Hannah McLaughlin

Web Tracking Lab

CIS5370 – Computer Security

Task 1: Understand the basic working of the web tracking

I began by clearing my history and cache in the InPrivate Firefox browser. Next, I closed out my current tab, opened a new NON-Private tab and navigated to the `Elgg` website. This was a blank page with nothing under "Latest activity." In separate tabs, I opened the `CameraStore, MobileStore, ElectronicsStore,` and `ShoeStore`. I clicked on a product and viewed the details on each store page. I navigated back to the `Elgg` website and refreshed the page to find that the camera I viewed was on the homepage. Even after closing the tab and opening it up again, the camera preview picture was still there.

Task 2: Importance of cookie in Web tracking

I opened up the `MobileStore` and the LiveHTTPHeader tool. I clicked on the second product and captured the traffic. The **HTTP Request** was GET /track.php?guid=1500189875939495 HTTP/1.1 and the **Cookie**: track=3471629850949556

---

http://www.wtlabadserver.com/track.php?guid=1500189875939495

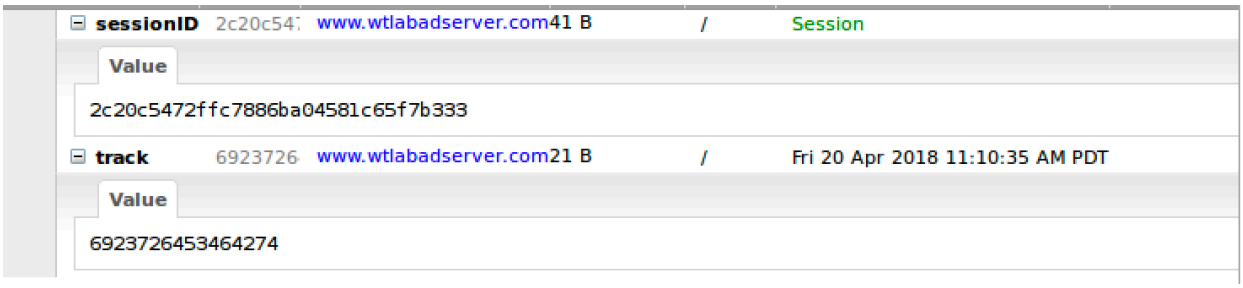
GET /track.php?guid=1500189875939495 HTTP/1.1
Host: www.wtlabadserver.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.wtmobilestore.com/productDetail.php
Cookie: track=3471629850949556
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 10 Apr 2018 16:51:54 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.14
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 21
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Next, I opened the page source and found the request for the tracking cookie. It looks like it sends the product ID to the track.php file which probably returns the tracking cookie.

```
    </div>
</div>
<div class="clear">
    <img width="1" height="1" src="http://www.wtlabadserver.com/track.php?guid=1500189875939495"  />
</div>
```

Next, I opened the `MobileStore` clicked on a product. I also opened another tab with wtlabadserver.com. I opened the Firebug extension and analyzed the cookie. This is considered a third-party tracking cookie because the domain "wtlabadserver.com" is different from the `MobileStore` domain. The cookie was the same for both tabs. (The cookie value changed because I redid the task and cleared my history and cache)



Task 3: Tracked user interests and data

I began by clearing my history and cache and opened fresh tabs for the `MobileStore, ElectronicsStore, ShoeStore,` and `CameraStore`. I clicked on a product on each page. Next, I opened another tab to view the preferences.php page. Below is a screenshot.

Product Guid	Product	Category	Impression Count	UserTrackID
6449377887088520	Canon	Camera	1	9902404778554600
1264893761278606	Woodland	Shoes	1	9902404778554600
9836573923177230	Videocon	Electronic LCD	1	9902404778554600
8326918373014243	HUAWEI	Mobiles	1	9902404778554600

Every item that I previewed was stored in the database with my specific UserTrackID. I decided to go back to the `ShoeStore`, refresh the page and look at another shoe to see how the preferences page would change. You can clearly see that the items I viewed changed in the table.

