JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Hijacking Spoofing Attack & Defense Strategy Based On Secured Network protocols

[1]Prof.Arunadevi P, [2]Manoj P, [3]Jeffinisha T, [4]Samnickolas P,

[1]Assistant Professor, [2]UG Student, [3]UG Student, [4]UG Student, [5]UG Student
[1]Department of Computer Science and Engineering,
[1]RVS College of Engineering and Technology, Coimbatore, India

Abstract : The communication networks are essential for sharing information, but they are also vulnerable to cyber threats like hijacking and spoofing attacks. These attacks allow hackers to take control of network connections, steal sensitive data, and disrupt services. This creates serious security risks, as unauthorized users can access private information, manipulate data, or interfere with communication systems. To protect networks from these threats, this paper introduces a security strategy based on secure network protocols. The strategy includes four key components: authentication, encryption, intrusion detection, and secure routing. Authentication ensures that only verified users and devices can access the network. This prevents hackers from pretending to be someone else to gain entry. Encryption protects data by converting it into a secure format that cannot be easily read or modified by attackers. This ensures that even if hackers intercept the data. Intrusion Detection Systems act as security guards, continuously monitoring the network for any suspicious activity. If an attack is detected, the system quickly takes action to stop it. Secure Routing ensures that data travels safely across the network, preventing attackers from redirecting or altering the flow of information. By combining these security techniques, the proposed strategy creates a strong defense against hijacking and spoofing attacks. It helps protect sensitive information, ensures secure communication, and minimizes the risk of cyber threats.

Index Terms - Hijacking attacks, Spoofing attacks, Client side request forgery, Network security, Secure network protocols, Authentication, Encryption, Intrusion Detection System , Secure routing.

I. INTRODUCTION

Hacking and spoofing are two of the most significant cyberthreats, and they are getting increasingly sophisticated. Sensitive data is at risk from these attacks, which target communication networks, critical systems, and data-sharing procedures. These methods are employed by hackers to obtain unauthorized control over networks, interfere with services, or steal data. When a hacker gains control of a network connection, a communication session, or even an entire system, this is known as a hijacking assault. This enables them to take over accounts, disrupt services, or steal or alter data. In order to fool the system into allowing access or disclosing information, spoofing attacks entail an attacker posing as a reliable source, such as a genuine user, website, or device. Many traditional security measures, like simple passwords, basic firewalls, and outdated antivirus programs, are not strong enough to detect and prevent these attacks. Hackers are constantly finding new ways to bypass these defenses, making cybersecurity a major concern for businesses, governments, and individuals.

II. RELATED WORK

TITLE: Encryption Algorithm for TCP Session Hijacking
AUTHORS: Minghan Chen.,
PUBLICATION: IEEE Access, 2020

DESCRIPTION:

One kind of man-in-the-middle (MITM) attack is TCP session hijacking, in which a hostile actor seizes control of an ongoing TCP session between two computers. By protecting communication and confirming the legitimacy of data, encryption techniques play a critical role in thwarting such attacks.

TITLE: Neutralizing BGP Hijacking within a Minute
AUTHORS Pavlos Sermpezis.
PUBLICATION: IEEE Access, 2021

DESCRIPTION:

An attack known as BGP (Border Gateway Protocol) hijacking occurs when a malicious or improperly configured network publishes fictitious IP routes in an attempt to reroute or intercept internet traffic. This may result in denial of service attacks, traffic rerouting, or spying.Rapid identification and mitigation utilizing a number of crucial strategies are necessary to neutralize such attacks rapidly (within a minute).

TITLE: Defending Wireless Networks Against Evil Twin and Deauthentication Attacks

AUTHORS: C. Kaufman
PUBLICATION: IEEE Access, 2019

DESCRIPTION:

Because wireless networks operate outdoors, they are by nature more vulnerable than cable ones. DE authentication and Evil Twin attacks are two of the most prevalent wireless risks. A detailed explanation of these attacks and how to successfully ward them off can be found below.

