HTTP Cookie Hijacking in the Wild: Security and Privacy Implications

Suphannee Sivakorn*, Jason Polakis*,
Angelos D. Keromytis

*Joint primary authors

JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

Who we are

Suphannee Sivakorn
PhD Student @ Columbia University

Jason Polakis
Assistant Professor @ University of Illinois at Chicago

Current State of Affairs

- ☑ Public discussion about need for encryption
  - Crypto Wars, part 2
- ☑ Getting crypto right is difficult
  - DROWN, FREAK, POODLE, Logjam, …
- ☑ SSL/TLS is fundamental for protecting our communications

- ☒ Talk about encryption?
  - More about lack of encryption
  - "*Web Services and the Quest for Ubiquitous Encryption*"

    …sad tale without a happy ending … or perhaps partially happy?

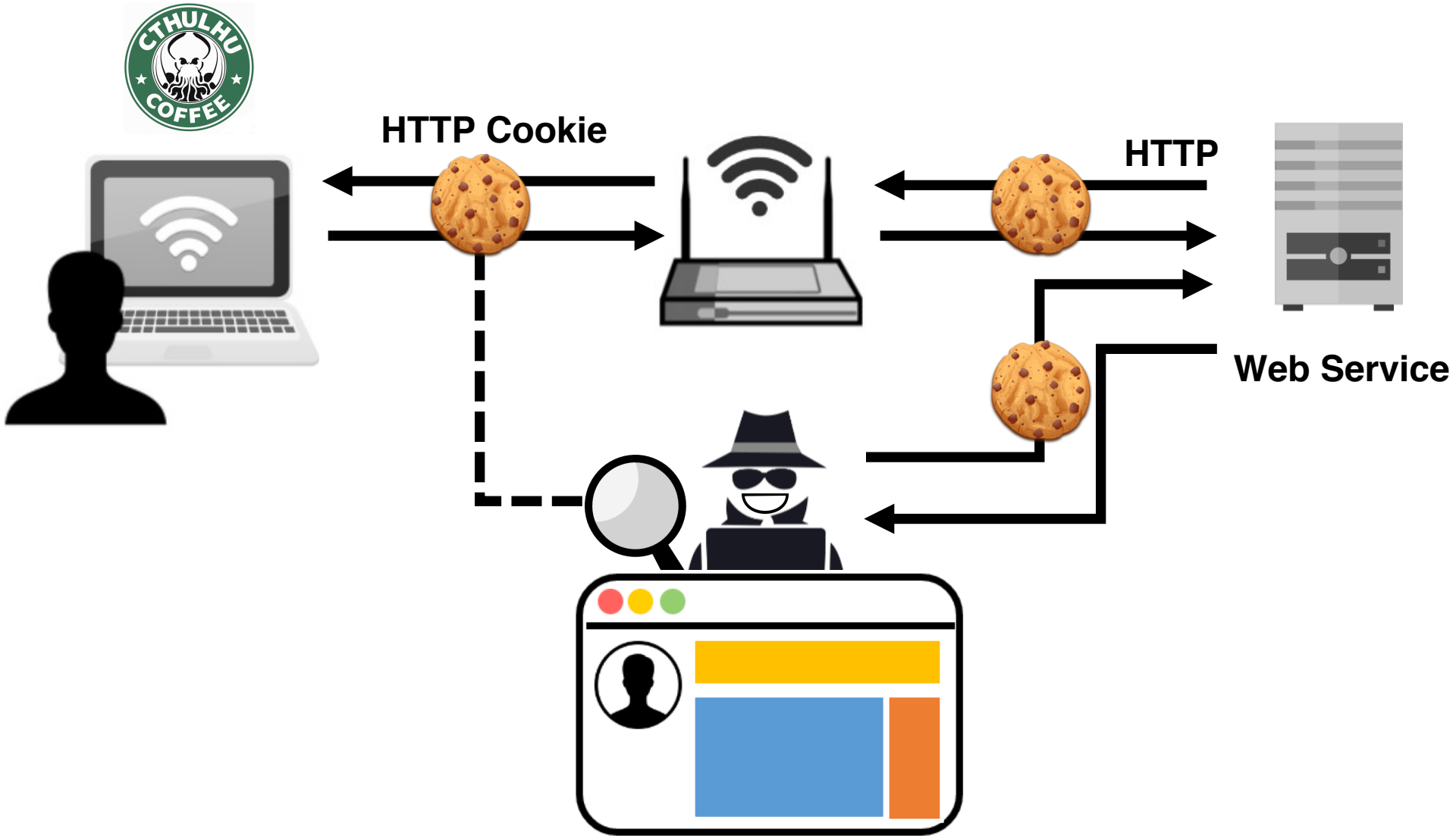
Outline

Bad Cookies!!!

User tracking using third party cookies
(Englehardt et al., WWW 2015)

Cookie injection attacks via HTTP response
(Zheng et al., Usenix Security 2015)

