COOKIE MONSTER: THE SECURITY AND RISKS OF ONLINE COOKIES

Dustin Edgerton - Mentors: Dr. Clemente Izurieta, Yvette Hastings

Introduction

Cookies are blocks of data stored on a user's web server which contain personal information, such as a user's passwords and credit card information. This sensitive data opens the window for cyber threats to those using the internet.

Objective

The objective of this research project is to identify the threats that online user's face due to cookies. By examining cookie security vulnerabilities, encryption methods, and the possibility of attack, this research aims to enhance our understanding of current cookie security practices and to inform users of mitigation measures to protect privacy.

Methods

A literature review was conducted using the search string 'cookie security' on the Google Scholar and IEEE databases. I filtered search results to include literature from 2015-present, reviewing 20 of 1500 papers.

Results

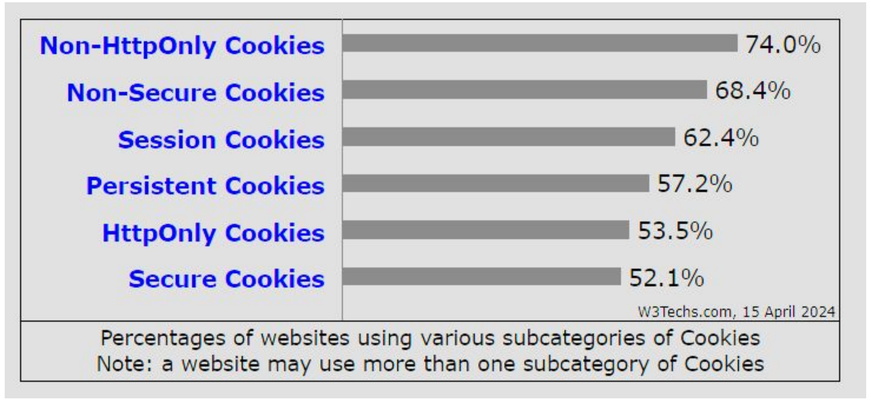

Figure 1: Usage Statistics of Cookies For Websites, April 2024
From: https://w3techs.com/technologies/details/ce-cookies

Previous research shows that the majority of websites use cookies, with an alarming number of websites that use non-secure cookies (Figure 1). The transmission of cookie data over insecure channels, such as HTTP, exposes users to significant security risks. Phishing attacks represent a prevalent threat, with attackers using fake websites or hyperlinks to redirect users to unsecure servers where cookie data can be compromised [2]. Vulnerabilities in web servers and internet service providers create opportunities for malicious actors to intercept and exploit cookie data. Encryption helps mitigate the risk of unauthorized access to sensitive information contained within cookies, enhancing overall security [3,4].

Conclusion

With the use of online cookies becoming more and more prevalent in today's digital world, the risks have also increased. While encryption offers a base layer of protection, it is important for a user to stay vigilant when surfing the web. By remaining mindful of the information we share and the sites we visit, we can better safeguard our personal cookie information from potential threats.

References

[1] Figure 1: Usage Statistics of Cookies for Websites, April 2024

[2]S. Sivakorn, I. Polakis and A. D. Keromytis, "The Cracked Cookie Jar: HTTP Cookie Hijacking and the Exposure of Private Information," *2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2016

[3]H. Kwon, H. Nam, S. Lee, C. Hahn and J. Hur, "(In-)Security of Cookies in HTTPS: Cookie Theft by Removing Cookie Flags," in *IEEE Transactions on Information Forensics and Security*, vol. 15, 2020.

[4]K. Nirmal, B. Janet and R. Kumar, "It's More Than Stealing Cookies - Exploitability of XSS," *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, 2018

Acknowledgments

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute