Cyberattack

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows:

- Injection attacks
- DNS Spoofing
- Session Hijacking
- Phishing
- Brute force

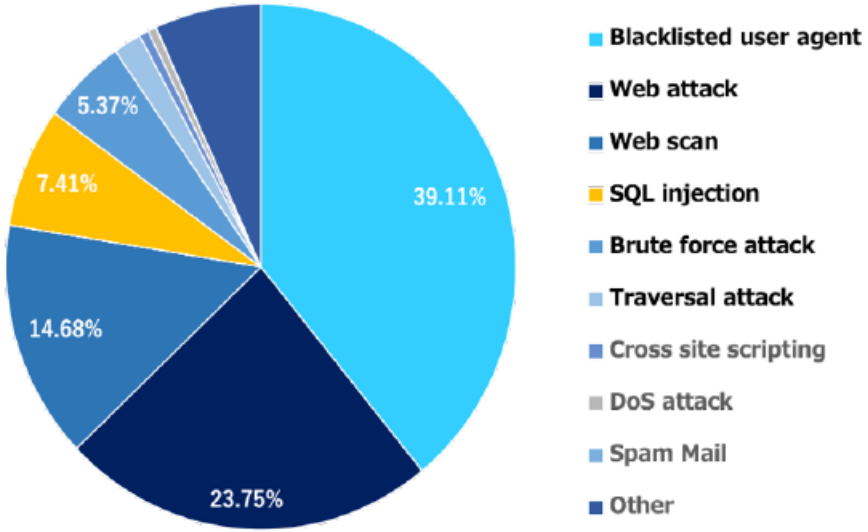
Web-based attacks

- Injection attacks

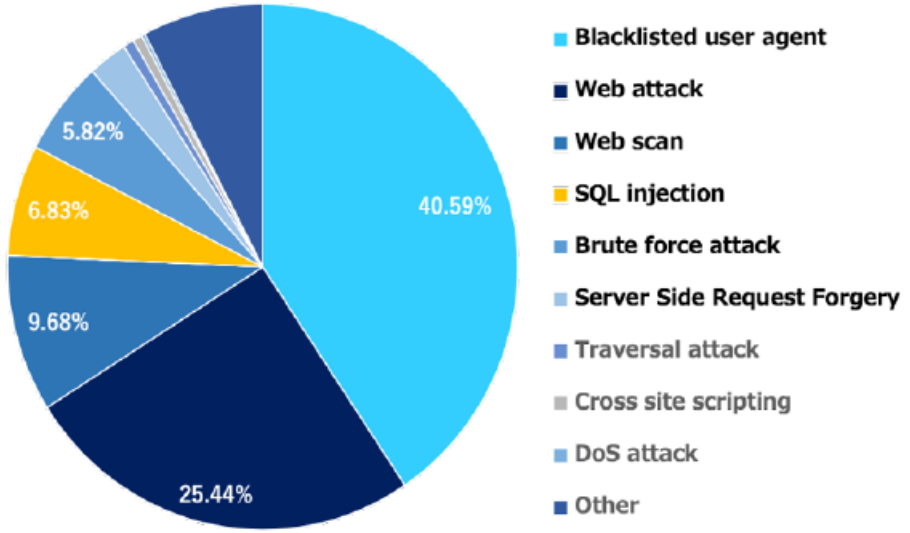
It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example: SQL Injection, code Injection, log Injection, XML Injection etc.

Jan.-June, 2021



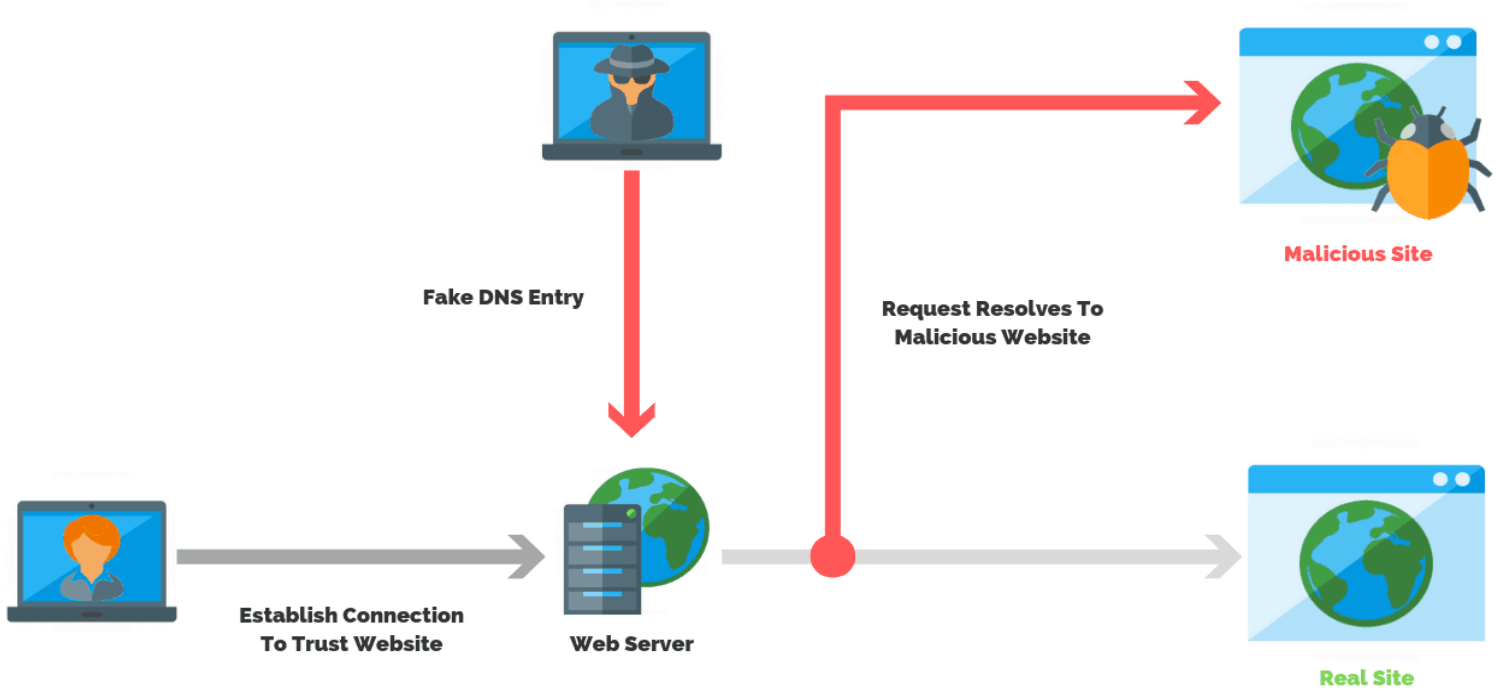
Jan.-June, 2022



Web-based attacks

- DNS Spoofing

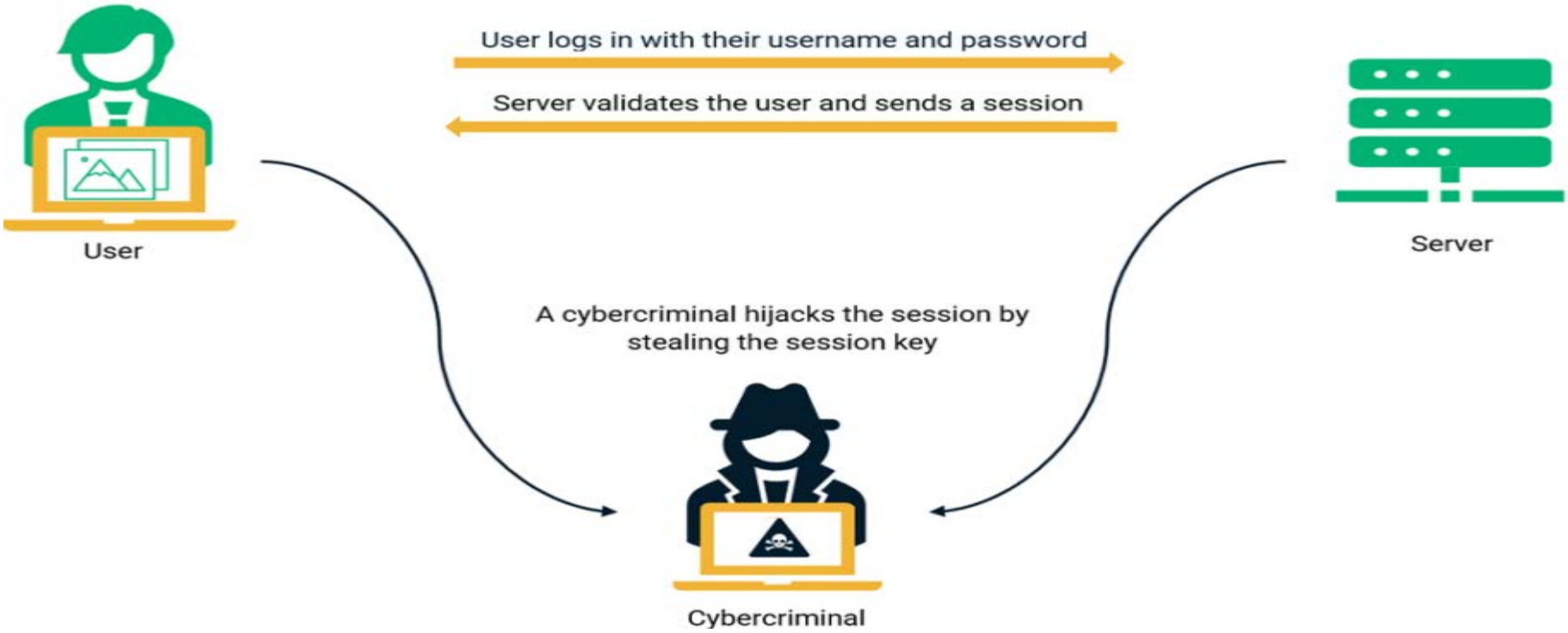
DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.



Web-based attacks

- Session Hijacking

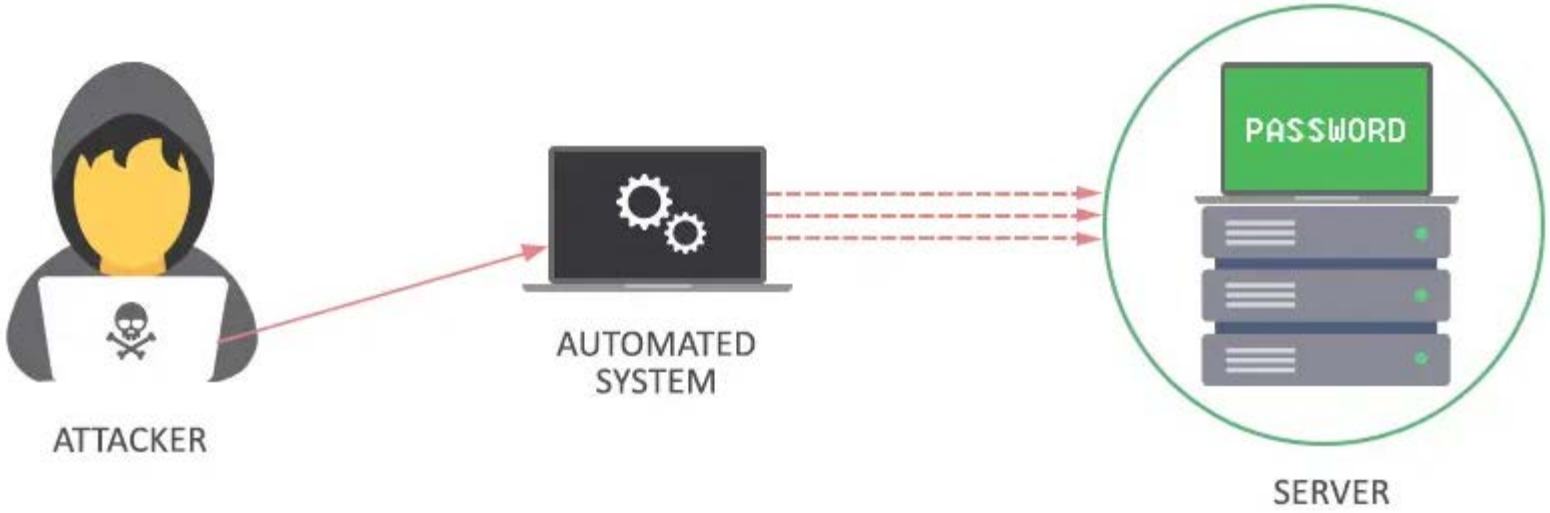
It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.



