GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Cookies – Exploitations and Invasion of Privacy

GSEC Practical Assignment
Version 1.2c
Randall S. Miller
April 19, 2001

Summary

Cookies are data snippets used by client/server applications to help identify and track web users. Over the years, cookies have garnered a bad reputation as being able to scan PC hard drives, take over systems by stealing valuable information such as passwords, and passing viruses. These myths are untrue, but cookies have been used to collect information on browsing habits, browser specifications, system information, and web-based spending and viewing habits.

I will be presenting information on the mechanics of cookies, the misuse of cookies and how cookie technology can be exploited, and some of the legal issues surrounding the use of cookies for data profiling as it relates to invasion of privacy issues.

Introduction

As listed in the article Persistent Client State HTTP cookies by Netscape, "Cookies are a general mechanism which server-side connections (such as CGI scripts) can use to both store and retrieve information on the client side of the connection. The addition of a simple persistent, client-side state significantly extends the capabilities of web-based client/server applications".[1] Cookies are small pieces of data, which are limited in size to 4kb. The http cookie protocol (HTTP State Management Mechanism) specification is described in RFC 2109.[2] Including a set-cookie header in the HTTP response creates a cookie. The set-cookie response header has a distinct format, which includes the following parameters:

Set-Cookie: Name = name of the cookie;
Value = value stored in the cookie;
Expires = defines the life time of the cookie;
Path = specifies the subset of URLs to which the cookie applies
Domain = specifies the domain for which the cookie is valid
Secure = directs the user-agent to only use secure means to communicate

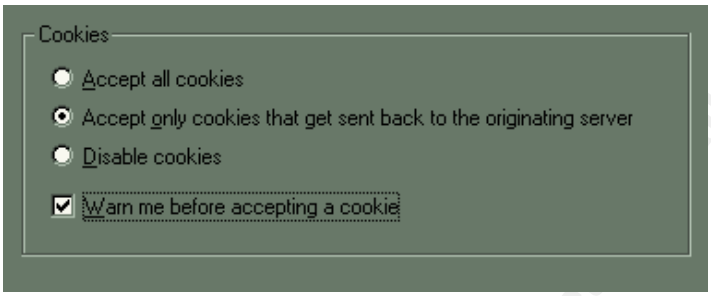
The name = value pair attribute is the only required parameter needed to set a cookie. Setting a cookie with just a name and no value will delete the cookie. Multiple set-cookie headers can be issued in a single server response.[3] Most browsers have limits on the number and size of cookies that they can store. These are at least 300 cookies with a size restriction of 4096 bytes, with no more than 20 cookies per server or domain.

Cookie Exploits

A paper on cookie exploits written by Jasmir Beciragic[4] touched upon two of the cookie exploits, JavaScript embedded in cookies and the Open Cookie Jar. I will investigate some of the other exploits/bugs that have been discovered in the use of cookies.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

An exploit (flaw) has been discovered in several versions of Netscape Communicator (4.6 for x86 Linux, 4.51 and 4.61 for Windows). It has been found that these versions do not enforce the "originating server" restrictions set forth in the cookie specifications. In the Communicator preference settings (edit -> Preferences -> Advanced), there is a section where you can set cookie preferences:



The setting to "Accept only cookies that get sent back to the originating server" is ignored in this exploit if JavaScript is enabled on the browser and the page being accessed has a section of code like:

<script language="JavaScript1.1" src="http://evil-people.com/…">

The browser interprets this code snippet as a page and therefore it believes it is originating on the accessed server, and sets the cookie from evil-people.com, which can now be used to collect information on the unsuspecting user. The browser exploit to sneak cookies past the originating server restrictions can also be achieved by linking a style sheet from a different domain that contains embedded cookies. For this exploit to work, both JavaScript and style sheets must be enabled.[5] There is a method available to counter this exploit. In the cookie preference section as described above, check the box that states "Warn me before accepting a cookie". Every cookie being set will appear for you either to allow or disallow.