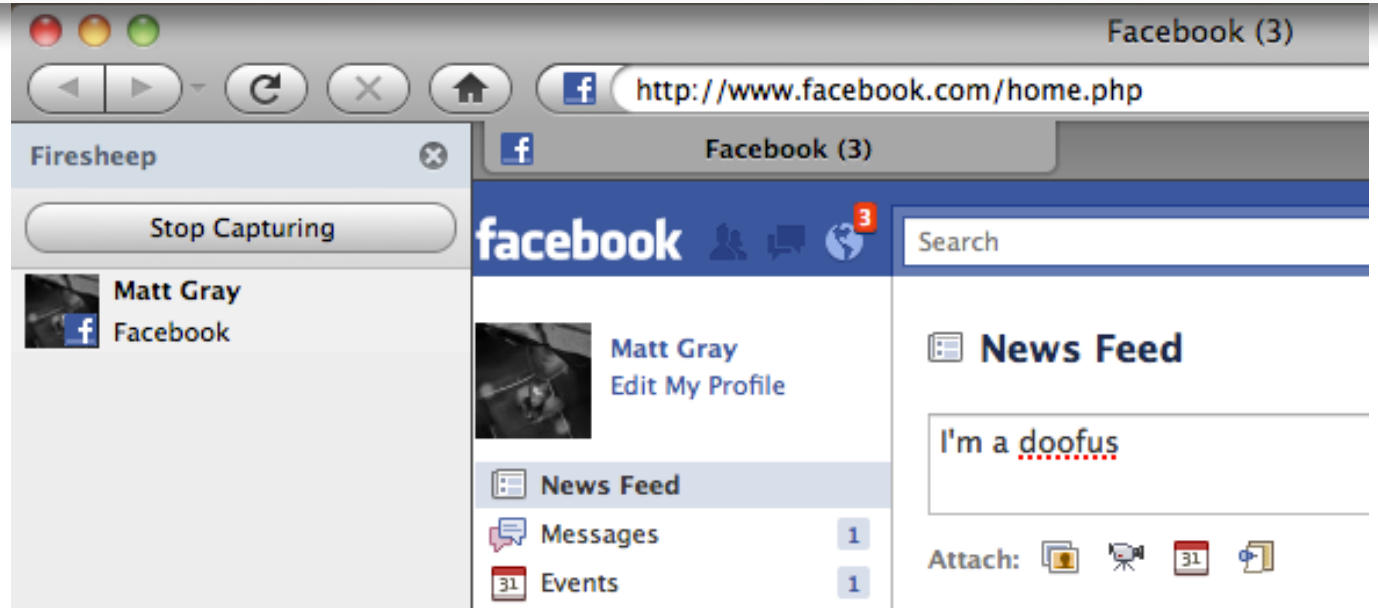
HTTP Cookie Hijacking



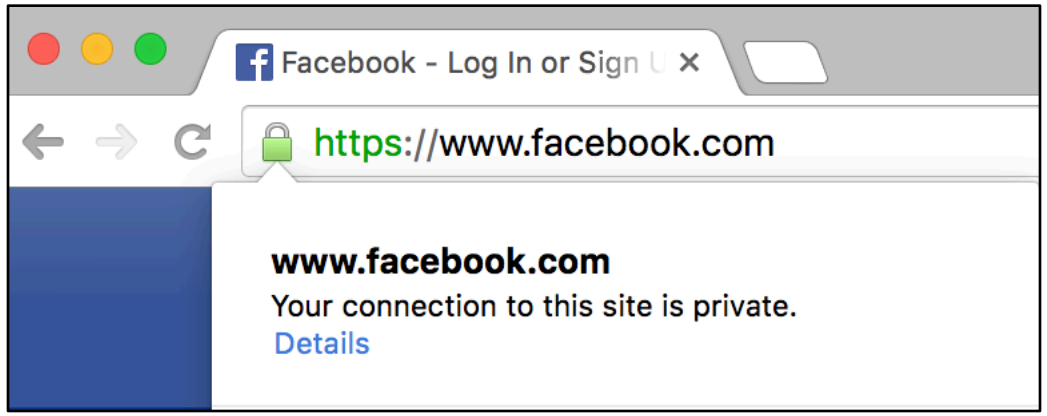
HTTP Cookie Hijacking – Known Threat

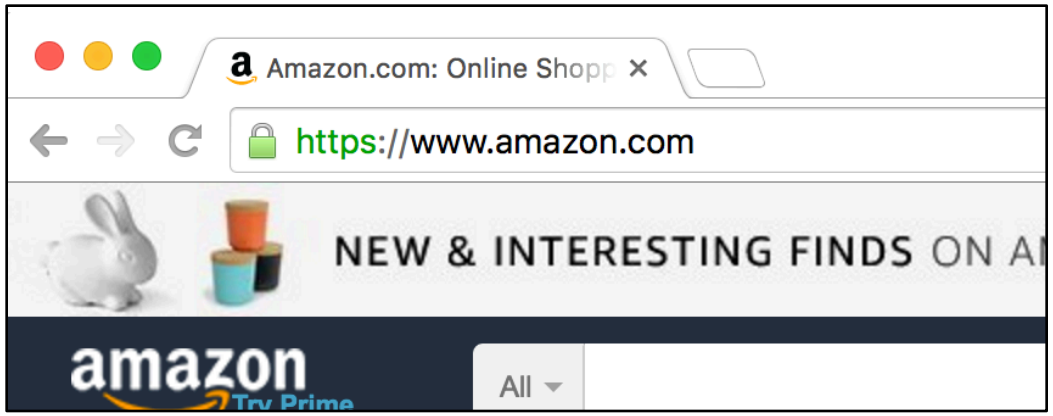
Firesheep In Wolves' Clothing: Extension Lets You Hack Into Twitter, Facebook Accounts Easily

