Tutorial 3: Solutions

Computer Security
School of Informatics
University of Edinburgh

November 14, 2016

The outreach pages you visited in this tutorial are part of an effort to make security and privacy more salient to the general population by giving them the tools necessary to see how security and privacy impact them.

1 Cookies: create a basic cookie

Step 4: Online cookie setting page In this step you opened a webpage on vaniea.com which set a cookie on your computer. You needed to find several ways to get the webpage to forget who you are:

- Delete the cookie using a cookie editor like Cookie Manager+
- Set Firefox to not accept cookies
- Set Firefox delete cookies when the browser is closed
- Open another web browser like Chrome or Internet Explorer (cookies do not travel between browsers)
- Open a new profile on Firefox (cookies are not shared between profiles)
- Use the Firefox Tor browser bundle which already has settings to delete cookies periodically
- Use a different computer entirely (may not work with Chrome which likes to sync data)
- Change the content of the cookie which will cause the site to get different information

Step 5: Cookies on multiple websites In this step you looked at two different web pages located on two different sites: vaniea.com and kamivaniea.com. The step asks you to make one site forget who you are without making the other site forget who you are. To do this you just need to delete the cookie. Deleting, or modifying, the cookie is the only correct answer. The rest of the answers from Step 4 will delete both cookies.

You are also asked to try adding 'www' to the front of the web address. So that vaniea.com becomes www.vaniea.com. Doing so will cause it to ask you for your name again and then put your new name on the top of the page, while your prior answer to your name will still show up in one of the boxes. It does this because cookies are linked not only to a domain but also to the subdomain. So a cookie for www.vaniea.com is not shared with vaniea.com by default. If you visit: `http://www.vaniea.com/teaching/privacyToday/cookieAdExample.html` you will actually set and read three different cookies from three different sites: www.vaniea.com, vaniea.com, and kamivaniea.com.

2 Web bugs and browser fingerprinting

Step 1: Look at the data your browser shares with websites In this step you used Panopticlick to learn what kinds of data web pages can learn about your web browser.

Opening in two different web browsers should cause quite a few data elements to change. For example, the user agent string should change. The list of plugins should also be different.

Opening Panopticlick in Private Browsing mode should cause only a few things to change. The list of plugins should get shorter, Private Browsing mode disables unique plugins. It is hard to predict everything that will change since the code just generally tries to make you less identifiable.

Step 2: Change the data you send to websites In this step you installed a plugin that modifies the user agent string.

When you modify the user agent string to be a mobile device some web pages will start redirecting you to their mobile version. This should be very clear on twitter. Facebook will also do it.

Some websites show you different content depending on what software you are running. In extreme cases they even change the price or sort order of items based on what device you are on. You can control how sites see you by modifying the user agent string.