Kausar *et al. (IJECI)* 2023

(IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0704167

Research Article

Vol. 7 issue 4 Oct-Dec 2023

Cookie Hijacking: Privacy Risk

Kausar Parveen and Noor Fatima

Department of Computer Sciences, University of Engineering and Technology, Lahore

Corresponding author: kausarnawaz6@gmail.com

Received: September 29, 2023; **Accepted:** November 27, 2023; **Published:** December 22, 2023

ABSTRACT

Users may accept more cookies than they require because of suspicious behavior in cookie claimers. And, like, more than they even know. So, as we were measuring real behavior, we were also assessing each of these components' effectiveness, correct? Learning about user opinions of those cookie disclaimers and their entire process of deciding which cookies to accept or, like, reject, bro, was very fascinating. So, guess what? We have conclusively shown that the various images associated with the accept/reject option significantly influence the judgments made by consumers. You won't believe it, but we also discovered that assigning a label to the rejected option has a really big impact. Furthermore, we have confirmed previous studies showing that, well, biased content doesn't actually have a significant impact on customers' judgments. To sum up, black patterns in cookie disclaimers are really important. Users are forced to accept more cookies than they really need, and decision-making is greatly influenced by images and labels. Getting folks to accept those cookies is the main goal. According to our research on user attitudes about cookie disclosures, the presence of the disclaimer only slightly affects the way that various user types make decisions. We provide advice on how to improve. Conditions that apply to different user groups.

Keywords: Cookie utilization, Regulations, Types, literacy of cookies, cyber security, Cookie Notice Analysis.

1. INTRODUCTION

Because the data they contain is always the same, cookies by themselves don't present a concern. They could not infect a computer with a virus or any other malicious programmed. Conversely, if cookies are stolen, certain network attackers could be able to gain access to the browsing session. A significant portion of the internet population uses cookies, making them a pertinent and vital piece of technology. Many individuals in the globe nowadays. Cookies can be used to implement the functionality and history of cookies, but they are not designed to be secure. The accuracy, security, or dependability of the information is not guaranteed. When the security of the transport layer is not enough to prevent online browsing, security load limits cookies to a secure route. The http only feature of the cookie can also help prevent attackers from perfecting their transmission requirements to secure websites. Hackers breached systems and networks to obtain comprehensive and confidential messages [1].

1.1. Cookie utilization

For several features of web browsing, cookies are required. They facilitate website navigation, login, product addition to a shopping cart, and persistent sign-in for the user agent. The language and style preferences of the user can be saved on the website. As of 2023, Cookiepedia. The way people navigate a website can be tracked thanks to cookies. "Web analytics" is the term used within the area to describe this type of tracking. The web host can use it to enhance the website by finding out about and highlighting the most common methods that users navigate it. Additionally, this allows the website to provide the customer more material, product recommendations, and, well, tailored adverts. Even though this tracking is anonymous and doesn't require sensitive information, it is nonetheless considered private information according to EU data protection laws. Bolinger [2] They definitely offer users better support and a more pleasurable browsing experience in this way. There are other parties besides website hosts or users who may benefit from similar uses of cookies. User profiling and targeted advertising are two uses for cookies. Multiple uses, such as online advertising and espionage, may benefit from web user tracking or profiling. The internet and other websites can be used by third parties to track users. Parties or other similar cookie setups [3].

1.2. Cookie regulations

Official legislation has addressed cookies because of privacy, surveillance, and profiling concerns. The majority of online operations are funded by advertising . The practise of advertising online is super-duper common, and like, super quick growing industry and stuff, like seriously, it's worth like, a lot of money, estimated to be around 227 billion US dollars in the year 2018. It was stated that over 600 billion USD had been spent total on digital advertisements. by a Statista study conducted in 2021. A rise in digital advertising is expected. Notably, expected exceed USD 870 billion by 2026 [4].

1.3. Types of cookies

1.3.1. Session cookies

Session cookies are those that are briefly stored in the memory of the browser. Upon closing the browser, the cookies will be removed. Even if the user leaves the page momentarily, they will still be in the same surfing period! They can save things like login passwords and that kind of thing. In that instance, the user can't just browse the website without having to log back in between sessions and other things! And, they have to repeatedly log in because they can't remember their login information forever and other things [3].

