IJCSN - International Journal of Computer Science and Network, Volume 9, Issue 3, June 2020
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Security and Privacy Concern of Web Cookies, with User's Understanding and Management of their Web Cookie

[1] Shehu Mohammed Ahmed; [2] Song Shombot Emmanuel; [3]Avong Emmanuel John

[1] Department of Computer Science, Federal University Lafia
Lafia, Nasarawa State, Nigeria

[2] Department of Computer Science, Federal University Lafia
Lafia, Nasarawa State, Nigeria

[3] Department of Computer Science, Federal University Lafia
Lafia, Nasarawa State, Nigeria

Abstract - Cookies have come forth as one of the most proficient ways to keep track of browser-server interaction. However, security and privacy remains its major issues due to the level of progression. In this research, most common types of cookies in terms of security and the relevant privacy concerns have been identified and briefly analyzed. The research was carried out by means of systematic theory review to understand the research through previous studies. It involved a survey with the use of questionnaires to get users' understanding on web cookies and also use existing systems such as www.cookiepro.com and www.cookiechecker.com to gather information about cookies used by the websites. This was achieved by scanning through these websites when their URLs are provided. Findings of this research indicated that a lot of websites use cookies that keep track of its users without users knowing, a lot of websites that users visit daily use marketing cookies which constitute for about 50% of cookies found in websites, and are good examples of persistent cookies that are used to monitor users' behavior on the internet, which in turn leads to security and privacy issues.

Keywords – *Cookies, Security, Privacy*

1. Introduction

Researchers have considered cookies to be another means of simplifying a browser-server stateless interaction, in a stateless protocol (Rodica, *et al*, 2016). They are broadly used by different available service providers. A survey carried out by European Network and Information Security Agency (ENISA) in 2010, shows that approximately 80% of service providers gathered data through cookies. According to (David, 2001), Privacy has been a viral issue especially for third-party cookies which has received much attention. To improve tracking capabilities and request of the market, innovative techniques on new types of cookies have been deployed i.e. Flash and Super cookies (Soltani, *et al*, 2009).

Cookie is a small piece of file or text data, alternatively known as Hypertext Transfer Protocol (HTTP) cookie, which are propagated and improved by the server, stockpiled by the browser and transmitted between browser and server at each communication. HTTP cookie is produced when a user visits a website, and that website uses these cookies to keep track of the user's activities. Every time the user visits the website, the browser to send the cookie value to the server to notify the previous activity of the user, to server. Web cookies were developed in 1994 as a means of enabling the state of the clients and servers to be conserved. In 1997, the first standard for web cookies was published (Kristol, 2001).

Generally, cookie stores name, value, expiration date, valid domain name, valid cookie path, and security information for the cookie as the cookie information.

2. Purpose of Work

With the growing concerns among internet users regarding their Information privacy and the security of their activities as they surf the internet, it is imperative to assimilate that this confidential information is stored in a cookie and should be secured so that privacy integrity can be maintained. Due to continuous evolution in technology,

anxieties continues to escalate with users having little understanding and proper management of web cookies. Furthermore, this work identifies some security and privacy concerns, with a narrative that users understand all it takes to effectively manage web cookies. However, contrary to that preposition, users demonstratively lack adequate insight regarding the functional mechanics of website cookies hence, it is certainly not far-fetched to conclude that the security and privacy of cookies will continue to be misunderstood.

The submitted typeset scripts of each contribution must be in their final form and of good appearance because they will be printed directly. The document you are reading is written in the format that should be used in your paper.

This document is set in 10-point Times New Roman. If absolutely necessary, we suggest the use of condensed line spacing rather than smaller point sizes. Some technical formatting software print mathematical formulas in italic type, with subscripts and superscripts in a slightly smaller font size. This is acceptable.

2. Contribution to Knowledge

This study attempts to provide elaborate and comprehensive information for deployed cookies by several websites and online service providers by providing users with decent insight on the behavior of these cookies and ways to manage them. The privacy and security of data in a stored web cookie is of great importance as internet users seemingly do not feel protected browsing the internet. Regulatory agencies will find this study useful, in order to enhance on policies that enforce the explicit declaration of cookies on websites, as the case with the European Union.

