Exposing Flaws in Web Security with Emphasis on Interception Assaults and Session Breach Exploits.

[1] Rakesh S N, [2]Miss Renuka B N

[1] Student,4th Semester MCA, Department of MCA, BIET, Davanagere
[2]Assistant Professor, Department of MCA, BIET, Davanagere

ABSTRACT:

In today's digital age, the widespread use of the Internet has made data highly susceptible to various cyberattacks due to its inherently open-access nature. Among the most concerning threats to data privacy are web-based attacks. This Systematic Literature Review (SLR) focuses specifically on two such attacks: Man-in-the-Middle (MITM) and session hijacking. It analyzes approximately 30 research studies published between 2016 and 2023, selected through a structured and rigorous review process. The SLR is guided by three main research questions. The first question explores general trends in research on MITM and session hijacking attacks. Findings indicate a peak of 7 publications in 2018, which declined to 4 by 2021. It was also observed that 73% of these studies were presented at conferences, with India emerging as the leading contributor in this research area. Additionally, IEEE was identified as the most prominent publisher. The second research question looks at the ways that session hijacking and MITM take advantage of the Transmission Control Protocol/Internet Protocol (TCP/IP) stack. Findings indicate that while session hijacking mainly impacts the application and network layers, MITM attacks can target any layer of the stack.

Keywords: SLR, Man-in-the-Middle, MITM, cyber security.

1. INTRODUCTION

In the modern digital era, the rapid growth and widespread use of the Internet have greatly increased the vulnerability of information to cyberattacks. Owing to open and interconnected nature of the web, sensitive information is frequently exposed to a variety of threats—among which web-based attacks remain particularly concerning. Two such critical threats are Man-in-the-Middle (MITM) attacks and session hijacking, both of which pose serious risks to data confidentiality, integrity, and user trust. This Systematic Literature Review (SLR) specifically focuses on these two attack types, aiming to deliver all-inclusive outline of recent progresses in the field. By reviewing approximately 30 research studies published between 2016 and 2023, this study follows a structured methodology to address three main research questions. The first question explores overall research trends related to MITM and session hijacking. It was found that interest in the topic peaked in 2018, with a gradual decline in subsequent years. Notably, India emerged as the leading country in terms of publication output, and IEEE was the most frequent publishing body, indicating significant academic and industry interest. The second question investigates the technical mechanisms of these attacks, especially how they exploit the TCP/IP stack**.** Findings reveal that MITM attacks are capable of targeting all deposits of the protocol stack, while session hijacking is primarily concentrated proceeding the application and network layers.

The third and final research question focuses on the countermeasures proposed in the literature to detect, prevent, and mitigate these attacks. This analysis underscores the need for stronger and more adaptive cybersecurity strategies to protect online communications.

In summary, this review emphasizes the urgent need to strengthen digital defenses against MITM and session hijacking threats. It contributes to the ongoing efforts in cybersecurity research by identifying key trends, contributors, and practical solutions aimed at enhancing data privacy in today's Internet-driven world.

2. RELATED WORK

O. B. Al-Khurafi and M. A. Al-Ahmad, “Survey of web application vulnerability attacks,” in *Proc. 4th Int. Conf. Adv. Comput. Sci. Appl. Technol. (ACSAT)*, Dec. 2015

Web applications have become an important part of our life. Since web applications contain valuable sensitive information, hackers try to find vulnerabilities and exploit them in order to impersonate the user, steal information, or sabotage the application. This paper illustrates in detail the most prevailing and harmful web application vulnerability attacks: SQL Injection, Broken Authentication and Session Management, and Cross-Site Scripting (XSS) [1].

M. S. Hossain, A. Paul, M. H. Islam, and M. Atiquzzaman, “Survey of the guard instruments to the SSL-based session hijacking attacks,” *Netw. Protocols Algorithms*, vol. 10, no. 1, pp. 83–108, Apr. 2018.

