SocketLabs
the science of hitting the inbox

Your In-Depth Guide to Email Authentication

An Email **Best Practices** Whitepaper

WHAT YOU WILL LEARN

- **What is email authentication?**
- **Why is email authentication necessary?**
- **A brief history of email authentication**
- **What is Sender Policy Framework (SPF) authentication?**
- **What is DomainKeys Identified Mail (DKIM)?**
- **What is Domain-based Message Authentication, Reporting & Conformance (DMARC)?**

CONTENT

Introduction

The objective of this paper is to provide a brief overview and description of the most commonly used authentication practices and methodologies in today's email industry. This guide will cover the main topics and points of discussion with regard to the mainstream standards used today for authenticating email.

The Growth of Email Spam

In **an email and spam data report by Cisco Systems**, it was revealed that over 400 billion spam email messages are sent each day – approximately 85% of worldwide email. This alarmingly high rate of spam being sent out is the direct result of an increase in spamming tactics like phishing, botnets, social engineering, and reputation hijacking. Because spam and other cyber security issues continue to increase year after year, technology integrators have turned to alternative methods to secure their communications. Email authentication is one such method.

Email Spoofing and Phishing

One of the main benefits of using email authentication is that it dramatically reduces the use of one of the most malicious types of email mischief: **phishing (also known as spoofing).** This is where a user will receive an email that appears to originate from one source, when in reality it was sent from another source. Email spoofing is a classic spammer tactic used to coerce unsuspecting users into disclosing secure or confidential information without their knowledge or authorization.

A classic example of email spoofing that still occurs today are emails purportedly from a bank or financial institution, alerting the user that their account has been compromised and, in order to resolve the situation, they must click the link in the email to log into their account. Both the link, as well as the sender information have been spoofed or forged to look as if the message came from the purported bank.

What is Email Authentication?

Email authentication is a multi-method approach to securing email communications.

Generally defined, email authentication is a multi-method approach to securing email communications using either IP based and/or cryptographic standards. Email senders create a public record that verifies their sending domain is authorized to send email from a particular IP address or mail server. Receiving Internet Service Providers, ISPs, can then use this record to validate the legitimacy of the sender and the messages they are sending. Additionally, ISPs commonly use this validation along with other metrics to determine the reputation of a sender, and ultimately if they will deliver the sender's messages.

There are currently two primary methods that are used to authenticate email: Sender Policy Framework (SPF), and DomainKeys Identified Mail (DKIM). In addition to SPF and DKIM, there is Domain-based Message Authentication, Reporting & Conformance, aka DMARC, which is not an authentication method but rather a policy built atop SPF and DKIM that works to further the effectiveness of both methods. While a sender can authenticate using SPF and/or DKIM with DMARC alignment, an ISP may choose to only verify one or more of them.

The History of SPF Authentication (Sender Policy Framework)

The concept of email authentication dates back as far as 1997. Multiple specifications and proposals had been submitted to the Internet standards community for acceptance, including a set of six "designated sender" proposals called Lightweight MTA Authentication Protocol (LMAP). Sender Policy Framework (SPF) was one of these proposals.

In April 2006, the SPF RFC standard was published.

Sender Policy Framework evolved when two LMAP proposals, "Reverse MX" (RMX) and "Designated Mailer Protocol" (DMP) were merged together. With much collaboration from the email and internet industry, the specification was approved and, in April 2006, the SPF RFC standard was published. Originally, SPF stood for "Sender Permitted From" and was sometimes also called SMTP+SPF. However, in February 2004, the name "Sender Policy Framework" was finalized.

The History of DKIM Authentication (DomainKeys Identified Mail)

With multiple authentication approaches in development across the Internet (at the time), Yahoo also submitted their contribution by creating a new standard that utilized cryptographic signatures to authenticate outbound messages. In partnership with Sendmail, Yahoo implemented this standard on their servers in November 2004. Within days of implementation, Earthlink began testing DomainKey verification process. Yahoo developed DomainKeys (and implemented on their own systems) in the hopes that it would create a broader adoption of the technology, and ultimately stem the rise of spam and phishing attacks through email.

At about the same time, Cisco also created a cryptographic email authentication standard called Identified Internet Mail (IIM). Very similar to DomainKeys, a cryptographic signature was embedded into the email message, however there were additional authorization metrics that were not part of the DomainKeys standard.

