Luke Pederson

Internet cookies

The increasing number of Internet users has led companies to develop technologies to interact with consumers in the digital market. One of these technologies is Internet Cookies. Cookies have made Internet surfing much simpler, but have also led to intrusive and illegal behavior by companies and malicious parties. Today, cookies are the cause of the numerous incidents of unwanted behavior on a user's computer, intrusion of privacy, and security risks. Despite their popularity, regulation of cookies and repercussions for malicious use of cookies has not been effectively implemented. For the security of Internet users, awareness of the issue must grow in order for effective changes to occur. Cookies, as they are currently used, are a threat to Internet users everywhere.

Use of Internet cookies, also referred to as cookies, is common practice for websites today. Cookies can be used for various applications by websites including user authentication, website tracking, or simple temporary data storage. A common misconception is that a cookie is a program capable of directly accessing information on the user's computer; this is incorrect. Cookies are HTTP text based files placed on the user's computer by a website for later use (Brain, 2001). These cookies are stored in a location typically defined by the user's Internet browser and can be easily modified or removed; these types of cookies are not a particularly outstanding risk to security or privacy because of this. However, this simple description is no longer accurate as cookies continue to change.

A new type of cookie called a "Flash Cookie" has become commonly used for popular websites. Flash cookies are stored in a separate location from normal text cookies and also have a higher instruction capacity. One ability of a flash cookie is to "respawn" data that is deleted by the user. This means the flash cookie and normal HTTP cookie are given the same data, but if the user deletes the HTTP cookie the flash cookie will generate a new HTTP cookie (Soltani, Canty, Mayo, Thomas, & Hoofnagle, 2009). No notice is given to the user regarding these intrusive actions or the placement of the cookie on the

user's computer. This behavior is unethical, but has not become a particularly open issue due to businesses trying to hide these actions from consumers. One way a user can protect themselves is to consistently remove unwanted flash cookies from their computer. Flash cookies have the ability to carry out harmful actions on a user's computer and the capacity of flash cookies and their instructions is still in development.

Flash cookies create more security risks than HTTP cookies since they typically aren't removed as frequently or as easily. Also, HTTP cookies usually expire at the end of a session unless otherwise programmed by the server, but flash cookies have no expiration date (Soltani, et al., 2009). Altering the life span of cookies is no easy task; companies placing these cookies on users' computers don't want the cookies to be easily removed. The major threat for users are malicious cookies and malicious websites. Malicious websites can gather cookies from a user's computer and extract all the data stored in the cookies. Malicious cookies are designed to gather information about the user of the host computer. The cookie may be designed to gather personal information like passwords and credit card numbers. The cookie may also be given an abstract name to remain hidden from the user. In these cases, it is wise for the user to remove all flash cookies that have been created on their computer.

Websites also have the ability to place third party cookies on a user's computer (Mizaki, 2008, 16). An example of this is a website that hosts a banner ad which places a cookie on the user's computer whether or not the banner ad is clicked on. Regulation of the placement of third party cookies is controlled by the website, and of course, the user is typically not given notice regarding third party cookies being placed (Mizaki, 2008). Cookies may stay on a host computer and gather information until removed by the user, or until the cookie expires; these cookies can become trackable records of Internet usage. This behavior has been the cause of many unwanted and malicious cookies being placed onto users' computers. Users can stop third party cookies from being placed on their computer by disabling the option in most Internet browsers. Users should also consistently remove unwanted cookies. The use of third party cookies is a

way companies spread data and gather information while neglecting the safety of users.

The growth of the Internet has changed society many ways including how consumers interact with companies. Palmer says, “By 2002, 67 million Americans were buying products on-line, and Internet sales of all kinds have skyrocketed in recent years” (Palmer, 2005). Companies have been forced to adapt to this shift and create new ways to reach target audiences. However, companies are not concerned with the security or privacy of their target audiences; their only concerns are profit. Companies use tracking cookies to follow user's in order to analyze if a particular user would be more likely to purchase their product or service. Using this statistical data, companies can generate consumer profiles to target advertisements on a per user basis (Cunningham, 2002). Companies may also choose to sell this tracking data to other advertising companies who can use the data to find their target consumers (Brain, 2001). All of these transactions of data are not reported to the users the information is derived from, since there are no laws forcing companies to do so. To help stop collection of private information, users can use various methods or software to help disable websites from harvesting data. These methods might include consistently clearing cookies and other tracking data or using software to hide from data harvesting programs or websites. Legislative changes must also be made to alter company processes that gather user data and to better protect this private information. User awareness of this issue will be a driving force behind the alteration or creation of laws to protect personal data.