3. Method of Achieving Objectives

For this work, *www.cookiepro.com* and *www.cookiechecker.com* will be utilized. The two websites function as tools that can be leveraged upon to examine commonly and regularly visited websites to uncover the presence of cookies, their categories, behaviors, and eventually analyze their effect on user's security and privacy.

Microsoft excel package will be used to present a pictorial representation and informative result of the analyses. Also, questionnaires will be used to collect users' opinion and response to security and privacy issues regarding their experience with browsing websites.

4. Literature Review

In as study conducted by Sowmyan 2008 on "Security, Privacy, and Usability; Cookies Invading Our Privacy for Marketing, Advertising and Security Issues", conveyed the idea that users should be made aware of the way their online activities are secured, how the information is used, the transparency levels to be maintained, the current state of operation of the cookie and online marketing techniques that is seen as a distress which provides a lot of insecurity to the users. The study asserts that it's purely a security breach for websites not to ask permission for the usage of cookies and setting them into the user's browser and the most important thing is no privacy statement is issued, regarding how the information is used for targeted marketing.

In a similar research by Joon and Ravi (2000) titled "Secure Cookies on the Web", employed role-based access control on the Web as a possible application for secure cookies. They used CGI scripts and Pretty Good Privacy to create and verify secure cookies cryptographically. They also used a role server that issues a set of secure cookies, including the user's authentication information (encrypted passwords or IP number), role, and the server's signature.

In 2018 Juha presented a methodical literature review on "Http Cookie Weaknesses, Attack Methods and Defense Mechanisms" to the department of computer science, University of Jyväskylä. His review stated that investigators in the IT field have highlighted some vulnerabilities and weak points in cookies, which in turn cause security and privacy issues. The research discussed several attack methods that exploit the weaknesses of cookies, and defense methods to mitigate these attacks.

Xiaofeng et al. (2015) In their research "Cookie lacks integrity; real world implication", presented a paper which targeted to fill the gap in cookie threats and security with an in-depth empirical assessment of cookie injection attacks. They found out that cookie-related vulnerabilities are present in important sites (such as Google and Bank of America), and can be made worse by the implementation weaknesses which they discovered in major web browsers (such as Chrome, Firefox, and Safari). Their successful attacks have included privacy violation, online victimization, financial loss and account hijacking.

Edward et al. (2015) studied the ability of a passive eavesdropper to leverage 3rd party HTTP tracking cookie for mass surveillance. They provided two instances of web pages which embed the same tracker and tag the browser with a unique cookie, the adversary can link visits to those

pages from the same user even if the user's IP address varies.

Rodica et al. (2013) published a paper on "Bittersweet cookie; some security and privacy considerations". in their work, they took into consideration the new types of cookies being deployed in the online environment; and assert that these new cookies do not have enough exposure to demonstrate how they are being used and, as such, their security and privacy implications are not easily quantifiable.

Edward and Michael (2009) studied similar work "Timing Attacks on Web Privacy". In this research, they pin-point a well-defined class of attacks that can compromise the privacy of users' web-browsing histories and that the attacks allow a malicious web site to decide whether or not the user has recently visited some other, unrelated web page.

4.1 History of Internet Web Cookie

The term "cookie" was invented by web browser programmer Lou Montulli. It was derived from the term "magic cookie", which is a packet of data a program receives and sends back unchanged, used by Unix programmers (Raymond and Eric, 2017).

At this time, introduction of cookies was not broadly known to the public. Cookies were accepted by default, and users were not alerted of their existence in any web sites. The general public learned about cookies after the Financial Times published an article about them (Jackson, 1996).

4.2 Categories of Internet Web Cookies

Internet web cookies, widely known as small text files that can be saved on a user's computer when visiting a website, effectively act as a memory of what has happened previously when a user's computer has interacted with a website. They can be broadly categorized as session based and expire after a session or persist beyond the current web session:

1. Session internet web cookies are used to 'keep state' and expire after a session, also allows websites to remember the actions of a user across a website during a particular session. For example, an online retailer may use session internet cookies to store information on items that have been added to the 'basket' ready to be purchased together with other items in a single transaction. Furthermore, it is known as an in-memory cookie which exists only in temporary memory while the user navigates the website (Microsoft Support, 2007). Web browsers normally delete session cookies when the user closes the browser (Microsoft Developer Network, 2012). Unlike other cookies, session cookies do not have an expiration date assigned to them, which is how the browser knows to treat them as session cookies.