1.3.2. President cookies

Persistent cookies have a tendency to remain on a user's device or browser after the user ends their browsing session. The server establishes cookies that are persistent and have a defined expiration date. Users can delete the cookie prior to its expiration. By supplying cookies with an expired date that are erased upon the client's request, websites have the option to remove cookies from users' browsers. Servers are able to change persistent cookies and change when they expire [3].

1.3.3. First party cookies

First-party cookies are similar to those made by the website the user is visiting or has visited before. They are absolutely necessary for using a certain website's browsing features. And a first-party cookie's domain name and host property are exactly the same. And if you can set and get those cookies, you know, you don't have to log in every time you surf [5].

1.3.4. Third party cookies

Websites other than the one the user is now on are setting third-party cookies, and they are coming from a different domain than what is seen in the address bar of the browser. Since third-party cookies allow advertisers to track visitors across numerous irrelevant websites, advertising is the most popular use case for them. In reality, websites other than the one the user is currently using that is, websites with a domain other than the one seen in the browser's address bar are the ones that set third-party cookies. Third-party cookies are most frequently used in advertising! It makes it possible for advertisers to follow consumers across numerous irrelevant websites [3].

1.3.5. DNS Hijacking

An essential part of the internet infrastructure that enables websites to be identified by their domain names and other attributes rather than their IP addresses is the Domain Name System (DNS). An attacker may be able to steal cookies and personal information through an exploit called DNS hijacking. DNS hijacking involves the compromising of the victim's DNS queries. The DNS queries may end up being answered by a hacked DNS server or one controlled by an attacker. For example, the attacker could employ malware that is placed on the device, infect a nameserver, access the user's router settings and change them. Because of its many guises and methods, it is difficult to defend against [6].

2. LITERATURE REVIEW

2.1. Literacy of cookies

2.1.1. Cookies are not malware however it does brought risks

Cookies don't always represent a risk. They are only text files that assist in coordinating the browser and the remote webserver so that the entire feature set of the website can be accessed. In the midst lie lurking automata and verification. Logging in oh so delightfully allows you to access shopping cart features, preference settings, and some very fancy third-party add-on services. In order to allow users to visit restricted pages without constantly thinking about verifying themselves, cookies are employed to store authentication information. You know, usernames and passwords. Therefore, it is imperative to guarantee the secrecy and integrity of cookies, without a doubt. Alternatively, the user might be anyone with access to the cookies. Even so, the fact that when a server-specific form is filled out, credential data stored in cookies is frequently displayed, where the Even if the contents are hidden from the viewer, an attacker might still be able to replicate the intercepted cookie and assume the identity of the user. The safety of customers may also be jeopardised by implementation problems, particularly when they include web browsers. Internet Explorer versions five and four for Windows 98, 95, 2000, and NT expose a vulnerability allowing websites to view cookies used by other websites, as web browsers hide webpages behind lengthy URLs [7].

2.1.2. Fundamental Types of Cookies

Every action a new user takes on the website is viewed as a fresh business. Online shopping is an excellent example of how session cookies are put to use because they make an item easier to find. When a user checks in again, these cookies will take note of the modifications they made to the website. Similar to these cookies, computers operate by storing all of their settings, such as language selections and bookmarks, on each login. Usually, these incredibly tasty cookies aren't kept on an extremely sophisticated hard drive. And they are stored for an extremely long time forever and beyond. The third group of these incredible treats are, third-party cookies. Another name for them is tracking cookies. They gather data regarding a person's internet activity. Every time a user visits a website, a variety of information about their activities is gathered and sent to the website that set these cookies. Advertising is thus purchasing the gathered data. An individual's preferences, interests, and trends are monitored in this way. Hence, marketers may send a customised advertisement based on the information these cookies gathered. In many ways, nevertheless, this is seen as a faith in the user's online privacy [8].

