Cookies Privacy and Cyber Security

Ashok Kumar Reddy Nadikattu

Sr. Data Scientist & Department of Information Technology

California USA

Abstract

If you use the word "cookies," some people would believe you're about to give them a treat. However, from a computer standpoint, these are not dessert menu objects, and they cannot be tangible objects. Still, they serve essential functions in assisting someone who is searching the internet, and they may cause problems if not handled properly. A computer cookie is a tiny text file that is stored in the browser of a computer. A device cookie is also known as a browser (internet/web) cookie or an HTTP cookie informally. A cookie is a set of data, regardless of its name. A cookie allows a website to remember information and details such as a user's interests to be recognized when they return. In layman's terms, a cookie can be thought of as a "memory" that allows a website to recognize and react to a user. When a computer user visits a website, the website sends a cookie to their computer, which the computer receives and stores in a designated location of the browser. It aims to aid the browser in tracking and recording browser activity. Many users tend to keep records of their searching and download activities by saving their login information on frequently visited websites (Lacy and Prince, 2018). Despite their monitoring and storage capabilities, fraudsters and cyber-attackers may use these cookies to monitor users' online activities and commit cyber-crimes such as sending malicious ads (Zarouali et al., 2017). This paper aims to describe the different types of cookies and how they are used to invade data privacy. Additionally, the report will discuss cybersecurity threats that may arise when cookies are used in a computer or browser.

Keywords

Cookies, Cybersecurity, data privacy

Introduction

In contemporary society, technological innovation has elicited a mixed response. Despite the fact that information technology makes person and business activities much more accessible, there are many problems associated with its use. Within minutes, you can lay back, make a purchase, and have ordered goods to your home. In the same way, automation and improvements in technology have helped businesses significantly reduce the cost of manual effort in manufacturing processes. Social networking is possible thanks to various social media sites that provide unique services to their users. Human beings pay the price for information technology. When it relates to the use of information technology by individuals and companies, one of the significant points of concern is Cybersecurity

(Gootman, 2016). Data has become the new digital gold, and it is expected to become more costly, especially as the digital age continues. Awareness is a critical component of nearly any project being initiated, whether it is a research study or an advertising campaign for businesses. Also, for small companies, data is essential for determining the project's viability.

Because of the risks that could come with the disclosure, internet users have been concerned about their personal information being exposed as they use social media sites. With the increased use of the internet for purchasing and selling, online users have expressed concern about the security of their personal information exchanged with different websites. As a result, Cybersecurity has become one of the most critical aspects of treatment for many people and organizations. In today's world, identity fraud has become commonplace. It's difficult to read or watch the news without seeing any incidents involving Cybersecurity. It is clear that advancements in security practices have not balanced advancements in information technology. It's become increasingly difficult for systems to be entirely safe, as technological advances have exposed flaws in even the most secure methods. As a result, researchers and I.T. experts must devise new strategies for improving Cybersecurity while still keeping up with technological advancements to plug the gaps in current security measures (Baumann & Schunemann, 2017). All security risks are faced by humans interested in mining personal data for various purposes, including identity theft and service denial. Different laws regulate the use of technology; online privacy is something that many cyber rules that have been enforced across the world take seriously (Confer & Heuple, 2017).

Literature Review

Cookies

It would be impossible to talk about Cybersecurity without mentioning cookies. These can be defined as small text files that are found on a computer. They recognize the activities of a network as shared between web pages (Kulyk, Hilt, Gerber, & Volkamer, 2018). They mainly help in logging in to a website and purchase of items on an online platform. Through cooks, servers can identify one's computer and remember things that are conducted by an individual through his laptop. Cookies are widely used by advertisers and online businesses in marketing their operations online (Zarouali et al., 2017). The use of cookies has been a subject of heated discussion regarding vulnerabilities they create in one's system through the sharing of information about the online activities of a user. While many people view cookies as a security threat, an equal number of people feel that cookies indeed pose no danger to Cybersecurity and only the privacy of IT users. Much research has been done on the same, and answers vary from one research work to another. The history of cookies dates as early as 1994. In this year, Lou Montulli developed one of the earliest web browsers in the world of computers. He acquired a lot of experience, and his innovative minds helped him come up with cookies, HTTP proxying, and Server push and Client push. According to Montulli, cookies got their name after a computer science word, "Magic Cookie," which is described as something passed by routineness of applications that allows the recipient to conduct some operations. At Netscape browse, Montulli had an idea of using some programs similar to cookies in the company's browser for communication. Cookies then became the first to be used in the company's brewers in knowing whether users had visited the company's website. These cookies allowed the website to remember a person's preferences and keep a history of the items viewed by a visiting customer as placed in the virtual carts.

