Analysis on Cookies and Cybersecurity

Jiakun Yang *[a]
[a]College Of Science, Purdue University, West Lafayette, USA
* Corresponding author: yang1800@purdue.edu

ABSTRACT

Cookies are essential to the modern internet. People use cookies and other tracking technologies to integrate the browsing experience of websites, present personalized content and targeted advertising, understand the origin of their audience, and analyze web traffic. In most cases, by clicking "yes" or "I accept," people will agree to the use of tracking technologies and cookies. An investigation of cookies and cybersecurity is necessary and imperative. This thesis is going to thoroughoy investigate the function that cookies present within the internet world, the actual challenges it poses to cybersecurity and its existence. In order to accomplish the investigation, the thesis analyzes the pros and cons of cookies on cybersecurity, the pros and cons of cookies and cybersecurity through consumer feedback. The findings indicate that there are gaps in privacy. A critical set of effective actions have emerged for organizations that are looking for methods to address the consumer protections and data security requirements. From security perspective, organizations ought to be aware of what data they actually need to serve consumers.

Keywords: Cybersecurity, Cookies, technologies

1.INTRODUCTION

Since the data within cookies do not change, cookies themselves are not hazardous. They could not attack a computer with a virus or other malicious software. However, some network attackers could hijack cookies and have entry to the browsing session. Cookies are a vitally significant and relevant technology that the internet is utilised by an enormous number of people nowadays. Cookies are crucial to the internet experience. It is pleasurable solution to handful of missing protocols. Based on the cookies, a consumer could be capable to remember the schedules according to which a user could visit his or her website. It is as well being able to provide a better personal content, better online shopping experience and more accurate advertisement. However, cookies could be utilised to implement the functionality and history of a cookie and is not secure by design. It does not ensure the trustworthiness, security or integrity of the information. When the web surfing requirement exceeds transport layer security, security load constrains the cookies to a secured channel. Although this can preserve the attacker from perfection as sending requires to the secure sites, another cookies characteristic is http solely. Hackers were able to access to networks and computers to steel messages that is confidential and comprehensive. These specifics might belong to financial, science, medical or other sectors. It is critical to ensure the information confidentiality, since these parties are connected with the individuals to whom the information belongs to already. Cookies can critically provide two significant attributes in security and http. First, the thesis is going to provide a thorough investigation of cookies and cybersecurity via a second research method with the combination of qualitative and quantitative data collection. Secondly, the thesis is going to analyze the benefits and the disadvantages of cookies for cyber security. Finally, at the end of the thesis, conclusions and recommendations are going to be presented.

2.LITERATURE REVIEW

2.1 Literature of cookies

2.1.1 Cookies are not malware however it does brought risks

Cookies are not inherently dangerous. They are merely text files that facilitate the coordination between the remote web server and the browser for the entire functionality of the website. These features range from verification and automatic login to shopping cart functionality, preference settings, and third-party add-on services [1]. To enable users to browse the restricted pages while not having to repeatedly verify their identity, cookies are utilised to save authentication data such as passwords and usernames. Accordingly, it is essential to ensure the authenticity and confidentiality of cookies that contain information. Alternatively, any individual with access to the cookies might impersonate the user. Despite the

Third International Symposium on Computer Engineering and Intelligent Communications (ISCEIC 2022),
edited by Xianye Ben, Proc. of SPIE Vol. 12462, 124620U · © The Authors. Published under a
Creative Commons Attribution CC-BY 3.0 License · doi: 10.1117/12.2660965

fact that credential information stored in cookies is frequently presented during a server-specific form, where the contents are hidden from the viewer, an attacker may still be able to simply replay the intercepted cookie and impersonate the user. Implementation flaws, particularly within web browsers, could present a safety risk to users as well. For instance, a vulnerability in Internet Explorer versions five and four for Windows 98, 95, 2000, and NT permits any website to view the contents of cookies from other sites. This is due to the fact that web browsers obfuscate sites with lengthy URLs ending in the server's domain name with that other server. Therefore, it is conceivable that a malicious site could potentially offer itself a lengthy URL that ended with the same sequential characters as another site's URL, the web browsing demonstrated through Figure 1.

