1 Prepraration

1. Make sure you have Burp Suite installed, with its certificate installed as well; proxy setting in your browser is correct so that Burp Suite will serve as your proxy.

2 Background

Cookies are typically represented by name-value pairs, but they can have more attributes, including domain, path, expiration, etc. In this lab session, we want to figure out how Google deals with multiple accounts signed in from the same browser.

3 Instructions

1. Login to your BSU email account, and then login to your gmail account, using the same browser. If you look at the address bar, you should see something like: https://mail.google.com/mail/u/0/#inbox and https://mail.google.com/mail/u/1/#inbox.

2. Switch to Burp Suite, and make sure the 'Intercept' is on. Refresh your BSU email page, and observe what cookies are sent to Google. Turn "Intercept" off and then turn "Intercept" on. Refresh your gmail page, and observe what cookies are sent to Google. Pay attention to these cookies: SID, SSID, HSID, APISID, SAPISID, and GMAIL_AT. Basically these 6 cookies tell Google who you are. When you send two requests (Request #1 representing the first "refresh" operation and Request #2 representing the second "refresh" operation) to Google, if these 6 cookies in Request #1 are exactly the same as those 6 cookies in Request #2, then Google won’t be able to distinguish your two accounts. Therefore, (at least) one of these 6 cookies has to be different in Request #1 and Request #2, which one?

3. Every time when you access a URL, the unexpired cookies whose domain and path attributes match with the requested URL will be sent to the server. Two cookies can have the same name, and they can be co-existing in your computer as long as they have different domain/path attributes. GMAIL_AT is such an example - when you have multiple google accounts, you may have multiple cookies named GMAIL_AT, their domains are the same - mail.google.com; but their paths should be different. Examine the domain and path attributes of each GMAIL_AT cookie, and you will find out which GMAIL_AT cookie was sent in which request (Request # 1 or Request #2). Here
is how you can view your cookies for different browsers. https://kb.iu.edu/d/ajfi (Hints: these 6 cookies belong to either the site google.com or the site mail.google.com).

4. Turn "Intercept" on. Log out of either your BSU email account or your gmail account, see if the other account will be automatically logged out. Make sure you intercept the response (of that log out request). Examine the response and pay attention to Set-Cookie headers, then you will find out why the other email account is also out.

4 Takeaway

1. In lab session-2, we learned that if someone can capture your SID and HSID, he can figure out your email address, your first name, and your last name. In fact, when you have only one google account, Google use SID, SSID, HSID, APISID, SAPISID to identify you; when you have multiple google accounts, Google will use other cookies to distinguish your multiple accounts. GMAIL_AT is such an example. When you access multiple gmail accounts, the URLs will be different, and the PATH attribute of the GMAIL_AT cookies will be different as well. Cookies whose domain and path attributes match with the domain and path of the URL will be included in the request and sent to the server. This is why you can have two gmail pages active at the same time.

2. When you log out, Google would set SID, SSID, HSID, APISID, SAPISID to EXPIRED; but it wouldn’t do anything with GMAIL_AT, however, without a valid SID, SSID, HSID, APISID, SAPISID, you won’t be able to access any of your Google/Gmail accounts. Therefore you have to sign in again to access your Google accounts.

5 Extra Instructions

If you have time, you can also try something to understand another cookie attribute: HttpOnly. This attribute, if is set, means that cookie can not be accessed by Javascript; namely, it can only be sent over HTTP/HTTPS traffic.

In your address bar, type in this:

javascript:alert(document.cookie);

It will show you which cookie is accessible via Javascripts. Among the above 6 cookies, you should only see 4 of them, as the other 2 have that HttpOnly attribute set. Figure out which two.