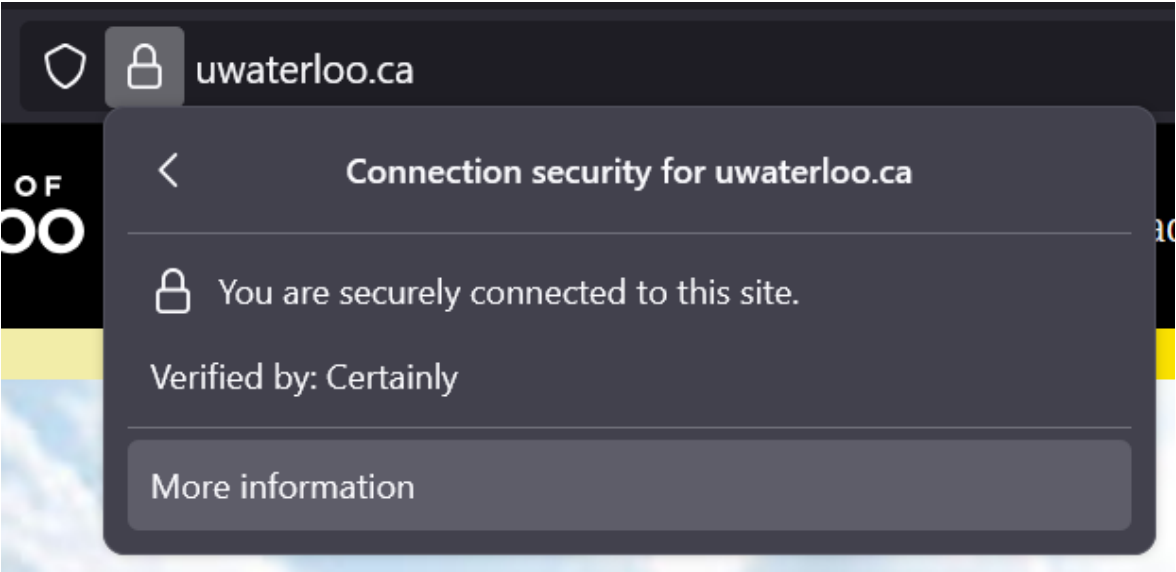
### What's a root store or root program, anyway?

Chrome uses [digital certificates](#) (often referred to as "certificates," "HTTPS certificates," or "server authentication certificates") to ensure the connections it makes on behalf of its users are secure and private. Certificates are responsible for binding a domain name to a public key, which Chrome uses to

The Chrome Certificate Verifier considers locally-managed certificates during the certificate verification process. This means if an enterprise distributes a root CA certificate as trusted to its users (for example, by a Windows Group Policy Object), it will be considered trusted in Chrome.

authorities to trust. The [Chrome Root Store](#) contains the set of [root CA](#) certificates Chrome trusts by default.

# UWaterloo.ca Certificate



## Certificate

uwaterloo.ca	Certainly Intermediate R1	Starfield Root Certificate Authority - G2
Subject Name		
Country	US	
State/Province	Arizona	
Locality	Scottsdale	
Organization	Starfield Technologies, Inc.	
Common Name	Starfield Root Certificate Authority - G2	
Issuer Name		
Country	US	
State/Province	Arizona	
Locality	Scottsdale	
Organization	Starfield Technologies, Inc.	
Common Name	Starfield Root Certificate Authority - G2	
Validity		
Not Before	Tue, 01 Sep 2009 00:00:00 GMT	
Not After	Thu, 31 Dec 2037 23:59:59 GMT	
Public Key Info		
Algorithm	RSA	
Key Size	2048	
Exponent	65537	
Modulus	BD:ED:C1:03:FC:F6:8F:FC:02:B1:6F:5B:9F:48:D9:9D:79:E2:A2:B7:03:61:56:18:C3:4...	



# Questions: Coffee shop attack

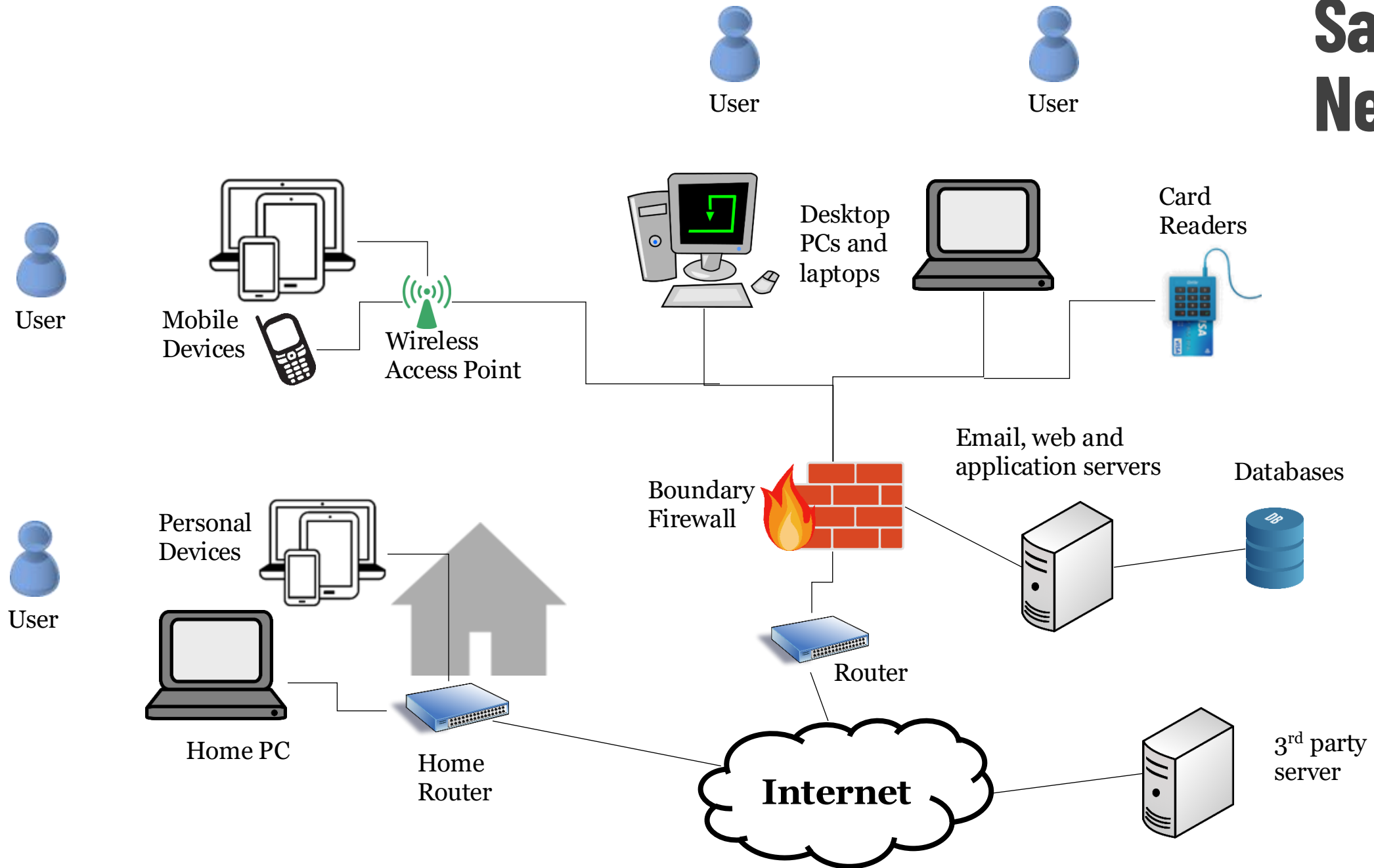
- Assume an attacker is able to intercept traffic. For example, a coffee shop offering free wifi.
- How might the attacker be able to Man-in-the-middle *any* traffic coming from a laptop running Superfish?

# Questions

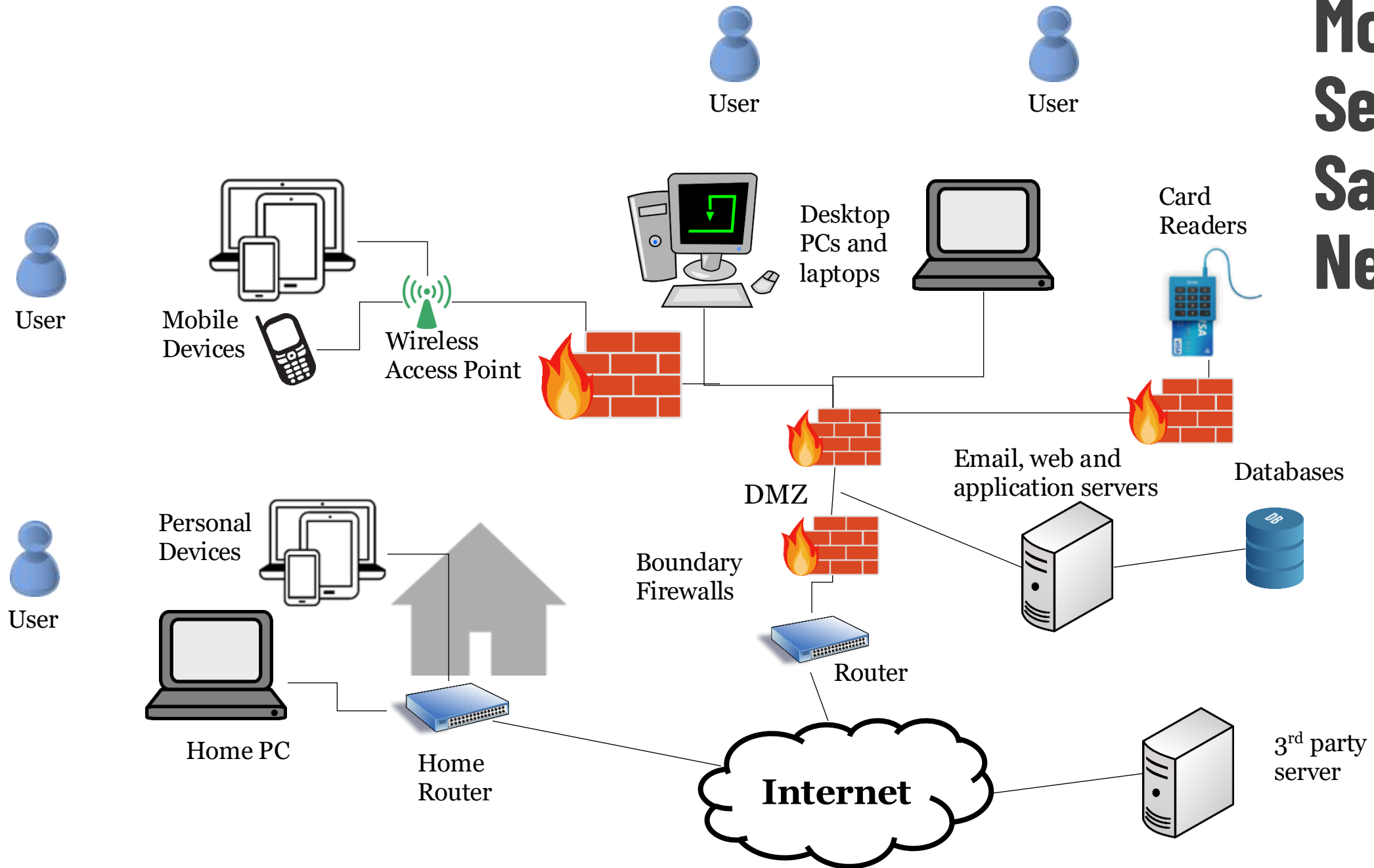
- Why was the Superfish software illegal?
  - MITM attacks are not necessarily illegal.
  - Root certificate insertion on a laptop is not necessarily illegal.

# EXTRA SLIDES FOR REFERENCE

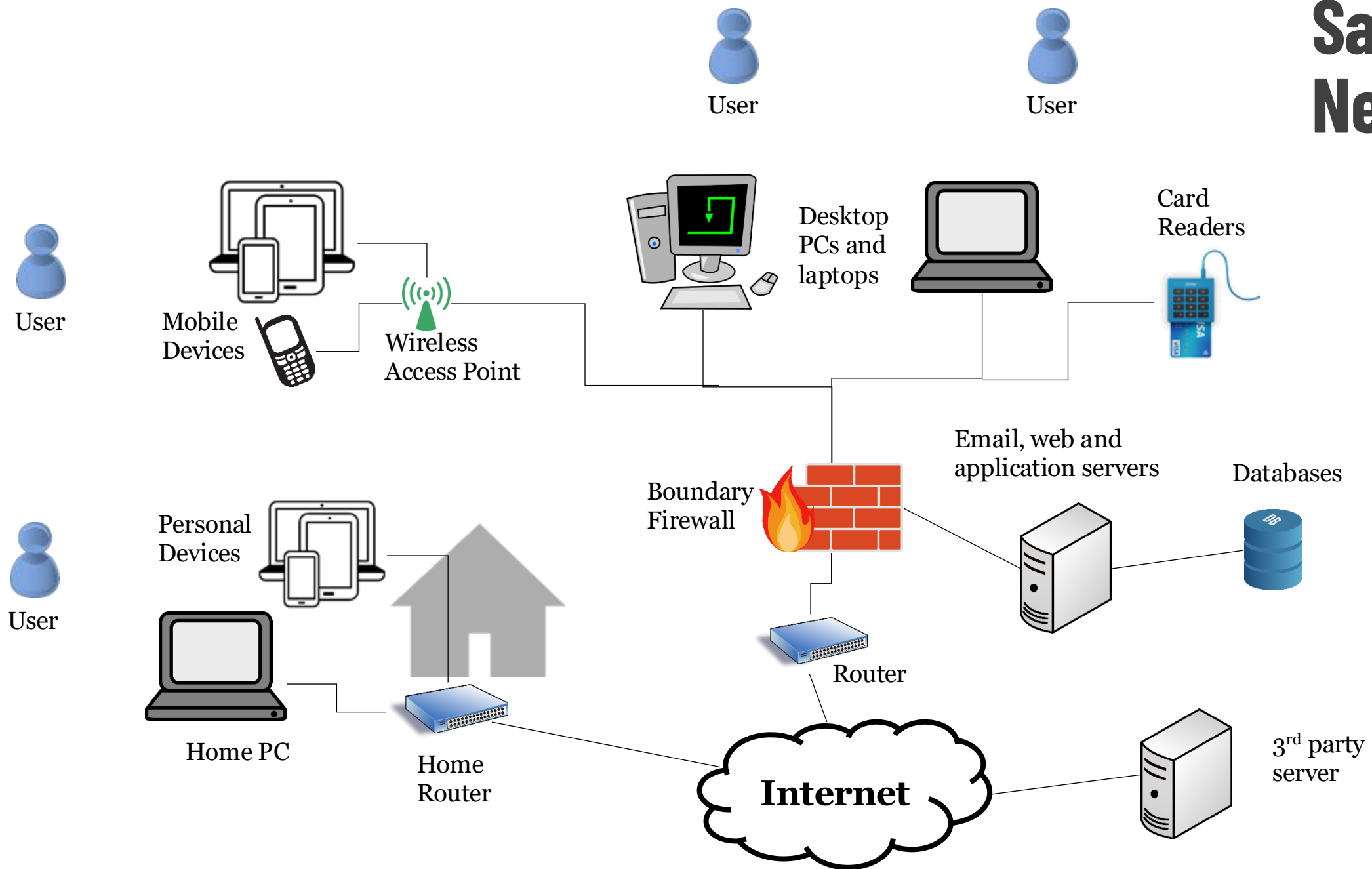
# Sample Network



# More Secure Sample Network

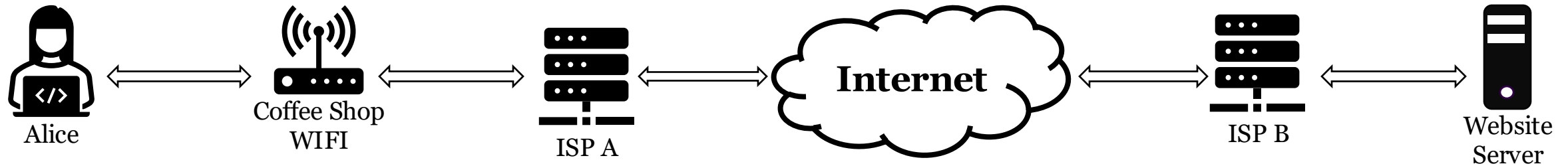


# Sample Network



# Sample connection: Alice loads a website

Alice visits: `http://example.com`



For each of the above icons, answer the following:

1. The name and/or IP address of the website Alice is visiting
2. The content of the webpage Alice is viewing
3. The IP address of Alice's computer (i.e. `ifconfig` or `ipconfig`)
4. The IP address of the Coffee Shop
5. Alice's Operating System