ECE458/ECE750T27: Computer Security

3 Attack Cases – Lenovo Superfish

Dr. Kami Vaniea,
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

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

3 Cases

- Verizon Supercookie
- Lenovo Superfish
- Cambridge Analytica

LENOVO SUPERFISH

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."

On-device MITM Attack

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

ars TECHNICA

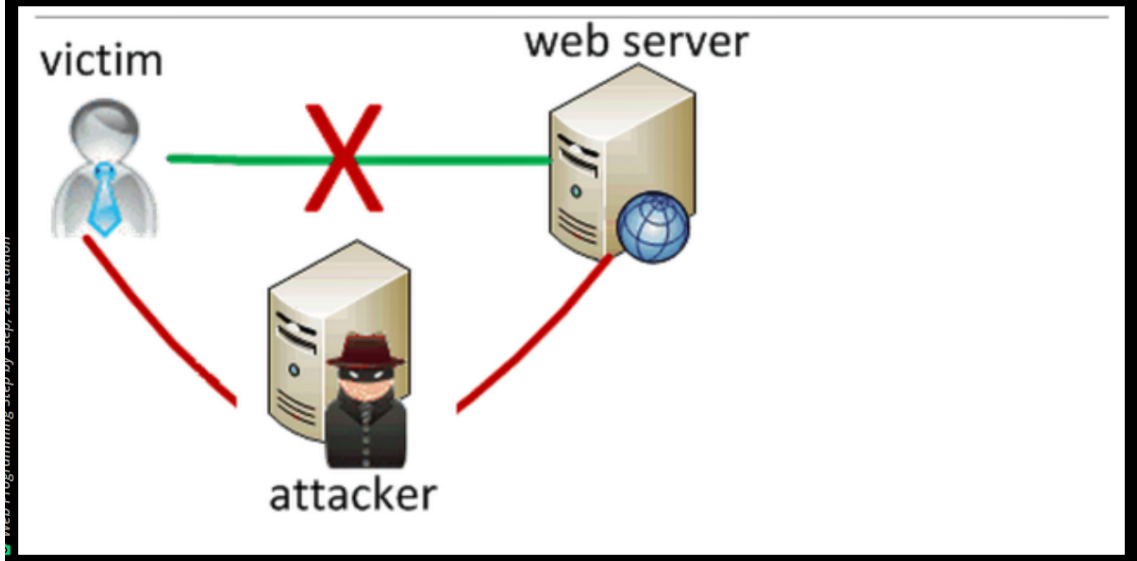
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

BIZ & 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.

Lenovo, a laptop manufacturer

- Pre-installed Superfish VisualDiscovery
- Superfish man-in-the-middled 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 McSweeny

In the Matter of	)	
	)	
LENOVO (UNITED STATES) INC.	)	**Docket No. C-**
a corporation.	)	

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.