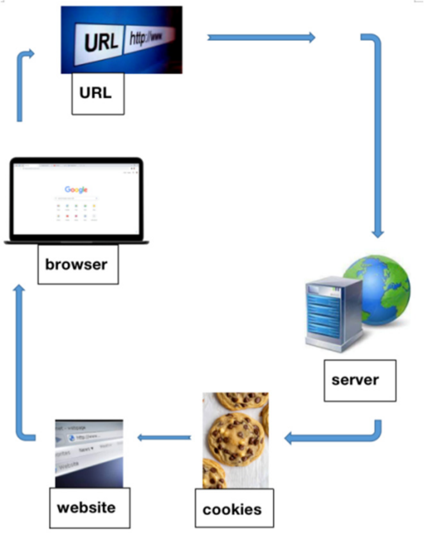

Figure 1. Web browsing demonstration

The malicious site would then be capable of accessing cookies stored by the other website. The ramifications of this scenario could be severe if the cookie content contains personal information such as confidential data with account information. Although the web browser vulnerabilities have been fixed, there might be additional undiscovered vulnerabilities that would pose a safety threat to the users[2].

2.1.2 Concerns for Cookies

A notably controversial concern regarding cookies is that they could be utilised as tracking equipment to track the user's equipment to track the user's actions on the web. Firstly, a graph is downloaded from a website, and the user's browser is going to receive a cookie consisting of a random ID. From that point, each time the browser connects to a website and includes an advertising company's banner. It is going to deliver the cookies with a random ID, alongside the URL of the web page being read. After a certain period of time, the advertisement corporation will be able to produce a user profile that discloses the user's viewing interests and habits. This could potentially be used to refine ad campaigns, target users' interests with ads, and prevent the same ads from being shown to users repetitively. The capability to trace users is a potential violation of user privacy. It is also possible for ad servers to store and share this information without the user's permission, albeit without strong evidence of the activity at the time. Even though the use of cookies as a tracking device might not disclose a user's actual identity, the fact that an advertisement agency's server could retain a list of URLs that a consumer has viewed could potentially lead to the disclosure of a user's personal information [2].

2.1.3 Fundamental Types of Cookies

There are three specific types of cookies, namely, persistent cookies, third-party cookies, and session cookies as illustrated within Figure 2.

Figure 2. Three types of cookies

Each type of cookie has a different mission and function. The first type of cookie is session cookies. Which are basic cookies that remember a person's online activity. Each activity performed on the site is treated as a new business for a new user. Some applications of session cookies could be well illustrated by using online shopping, and the item is going to be found due to the presence of cookies. The second cookie type is persistent cookies. These cookies are known as first-party cookies as well. Their function is usually to track all online activity and preferences, as well as to give advice. For example, for the first visit to a website, these cookies are essentially within their default state. As a person personalises a website, these cookies have the ability to remember those settings and put them in place each time that person logs in. Computers function similarly to these cookies, and each login causes the machine to set all of its preferences, concluding language preferences and bookmarks. These cookies are typically stored without the hard drive and are generally kept for a long period of time. The third cookie type is third-party cookies. These are known as tracking cookies as well. They gather data regarding a person's online activity. Each time an individual visits a website, a variety of information regarding the user's activities is gathered and sent to the website that generated these cookies. The data gathered is thus being sold to advertisers. The tracking of a person's interests, preferences, and trends is done in this manner. Hence, marketers could send personalised ads to a person due to the information obtained through these cookies. Nevertheless, this is in numerous ways considered a trust in the user's online privacy [3].

