
Print

Overcoming cookie phobia
By: Alan K'necht
ComputerWorld Canada (01 Apr 2005)

Most people love cookies, whether they're chocolate chip, shortbread or gingerbread. Yet when a little technology, which emerged in the early days of the Internet, appropriated this delectable term, laypeople, privacy advocates and even some tech gurus put fear into the hearts of computer users everywhere.

These tiny snippets of code didn't add calories or trans fats to our diet, but depending on whom you asked, cookies clogged up computers with useless garbage and made it possible to track everything an individual did on the Internet. Cookies became the beachhead of Big Brother.

Since then, times have changed. Virtually every major Web application server has some feature that can be enhanced by using cookies. These bits of code can manage user sessions, remember user IDs and passwords and track visitor habits on a Web site. Despite the growing benefits of cookies and the fact that most users have lost their cookie-phobia, many companies and government offices around the world continue to maintain policies that forbid the use of cookies on their Web sites.

As a consultant, on many occasions I have recommended my clients use cookies to help improve user tracking as part of making Web analytics more accurate, especially with tools from Web analytics solution providers like San Jose, Calif.-based WebTrends. Yet, when confronted with all the advantages of introducing cookies to their sites, most people simply throw up their hands and say they have an immovable corporate policy that says "no cookies."

When you dig into these policies you find they were set five to eight years ago when cookie fear was rampant and Netscape 4 was king. Well, it's time to review these policies and to present the straight goods on how cookies can benefit organizations to those who have the authority to change the policy.

Here are some facts about cookies: These small bits of plain text are sent to the Web site visitor's computer from the Web server or site they are visiting. Cookies may have a short session life, where no physical code is written to the visitor's hard drive, or a longer life through the use of persistent cookies, whereby some plain text code is written to the visitor's hard drive.

These bits of code must meet the following criteria:

• Maximum number of characters: 256

• Maximum size: 4KB

• No more than 20 cookies from one server (oldest ones are replaced)

• Total number of cookies stored on a single computer cannot exceed 300 (oldest ones are replaced)

• Cookie can only be read by the server that issued it

After a brief reality check, one will realize there is nothing sinister about cookies. Remind those responsible for creating policies around cookie usage that what really matters is the type of information stored in those 256 characters.

For example, it is undesirable to store credit card details in a cookie, but it is OK to save a randomly-generated unique identifier that merely allows a Web analytics program to track user activity, help pinpoint problem areas in a Web site or identify which advertising campaigns are generating online sales.

Cookies demonstrate real power when they are the persistent kind. When the cookie is properly configured and used in conjunction with a Web analytics program that recognizes persistent cookies, one can track users across servers — an absolute necessity in load-balanced environments and when the content and commerce portions of a Web site reside on different servers.

This type of path analysis is vital in the Web site maintenance life cycle: Build, analyze and improve. One way to get cookie policies changed is to point out that by using cookies, Web analytics can better identify which online and offline advertising campaigns are generating online sales. Companies can save significant dollars — and increase

revenue — by quickly removing unsuccessful campaigns and placing those dollars into the profitable campaigns. This kind of change could mean huge increases in ROI for the same marketing spend.

Another point of resistance is the technology for generating cookies. Traditionally cookies were created through a small Java script on each Web page. There is always a potential this Java script will conflict with existing Web pages and other Java scripts. Some companies worry that these few extra lines of code will slow down page load speed by increasing the file size, which could potentially increase hosting costs. To avoid this point of conflict, the Web server could manage the cookies. For Microsoft IIS servers, one could write an ISAPI filter and for Apache, a module could be added.

Both solutions work the same way: The server sets the cookie and tests for existing cookies, which means there is no extra code on the Web page. That eliminates potential conflict with other code and ensures the page size is smaller, which speeds up the whole page-load process. If you've managed to persuade your policy makers to allow cookies, remember to update your privacy policy.

Don't be afraid to give users the name of your cookie reporting in the Web site's access logs. Without this last step, you won't be able to record the benefits of cookie usage or use these digital helpers for Web analytics purposes.

056535