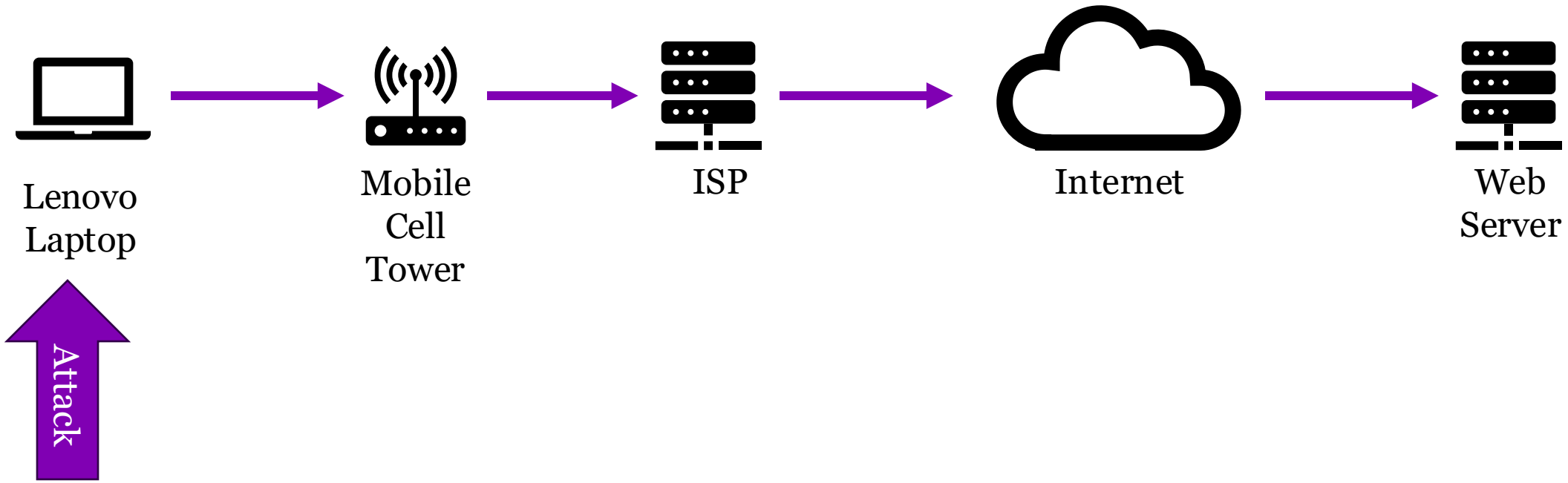
RESPONDENT'S BUSINESS PRACTICES

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.

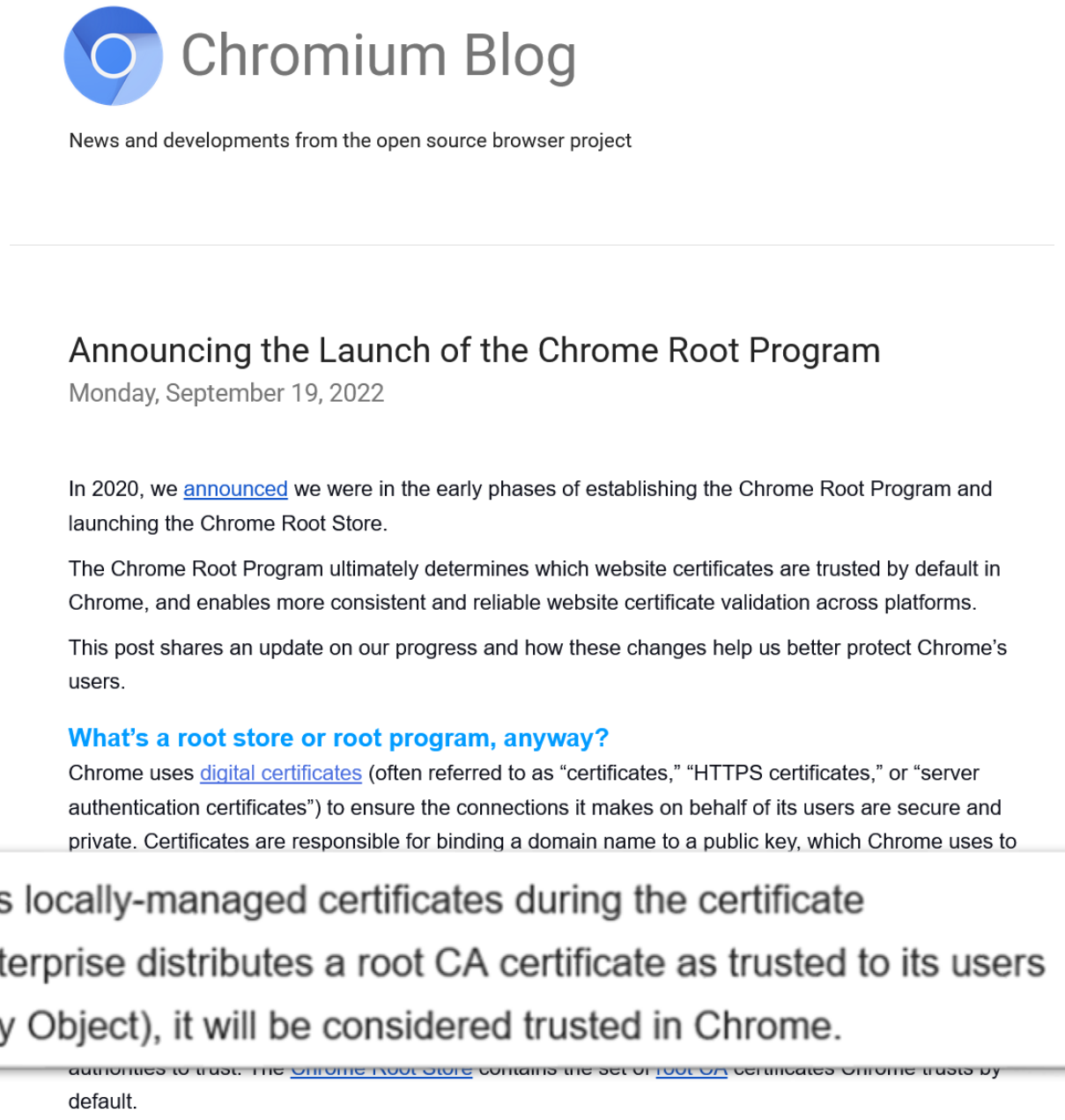
5. VisualDiscovery delivered pop-up ads to consumers of similar-looking products sold by Superfish's retail partners whenever a consumer's cursor hovered over the image of a product on a shopping website. For example, if a consumer's cursor hovered over a product image while the consumer viewed owl pendants 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.