Web-based attacks

- Brute force

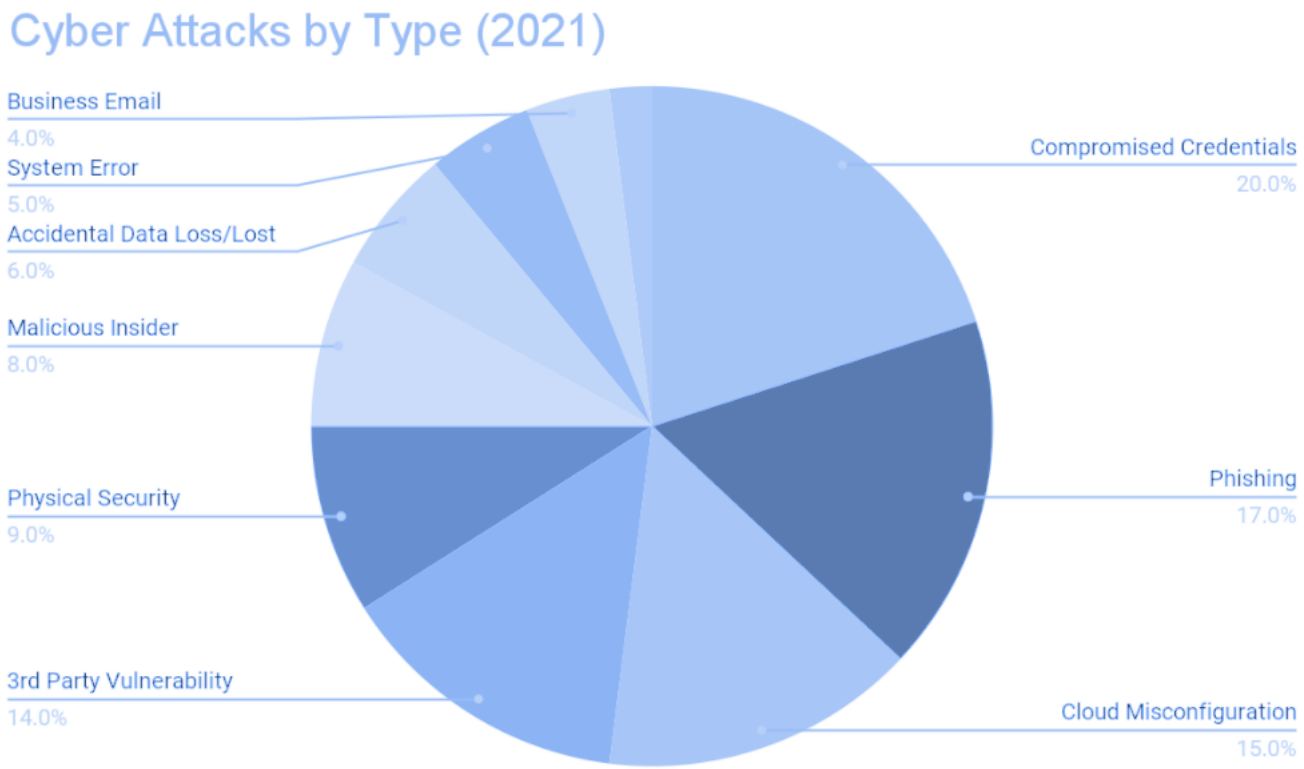
It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.



Web-based attacks

- Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.



Email Spoofing

Overview

The web relies just upon **trust**. At the point when we click on a connection, **we hope** to go to where it says it will take us. At the point when we enter the secret word, **we hope** to be allowed into a private, **safe spot**. At the point when we contact somebody, **we expect** they are who they say they are. At the point when we make a monetary exchange, **we expect** the cash we send will get to the objective we need.

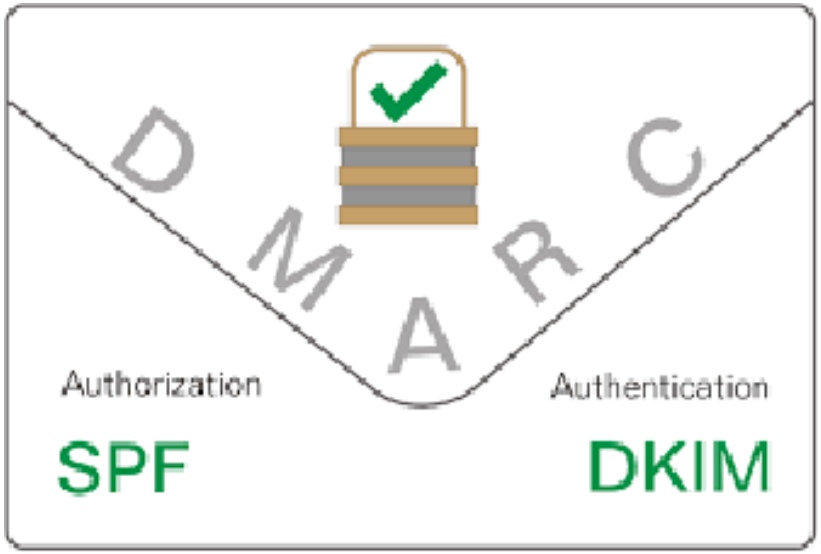
Every one of the assaults depend on some kind of mocking, can exploit somebody's unequivocal or understood trust. As email stays **one of the essential way** for spammers to control individuals and get their own data. Email parodying is the phony of an email that seems to be begun **from one source** when **it was really sent from another source**.

Spammers utilize an email which give off an impression of being from an email address that may not exist. This way the email can't be followed back to the originator. Professing to be somebody can enjoy many benefits.