2.2 Literature of cybersecurity:

2.2.1 Corporation situation for cybersecurity

Every aspect of digital business has significant cybersecurity implications. For instance, as corporations pursue generating more digital consumer experiences, they require determining paths to adapt their teams governing security, fraud prevention, and product development to enable them to design controls and produce experiences that are convenient and secure with authentication. As corporations employ massive quantities of data analytics, they have to ascertain paths to discern the risks posed by data sets that integrate numerous types of exceptionally sensitive client information. They had to incorporate security controls into analytical solutions as well, which might not utilise formal software development approaches. As corporations employ robotic process automation, they have to manage robotic credentials effectively and assure that boundary cases, cases with unusual or unexpected factors, or input that exceeds normal limitations, do not introduce safety risks. As well, as corporations establish application programming interfaces for external clients, they have to identify methods for identifying vulnerabilities generated by the interaction between numerous application programming interfaces and services, and they have to enforce and establish proper developer access criteria. As they transition from waterfall application design to agile application construction, they have to continue to be rigorous about application security [4].

2.2.2 Data management for cybersecurity

Data governance is at the center of privacy. Data is a nebulous concept that could encompass a broad array of information, so it is valuable to break down the various collections before examining the way each area is relevant to people's privacy and security. All of this data, whether lost in various data breaches or stolen piecemeal through phishing activities, could provide attackers with sufficient information to engage in identity theft, utilize the name to obtain loans, and possibly harm online accounts that depend on properly responding to security questions. The information could as well prove to be a gold mine for advertisers lacking ethical boundaries as it falls into the wrong hands. Browsing habits and websites accessed via internet activity are monitored by internet service providers and could be hijacked. While consumers are powerless against attacks at the internet service provider level, the websites people visit might be tracked by cookies as well, which are small segments of text downloaded and stored by the browser. Browser plug-ins might track the activity on multiple websites as well [5].

2.2.2.1 Cybersecurity in data Management of finance sector concern

In a purposeful attack, fraudsters are employing societal engineering techniques to impersonate consumers in calls to phone service vendors. They accomplish this in order to transfer a number from the phone, even if merely temporarily, and then possess the number within the time required to capture the two-factor authorization issued to the phone number and gain access to the intended account, a bank, cryptocurrency wallet, or email. As the phone bug ends up being out of control, which implies the two factor authorisation code could be stolen, any online accounts connected to this number are risking being hijacked [6].

2.2.2.2 Cybersecurity in data management of medical sector concern

Another entrant, hospitals, is currently transitioning to electrical records, with family DNA services records storing, DNA services, storing genetic information pertaining to their users, to be submitted in the event of a sought, after health-related query or to track family history. The disappearance of medical information is extremely personal and could be distressing and catastrophic for each individual. However, when it comes to DNA, the decision to release this information is personal, except for those in law enforcement, as well as often those in ancestral services, who release this data first. The privacy concerns associated with DNA searches were cited in the decline in sales of several popular family ancestry kits.s [7].

2.2.2.3 Cybersecurity concerns of cookies

It is impossible to talk about web security without mentioning cookies. These could be defined as small text files discovered on a computer. They identify the web activity shared among web pages. They mainly assist with logging in to websites and purchasing items on online platforms. Through cookies, a server could identify a person's computer and remember what the individual has done on her or his laptop. Advertisers and online businesses utilise cookies extensively to market their businesses. The usage of cookies has been an intense topic of discussion. They generate vulnerability in one's system via sharing information regarding a user's online activities. While numerous people believe that cookies pose a security risk, others believe that cookies only threaten the privacy of IT users and do not pose a threat to cyber security. Many researches have been done on this point, and the answer differs from one study effort to another. This history of cookies goes back to 1994. During this year, Lou Montulli created one of the first web browsers in the computer world. He gained experience and his innovative thinking enabled him to come up with cookies, client push, server push, and HTTP proxies. According to Moutulli, the name cookie is generated from the computer science word magic cookie, described as something delivered by an application's routine which permits the recipient to perform an action. At Netscape browse, Moutilli had an idea to utilise cookie-like programs to connect within corporations. Cookie will becomes the prior application of the corporation's brewers in terms of knowing if a consumer has visited the corporation's website. These cookies enable the site to remember a user's preferences while browsing and to save the times' history, essentially shopping carts [3]. Cybersecurity concerns cookies during every web browsing as shown in