2. Persistent internet web cookies are stored on end users' devices beyond the current session. They send information to the server whenever the user visits the site until the internet cookies' expiry date. These internet cookies allow websites to remember the actions of a user across a website (or a number of websites) and across sessions. For example, persistent internet cookies enable websites to remember settings for personalized content. Instead of expiring when the web browser is closed as session cookies do, a persistent cookie expires at a specific date or after a specific length of time. This means that, for the cookie's entire lifespan (which can be as long or as short as its creators want), its information will be transmitted to the server every time the user visits the website that it belongs to, or every time the user views a resource belonging to that website from another website (such as an advertisement). For this reason, persistent cookies are sometimes referred to as tracking cookies because they can be used by advertisers to record information about a user's web browsing habits over an extended period of time. However, they are also used for "legitimate" reasons such as keeping users logged into their accounts on websites, to avoid re-entering login credentials at every visit.

4.3 Uses of Internet Web Cookies

1. Cookies are use for Internet session management.
2. Cookies are use for personalization of dynamic and static websites.
3. They are also use by some for advertising campaigns.
4. Cookies are use by online store on items that have been added to the 'cart', ready to be purchased together with other items in one transaction.
5. They are use to track users' browsing habit.

5. Research Methodology

Identifying a research question is the initial stage of any systematic theory. In this research, the main aim is to analyze the security and privacy concerns with internet web cookies research, literature and online sources were examined. After defining the research questions, different web sites as shown in table 3.1 (based on types of websites) were scanned using two (2) renowned websites: www.cookiebot.com and www.cookiepro.com. These websites analyze other websites to determine if they are compliant to the European Union (EU) regulations on the use of cookies and online tracking, they follow the requirements in the General Data Protection Regulation (GDPR) and the ePrivacy Directives 2009/136/EC (ePR). The research work syndicates the basic research methodology of collecting and analyzing data, which include qualitative and quantitative approaches. Other statistical and analyzing package were also used to further analyze the result from the scan, obtained from the website analyzer, this package Microsoft Excel provides great tools for handling statistical computations and representation suitable for this research work.

Table 1: Categories of Websites

E-commerce	Entertainment	Portfolio	Media	Educational
Jumia.com	Nairaland.com	Fiverr.com	Vanguardngr.com	Researchgate.com
Konga.com	Naijaloaded.com	Github.com	Naij.com	Academia.com
Bet9ja.com	Youtube.com	Jobberman.com	Livescores.com	Googlescholar.com
Amazon.com	Facebook.com	Ngcareers.com	Goal.com	Acm.org
Ebay.com	Twitter.com	Pinterest.com	Yahoo.com	Grammarly.com
Godady.com	Imdb.com	Ijert.org	Aljazeera.com	Stackoverflow.com
Wordpress.com	Linkedin.com	Ieee.org	Wazobiafm.com	Udemy.com
Appiventor.mit.com	Tubidy.mobi	Olledo.ng	Instructable.com	Fulafia.edu.ng

6. Findings and Discussions

The use of cookies offers supportive information to the web service provider and improved browsing experience to the user. The challenging aspect with the use of cookies is that web service providers fail to openly seek user consent before they place cookies in users' devices and users do not pay much attention to the use of cookies by websites to keep track of their information and online movement. The findings from security concerns of web cookies are presented first. The findings from the privacy concerns of web cookies are presented next. Again, the results from questionnaires presented to respondents are presented.

Figure 1 shows how internet users understand the working of web cookies. This was gathered from the survey that was conducted, the result shows that 44% of respondents have heard of web cookies but do not understand how they work, 17% understood fully how cookies work, 14% had some understanding of how they work. This points out that a large number of internet users do not have an understanding of how cookies work.