2.2. Literacy of cyber security

2.2.1. Corporation situation for cyber security

Digital businesses face significant cybersecurity challenges. Companies must adapt security, fraud prevention, and product development teams to design secure, convenient experiences. They must also recognize risks associated with large data sets containing sensitive consumer information. Analytical solutions, which may not have followed conventional software development processes, must also include security safeguards. Companies that use robotic process automation need to make sure that cases with unusual or unexpected components, input cases, and border instances managed and that robotic credentials don't go beyond accepted bounds and endanger public safety. In addition to learning how to enforce and set acceptable developer access rules, companies that create application programming interfaces for external customers also need to learn how to detect vulnerabilities produced by the interaction of different APIs and services. When transitioning from waterfall application design to agile application construction, they need to maintain their tight application security policies. Businesses hoping to increase their digital consumer contacts, for instance, must figure out how to modify the teams in charge of product development, security, and fraud protection so they can build controls and provide experiences that are. Absolutely safe and convenient with authentication! Businesses that use a lot of data analytics must learn how to identify the hazards. Analytical solutions, which may not have followed conventional software development processes, must also include security safeguards. Companies that use robotic process automation need to make sure that cases with unusual or unexpected components, input cases, and border instances are appropriately managed and that robotic credentials don't go beyond accepted bounds and endanger public safety. In addition to learning how to enforce and set acceptable developer access rules, companies that create application programming interfaces for external customers also need to learn how to detect vulnerabilities produced by the interaction of different APIs and services. When transitioning from waterfall application design to agile application construction, they need to maintain their tight application security policies [9].

2.2.2. Data management for cyber security

Data governance is the foundation of privacy. It is helpful to first describe the many forms of data before examining how each one relates to people's security and privacy, as the term "data" is ambiguous and can apply to a vast range of information. It might as well become a gold mine for dishonest advertisers if the information falls into the wrong hands. Internet service providers monitor the websites and browsing habits of their customers and have the ability to take control of them. Cookies are text segments that are downloaded and retained by the web browser, and even while consumers cannot avoid attacks at the level of internet service providers, they may still be able to track websites they visit. Furthermore, browser plug-ins have the ability to track activity on multiple websites [10].

2.3. Cyber security in data management of finance sector concerns

In a calculated attack, fraudsters are calling phone service providers pretending to be consumers by employing sociological engineering techniques. This is the process they use to transfer a phone number, even if it's only temporarily, and keep it in their control long enough to obtain the two-factor authentication associated with it and gain access to the intended account, bank, cryptocurrency wallet, or email. As the phone bug gets unmanageable, there is a chance that any internet accounts connected to this number could be penetrated, which means that the two-factor authorization code could be stolen. In a calculated attack, fraudsters are calling phone service providers pretending to be consumers by employing sociological engineering techniques. This is the process they use to transfer a phone number, even if it's only temporarily, and keep it in their control long enough to obtain the two-factor authentication associated with it and gain access to the intended account, bank, cryptocurrency wallet, or email. As the phone bug gets unmanageable, there is a chance that any internet accounts connected to this number could be penetrated, which means that the two-factor authorization code could be stolen [11].

2.3.1.. Cyber security in data management of medical sector concern

Another recent addition to the market is hospitals. For family DNA services, which preserve genetic information about their clients to be offered in the event of a sought-after medical inquiry or to trace family history, they are currently transitioning to electronic records. If a person's medical records are lost, it could cause them a lot of grief and have tragic consequences. The choice to distribute DNA information is private, with the exception of those who share it first law enforcement officers and often people working in ancestral services. A decrease in sales of several popular family ancestry kits was ascribed to privacy issues related to DNA searches [9].

2.4. Developing security best practices for cookies

To prevent cookie hijacking, a lot of research have been carried out. RPS checks implemented session ID, IP address, OTC, and browser fingerprint. According to Lee et al. [12], a secure and efficient three-stage cookie protection technique is as follows: cryptographic key generation, cookie issuing, and login.

