Global Information Security Society for Professionals of Pakistan

Topic : Email Security Simplified – Lesson 1

Speaker’s Name : Shahzad Subhani

Agenda

- What is Email Security
- Why Email Security ?
- How Email Works
- Email Protocols ,Ports and Key Terms
- SMTP Response Codes
- Email Related DNS Records
- Typical Email Scenario
- Quick Demonstration for DNS Records

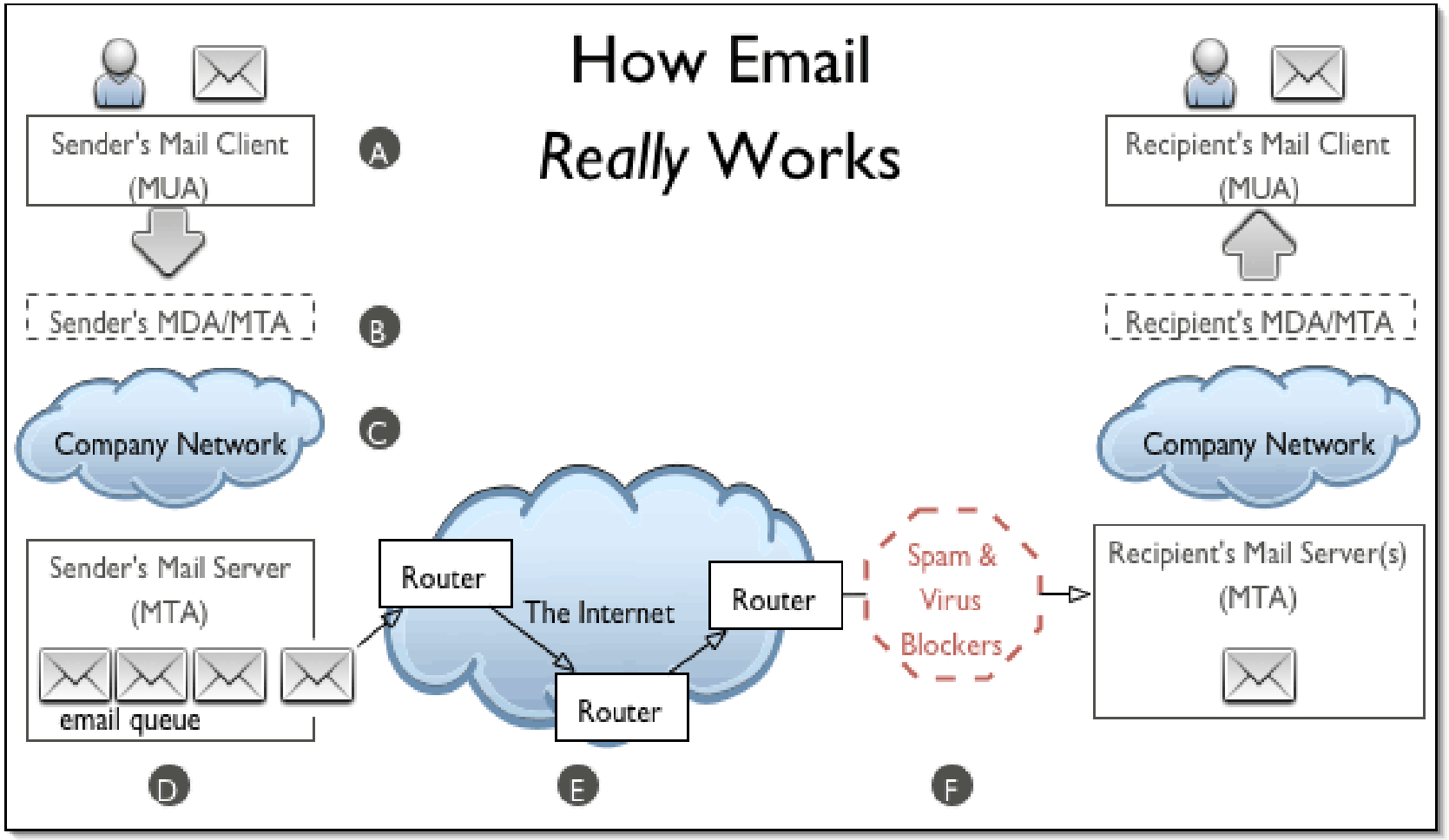
What is Email Security

- Email security can be defined as the use of various techniques to keep the sensitive information in email communication and accounts secure.
- To Understand Email Security , One Needs to Understand on How Email Works and what are the different elements that comprise of an Email System .
- The Whole Objective of Email Security is to ensure that the Users receive secure and good emails and they should not waste valuable company time in filtering good email from the bad emails .

Why Email Security

- Enterprise rely heavily on email for daily business communications
- Email is Most common vector to attack an enterprise by which enterprises are attacked.
- Most of the Enterprise business communication is done via Email and people exchange millions of files every day via Email Messages
- Email is a common entry point for attackers looking to gain a foothold in an enterprise network and attack valuable business data.
- Most of the attackers use Email as their First Priority attack vector

How Email Works



Courtesy : https://www.oasis-open.org/khelp/kmlm/user_help/html/how_email_works.html

Protocols/Ports and Key Terms

- SMTP Stands for Simple Mail Transfer Protocol
- SMTP Port is 25
- SMTP was initially defined in RFC 821 which was later revoked by RFC 2821 (https://www.ietf.org/rfc/rfc2821.txt)
- SMTPS (SMTP Secure via TLS OR SSL and Port is 567) however it not used widely
- TLS (Transport Layer Security) is used to Send email Securely (Encrypted) between Two Servers by issuing STARTTLS Command
- MTA (Mail Transfer Agent)
- MUA (Mail User Agent)

SMTP Response Codes

SMTP Response Codes is a way for Servers to communicate or talk with each Other . If an Email is not being delivered , always look at the Response code given by Destination Server . Here are some common SMTP Response Codes .