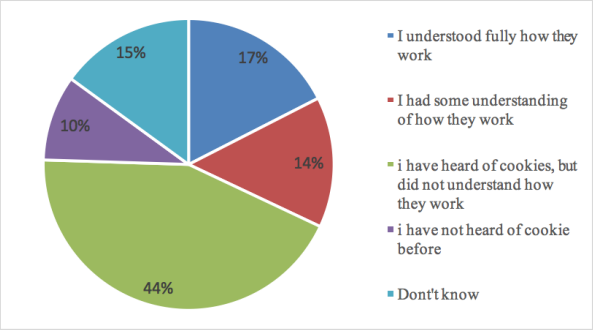


Fig 1 Understanding how cookies work (Question 5)

6.1 Internet Web Cookies Security Concerns

Joon, and Ravi, 2000 have identified three types of threat namely (network threats, end-system threats and cookie-harvesting threats). Network threats came due to the spreading of cookies in clear-text and can be modified

during the transfer. SSL (Secure Socket Layer) can be used to protect cookies while they are communicated over the network. End-system threat is associated with vulnerabilities, such as cookie information forgery and impersonation of other users.

This section presents several examples of attacks on cookies. Some of these attacks may expose cookies, while others exploit cookies' vulnerabilities to attack. Among them, are:

Cache sniffing: If the attacker accesses the browser or the proxy cache, the attacker could also obtain the cookie content.

XSS cookie sniffing: Cross-site scripting (also abbreviated as XSS) cookie sniffing occurs when a web application maliciously gathers data from a user. XSS attacks allow for account hijacking, changing of user settings, cookie theft/poisoning, or false advertising. The attacker can capture the cookie and extract data from it. In (Claude *et al*., 2010) a session hijack attack is presented. This type of attack is harmful, as it allows the attacker to collect private information and, at the same time, modify information such as search results. This attack is used as starting point for a more powerful one, which reconstructs users' search histories stored by Google through the exploitation of application-specific cookies. In the first stage, a session is hijacked by eavesdropping on the traffic.

The attack could be launched against any user connected via an unsecured channel. In the second phase, the search history is reconstructed using an inference attack (a technique used to disclose sensitive and protected information from presumably non-sensitive data) (Claude *et al*., 2010). The reconstruction of history is partial (not always all information is gathered from history) and precise (what is retrieved is correct). In this study, it is estimated that potential victims of such an attack are any users signed in and at the same time using other Google services (i.e. its search engine). The attack however, is general and highlights privacy concerns raised by mixed architectures using both secure and insecure connections. Typically, cookies do not have integrity checks and do not support authentication. Cookie poisoning tampers with the data stored in the cookie; the attributes of the cookie are altered before it is sent to the server (Pujolle *et al*., 2009).

Solutions to overcome such attacks are proposed in most of the papers identifying vulnerabilities. However, existing solutions do not address all the security requirements at the same time; confidentiality which protects against cookies' attributes being revealed to an unauthorized entity (i.e. during transfer or to another server), integrity protecting against unauthorized modification of cookie, and user authentication, so that the cookie owner could be authenticated.

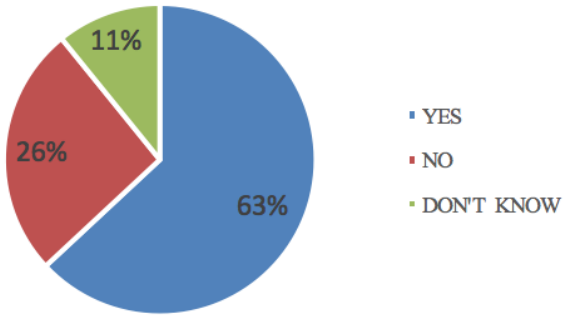


Fig 2 Internet Security Concerns (Question 2)

Fig 2. Shows that 63% of respondents are concerned about their security when they are on the Internet. 26% of the respondents show they not concerned about their security on the internet while 11% feel indifferent about it.

6.2 Internet Web Cookies Privacy Concerns

Web tracking has been considered as one of the source of information used for profiling for tracking users across different activities across different sites (Pujolle *et al*., 2009). Data collected during profiling includes pages viewed, time spent on each page and the sequence of sites visited. Cookies are sent only to the web sites that initiated them. However, a web page may contain links, web bugs, multimedia file (Shuo *et al*., 2009), HTML IFrame, JavaScript, or other components stored on servers in other domains.

