University of Colombo School of Computing

IS 2009- Information Systems Security

Lab Session- I

SECURE WEB BROWSING

Threats in Web Browsing:

Your web browser is the vehicle you use to surf the dangerous territory of world wide web. There are so many potential threats to you from the things and people out there. It is really important to understand these threats and configure your web browser to protect you from those threats. It is not easy to teach each and every important point you need to remember to be safe on the web. You have to search and read about threats you face while browsing the web on your computer.

A good reference as a start point:
https://www.us-cert.gov/publications/securing-your-web-browser
https://www.tutorialspoint.com/internet_security/index.htm

Private Browsing:

Your web browser keeps track of activities you perform in the web. In order to stop it from doing so, you can use the private browsing mode of your web browser.

1. ***Purpose of Private Browsing***

Private browsing, **privacy mode** or **incognito mode** is a privacy feature in some web browsers to disable browsing history and the web cache. This allows a person to browse the Web without storing local data that could be retrieved at a later date. Privacy mode will also disable the storage of data in cookies and Flash cookies.

2. ***Which occasions can you use them?***

- **Signing into multiple email accounts at once**

  You could set up different browser "profiles" to switch between email accounts within one browser, but the private or the incognito mode is the quick and easy way of doing this on the fly— no setup required.

- **Using computers that aren't yours**

  If you need to log into your email or your banking account or whatever on a computer away from home, just pop open incognito mode to provide a layer of protection against your passwords or user info being

saved to that computer (not totally infallible, that computer could have keystroke logging software on it or something, but it helps).

3. ***Private browsing in different browsers.***

   a. *Chrome*: Menu -> New incognito window (CTRL + SHIFT + n)
   b. *Firefox*: Menu -> New Private window (CTRL + SHIFT + p)

4. ***What is tracking protections in browsers?***

Tracking generally refers to the collection of a person's browsing data across multiple sites.
The **Tracking Protection** feature uses a list provided by Disconnect to identify and block trackers.

   a. *Chrome :*
      Settings -> Advanced -> Send a "Do not track " request with your browsing traffic
   b. *Firefox :*
      Menu -> Options -> Privacy & Settings -> Tracking Protection Section

Browser History, Cache and Cookies:

Your web browser keeps track of activities you perform in the web. You can decide which information your browser should keep and which should not.

1. ***What is history in web browsers?***

A browser's history is a log of sites that you visit. When you press a browser's Back button, you are moving back one entry in the history log. Browsers will normally clear history at regular intervals, but you may want to clear it manually for privacy reasons.

2. ***What is cache in web browsers and what is it for?***

Each time you access a file through your web browser (Internet Explorer, Firefox, Chrome, etc), the browser caches (i.e., stores) it so it doesn't have to keep retrieving the same files or images from the remote web site each time you click Back or Forward.

Browser cache or temporary internet files are a way that browsers download website images, data and documents for faster viewing in the future. By keeping a local copy of some website information, your browser will be able to load at least some information from each page you have visited without downloading that information again from the server. This can decrease the time it takes to load a webpage.

The downside is that the information on a website may have changed while your browser loads an older version. It is recommended that you clear your browser cache every few weeks to keep it running efficiently. You may want to configure your browser's settings to delete or remove your browser's cache upon closing or exiting the browser window.

3. ***What is cookies in web browsers, what information is stored there and what are they used for?***

A cookie is a file created by a web browser, at the request of a website, that is stored on a computer. It is a passive file and can not spread computer viruses or other malicious programs.

They can store previous activity on that site and user preferences so this information can be retrieved the next time you visit the same site. These files typically store user-specific information such as selections in a form, shopping cart contents, or authentication data. Cookies may also be used by 3rd parties to track a user's browser history over a long period of time which can be considered a privacy concern.

Often cookies help analyze how the website is used, and the web editor can improve the user experience. In several cases, cookies may be necessary to provide a service.

Cookies are mostly erased automatically from the browser when it is closed (so-called session cookies). Cookies can also be set with an expiration time so that data exists for a shorter or longer period (persistent cookies).

Browsers will normally clear cookies that reach a certain age, but clearing them manually may solve problems with websites or your browser. It is recommended that you clear your browser cookies every few weeks to keep it running efficiently. You may want to configure your browser's settings to not accept cookies (on work computers) or remove cookies upon closing or exiting the browser window.

4. What is cookie theft?

Cookie theft occurs when a third party copies unencrypted session data and uses it to impersonate the real user. Cookie theft most often occurs when a user accesses trusted sites over an unprotected or public Wi-Fi network. Although the username and password for a given site will be encrypted, the session data travelling back and forth (the cookie) is not.

5. What is session hijacking?

Cookie hijacking is a hacking process by which the hacker gains unauthorized access to some confidential information in a way which is not facilitated by the user or a secure session.

Cookie hijacking can be performed by the hacker by using a computer between the node and server or by obtaining access to the cookies stored on the user's computer. A hacker can also use source router Internet protocol or IP packets to gain unauthorized access between two communicating nodes. The hacker would then route the packets containing cookies to pass through his computer before reaching the destination.

Cookie hijacking sometimes is used to perform denial of service attacks also known as DOS attacks.

Study on the above topics and answer the following.

1. How safe is private browsing?
2. What are the things you can't use Private Browsing?
3. What are the disadvantages of private browsing?
4. What are the kinds of caches?
    a. Browser Caches
    b. Proxy Caches
    c. Gateway Caches
5. How to view cookie details on your browser?

Your answers should be in a PDF named with your eight-digit index number.
(Ex: 16XXXXXX.pdf)