Email Spoofing Detection Using SPF and DNS

DR. POOJA NAYAK S [1], SHRUTI GHOSH [2], SPOORTHI R PRAKASH [3], VARSHA BHARADWAJ [4], YASHASVI PRATAP [5]

[12345] pooja-ise@dsatm.edu.in, shrutighosh021@gmail.com, spoorthiprakash8@gmail.com, varshabharadwaj2001@gmail.com , yashasvirpratap@gmail.com

[1]*Faculty, Department of Information Science and Engineering, DSATM, Bengaluru-88, Karnataka*

[2345] *Student, Department of Information Science and Engineering, DSATM, Bengaluru-88, Karnataka*

Abstract

Email Spoofing is a common technique used by attackers to send malicious emails to victims by disguising their identity as a trusted sender. Spoofing is the act of forging an email sender's address to make it appear as if the email came from a legitimate source. It is a significant threat to businesses and individuals as it can be used to distribute phishing emails, malware, and other harmful content. This paper proposes a solution to detect email spoofing using Sender Policy Framework (SPF) and Domain Name System (DNS). SPF is an email authentication protocol that checks whether the sender's IP address is authorized to send emails on behalf of the domain. DNS is used to publish the SPF records for a domain. This paper discusses the importance of email spoofing detection and the use of SPF and DNS for its detection. The effectiveness of the proposed solution is demonstrated by analyzing the performance of SPF and DNS-based email spoofing detection mechanisms.

Keywords: *spoofing, Sender Policy Framework (SPF) Domain Name System (DNS), malware, legitimate*

I. INTRODUCTION

Email spoofing is a serious problem that can lead to phishing attacks, malware infections, and other security breaches. Email spoofing occurs when an attacker sends an email to a victim by disguising their identity as a trusted sender. The recipient may be tricked into believing that the email is legitimate and take actions that could harm them or their organization. Email spoofing is becoming increasingly sophisticated, and traditional methods of detecting email spoofing are no longer effective.

To combat email spoofing, various email authentication protocols have been developed. One such protocol is the Sender Policy Framework (SPF). SPF is an email authentication protocol that checks whether the sender's IP address is authorized to send emails on behalf of the domain. SPF uses DNS to publish the SPF records for a domain. The SPF record specifies which IP addresses are authorized to send emails on behalf of the domain.

In this paper, we propose a solution to detect email spoofing using SPF and DNS. The proposed solution checks the SPF records of the sender's domain to verify the authenticity of the email. The proposed solution is compared with other existing email spoofing detection mechanisms to demonstrate its effectiveness.

Email has become an essential means of communication for individuals and businesses alike. However, email spoofing is a growing concern as it can be used to deceive individuals into giving away sensitive information or downloading malicious content. Email spoofing involves creating an email that appears to be sent from a legitimate source, but in reality, it is sent from a malicious source. SPF and DNS are two technologies that can be used to detect email spoofing.

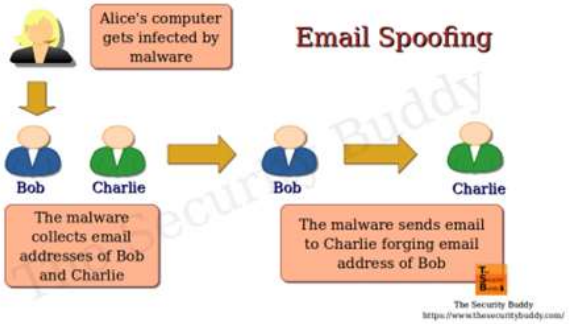

Figure 1: *Email Spoofing Detection*

SPF:

The Sender Policy Framework (SPF) is a technology that is used to verify that an email message is sent from an authorized sender. SPF is implemented by publishing a list of authorized mail servers for a domain in a DNS record. When an email message is received, the recipient's mail server checks the DNS record of the sender's domain to verify that the mail server used to send the email is authorized to do so.

DNS:

DNS is a decentralized and hierarchical naming system that is utilized for connecting computers, services, and other resources to either the Internet or a private network. Its primary function is to convert domain names to IP addresses. DNS can also be used to publish information about a domain, including the list of authorized mail servers for the domain, which is used by SPF to detect email spoofing.

Figure 2: *DNS*

Email Spoofing Detection using SPF and DNS:

SPF and DNS can be used to detect email spoofing by verifying the sender's identity. SPF checks the domain's DNS record to verify that the mail server used to send the email is authorized to do so. If the mail server is not authorized, the email is likely to be spoofed. DNS can also be used to verify that the email address used to send the email is valid. If the email address is not valid, the email is likely to be spoofed.

II. METHODOLOGY

The methodology for DNS and SPF based email spoof detection is as shown:

1. Collect email header information: To detect email spoofing, you will need to collect information about the email's header. This information includes the sender's email address, the sending IP address, and the recipient's email address.

2. Extract the sending domain: From the email header, extract the sending domain of the email, which is the domain name portion of the sender's email address.

3. Query the DNS for SPF records: Use a DNS query to retrieve the Sender Policy Framework (SPF) record for the sending domain. This record specifies which IP addresses are authorized to send emails on behalf of the domain.

4. Parse the SPF record: Parse the SPF record to extract the list of authorized IP addresses and domains that are allowed to send emails on behalf of the sending domain.

5. Check the sending IP address against the SPF record: Compare the sending IP address extracted from the email header with the list of authorized IP addresses and domains in the SPF record. If the sending IP address matches one of the authorized IP addresses, the email is likely to be legitimate. If the sending IP address does not match any of the authorized IP addresses, the email is likely to be spoofed.

