Global Information Assurance Certification Paper

Cookies vs. Internet Privacy

Lee Walswick
17 December 2000

Introduction

What is a cookie? What does a cookie do? What information, if any, do web sites through the use of cookies transmit? Does this constitute an invasion of privacy? These are questions that we have asked others and ourselves time and again. The purpose of this paper is to enlighten, inform and possibly dispel some of the myths surrounding cookies.

The main issue for any System Administrator, Network Administrator, or even your average home PC user, is awareness. Being aware of what is taking place on your system or network, whether at work or at home is essential to safe and productive computing.

Cookies are integral part of the Internet; there is no escaping them. In the following pages I will define what a cookie is, what it does, some of its uses and of course, some of the issues surrounding the legal, or possibly illegal use of cookies.

Definitions

A cookie by definition is a small text file sent by a web server to a web client (browser) and stored there either temporarily or for a fixed period of time to be read later by the server.

There are two types of cookies – Persistent Client State and Session. Persistent Client State cookies are stored on a users hard drive for a fixed period of time as specified by the cookie. Session cookies expire when the current session using the cookie ends.

Cookie Parameters and Restrictions

Cookies transport from server to client and back again as an HTTP header. This header has six parameters, two of which are mandatory. They are as follows:

1. The name of the cookie.
2. The value of the cookie.
3. The expiration date of the cookie.
4. The domain the cookie is valid for.
5. The path the cookie is valid for.
6. The need for a secure connection.

The name and value of the cookie are mandatory fields. The expiration date, domain, path and need for a secure connection are optional. If the expiration date is set, the date string defines the valid life of the cookie. If it is not set, then the cookie expires when the users' session ends. The default domain is the host name of the server that generated the cookie. If the path is not specified, it is the same path as the document being described

by the header. If the cookie is marked secure, it will only be transmitted if the communications channel with the host is a secure one.

As with anything else, cookies do have some restrictions. You cannot set a cookie in any domain other than the one the document that originated the cookie resides in. Will the acceptance of cookies eventually fill up your hard drive, not likely? First of all, the HTTP header for a cookie must be no more than 4Kb in size. Second, domains can only set a maximum of 20 cookies on specific clients. Third, Netscape for example, only allows enough space for a maximum of 300 cookies from all sources.

General Information and Uses of cookies

Cookies cannot get sensitive information off your hard drive, such as, personal information, e-mail addresses, etc. You provide more information to a web site when you log into it than a cookie can provide. For example, when you log in you give away your service provider, operating system, browser type, screen resolution and amount of colors (Internet Explorer only), CPU type, your IP address (although this changes all the time) and what server you were on last.

They cannot pass a virus to your hard drive because they are nothing more than a simple text file that contains no executables or macros. Cookies can be encrypted and multiple cookies can be contained in one file and can only be accessed by the site that created them.

Websites use cookies to track users on that site to determine which banners they are looking and where they are going. This data is used for targeting users for different types of marketing schemes and ensuring users are not clobbered with advertising that they have no interest in.

Other uses would be storing user id's and passwords at sites that require them. Storing preferences for personal web pages from sites such as, Yahoo, Excite, e-bay, etc. Online ordering systems use cookies to keep track of purchases and account information.

Internet Privacy Issues

One of the biggest problems with cookies is the transmittal of information back to a particular web site and the storing of a cookie on a user's hard drive without the user's consent or knowledge. Does this constitute an invasion of privacy? Some think it does and others feel that the gathering of this information is harmless. Either way, do companies have the right to gather information from users without their consent?

The following is an excerpt from Peacefire.org's article on Internet Explorer "Open Cookie Jar":

> Jamie McCarthy came up with a list of cookies set by various sites that could be used to retrieve sensitive information:

- By intercepting a cookie set by HotMail, Yahoo Mail or any other free Web-based email sites that use cookies for authentication, the operator of a hostile Web site could break into a visitor's HotMail account and read the contents of their Inbox. (HotMail cookies do not contain user passwords, but they do allow a third party to access a user's HotMail account for as long as that user stays logged in, since each separate login generates a new cookie.)
- A user's Amazon.com cookie could be used to visit Amazon.com impersonating that user, and access their real name, email address, and the user's list of "recommended titles" -- which can be used to determine what types of books or CD's the user has purchased from Amazon in the past. (You cannot, however, access the user's credit card number or their actual list of previous Amazon.com orders, since accessing this information requires a password that is not contained in the cookie.)
- A user's MP3.com cookie stores their email address.
- A user's NYTimes.com cookie stores their NYTimes.com password. This isn't useful by itself, since the password is only needed to browse articles on NYTimes.com, but exposing this password is still dangerous since users might have the same password set up for several different sites.
- A user's Hollywood.com cookie stores their city, state, and zip code.
- A user's Playboy.com cookie stores the fact that the user has visited Playboy.com -- which not every Playboy visitor would want the whole world to know. (Yeah, we know, you just wanted to read the Jesse Ventura interview.)
- A user's Zip2.com cookie can be used to access the user's home address.

I believe the main issue here is awareness. The user needs to be more aware and informed on who is collecting what information and for what purpose. The two main browsers (Netscape and Internet Explorer) allow some control for cookies. They will let you accept all cookies, accept only those cookies that get sent back to the originating server, disable cookies and warn you before accepting cookies.

I prefer to be warned before accepting any cookies. This is a little inconvenient at times but it does give me a sense of control. However, my browser may alert me to the use of a cookie, but the formatting of the information may tell me nothing of what is being stored. The main thing is, is that I can see who is sending me a cookie and I have the option of accepting or declining its' use.

In declining the use of a cookie you create a Catch 22 situation as seen in the quote from CookieCentral.com: "Essentially, without a cookie to tell the server who you are, it can't remember not to send you any cookies"!

Summary

We have looked at what a cookie is what information it contains what it is used for and some of the issues concerning the use of cookies. Does this make us experts in the use of cookies, hardly; however, it does make us a little more aware.

I am concerned about the information and type of information that is collected through the use of cookies. Where do we draw the line, will we become targets for businesses, special interest groups or our own government based upon the sites we visit on the Internet? I hope not, in the meantime, you as a user or Administrator can exercised some control by simply looking at the cookies being sent to you and not accepting any cookies

from sites that you are not familiar with. Nobody has a right to any sensitive information on your hard drive, but you!

Sources

- Cookie Central, "Persistent Cookie FAQ". URL: http://www.cookiecentral.com/faq.htm
- Netscape, "Persistent Client State HTTP Cookies". URL: http://home.netscape.com/newsref/std/cookie_spec.html
- Cookie Central, "Cookies". URL: http://www.cookiecentral.com/cm002.htm
- Cookie Central, "Cookie Values". URL: http://www.cookiecentral.com/mim03.htm
- Privacy.net, "Bake Your Own Internet Cookie". URL: http://privacy.net/cookies
- Cookie Central, "Cookies and Internet Privacy". URL: http://www.cookiecentral.com/ccstory/cc3.htm
- Junkbusters, "How Web Servers' Cookies Threaten Your Privacy". URL: http://www.junkbusters.com/ht/en/cookies.html
- Haselton, Bennett & McCarthy, Jamie, 5/11/2000, "Internet Explorer Open Cookie Jar". URL: http://peacefire.org/security/iecookies

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS