ECE458/ECE750T27: Computer Security

3 Attack Cases – Verizon Supercookie

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

VERIZON SUPERCOOKIE

2012 - 2014

This attack touches on:

- Networking
- Cookies
- Web design
- Privacy
- Law

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[l$Q#)..?..b.!%[q..n_Z.<..
9......l.~|..&..IZ)/.......z{=].......FMI....W_|..oI..:...
3.7o....Maj.U.J]O.U.dl.F.~..._E....K]?Ra..z.|W..tP....]....G$}.,.MN......ld1M..
$Mbj...]6........OV4..P.o..-.r-.z#.6u..wJ.....0..Vn..O...+MD.&.;......
7..C..-..].Z...Gw..o..:W_z.w+.z.....I[r..0.......P..
8...b.j..'i............XIxi....f..-G{...].u...s...Ma..Rh..t]...J..o..y.b]..
6_X.J......V...1.?7.i.6..`.] .....Ul5....5[.....c......c9C...K/yvJ..e.MM...~q}/
q/.cJ2...C...z....c...i..Mq(..x......."{..m.
.C.....s......a;..4.9. 2O...pr@...:...+F....y.....WJ........gRqWI...
4.....6U"E..\.DU+...{.......tS       ]..4...$..u4h.:.q8.........H..1.O.
5..C.~....."W......^.....4.!?MX4....~.@UN   +.t.+|xG.*|./..m%jZ...:..S...
```

HTTP Headers

HTTP Headers

Client -> Server: give me the cookieExample.html page