Cookies that are set during access of the above mentioned components are termed as third-party cookies (Katherine, 2008) in contrast to first-party cookies. Some sites, such as those belonging to advertising companies use third-party cookies to track a user across multiple sites. However, third-party tracking alarms pose real serious privacy concerns.

This new type of cookie identifies a client even when standard cookies, Flash cookies, and others have been removed. This is accomplished by storing the cookie material in several types of storage mechanism that are available on the local browser.

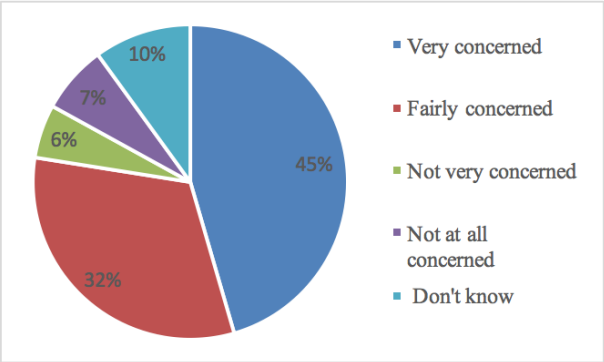


Fig 3 Privacy Concerns (Question 10)

6.3 Implementation of Cookies

Cookies inspire web server operators to separate designation from authorization. Hence, an agent might label a resource that can be supplied an authorization by a user agent. This may lead into situation where security control might be undertaken by a web server or the clients of the web server.

As a result of risks in data inputs, user input should never be trusted and should be validated in web services to ensure the user has by no means unravel the security and deficiency of the website. There are potential untrusted users in web service with data inputs as a threat. Even if the web server is equipped with HTTPS protocol, and the cookie is not set to "Secure" in its attribute, it exposes the ongoing requests to any unsecured channel that may intercept any out bounding requests of the user agent.

Table 2. Category and Number of Cookies for e-commerce Websites (Cookie-cecher.com)

Transmission of cookies over HTTPS provides greater protection to cookies when compared to transmitting cookies over insecure channel (HTTP). Cookies are transmitted in clear text when transmitted over insecure channel. Consequently, sensitive information such as the Cookie header, path may be predisposed to eavesdropping.

Table 2, 3, 4, 5, and 6 gives detailed list of cookie categories that are used by most popular websites, the tables are presented based on the categories of websites.

Table 2

	Necessary	Statistical	Preference	Marketing	Unclassified	Total
Appinventor.mit.edu	2	4	0	17	0	23
Ebay.com	2	1	2	5	12	22
Jumia.com.ng	8	7	0	28	14	57
Bet9ja.com	6	10	1	94	19	130
Godady.com	3	12	4	14	19	52
Wordpress.com	1	2	0	3	10	16
Konga.com	9	3	2	20	16	50
Amazon.com	13	7	3	17	11	51
Aliexpress.com	7	8	1	34	13	63
Jiji.com	5	11	5	31	17	69
Total	56	65	18	263	131	533

Table 2 shows the categories of cookies use by e-commerce websites; these types of websites are visited everyday with lots of these cookies placed on user devices, in most cases without the user's consent.

Users who browse these types of websites based on the scope of this research will on an average accept 53 different types of cookies.

Table 3. Category and number of cookies for entertainment website (Cookie-cecker.com)

	Necessary	Statistical	Preference	Marketing	Unclassified	Total
Naijaloaded.com	5	12	0	62	17	96
Nairaland.com	2	4	0	9	12	27
Facebook.com	2	0	0	0	0	2
Imdb.com	1	0	0	6	37	44
Linkedin.com	1	8	1	29	31	70
Youtube.com	1	2	0	3	10	16

Twitter.com	9	3	2	20	16	50
Tubidy.com	11	7	3	17	11	49
Fzmovies.net	7	8	1	19	15	50
Netnaija.com	4	11	5	31	9	60
Total	43	55	12	196	158	464

Table 3 shows the categories of cookies used by entertainment websites, which provide daily news of entertainment to its visitor. Users who browse such websites based on the scope of this research will on an average accept 47 different types of cookies.