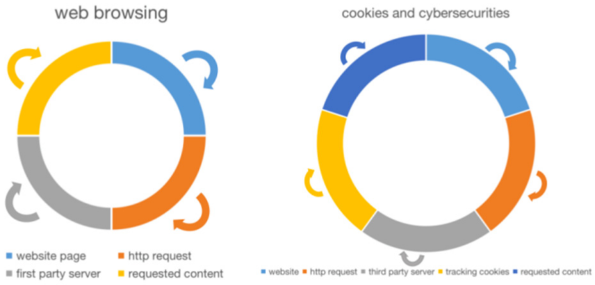

Figure 3. Web browsing and cybersecurity

3. METHODOLOGY APPROACH AND DATA COLLECTION

3.1 Secondary data collection

Secondary data served as a starting point for basic researchers to try to move beyond. Applied researchers, on the other hand, are more concerned with utilising knowledge that exists already, in several forms at least, to solve specific issues. Secondary data is a prerequisite condition for successful practice. Secondary research assists in setting the agenda for subsequent primary studies by indicating issues within the previous studies. Secondary information identifies the instruments for conducting primary research in terms of the issues that ought to be addressed as well as the measurement instruments and relevant interviewees. Secondary information is a significant resource for all social scientists [8]. Secondary research utilises exclusively existing secondary data or information collected with respect to other purposes or programs. It's primary purpose is to examine whether the research on a subject already exists. This assists in formulating the research question more accurately and identifying viable methods for visualisation, synthesis, and data collection. Desk research ought to always be considered the entry point of the research procedure in order to avoid repeating the same mistakes and standing on the shoulders of giants [9]. The prospects for secondary data analysis are manifold. It could enable researchers to generate data that they could not reproduce in the first place. The technological expertise associated with developing well-conducted surveys and robust datasets could lead to data of the utmost quality. It could also permit data to be analysed and copied from a variety of standpoints. Secondary data analytics is the ideal complement to hybrid methods and, crucially, a methodology that actually permits social scientists to stand on the shoulders of giants [10]. Data collection indicated through Figure 4.

Figure 4 Data collection

3.1.1 Limitation

Secondary data was originally collected for a specific purpose, which might raise other issues. Specific classifications, specific measures, or therapeutic impacts might not be the optimal fit for the present purpose. Secondary data is defined as older information. As a result, this data might not be exceptionally contemporary for certain purposes [8].

3.2 Qualitative data collection

Qualitative surveys present a fairly accessible and straightforward instrument for qualitative researchers, but things could go wrong and there are pitfalls to avoid. Two of the biggest potential issues are random completion and roll-out. For instance, while as many as nearly six hundred finished BHRA surveys were collected, approximately a thousand people initiated the survey. The majority of those who did not finish answered the demographic questions. However, no additional questions were given. The online form implies the uncertainty that the reason occurred. Nevertheless, this high roll over ratio is unlike what might happen within quantitative survey recruitment. Qualitative surveys demand effort, expertise, and time from participants, and this truth requires recognition. For both the hard copy format and the dead email format, whereby participants provide their details, email reminders could foster completion and return. However, online survey instruments provide automatic email reminders as well. For qualitative surveys, people rely on individuals' self-selection to demonstrate their interest in being a project participant, particularly as they conduct the survey online with no researcher contact [11].

3.3 Quantitative data collection

A major research tradition regards social reality as exterior to the people involved; it is the context within which their activities take place and it has the power to regulate their actions. Knowledge regarding reality could be acquired by constructing a bridge to that reality through the utilisation of concepts as well as their measurement. The concept determines facets of reality, and the instruments are devised to gather data associated with the concepts. With this approach, the data is supposed to signify certain dimensions of reality or ongoing happenings. This tradition is related to positivism and critical reasoning, and its data collection processes are primarily quantitative [12]. Quantitative approaches are utilised to gather data or are about to be converted into figures for analytics. Within quantitative studies, dimensions of societal reality are converted into figures in various ways. Measurement is performed by assigning objects, events, or people into discrete classifications, or by featuring them according to arbitrary rules on a numerical scale [12].