Counter measures to shield from Email Spoofing

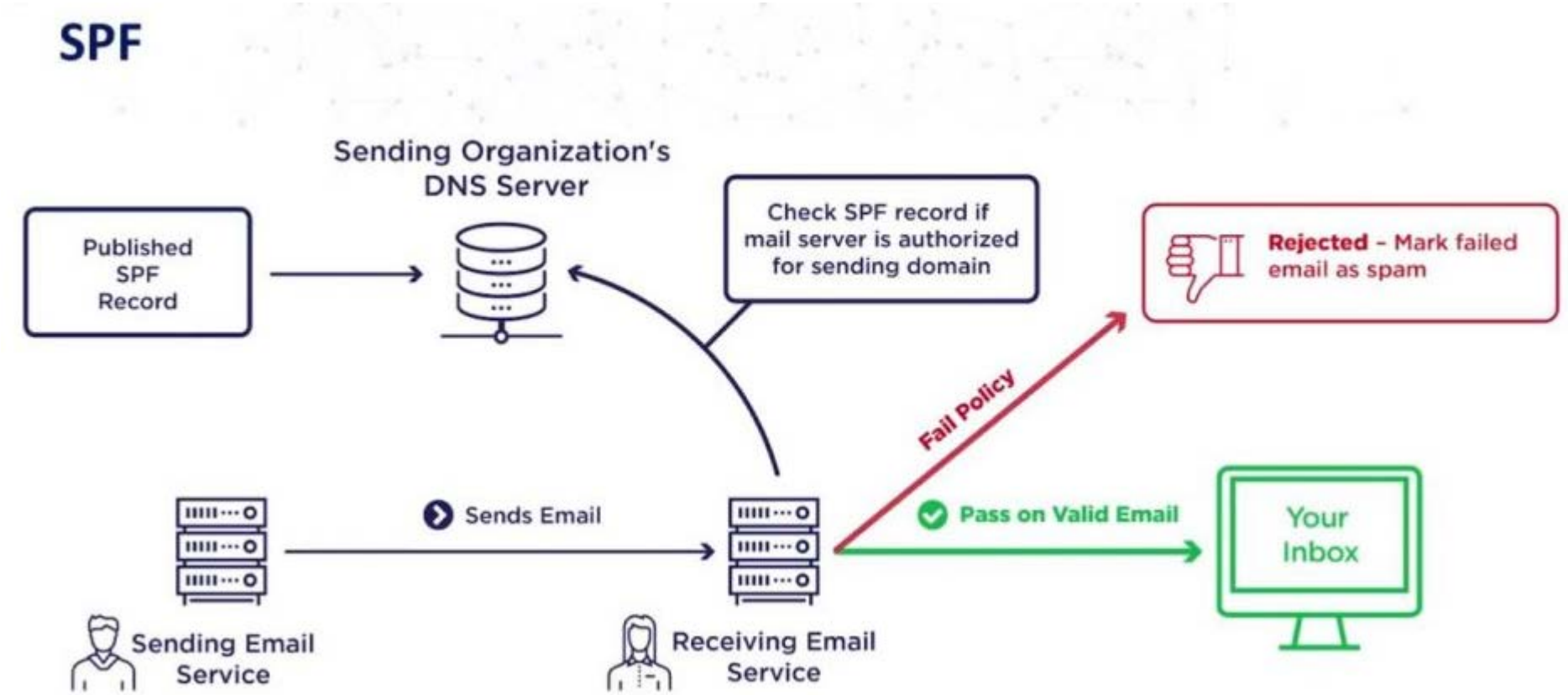
Since the email convention SMTP is a **message based**, security consultant used to be incredibly simple to fake a sender address. There is no security/confirmation with SMTP itself. Most email suppliers are *veterans* of capturing spam before it hits the inbox.

Wouldn't it be vastly improved on the off chance that they had the option to prevent it from being sent in any case?



SPF (Sender Policy Framework)