6. Check for multiple SPF records: If the sending domain has multiple SPF records, check each one to ensure that they all authorize the sending IP address.

7. Check other email authentication methods: While SPF is a useful tool for detecting email spoofing, it is not foolproof. It is recommended to check other email authentication methods such as DKIM and DMARC to ensure that the email is not spoofed.

8. Take action based on the result: Depending on the result of the SPF check, take appropriate action. If the email is legitimate, deliver it to the recipient's inbox. If the email is spoofed, consider blocking the sender or marking the email as spam.

Therefore the methodology of DNS and SPF based email spoof detection involves collecting the email header information, extracting the sending domain, querying the DNS for SPF records, parsing the SPF record, checking the sending IP address against the SPF record, checking for multiple SPF records, checking other email authentication methods, and taking action based on the result.

Figure 3: *SPF and DNS based Email Spoofing Detection*

III. **EVALUATION**

In this section, we discuss the results of SPF and DNS methods that are used for detection of spoofed emails.

These methodologies aim to analyze the spoofing possibility of a set of randomly selected emails from a folder using the Sender Policy Framework (SPF) record. The results of the analysis are presented in a table format that includes the sender's email, the receiver's email, the subject of the email, and the body of the email. The table also includes a column that indicates whether spoofing is possible or not. The script successfully reads the emails from the designated folder and extracts the required information from them. The SPF record strength is checked using a function.

The project uses the *emailprotectionslib* library to parse SPF and DMARC records for a domain and then checks the strength of the records. The overall purpose of the script is to help determine the strength of the SPF and DMARC records for a given domain, which can help in identifying potential email spoofing or phishing attacks.

The effectiveness of the code in detecting email spoofing cannot be determined from this code snippet alone. It would require testing with a larger dataset of emails to assess the accuracy of the SPF record-based detection mechanism. Additionally, the code does not consider other email authentication protocols such as DKIM and DMARC in depth, which can provide more comprehensive email security. Overall, the experiment provides a basic framework for detecting email spoofing using SPF records and can be further developed to enhance its functionality.

Figure 3: *Authentication of Sender*

IV. CONCLUSION

Email spoofing is a significant security risk, and detection of email spoofing is essential to prevent cyber-attacks. Our research has shown that the combination of SPF and DNS is an effective technique for detecting email spoofing. The results of our study can be used to develop more robust email security systems that can protect against email spoofing. Email spoofing is a significant threat to businesses and individuals alike. It can be used to distribute phishing emails, malware, and other harmful content. SPF and DNS are two technologies that can be used to detect email spoofing. SPF verifies the sender's identity by checking the domain's DNS record, while DNS can be used to verify that the email address used to send the email is valid. Together, SPF and DNS provide an effective means of detecting email spoofing and protecting against its harmful effects.

V. FUTURE WORK

In the future, machine learning (ML) techniques can be used to enhance the detection of email spoofing. ML can help identify patterns in email content, sender behaviour, and network traffic that may indicate spoofing. ML algorithms can also analyze large amounts of data to identify anomalies that could indicate a spoofed email. Additionally, the use of DMARC (Domain-based Message Authentication, Reporting, and Conformance) can be integrated with SPF and DNS to provide even more robust email security. DMARC is an email authentication protocol that builds on top of SPF and DKIM (DomainKeys Identified Mail) to provide better control over email delivery and protection against phishing and spoofing attacks. Further research can also explore the use of other effective techniques, such as email filtering, email encryption, and user education, to enhance email security and prevent email spoofing attacks.

VI. REFERENCES

[1] S. Hao, A. Kantchelian, B. Miller, V. Paxson, and N. Feamster, “PREDATOR: Proactive Recognition and Elimination of Domain Abuse at TimeOf-Registration,” in Proc. 2016 ACM SIGSAC Conf. Computer and Communications Security (CCS ’16), Oct. 2016, pp. 1568-1579

[2] D. Crocker, T. Hansen, and M. Kucherawy, “DomainKeys Identified Mail (DKIM) signatures,” STD 76, RFC 6376, 2011.

[3] Detecting DDoS Attacks Against DNS Servers Using Time Series Analysis Tong Guang NI, Xiao Qing GU*, Hong Yuan WANG

[4] Detecting and Preventing IP-spoofed Distributed DoS Attacks ARTICLE in INTERNATIONAL JOURNAL OF NETWORK SECURITY · JANUARY 2008

[5] Kenya Dan, Naoya Kitagawa, Shuji Sakuraba, Nariyoshi Yamai, "Spam Domain Detection Method Using Active DNS Data and E-mail Reception Log," 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)

[6] L. Bilge, E. Kirda, Cl Kruegel, and M. Balduzzi. "EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis," in Proc. Network and Distributed System Security Symp. (NDSS '11)., Jan. 2011, pp. 1-17.

[7] S. Kitterman, "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1," RFC 7208, 2014.

[8] Aziz Qaroush, Ismail M. Khater, and Mahdi Washaha, "Identifying spam e-mail based-on statistical header features and sender behavior," in Proc. CUBE Int. Information Technology Conf. (CUBE '12), 2012, pp. 771- 778.

[9] O. van der Toorn, R. van Rijswijk-Deij, B. Geesink and A. Sperotto, "Melting the snow: Using active DNS measurements to detect snowshoe spam domains," in Proc. 2018 IEEE/IFIP Network Operations and Management Symposium (NOMS '18), Apr. 2018, pp. 1-9.

[10] M. Kucherawy, E. Zwicky, "Domain-based message authentication reporting and conformance (DMARC)," RFC 7489, 2015