I-034: Internet Cookies

March 12, 1998 23:00 GMT
[REVISED 1 Feb 2007]

PROBLEM:	Cookies are short pieces of data used by web servers to help identify web users. The popular concepts and rumors about what a cookie can do has reached almost mystical proportions, frightening users and worrying their managers.
PLATFORM:	Any platform that can use a modern web browser.
DAMAGE:	No damage to files or systems. Cookies are only used to identify a web user though they may be used to track a user's browsing habits.
SOLUTION:	No files are destroyed or compromised by cookies, but if you are concerned about being identified or about having your web browsing traced through the use of a cookie, set your browser to not accept cookies or use one of the new cookie blocking packages. Note that blocking all cookies prevents some online services from working. Also, preventing your browser from accepting cookies does not make you an anonymous user, it just makes it more difficult to track your usage.
VULNERABILITY ASSESSMENT:	The vulnerability of systems to damage or snooping by using web browser cookies is essentially nonexistent. Cookies can only tell a web server if you have been there before and can pass short bits of information (such as a user number) from the web server back to itself the next time you visit. Most cookies last only until you quit your browser and then are destroyed. A second type of cookie known as a persistent cookie has an expiration date and is stored on your disk until that date. A persistent cookie can be used to track a user's browsing habits by identifying him whenever he returns to a site. Information about where you come from and what web pages you visit already exists in a web server's log files and could also be used to track users browsing habits, cookies just make it easier.

REVISION HISTORY:

02/01/2007 - revised to fix a broken link to the jscookies example.

Internet Cookies

The popular rumors about web cookies describe them as programs that can scan your hard drive and gather information about you including: passwords, credit card numbers, and a list of the software on your computer. None of this is close to the truth. A cookie is a short piece of data, not code, which is sent from a web server to a web browser when that browser visits the server's site. The cookie is stored on the user's machine, but it is not an executable program and cannot do anything to your machine.

Whenever a web browser requests a file from the web server that sent it a cookie, the browser sends a copy of that cookie back to the server along with the request. Thus a server sends you a cookie and you send it back whenever you request another file from the same server. In this way, the server knows you have visited before and can coordinate your access to different pages on its web site. For example, an Internet shopping site uses a cookie to keep track of which shopping basket belongs to you. A server cannot find out your name or e-mail address, or anything about your computer using cookies.

Normally, cookies are only sent back to the server that originally sent them to the browser and to no one else. A server can set the domain attribute for a cookie so that any server in the same Internet subdomain as the computer that sent the cookie will have the cookie sent along with a file request. This is so those larger sites that utilize multiple servers can coordinate their cookies across all the servers. The domain path can not be set to send cookies to a subdomain outside of the subdomain where the server resides.

A cookie is sent to a browser by including a line with the following syntax in the header of an HTML document. Note that the header is removed from the document before the browser displays it. Thus, you will not see the header lines if you execute the View, Source or View, Document Source commands in your browser.

```
Set-Cookie: NAME=VALUE; expires=DATE;path=PATH; domain=DOMAIN_NAME; secure
```

Here the upper case names are strings the server can set.

NAME=VALUE is the name of the cookie and its VALUE. This is the data that the web server wants passed back to it when a browser requests another page.

DATE is an attribute that determines how long the cookie persists on your system. If there is no expiration date, the cookie is stored in memory only and expires at the end of the current session (that is, when you quit the web browser). If the DATE attribute is in the future, the cookie is a persistent cookie and is saved in a file. Only persistent cookies can be used to track a user at more than one site. Setting the date for an existing cookie to be some day in the past deletes the cookie.