Table 4 Category and number of cookies for portfolio websites (Cookie-cecker.com)

	Necessary	**Statistical**	**Preference**	**Marketing**	**Unclassified**	**Total**
Github.com	2	3	0	12	7	24
Ieee.org	14	11	0	11	7	43
Ijert.org	1	4	0	1	0	6
Olledo.ng	1	7	5	6	9	28
Fiverr.com	16	8	2	22	0	48
Jobberman.com	10	2	3	17	4	46
Ngcareers.com	9	3	1	19	9	41
Pinterest.com	3	0	0	4	0	9
Careerme.com	5	0	1	19	6	31
Stacklook.com	4	3	0	25	9	41
Total	65	41	12	136	51	317

Table 4 shows the category of cookies used by portfolio type of websites which allows users to have an account and upload their curriculum vitae and other necessary information about themselves. These types of websites are mostly dominated by freelancers, and users who browse such websites based on the scope of this research accept on an average 32 different types of cookies.

Table 5. Category and number of cookies for media websites (Cookie-checker.com)

	Necessary	**Statistical**	**Preference**	**Marketing**	**Unclassified**	**Total**
Vanguardngr.com	10	17	3	62	15	107
Wazobiafm.com	8	4	0	0	1	13
Aljazeera.com	11	14	0	72	19	116
Goal.com	3	12	1	20	36	72
Livescores.com	0	3	0	5	4	12
Instructable.com	0	0	0	0	0	0
Naij.com	8	3	2	18	12	43
Yahoo.com	11	7	5	31	8	62
Tvcnews.com	7	14	1	20	18	60
Channels.com	7	11	5	17	9	49
Total	65	92	17	245	122	534

Table 5. shows the categories of cookies used by media type of websites which provide daily news and happenings around and outside the region of its visitors, these types of websites receive great traffic daily, and users who browse these types of websites based on the scope of this research accept on an average 53 different types of cookies.

Table 6. Category and number of cookies educational websites (Cookie-checker.com)

	Necessary	Statistical	Preference	Marketing	Unclassified	Total
Academia.edu	5	7	0	110	15	137
Acm.org	1	4	0	26	6	37
Grammarly.com	2	8	2	17	68	97
Stackoverflow.com	1	4	2	25	6	38
Udemy.com	5	3	0	1	35	44
Fulafia.edu.ng	1	0	0	0	0	1
Cookie-checker.com	2	3	2	1	0	8
Researchgate.com	6	1	0	13	3	23
Googlescholar.com	7	2	1	10	7	27
Tutorialspoint.com	4	5	3	7	5	24
Total	34	37	12	210	145	436

Table 6 shows the categories of cookies used by educational type of websites which provide academic resources to its visitors and users, these types of websites is often visited by students, researcher, lecturer, scholars, editors. Users who browse these types of websites based on the scope of this research will on an average accept 44 different types of cookies.

Table 7. Category and number of cookies base on types of websites (Cookie-checker.com)

	E-commerce	Entertainment	Portfolio	Media	Educational	Total
Necessary	56	43	65	65	34	263
Statistical	65	55	41	92	37	290
Preference	18	12	12	17	12	71
Marketing	268	196	136	245	210	1055
Unclassified	131	158	51	122	145	607
Total	538	464	305	541	438	2286

Table 7 presents a broader view of the categories and numbers of cookies used by websites based on the type of website the fall under, it shows that marketing category of cookies has the highest number of use by websites; these cookies mainly constitute third party cookies which are used to monitor users browsing behavior across the internet. Furthermore, the information shows media and e-commerce types of websites use a lot of cookies on their websites, and this happen to be the most visited types of websites on the internet.

