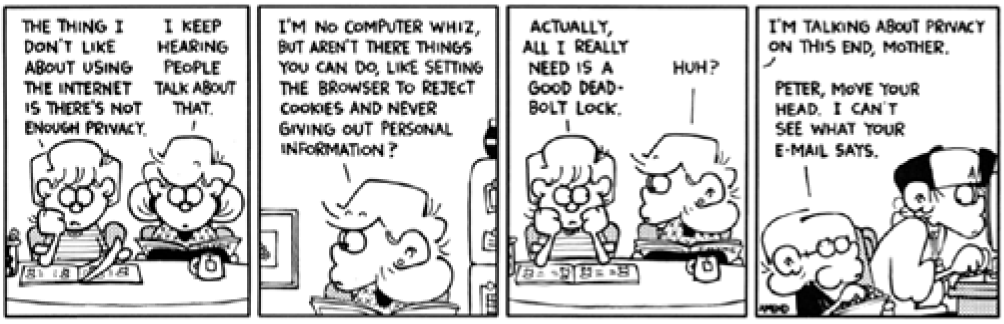
8.2 Some Problems with Cookies

Providing convenience to the user and added value to the site owner is the purpose behind cookies. And despite much misinformation, cookies are not a serious security threat. Cookies are *never* interpreted or executed in any way and thus cannot be used to insert viruses or attack your system. Furthermore, since browsers generally only accept 20 cookies per site and 300 cookies total, and since browsers can limit each cookie to 4 kilobytes, cookies cannot be used to fill up someone's disk or launch other denial-of-service attacks.

However, even though cookies don't present a serious *security* threat, they can present a significant threat to *privacy*.

FOXTROT © 1998 Bill Amend. Reprinted with permission of UNIVERSAL PRESS SYNDICATE. All rights reserved.


THE THING I DON'T LIKE ABOUT USING THE INTERNET IS THERE'S NOT ENOUGH PRIVACY.
I KEEP HEARING PEOPLE TALK ABOUT THAT.
I'M NO COMPUTER WHIZ, BUT AREN'T THERE THINGS YOU CAN DO, LIKE SETTING THE BROWSER TO REJECT COOKIES AND NEVER GIVING OUT PERSONAL INFORMATION?
ACTUALLY, ALL I REALLY NEED IS A GOOD DEAD-BOLT LOCK.
HUH?
I'M TALKING ABOUT PRIVACY ON THIS END, MOTHER.
PETER, MOVE YOUR HEAD. I CAN'T SEE WHAT YOUR E-MAIL SAYS.
AMEND

First, some people don't like the fact that search engines can remember what they previously searched for. For example, they might search for job openings or sensitive health data and don't want some banner ad tipping off their coworkers or boss next time they do a search. Besides, a search engine need not use a banner ad: a poorly designed one could display a textarea listing your most recent queries ("Jobs anywhere except at this stupid company!"; "Will my SARS infection kill my coworkers?"; etc.). A coworker could see this information if they visited the search engine for your computer or if they looked over your shoulder when you visited it.

Even worse, two sites can share data on a user by each loading small images off the same third-party site, where that third party uses cookies and shares the data with both original sites. For example, suppose that both `some-search-site.com` and `some-random-site.com` wanted to display directed ads from `some-ad-site.com` based on what the user searched for at `some-search-site.com`. If the user searched for "Java Servlets," the search engine at `some-search-site.com` could return a page with the following image link:

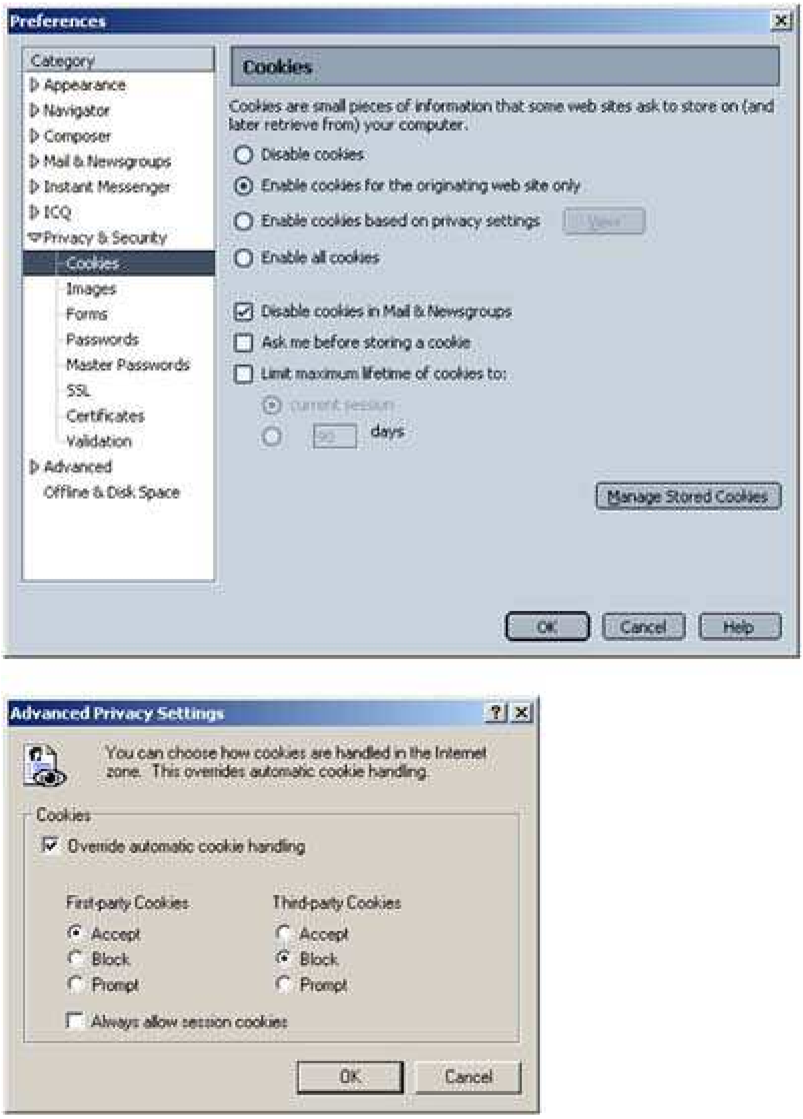
```
<IMG SRC="http://some-ad-site.com/banner?data=Java+Servlets" ...>
```

Since the browser will make an HTTP connection to `some-ad-site.com`, `some-ad-site.com` can return a persistent cookie to the browser. Next, `some-random-site.com` could return an image link like this:

```
<IMG SRC="http://some-ad-site.com/banner" ...>
```

Since the browser will reconnect to `some-ad-site.com`—a site from which it got cookies earlier—it will return the cookie it previously received. Assuming that `some-ad-site.com` sent a unique cookie value and, in its database, associated that cookie value with the "Java Servlets" search, `some-ad-site` can return a directed banner ad even though it is the user's first visit to `some-random-site`. The `doubleclick.net` service was the most famous early example of this technique. (Recent versions of Netscape and Internet Explorer, however, have a nice feature that lets you refuse cookies from sites other than that to which you connected, but without disabling cookies altogether. See Figure 8-1.)

Figure 8-1. Cookie customization settings for Netscape (top) and Internet Explorer (bottom).



Cookies

Cookies are small pieces of information that some web sites ask to store on (and later retrieve from) your computer.

○ Disable cookies
● Enable cookies for the originating web site only
○ Enable cookies based on privacy settings
○ Enable all cookies

☑ Disable cookies in Mail & Newsgroups
□ Ask me before storing a cookie
□ Limit maximum lifetime of cookies to:
● current session
○ 90 days

You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

Cookies

☑ Override automatic cookie handling

First-party Cookies	Third-party Cookies
● Accept	○ Accept
○ Block	● Block
○ Prompt	○ Prompt

□ Always allow session cookies

This trick of associating cookies with images can even be exploited through email if you use an HTML-enabled email reader that "supports" cookies and is associated with a browser. Thus, people could send you email that loads images, attach cookies to those images, and then identify you (email address and all) if you subsequently visit their Web site. Boo.

A second privacy problem occurs when sites rely on cookies for overly sensitive data. For example, some of the big online bookstores use cookies to remember your registration information and let you order without reentering much of your personal information. This is not a particular problem since they don't actually display your complete credit card number and only let you send books to an address that was specified when you *did* enter the credit card in full or use the username and password. As a result, someone using your computer (or stealing your cookie file) could do no more harm than sending a big book order to your address, where the order could be refused. However, other companies might not be so careful, and an attacker who gained access to someone's computer or cookie file could get online access to valuable personal information. Even worse, incompetent sites might embed credit card or other sensitive information directly in the cookies themselves, rather than using innocuous identifiers that are linked to real users only on the server. This embedding is dangerous, since most users don't view leaving their computer unattended in their office as being tantamount to leaving their credit card sitting on their desk.

The point of this discussion is twofold:

1. Due to real and perceived privacy problems, some users turn off cookies. So, even when you use cookies to give added value to a site, whenever possible your site shouldn't *depend* on them. Dependence on cookies is difficult to avoid in some situations, but if you can provide reasonable functionality for users without cookies enabled, so much the better.

2. As the author of servlets or JSP pages that use cookies, you should be careful not to use cookies for particularly sensitive information, since this would open users up to risks if somebody accessed the user's computer or cookie files.

[Team LiB]

◄ PREVIOUS NEXT ►