DOMAIN_NAME is an attribute that contains the address of the server that sent the cookie and that will receive a copy of this cookie when the browser requests a file from that server. It defaults to the server that set the cookie if it is not explicitly set in the Set-Cookie: line. DOMAIN_NAME may be set to equal the subdomain that contains the server so that multiple servers in the same subdomain will receive the cookie from the browser. This allows larger web sites to coordinate multiple servers in the same subdomain. For example, if the DOMAIN_NAME equals www.mydomain.com then machines named one.www.mydomain.com, two.www.mydomain.com, and three.www.mydomain.com would all receive the cookie from the browser. The value of DOMAIN_NAME is limited such that only hosts within the indicated subdomain may set a cookie for that subdomain and the subdomain name is required to contain at least two or three dots in it. Two dots are required if the top level domain is: .COM, .EDU, .NET, .ORG, .GOV, .MIL, or .INT. Three dots are required for any other domain. This is to prevent the subdomain from being set to something like .COM, the subdomain of all commercial machines.

PATH is an attribute that is used to further refine when a cookie is sent back to a server. When the PATH attribute is set, a cookie is only sent back to the server if both the DOMAIN_NAME and the PATH match for the requested file.

secure is an attribute that specifies that the cookie is only sent if a secure channel (https) is being used.

What Information Can A Server Get From A Browser

When a browser sends a request to a server, it includes its IP address, the type of browser you are using, and the operating system of your computer. This information is usually logged in the server's log file. A cookie sent along with the request can add only that information, which is contained in the cookie and which, was originally sent to the browser by the same server. Thus,

there is no additional personal information explicitly sent to the server by allowing cookies.

Cookies and shopping Sites

As mentioned above, cookies are used by Internet shopping sites to keep track of you and your shopping cart. When you first visit an Internet shopping site, you are sent a cookie containing the name (ID number) of a shopping cart. Each time you select an item to purchase, that item is added to the shopping cart. When you are done with your shopping, the checkout page lists all the items in the shopping cart tied to that cookie. Without cookies, you would have to keep track of all the items you want to buy and type them into the checkout page or buy each item, one at a time.

Another method is for the shopping site to send a separate cookie containing the item number to your browser whenever you select an item to purchase. Your browser sends all those cookies along with the request for the checkout page. The checkout page uses the cookies to make a list of the items you want to purchase.

Cookies and Custom Home Pages

Another use of cookies is to create customized home pages. A cookie is sent to your browser for each of the items you expect to see on your custom home page. Whenever you request your custom home page your cookies are sent along with the request to tell the server which items to display. Without cookies, a server would require you to identify yourself each time you visit the custom page so it knows what items to display. The server would also have to store the custom page settings for every visitor.

Cookies and Buying Habits

One of the less admirable uses of cookies, and the one that is causing all the controversy, is its use as a device for tracking the browsing and buying habits of individual web users. On a single web site or a group of web sites within a single subdomain, cookies can be used to see what web pages you visit and how often you visit them. This information is also in the server's log files and so the use of a cookie here does not increase a server's ability to track you, it just makes it easier.

On multiple client sites being serviced by a single marketing site, cookies can be used to track your browsing habits on all the client sites. The way this works is a marketing firm contracts with multiple client sites to display its advertising. The client sites simply put an <IMG> tag on their web pages to display the image containing the marketing firm's advertisement. The tag does not point to an image file on the client's machine but contains the URL of the marketing firm's advertisement server and includes the URL of the client's page. Thus when you open a page on the client's site the advertisement you see was actually obtained from the advertising firm's site.

The advertising firm sends a cookie along with the advertisement, and that cookie is sent back to the advertising firm the next time you view any page containing one if its advertisements. If many web sites support the same advertising firm, that firm will be able to track your browsing habits from page to page within all the client sites. They will not be able to see what you do with the pages you view; they will only know which pages you are viewing, how often you view them, and the IP address of your computer. This information can be used to infer the things you are interested in and to target advertising to you based on those inferences.

NOTE: A URL is a Uniform Resource Locator, which is a string containing the type of resource, IP address of the server machine containing the resource, and the path to the resource on the server. When you access a web page, the URL is what you type in the address field of the web browser. For example: http://ciac.llnl.gov/ciac/CIACHome.html is a URL for the CIACHome.html document, which is an http document, on the ciac.llnl.gov server in the /ciac directory.