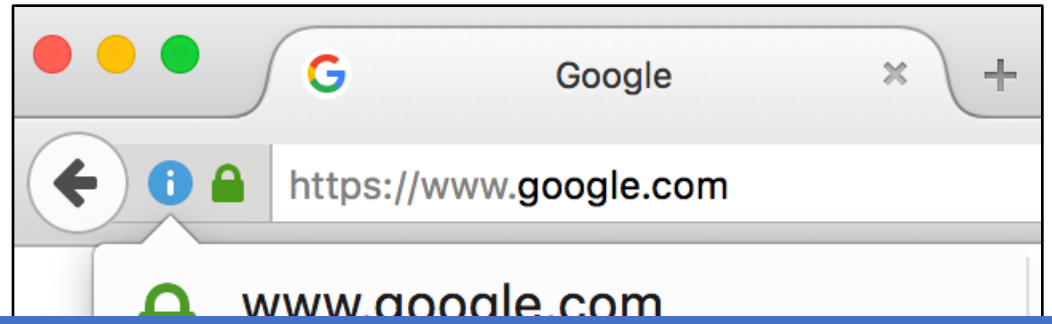
Posted Oct 24, 2010 by Evelyn Rusli

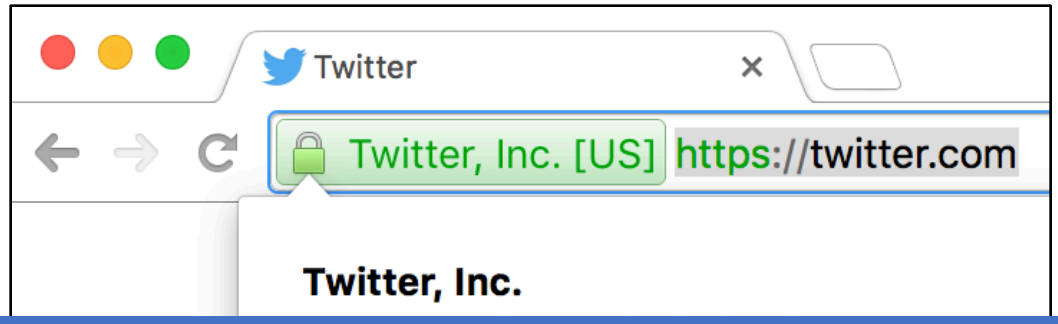


Migrating to HTTPS



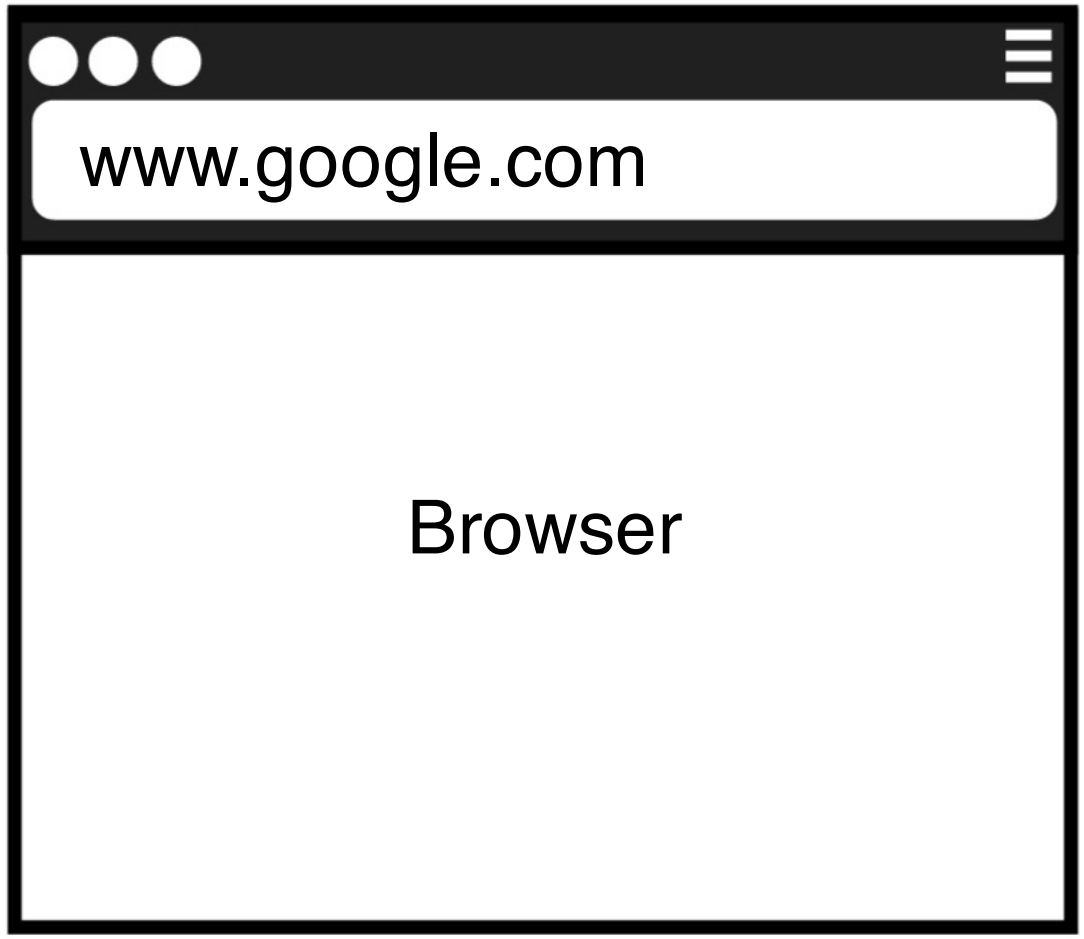


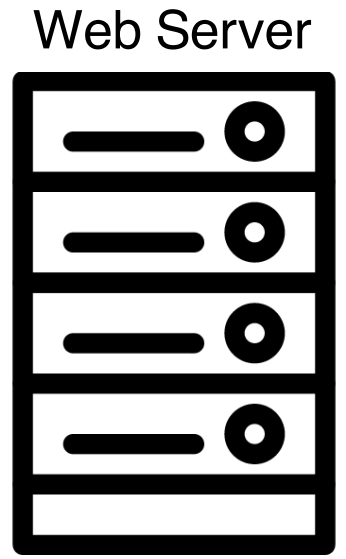




~40% of top sites (140k) on the internet support HTTPS
– SSL Pulse, 2016

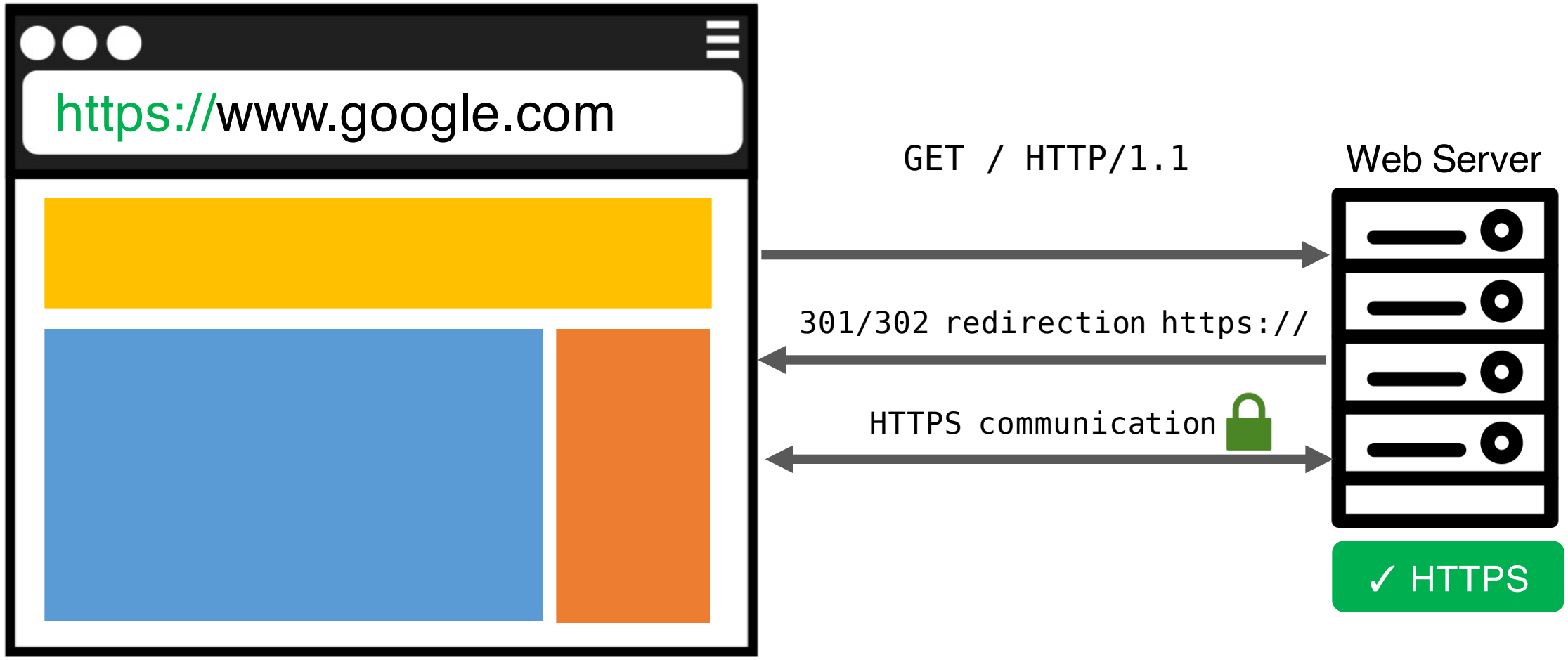
Oh, you thought it was encrypted?



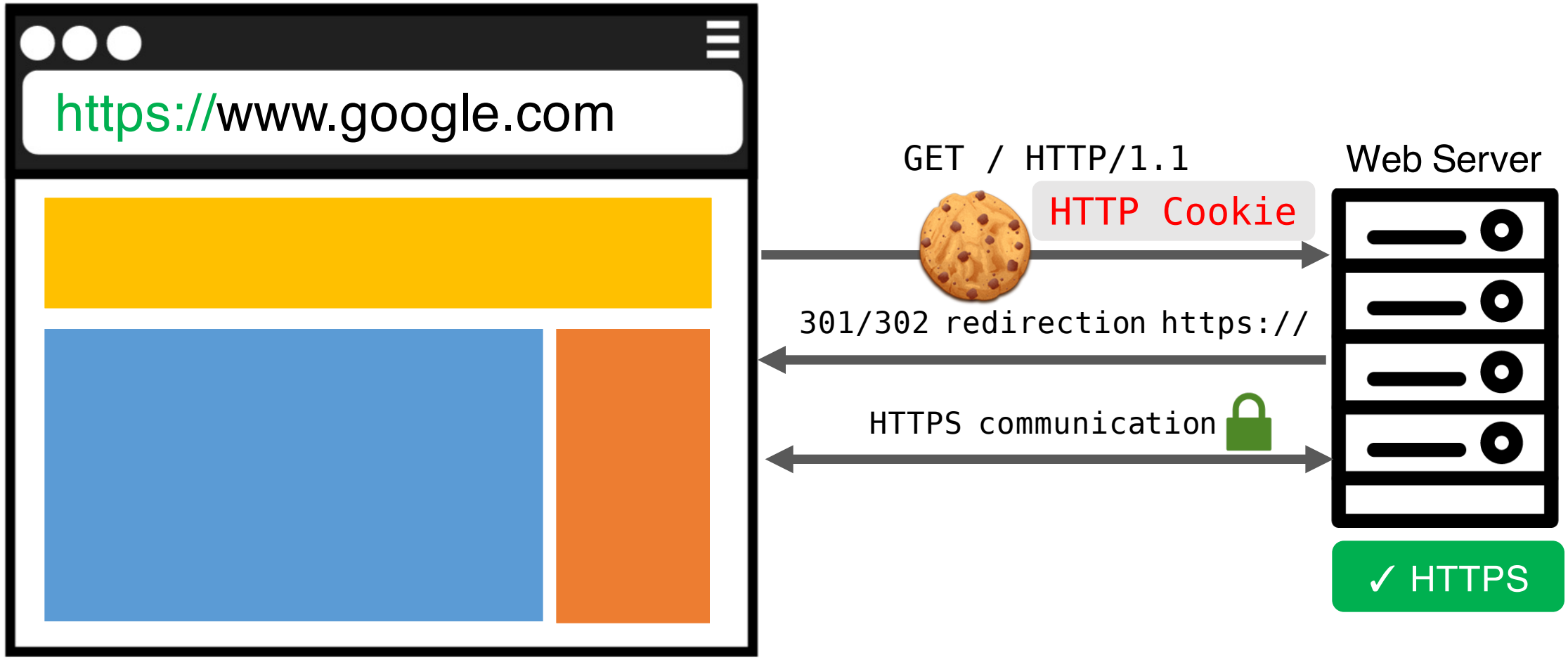


Oh, you thought it was encrypted?