4.DISCUSSION ON THE PROS AND CONS FOR CYBERSECURITY OF COOKIES

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

4.1 Advantages of cookies for cybersecurity

Cookies are not inherently dangerous. They are merely text files that facilitate the coordination between the remote web server and browser for the entire functionality of the website. These features range from verification and automatic login to shopping cart functionality. preference settings and third party add services verification and automatic login to shopping cart functionality, preference settings and third party add services. To enable users to browse restricted pages while not have to repeatedly verify their identity, the cookies are utilised to save authentication data, as passwords and username [1]. Cookie becomes the prior application of the corporation's brewers during terms of knowing if a consumer had visited the corporation's website. These cookies permit the site to memorise one person's preference browser and to remain the times' history, virtually shopping carts. There are numerous perils associated with the utilisation of cookies. However, within reference to cookies, the issue of cybersecurity is editable. On average, a website stores twenty cookies. Although cookies have a date of expiration, this data might be a long time within the future, as months, years or weeks, google ads allows cookies to last five hundred and forty days. Consequently, at the most basic level, consumers ought to know exactly what cookies are, what information they consist of, how the information is utilised, and how to prevent such use [1]. Besides deleting cookies and altering privacy settings, consumers might utilize technological measures to protect data privacy all well. For instance, consumers might utilise browser extensions as a privacy badger and generate a digital rights community the electronic frontier foundation, in order to block data tracking devices. Additional examples involve the usage of tracker blockers as ghostly, disconnect and ublock origin to block banner or pop-up ads and to depersonalise surfing sessions. Other utilities, as consent-o-matic could store consumer behaviour and automatic application of consent denial to visited novel sites. Ultimately, HTTPS everywhere is an extension that automates the rewriting request, establishes an SSL/TLS connection, and then directs the consumer to a secure variant of the site. The latter measurement is helpful within enabling encryption coverage for sensitive data desired for performing ecommerce or other online transactions [1].

4.2 Disadvantages of cookies for cybersecurity

Consumer feedback to the survey driven to several significant insights about data privacy and management. First, confidence levels among consumers are low overall, however differ by industry. Two industries, financial and healthcare services garnered the highest confidence scores as forty four percent. Notably, client interactions within these sectors involve the usage of individual and highly sensitive data. Other sectors had significantly lower levels of confidence. Solely approximately ten percent of consumer respondents indicated that they believe within consumer packaged goods corporations or media and entertainment corporations. Approximately two thirds of U.S. internet consumers indicated that it is critical that people merely they authorise view the contents of their email and that the names and identities of their email contacts remain confidential. Approximately half of consumer respondents that it is more likely to believe corporations that require solely information relevant to their products or to limit the amount of personal information requested. These markets are obviously singling to consumers that corporations are adopting a thoughtful approach to data governance [13].

Internet activity is monitored by internet service providers and might be hijacked as a consequence of surfing habits and site visits. Whilst consumers are vulnerable to attacks at the IPS stage, the websites visit might be traced by cookies as well, which are small sections of text stored and downloaded by the browser. Browser plugins might track the activity on multiple websites as well [7]. Cybercriminals prior contact YouTube creators through commercial emails posted upon their channels, asking for video advertising partnerships for a diverse of products. From VPN to online game. Within one instance, they pretended a news provider giving covid 19 news software. As the target agreed to the advertisement deal, the attacker sent them a malware landing site, normally posing as a legitimate site, as steam or luminary's game that consists an URL pretending as a software download. These were sent via email or a PDF on google docs or google drive. As the target operates the fake software. The cookies stealing malware is performed. This malware steals browser cookie from the victim's machine and uploads them to the attackers control server and command [14].