Superfish 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.
- Locally installed root certificates are theoretically used by all programs on the computer.



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.

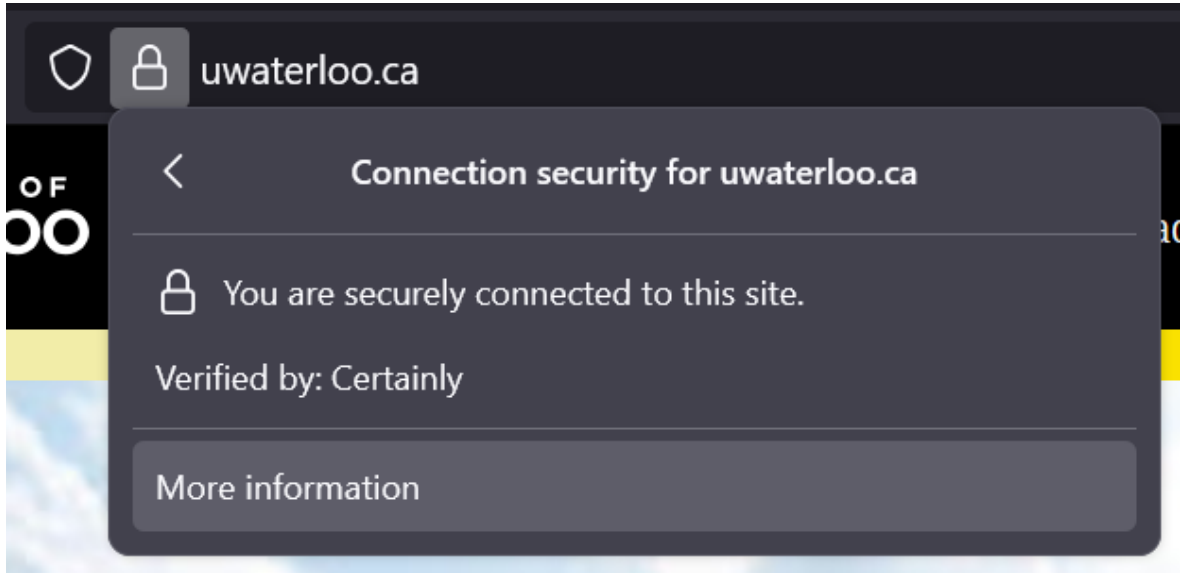
What's a root store or root program, anyway?

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.