At this period, people did not understand cookie until the year 1996, when potential threats by cookies on personal information were popularized by the media. The issues raised by the numerous media reports revolved around the fact that cookies were storing information on personal computers without the user's knowledge. The news spread and created panic in the country, such that in the year 1998, the U.S. Department of Energy Computer Incident Advisory Capability released a report that entailed its assessment on the issue of cookies. The report asserted that the vulnerably of various system or snooping through the use of cookies could not be ascertained in any way (Floros et al., 2013). The report conducted that cookies could only tell a web server whether a person had been visiting the website before. The limited information shares with the website servers included several visits to remind the site of the next stop. The report clarified that the information on the places that a user had visited before could easily be located from the browser log files and could be used in tracing the user's browsing habits. Therefore, cookies only made this function easier.

Types of Cookies

There are three different types of cookies; they include third party cookies, persistent cookies, and session cookies. Cookies are virtually visible small text files that significantly differ from one another. Each type of cookie has a distinct function and mission as described below.

Session cookies

These are simple cookies that remember the online activities of a person. Owing to the fact that websites do not have memory, it would be typically impossible to remember the browsing history of an individual without these cookies. Each activity done on a website would be treated as a new user with a new business. Some application of session cookies can well be illustrated by looking at online shopping. Here checking out guarantees the items will be found thanks to the cookies.

Persistent cookies

These are also known as first-party cookies. They usually function by tracking all online activities and preferences of and a giver person. For instance, for the first visit to a site, the cookies are basically at their default state. When one personalized the website, these cookies have the ability to remember these settings and put them in place with each login by that individual. The functioning of computers is similar to these cookies in that each login makes machines set all the preferences set, including the language selection and the bookmarks. These cookies are usually stored on the hard disk, generally for a long time.

Third-party cookies

These are also known as tracking cookies; they collect the data regarding one's online activities. Each time a person visits a website, various information regarding the user's activities are collected and sent to the website that created these cookies. The data collected is hence sold to the advertisers. Tracking of one’s interests, preferences, and search trends is done through this. Therefore, marketers can send customized ads to a person thanks to the information revered through these cookies. However, this is viewed in many aspects as being intrusive to the users' online privacy.

Privacy

There is nothing valuable in the world of information technology as having privacy with your online activity and information shared. Privacy touches on various aspects of life, ranging from access to the medical history of a patient: personal bio and other necessary information, such as credit and social security number (Torra, 2017). According to the Health insurance portability and accountability act (HIPAA), individuals have the right to autonomy for their personal information from unauthorized access by third parties. Entities such as hospitals have the duty to ensure that the information shared by the patients remains secure and private, as stipulated by the act. Failure to adhere to the provisions of the law is liable for a fine or a jail term. The essence of privacy for individuals is to ensure that one's personal information remains in one's realms. No one can be jeopardized based on the information shared with entities such as hospitals. It also protects one from incidences that may be brought about by exposing one’s personal information to third parties.

Privacy and Cybersecurity are intertwined in a manner that one cannot detach privacy from Cybersecurity. There are various components of Cybersecurity. It would be impossible to attain complete Cybersecurity without privacy in I.T. At the same time, it would be hard to achieve privacy without Cybersecurity. This means that the two terms complement each other in the world of Information technology. There are various roles that both I.T. users are anticipated to play in enhancing their security. On the other hand, the developers of sites and applications are also expected to increase the security features of their websites to protect the user data from being accessed or stolen by attackers (Zhelang, 2017). The growth of information technology has prompted a regular revision of the cyber laws to ensure all the emerging issues in the cyber world.

Cookies and Privacy

For quite some time, cookies and privacy have taken the forefront in various discussions, with many people arguing that cookies do not pose any vulnerability to privacy concerns of uses of information technologies. The same opposition is seen from the people who say that cookies have nothing to do with vulnerabilities on people's privacy concerns and their systems. The reality is that cookies do not damage computer systems in any way. They’re all text files that can be disabled whenever you want (Cavusoglu et al., 2005). They aren’t plug-ins, and their applications aren’t either. Cookies cannot be used to spread malware or gain access to your computer’s hard drive. This isn’t to say that cookies aren’t crucial for a user’s online privacy and anonymity. Cookies cannot access your hard drive to obtain information about you; however, unless you have disabled cookies in your browser, any personal information you provide to a Web site, even credit card information, will certainly be stored in a cookie. Cookies are just a threat to privacy in this way. Only information that you freely submit to a website will be held in the cookie.