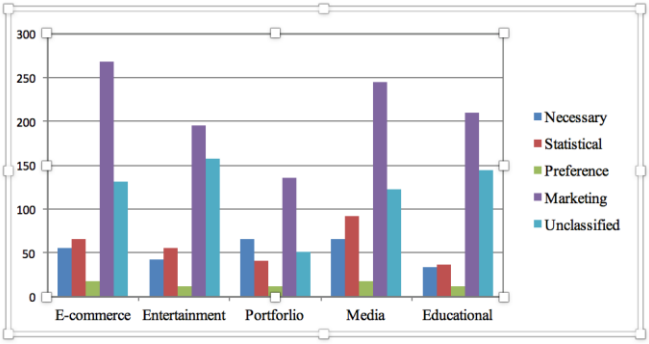


Fig 4 Categories and number of cookies based on types of websites

Figure 4 show a more graphical representation of the various categories of cookies used by several websites, classified based on the different types of websites. They use of marketing cookies by websites indicate the presence of persistent cookies which are used to track they activities of users. This in turn, will lead to interference with users' security and privacy.

Preference cookies enable a website to remember information that changes the way the website behaves or

looks, like your preferred language or the region that you are in.

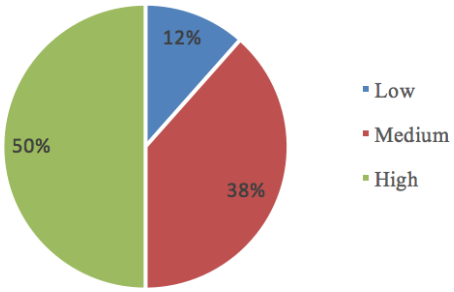
Statistic cookies help website owners to understand how visitors interact with websites by collecting and reporting information anonymously.

Marketing cookies are used to track visitors across websites. The intention is to display ads that are relevant

and engaging for the individual user and thereby more valuable for publishers and third party advertisers.

Unclassified cookies are cookies that the web analyzer could not classify, together with the providers of the individual cookies.

Findings from this report shows that, a lot of websites that users visit daily uses marketing cookies which constitute for about 50% of cookies found in websites, and are good examples of persistent cookies, that are used to monitor user behavior on the internet, which in turn lead to privacy issues. The use of these third party cookies on these websites increases the chances of privacy risk, as shown in figure 4.5 below, 50% of the websites users visit daily have high privacy risk and only 12% have low privacy risk



.

Fig 5 Percentage risk status (www.kiosk.cookiepro.com report)

6.4 Cookie Disclaimer Alert

The purpose of the cookie disclaimer is to provide clear and understandable information regarding cookie been use to user. However, as evidenced from responses in this study, users often click the disclaimer away without paying attention, or ignore it. Some claim not to understand what the disclaimer is saying, they are suspicious due to perceived lack of transparency (e.g. not being able to tell how the collected data will be used by the service provider), are not aware of possible privacy related consequences of cookie use or have other misconceptions regarding what the collection of cookies means to them. Hence, the disclaimer often fails its purpose of informing the users. Moreover, prescribing an opt-in solution might not alleviate the issue. As long as users do not read the disclaimer and try to click it, it is possible that in trying to get rid of the disclaimer they click on the "agree" button, without realizing the consequences for their privacy. As such, additional measures for educating the user might be necessary.

Fig 6 Cookie disclaimer as seen on cookielaw.org

This study did not reveal any significant effects of the disclaimers' text on users' behavior. Still, as evidenced from prior responses, the perceived differences between the disclaimers are not critical enough to change the users' decision to stay or leave the website. On the other hand, a commonly named factor in users' decisions is the characteristic of the website itself. As such, many users claimed that they would be more likely to allow the use of cookies on websites they considered trustworthy or were familiar with, as well as on websites with contents or services important to them.

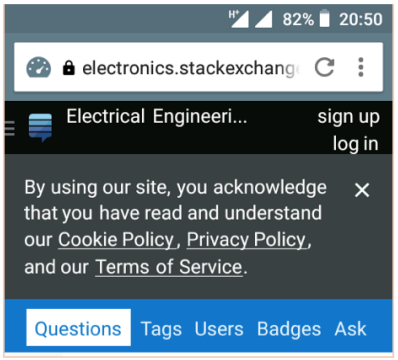


Fig 7 Cookie disclaimer as seen on electronics.exchange.com

This finding suggests that trustworthy websites can include more information in the cookie disclaimer, such as including use of cookies by third parties that would normally put users off, without users leaving the website. The trade-off to the user between the trustworthiness of the website and potentially privacy-infringing practices of cookie use as indicated in the disclaimer is yet to be studied.