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

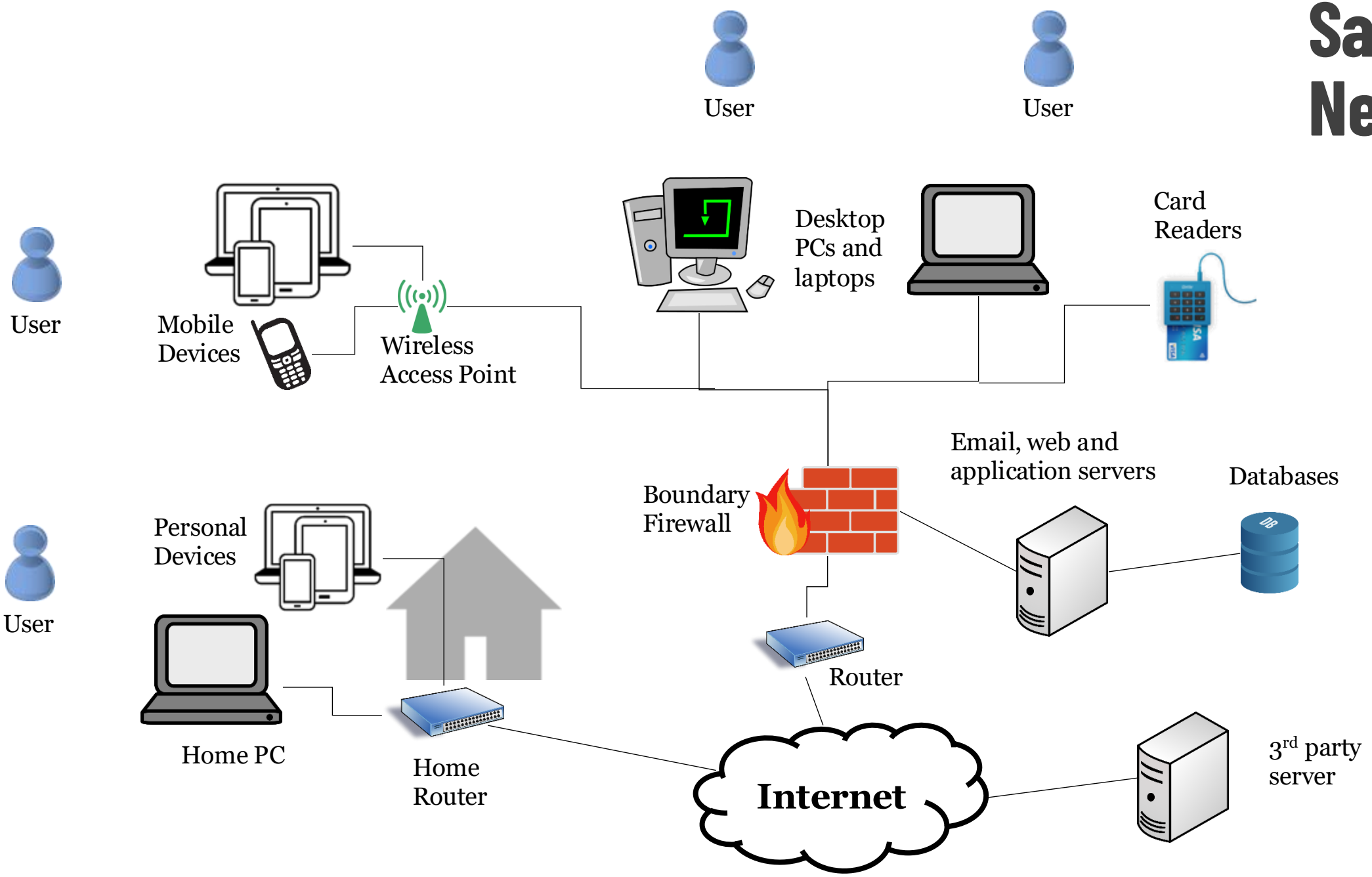
- Assume an attacker is able to intercept traffic. For example, a coffee shop offering free wifi.
- How might the attacker be able to Man-in-the-middle *any* traffic coming from a laptop running Superfish?
- Is that attack computer-detectable?
- Is the attack human-visible (if they looked)?