- 220 –SMTP Service Ready
- 221 – Service Closing
- 250 – Requested Action taken and Completed
- 421 – Please Try Later OR Service is not available
- 50x – Server Could not recognize the command
- 550 – No Such User Here OR User Mailbox not Available

SMTP Related DNS Records

- **MX Record** - A DNS Record created to show which server will receive emails for an organization
- **MX Record Priority** - The Smaller it is , The Higher the Priority is
- **SPF Record** : A DNS Record which will show which IP Addresses are authorized to send email on an organization's behalf
- **DKIM (DomainKeys Identified Mail):** Digitally Signing all outgoing emails with a Private Key to ensure that Email is actually sent by the Sender Domain itself and it is not spoofed Standard
- **DMARC (Domain-based Message Authentication, Reporting & Conformance)** : It is an Email Authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols .

Typical Email Scenario

- This SMTP example shows mail sent by Smith at host bar.com, to Jones, Green, and Brown at host foo.com. Here we assume that host bar.com contacts host foo.com directly. The mail is accepted for Jones and Brown. Green does not have a mailbox at host foo.com.

S Shows Responses from SMTP Server and C shows Responses from Client .

S: 220 foo.com Simple Mail Transfer Service Ready

C: EHLO bar.com

S: 250-foo.com greets bar.com

S: 250-8BITMIME

S: 250-SIZE

S: 250-DSN

S: 250 HELP

C: MAIL FROM:<Smith@bar.com>

S: 250 OK

C: RCPT TO:<Jones@foo.com>

S: 250 OK

C: RCPT TO:<Green@foo.com>

S: 550 No such user here

C: RCPT TO:<Brown@foo.com>

Courtesy : RFC 2821

Demonstration/Explanation of DNS Records

- Quick Demonstration using few Websites like

- MX Toolbox (https://mxtoolbox.com/)
- SPF Record Checker (https://www.dmarcanalyzer.com/spf/checker/)
- Nslookup

Next Lecture

In my next video , I will talk about these Topics . If you want to add any more topic , please mention that in the comments section .

- Email Attacks Types
- Email Relaying
- Email Spoofing
- Email Header Analysis