III. EXISTING SYSYEM

3.1 Encryption using TLS/SSL

What it is: The communication between a user's browser and the server is encrypted using the cryptographic protocols SSL (Secure Sockets Layer) and TLS (Transport Layer Security).Prevents hackers from viewing or altering data (such as credit card information and passwords) while it's in transit. Where it's utilized: HTTPS (secure version of HTTP) is now used on all contemporary websites. If a website doesn't employ HTTPS, browsers like Chrome and Firefox block it or issue a warning. Protection Against: Taking over a session, Attacks via man-in-the-middle (MITM), Modification of data while it's being transmitted

3.2Internet Protocol Security or IPSec

IP sec is a set of protocols that encrypts and authenticates every IP packet in a session, thereby securing IP communications. The goal is to guarantee the confidentiality and integrity of data transmitted over networks, particularly the public internet. Where to utilize it: Virtual Private Networks, or VPNs, Devices on corporate networks can communicate securely with one another. Protection Against: Spoofing, IP Taking over a session, Attacks by replay

3.3 Secure Email Gateways

If an email comes from an authorized mail server. DKIM (DomainKeys Identified Mail): Attaches a digital signature to emails to prove they haven’t been altered. DMARC (Domain-based Message Authentication, Reporting, and Conformance): Tells email receivers how to handle emails that fail SPF or DKIM checks. Purpose: Stop email spoofing where attackers send emails pretending to be someone else (phishing attacks). Where it's used: Email providers (like Gmail, Outlook, Yahoo) and corporate email servers. Defence Against: Email spoofing Phishing attacks

3.4 ARP Monitoring Tools

A tool that monitors Ethernet activity and keeps track of IP and MAC addresses to detect suspicious ARP changes. Dynamic ARP Inspection (DAI): A network switch feature that intercepts, validates, and discards invalid ARP packets. Purpose: Detect and stop ARP spoofing where attackers fake the ARP responses to intercept or alter communications inside local networks. Where it's used: Enterprise LANs (Local Area Networks), data centres, Wi-Fi networks. Defence Against: ARP spoofing Man-in-the-middle attacks inside local networks

IV. PROPOSED SYSTEM

To protect against hijacking and spoofing attacks, we suggest using a multi-layered security system. This means not depending on just one method, but combining several techniques to make the network much safer. To defend against hijacking and spoofing attacks, we propose a multi-layered security framework based on advanced network protocols and modern cybersecurity techniques. Our strategy includes the following key components

4.1 Machine Learning-Based Anomaly Detection

Artificial Intelligence plays a very important role in protecting networks today. It works like a smart security guard who is always watching and learning. AI constantly monitors the network all the time, without getting tired, observing everything that happens such as user logins, file transfers, and website access. If anything looks strange or different from the usual behavior, AI immediately notices it. Over time, AI learns from past attacks and becomes smarter by understanding the patterns of hijacking and spoofing attempts. This means that even attackers come up with new methods, AI can recognize early warning signs faster than traditional systems. Attackers often try to disguise themselves to look like normal users or systems, but AI goes deeper than just checking usernames or IP addresses.

4.2 Blockchain-Based Authentication

Blockchain records who is permitted access, functioning as a permanent, impenetrable guest list. All of the blockchain's entries are safely stored and cannot be altered, removed, or falsified. The blockchain instantly detects any attempt by a hacker to impersonate someone else, for as by using a counterfeit credential or a duplicate key card. Any effort to falsify or alter information will not match the original record because the true identity is already saved in the blockchain and is safeguarded by robust cryptographic measures. Anything that doesn't match its trusted data is automatically rejected by the blockchain network. This makes spoofing attacks, in which hackers fabricate identities to deceive systems, all but impossible.

4.3 Enhanced Encryption Protocols

Encryption locks sensitive information so only the intended receiver can open it. Even if a hacker intercepts the data (like someone stealing your letter), they won’t be able to read it without the key. This protects against Man-in-the-Middle (MITM) attacks, where hackers try to eavesdrop on your communication.

4.4 Real-Time Threat Intelligence

This technology is intended to continuously scan the network for indications of unusual activity or threats. Like a security guard who never sleeps, it never takes a break from work. The system is able to identify the threat almost immediately if a hacker attempts to start an assault. Before any serious harm is done, the system acts immediately to stop the hacker or shut down the impacted areas of the network, rather than waiting for a human to notice the issue. Compared to traditional security systems, which typically identify threats only after they have already caused harm, this prompt response is a significant gain.

V. RESEARCH METHODOLOGY

This research employs a methodical approach based on real-world tests, simulations, and theoretical analysis to create and validate a robust security mechanism against hijacking and spoofing assaults. The following are the steps:

5.1 Identification of the Problem

Finding and comprehending several kinds of hijacking and spoofing attacks, including IP spoofing, ARP spoofing, DNS spoofing, session hijacking, and email spoofing, is the first step in the research process. The research finds the flaws in the current network systems that expose them to these dangers by examining these attacks.