Another cookie exploit that has been discovered, that all browsers are vulnerable to, allows the domain restrictions enforced on the sharing of cookies to be overridden. This is a bug in the current implementation of the cookie specification by the browser manufacturers. This exploit allows malicious sites to set cookies containing personal or sensitive information that could then be retrieved by any site. This exploit is accomplished by placing three "." Characters appended to the domain name in the set-cookie header response DOMAIN attribute and setting the "PATH" attribute (it seems that setting the path is a must for the exploit to work). This confuses the browser as to the actual domain name, and as it does not know which domain to restrict the cookies to, it allows the cookie to be accessed from any domain. This problem only affects URLs accessed by their domain name and not by their IP address. In Internet Explorer, the malformed cookie cannot be stored in the cookies directory (persistent cookie), but can be stored in memory as a session cookie.[6]

A third cookie exploit, the "Cookie Monster" vulnerability, allows cookies that are set by domains other than American registered, i.e., .au, .ru, etc.., to be returned to servers on other domains. As an example, a cookie set by the site mysite.co.ru could be returned to all servers below that domain. Most standard browsers are affected by this exploit and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Netscape's setting in the cookie preference section to "Accept only cookies that get sent back to the originating server" does not stop this vulnerability. There are many implications to this exploit. Personal information could be picked up and used by other servers. A cookie set to a second level domain (outside of a US domain) can be returned to all servers in that classification. As an example of this problem, which deals with wasted bandwidth, the article, Cookie Monster Vulnerability, lists "a web user might acquire a cookie set to the domain co.nz, and that cookie will be transmitted on each and every HTTP request that user makes when viewing commercial web sites in New Zealand".[7] The major implication with this exploit is its ability to be used maliciously to take over the cookies used by one site or to stop those cookies from functioning properly. A malicious site could name its second level domain cookies the same as another site that uses cookies to set a users viewing preferences, and when the user visits the malicious site and then returns to the other site, the cookies set could display offensive or unpleasant material. This exploit could be used in a competitive e-commerce market, to block a competitor site by interfering with their cookie-based shopping carts, effectively causing them to malfunction. If a consumer had visited site A and then tried to purchase an item from site B, a competitor, the cookies set by site A could override the site B cookies, blocking the transaction.[7]

Privacy Issues

As previously stated, cookies are pieces of information generated by a web server and stored either in memory (session cookie) or on the user's computer (persistent cookie) ready to be retrieved by the web site that set the cookie. Cookies were implemented to allow the customization of information for a particular user, such as remembering your name, information you submitted previously on forms, and the contents of shopping carts. The storage and retrieval of this information usually goes unnoticed by the user unless they knew how to set their cookie preferences on the browser to warn them of cookie activity.

Cookie usage is a two-step process. The cookie is first stored on the user's computer, usually without their knowledge. As an example, customizable web pages such as "My Netscape" use cookies to store preferences set by the user. In the second step of the process, the cookie is transmitted from the user's machine to the web server. Whenever a web page using cookies is displayed, the browser will transmit the cookie information back to the server where the information can be collected or used to display the page in a certain fashion. It is the notion of websites collecting the cookie information that most people feel is an invasion of privacy.[8] There is much information that can be gathered about you by you just by accessing a site. Your browser can reveal information about you: the computer you are coming from, what software and hardware you are using, detail of the referring page, and possibly even your email address. These values are collected from information contained within the HTTP request, such as the HTTP referrer, which lists the site you came from. The Remote Address and the Remote Host will list your IP address and possibly your fully qualified domain name e.g., jdoe.mycomany.com which could tell someone where you lived or worked. The User Agent value will list your browser and the system it is running on. Some times other

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

variables are also set which could give away other indications of your identity like the "HTTP from" and the "REMOTE_USER"[9].

A lot of hype and concern over the use of collected cookie information has arisen lately. In 1997, a weekly newspaper in Tennessee, the *Putnam Pit*, sued a local municipality in an attempt to obtain the cookie files stored on the employee computers. This was the first case to test whether cookies set on employee computers were considered public under a states public record law. The local municipality stated in their defense of not producing the information that "a cookie is about the equivalent of scratching notes on a yellow pad" and it did not believe the files to be public documents. The plaintiff in the case stated that the cookie files could provide detailed information on the employees browsing habits, such as which sites were being visited and when, and could show whether taxpayers are footing the bill for employees accessing non-work related sites.[10]