Product Guid	Product	Category	Impression Count	UserTrackID
6449377887088520	Canon	Camera	1	9902404778554600
3957353166949466	Adidas	Shoes	2	9902404778554600
1264893761278606	Woodland	Shoes	1	9902404778554600
9836573923177230	Videocon	Electronic LCD	1	9902404778554600
8326918373014243	HUAWEI	Mobiles	1	9902404778554600

When I closed all of the tabs and went back to the shoe store to view another product, I noticed that my UserTrackID did not change.

Task 5: Tracking in a Private browser window

I started by opening a Private browsing session. I navigated to the Elgg website and saw a blank page. In some new tabs, I opened up products on each of the product websites. I refreshed the InPrivate browser and discovered a the camera that viewed on the web page. When I closed the browser and opened a new InPrivate browser, the page went back to blank. However, when I opened a regular browser, I saw the last pair of shoes (from Task 2) that I browsed, because the cookie was still stored in my browser.

Task 6: Real World Tracking

In this task, I visited www.amazon.com to identify the HTTP request and response and cookies in `LiveHTTPHeaders`. It looks like it does a HTTP Post request and the response (second picture) is a HTTP/1.1 202 Accepted. Amazon sends three different cookies to enhance web tracking: a session ID, a session ID-time, and session-token.

```
POST /ah/ajax/record-impressions?c4i=ePm_fHprxdHLCsIwEIXhJxqYJNNclkpFpBsREbeTZIJSsaIFEV_eCoJQBZfuzuJffec-Es5y...
Host: www.amazon.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
```

```
HTTP/1.1 202 Accepted
Content-Type: text/html;charset=UTF-8
Content-Length: 0
Connection: keep-alive
Server: Server
Date: Tue, 10 Apr 2018 18:47:07 GMT
Strict-Transport-Security: max-age=47474747; includeSubDomains; preload
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
X-UA-Compatible: IE=edge
X-Frame-Options: SAMEORIGIN
Set-Cookie: session-id=141-8078171-6248433; Domain=.amazon.com; Expires=Tue, 01-Jan-2036 08:00:01 GMT; Path=/
Set-Cookie: session-id-time=2082787201l; Domain=.amazon.com; Expires=Tue, 01-Jan-2036 08:00:01 GMT; Path=/
Set-Cookie: session-token=NbaeaK19qfshuoQXNykI7BNyMM6I5URY9QmPGn9CdnHLq3yw9rA8j4UxdyHqj7Zmssn1II0+gTFLo…
Vary: Accept-Encoding,User-Agent
X-Cache: Miss from cloudfront
Via: 1.1 65aebe266f727f3ba28b110424962e9e.cloudfront.net (CloudFront)
X-Amz-Cf-Id: dyO0IlLFWRLbGnUJeraoZ5fWKfAZbYYKuHRM7pY-SWiV_hzDNOIGlw==
```

The third party cookie for Amazon is .amazon.com, which isn't too shocking that a mega company like Amazon sends their own cookies. However, since the domain is the same, I'm not sure if this is considered a "third-party" cookie.

Task 7: Countermeasures

To turn off third party cookies, I went to Edit -> Preferences -> Privacy. In the drop down menu, I selected Never so that third party cookies are never saved. Next I navigated to the ShoeStore and opened the LiveHTTPHeader and selected a product. In the screenshot below, you can see that the HTTP GET request set the cookie, but now it has an expiration date.

```
http://www.wtlabadserver.com/track.php?guid=8678892570671441

GET /track.php?guid=8678892570671441 HTTP/1.1
Host: www.wtlabadserver.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.wtshoestore.com/productDetail.php
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 10 Apr 2018 19:01:44 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.14
Set-Cookie: track=4334184875043687; expires=Fri, 20-Apr-2018 19:01:44 GMT
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 21
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Hannah McLaughlin

On the `Elgg` website, I did not notice any product previews since third party cookies were disabled. When I looked at the LiveHTTPHeader feed where it sent its request to the ad server, this is what I saw:

http://www.wtlabadserver.com/displayads.php

```
GET /displayads.php HTTP/1.1
Host: www.wtlabadserver.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
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
Referer: http://www.wtlabelgg.com/
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 10 Apr 2018 19:06:18 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.14
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 20
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Previously there was a cookies section (in Task 4), but now it has disappeared. There no longer needs to be an exchange of cookies.