Eventually the two standards were merged, and in May 2007, the DomainKeys Identified Mail (DKIM) RFC standard was published.

In May 2007, the DomainKeys Identified Mail (DKIM) RFC standard was published.

What is Sender Policy Framework (SPF) Authentication?

Sender Policy Framework (SPF) is an open email authentication standard used to prevent sender address forgery. Using DNS records, it allows senders to publish a list of IP addresses, or server names that are authorized to send on their behalf. SPF authenticates the domain used in the “envelope” or return-path email address. This address is used during the transport of the message (from mail server to mail server,) and is primarily used to “bounce” or return undeliverable mail back to the sender. It is an internal address and is typically not displayed by mail programs.

The return-path address is an internal address and is typically not displayed by mail programs.

Creating and Publishing SPF Records

A sender will publish an SPF record for a given domain. This record is a DNS text record that uses different “mechanisms” to identify what hosts are authorized to send on behalf of that domain. These mechanisms include: IP addresses, A records, MX records, and PTR records. SPF records can also include other SPF records as mechanisms to identify authorized hosts.

The following is an example of an SPF record:

Example: example.com. TXT “v=spf1 a mx ip4:192.168.1.1 include:example.net –all”

Item	Description
example.com	The sending domain that is publishing the SPF record
TXT	Specifies that this is a DNS text record
v=spf1	Tag that specifies that the text record is using SPF
a	Specifies that the A record of example.com is an authorized host to send on behalf of example.com
mx	Specifies that the MX record of example.com is an authorized host to send on behalf of example.com
ip4:1.2.3.4	Specifies that the IP address 1.2.3.4 is authorized to send on behalf of example.com
include:example.net	Specifies that the mechanisms found in the SPF record of example.net can also be authorized to send on behalf of example.com
-all	Specifies that the hosts included in the SPF record are the only hosts allowed to send on behalf of example.com – all other hosts are not authorized

A key part of an SPF record is the "all" mechanism. It is used as the rightmost mechanism, and is also what determines how complete the record is. In the above example, a dash (-) "qualifier" is used to signify that only the hosts included in the respective SPF record are authorized for that domain. There are other qualifiers that can be used as well. For example:

To signify that there are other hosts that can possibly send, or are in transition to do so on behalf of the domain, the SPF record would be terminated with "~all". To signify that it is not known if any of the hosts are authorized to send on behalf of the domain, the SPF record would be terminated with "?all".

Despite its seemingly cut and dry functionality, the "all" mechanism marks one of the most non-universally adopted aspects of the SPF standard. Implementations over the years by different mailbox providers have treated each of these qualifiers very differently. Some mail systems reject messages from domains when the IP isn't in the record with a "-all" terminating it, but most will still accept the messages.

Authenticating SPF Records

ISPs that authenticate inbound email using the SPF record will check the mechanisms in order until one is found that authenticates the domain successfully. If a mechanism is found that passes, the ISP can then accept the message for delivery. If a mechanism is found that is either not valid, or not definitive in what hosts are authorized to send on behalf of the respective domain, the ISP can opt to either accept the message but mark as invalid, or to not deliver the message at all. The validity of the message can be determined through a result outcome that is recorded in the "Authentication Results" header of the email. **A few common results are as follows:**

- spf=pass
- spf=temperror
- spf=fail

What is DomainKeys Identified Mail (DKIM) Authentication?

DomainKeys Identified Mail (DKIM) is the successor to Yahoo DomainKeys that provides more flexibility and security than its predecessor. It is an email authentication mechanism that allows the recipient mail server to check if a message has been altered during transit. This is done by the recipient server, checking and verifying an encrypted signature left on the message by the sending server to ensure the message arrived in the same form that it was sent.

An email authentication mechanism that allows the recipient mail server to check if a message has been altered during transit.

DKIM Message Configuration and Signing

Within a DKIM signature, there are a number of tags available that authenticate different aspects of an email message.

Consider the following sample email and accompanying DKIM signature:

Example:

```
DKIM-Signature:v=1; a=rsa-sha256; d=example.net; s=v1;
c=simple/simple;

q=dns/txt; i=@example.org; t=1231537955;
h=Received:Date:From:Reply-to:To:Message-ID:Subject;
bh=YXMEQF450z/x8OwmM2cXB0sn8pQ=;
b=V4eYEm7zx1aNgbBaTgljjJ6lvU7xCEDeg2lE5KXMRZW...
HSkBHIKnbICHCu3CTxqe8ys=;
Received: from [192.168.1.1]; Fri, 09 Jan 2009 13:52:35 -0800
Date: Fri, 9 Jan 2009 13:52:30 -0800 (PST)
From: Example-Announce
Reply-to: announce@example.net
To: john@example.com
Message-ID: <12988903062.1231537950554@example.net>
Subject: January Announcements
```

What is DomainKeys Identified Mail (DKIM) Authentication?