5.2 Examining Current Security Procedures

Current secure network protocols, including TLS/SSL, IPSec, DNSSEC, and ARP inspection, were thoroughly reviewed. We looked at the operation of these protocols, the threats they defend against, and their vulnerabilities to contemporary, complex attacks.

5.3 Creating a Multi-Layer defence Structure

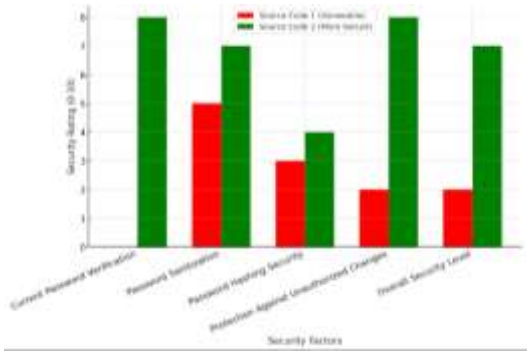
A multilayered security framework is created based on the vulnerabilities found in the systems that are currently in use. To protect against spoofing and hijacking attacks, this framework integrates blockchain-based identity verification, AI-based real-time threat detection, authentication protocols like SPF/DKIM/DMARC, encryption techniques like TLS/SSL and IPSec, and cloud-based protection services like Cloudflare and AWS Shield.

5.4 Testing and Simulation

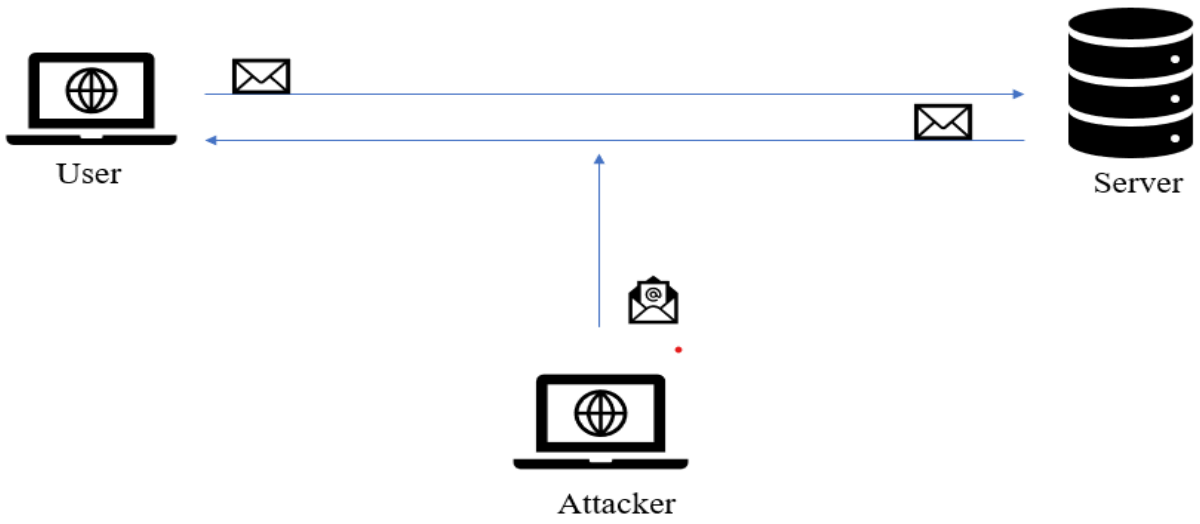
A controlled test environment that mimics several kinds of hijacking and spoofing attacks is established in order to verify the suggested defence approach. These attacks include efforts at email spoofing, session hijacking on unprotected web applications, DNS spoofing to reroute users to malicious websites, and ARP spoofing within a local network. To determine how well the suggested security measures identify and stop these assaults, they are put into practice and put through testing.

5.5 Analysis of Performance

Key performance indicators like detection speed, attack prevention success rate, false positives, and network performance effect are used to assess the system's performance. This analysis aids in determining the multi-layered defences framework's advantages as well as its shortcomings.



