Name: Raviteja S Jyothi

Assignment
Topic: SPF, DKIM and DMARC

1) What is Sender Policy Framework (SPF)?

SPF is a form of email authentication that defines a process to validate an email message that has been sent from an authorized mail server in order to detect forgery and to prevent spam. The owner of a domain can identify exactly which mail servers they are able to send from with SPF protocols.

Advantages and Potential Drawbacks of SPF

SPF is adept at preventing phishing. Without it, SMTP would expose your address to those who could forge it for spamming purposes. With SPF in place, when a hacker attempts to initiate an email from your address, the receiving server's SPF security detects it and identifies it as invalid. Using SPF shows your organization is committed to protecting against cyber threats, a sign that positively impacts your sender reputation.

When a user outside your domain forwards an email that originated from you, the delivery may not occur because of a mismatch between the IP record and the SPF record. Many mail exchange and transfer agents are now using the Sender Rewriting Scheme (SRS) to enhance the deliverability of email forwards. The SPF record also must reflect any changes in third-party email services providers to ensure they correspond for deliverability.

How SPF Works?

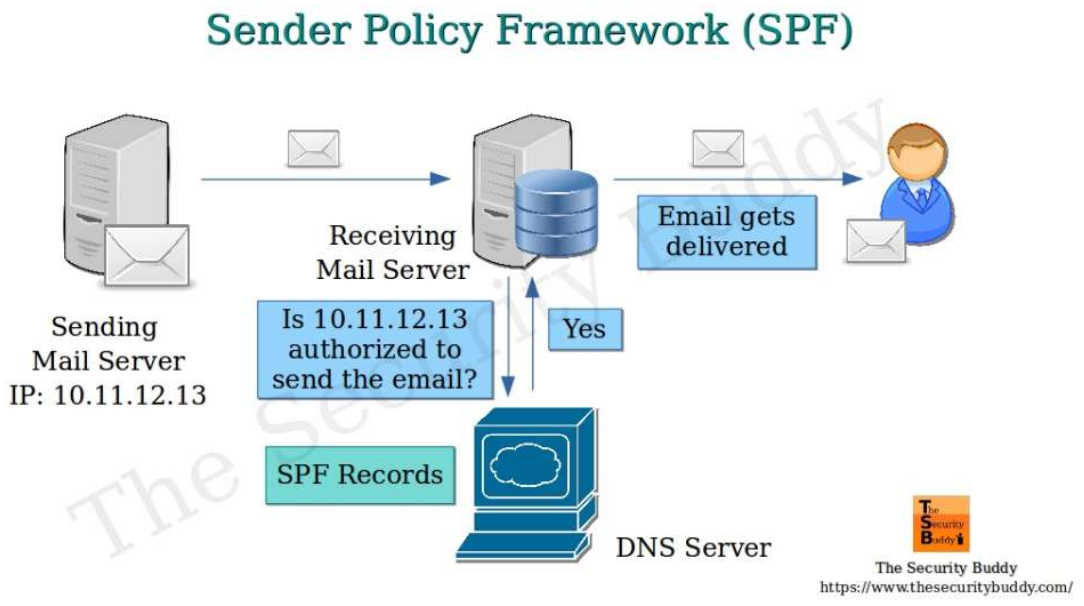
At the most basic level, SPF email establishes a method for receiving servers to verify that incoming email from a domain was sent from a host authorized by that domain's administrators. The following three steps outline how SPF works:

1. A domain administrator publishes the policy defining mail servers that are authorized to send email from that domain. This policy is called an SPF record, and it is listed as part of the domain's overall DNS records.

2. When an inbound mail server receives an incoming email, it looks up the rules for the bounce (Return-Path) domain in DNS. The inbound server then

compares the IP address of the mail sender with the authorized IP addresses defined in the SPF record.

3. The receiving mail server then uses the rules specified in the sending domain's SPF record to decide whether to accept, reject, or otherwise flag the email message.



2) What is DomainKeys Identified Mail (DKIM)?

DKIM is a form of email authentication that allows an organization to claim responsibility for a message in a way that can be validated by the recipient. DKIM uses "public key cryptography" to verify that an email message was sent from an authorized mail server, in order to detect forgery and to prevent delivery of harmful email like spam.

Advantages and Potential Drawbacks of DKIM Authentication

DKIM email's primary advantage is its ability to protect against both spoofing and phishing attacks. The authentication appears within the message itself to prevent forgery and safeguard users from replying to illegitimate emails with sensitive personal data. Both spoofing and phishing have the potential to harm your sending reputation and future deliverability, so protection against the two is beneficial.