Oh, you thought it was encrypted?



Oh, you thought it was encrypted?



Cookie Hijacking in the Wild

- Studied 25 major services
- 15 support HTTPS, but **not ubiquitous**
  - Offer personalization over HTTP
  - Many cookies, complicated inter-operability → flawed access control
  - Expose sensitive information and/or account functionality

Threat Model

Eavesdropping

- Access to the targeted network
  - **Open Wi-Fi Network**, Wiretapping, Middle box, Proxy, **Tor exit node**
- Network traffic sniffing tools
  - e.g. TCPdump, Wireshark, TShark, Kismet, KisMac
- TCP Reassembly (if necessary)

Stealing the Cookies

- HTTP Request: **Host, Cookie**

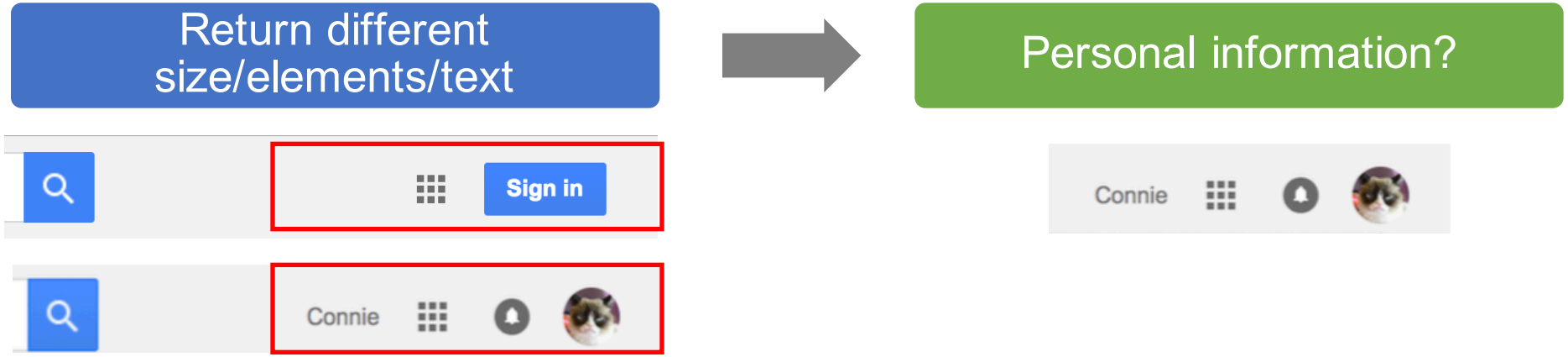
```
GET /dst_path HTTP/1.1
Host:                   www.google.com
Connection:             keep-alive
Cookie:                 SID=XXXXX; HSID=YYYYY; APISID=ZZZZZ
User-Agent:             Mozilla/5.0 (X11; Linux x86_64; rv:47.0)
Gecko/20100101 Firefox/47.0
Accept-Language:        en-US
Accept-Encoding:        gzip, deflate
```

- HTTP Response: **Set-cookie**

```
Set-cookie:             SID=XXXXX; Expires=Mon, 01 Jan 1970 00:00:01 GMT;
Path=/; Domain=.google.com;
```

Accessing the Data

- Send requests with the stolen cookies
  - **Try both HTTP** and **HTTPS**
  - Reveal access control flaws
- Getting personal information?
  - Requests with and without the stolen cookies



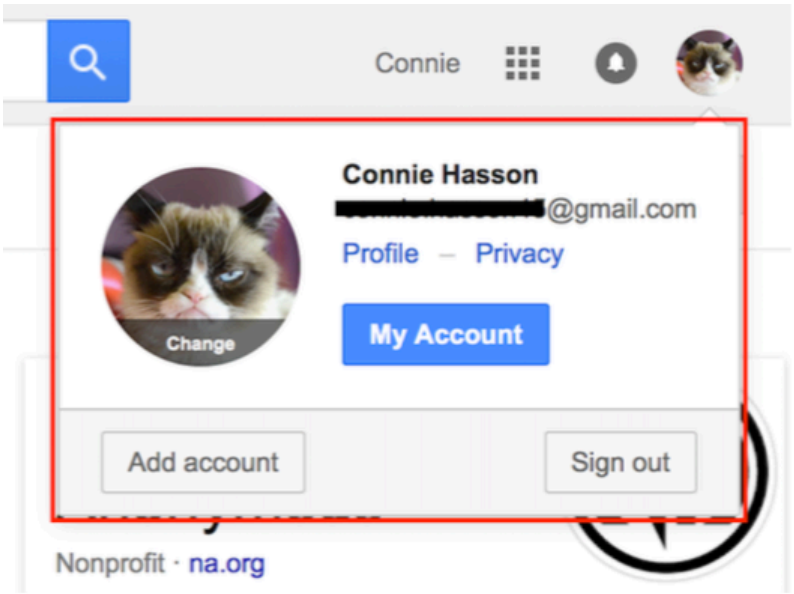
  - curl, Selenium WebDriver, PhantomJS (renders active contents)
  - Identify HTML elements

What can we access using the stolen HTTP cookies?

Search engines

Google | Baidu | Bing | Yahoo

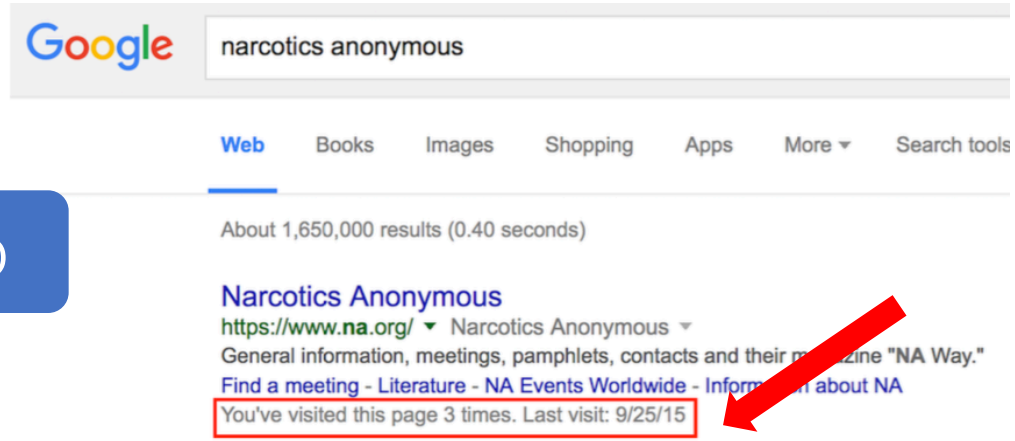
- User information
  email, profile picture, first/last name