There is widespread use of web communications between the client and the server. However, for the majority of client-server communications, session hijacking has emerged as a serious issue. SSL stripping is the most dangerous of the various session hijacking attacks. Several strategies have been put forth to stop session hijacking attacks that rely on SSL tripping. Nevertheless, previous surveys did not provide a thorough summary of all preventive measures (with limited categorization and illustration). This paper's goal is to present a thorough analysis of current defenses against session hijacking attacks based on SSL stripping and compare them. All of the current defenses against SSL stripping-based session hijacking attacks have been divided into two primary groups in this paper: client-side defenses and server-side defenses. [2]

L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, “Ethical dilemmas and privacy issues in emerging technologies: A review,” *Sensors*, vol. 23,

no. 3, p. 1151, Jan. 2023.
In order to overcome the shortcomings of Industry 4.0, Industry 5.0 is anticipated to be a model improvement in digital transformation that will enable mass customization and production efficiencies using cutting-edge technologies like universal machines, autonomous and self-driving robots, self-healing networks, cloud data analytics, etc. We must be constrained and follow legal and ethical guidelines if we are to successfully clear the path for the adoption of these technologies. Being compliant is becoming more difficult at the moment because ethical standards are still being developed and because different regions have different standards and policies. There are potential gray areas that could result in privacy, ethical, and data breaches that need to be addressed when ethical guidelines are ambiguous and inconsistent. This essay explores the moral implications and conundrums of new technologies and offers possible solutions.[3]
H. Corrigan-Gibbs, A. Henzinger, and D. Kogan, “Retrieving private data from a single server with sublinear amortized time,” in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn*. Trondheim, Norway : Springer, 2022

We develop novel protocols for retrieving private information in a single-server environment. With our schemes, a client can discreetly retrieve a series of database records from a server, and the server responds to each query in an average time that is sublinear to the database size.
Our protocols only use common cryptographic techniques [4].

D. Glăvan, C. Răcuciu, R. Moinescu, and S. Eftimie, “Sniffing attacks on computer networks,” *Sci. Bull. Mircea cel Batran Naval Academy*, vol. 23, no. 1, pp. 202–207, 2020.
In terms of network security, the sniffing attack, also known as the sniffer attack, is equivalent to data theft or interception through the use of a sniffer (an application designed to capture network packets) to capture network traffic. If data packets are not encrypted when they are sent over networks, a sniffer can read the data contained in the packet. An attacker can use a sniffer application to examine the network and gather data that will eventually allow them to read network communications or cause the network to crash or become corrupt. Because sniffing attacks are similar to touching wires and listening in on conversations, they are also referred to as "wiretapping" when used on computer networks. This paper discusses a sniffing attack that can seriously harm computer networks and how to defend against it. Typically, sniffing is done to examine network usage, diagnose network issues, and keep an eye on sessions for testing and development [5].

M. Nasereddin, A. ALKhamaiseh, M. Qasaimeh, and R. Al-Qassas, “A systematic review of detection and prevention techniques of SQL injection attacks,” *Inf. Secur. J., Global Perspective*, vol. 32, no. 4, pp. 252–265, Jul. 2023.
SQL injection is a type of database-targeted attack for data-driven applications. It is performed by inserting malicious code in the SQL query to alter and modify its meaning, enabling the attacker to retrieve sensitive data or to access the database.

Many techniques have been improved and proposed to detect and mitigate these types of attacks. This paper provides a systematic review for a pool of 60 papers on web applications' SQL injection detection methods. The pool was selected using a developed searching and filtering methodology for the existing literature based on scholar databases (IEEE, ScienceDirect, and Springer) with the aim to provide specific answering for several research questions in the area of SQL injection detection. This provides a basis for the design and use of effective SQL injection detection methods [6].

7.V. Nithya, S. L. Pandian, and C. Malarvizhi, "A survey on detection and prevention of cross-site scripting attack," *Int. J. Secur. Appl.*, vol. 9, no. 3, pp. 139–152, Mar. 2015.

In present-day time, securing the web application against hacking is a big challenge. One of the common types of hacking technique to attack the web application is Cross-Site Scripting (XSS). Cross-Site Scripting (XSS) vulnerabilities are being exploited by the attackers to steal web browser's resources such as cookies, credentials etc. by injecting the malicious JavaScript code on the victim's web applications. Attackers can use this feature to force the execution of malicious code in a user's Web browser because Web browsers allow commands embedded in Web pages to enable dynamic Web pages. Avoiding this kind of attack is made easier by the analysis of Cross-Site Scripting (XSS) detection and prevention. We outline a method to identify and stop this type of manipulation, thereby removing Cross-Site Scripting attacks [7].

A. Bernal, O. Parra, and R. Díaz, "Man in the middle attack: Prevention in wireless LAN," *Int. J. Appl. Eng. Res.*, vol. 13, no. 7, pp. 4671–4672, 2018.

This document describes some strategies to prevent man in the middle attack on a network wireless LAN 802.11 n, to do this, the man in the middle attack is implemented in a LAN domestic network and each proposed approach has been legalized in order to register the results. Man in the middle attack consists of ARP poisoning and DNS spooling which aims to redirect victim's HTTP requests to a web server installed on the machine of the attacker, in this way, the victim would always be re-directed to a site hosted on the web server of the attacker, disregarding to which domain the victim is pointing at; each strategy was validated and moderately successful results were found due to technical or administrative implications of each setting. Considering that for this article, an attack with particular characteristics was done, some strategies are expected not to work in all scenarios in which case it would be required to combine them or modify them[8].

3. METHODOLOGY

3.1 Dataset Used

This Systematic Literature Review (SLR), which focuses on Man-in-the-Middle (MITM) and session hijacking attacks, is based on an analysis of about 30 research papers published between 2016 and 2023. The dataset used in this review was constructed by selecting relevant studies from reputable digital libraries such as IEEE Xplore, SpringerLink, ScienceDirect, and ACM Digital

Library. The selection criteria involved filtering papers based on keywords like "MITM attack", "session hijacking", "cybersecurity", and "TCP/IP vulnerabilities". Only peer-reviewed research with well-defined goals, procedures, and conclusions pertaining to MITM and session hijacking was taken into consideration thanks to the inclusion criteria. To find patterns in research trends, suggested countermeasures, and technical approaches, these studies were subsequently grouped and compiled.

3.2 Data Preprocessing

In this review-based methodology, data preprocessing involved organizing and refining the selected research papers to ensure relevance and consistency. First, duplicate entries and non-English publications were removed. Next, papers not directly addressing MITM or session hijacking attacks were excluded based on designation and intangible screening. A thorough full-text review was then conducted to extract specific information regarding the attack mechanisms, protocols affected, and proposed solutions. To each learning was oblique based on publication year, publishing platform, country of origin, and type of venue (conference or journal). This structured preprocessing enabled a more systematic and comprehensive analysis of the literature, facilitating trend identification and deeper insights into the evolution of techniques over time.

3.3 Algorithm Used

Since this is a literature-based review, no specific machine learning or computational algorithm was applied directly to raw data. However, the analysis did involve a qualitative synthesis of the methodologies and algorithms reported in the selected studies. Many of the reviewed papers used algorithms such as support vector machines (SVM), decision tree and neural networks to detect MITM and session hijacking attempts. Others relied on cryptographic protocols like SSL/TLS and key-exchange mechanisms. Some studies employed anomaly detection techniques using statistical and machine learning models to recognize unusual network behavior. These reported algorithms were documented and categorized in this review to comprehend the prevailing trends in computational approaches used to address web-based cyberattacks.

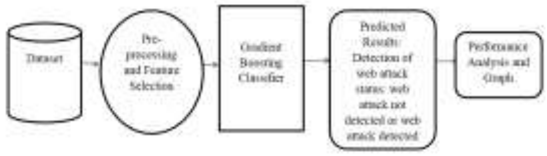
Dataset
Pre-processing and Feature Selection
Gradient Boosting Classifier
Predicted Results: Detection of web attack status: web attack not detected or web attack detected
Performance Analysis and Graph

Figure 3.3.1 : System architecture

3.4 Techniques

Several methods for identifying, stopping, or mitigating Man-in-the-Middle (MITM) and session hijacking attacks were found in the chosen studies for this Systematic Literature Review. These strategies range from conventional cryptography to more sophisticated approaches that use artificial intelligence and behavioral analysis. One of the most commonly discussed techniques is the use of end-to-end encryption protocols, such as HTTPS and SSL/TLS, which help protect data in transit and prevent unauthorized interception. These protocols ensure that even if data is intercepted, it remains unreadable without the correct decryption keys.Another frequently proposed technique involves the implementation of multi-factor authentication (MFA).