Examining Persistent Cookies Already On Your System

Persistent cookies are stored in different places on your system depending on which web browser and browser version you are using. Netscape stores all its persistent cookies in a single file named cookies.txt on the PC or magiccookie on the Macintosh. Both files are in the Netscape directory. You can open and edit this file with a text editor and delete any cookies that you don't want to keep or delete the file itself to get rid of all of your cookies.

Internet Explorer stores persistent cookies in separate files named with the user's name and the domain name of the site that sent the cookie. For example: yourname@ciac.txt. The cookie files are stored in /Windows/cookies or in /Windows/profiles//cookies directories, where is replaced with the user's login name. If your operating system directory is not named Windows (such as Winnt for Windows NT) then look in that directory instead of the Windows directory. You can delete any of these files you do not want to keep.

You can open these files to see where they came from and what information they contain. For example, the following are the contents of an Internet Explorer cookie file.

```
Counter_Cookie
7
www.myplace.com/Java/
0
2750889984
29260821
2802449904
29177426
*
```

This particular cookie file was named orvis@java.txt. The file name is made up of the username (orvis) and the last part of the domain (java). The text "Counter_Cookie" is the name of the cookie and 7 is its value. The URL is the domain attribute and the numbers contain the date and other cookie attributes. This particular cookie implements a page counter that lists how many times you have visited a particular page. Whenever you visit that page, this cookie is sent along with the page request. The server then knows that this is the eighth (7 + 1) time you visited the page and inserts that number into the web page. It then increments the value of the cookie from 7 to 8 and sends it back to the browser along with the requested page. The new cookie replaces the old one so the next time you visit the number 8 is sent to the server. See the example in the "Cookies, VBScript, JavaScript, and Java" section below to see this page in action.

Preventing Any Cookies from being Placed On Your System

You can prevent any cookies from being sent to your system using the browser options. In Internet Explorer 4.0, choose the View, Internet Options command, click the Advanced tab and click the Disable All Cookie Use option. In Netscape 4.0, choose the Edit, Options command, click on Advanced and click the Disable Cookies option. After that, no cookies will be stored on your

system. You will need to turn cookies back on if you want to use any online services that require them. You can also choose the option to prompt you before accepting a cookie, but at many sites you will be continually closing the warning dialog box.

If you are using earlier versions of Netscape or Internet Explorer, you can require that the browser warn you before accepting a cookie, but it cannot block all cookies. At a busy shopping site, acknowledging all the warnings can get really tedious. There are some other methods for fooling your browser into not accepting a cookie discussed in the cookie web pages listed at the end of this bulletin.

Cookie Blocking Software

Several companies are offering special software packages that work with your web browser to control who can send you a cookie. In these packages, you designate which sites can send you a cookie and which can not, alleviating the need to turn cookie use on and off by hand. If you want to use cookies in some instances and not in others, one of these packages may make things easier.

Several packages are listed at the following sites:
http://www.cookiecentral.com/files.htm
http://www.junkbusters.com/ht/en/links.html#nsclean

Cookies, VBScript, JavaScript, and Java

Programs written in VBScript, JavaScript, and Java that are attached to a web page can read and store cookies on your system. The limitations on these cookies are the same as cookies sent to your browser by the server that sent you the program. Cookies created by these programs can only pass information from one page to the next.

The following site demonstrates a page counter using JavaScript.
http://willmaster.com/possibilities/demo/cookies/jscookies.html

More Cookie Information

The following web sites are just a few of the sites that specialize in cookie information.

Yahoo: http://www.yahoo.com search for "cookie".

Netscape's cookie specification:
http://www.netscape.com/newsref/std/cookie_spec.html

Netscape's cookie security FAQ
http://search.netscape.com/assist/security/faqs/cookies.html

Cookie Central: http://www.cookiecentral.com

Junkbusters: http://www.junkbusters.com

DOE-CIRC can be contacted at:
Voice: +1 866-941-2472 (7 x 24)
E-mail: doecirc@doecirc.energy.gov
World Wide Web: http://www.doecirc.energy.gov/