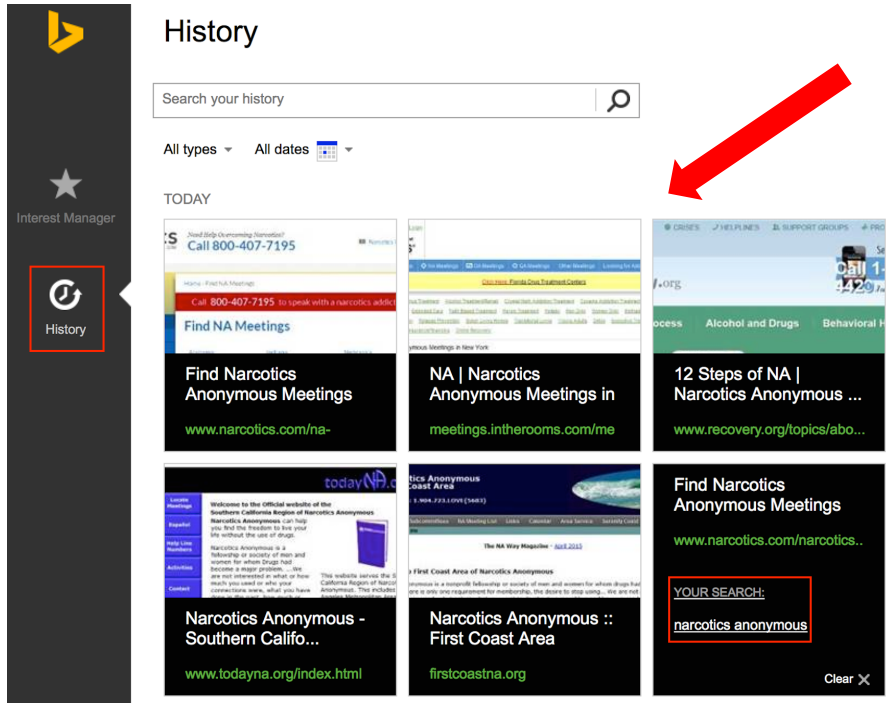


Search engines

Google | Baidu | Bing | Yahoo

- User information
  email, profile picture, first/lastname
- **Search/visited history**

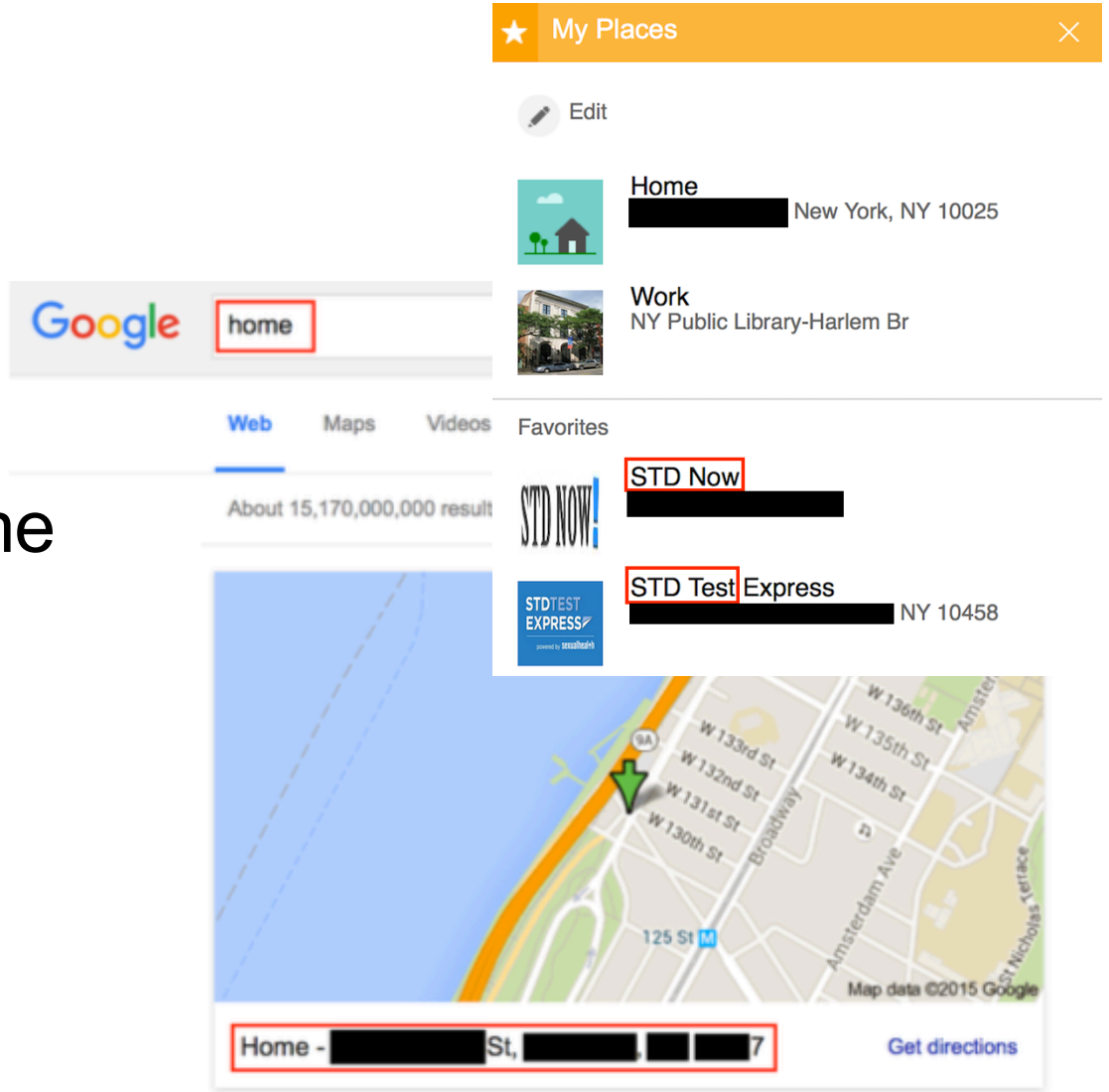




Search engines

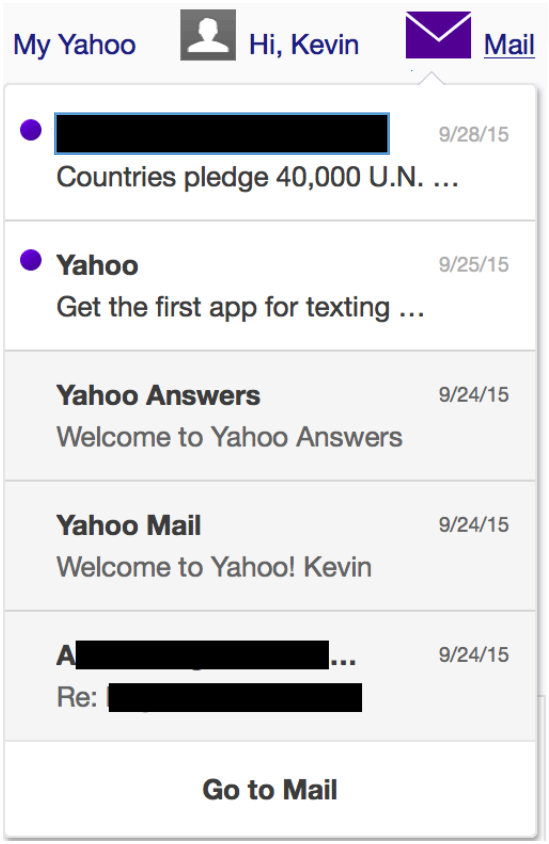
Google | Baidu | Bing

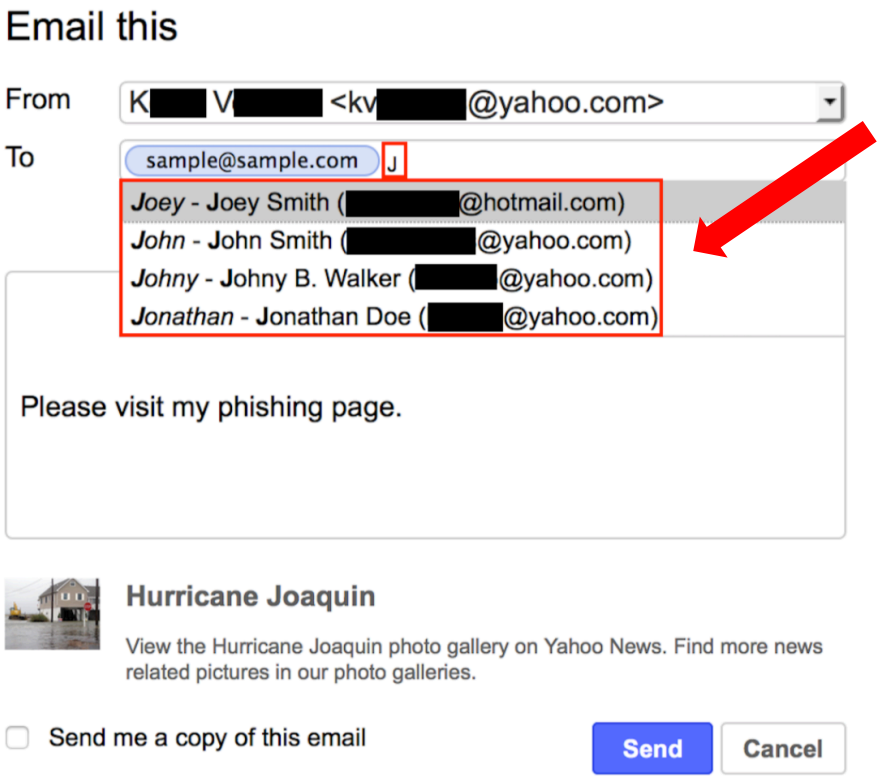
- User information
  email, profile picture, first/lastname
- Search/visited history
- **Saved locations**



Yahoo

- Many services
  - Yahoo answers
- Email notification title and snippet
- Extract contact list
- Send email as user





E-commerce

Amazon | Ebay | Walmart | Target

- All support HTTPS
- HTTPS pages only for login, account and checkout pages
- User information: username, email
- **Items in cart, wish list, recent view items, purchased items**

E-commerce

Amazon | Ebay | Walmart | Target

- All support HTTPS
- HTTPS pages only for login, account and checkout pages
- User information: username, email
- Items in cart, wish list, recent view items, purchased items
- **Ebay reveals shipping address**

E-commerce

Amazon | Ebay | Walmart | Target

- All support HTTPS
- HTTPS pages only for login, account and checkout pages
- User information: username, email
- Items in cart, wish list, recent view items, purchased items
- Ebay reveals full shipping address
- **Facilitate spam and phishing**
  - Send recommendations to any email with custom message

E-commerce

Amazon | Ebay | Walmart | Target

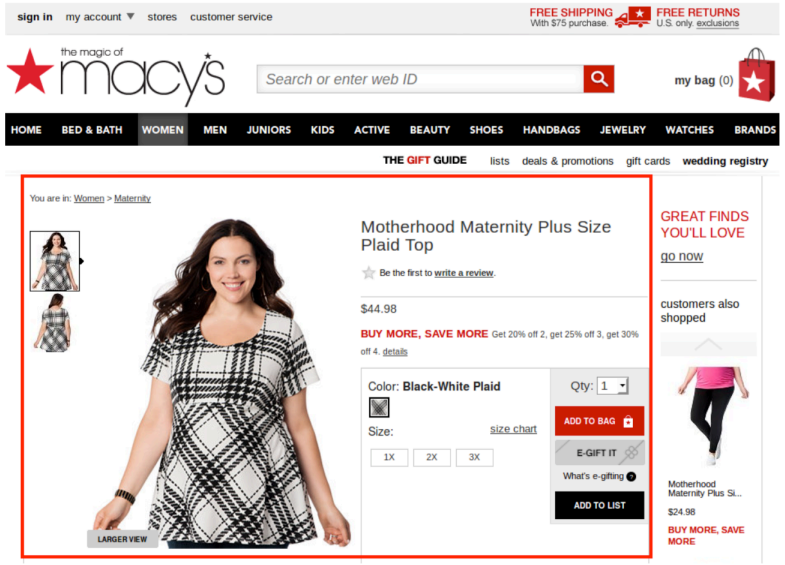
- All support HTTPS
- HTTPS pages only for login, account and checkout pages
- User information: username, email
- Items in cart, wish list, recent view items, purchased items
- Ebay reveals full shipping address
- **Facilitate spam and phishing**
  - Send recommendations to any email with custom message

Amazon now redirects to **HTTPS**, but attack still works!

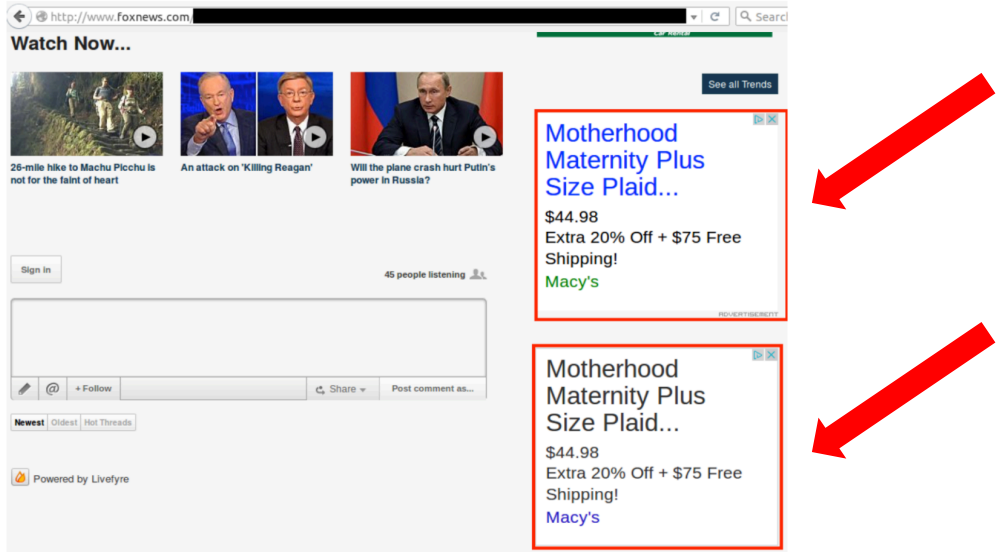
Ad Networks

- Ads presented to user based on user's profile
- Ads reveal browsing history and/or sensitive user data

visited by user



shown to attacker



Cookie Hijacking Cheat Sheet

Site	HttpOnly	non—HttpOnly
Amazon	—	x-main
Bing	—	_U, WLS
Baidu	—	BDUSS
CNN	—	CNNid, authid
Doubleclick	—	id
Ebay	—	cid, nonsession
Google	HSID	SID
Guardian	—	GU_U
HuffingtonPost	huffpost_s	huffpost_user huffpost_user_id last_login_username
MSN	MSNRPSAuth	—
New York Times	—	NYT-S
Target	—	WC_PERSISTENT guestDisplayName UserLocation
Walmart	—	customer, CID
Yahoo	F	T, Y
Youtube	VISITOR_INFO1_LIVE	—