VI. BLOCK DIAGRAM



The User, the Server, and the Attacker are the three primary entities shown in the block diagram. Requests like signing in or changing a password are often sent by the User to the Server directly, and the Server reacts as necessary. But in the event of an assault, the attacker attempts to obstruct this line of communication. The attacker can intercept, alter, or introduce malicious material into the user-server communication by employing techniques like session hijacking or man-in-the-middle assaults. For example, without the user's awareness, an attacker could alter a password reset request or steal a session cookie. There are various protection techniques that are suggested to stop such attacks. Implementing HTTPS, which encrypts all communications to make interception exceedingly difficult, is the first line of protection. Additionally, CSRF tokens are employed to guarantee that private operations, such as changing a password, are authentic and started by the authorized user. Regenerating session IDs each time a user checks in is another crucial protection tactic that prevents attackers from using stolen session IDs.

VII. RESULT

The project's main goal was to comprehend how hijacking and spoofing attacks work and how to employ secure network protocols to protect against them. To illustrate how attackers could intercept and alter data between users and servers, a simulation was conducted in the first phase, known as Attack Analysis, utilizing tools such as Burp Suite. It was demonstrated that an attacker could readily intercept session cookies or alter HTTP requests in the absence of appropriate security, such as HTTPS, thereby jeopardizing the user's session. The second stage, known as Attack Simulation, involved creating a phony link that looked like a genuine movie download page. Unbeknownst to the user, a covert malicious request altered their account password when they clicked the link, effectively breaching their account.

Module	Description	Output/Outcome
Module 1 Attack Analysis	Simulated session hijacking and MITM attacks using Burp Suite	Attack successfully intercepted and modified HTTP/HTTPS traffic
Module 2 Attack Simulation	User tricked into clicking a fake link causing password change	User's account compromised
Module 3 Defense Strategy	Implemented CSRF tokens and session ID regeneration	Attack prevention successful

Module	Description	Output/Outcome
Tools Used	Burp Suite, Metasploit Framework, Custom Scripts	Simulated real-world attacks
Outcome	Effective defense mechanisms developed	Enhanced network security recommendations

VIII. CONCLUSION

Modern communication networks are seriously threatened by spoofing and hijacking attacks, which provide hackers the ability to obtain unauthorized access, interrupt services, or steal data. This study presents a robust security approach that integrates intrusion detection, encryption, authentication, and secure routing methods to address these threats. Together, these techniques safeguard networks, guaranteeing data security and thwarting online attacks. By confirming users' and devices' identities, authentication helps prevent unwanted access. Data is protected during transmission via encryption, which prevents hackers from reading it. Intrusion detection systems keep an eye on network activity in order to identify and halt questionable activity. The suggested architecture builds a robust defence mechanism that protects communication networks from spoofing and hijacking threats by incorporating these security features. It guarantees uninterrupted communication, privacy, and data integrity.

IX. FUTURE WORK

- **Blockchain-Based Security Protocols**– By using blockchain's decentralized structure to authenticate and validate communications, man-in-the-middle attacks can be reduced.
- **Real-World Environment Testing–** To assess the suggested solutions' applicability and flexibility, test them in real-world network scenarios, such as public Wi-Fi, business intranets, and Internet of Things networks.
- **Automation of defence Mechanisms -** Creating self-repairing networks that can recognize threats and modify their security settings on their own without assistance from humans**.**
- **Education and Awareness-** To inform developers and end users about the dangers of spoofing and hijacking, future research can also concentrate on establishing training simulators and user-awareness initiatives.

X. REFERNCE

[1] Unveiling Vulnerabilities of Web Attacks Considering Man in the Middle Attack and Session Hijacking, Muteeb bin muzammil1, Muhammad Bilal 2,3, Sahar Ajmal 4,Sandile c. Shongwe 5, and Yazeed y. Ghadi6ieee April 2023

[2] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson Education.

[3] Kaufman, C., Perlman, R., & Speicher, M. (2021). *Network Security: Private Communication in a Public World*. Prentice Hall

[4] Per rig, A., Szewczyk, R., Wen, V., Culler, D. E., & Tiger, J. D. (2002). *SPINS: Security Protocols for Sensor Networks*. Wireless Networks, 8(5), 521-534.

[5] Kent, S., & Seo, K. (2005). *Security Architecture for the Internet Protocol*. RFC 4301, IETF.

[6] Goldberg, I. (2000). *A Pseudonymous Communications Infrastructure for the Internet*. Privacy Enhancing Technologies (PET).