In many cases, cookies can be blocked, but after doing this, many websites are rendered less active as they were when cookies get blocked. When one needs the entire functioning of the site, one is prompted to accept the cookies to get the entire operation of the website. People concerned about their security find cookies a nuisance to their autonomy due to their impact on the effectiveness of a web page. However, there are various ways through which this issue can be addressed. One of the best methods is to delete cookies once we close the browser. Another critical purpose is to browse by anonymizing; this ensures that one's identity is masked. It, therefore, becomes complicated for the cookies to track down the activities of a person. However, in respect to jeopardizing the privacy and security of people, cookies cannot be categorized as such. People, therefore, need to be much concerned about other technologies that can use these cookies break down the security protocols of a system.

In many cases, cookies are usually set by the sites that one visit; this is not always the case, in some instances, they are set by the third parties associated with the places that people visit. Not once that one tends to get cookies from the website that he has never heard or visited. The truth of the matter is, these sites are usually related to the places we visit. The essence of these cookies is aimed at helping entities in marketing their brands with the aim of increasing their sales revenues, which leads to an increased profit margin. Through these cookies, personal browsing data is analyzed using the items viewed from one website to another (Jegatheesan, 2013). The information gathered is of great essence to the marketing body as it helps predict the purchasing behavior of the targeted customers and hence allows the business to serve with the right products and services following their purchasing patterns.

How Cookies Invade Privacy

There are many ways online users have to describe and attested cookies to have invaded their privacy. To explain this, it is essential to use an example of an actual situation that can face anyone as they use the Internet—taking the case of a person entering a restaurant or a lodge. One is stopped by the security personnel at the entrance who ask to do a thorough search (Hessler et al., 2018). They record all the items found with you and also take notes of the items found with you. As if not enough, there are hidden cameras that record every activity and movement of a person. The functioning of cookies can be said to work similarly to this example. Cookies gather information about the browsing activities of a person once they are allowed into one's computer (Gupta et al., 2016). This is viewed as a significant issue of concern regarding the privacy of the people involved.

On top of tracking down the activities that one engages in on his browser, cookies bring endless ads that, apart from cutting disrupting browsing sessions, may prompt one to look at the items being displayed. The issues with these adverts are that they are usually from the same website, and the likelihood of a similar thing being shown is very high. It eliminated the chances of a person viewing new themes and products from other business entities. Many people do not feel comfortable with the endless ads courtesy of cookies as they make the overall experience of browsing to be clogged by unnecessary popups (Isaak & Hanna, 2018). There have been some development done on some browsers to ensure that cookies are blocked automatically to address this issue. However, this is not the final solution as it also limits access to sites that one must allow cookies to access the contents of the websites.

Security Concerns Regarding Cookies

Although security issues are not directly associated with cookies, there are some incidences that cookies indirectly cause a security alarm for the users of I.T. For websites that generally use cookies to provide access control schemes, having many users usually set cookies and login credentials and the session details in some cases. When not correctly implemented, the system becomes prone to various vulnerabilities imposed by third parties. In many cases, packed sniffer programs can get into cookies when transferred between the server and the browser, hence getting into a website in question that grants cookies (Degeling et al., 2018). With Domain name server (DNS) used in determining the cookies used with a given served, it becomes quite possible for one to cheat and play ahead with a browse in sending cookies to the server through subversion of Domain name server temporarily. The chances of compromising a person's login credentials become one of the significant issues of concern through this vulnerability created through cookies.

Another critical security compromise that can be attributed to the use of cookies is the exposure of personal information. Information shared on a browser is likely to be collected by the cookies and stored. If the website whose cookies have been allowed is malicious, the shared information can be used by people with ill motives to commit a cybercrime (Aggarwal & Reddie, 2018). Information such as credit card number and passwords, when stored by the cookies, serves as a significant risk to users' online privacy. When accessed by third parties through cookies, this can be a considerable security threat to the online users of government services (Houser & Voss, 2018).

How Improving Cybersecurity Will help the U.S.