Collateral Exposure – Extensions & Mobile Apps

Name	Type	Browser	#	Cookie leaked
Google Maps	app	Chrome	N/A	✓
Google Search	app	Chrome	N/A	✓
Google News	app	Chrome	1.0M	✓
Amazon Assistant	extension	Chrome	1.1M	✓
Bing Rewards	extension	Chrome	74K	✓
eBay for Chrome	extension	Chrome	325K	✓
Google Dictionary	extension	Chrome	2.7M	✓
Google Hangouts	extension	Chrome	6.4M	✗
Google Image Search	extension	Chrome	1.0M	✗
Google Mail Checker	extension	Chrome	4.2M	✗
Google Translate	extension	Chrome	5.5M	✗
Yahoo Mail Notification	extension	Chrome	1.2M	✗
Amazon	default search bar	Firefox	N/A	✓
Bing	default search bar	Firefox	N/A	✗
Ebay	default search bar	Firefox	N/A	✓
Google	default search bar	Firefox	N/A	✗
Yahoo	default search bar	Firefox	N/A	✗
Amazon 1Button	extension	Firefox	157K	✓
Bing Search	extension (unofficial)	Firefox	28K	✓
eBay Sidebar	extension	Firefox	36K	✓
Google Image Search	extension	Firefox	48K	✓
Google Translator	extension (unofficial)	Firefox	794K	✓
Yahoo Toolbar	extension	Firefox	31K	✓

Application	Platform	Version	#	Cookie leaked
Amazon	iOS	5.3.2	N/A	✗
Amazon	iOS	5.2.1	N/A	✓
Amazon	Android	28.10.15	10-50M	✗
Bing Search	iOS	5.7	N/A	✓
Bing Search	Android	5.5.25151078	1-5M	✓
Spotlight (Bing)	iOS	iOS9.1	N/A	conditionally
Siri (Bing)	iOS	iOS9.1	N/A	✗
Ebay	iOS	4.1.0	N/A	conditionally
Ebay	Android	4.1.0.22	100-500M	conditionally
Google	iOS	9.0	N/A	✗
Google	Android	5.4.28.19	1B+	✗
Gmail	iOS	4.1	N/A	✗
Gmail	Android	5.6.103338659	1-5B	✗
Google Search Bar	Android	5.4.28.19	N/A	✗
Yahoo Mail	iOS	4.0.0	N/A	conditionally
Yahoo Mail	Android	4.9.2	100-500M	✗
Yahoo News	iOS	6.3.0	N/A	✓
Yahoo News	Android	18.10.15	10-50M	✗
Yahoo Search	iOS	4.0.2	N/A	✗
Yahoo Search	Android	4.0.2	1-5M	✗
Yahoo Sports	iOS	5.7.4	N/A	✓
Yahoo Sports	Android	5.6.3	5-10M	✗

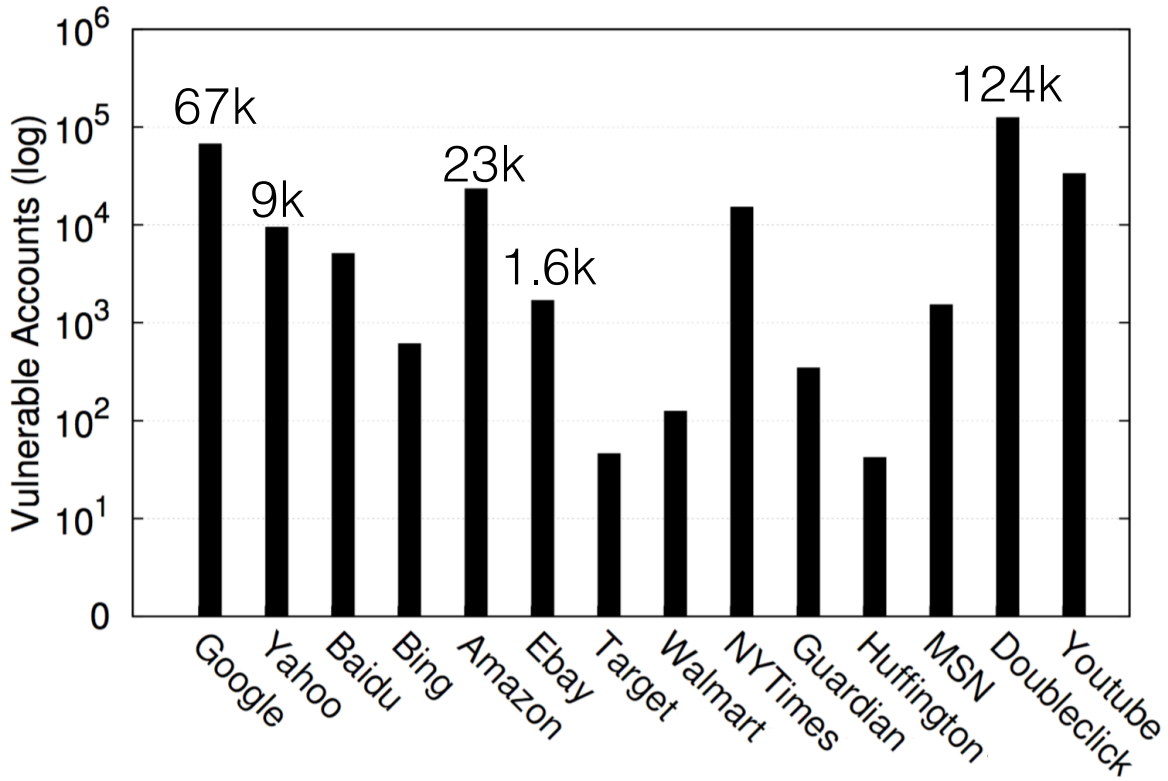
Attack Evaluation

- Different behavior when on public WiFi?
- Mechanisms that prevent hijacking?

- Monitored ~15% of Columbia's public WiFi for 30 days (IRB approval)

- Collected HTTP and HTTPS traffic
  - URL / SNI
  - Cookie name
  - Hash of cookie value (differentiate users per website)

Large-scale Cookie Exposure

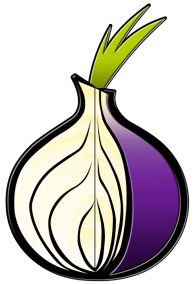


In total, 282K vulnerable accounts

"Government agencies can collect HTTP traffic without notice to users or admins."

– Edward Snowden

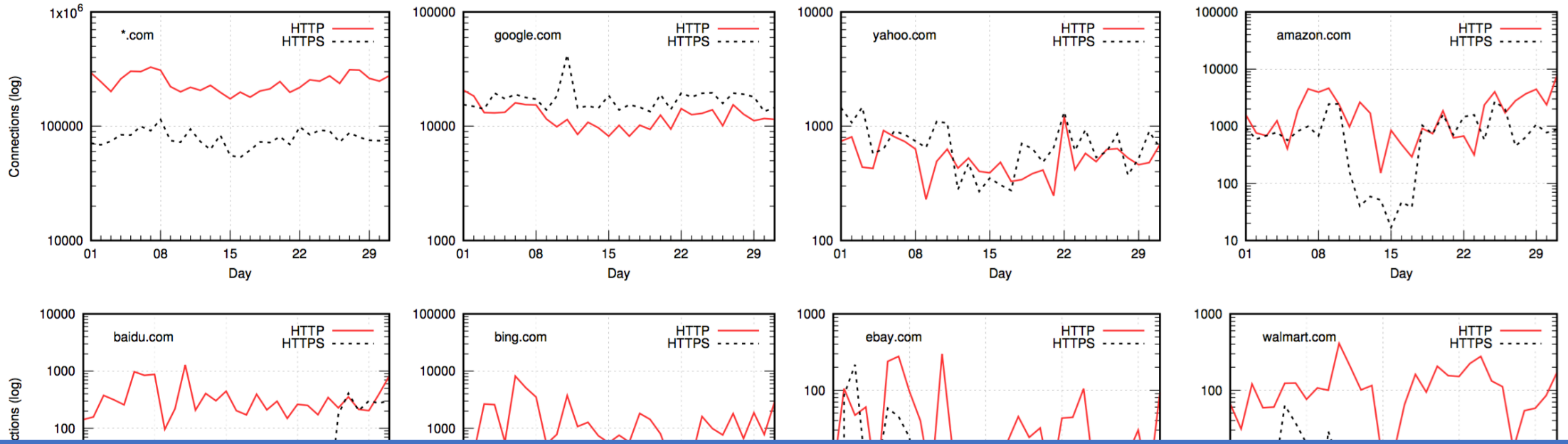
Attack Implications – Tor Network



- Used by privacy-conscious users, whistleblowers, activists
- Tor Bundle is *user-friendly*
  - HTTPS Everywhere pre-installed