Questions

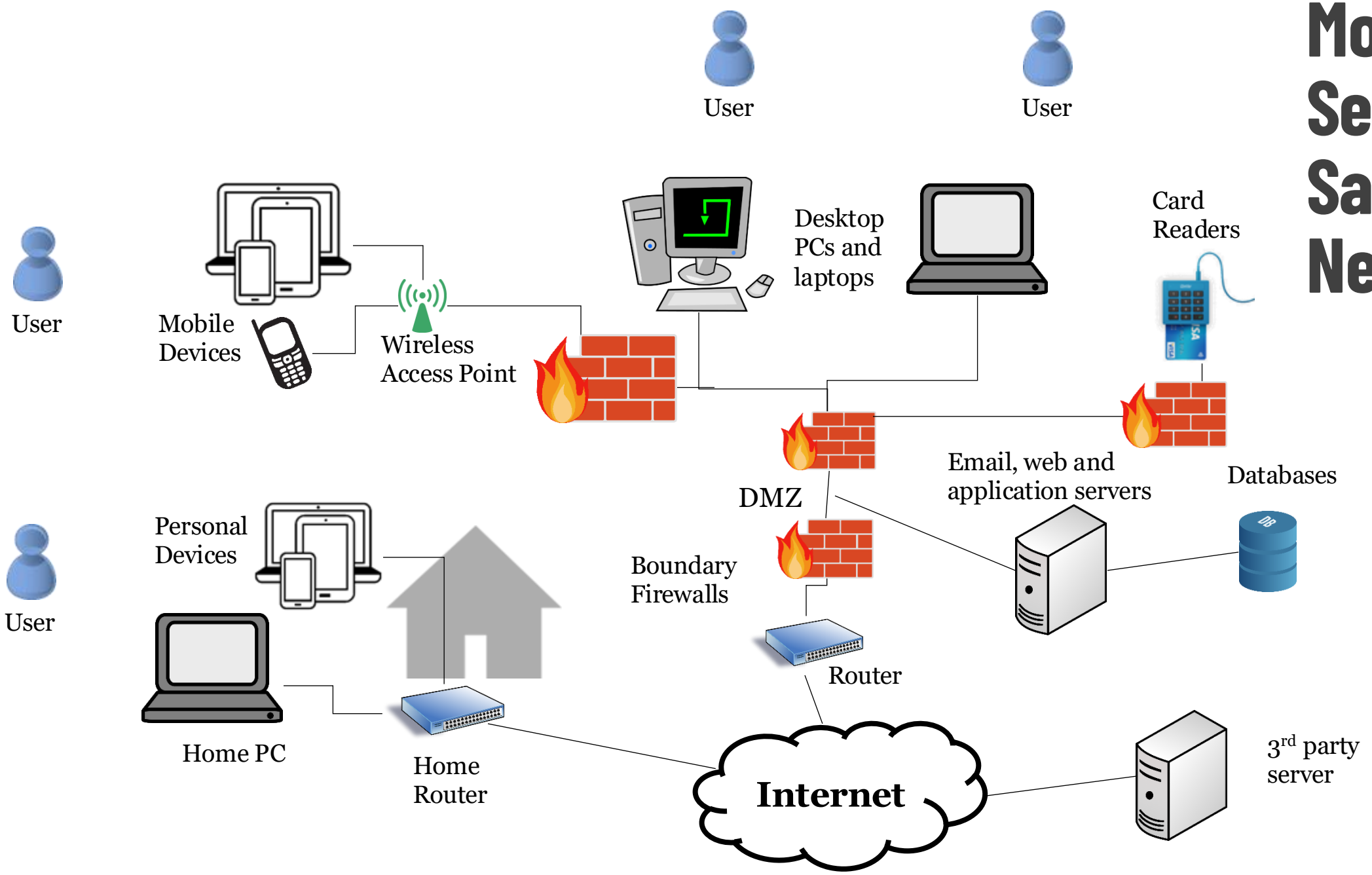
- Why was the Superfish software illegal?
  - MITM attacks are not necessarily illegal.
  - Root certificate insertion on a laptop is not necessarily illegal.

