Global Information Assurance Certification Paper

Cookie crumbs, an introduction to cookies

Introduction:

The purpose of this paper is to give an introduction and overview of cookies. Their use and development have enabled Internet browsing, as we know it today, to exist. They are an important component of browsing and information systems. Marketing tactic is the first thought that one has when discussing cookies, but in fact their creation and evolution bring to the forefront issues like security, right to privacy and the continual pursuit to build a better mouse trap, the ingenuity that exists in the world today.

The recipe, or the origin of the cookie:

Cookies were first used in Netscape Navigator 1.0; two theories found take the mystery out of the name one is cookie is a common techie term used to describe "an opaque piece of data held by an intermediary". [1] The other from the UNIX world where they use "magic cookies" to name their tokens and credit The "Hansel and Gretel" Fairy tale where crumbs were placed to mark their trail.

Cookies are files that store user specific and web server information, which is saved to the user's machine. They are created by a web server and as needed are transmitted back to that server.

Originally intended to aid browsing by keeping information about the site browsed to on the users computer that could be accessed later, thus speeding up the transmission time to the site. When browsing the Internet a web page is loaded to the users' machine from a site then disconnected from the site. The method is practical for two reasons, firstly other users can log in and receive pages from the same site and secondly pages can be downloaded from different machines.

Additionally this disconnected idle time allows the user time to read through the site at their own pace. Cookies were developed to help the web server know where the user left off. When the user browses back to that site the cookie tells the server where they have already been making the access time much quicker.

To further explain and formalize the evolution of cookies, it is paramount that one understands the premise of HTTP (HyperText Transfer Protocol). "In HTTP 1.0 a lack of "state" or persistent connection is the fundamental weakness in this protocol". [2] Basically there is a user request and a server response, asking for, then receiving a page. However each request is not associated with the previous response, meaning there is no ongoing or continuous relationship between the requests.

A basic work around had to be developed because without maintaining "state" the server had no way of knowing who was sending a request. The cookie provided a solution by capturing information about the user, the page URL and whatever information deemed

needed, and then on demand send it back to the server.

The cookie's dough, or how the cookie works:

Cookies are located in the HTTP header and can contain as many as 6 parameters, listed below: [3]

- Name of the cookie.
- Value of the cookie.
- Expiration of the cookie.
- Path the cookie is valid for.
- Domain the cookie is valid for.
- Need for a secure connection to exist to use the cookie

An example is a as follows:
Set-Cookie: NAME=VALUE; expires=DATE; path=PATH; domain=DOMAIN_NAME;

They can be set of run from set from CGI (common gateway interface) or Java scripts. A persistent or session specific cookie may be created. Persistent cookies are stored on one's hard drive, where session cookies are temporary and are deleted when your browser is shut down or logged off.

A bad batch, or the problem that developed:

This functionality of the cookie easily lent itself the ability to send other information about the user to a server as well. Cookies have been used to note and transmit where, how, and when, people browse to web sites. While cookies do not steal information from one's hard drive, they can in fact gather private information that is sent back to a number of web servers. Most times information transmitted to a server is done so without consent of the user.

Since cookies are text files at first glance one might say, why all the fuss? They pose no inherit security breach. Cookies can not execute programs so you can not "catch" a virus, and no other server except the one that set the cookie can retrieve it. As it turns, out much the fuss is about user privacy.

Creative marketing companies and corporations continue to use this information to develop buying habits and preferences about consumers. With this information complied, marketers can send targeted ads and banners to Internet users advertising products that their buying and browsing patterns reflect. By obtaining the users email address, companies can send notices right to a person's email box. Recent tactics included using the cookie to obtain users home or business address and send paper adverts by snail mail.

An ever increasing amount of online advertising companies are embedding cookies in

their banners, enabling them to retrieve this user information at a later time.

Common uses today are: [4]

- On line order systems, those remember where you visited.
- Site Personalization, and customization, remembers what options users wants.
- Website tracking, show dead-end paths in web site where users browse to and then wander off, since no more interesting links.
- Target marketing; build a profile of the user so the same ad does not display more than once.
- User Id's.