4.3 Advantages and disadvantages about cookies and cybersecurity

Corporations have been employing cookies, small text files placed on browsers, for years to track website monitor and visits consumer actions online. Cookies could deliver a rich data set that enables brands to better understand who their consumers are and enables them to address those consumers with more pertinent offerings. However, this personalisation comes at a cost. Consumers are increasingly interested in what corporations are doing with the data, who is collecting the data, how much their actions are tracked and who they might be selling the information to. As a matter of fact, a recent report discovered that seventy nine percent of Americans are worried about the way corporations utilise their data. Forty one percent of U.S. customers routinely delete cookies, and thirty percent have deployed ad blockers. This increasing mistrust has been increasingly echoed within government regulation. Among the most prominent pieces of legislation addressing cookies is the 2018 general data protection regulation, a significant broadening of data privacy mandates. Recently, regulators began demanding a comprehensive ban on ad targeting, both Virginia and California adopted sweeping privacy bills, and google chrome unveiled plans to cease support for third-party cookies completely by 2022. The era of the cookie is ending. That does not imply that companies ought to abandon personalisation, simply that now is a time for a new and better approach. What this has to do with the fact that cookies are being utilised to personalise the web experience, which might consist of tailor made advertisements. However, this tracing might possibly go too far and reveal itself as the distinctive identifiers appended to the cookie are utilised for various services and various marketing platforms. This practice is usually intrusive [7].

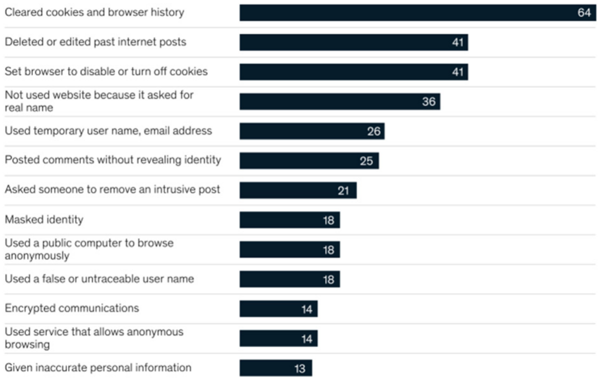

Figure 5 Survey of cookies action [4]

As Figure 5 illustrated that consumer concerns data collection and cybersecurity, however, few take adequate protective precautions. The data sample was collected from 792 participants [4].

5.CONCLUSION

With cookies, consumers are going to be able to retain the schedule of the moment the client visits his or her website. It enables the delivery of better individual content, more precise advertising and a better online purchasing experience as well. However, a significant range of effective actions have emerged for enterprises that are looking for approaches to tackle the enhanced consumer protection and data security requirements. These actions span the enterprise data lifecycle, including infrastructure and operations steps as well as consumer-facing practices.

The average website records twenty cookies. While cookies have an expiry date, this data might be significantly far within the future. However, at its most fundamental level, the consumers ought to be increase the aware of what cookies contain, what cookies are, how the data is used, and how to protect against the usage. Organizations ought to be aware of what data they actually require to serve consumers. Organizations have established management practices based on individuals and have defined security access levels for data categories. Risk could be mitigated by ensuring that solely those who need it have access to data sets and that no one has access to all available data. Therefore, additional activity monitoring might be necessary.

REFERENCES

[1] Paul, W. Cookies, privacy risks, attacks, and recommendations. (2020).
[2] Chris, J. M. Enhancing the security of cookies, university of London. (2001).
[3] Ashok, K.R.N. “Cookies privacy and cyber security.” International journal of creative research thoughts, Vol7. (2019).
[4] McKinsey. http://www.mckinsey.com. (2020).
[5] Peter, R.J. T., and Yang-lm L. Cyber security management. Henry ling limited. (2014).
[6] The federal reserve.Fraud types and authentication for remote payment use cases. (2021).
[7] Charlie, O. Cybersecurity, protect your privacy from hackers, spies, and the government. (2022).
[8] David, W. S., & Michael A. G. Applied social research methods series. Sage publications. (1993).
[9] Marc, S., Markus H., Adam L., and Jacod S. This is service design doing. O’Reilly. (2018).
[10] Emma, S. Using secondary data in educational and social research. McGraw Hill. (2008).
[11] E., Murphy, R, Dingwall, D., Greatbatch, and S., Parker. Qualitative research methods in health technology assessment: a review of the literature. (1998).
[12] Norman, B.Analysing quantitative data. Sage publication. (2004).
[13] Timothy, M. Customer data, designing for transparency and trust. Harvard business review. (2015).
[14] Lindsey, O. Google disrupts cookie theft malware attacks. (2021).