EXTRA SLIDES FOR REFERENCE

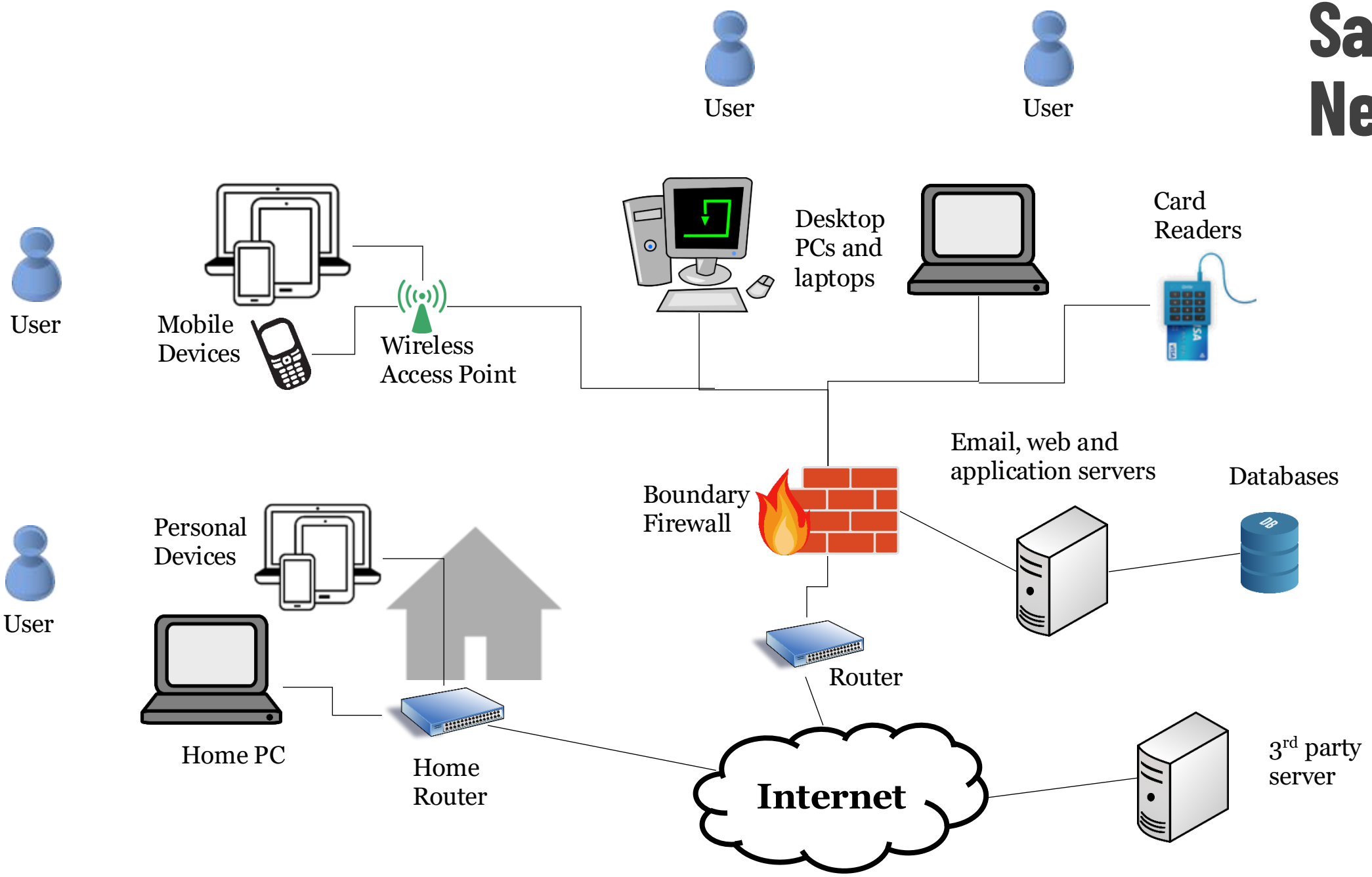
Sample Network



More Secure Sample Network

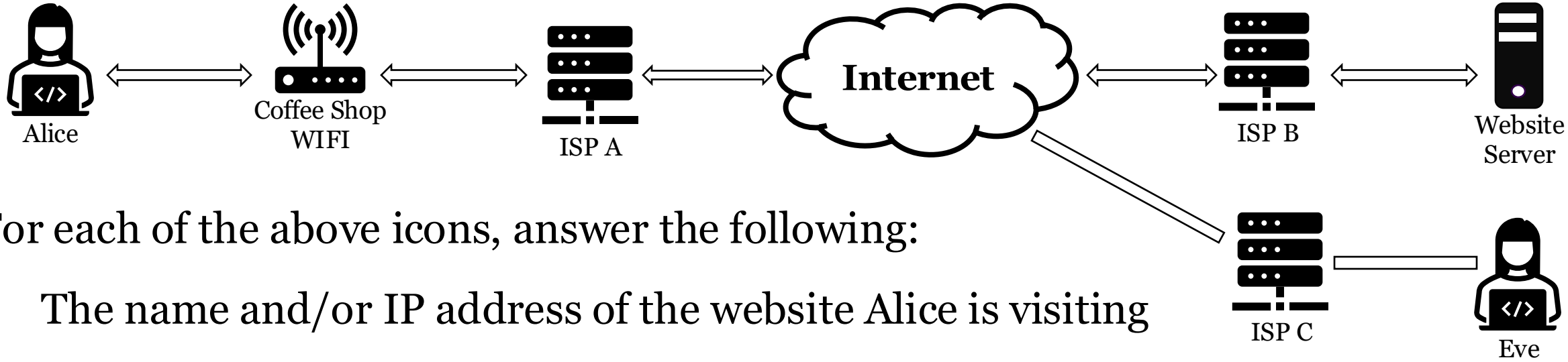


Sample Network



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