able 1: Websites that recognize errors found with Newton

Site	**Fixed**	**Notes**
Yahoo	Incorrect	Attackers can still access a user's search history, notes, and stock listings even if they only use Yahoo over HTTPS. Yahoo informed us that they will not be fixing this issue at this time due to the intricacy of the code.
Vimeo	Correct	Even if a user only ever uses HTTPS to access Vimeo, his whole account could still be compromised. We alerted Vimeo, and they fixed it.
Magento (250K sites)	?	If a patch is being developed, it was not made clear by the Magento developers.
WooCommerce (650K sites)	Incorrect	WooCommerce developers blamed the vulnerability on the underlying WordPress framework.
BigCommerce (50K sites)	Correct	We applaud the BigCommerce developers for their quick verification process and for releasing a fixed version into production.
Amazon	In progress	A session hijacking attack may be caused by a cross-site scripting attack. An attacker has total access to the user's account. In response, Amazon stated that they are aware of the issue and are developing a solution.

2.4.1. HTTP cookie

A user's web browser receives an HTTP cookie, which is generated by a server and functions something like a small message. To maintain the session's direction and to confirm that both requests are coming from the same browser. These cookies are used for session management (because sessions need to be managed), customization, and tracking. They are returned in answers and other formats as HTTP headers!

Set – Cookie:<name for cookie >=<value for cookie >

Other characteristics that the server may set include expiration, which indicates how long the cookies are valid, and Http Just Bag, which indicates whether the cookie was sent over a secure channel [9].

Table 2: HTTP queries to the domain we have identified as being at risk

Protocol	Connections	Requests	Vulnerable Requests	Exposed Account
HTTP	685,500,365	1,398,044,178	29.908,099	282,459
HTTPS	772,562,024	-	-	-

2.4.2. Cookie notice studies

Cookie alerts are used by websites, you know, to ask for users' permission and, most of the time, to provide them control over these cookies. Consent Management Platforms (CMPs) provide APIs for handling cookie notices, which helps websites comply with, uh, rules. These platforms are third-party interfaces that offer user permission and convenient data storage options, among other things. The rate at which various CMPs are being implemented listen, by 2020 was, like, restricted to the top 10% of websites, many of which, elect to use customized versions of the cookie notice [8].

2.4.3. Cookie notice analysis

2,000 websites inside the European Union were manually inspected in order to determine the scope of cookie-based tracking. It was discovered that there were cookie notices on 57% of them. Using a list of popular CSS selectors were able to recognize cookie notifications on 17,000 websites in Greece and the UK! They noticed that 45 percent of these offer a cookie notice. Based on their study of the notices to determine compliance, very few of them provide a straightforward opt-out choice. To ascertain how user location impacted cookie notice visibility [11].

Table 3: Specifics of the websites that were examined. The percentage is computed using the total number of websites with a cookie notice (45, 044) after the first row.

Type	% websites	Avg, #settings (per site)	One click opt- out (% websites)
No notice	47.3	-	-
Single view	64.6	2.17 (3.01)	11.5
Multiple views	35.4	28.7 (103)	9.96

Thus, it can be said that a good deal of frameworks had security flaws brought on by a variety of circumstances. It is concerning to note that these problems have been discovered in 37 out of the 44 frameworks that were evaluated. Despite its stated purpose as a security precaution, the synchronizer token pattern has been linked to implementation errors. These errors, which result from combining various libraries, could make it easier for attackers from the same website to get around security protections. Moreover, the CORF token fixation attack is one particular instance of this type of attack. The Flask framework, which was thought to be secure until this specific attack, is now vulnerable. The CORF token fixation attack's security breach emphasizes how critical it is to find and solve these framework flaws. Priority one when developing useful privacy instruments for decision support is usually accorded to understanding users' mental models [8].

3. METHODOLOGY

3.1. Secondary data collection

Secondary data was utilised by basic researchers as a starting point for further investigation. On the other hand, applied researchers are more focused on using the body of knowledge at least in a few different forms to solve specific issues. Secondary data is a prerequisite for good practise. Secondary research aids in determining the direction of Lead to additional primary investigations by highlighting issues with the previous findings. Secondary data provides the measuring tools, relevant interview participants, and instruments for doing primary research into the issues that need to be addressed [12].

The intended goal of the collection of secondary data may have given rise to additional concerns. It's possible that some metrics, classifications, or therapy effects aren't the best fit for the current situation. Definition of secondary data as outdated data. This means that for some uses, this information may not be very current.

