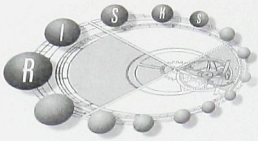

Web Cookies: Not Just a Privacy Risk

Most people have heard about the risks of Web cookies in the context of user privacy. Advertisers such as DoubleClick use cookies to track users and deliver targeted advertising, drawing significant media attention (see Hal Berghel's "Caustic Cookies, *Communications*, May 2001). But cookies are also used to authenticate users to personalized services, which is at least as risky as using cookies to track users.

A cookie is a key/value pair sent to a browser by a Web server to capture the current state of a Web session. The browser automatically includes the cookie in subsequent requests. Servers can specify an expiration date for a cookie, but the browser is not guaranteed to discard the cookie. Because there are few restrictions on their contents, cookies are highly flexible and easily misused.

An advertiser can track a user's movements between Web sites because the first banner advertisement presented can set a cookie containing a unique identifier. As subsequent advertisements are read, the advertiser can construct a profile about a user based on the cookies it receives from the user. Cookies can also authenticate users for multistep Web transactions. For example, WSJ.com sets a cookie to identify users when they log in. This allows users to download content from WSJ.com without having to reenter a password. E-commerce sites like Amazon.com use cookies to associate you with a shopping cart. In all cases, a valid cookie will grant access to data about you, but the information protected by an authentication cookie is especially sensitive. Unlike tracking cookies, authentication cookies must be protected from both exposure and forgery.

Unfortunately, cookies were not designed with these protections in mind. For example, there is no standard mechanism to establish the integrity of a cookie returned by a browser, so a server must provide its own method. As might be expected, some servers use much better methods than others. The cookie specification also relies heavily on the cooperation of the user and the browser for correct operation. Despite the lack of security in the design of cookies, their flexibility makes them highly attractive for authentication. This is especially true in comparison to mechanisms such as HTTP Basic Authentication or SSL that have fixed requirements, are not extensible, and are confusing to users. Thus, cookie-based authentication is very popular and often insecure, allowing anything from extension of privileges to the impersonation of users.

Most sites do not use cryptography to prevent forgery of cookie-based authenticators. The unsafe practice of storing usernames or ID numbers in cookies illustrates this. In such a scheme, anyone can impersonate a user by substituting the victim's username or ID number in the cookie. Even schemes that do use cryptography often crumble under weak cryptanalytic attacks. Designing a secure cookie-based authentication mechanism is difficult because the cookie interface is not amenable to strong challenge-response protocols. Thus, many designers without clear security requirements invent weak, home-brewed authentication schemes (K. Fu et al., "Dos and Don'ts of Client Authentication on the Web," *Proc. of 10th USENIX Security Symposium*, Aug. 2001).

Many sites also rely on cookie expiration to automatically terminate a login session. However, cookies can be modified by users to extend expiration times. Furthermore, most HTTP exchanges do not use SSL to protect against eavesdropping; anyone on the network between the two computers can overhear the traffic. Unless a server takes stronger precautions, an eavesdropper can steal and reuse a cookie, impersonating a user indefinitely.

These examples illustrate just a few of the common problems with cookie-based authentication. Web site designers must bear these risks in mind, especially when implementing privacy policies and designing Web sites. Although there is currently no consensus on the best design practices for a cookie authentication scheme, we offer some guidance in "Dos and Don'ts of Client Authentication on the Web." To protect against the exposure of your own personal data, the best (albeit extreme) defense is to avoid shopping online or registering with online services. Disabling cookies makes any use of cookies a conscious decision (cookies must be reenabled) and prevents any implicit data collection. Unfortunately, today's cookie technology offers no palatable solution for users to securely access personalized Web sites. C

Emil Sit and **Kevin Fu** ({sit, fubob}@mit.edu) are graduate students at the MIT Laboratory for Computer Science in Cambridge, MA.

MARTIN MAYO