

Are Cookies Monsters?

by Stephen Turbek



RAZORFISH REPORTS

a publication of the razorfish science department | 23 october2000 | report 037

Internet cookies are a simple, beautiful system for letting people interact with Web sites in a more intelligent fashion. They are also mistakenly blamed for spying on people, breaching security, and giving away personal information.

What Are Cookies?

A "cookie" is a bit of text in a file on the hard drive of a desktop computer. Each cookie can be saved into the file or "set" when the browser loads a page on a Web site. The cookies are sent to the Web site whenever another file is loaded.

The browser looks on the hard drive to see if there is a cookie for the domain name (for example, amazon.com) of the site it is loading from. If there is, it sends the cookie information to the server along with the request for the page. The server then can read the cookie information and send personalized information, for example welcoming you to the site by name.

Cookies were invented in 1995 primarily by David Kristol of Bell Labs and Lou Montulli of Netscape. It was originally implemented in the Netscape Navigator browser and was quickly adopted by all the browsers. The term 'cookie' was internal slang referring to their size.



Stephen Turbek <stephen@razorfish.com> is in the razorfish science department.

Cookies Are Generally Safe

The beautiful aspect of the cookie system is that a Web site can only have access to what it knew already - it can not touch another site's cookies. Each cookie has a domain address associated with it - a cookie set by coke.com can never be accessed by pepsi.com, but the site diet.coke.com server has the same domain name and can share it.

Cookies are small text files used to store information like the user name, on the desktop computer.

They cannot travel to other computers or be put on mailing lists. They are not active programs and definitely cannot read your files or erase your hard drive.

The other important aspect of cookies is that they can only hold what you tell the Web site that saved it. If you never typed in your credit card number to a Web site, it can not save it into a cookie. That said, it is extremely unlikely that anyone would hold such private information in a cookie.

Cookies Store "State" Information

The biggest problem with creating compelling Web experiences is that sites rarely know who the visitors are. Each page load is almost a completely separate event. This can be likened to the department store frustration of walking to yet another help desk only to have to re-tell all your information. A cookie can be seen as a name tag that lets each helpdesk recognize you and look your case up on their computer.

The most common use of these is to store a user ID. This allows the Web site to recognize you again when you return, and is used to reference the personal information that is stored securely on the Web site's server.

They can also save information about your preferences, often simple things for example, your zip code to give you personalized news reports.

Shopping sites can also store a visitor's shopping cart information in a cookie, keeping a list of the products for check-out.

Your Trail of Crumbs

You can look at your cookie file and see an interesting track of your forays through the internet. Search for the word 'cookie' and open the file, or check your browser's preferences.



Not bad for you.

The site can keep track of a user's progress through their IP address (the universal address for every computer connected to the Internet), but many people log on from home through Internet service providers, such as AOL, which give them a new address every time they connect. So this address is only temporary.

A cookie stores the following fields:

Name of the cookie

Text data (what the cookie stores)

Expiration **date** of the cookie

Domain of server

Pathname of domain that cookie is restricted to

Whether a **secure** HTTP connection is required to send the cookie

A Cookie Example

This cookie was set as a demonstration on the site www.cookiecentral.com

```
www.cookiecentral.com    FALSE
973977299 VisitorName stephen
```

“www.cookiecentral.com” is the URL of the server that set the cookie. If there was another server named chip.cookiecentral.com, that other server would not be sent the cookie by the browser.

The “FALSE” note shows that the connection between the browser and the server does not have to be secure (encrypted) for the cookie to be sent. “973977299” is the expiration date of



They store information inside.

the cookie, written in an encoded form. The expiration date is the date when the cookie will be deleted. All cookies have an expiration date.

“VisitorName” is the name of the cookie, chosen by the site makers.

“stephen” is the name entered on the site.

This cookie is used to put a name on

the page when it loads, personalizing it, similar to the amazon.com home page. In the interests of security, Amazon does not store your name on the cookie, but simply a user number. The rest of your profile is securely stored on their server.

DoubleClick, an ad service ignited a firestorm of criticism by attempting to connect cookies and personal information.

Negative Aspects of Cookies

Because cookies are stored on the local desktop machine, if multiple people use the same machine, as in a library, the cookies set by the different people get mixed up.

Conversely, cookies do not follow you if you use another computer. If you surf at work and at home, you might as well be two separate people.

Cookie trails are circumstantial, forcing site managers to guess what user actions mean. This is true of all Web tracking systems.

Cookies generally happen without the user knowing about them, leaving the impression that the use is being spied upon. To notify the user each time a cookie is set would be annoying, though.

Cookies are fragile. They get reset often when changing browsers or trouble-shooting your computer.

Cookies could be used to track your buying habits, leading to more ads by the sites you visit. DoubleClick, an Internet ad firm, uses cookies to track

users across Web sites. They created a furor by attempting to buy a direct mail company with a list of names and addresses. This could have violated the anonymity of cookies by linking your buying habits with your physical person. The Internet audience’s outrage caused them to back down.

You Do Have Control

You can turn off cookie storage in your browser’s preferences control. This prevents cookies from being stored on your computer, but can limit your interaction with the some sites. Using third party programs, such as “CookieCutter”, you can edit your cookies.

To sum up, cookies are a more convenient way of creating compelling interactivity, but may have the now-familiar side effect of allowing us to be tracked anonymously. Because cookies can only be seen by the Web site that created them, they are not a big risk of becoming monsters.

for more information

Netscape’s Description

http://home.netscape.com/newsref/std/cookie_spec.html

Cookie Discussion

http://developer.netscape.com:80/viewsource/archive/goodman_cookies.html

How Cookies Work

<http://www.howstuffworks.com/cookie7.htm>

razorfish reports are published regularly by the razorfish science department for our colleagues and the interested public.