Websites are hosted all over the world, but regulation of the cookies is not prevalent. Internet advertisement companies have significant persuasion in the development of regulatory actions in legislation (Marsh, 2009). Protection of users at the legislative level requires more awareness of the issues of cookies and Internet users. Voting or other legal methods on a large enough scale to counteract company persuasion should a goal for users who want to protect themselves on the internet. A serious threat for users is the security of the statistical user data that companies collect. These large banks of personal user information have on many occasions been stolen or inadvertently released to the public.

Marsh reports a specific example of this, “In 2004, Scott Levine stole 8.2 gigabytes of information from Acxiom. The stolen data included names, home addresses, bank accounts, and credit card information” (2009). Not all the data obtained was through the use of cookies, but self replicating and difficult to remove cookies run in the same vein. Without proper security measures taken by companies, cookies can become extremely hazardous to the privacy and security of Internet users.

Websites have different privacy policies; they use cookies for a variety of applications. There are also different levels of information which can be derived from a user accessing a website. Cookies are often used to retain a name-value pair generated by the website (Brain, 2001). Cookies are also capable of collecting a user’s search queries, username and password, and even credit card numbers (Marsh, 2009). This information can be stored on the user’s computer or the website server. When accessing a website, the site can look for cookies that it placed in the user’s computer, but it may also access other cookies on the user’s computer (Marsh, 2009). Privacy policies often appear to the user more robust than they actually are. Marsh reports,

> These policies are usually unintelligible... These policies also fail to disclose how data will be used, making it impossible for users to object to bad practices. Without knowing how data is collected and sold, poor practices are difficult, if not impossible, to prohibit (2009).

Today, legislation regarding privacy policies and cookies are unable to effectively protect users. With no ramifications for malicious use of cookies, users are unable to protect themselves. Again, users who seek change in legislation regarding security and privacy on the internet should seek groups devoted to this issue. Since companies do have persuasion in the development of these laws, a strong effort must be made to promote awareness in the issue.

The use of cookies makes the Internet much simpler to traverse, but at the cost of privacy and security. Cookies allow users to access web pages without having to input their username and password for each page. It also allows websites to store user define preferences and records of pages viewed.

Also, there are no realistic alternative to cookies. Cookies when used with privacy and security in mind, serve a valuable purpose for users. However, abuse of cookies by companies and malicious parties has created new issues in the privacy and security of user data. Legislation for Internet cookies has not been developed to protect users and their data from this abuse.

Changes to the implementation of cookie technologies would help solve issues of privacy and security while still allowing their use to make the Internet easier to traverse. However, companies and lobbyists that use cookies have strong persuasion in legislation. Current legal repercussions for the abuse of cookies are not enough to stop these companies from harvesting user data. For effective change in legislation, users must become more aware of this issue and seek change. This can be done through voting or joining groups devoted to the protecting personal user information. Users should also protect themselves by constantly removing unwanted cookies, disabling third party cookies, and using software for help protect their private information when accessing the Internet. Today, despite the benefits, cookies have a become a serious threat to users.

References

Brain, M. (2001). How internet cookies work. Retrieved, October 31, 2011, from http://www.howstuffworks.com/cookie.htm

Palmer, D. (2005). Pop-ups, cookies, and spam: toward a deeper analysis of the ethical of internet marketing practices. *Journal of Business Ethics, 58,* 271-280.

Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. (2009). Flash cookies and privacy. UC Berkeley School of Law.

Cunningham, P. (2002). Are cookies hazardous to your privacy? Cookies allow business to collect information about Internet users, but some question whether they are valuable records or unethical tracking mechanisms. Retrieved October 28, 2011, from http://www.freepatentsonline.com/article/Information-Management-Journal/87454389.html

Marsh, R. (2009). Legislation for effective self-regulation: a new approach to protecting personal privacy on the internet. 15 Mich. Telecomm. Tech. L. Rev. 543. Retrieved October 29, 2011, from http://www.mttlr.org/volfifteen/marsh.pdf

Miyazaki, A. (2008). Online privacy and the disclosure of cookie use: effects on consumer trust and anticipated patronage. Retrieved October 25, 2011, from ftp://ftp.cba.uri.edu/Classes/oliver/JPPM%20-%20Hillary/Miyazaki%202008.pdf