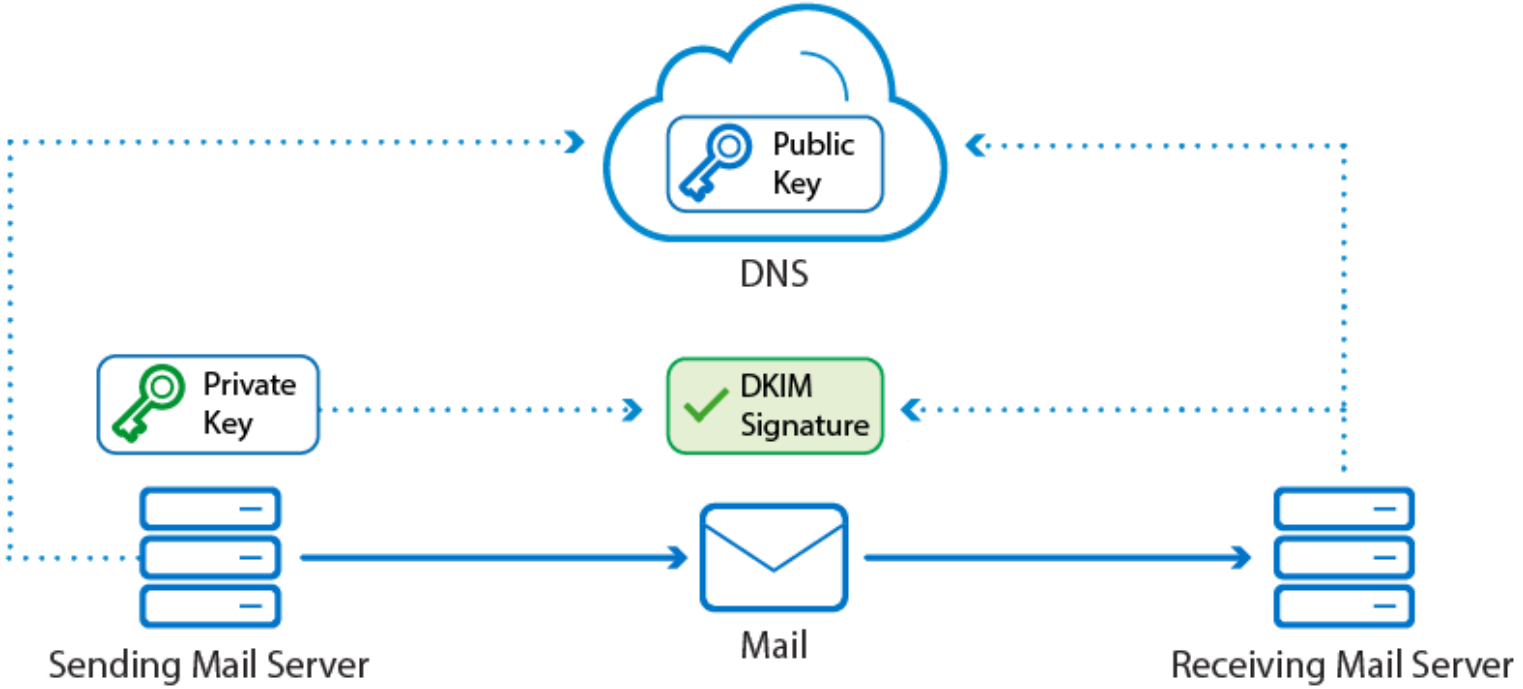
This checks whether a specific IP is approved to send letters from a given area or an email approval convention intended to distinguish and obstruct email fake. This strategy will tell getting mail servers whether an IP is on the rundown for the sending area.



DKIM (Domain Key Identified Mail)

