COOKIES AND ITS USES

Cookie, also known as a **web cookie**, **browser cookie**, and **HTTP cookie**, is a text string stored by a user's web browser. A cookie consists of one or more name-value pairs containing bits of information, which may be encrypted for information privacy and data security purposes.

The cookie is sent as an HTTP header by a web server to a web browser and then sent back unchanged by the browser each time it accesses that server. A cookie can be used for authentication, session tracking (state maintenance), storing site preferences, shopping cart contents, the identifier for a server-based session, or anything else that can be accomplished through storing textual data.

As text, cookies are not executable. Because they are not executed, they cannot replicate themselves and are not viruses. However, due to the browser mechanism to set and read cookies, they can be used as spyware. Anti-spyware products may warn users about some cookies because cookies can be used to track people—a privacy concern.

Most modern browsers allow users to decide whether to accept cookies, and the time frame to keep them, but rejecting cookies makes some websites unusable.

Uses

Session management

Cookies may be used to maintain data related to the user during navigation, possibly across multiple visits. Cookies were introduced to provide a way to implement a "shopping cart" (or "shopping basket"),[2][3] a virtual device into which users can store items they want to purchase as they navigate throughout the site.

Shopping basket applications today usually store the list of basket contents in a database on the server side, rather than storing basket items in the cookie itself. A web server typically sends a cookie containing a unique session identifier. The web browser will send back that session identifier with each subsequent request and shopping basket items are stored associated with a unique session identifier.

Allowing users to log in to a website is a frequent use of cookies. Typically the web server will first send a cookie containing a unique session identifier. Users then submit their credentials and the web application authenticates the session and allows the user access to services.

Personalization

Cookies may be used to remember the information about the user who has visited a website in order to show relevant content in the future. For example a web server may send a cookie containing the username last used to log in to a web site so that it may be filled in for future visits.

Many websites use cookies for personalization based on users' preferences. Users select their preferences by entering them in a web form and submitting the form to the server. The server encodes the preferences in a cookie and sends the cookie back to the browser. This way, every time the user accesses a page, the server is also sent the cookie where the preferences are stored, and can personalize the page according to the user preferences. For example, the Wikipedia website allows authenticated users to choose the webpage skin they like best; the Google search engine allows users (even non-registered ones) to decide how many search results per page they want to see.

Tracking

Tracking cookies may be used to track internet users' web browsing habits. This can also be done in part by using the IP address of the computer requesting the page or the referrer field of the HTTP header, but cookies allow for a greater precision. This can be done for example as follows:

1. If the user requests a page of the site, but the request contains no cookie, the server presumes that this is the first page visited by the user; the server creates a random string and sends it as a cookie back to the browser together with the requested page;
2. From this point on, the cookie will be automatically sent by the browser to the server every time a new page from the site is requested; the server sends the page as usual, but also stores the URL of the requested page, the date/time of the request, and the cookie in a log file.

By looking at the log file, it is then possible to find out which pages the user has visited and in what sequence. For example, if the log contains some requests done using the cookie id=abc, it can be determined that these requests all come from the same user. The URL and date/time stored with the cookie allows for finding out which pages the user has visited, and at what time.

Third-party cookies and Web bugs, explained below, also allow for tracking across multiple sites. Tracking within a site is typically used to produce usage statistics, while tracking across sites is typically used by advertising companies to produce anonymous

user profiles (which are then used to determine what advertisements should be shown to the user).

A tracking cookie may potentially infringe upon the user's privacy but they can be easily removed. Current versions of popular web browsers include options to delete 'persistent' cookies when the application is closed.

Third-party cookies

When viewing a Web page, images or other objects contained within this page may reside on servers besides just the URL shown in your browser. While rendering the page, the browser downloads all these objects. Most modern websites that you view contain information from lots of different sources. For example, if you type www.domain.com into your browser, widgets and advertisements within this page are often served from a different domain source. While this information is being retrieved, some of these sources may set cookies in your browser. First-party cookies are cookies that are set by the same domain that is in your browser's address bar. Third-party cookies are cookies being set by one of these widgets or other inserts coming from a different domain.

Modern browsers, such as Mozilla Firefox, Internet Explorer and Opera, by default, allow third-party cookies, although users can change the settings to block them. There is no inherent security risk of third-party cookies (they do not harm the user's computer) and they make lots of functionality of the web possible, however some internet users disable them because they can be used to track a user browsing from one website to another. This tracking is most often done by on-line advertising companies to assist in targeting advertisements. For example: Suppose a user visits www.domain1.com and an advertiser sets a cookie in the user's browser, and then the user later visits www.domain2.com. If the same company advertises on both sites, the advertiser knows that this particular user who is now viewing www.domain2.com also viewed www.domain1.com in the past and may avoid repeating advertisements. The advertiser does not know anything more about the user than that—they do not know the user's name or address or any other personal information (unless they obtain it from another source such as from the user or by reading another cookie).