The legality of Cookies:

The European community already has developed an Internet policy that addresses the cookie. Specifically this Directive, created by the European Parliament and of the Council of 24 October 1995 discusses the protection of individuals regarding processing and free movement of personal data available on the Internet. The directive was bold enough to require all member countries to an act similar legislation by the year 1998. It has been difficult to effectively enforce this policy because it does not apply to Countries outside of the EC.

One specific issue addressed is how cookie information can be transmitted without the consent of a user. Most times sending this data back to a web server is transparent, there by not requiring consent of the user. Recent web browsers allow users a flag option that notifies when a cookie is set, but under the directive the cookie value must also be displayed. This addresses the root of the cookie; http coding does not lend itself to reporting this information to the user in clear understandable English text, so one can decide whether that cookie should be transmitted back to a server.

Legislation has begun in the U.S., on February 12, 2000 Senator Torricelli, (D- NJ.) introduced a new bill that would limit the use of cookies. If Web advertisers are keeping a log of user browser activity this could be viewed as an invasion of privacy. This bill S.2063 would limit how Internet advertisers may use cookie files and information.

Additionally the EPIC (Electronic Privacy Information Center) along with FTC (Federal Trade commission) filed a complaint against DoubleClick, on February 10, 2000. Simply, this alleges that DoubleClick is using unlawful web browser activity tracked with cookies and, cross matching this information against national marketing databases which contain private personal information.

A smaller crumb, or new cookies on the horizon:

Richard Smith discovered and coined the term "web bugs". [5]
Web bugs are graphics usually 1 X 1 pixel in size whose purpose is to monitor information about the reader of the web page. They are HTML IMG tags and typically the image is loaded from a different server. They can be found embedded in web pages, emails and, if you using Outlook Express or Netscape mail, Newsgroups.

Web bugs can be a visible or invisible graphic, and are only considered bugs if are performing a monitoring function.

They are a trickier off shoot of the original cookie concept, because they transmit much of the same detail about the reader, but are harder to detect because of their small size. Additionally they are proof that businesses & marketers continue to value Internet users browsing habits and interests. They are good examples of continual ingenuity and creativity of programmers today.

Some of the information transmitted can be:
- IP Address of computer
- URL of Page that the Web Bug is located on
- URL of the Web Bug image
- Time the web Bug was viewed
- Type of browser that fetched the Web Bug image
- Previously set cookie value

Stopping Cookies:

There are three basic theories developed to combat cookies, they are disabling, setting your browser to alert you when accepting a cookie or blocking cookies selectively. One can disable cookies in Netscape Navigator by editing the preference or selecting Internet options in Internet Explorer. This solution may also prevent access to e-commerce sites.

Purchasing a software program that selectively blocks or disables cookies is the best option. It still must be noted that this even with some of these software packages cookies created in JavaScript of Metatags may not be blocked.

One can use Wordpad or Notepad to view cookies because they are ordinary text files. They may be deleted at will; your browser will start with out them. In Netscape these cookies may be removed from the cookie.txt file. In Internet Explorer they may just deleted. Even though there are warning against this tact, the sources found recommend this practice.

Remember a cookie may be set at every web site or page that one visits. This takes up

valuable space on your hard drive, waiting for you to travel to that site again. It is logical to free up this space.

A good practice is drafting and implementing corporate policies and procedures that deal with ways to combat or employ the use cookies. A policy like the U.S. government adopted recently is a great example, which states that Federal web sites must not contain any cookies, acknowledges the legal right to privacy on the Internet.

Lastly, research corporations or e-commerce sites that publish their use of cookies, and review their policies to decide if the practices are ethical or legal before engaging in business with the site.

Baked not burnt, or conclusion and comments:

While at first glance this topic appeared to be "old news" and already said by some one else. It was a concept that I took for granted and did not know the details of. This paper has enabled me to learn and understand the premise and consequences of cookies.

The research and current issues associated with it prove the cookie crumbs will continue to play an important part of information technology today. It is a dynamic area of the Internet that will be debated for years to come.