HTTP Cookie Hijacking in the Wild: Security and Privacy Implications

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

*Joint primary authors
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?
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

HTTP

Web Service

CTHULHU COFFEE

black hat USA 2016
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?

www.google.com

Browser

Web Server
Oh, you thought it was encrypted?

Browser

http://www.google.com

GET / HTTP/1.1

Web Server

301/302 redirection https://

✓ HTTPS
Oh, you thought it was encrypted?

```
GET / HTTP/1.1

HTTPS communication

301/302 redirection https://

HTTPS communication

✓ HTTPS
```
Oh, you thought it was encrypted?
Cookie Hijacking in the Wild

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

• curl, Selenium WebDriver, PhantomJS (renders active contents)
• Identify HTML elements
What can we access using the stolen HTTP cookies?
Search engines

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

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

- 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

- 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

- 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

- 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

- 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
# Cookie Hijacking Cheat Sheet

<table>
<thead>
<tr>
<th>Site</th>
<th>HttpOnly</th>
<th>non—HttpOnly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>—</td>
<td>x-main</td>
</tr>
<tr>
<td>Bing</td>
<td>—</td>
<td>_U, WLS</td>
</tr>
<tr>
<td>Baidu</td>
<td>—</td>
<td>BDUSS</td>
</tr>
<tr>
<td>CNN</td>
<td>—</td>
<td>CNNId, authid</td>
</tr>
<tr>
<td>Doubleclick</td>
<td>—</td>
<td>id</td>
</tr>
<tr>
<td>Ebay</td>
<td>—</td>
<td>cid, nonsession</td>
</tr>
<tr>
<td>Google</td>
<td>HSID</td>
<td>SID</td>
</tr>
<tr>
<td>Guardian</td>
<td>—</td>
<td>GU_U</td>
</tr>
<tr>
<td>HuffingtonPost</td>
<td>huffpost_s</td>
<td>huffpost_user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>huffpost_user_id</td>
</tr>
<tr>
<td></td>
<td></td>
<td>last_login_username</td>
</tr>
<tr>
<td>MSN</td>
<td>MSNRPSAuth</td>
<td>—</td>
</tr>
<tr>
<td>New York Times</td>
<td>—</td>
<td>NYT-S</td>
</tr>
<tr>
<td>Target</td>
<td>—</td>
<td>WC_PERSISTENT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>guestDisplayName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UserLocation</td>
</tr>
<tr>
<td>Walmart</td>
<td>—</td>
<td>customer, CID</td>
</tr>
<tr>
<td>Yahoo</td>
<td>F</td>
<td>T, Y</td>
</tr>
<tr>
<td>Youtube</td>
<td>VISITOR_INFO1_LIVE</td>
<td>—</td>
</tr>
</tbody>
</table>
## Collateral Exposure – Extensions & Mobile Apps

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

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

TOR users become FBI's No.1 hacking target after legal power grab
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
  account.google.com
  mail.google.com
  Not protected
  google.com/account
  google.com/mail

• Early state of adoption and misconfigurations
  [Kbranch 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 Everywhere: Effectiveness

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

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

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"."
Aftermath

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