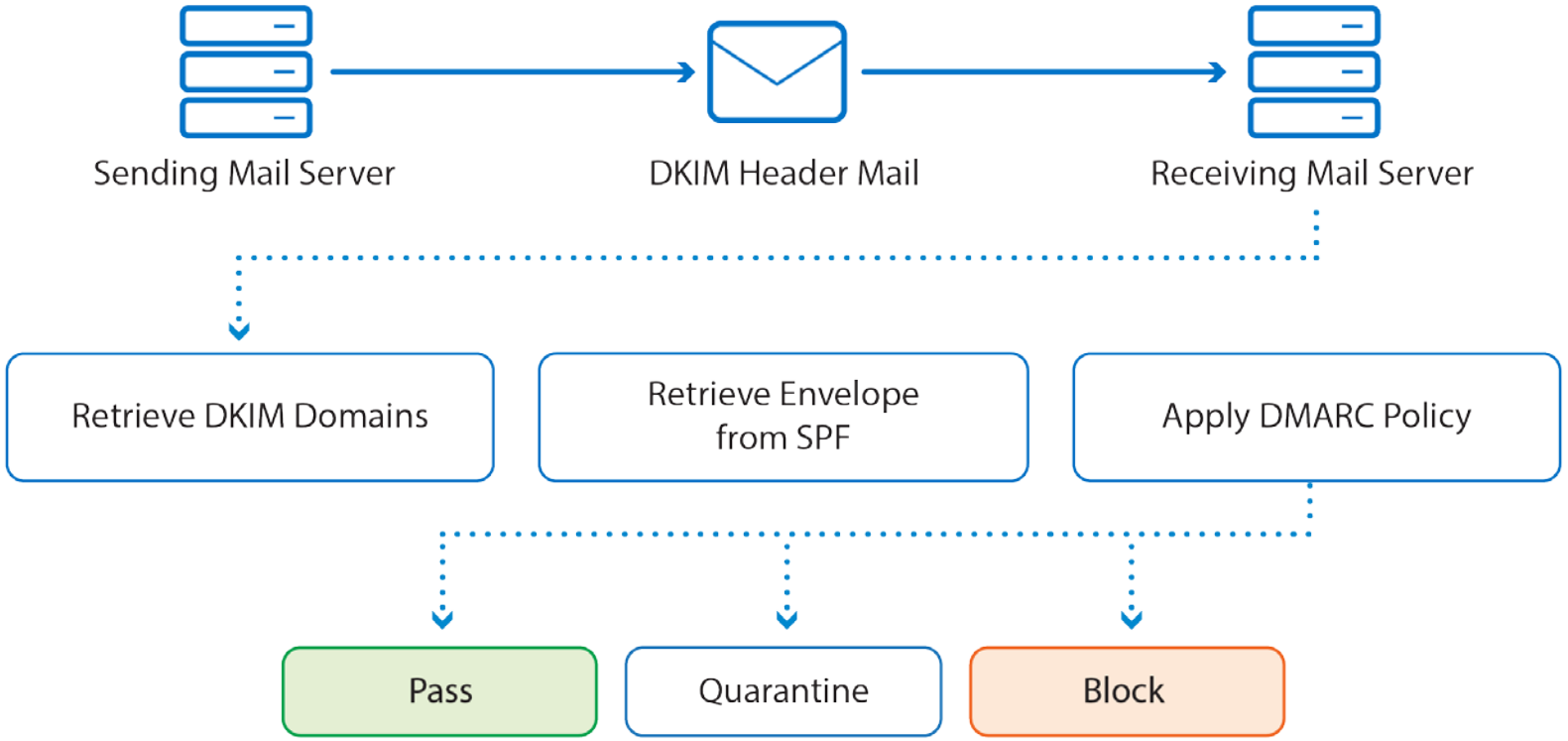
Two Types of Encryption

DKIM is really muddled. This technique utilizes a private and a public key brought by a Mail Transfer Agent (MTA). These are looked at and provided that it is a match the mail will be sent on. Be that as it may, this main signs the predefined parts of the message, the message can be sent and the mark will in any case coordinate. This is known as a replay assault. The issue with DKIM is that it's more hard to carry out.



DMARC (Domain-based Message Authentication, Reporting, and Conformance)

DMARC guarantees that real email is appropriately validating against set up DKIM and SPF guidelines and what moves to make and who to answer to when managing sends that bomb verification, yet sadly **DMARC isn't broadly utilized**.



SPF, DKIM, DMARC - Tools

- **https://dmarcly.com/tools/**
- **https://mxtoolbox.com/**
- **https://www.dmarcanalyzer.com**

Configuration

- How to Setup SPF, DKIM & DMARC Records for Email Authentication:

https://www.stechies.com/setup-spf-dkim-dmarc-records-email-authentication/

- DKIM, DMARC, and SPF: Setting Up Email Security:

https://www.howtogeek.com/devops/dkim-dmarc-and-spf-setting-up-email-security/

- Email Authentication Best Practices:

https://www.cisco.com/c/dam/en/us/products/collateral/security/esa-spf-dkim-dmarc.pdf