7. Conclusion

This project has investigated and presented in brief, some of the common types of cookies used on the Internet or websites. During the inception of first cookies design and implementation, it was aimed to provide efficient state management in the interactions of user's web browsers and web servers; before subsequently extended for other purposes, such as user activities tracking, profiling advertising, profiling, etc. This project analyzed security and privacy concerns generated by the use of cookies. Users must be able to find out how a web site plans to use the information from the cookie and should be able to choose whether or not those policies are acceptable. Both the user browser and the origin server must assist in gaining informed consent. For a user with limited IT expertise there is not enough information available to explain cookies' management

Based on this research work, the importance of cookies cannot be over emphasized. nevertheless, as they continue to evolve, issues regarding them will continue to rise thus, these recommendations are to individuals and organizations:

User should be able to control how they are being tracked on a day to day routine on different sites through the help of sophisticated applications accessible to all internet users. The storage of these cookies outside browser control should be controlled and limited.

Websites that provides information on digital advertising should device more optimal means with better understanding rather than something that custom monitoring of their internet browsing privacy such as cookies.

References

[1] Claude Castelluccia, Emiliano De Cristofaro, Daniele Perito (2010). Private Information Disclosure from Web Searches (or how to reconstruct users' search histories), inProceedings of the 2010 Privacy Enhancing Technologies Symposium (PETS), LNCS 6205, pp. 38-55.

[2] David Kristol (2001). HTTP Cookies: Standards, privacy, and politics, ACM Transactions on Internet Technology, 1(2), pp.151–198, http://www.cs.stevens.edu/~nicolosi/classes/sp10 cspriv/ref5-1.pdf

[3] Edward W. Felton, Peter Zimmerman, Christian Eubank, Steven Englehardt (2015). Cookies that give you away: the surveillance implication of web tracking. Florence, In Proceedings of the 24th International Conference on World Wide Web. International World Wide Web Conferences Steering Committee. Italy. ACM 978-1-4503-3469.

[4] Joon S. Park and Ravi Sandhu (2000). "Secure Cookies on the Web". George Mason University. IEEE Internet Computing. http://computer.org/internet/ 1089-7801/000.

[5] Raymond Eric (ed.) (2017). "Magic cookie". The Jargon File (version 4.4.7).

[6] Rodica Tirtea, Claude Castelluccia, and Demosthenes Ikonomou (2013). "Bittersweet cookie; some security and privacy considerations". European Network and Information Security Agency http://www.enisa.europa.eu/.

[7] Soltani Ashkan, Canty Shannon, Mayo Quentin, Thomas Lauren, and Jay Hoofnagle Chris (2009). Flash cookies and privacy, Technical report, University of California, Berkeley, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862

[8] Xiaofeng Zheng, Jian Jiang, Jinjin Liang, Haixin Duan, Shuo Chen, Tao Wan, and Nicholas Weaver (2015). "Cookies lack integrity: real world implication". Institute for NetworkScience and Cyberspace, Tsinghua University, Department of Computer Science and Technology, Tsinghua University, Tsinghua National Laboratory for Information Science and Technology, International Computer Science Institute, Microsoft Research Redmond, Huawei Canada,UC Berkeley.

Shehu Mohammed Ahmed is a graduate from Federal University of Technology Minna with bachelor's of Technology in Mathematics and Computer Science 2010 and Master's of Technology in Mathematics 2016. He is currently working as Lecturer in Department of Computer Science Federal University of Lafia. The Authors current research area is Algorithms and Computational mathematics.

Song Shombot Emmanuel graduated from the University of East London with a Bachelor's degree in Software Engineering in 2012 and a Master's degree in Information Security and Digital Forensics in 2017. He is currently working as a Lecturer in Federal University Lafia, Nigeria. S.S. Emmanuel has been a constant recipient of the Dean's list award of academic excellence in 4 consecutive semesters during his Undergraduate years and also won the Tertiary Education Trust Fund Award (TETFUND in 2016. The author's current research interest is IoT and Big Data Analytics.

Avong Emmanuel John is an outstanding student who graduated from the department of Computer Science in Federal University Lafia in 2019. His current research area is web development technologies.