```
GET /cookieExample.html HTTP/1.1

Host: kamivaniea.com

Cookie: testcookie=12345; flavor=chocolatechip

User-Agent: Mozilla/5.0

Accept: text/html,application/xhtml+xml

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive
```

Headers are how cookies are sent

Mock-up header based on “Set a cookie” activity

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

ars TECHNICA

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

65

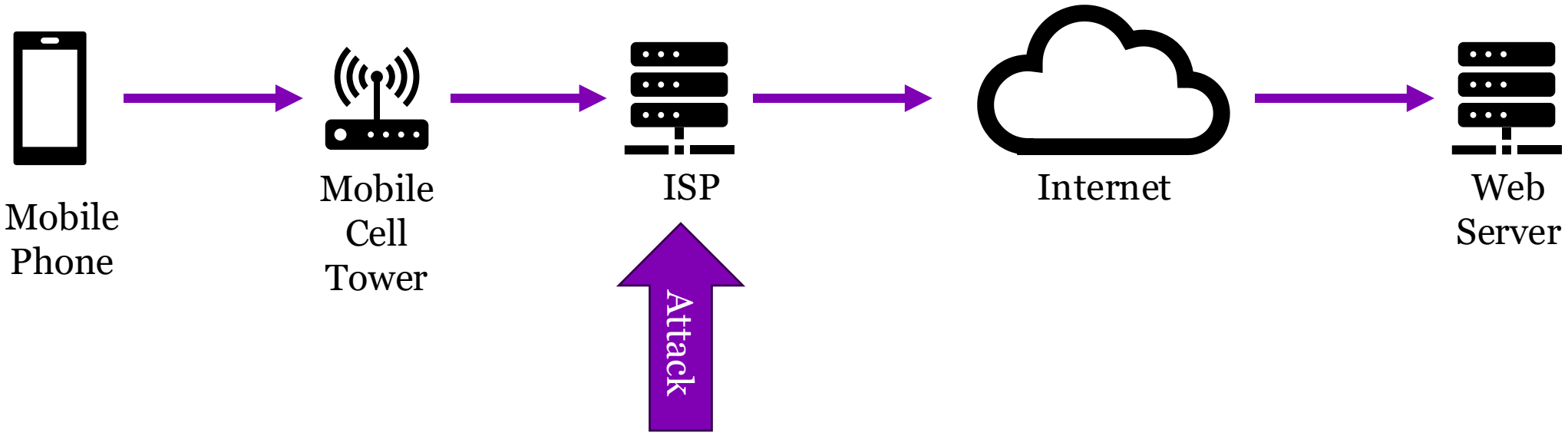
Verizon is giving a new mission to its controversial hidden identifier that tracks users of mobile devices. Verizon said in a little-noticed announcement that it will soon begin sharing the profiles with AOL's ad network, which in turn monitors users across a large swath of the Internet.

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 Man-in-the-Middle



