The Effectiveness of DKIM and SPF in Strengthening Email Security

Mohamed Sami Ragheb
University of Bahrain
Sakheer, Bahrain
mabdulmohsin@uob.edu.bh

Wael Elmedany
University of Bahrain
Sakheer, Bahrain
welmedany@uob.edu.bh

Mhd Saeed Sharif
University of East London (UEL)
London, United Kingdom
s.sharif@uel.ac.uk

***Abstract*—Email security is of utmost importance to organizations, and to enhance it, frameworks such as Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are utilized for authentication. In this research work, we conducted a comparative analysis of the efficacy of SPF and DKIM in authenticating emails. Both frameworks offer a certain level of protection against email threats. However, our research indicates that DKIM is more effective as it adopts a more comprehensive approach. Based on our findings, we recommend that businesses prioritize the implementation of DKIM and the Domain-based Message Authentication, Reporting, and Conformance (DMARC) framework to enhance email security and resilience against email impersonation.**

***Index Terms*—SPF, DKIM, DMARC, Email Security, Cybersecurity**

I. Introduction

Email spoofing has become extremely common as criminals rely on it to carry out phishing attacks, spam campaigns, and malware distribution. Technologies like Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) were created to authenticate emails and greatly reduce the threat of spoofing as in [1]. This study aims to determine how effective SPF and DKIM truly are at securing emails from being spoofed. It will analyze both the pros and cons of each technology, how they function individually and together, and how they could work in tandem to provide very strong email security against spoofing.

The study will perform a very thorough comparison of the features, benefits, and drawbacks of both SPF and DKIM. It will assess in full detail how they can complement one another to provide extremely strong email security. The research questions seek to conclusively determine which authentication method is significantly more important for achieving high levels of email security, the major weaknesses of SPF, how DKIM addresses those major issues, and how "Domain-based Message Authentication, Reporting, and Conformance" (DMARC) and Authenticated Received Chain (ARC) frameworks, which are discussed in [2], work together seamlessly with SPF and DKIM.

The comparison analysis will involve a thorough examination of the features, benefits, and drawbacks of both SPF and DKIM. The findings will provide insight into the pros and cons of each technology as well as their role in improving email security. This will help develop more effective ways to prevent email spoofing attacks and protect users from spam, phishing attempts, and malware spread through spoofed emails. The research questions will evaluate which authentication method is more important, the shortcomings of SPF and how DKIM addresses them, the similarities and differences between SPF and DKIM, and how DMARC works on top of SPF and DKIM to provide comprehensive security.

II. Literature Review

The Domain Name System (DNS) allows websites to be accessed using domain names instead of IP addresses. DNS is used for many purposes including email routing and validation. However, DNS records like Text (TXT) resource records can inadvertently expose information to unauthorized parties. Some applications were developed without thoroughly considering security, which could lead to vulnerabilities in TXT records [3].

Email spoofing is when attackers falsify the sender's email address to appear like a legitimate source. It results in huge financial losses. Technologies like SPF, DKIM, and DMARC were created to authenticate senders and prevent email spoofing. But these technologies only work if both the domain owner and email provider implement them correctly. Misconfigurations can still allow spoofing [3].

One study [2] tested if email spoofing still works despite protocols like SPF, DKIM, and DMARC. They set up an email server and attempted to spoof emails sent to major providers like Gmail, Outlook, Yahoo Mail, etc. They found that their spoofed emails were able to reach the inboxes of most major providers except Outlook, showing email spoofing still works despite anti-spoofing protocols.

Another study [4] focused on identifying spear phishing attacks by evaluating the sender domain. Phishing attacks have become more sophisticated, making prevention difficult. Businesses like e-commerce, banking, and Internet Service Providers (ISPs) are common phishing targets due to the sensitive information they contain. Blacklisting is a common phishing prevention method but requires constant updates and is not always effective.

A study [5] examines the use of Secure Multipurpose Internet Mail Extensions (S/MIME) digital certificates for secure email communication. It compares S/MIME and TLS client certificates, discussing the information required for

S/MIME. The study emphasizes the need for each user to have their own unique S/MIME certificate for authentication and the importance of exchanging certificates through a common address book. S/MIME provides end-to-end encryption and authentication using digital certificates based on a Public Key Infrastructure (PKI). S/MIME certificates are similar to Transport Layer Security (TLS) certificates but with some differences. Public hierarchy S/MIME certificates are recommended, but private hierarchy can be used within a group.