Privacy infringement and Cybersecurity attacks in the recent past have increased. Businesses and individuals have suffered losses due to data loss and identity theft. Despite technology seeing some rapid developments, there have never been effective security enhancement measures that address the security concerns people currently have. There are, however, some possible ways that can be implemented to reduce vulnerabilities and risks. One of the best ways to ensure that security and privacy are enhanced is by reducing over-reliance on I.T. (Aladeokin, Zavarsky, & Memon, 2017). This ensures that critical information is not shared through the Internet. Another important way to enhance privacy and security is by employing new technology in managing incidences. This entails moving with the latest technology is addressing security concerns. The use of antimalware may help detect malicious cookies directed at collecting personal information.

Conclusion

Though computer cookies are essentially harmless, they can only store data in several different ways. They cannot dig up personal information or reveal data on computers by themselves. Users upload their information web sites in order forms, login sites, payment sites, and other internet pages, not cookies. After that, the data is encoded and protected against attacks using security features such as stable sockets layers (SSL). On the other hand, Cookies have been heavily criticized in the past for being seen as a potential threat to user privacy. This is because they monitor user activity and save browsing history. This creates a significant challenge in ensuring cybersecurity as web users are exposed to malicious ads, and their information can be tracked through the internet.

In summary, security is one of the major concerns for online users. Privacy touches on various aspects of life, ranging from access to the medical history of a patient. Personal bio and other necessary information such as credit and social security number while security guarantees the safety of the information stored from being accessed through breaching security protocols. Cookies, on the other hand, are primarily meant to enhance the user experience with the website. In many cases, they have been associated with the infringement of privacy rights of the online users. It is essential, too, therefore, to understand how cookies work and the truth about them.

References

1. Aggarwal, V. K., & Reddie, A. W. (2018). Comparative industrial policy and cybersecurity: the US case. *Journal of Cyber Policy*, *3*(3), 445-466.
2. Aladeokin, A., Zavarsky, P., & Memon, N. (2017, September). Analysis and compliance evaluation of cookies-setting websites with privacy protection laws. In *2017 Twelfth International Conference on Digital Information Management (ICDIM)* (pp. 121-126). IEEE.
3. Baumann, M. O., & Schünemann, W. J. (2017). Introduction: Privacy, data protection and cybersecurity in Europe. *Privacy, Data Protection and Cybersecurity in Europe*, 1-14.
4. Confer, S., & Heuple, K. (2017). A socialist theory of privacy in the internet age: An interdisciplinary analysis. *Philologia*, *9*.
5. Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2018). We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. *arXiv preprint arXiv:1808.05096*.
6. Edwards, L. (2018). Data protection and e-privacy: From spam and cookies to big data, machine learning and profiling. *Machine Learning and Profiling (May 23, 2018). Forthcoming in L Edwards ed Law, Policy and the Internet (Hart, 2018).*
7. Gootman, S. (2016). OPM hack: The most dangerous threat to the federal government

today. *Journal of Applied Security Research*, *11*(4), 517-525.

8. Gupta, B., Agrawal, D. P., & Yamaguchi, S. (Eds.). (2016). *Handbook of research on modern cryptographic solutions for computer and cyber security*. IGI global.
9. Hessler, M., Pöpping, D. M., Hollstein, H., Ohlenburg, H., Arnemann, P. H., Massoth, C., & Wenk, M. (2018). Availability of cookies during an academic course session affects evaluation of teaching. *Medical Education*, *52*(10), 1064-1072.
10. Houser, K. A., & Voss, W. G. (2018). GDPR: The end of Google and Facebook or a new paradigm in data privacy. *Rich. J.L. & Tech.*, *25*, 1.
11. Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56-59.
12. Kulyk, O., Hilt, A., Gerber, N., & Volkamer, M. (2018, April). this website uses cookies": Users' perceptions and reactions to the cookie disclaimer. In *European Workshop on Usable Security (EuroUSEC).*
13. Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse*, *8*(1), 100-115.
14. Torra, V. (2017). *Data privacy: Foundations, new developments and the big data challenge*. Berlin: Springer International Publishing.
15. Wang, H., Gao, C., Li, Y., Zhang, Z. L., & Jin, D. (2017, November). From fingerprint to footprint: Revealing physical world privacy leakage by cyberspace cookie logs. In *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management* (pp. 1209-1218).
16. Zarouali, B., Ponnet, K., Walrave, M., & Poels, K. (2017). "Do you like cookies?" Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior*, *69*, 157-165.
17. Zerlang, J. (2017). GDPR: a milestone in convergence for cyber-security and compliance. *Network Security*, *2017*(6), 8-11.