(continued)

Following is a description of the tags used in the above example:

Item	Description
v	The version of the DKIM specification being used to sign the message
a	The algorithm used to generate the signature
d	The domain of the signing entity
s	The selector used in the public key
c	The canonicalization algorithm – or the method by which the headers and content are prepared for presentation to the signing algorithm
q	The query method(s) used to retrieve the public key
i	The identity of the user or agent (e.g., a third party) on behalf of which this message is signed
t	Signature timestamp. The format is UNIX time format
h	A colon-separated list of header field names that identify the headers in the email message — the values in this tag MUST contain the complete list of headers in the order presented to the signing algorithm
bh	The hash of the canonicalized body part of the message
b	The signature data or public key, encoded as a Base64 string

What is Domain-based Message Authentication, Reporting & Conformance (DMARC)?

DMARC is not an authentication protocol, per se, but rather a security policy for domain owners built on top of existing SPF and DKIM authentication technologies. The primary function of DMARC is to align the "From" address domain of a message with either SPF and/or DKIM and to determine what action is taken on unauthenticated email. DMARC contemporaneously works to standardize and incentivize the use of SPF & DKIM authentication.

DMARC requires that a message must have a passing authentication mechanism (either SPF or DKIM) that aligns to the "From" address domain. A message will fail DMARC if SPF doesn't pass or is unaligned and DKIM doesn't pass or is unaligned. More specifically, to pass DMARC an email must:

1. Pass either SPF or DKIM authentication
2. The authentication method that "passes" must also be in alignment to the "From" address domain

For example, a message can have a valid DKIM signature, but if the DKIM signing domain is unrelated to the domain of the "from address", there is no alignment and DMARC will be considered a failure (assuming there is no validated and aligned SPF). For SPF alignment, the "From" address field in the email's message header must match the domain name in the "Envelope From" used during SMTP communication.

Another valuable resource DMARC provides is reporting through a product known as DMARC reports. While the reports do not give much insight into the actual emails themselves, they provide a wealth of data-driven visibility into the overall status of your email program as it relates to authentication results, domain alignment, potential email threats, and more.

DMARC is not an authentication protocol, per se, but rather a security policy.

Adoption of Email Authentication

As stated earlier, there has been no general-adoption of one specific email authentication standard by mailbox providers and recipients. SPF and DKIM authentication started off with slow adoption from major mailbox providers however now, they are widely supported by industry leaders today. DMARC, being a little bit later to the game, is also catching on as a widely supported protocol throughout the email industry.

Conclusion

As spam and online threats continue to plague user inboxes, internet and email providers will continue to aggressively take steps to protect their users by implementing the latest technologies and standards available. Email authentication is a large part of this movement.

With nothing but year-over-year increases in spam and other malicious email tactics, email senders are encouraged to incorporate the latest authentication methods into their email infrastructures. By doing so it will not only show that their email messages are authentic, but will also show that they are accountable in their sending practices, and will gain more trust in the eyes of the email receiving community.

Sending high volume email through an email service provider like SocketLabs means you will automatically have the ability to send your email with the latest authentication and encryption techniques across multiple mail streams.

Contact us today to learn more, or visit our website at www.socketlabs.com.

About SocketLabs

SocketLabs is a B2B technology firm that provides flexible SaaS and on-premises solutions for solving a variety of complex email delivery challenges for both transactional and marketing messages. We are a pioneer in the Email Service Provider (ESP) market with a decade-long track record of excellence. Our unique, proprietary mail transfer agent (MTA) technology is trusted by clients around the globe who invigorate their SaaS platforms, mobile apps, and custom applications by “plugging in” to an unmatched email experience. Our founders have been creating cutting-edge email solutions for over 20 years and have built a customer support organization that considers “responsiveness and satisfaction” as our key performance objectives.

Email us!

support@socketlabs.com

Call us!

USA:
800.650.1639
International:
484.418.1285

Chat with us!

www.socketlabs.com/chat