In 1998, the Energy Department's Computer Incident Advisory Capability (CIAC) issued an information bulletin (I-034) on cookie technology and it's uses on the web. They deemed that the use of cookies generally to be safe, but noted there was some concern that persistent cookies could be used to track peoples' browsing habits and that there was paranoia present in peoples' view of cookies and their use in profiling users. One note that I found interesting in this bulletin was the lack of information on cookie exploits. The CIAC bulletin I-034 states "a cookie is a short piece of data, not code, which is sent from a web server to a web server …".[11] This has proven to be untrue, as it has been shown that JavaScript can be embedded in cookies. The bulletin basically stated that the hype about cookies has far outweighed the actual hazards of the technology.

The above view by the government is not shared by other organizations, such as the Electronic privacy Information Center (EPIC). EPIC filed a complaint with the Federal Trade Commission on February 10, 2000, concerning collection of web-based preferences, collected using cookies, by the company DoubleClick, Inc. and it's business partners. The complaint addresses user profiling, i.e., the tracking of online activities of Internet users and combining these records with detailed personal profiles contained in other marketing databases. DoubleClick recently merged with the largest catalog database firm and announced it's intent to merge the data from both companies into a single repository. DoubleClick embeds their cookies on other sites (advertising revenue for the site), and if the cookie preferences are not set to only allow cookies from the calling site or with the right browser, a cookie exploit is used, DoubleClicks' cookies are set and they can collect information on your browsing habits.[12] As an example, look in the cookies.txt file in the Communicator/user directory (if you are using Netscape Navigator), and you will most likely see an entry from doubleclick.net, even though you have probably never visited that site.

Recently, the privacy advocates, such as EPIC, lost the first round of a major battle to curtail the invasion of privacy by companies such as DoubleClick. This class action suit alleged that DoubleClick's online practices, through the use of cookies, violated three federal laws; the Electronic Communications Privacy Act, the Wiretap Act, and the Computer Fraud and Abuse Act. The plaintiffs are currently appealing the decision to the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

US Court of Appeals, though they state “even if the decision is upheld in appeal, other lawsuits are pending in state courts”. The court case showed that along with the use of cookies, DoubleClick and other data collection companies, violated users privacy by capturing information from three sources. The first is by the “GET” method, which could reveal what page a user was requesting. The second is information collected during a “POST” transaction, where information could be gleaned from input forms as users sign up for new services. The last method is by placing a “web bug” or gif tag, which could be used to monitor the users movements through the affiliated web sites. The use of cookies, in gathering information, helps DoubleClick build profiles of users, by reading the cookie information and cross-referencing that information with existing stored data profiles.[13]

Conclusion

Cookies started out as a way to create a stateful session with HTTP requests and responses. The protocol listed two headers, Cookie and Set-Cookie, which carry state information between participating web servers and clients. This was a method of making and storing preferences to make a users browsing experience more enjoyable and productive by allowing the server to recognize a user and enable features such as on-line commerce, storing passwords, and preferences. As with most technologies, there is always someone looking for exploitation, and many found cookies to be a surreptitious method of collecting information from users or maliciously affecting another web site by changing the content on the site or interfering with the sites on-line business. Cookie exploits also allow information to be collected by sites that you never visited or would ever visit. Most users are not aware that someone out in cyberspace is cataloging and profiling their habits, much like Food Lion (a grocery chain), does when you use their “MVP” card. In recent years, there has been a push to enact privacy laws for the Internet. In the article about the class action suit against DoubleClick, Paul Schwartz, a privacy expert who teaches at Brooklyn Law School, stated, "The court said the Web site is the 'user' of the electronic service and can give consent to DoubleClick," he said. "So what are the individual consumers, chopped liver?"[13] He agreed with the presiding judge that the federal laws were ill suited to regulate the Internet world of cookie-based advertising and that Congress at different times has been worried about invasions of privacy.