3.5 Flowchart

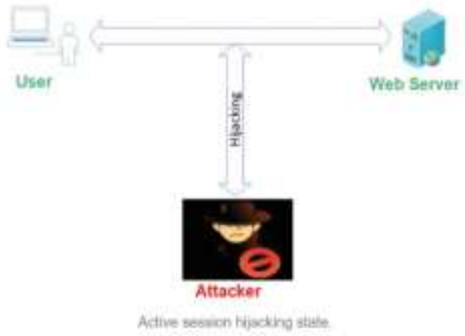

Figure 3.5.1: Flowchart

4. RESULT

4.1 Graphs

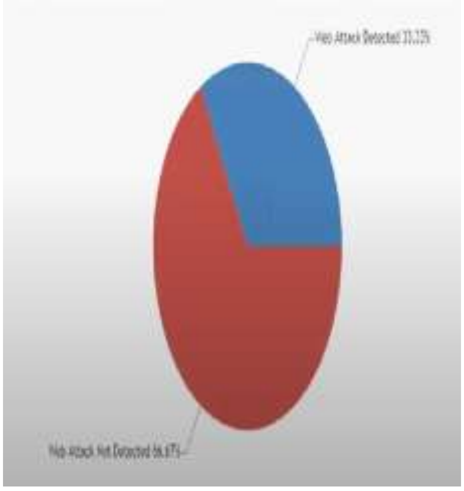

Figure 4.1.1 : Resulant graph

4.2 Screenshots

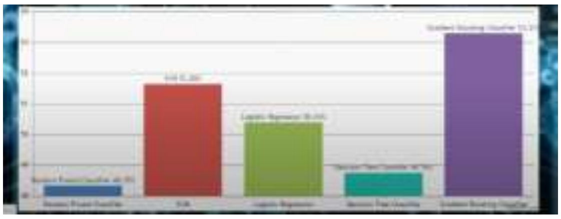

Figure 4.2.1 : Bar graph

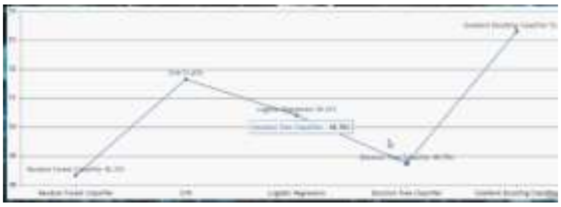

Figure 4.2.2 : Web attack status ration in line chart

5. CONCLUSION

This review emphasizes how urgently improved cybersecurity frameworks are needed to counter the rising threats of session hijacking and man-in-the-middle attacks. By analyzing publication trends, geographical contributions, and attack vectors, the study sheds light on research gaps and the need for collaborative security solutions. Granting numerous approaches have been proposed to counter these attacks, the dynamic and evolving nature of web threats necessitates continuous innovation in detection and prevention strategies. Strengthening data privacy and reinforcing security layers across all protocol levels is vital to safeguarding users in the modern internet landscape.

6. REFERENCES

1. "Survey of web application vulnerability attacks," in *Proc* O. B. Al-Khurafi and M. A. Al-Ahmad, *4th Int. Conf. Adv. Comput. Sci. Appl. Technol. (ACSAT)*, Dec. 2018

2. "Survey of the protection mechanisms to the SSL-based session hijacking attacks," M. S. Hossain, A. Paul, M. H. Islam, and M. Atiquzzaman, *Netw. Protocols Algorithms*, vol. 10, no. 1, pp. 83–108,

Apr.2018.

3. “Ethical dilemmas and privacy issues in emerging technologies: A review,” L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, *Sensors*, vol. 23, no. 3, p. 1151, Jan. 2023.

4. “Single-server private information retrieval with sublinear amortized time,” in *Proc.* H. Corrigan-Gibbs, A. Henzinger, and D. Kogan, *Annu. Int. Conf. Theory Appl. Cryptograph. Techn*. Trondheim, Norway : Springer, 2022

5. “Sniffing attacks on computer networks,” *Sci* D. Glăvan, C. Răcuciu, R. Moinescu, and S. Eftimie,. *Bull. Mircea cel Batran Naval Academy*, vol. 23, no. 1, pp. 202–207, 2020.

6. “A systematic review of detection and prevention techniques of SQL injection attacks,” *Inf* M. Nasereddin, A. ALKhamaiseh, M. Qasaimeh, and R. Al-Qassas,. *Secur. J., Global Perspective*, vol. 32, no. 4, pp. 252–265, Jul. 2023.

7. “A survey on detection and prevention of cross-site scripting attack,” *Appl.*, V. Nithya, S. L. Pandian, and C. Malarvizhi, *Int. J. Secur.* vol. 9, no. 3, pp. 139–152, Mar. 2015.

8. “Man in the middle attack: Prevention in wireless LAN,” *Int* A. Bernal, O. Parra, and R. Díaz,. *J. Appl. Eng. Res.*, vol. 13, no. 7, pp. 4671–4672, 2018.

*****