4. RESULTS

4.1. Address based authentication

Addresses serve as the basis for authentications. You must possess the IP address of that user. That's when IP Cookie, comes into play. In order to facilitate authentication, it aids in retrieving the IP address. The fact is that an environment is associated with an IP address. Variables for Web users that make it incredibly simple for a Web server (cookie issuer) to obtain the user's IP address and add it to the IP Cookie. When Alice, the user, tries to get in touch with a Web server that accepts the IP Cookie, the server, say, first makes sure that Alice's current IP address matches the IP Cookie that she submitted. If they seem exactly the same, the server believes Alice to be the real owner. Address-based authentication is a very convenient authentication method, even though the authentication process is completely transparent to consumers. But, it's not always the greatest choice [13].

4.2. Password-based authentication

Password-based authentication is supported d by dynamic IP addresses, proxy servers, and prevents IP spoofing. It is essential to make sure that credentials are sent securely when they are transferred from the browser to the Web server across the network. SSL (Secure Sockets Layer) is used in this situation. Through the use of the SSL protocol, secure network communication is possible. However, servers can also validate the cookie owner in another method. Passwords that are encrypted and kept in the Pswd Cookie can also be used by them. Upon receiving Alice's login credentials, the Web server hashes the passwords to increase their security and other features. The Pswd Cookie then stores these hashed passwords. Thus, Alice just needs to enter her previous passwords each time she wants to log in to a server that accepts the cookie. In the event that the password hash matches the one in Pswd Cookie, the server will identify Alice as the cookie's legitimate owner [13].

4.3. Digital signature based authentication

The idea of digital signature-based authentication advances in this new and advanced technological era. If web servers know users' public keys, they can use digital signature technologies like DSA7 or RSA8. Through the intriguing notion of cookies, it is possible to positively and definitively confirm a user's identity. Thus, users can enjoy the nice benefit of setting up a cookie with a signed time stamp, which removes the requirement for bulky, inconvenient add-on browser software. For example, we discover that, startlingly and enlighteningly, secure cookies are amazingly compatible with various authentication methods like as Kerberos and Radius9.10, when the endearing Alice, bless her heart, has to connect to a faraway Web server that knows Alice's public key. The information about Alice's authentication procedure can be used in conjunction with their authentication methodology, even though it is dependent on a number of variables. These crucial facts can be protected because of a group of secure cookies. Secure cookies are the foundation of our client-to-server authentication strategy. The best part is that SSL can even be used in situations when server-to-client authentication is required [14].

4.4. Maintaining Integrity

Integrity issues also affect cookies. An attacker may, for example, duplicate Alice's IP Cookie and alter it. Using an IP address, then afterwards pose as Alice in front of a Web server. Alice has the ability to modify the contents of her own cookies. The Life Cookie's Cookie Value field allows the Web server to verify the lifetime (expiration date) of the secure-cookie established. Integrity of the lifetime of the secure-cookie set, provided that the cookies are legitimate. Despite the fact that the browser only transmits to the Web server the pertinent Cookie Name and Cookie Value fields in order to verify the integrity of other fields, the Web servers inside the domain can set up a policy with the cookie-issuing server. For instance, the Web server utilises the values that the policy presets for the Domain, Flag, Path, and Secure fields acme.com, True, /, and False, respectively to verify the integrity of the cookies [13].

4.5. Implementation

For user identification, session management, and preference tracking, cookies are widely utilized. Cookies are saved and then given back to the server with each request, enabling it to identify and, for example, personalize the user experience. When employing cookies, security needs to be taken into account. It is recommended that developers utilize secure and HTTP-only settings to safeguard confidential information and prevent malicious attacks like cross-site scripting (XSS). Increased surveillance has resulted from privacy concerns, and laws like the GDPR mandate that websites get user consent before storing certain kinds of cookies and other data [14].

Table 5: Browser and their Connect over HTTP

Browser	**Connect over HTTP**
Desktop	
Chrome (v.45)	Correct
Firefox (v.41)	Correct
Safari (v.8.0)	Correct
Internet Explorer (v.11)	Correct
Opera (v.32)	Correct
Mobile	
Safari (IOS 9)	Correct
Chrome (v.46, Android 5.1.1)	Incorrect (conditionally)

5. CONCLUSION

Cookies allow customers to save the schedule as soon as they visit the page. Giving more personalised content, more focused advertising, and a better online shopping experience are all made possible by it. However, companies looking for ways to deal with the stricter rules on data security and consumer protection now have access to a wide range of workable solutions. From consumer-facing processes to operations and infrastructure phases, these activities encompass every phase of the company data lifecycle. Usually, a website records twenty cookies. Cookies do have an expiration date, but in the near future, there might be much more. Nevertheless, people need to understand cookies better on a fundamental level.

REFERENCES

[1] K. Renaud and L. A. Shepherd, ‘‘How to Make Privacy Policies both GDPR-Compliant and Usable’’, in 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), IEEE, pp. 1-8, 2018.

[2] I. Sanchez-Rola, M. DellAmico, D. Balzarotti, P. A. Vervier, and L. Bilge, ‘‘Journey to the Center of the Cookie Ecosystem: Unraveling Actors’ Roles

and Relationships'', in 2021 IEEE Symposium on Security and Privacy (SP), IEEE, pp. 1990-2004. 2021.

[3] C. Matte, N. Bielova, and C. Santos, ''Do Cookie Banners Respect my Choice: Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework'', in 2020 IEEE Symposium on Security and Privacy (SP), IEEE, pp. 791-809. 2020.

[4] G. Kampanos and S. F. Shahandashti, ''Accept All: The Landscape of Cookie Banners in Greece and the UK'', pp. 213-227. 2021.

[5] M. Hils, D. W. Woods, and R. Böhme, ''Measuring the Emergence of Consent Management on the Web'', in Proceedings of the ACM Internet Measurement Conference, New York, NY, USA: ACM, pp. 317-332. 2020.

[6] J. A. Alharbi, A. S. Albesher, and H. A. Wahsheh, ''An Empirical Analysis of E-Governments' Cookie Interfaces in 50 Countries'', Sustainability, vol. 15, no. 2, pp. 1231-1237, 2023.

[7] C. J. Hoofnagle, B. van der Sloot, and F. Z. Borgesius, ''The European Union general data protection regulation: what it is and what it means'', Information & Communications Technology Law, vol. 28, no. 1, pp. 65-98, 2019.

[8] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, ''(Un)informed Consent'', in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA: ACM, pp. 973-990. 2019.

[9] E. Ma and E. Birrell, ''Prospective Consent: The Effect of Framing on Cookie Consent Decisions'', in CHI Conference on Human Factors in Computing Systems Extended Abstracts, New York, NY, USA: ACM, pp. 1-6. 2022.

[10] B. M. DiCosola III and G. Neff, ''Nudging Behavior Change: Using In-Group and Out-Group Social Comparisons to Encourage Healthier Choices'', in CHI Conference on Human Factors in Computing Systems, New York, NY, USA: ACM, pp. 1-14, 2022.

[11] K. Bergram, M. Djokovic, V. Bezençon, and A. Holzer, ''The Digital Landscape of Nudging: A Systematic Literature Review of Empirical Research on Digital Nudges'', in CHI Conference on Human Factors in Computing Systems, New York, NY, USA: ACM, pp. 1-16, 2022.

[12] R. Houser, S. Hao, Z. Li, D. Liu, C. Cotton, and H. Wang, ''A Comprehensive Measurement-based Investigation of DNS Hijacking'', in 2021 40th International Symposium on Reliable Distributed Systems (SRDS), IEEE, pp.

210-221, 2021.

[13] Q. Chen, P. Ilia, M. Polychronakis, and A. Kapravelos, ‘‘Cookie Swap Party: Abusing First-Party Cookies for Web Tracking’’, in Proceedings of the Web Conference 2021, New York, NY, USA: ACM, pp. 2117-2129. 2021.

[14] X. Hu and N. Sastry, ‘‘Characterising Third Party Cookie Usage in the EU after GDPR’’, in Proceedings of the 10th ACM Conference on Web Science, New York, NY, USA: ACM, pp. 137-141. 2019.