Cookies and Privacy

Phillip J. Windley, Ph.D.
Chief Information Officer
State of Utah

Cookies (the Internet variety, anyway) have generated a lot of concern among people, particularly in the area of personal privacy. A recent example was the GSA announcement that many US Government web sites used cookies contrary to policy. The news media, of course, jumped on this even though there was nothing in the story to indicate why the policy existed or whether the presence of cookies posed a threat to anyone. Even though most people know that cookies are used on the Internet, most do not understand what a cookie is or in what form it might present a threat to their privacy.

Cookies

The Hacker's Dictionary defines a cookie as a handle, transaction ID, or other token of agreement between cooperating programs. The claim check you get from a dry-cleaning shop is a perfect mundane example of a cookie; the only thing it's useful for is to relate a later transaction to this one (so you get the same clothes back).

On the Internet, cookies are exchanged between the browsers people use to access the WWW (such as Internet Explorer and Netscape) and the servers that they visit. These cookies serve the same purpose as the claim check in the example—they tie seemingly unrelated transactions together.

To see how this works, suppose that I use my browser to visit a web site I've never been to before, let's call it www.foo.com. The people who maintain www.foo.com have set it up to give a cookie to everyone who visits. So, on my first visit to the site, the server passes a cookie back to my browser. My browser, since I have allowed cookies, dutifully stores the cookie in a file on my computer used especially for this purpose. The magic of cookies happens the next time I request a page from www.foo.com (which could happen in the same browsing session or days or weeks later). When I tell my browser to retrieve a page from www.foo.com, my browser sends back the cookie it received on the last visit.

So, let's review what has happened:

- The server asked my browser to store some information for it, knowing that it would be sent back verbatim when the browser makes its next request.
- The server chose the information it gave to my browser.

- My browser didn't add any information to the cookie, just passed it back.
- My browser stored the cookie in a special file that it chose, not one the server chose.
- The cookie does not contain any information about me.
- The cookie is not a program—it can't be executed and has no ability to access other information on my computer.
- The next time I retrieved a page from that web site, the information was sent back.

That's really the long and short of cookies. There are some more details, but all cookies obey these rules.

Cookies were added to servers and browsers to allow transactions separated in time to be linked together by the server. This ability is what allows a web site to run a shopping cart, remember who you are, fill in forms for you, or remember your password in between visits. Just as you wouldn't return to a dry cleaner who couldn't match up their customers with their clothes, web sites without the ability to link transactions across time are pretty boring.

Cookies and Privacy

So, after reading that explanation, you may be asking yourself why there is so much concern over cookies and privacy. As with most things, its not cookies themselves that cause concern, but how they are used. Here are a few examples:

- We've already discussed that a server picks the cookies, so how does your personal information come to be linked to the cookie and identify you? The server gives you a unique ID inside the cookie, but it doesn't know anything about you until *you* reveal that information. You might reveal that information by buying something from the site, filling out a form, or otherwise volunteering that information. Once you've volunteered the information, it can be linked to the unique ID in your cookie and then each time you visit the site, you'll tell them who you are by sending back the cookie.

- You may not be too concerned about a single web site who you trust knowing who you are, but can other web sites get access to that information? Technically no. I can only access cookies that come from my web site. Not even two web sites on a shared server can get access to one another's cookies. Even so, that's not the end of the story. Web sites can and do cooperate with each other so that they can gain more information about their visitors. Here's how it works: You visit web site A. On the page you visit is a small, invisible graphic from web company C. A has a contract with C to share information. You get a cookie from both A *and* from C on that visit. Later you visit web site B. You've never been there, but they also have a contract with C. When you visit B's web site you download another small, invisible graphic from C and send C's cookie back when you do. Now C can tell B all about you using information from A since it used its web site to bridge A and B's web sites together and they all agree to share information.

Protecting Privacy

Its much more important when examining a web site to know what they will do with your personal information than it is to know whether they use cookies or some other technology. In other words, focus on the behavior, not the implementation. Banning cookies doesn't make a web site more private, it just limits the implementation choices. What does make a web site more private is a well thought out policy and people who follow that policy.

Take the two examples above. The behavior in the first, remembering your personal information each time you visit, might seem like a terrible imposition to some and a convenience to others. I personally like when a web site I visit all the time fills out forms for me and makes my visits easier. I'm willing to give up some of my privacy to gain that convenience. The second example is not something I'm very excited about and I'd avoid web sites that I knew did this. Banning cookies might seem like a simple solution, but it also removes the convenience and my choice as a consumer.

If I'm concerned about my privacy there are a few things I can do:

1. Read privacy policies of any web site I give my personal information. These may seem dull and boring, but if you care, this is the easiest way to tell what a web site is doing with your information.
2. Don't give personal information to web sites without privacy statements.
3. Set my browser to warn me whenever someone wants to set a cookie. This may be too much work for most, but it is informative to do, even for a little while, to get some idea how often cookies are sent and what they look like.
4. Download and use a copy of a cookie program that allows you to see, manage, and delete your cookies.

Utah.gov

On the utah.gov web site we use cookies to provide some of the transactions that offer services to citizens. We will continue to do so. In the interest of privacy, we not only have a privacy policy, but a Chief Privacy Officer who will look after our behaviors, rather than our means of implementation, to ensure utah.gov is a trusted web site. The questions we will be asking are "what should be in our privacy policy?" and "does this application follow our policy?" The current utah.gov privacy policy can be accessed by clicking on the link at the bottom of the www.utah.gov page.