- Monitored fresh Tor exit node for 30 days (IRB approval)
- **Did not** collect cookies, only aggregate statistics

Attack Implications – Tor Network



a practical deanonymization attack

Countermeasures

Server-controlled mechanisms

HTTPS Strict Transport Security (HSTS)

HSTS Preload

Client-controlled mechanisms

HTTPS Everywhere

HSTS

- Server instructs browser to only communicate over HTTPS
- HTTP response header sent over HTTPS

```
Strict-Transport-Security: max-age=10886400; includeSubdomains; preload
```

- HSTS Preload protects initial connection to server
  - Eliminates HTTP → HTTPS redirection

HSTS: Issues

- Preload requires HTTPS on all subdomains
  Legacy URL and functionality
- HSTS partial adoption

Main google and regional pages (google.*) still not protected by HSTS

Protected	Not protected
account.google.com mail.google.com	google.com/account google.com/mail

FIXED!

- Early state of adoption and misconfigurations
  [Kranch and Bonneau, NDSS 2015]
- Attacks
  [J. Selvi, BlackHat EU ‘14], [Bhargavan et al., Security and Privacy ’14]

HTTPS Everywhere

- Browser extension from EFF and Tor Project
  - Pre-installed in Tor browser
- Ruleset collections (community effort)

```
<ruleset name="Example">
<target host="example.com" />
<rule from="^http:" to "https:" />
</ruleset>
```

- Regular expressions rewrite “http://” to “https://”

```
http://example.com/foo → https://example.com/foo
```

HTTPS Everywhere: Issues

- Rulesets do not offer complete coverage (also contain human errors)
- Exclude when HTTPS not supported
  Amazon: HTTPS breaks adding products to basket

```
<exclusion pattern="^http://(?:www\.)?amazon\.com/gp/twister/(?:ajaxv2|dynamic-update/)" />
```

- Complicated for large websites

```
http://rcm-images.amazon.com/images/foo.gif
```

```
https://images-na.ssl-images-amazon.com/images/foo.gif
```

HTTPS Everywhere: Effectiveness

- Extract URLs of HTTP requests from WiFi dataset
- Test URLs against rulesets

Services	Exposed Accounts	Reduction
Google	31,729	53.12%
Yahoo	5,320	43.55%
Baidu	4,858	4.63%
Bing	378	38.03%
Amazon	22,040	5.68%
Ebay	1,685	0%
Target	46	0%
Walmart	97	23.62%
NYTimes	15,190	0%
Guardian	343	0.29%
Huffington	42	0%
MSN	927	39.25%

Over 73% of accounts remain exposed!

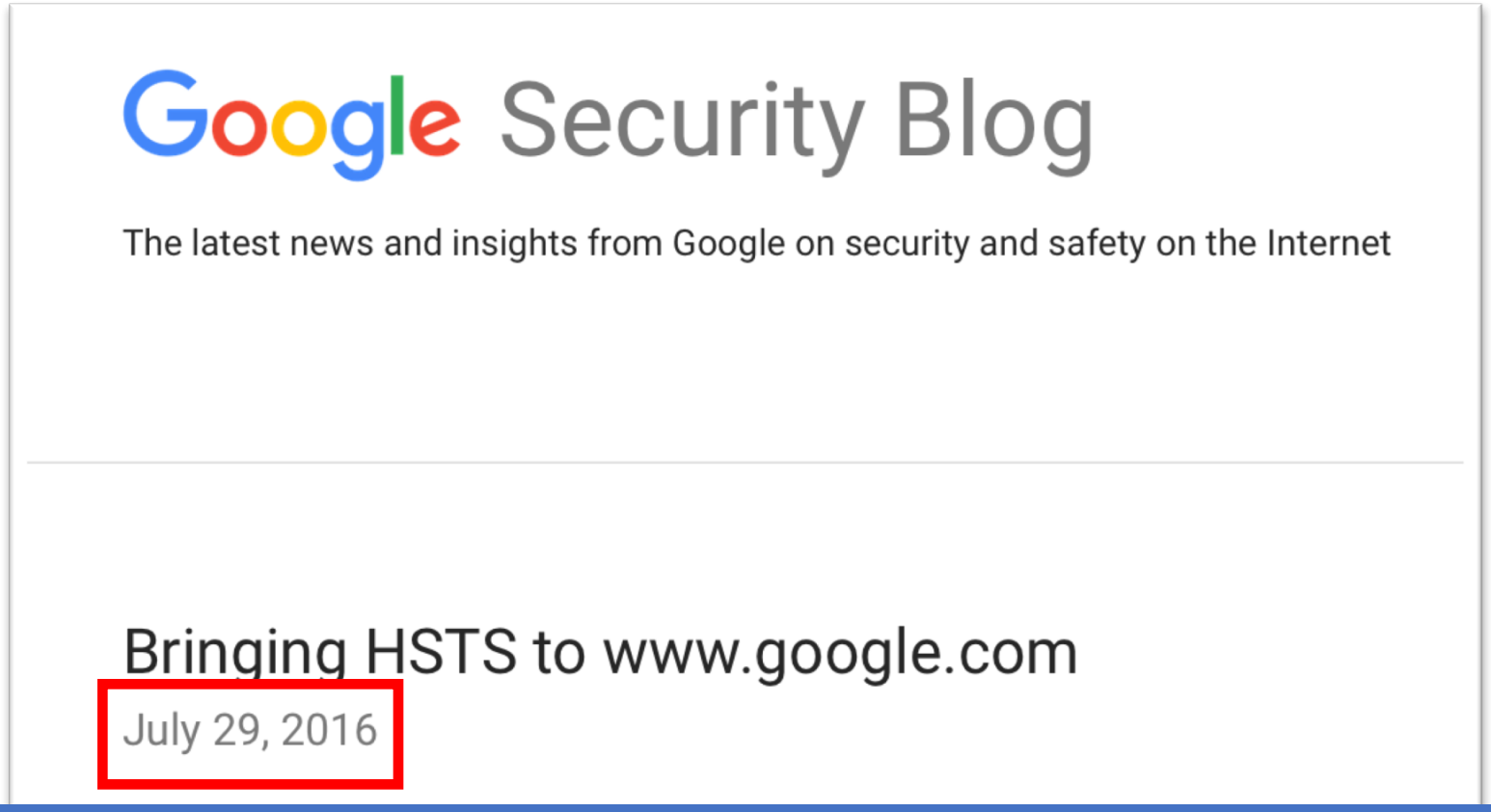
Disclosure

Sent detailed reports to all audited web services

> “The related tokens predate the existence of the HttpOnly setting and have several legacy applications that do not support this setting. On newer applications we're working on new session management tokens that are marked as "Secure" and "HttpOnly".”

> purposes and as such authentication would be required before visiting sensitive areas of an account.”

Aftermath



Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Bringing HSTS to www.google.com

July 29, 2016

Still in testing phase. Max-age is only 1 day.

Sound Bytes

- Back to Basics… *or "always assume the worst"*
  - Cookie hijacking remains a significant (yet overlooked?) threat
- Put in the effort … *or "stop accepting the risk"*
  - Services sacrifice security for usability, and support of legacy codebase
- Halfway is no way… *or "understand the limitations"*
  - Partial adoption of defenses not enough
  - Attack surface reduced, but *a single HTTP request is all you need!*

Questions

Feel free to contact us:

polakis@cs.columbia.edu

suphannee@cs.columbia.edu