Another paper [6] explains the history of Simple Mail Transfer Protocol (SMTP), which is used to send and receive emails. The protocol lacks security protections for confidentiality, integrity, authentication, and authorization, leaving it vulnerable. The paper proposes a new email transfer system with a central server for authentication, and the use of encryption and hashing to secure messages.

The paper [7] proposes a method to identify legitimate email forwarding servers. Current authentication methods have issues verifying forwarded emails. The proposed method analyzes DMARC reports focusing on authentication results and domain information. It then clusters senders' IP addresses based on transmission behavior. One cluster contains known forwarders, which are classified as forwarding servers. The evaluation showed the method can detect forwarders with high accuracy compared to spam lists and filtering results. The detected forwarders corresponded to a significant percentage of emails that would have been false positives using just DMARC authentication.

Reference [8] provides insights into the deployment status of ARC, a protocol designed to address the challenges of email forwarding for authentication. Email forwarding has long posed problems for protocols like SPF, DKIM, and DMARC. ARC aims to preserve authentication when emails are forwarded. However, the paper finds that despite trying to solve an important problem, ARC has seen limited adoption. Analysis of 600k emails shows that while major providers correctly implement ARC, some misinterpret results in ways that could enable spoofing attacks. Forwarding services break ARC, failing to propagate authentication and enabling spoofing attacks. More work is needed for ARC to fully meet its objectives. Widespread and accurate implementation could help address the remaining issues. Their research contributes to understanding current issues and opportunities to improve email authentication.

The objectives of Finland's cybersecurity center were discussed in [9], which aimed to increase cybersecurity awareness and guide organizations toward secure behavior. The paper addresses a lack of knowledge among Finnish organizations regarding the implementation of email forgery-preventing technologies. A study mapped implementation rates of SPF and DMARC in the Top-Level-Domain (TLD) ".fi" and the public sector, finding lower rates in the public sector. Guidelines were drafted for safe implementation.

Research [10] aims to provide more email security through DMARC and DNS data. The motivation is a personal experience with an email scam. The research proposes using DMARC to reduce phishing and malware attacks, and managing DNS settings to add records for more management. This can decrease business risk and provide robust email security.

The evolving threat landscape where attackers use sophisticated social engineering was studied in [11]. While organizations provide security awareness training, current phishing training is often ineffective. The paper presents a toolkit for deploying tailored phishing campaigns at scale. The toolkit enables customizable phishing email templates instantiated with target information and a semi-automated process to select phishing domain names. The paper demonstrates how tailored phishing campaigns can be enhanced to increase email credibility, addressing the limitations of previous studies.

III. Sender Policy Framework (SPF)

Sender Policy Framework (SPF) implements email authentication by configuring a TXT record in the domain's DNS zone. SPF uses mechanisms to authenticate sending domains and prevent email spoofing through a system of policies enforced by recipients. The SPF record specifies which IP addresses are authorized to send emails on behalf of a domain. This record begins with "v=spf1" and specifies the IP addresses allowed to send emails for that domain. Recipients validate this SPF record to verify the sender's authenticity [12].

The main mechanisms used in SPF policies are:

- "a" - Checks if the sender's IP matches the domain's A or AAAA records.
- "ip4" - Matches an IPv4 address within a specified range.
- "mx" - Checks if the IP matches one of the domain's Mail Exchange (MX) records.
- "exists" - Checks if the domain resolves to any IP address.
- "include" - Includes SPF records from other domains.
- "all" - Acts as a catch-all mechanism, often used with "FAIL" to reject any senders not matched.

The SPF also has some qualifiers, which specify how recipients should treat SPF results:

- PASS - Accept the email.
- FAIL - Reject the email.
- SOFTFAIL - Tag the email as potential spam.
- NEUTRAL - Treat the email without applying a policy.

Some mechanisms require additional DNS lookups, which count towards the limit of 10 lookups per SPF record. The "ptr" mechanism is not recommended, as it is considered slow. The "exists" mechanism is commonly used with "macros" to include multiple domains, which are described more in the next subsection. Finally, the "all" mechanism is often used with "FAIL" to reject unauthorized senders. Figure 1 shows the SPF workflow.

A. SPF Macros

SPF macros are codes that can be inserted into SPF records to make them more flexible and adaptive. They work by extracting information from the sender's email or IP address during email transmission and using that information to customize how the SPF record applies [13]

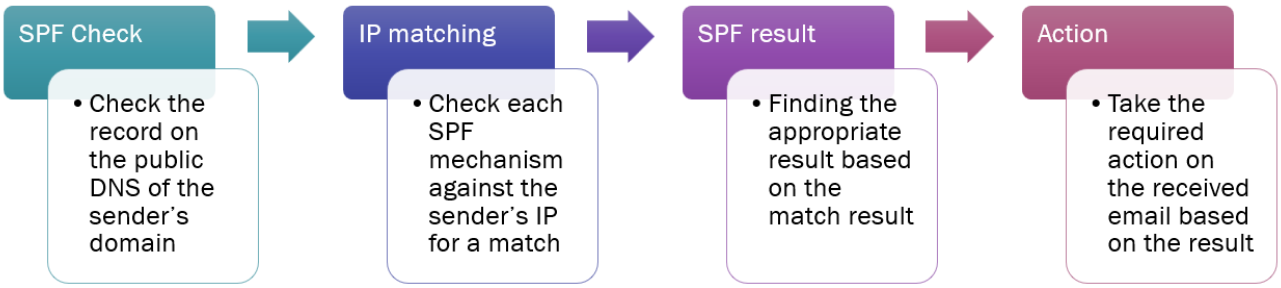

Fig. 1: SPF flow

Macros can be used to:

- Whitelist specific IP addresses or ranges
- Restrict third-party services to a single IP address
- Keep an audit log of whitelisted IP addresses
- Practical examples show how to effectively implement SPF macros in policies.

The article [14] outlines how SPF macros can be used effectively to whitelist IP addresses, IP ranges, and third-party services. Macros allow an unlimited number of IP addresses to be whitelisted while keeping the policy concise. They enable fine-grained control by restricting third-party services to approved IP addresses. Macros also permit maintaining an audit log of whitelisted IP addresses so administrators know the purpose of each authorized address.

B. SPF Vulnerabilities

The authors of [13] discuss the discovery and remote detection of vulnerabilities in the libSPF2 library. Through manual code inspection, they found two issues: a sprintf overflow when encoding non-ASCII characters and a buffer overflow that allowed arbitrary length.

The researchers were able to remotely detect the issues by observing the DNS queries generated when evaluating SPF records. One of the overflows uniquely modified outgoing DNS queries, making them detectable. Properly implemented macros reverse and truncate as specified, but the vulnerable libSPF2 implementation overwrote macro expansions, resulting in malformed DNS queries.

The malformed queries resulting from one of the overflows allowed the researchers to detect the issues without harming remote systems, by analyzing the domain names in the queries. The queries indicated compliant, non-compliant, or vulnerable libSPF2 behavior.

Researchers concluded that by observing DNS queries for SPF records containing macros, they were able to detect two vulnerabilities in libSPF2. One of the overflows modified the queries in a way that revealed the vulnerable behavior, without any risk to remote systems. This demonstrates a novel remote detection technique for vulnerabilities affecting DNS-based protocols.

IV. DomainKeys Identified Mail (DKIM)

DKIM is an important email authentication framework that aids in verifying the sender's identity and preventing spoofing on a domain. It uses digital signatures to ensure emails originated from the claimed sender and were not altered during the transmission [15]

Figure 2 demonstrates how DKIM works. The domain owner first generates a public/private key pair. The public key is published in a DNS TXT record called the DKIM record, associating the key with the domain. When sending an email, the server calculates cryptographic hashes of the email parts, like the body, headers, and full message. It then signs the hash using the private key and inserts the DKIM signature into the headers. This signature allows recipients to verify the email's integrity. When receiving an email, the server obtains the public key from the DKIM record. It uses the public key to decrypt the signature in the headers, and also, the recipient generates their own hash value and verifies whether they are matching. This process allows for validating the integrity of the message. If verification succeeds, the receiver knows the email came from the claimed sender and was not altered.

The DNS record syntax tags include the key type, acceptable hash algorithms, and the public key, whereas the digital signature tags include the signature algorithm, canonicalization algorithm, selector value, claimed sender's domain, headers covered by the signature, length of signed body text, the hash of signed body text, and actual signature value.

The researchers of [15] gathered data on DKIM deployment from two sources. First, they collected passive DNS datasets from 2015 to 2020 containing DNS queries for DKIM records. They extracted relevant DKIM records by matching specific domain patterns. Second, they obtained an email server log from March to October 2020 with 464 million DKIM signatures. They parsed domains and selectors from the signatures to look up the corresponding DKIM records.

By analyzing data from both sources, the researchers identified trends in DKIM deployment over time and uncovered issues with DKIM management. The passive DNS data provided a long-term view of changes to DKIM records, showing how deployment evolved. The email log allowed them to verify actual DKIM records in use. Additionally, combining the long-term perspective on DKIM record changes from passive DNS with a snapshot of real-world DKIM usage from email signatures enabled the researchers to assess DKIM adoption trends over time and detect issues impacting effectiveness.

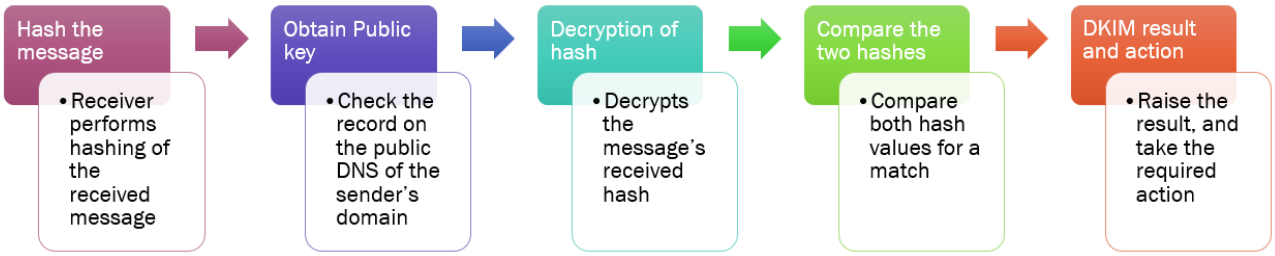

Fig. 2: DKIM flow

V. DMARC Framework

DMARC is a framework that operates with SPF and DKIM to provide email authentication and security. It enables email domain owners to establish policies for email authentication and obtain feedback about how their emails are being managed. The DMARC policy can be set to "none," "quarantine," or "reject" to deal with DMARC failure emails. The administrator of the sender domain must post the SPF record and public key for DKIM authentication on the DNS server and configure them appropriately to pass the DMARC authentication. DMARC reports provide helpful information to the sender domain's administrator, such as the sender's domain, IP addresses, and the effectiveness of the DMARC policy. The DMARC verification fails when the Header-From domain of the sender is both not aligned with the Envelope-From domain, and not aligned with the DKIM signature domain [7].

Thus, DMARC is considered a comprehensive solution because it operates in conjunction with SPF and DKIM to ensure email security. The DMARC framework allows email domain owners to set policies and receive feedback on their emails through the reports. By analyzing those DMARC reports, administrators can identify ways to enhance their email authenticity, improve SPF and DKIM configurations, and also prevent spoofed emails that abuse their domain. Therefore, implementing DMARC, alongside SPF and DKIM, can help organizations to protect against email-based attacks and keep their communications secure and trustworthy to their recipients.

VI. Results and Findings

The study found that while SPF is useful for straightforward implementation and ensuring that incoming emails originate from legitimate sources, it has several drawbacks: SPF only checks the IP address of the sending server, and therefore, it only provides proof of identity for the sender, but unable to verify email content itself. In contrast, DKIM adds digital signatures to email headers. This verifies the sender's authenticity and prevents tampering, providing an additional security layer SPF lacks.

In addition to that, SPF requires all authorized email servers to be listed in DNS records, which is challenging for complex email infrastructures. While on the other hand, DKIM requires a one-time configuration and typically no continuous changes, unless the rotating of the public key is required.

TABLE I: SPF DRAWBACKS AND DKIM RESOLUTIONS

SPF Drawback	DKIM Solutions
Forwarded emails fails SPF	Forwarded emails passes DKIM
Provides authentication only	Provides authentication and integrity
Auto-generated emails fail SPF	Auto-generated emails pass DKIM
Continuous changes are required	Typically, one-time configuration

There are also some more issues SPF faces that are addressed by DKIM. The first one is that forwarded emails always fail SPF due to different IP addresses, however, DKIM signatures can survive forwarding, resulting in emails passing DMARC.

Another challenge for SPF is that auto-generated emails like out-of-office alerts, typically fail SPF but still pass DKIM since DKIM signatures ensure messages have not been tampered with during this forwarding.