Think-pair-share

- How might Verizon do this attack?
- Think about the protections we learned about, would this attack have worked for all traffic?

- Verizon MITMed traffic and added “supercookies” to all connections so that advertisers could track better and link data to demographics Verizon provided.
- Only mobile customers targeted.
- Only headers were modified, no other content was changed.

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)

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-3gpdpcontext	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.

Vallina-Rodriguez, Narseo, et al. "Header enrichment or ISP enrichment? Emerging privacy threats in mobile networks." *Workshop on Hot Topics in Middleboxes and Network Function Virtualization*. 2015.

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

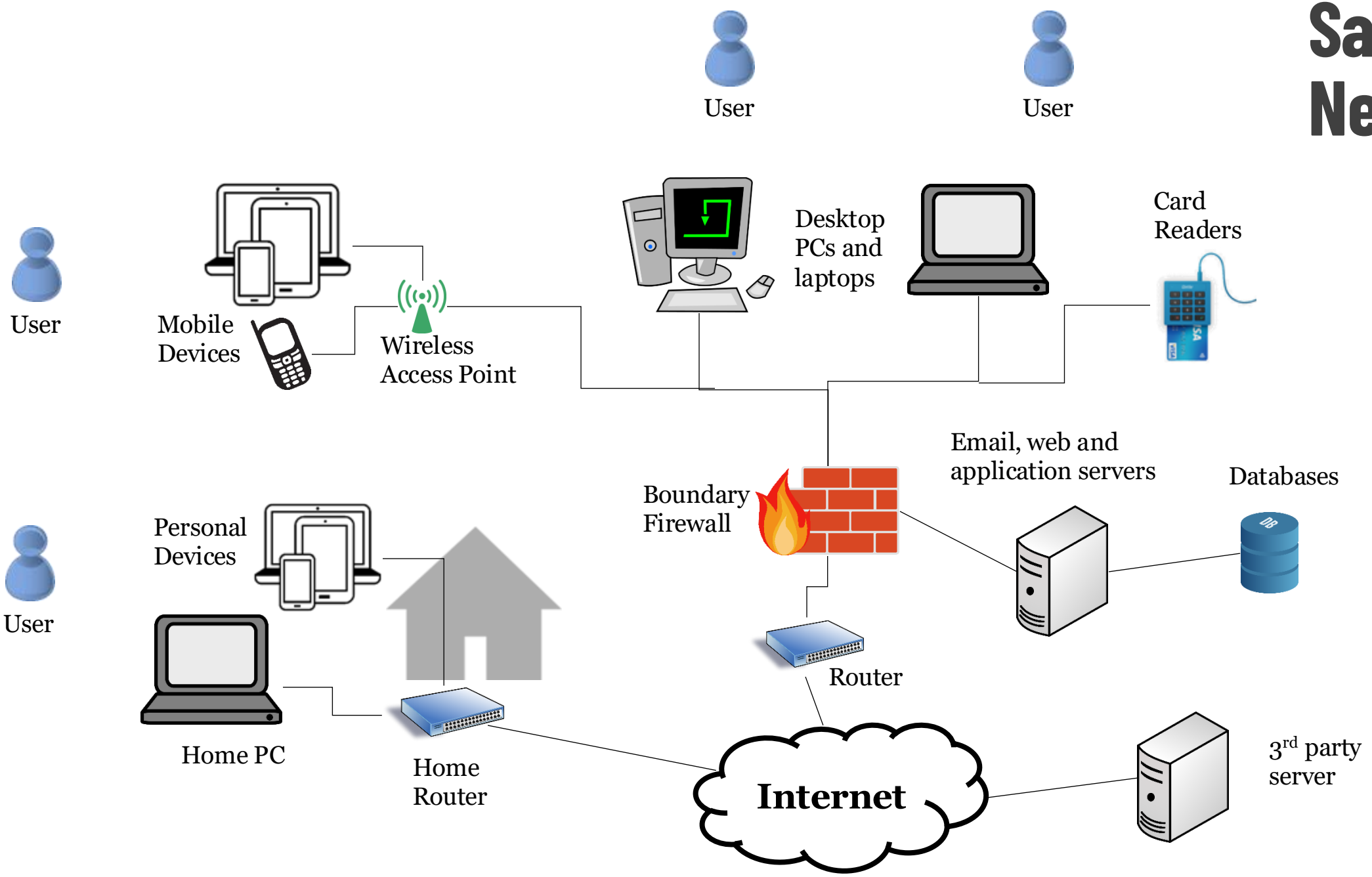
Verizon agreed to pay $1.35 million to settle Federal Communications Commission charges that it violated customers' privacy when it used a hidden undeletable number to track cellphone users.

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.

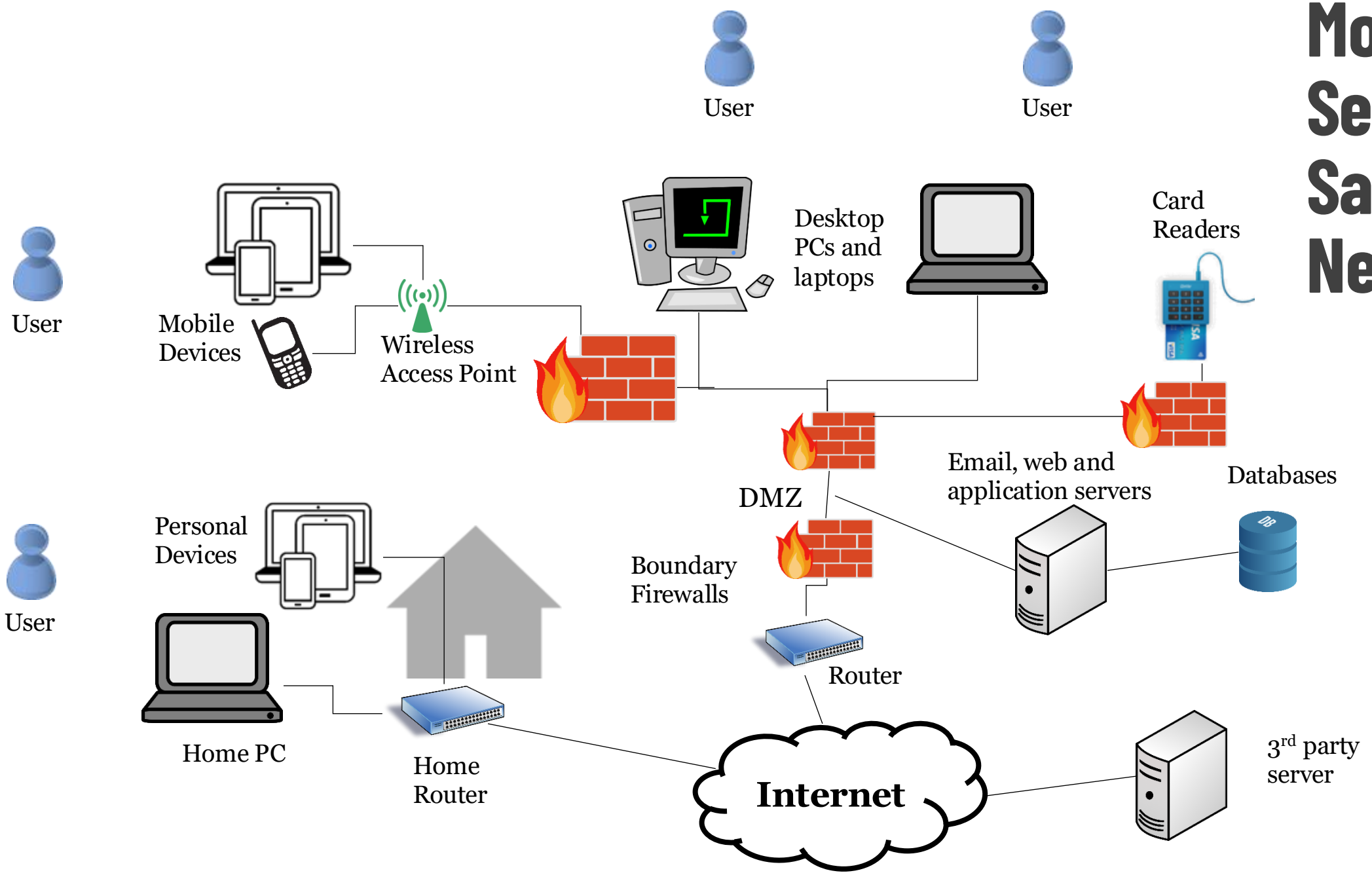
However, the settlement does not apply to Verizon's tracking of its customers who visit the 40 percent of websites that use AOL's ad network. That is because Verizon owns AOL, and therefore it is not considered a third party that requires opt-in.

EXTRA SLIDES FOR REFERENCE

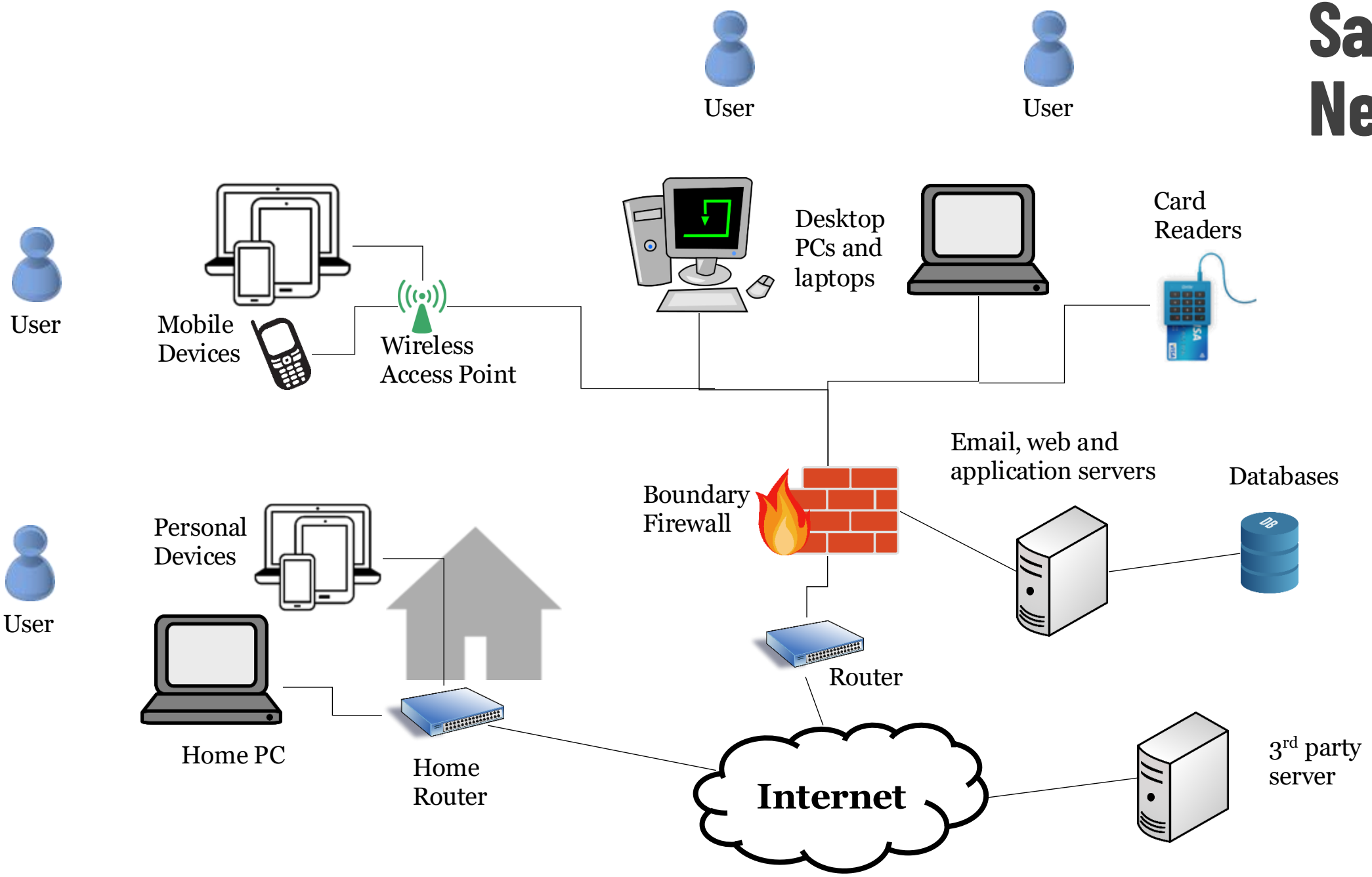
Sample Network



More Secure Sample Network

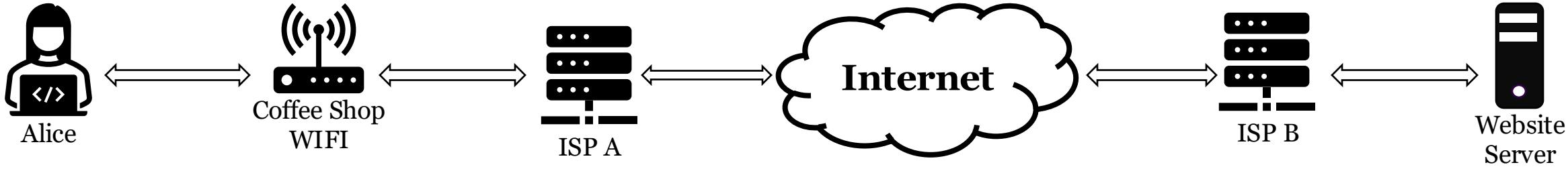


Sample Network



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