There are many tools available to help you curb the use of cookie data collection and to prevent some of the current cookie exploits, such as the browser cookie preference settings, or 3rd party tools like LPWA and Cookie Crusher. Browser settings allow you some security, as you can disable cookies from being used on your machine or, at a minimum, set the settings to warn you when a cookie is being set so you have the choice of whether to allow or disallow the cookie. Some exploits override cookie settings like the one you set to only allow cookies to be returned only to the originating server. This "was" the setting I used until writing this report. There are web sites that list methods of controlling cookies by corrupting a cookie file entry and then setting the file to read only. In looking into available cookie managers I found one of the most popular tools available to be Cookie Crusher, a cookie manager that works with your web browser to give you complete control over which cookies are accepted by and stored on your system. Cookie Crusher controls cookies in real-time before they are placed on your hard drive. This

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

allows cookies to be not placed on your hard drive unless you specifically allow them to be there, thus eliminating the need to edit cookies that are on your hard drive after browsing. This tool allows you to filter out cookies based on specific servers and has the ability to determining a cookie's classification, function, and inform you whether the cookie is used for ad tracking, online shopping, or site tracking. Another great tool is the Lucent Personalized Web Assistant (LPWA). LPWA enables you to enjoy personalized services on the web while keeping your privacy. The program creates individual usernames, passwords, and email addresses for you for each web site that you visit and these values cannot be used to find out your true information.

There are many security issues still to be resolved with the use of cookies. Most cookie exploits available today are due to incorrect implementation of cookie specifications by the browser manufacturers. As cookie use becomes more prevalent on the web, new exploits will be discovered, and the browser manufacturers will need to act quickly to resolve these new problems. On the subject of cookies and invasion of privacy, the collection of personal information poses some security risks for individuals. The information collected and collated on a user could be used, not for its intended purpose of tailoring a site to a specific user, but to gather intelligence on that user. Some Dot Com companies that collected personal information and are now failing are selling the information they have stored to pay off their debts, or the information is being absorbed by the companies purchasing the failing Dot Com company. Unscrupulous people for their own gains could purchase the collected information. Congress is moving to create more safeguards. Sen. Fritz Hollings, D-S.C., has sponsored legislation that, will help prevent creditors from including customer information among a failed company's assets and also make it illegal to share customer information without the customer's prior consent.[14]

References

[1] Netscape. Persistent Client State HTTP Cookies [www page]. URL http://home.netscape.com/newsref/std/cookie-spec.html

[2] Kristol, D. & Montulli, L. (1997). HTTP State Management Mechanism [text document]. URL ftp://ftp.isi.edu/in-notes/rfc2109.txt

[3] Stein, Lincoln (1998). Official Guide to Programming with CGI.pm. Wiley Computer Publishing

[4] Beciragic, Jasmir (2000). Cookies and Exploits [www page]. URL http://www.sans.org/infosecFAQ/covertchannels/cookies.htm

[5] W., Peter (1999). JavaScript used to bypass security settings [text document]. URL http://www.epic.org/privacy/doubletrouble/securityfoc7_7_99.txt

[6] Cookie Central (1998). Cookie Exploit [www page]. URL http://www.cookiecentral.com/bug/index.shtml

[7] Lineham, Oliver & Stephens, Arun (1998). Cookie Monster vulnerability [www page]. URL http://www.securiteam.com/exploits/Cookie_Monster_vulnerability.html

[8] Mayer-Schönberger, Victor. The Cookie Concept [www page]. URL http://www.cookiecentral.com/content.phtml?area=2&id=1

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[9] Junkbusters Corporation (2000). How Web Servers' Cookies Threaten Your Privacy [www page]. URL http://www.junkbusters.com/ht/en/cookies.html
[10] Goodin, Dan (1997). Are Cookie Files Public record? [www page]. URL http://news.cnet.com/news/0-1005-200-324762.html
[11] Computer Incident Advisory Center (1998). I-034: Internet Cookies [www page]. URL http://www.ciac.org/ciac/bulletins/I-034.shtml
[12] http://www.epic.org/privacy/internet/cookies/default.html
[13] Kaplan, Carl (2001). Legal Victory for Internet Advertising Industry [www page]. URL http://channel.nytimes.com/2001/04/06/technology/06CYBERLAW.html
[14] Sandoval, Greg (2000). Failed dot-coms may be selling your private information [www page] URL http://news.cnet.com/news/0-1007-2176430.html

© SANS Institute 2000 - 2002, Author retains full rights.

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event