Though SPF macros can address some drawbacks, and aid admins in more security, they remain complicated, underused, and also undocumented properly.

In conclusion, while SPF and DKIM are both important, DKIM is considered more crucial due to stronger protections against spoofing. SPF has limitations like only providing identity proof and insufficient against auto-generated and forwarded emails, which DKIM addresses through its ability to authenticate and check the integrity of emails.

Table I summarizes some of the SPF's challenges and how DKIM remediate them.

Conclusion

In the realm of email security, Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are both essential frameworks for authentication. While SPF is simpler to implement, it requires listing all authorized senders in DNS records. On the other hand, DKIM provides stronger protection due to its use of digital signatures. Our research has found that DKIM is more effective in authenticating emails due to its more comprehensive approach.

In addition to SPF and DKIM, implementing the Domain-based Message Authentication, Reporting, and Conformance (DMARC) framework can further improve email security and resilience against email impersonation. DMARC enforces alignment and provides actionable reports that complement SPF and DKIM.

However, email authentication technologies are constantly evolving, and organizations must monitor new developments and upgrade configurations as needed to stay ahead of threats. Adopting additional techniques such as machine learning, content analysis, and automated header analysis could further enhance protections. These areas are potential subjects for future research in email security.

REFERENCES

[1] S. Maroofi, M. Korczynski, and A. Duda, "From defensive registration to subdomain protection: Evaluation of email anti-spoofing schemes for high-profile domains," Traffic Monitoring and Analysis, 2020.

[2] P. Chauhan and A. Shah, "Email spoofing: In today's era," Research Square, 11 2022.

[3] A. Portier, H. Carter, and C. Lever, "Security in plain txt: Observing the use of dns txt records in the wild," in Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden, June 19–20, 2019, Proceedings 16. Springer, 2019, pp. 374–395.

[4] Y. Al-Hamar, H. Kolivand, M. Tajdini, T. Saba, and V. Ramachandran, "Enterprise credential spear-phishing attack detection," Computers & Electrical Engineering, vol. 94, p. 107363, 2021.

[5] L. E. Hughes, "Issue and manage s/mime secure email certificates," in Pro Active Directory Certificate Services: Creating and Managing Digital Certificates for Use in Microsoft Networks. Springer, 2022, pp. 359–404.

[6] H. P. Shitole and S. Divekar, "Secure email software using e-smtp," Int. Res. J. Eng. Technol, pp. 3967–3971, 2019.

[7] K. Konno, N. Kitagawa, and N. Yamai, "False positive detection in sender domain authentication by dmarc report analysis," in Proceedings of the 3rd International Conference on Information Science and Systems, 2020, pp. 38–42.

[8] C. Wang and G. Wang, "Revisiting email forwarding security under the authenticated received chain protocol," in Proceedings of the ACM Web Conference 2022, 2022, pp. 681–689.

[9] V. Kontinen, "Preventing email forgery in finland: Research on the current spf and dmarc implementations," Master's thesis, Dublin, National College of Ireland, 2020.

[10] R. R. Kolagotla, "Enhancing the security of an e-mail by dmarc and dns data," Ph.D. dissertation, Dublin, National College of Ireland, 2021.

[11] S. Kanhere, V. T. Patil, S. Sural, and M. S. Gaur, Eds., A Toolkit for Security Awareness Training Against Targeted Phishing, ser. Lecture Notes in Computer Science, Cham, 2020, vol. 12553, p. 137–159.

[12] G. M. Kahraman, "Characterizing sender policy framework configurations at scale," Master's thesis, University of Twente, 2020.

[13] N. Bennett, R. Sowards, and C. Deccio, "Spfail: discovering, measuring, and remediating vulnerabilities in email sender validation," in Proceedings of the 22nd ACM Internet Measurement Conference. Nice France: ACM, Oct 2022, p. 633–646.

[14] J. Scaife, "Using spf macros to solve the operational challenges of spf — jamieweb.net," 2020, [Accessed 03-Jun-2023]. [Online]. Available: https://www.jamieweb.net/blog/using-spf-macros-to-solve-the-operational-challenges-of-spf/

[15] C. Wang, K. Shen, M. Guo, Y. Zhao, M. Zhang, J. Chen, B. Liu, X. Zheng, H. Duan, Y. Lin et al., "A large-scale and longitudinal measurement study of DKIM deployment," in 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 1185–1201.