Creating an email with DKIM has the same potential disadvantage as SPF when it comes to forwarding messages. For example, an email that automatically routes from an office computer to a user's mobile may appear as illegitimate to the receiving server. Many popular email services have resolved this issue. One other challenge that may present itself is a DKIM that is too short in length. With more support for longer keys, shorter ones may not pass authentication.

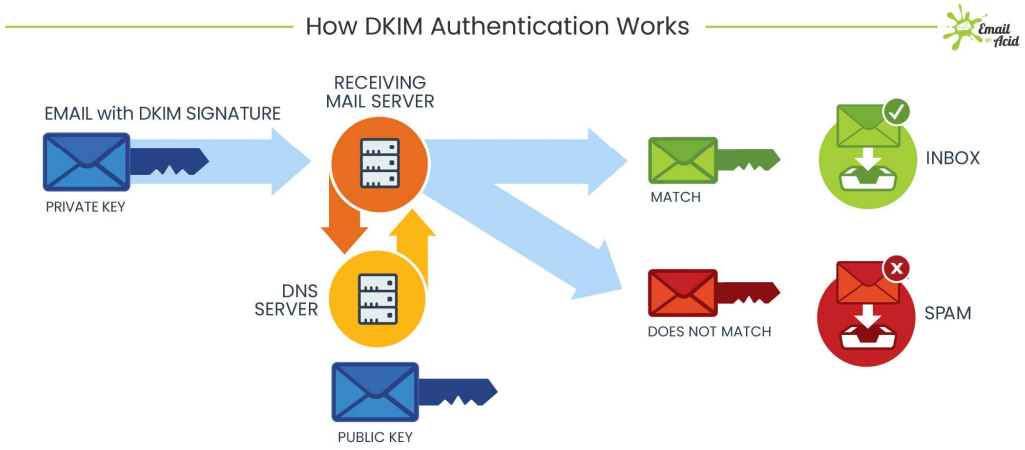
How DKIM Works?

Simply put, DKIM works by adding a digital signature to the headers of an email message. This signature can then be validated against a public cryptographic key that is located in the organization's DNS record.

The domain owner publishes a cryptographic key. This is specifically formatted as a TXT record in the domain's overall DNS record.

After a message is sent by an outbound mail server, the server generates and attaches the unique DKIM signature to the header of the message.

The DKIM key is then used by inbound mail servers to detect and decrypt the message's signature and compare it against a fresh version. If the values match, the message can be proved authentic, and unaltered in transit, and therefore, not forged or altered**.**



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

DMARC, which stands for **Domain-based Message Authentication, Reporting, and Conformance** is an email protocol; that when published for a domain; controls what happens if a message fails authentication tests (i.e. the recipient server can't verify that the message's sender is who they say they are).

Via those authentication checks (SPF & DKIM) messages purporting to be from the sender's domain are analyzed by receiving organizations and determine whether the message was really sent by the domain in the message. DMARC essentially handles the question of what should happen to messages that fail authentication tests (SPF & DKIM). Should they be Quarantined? Rejected? or should we let the message through even if it failed to prove its identify? Long story short, DMARC acts as a gatekeeper to inboxes and if setup properly can prevent phishing and malware attacks from landing in the inbox.

Advantages and Potential Drawbacks of DMARC Authentication

- Security. Disallow unauthorized use of your email domain to protect people from spam, fraud, and phishing.
- Visibility. Gain visibility into who and what across the Internet is sending email using your email domain.
- Delivery. Use the same modern plumbing that mega companies use to deliver email.
- Identity.

How Does DMARC Work?

DMARC is used in conjunction with SPF and DKIM (the authentication tests we mentioned earlier) and these three components work wonders together to autenticaticate a message and determine what to do with it. Essentially, a sender's DMARC record instructs a recipient of next steps (e.g., do nothing, quarantine the message, or reject it) if suspicious email claiming to come from a specific sender is received. Here is how it works:

1. The owner of the domain publishes a DMARC DNS Record at their DNS hosting company.

2. When an email is sent by the domain (or someone spoofing the domain), the recipient mail server checks to see if the domain has a DMARC record.

3. The mail server then performs DKIM and SPF authentication and alignment tests to verify if the sender is really the domain it says it is.

   - Does the message have a proper DKIM-Signature that validates?
   - Does the sender's IP address match authorized senders in the SPF record?
   - Do the message headers pass domain alignment tests?

4. With the DKIM & SPF results, the mail server is then ready to apply the sending domain's DMARC policy. This policy basically says:

- Should I quarantine, reject, or do nothing to the message if the message has failed DKIM/SPF tests?

5. Lastly, after determining what to do with the message, the receiving mail server (think Gmail) will send a report on the outcome of this message and all other messages they see from the same domain. These reports are called DMARC Aggregate Reports and are sent to the email address or addresses specified in the domain's DMARC record.