Enhancing Email Security Through Effective Header Analysis and Authentication Protocols

Sunay Bhoyar
Computer Engineering
Pune Institute of Computer Technology
Dhankwadi, Pune
bhoyar.sunay@gmail.com

Aditya Mittal
Computer Engineering
Pune Institute of Computer Technology
Dhankwadi, Pune
adityamittal355@gmail.com

Satvik Doshi
Computer Engineering
Pune Institute of Computer Technology
Dhankwadi, Pune
doshisatvik22@gmail.com

***Abstract*—This paper explored the issue of email spoofing, a Cybersecurity threat wherein attackers send the mail in the name of different senders to send recipients the fake messages. The study delved deep into email headers, understanding the anatomy of these headers and identifying key fields frequently manipulated by attackers during spoofing attempts. Focusing on this information, the paper proposed robust anti-spoofing solution and the important measures that must be taken by the mail providers to make their mails services safe.**

A major focus was made on utilizing protocols that enhance security by validating sender domains and signatures, significantly to reduce the success rate of spoofing attacks. The seminar showcased a detailed analysis of email headers, demonstrating a comprehensive approach to efficiently detect email spoofing attackers.

The paper provided the detailed relationship between email headers, spoofing, and Cybersecurity, highlighting the urgency of safeguarding crucial information embedded in email headers. Through this comprehensive study, the paper provided valuable insights, showing the way for enhanced email security protocols in the realm of Cybersecurity.

1. INTRODUCTION

In the rapidly evolving digital landscape, electronic communication has become an integral part of our daily lives, playing a important role in personal and professional interactions. However, with the increasing dependence on email communication, the threat scope has also expanded, posing significant challenges to the integrity and security of email correspondence. Among the most potent cyber threats targeting email systems is email spoofing, a deceptive technique where malicious actors impersonate legitimate senders to manipulate recipients into believing false information. This practice undermines the trustworthiness of digital communication, making it imperative to create strategies to combat it effectively.

The focus of this paper is to get into the intricate realm of email security, specifically addressing email spoofing. We explore the vulnerabilities inherent in email headers, the fundamental components of electronic messages, which are often exploited by attackers during spoofing attempts. By understanding the anatomy of email headers, our study aims to identify critical fields that are potential ways to manipulate, creating the importance of development of robust countermeasures. Through header analysis, we can unravel patterns and anomalies, empowering organizations and individuals alike to differentiate between genuine and fraudulent emails.

Additionally, this paper investigates authentication protocols designed to better the email security. By verifying sender domains and signatures, these protocols add an extra layer of validation, significantly reducing the success rate of spoofing attacks. Our research critically evaluates the working of these protocols in real-world scenarios, aiming to provide insights into their practical implementation .

2. LITERATURE SURVEY

"Email Spoofing in the Age of Anti-Spoofing Protocols"[1] in the pursuit of understanding the exhistence of email spoofing despite the widespread adoption of anti-spoofing protocols, Mr. Prashant D. Chauhan and Prof. (Dr.) Apurva M. Shah conducted a rigorous examination. Their study raised fundamental questions about the effectiveness of existing security measures. By delving into the details of the Simple Mail Transport Protocol (SMTP), a important protocol of email communication. SMTP, lacking authentication mechanisms for email senders, emerged as a weak link in the security, allowing potential spoofing attacks to breach supposedly verified domains. The paper, presented at the 2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT), underscored the urgent need for more robust and comprehensive authentication solutions in the face of evolving spoofing ways.

"Enhancing Email Security through Header Analysis and Machine Learning"[2], Craig Beaman and Haruna Isah embarked on an experimental exploration of email header information's potential in combatting spam and phishing attacks. Their research centered on the efficacy of machine learning techniques, including Random Forest, SVM, MLP, KNN, and their ensembles. Through detailed analysis, they revealed a remarkable accuracy in detecting spam (97%) and phishing emails (99%) by scrutinizing email header data. This study marked a significant advancement, showing the power of machine learning algorithms in enhancing email security. Their work contributed valuable insights into the fusion of technology and cybersecurity, paving the way for email security solutions.

"Challenges and Solutions in Simple Mail Transport Protocol (SMTP)"[3], in an insightful examination of the Simple Mail Transport Protocol (SMTP), M. Tariq Banday provided vulnerabilities that compromise email security and privacy. Published in the International Journal of Distributed and Parallel Systems (May 2011), Banday's research illuminated SMTP's security shortcomings, particularly its lack of features for ensuring message integrity. This absence opened the easy for spam and phishing attacks, leading to network congestion and storage misuse. Their findings served important call for highlighting the need for security enhancements within SMTP, a protocol foundational to global email communication.

"Authentication Protocols and Their Role in Mitigating Email Viruses"[5],Khairan Marzuki, Naufal Hanif, and Putu Hariyadi delved into the realm of email viruses and the evolving battle against them. Their study focused on the transformative impact of authentication protocols, specifically SPF and DKIM, on email server security. Published in the International Journal of Electronics and Communications Systems (December 2022), their research showcased the protocols' important role in email viruses and spoofing attempts. By meticulously authenticating and authorizing every email from the source, SPF and DKIM emerged as guardians against email-based threats. This study underscored the critical importance of robust authentication protocols in digital communication channels against cyber adversaries.

3. METHODOLOGY

The methodology begins with a review of established algorithms, techniques, and methods prevalent in the field of email security. We studied deep into existing email authentication protocols, including DMARC (Domain-based Message Authentication, Reporting, and Conformance), SPF (Sender Policy Framework), and DKIM (DomainKeys Identified Mail). This comprehensive analysis allows us to discern the strengths and limitations of these protocols. Additionally, we explore cryptographic algorithms such as RSA (Rivest-Shamir-Adleman) and SHA (Secure Hash Algorithm) employed in email encryption and digital signatures. Concurrently, existing header analysis techniques, encompassing anomaly detection and behavioral analysis, are important to identify patterns of email spoofing.

3.1. The Proposed Course Outline

3.1.1. Understanding Email Spoofing Threats and Consequences

It explores the various tactics employed by malicious actors and discusses the potential risks and consequences associated with successful email spoofing attacks. Emphasis is placed on the urgency of developing robust countermeasures to safeguard digital communication channels.

3.1.2. Deconstructing Email Security Protocols: DMARC, SPF, and DKIM

The core of email security, this segment offers an in-depth analysis of strong email authentication protocols, namely DMARC, SPF, and DKIM. It reveals their functionalities, strengths, and inherent limitations.

3.1.3. Initial Email Spoofing Endeavors and Importance of Domain Verification

The initial stages of the research journey, detailing the challenges encountered during the setup of test accounts and the attempts at email spoofing. It emphasizes the crucial role of domain verification in testing of spoofing attempt .

3.1.4. Strategies and Complexities of Domain Verification

Focusing on domain authentication, this part explores various strategies and techniques used to establish domain legitimacy. It delves into the complexities of domain verification processes, providing insights into the methods employed to ensure the authenticity of email senders. The content discusses both traditional and innovative approaches, emphasizing their effectiveness in the face of evolving spoofing tactics.

3.1.5. DEFCON Seminar Revelations and Exploration of Mail Channels

Building on real-world insights, this segment encapsulates the knowledge acquired during the DEFCON meet[4]. It explores the sophisticated impersonation techniques discussed at the meet, emphasizing the absence of passwords in spoofing attempts. Additionally, the research investigates mail channels, shedding light on their important role in facilitating email spoofing. The content delves into the mechanics of these channels, elucidating their exploitation by malicious entities.

3.1.6. Vulnerabilities and Exploitation

It focuses on a detailed analysis of Hostinger's mail channel feature. It scrutinizes the vulnerabilities identified within this specific platform and explores the methods employed by spoofers to exploit these weaknesses. By understanding the vulnerabilities unique to Hostinger's mail channels, the research aims to provide nuanced insights into service-specific challenges.

3.1.7. Reverting and Targeting Vulnerabilities

Investigating the flexibility of scripting approaches, this segment elaborates on the decision to revert to Python scripts. It discusses the advantages of script-based methodologies, particularly in targeting domains lacking DMARC authentication. The content delves into the customization options and techniques used to exploit vulnerabilities, showcasing the adaptability of script-based spoofing attempts.

3.1.8. Evaluating Email Service Responses to Spoofed Emails

It presents the meticulous testing process employed in the research. It outlines the methodology used to send spoofed emails to a fine array of email services. The content discusses

the observed responses of different email services, focusing on their filtering mechanisms, security protocols, and user notifications. By harshly evaluating these responses, the research aims to identify patterns and vulnerabilities in email service defenses.

3.1.9. Enhancing Email Security Measures

In the final section, the research synthesizes key findings, vulnerabilities identified, and recommendations formulated. It discusses the implications of the research outcomes on the broader landscape of email security. The content also introduces the development of an email analyzer tool in its alpha phase, highlighting its potential in verifying email legitimacy and combating phishing attempts. Furthermore, the section outlines future research directions, emphasizing the continuous evolution of email security measures in response to emerging spoofing techniques and cyber threats.

3.2. System Architecture

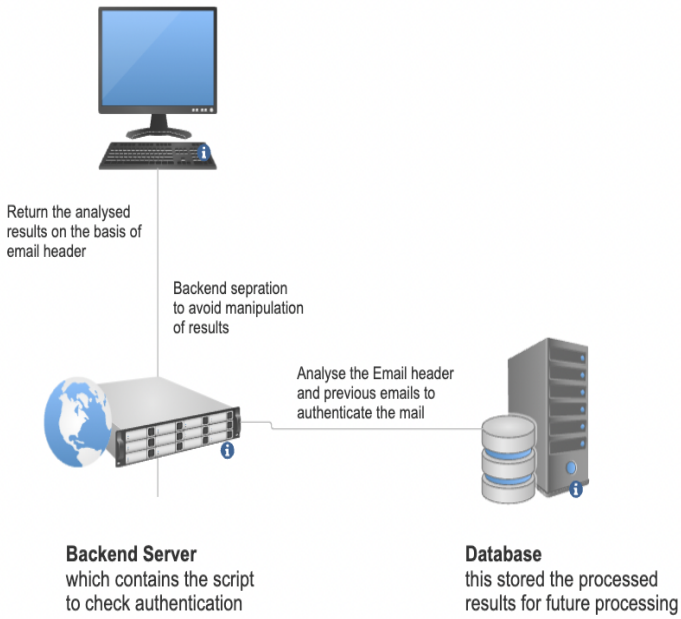

Figure 1 . Flow Architecture of the system

4. RESULTS

Table 1 presents a comprehensive analysis of how different email services respond to spoofed emails before and after domain verification. By examining the behavior of major email providers, including Gmail, Outlook, Yahoo, Proton, Zoho, and Rediff, this study sheds light on the intricate nuances of email service filtering mechanisms and domain verification protocols. The table highlights crucial details such as the initial landing destination of spoofed emails, the subsequent inbox placement after domain verification, and unique service-specific responses.

This detailed analysis of email service responses underscores the importance of robust email authentication mechanisms. Understanding the diverse responses aids in pinpointing vulnerabilities within existing email security protocols.

Email Service	Location	Email Lands in after verification	Comment
Gmail	Spam	Inbox	Once the domain is verified then even if we change the senders email then too it land to inbox
Outlook	Spam	Inbox	This email service finds difficult to distinguish the original sender and provides the details to even fake sender
Yahoo	Spam	Spam	Only mail to put it under span and then making it dangerous
Proton	Spam	Inbox	Similar to gmail
Zoho	Inbox	Inbox	When the newsletter is disabled then the mail lands directly to the inbox
Rediff	Inbox	Inbox	This mail service showed most poor service where it made the mail to get directly to the inbox without any verification and even omitted the changed domain

Table 1. Experimental Results : Based upon DMARC, SPF, DKIM parameters

5. CONCLUSION

One of the important findings of our study was the diverse responses exhibited by major email services in the face of spoofed emails. From Gmail's robust domain verification mechanisms to Rediff's most inefficient, each service showcased unique strengths and vulnerabilities. These observations underscore the urgency for standardization and enhanced vigilance across the email service spectrum. Service providers must invest in more sophisticated algorithms that not only identify spoofed emails but also distinguish between legitimate senders and their fraudulent guys.

Moreover, our research revealed the importance of domain verification. A verified domain emerged as crucial in ensuring the safe passage of emails to the recipient's inbox. It acts as a shield against even the most sophisticated spoofing attempts, reaffirming the significance of stringent authentication protocols.

In response to our findings, we initiated the development of an innovative email analyzer tool, designed to provide users with a user-friendly interface for email legitimacy verification.

This tool, in its alpha phase, showcases our commitment to translating research insights into practical solutions. However, it also serves as a testament to the ongoing challenges faced in the realm of email security.

As we conclude this research, it is evident that the battle against email spoofing is far from ago. It demands collaborative efforts between researchers, service providers, and end-users. By fostering a collective commitment to advancing authentication protocols, raising user awareness, and embracing cutting-edge technologies, we can confirm the digital realms we navigate daily.

Our study acts as a clear call, urging the cybersecurity community to rise to the challenge, adapt swiftly, and innovate relentlessly. Only through continuous vigilance and collaboration can we bolster email security, ensuring that our digital conversations remain private, secure, and devoid of malicious intent.

6. REFERENCES

[1] Mr. Prashant D. Chauhan, Prof. (Dr.) Apurva M. Shah, “Email Spoofing: In Today’s Era” , pp. 2-5, November 2022 .

[2] Craig Beaman, Haruna Isah, “Anomaly Detection in Emails using Machine Learning and Header Information”, VII. CONCLUSION, pp. 9, March 2022.

[3] M. Tariq Banday , “Effectiveness and Limitations of E-Mail Security Protocols” ,International Journal of Distributed and Parallel systems , May 2011

[4] Mercello Salvati , “DEF CON 31 - SpamChannel - Spoofing Emails From 2M+ Domains & Virtually Becoming Satan - byt3bl33d3r”, International Conference .

[5] Khairan Marzuki,Naufal Hanif,Putu Hariyadi , “Application of Domain Keys Identified Mail, Sender Policy Framework, Anti-Spam, and Anti-Virus: The Analysis on Mail Servers” , International Journal of Electronics and Communications Systems ,December 2022