ANALYSING SMTP SERVER AND ITS SECURITY ASPECTS

Lohith N[1], T H Sreenivas[2]

[1] *Student, Information Science and Engineering, National Institute of Engineering, Karnataka, India*
[2]*Professor, Information Science and Engineering, National Institute of Engineering, Karnataka, India*

ABSTRACT

Electronic mail (e-mail) is one of the most popular network services nowadays. Most e-mail systems that send mail over the Internet use simple mail transfer protocol (SMTP) to send messages from one server to another. The messages can then be retrieved with an e-mail client using either post office protocol (POP) or Internet message access protocol (IMAP). SMTP is also generally used to send messages from a mail client to a mail server in "hostbased" (or Unix-based) mail systems, where a simple mbox utility might be on the same system [or via Network File System (NFS) provided by Novell for access without POP or IMAP. SMTP is used as the common mechanism for transporting electronic mail among different hosts within the transmission control protocol/Internet protocol (TCP/IP) suite. It is an application layer protocol. With the increase of electronic communication, spams are widely increased targeting individuals, having a doubtful intension such as stealing personal information to be misused or even to paralyze the event system by injecting viruses. Therefore, to protect email users from spams and viruses, it is crucial to protect our SMTP servers .

Keyword : - *SMTP, SPF, network security*

1. INTRODUCTION

Email is nowadays considered to be the most widespread form of digital communication. Email not only accounts for most user communications in corporate environments, but it is also widely used in both residential and mobile environments to support citizens' personal communications[1] .Network as we realize that Email has ended up mainstream with the dangerous development of the web. Notions of security and privacy therefore are highly important and have recently gained further attention due to related revelations concerning mass surveillance programs, but also due to the increasing number of exposed security threats and vulnerabilities. Email systems are by and large based on the Simple Mail Transfer Protocol (SMTP), which was designed decades ago around a simple but powerful premise: interoperability. The goal was to promote a simple yet reliable and ubiquitous protocol for email communications. In the early days of the Internet, the email system quickly started to gain popularity giving birth to a rich and ever growing ecosystem of SMTP compatible email providers[1].

However, the simplicity of SMTP came at the cost of reduced support for security, which originally was regarded as secondary. Unfortunately, Internet has become a much more dangerous place than what we could have ever imagined more than three decades ago. Accordingly, the set of standards used in email communications has been extended over time in an attempt to cope with the ever changing privacy and security threat landscape. Email is broadly utilized inside extensive scale association; different e-trade applications utilized the email for trading the data [2].

Nevertheless, the effective mitigation of security risks provided by the current set of standards and implementations is still very limited. This comes as a result of a strong need to preserve the highest possible degree of compatibility between email providers to ensure the successful delivery of messages regardless the security mechanisms supported by the email servers involved in their transmission. Indeed, in order to achieve this goal, until the entire community has adopted a given security upgrade/mechanism, all systems must remain compatible with insecure ones, thus

greatly limiting the effective mitigation of security risks. As a result, email communications are currently subject to serious privacy and security risks, which can lead to spoofing of users' identities, interception of confidential communications and also modification of their contents[1].

2. EMAIL SERVICE DESIGN PROCESS

Email has become the prime communication for all organizations for business continuity, assurance, records management, documents exchange and knowledge sharing. With an advent popularization of email as prime means of communication, there has been tremendous rise in emails attacks including spear phishing, spam, distribution of virus and botnets through emails. The reason why email has become the epicenter of attacks is the inherit weakness in the security infrastructure of email. Email has been evolved with least security consideration with an only aim of communicating, even though there has been various methodologies developed for protecting email systems but none of them are self sufficient to combat extreme verticals and horizontals of security attacks. The only way to protect email systems from attacks is by adopting practices as a mix of best of all available email protection methodologies. One should understand secure email design process to ensure secure email infrastructure. Following are the important design considerations for designing secure email system

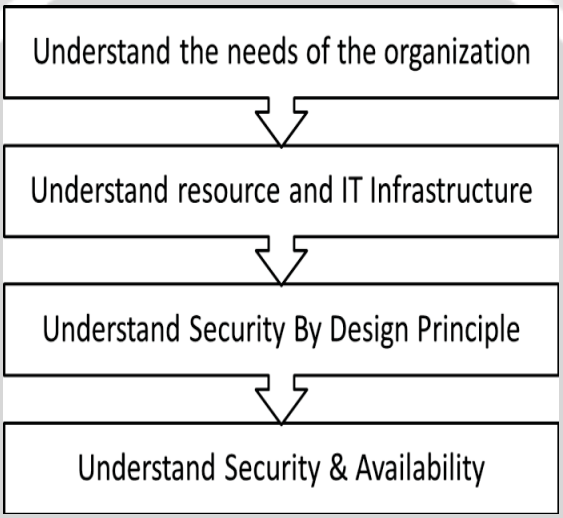

Fig-1: Design process for secure email infrastructure[3].

Further sections will explain each design step in detail and will also highlight some of the common practices and miss practices.

2.1 UNDERSTAND THE NEEDS OF THE ORGANIZATION

Understanding the needs of the organization is the prime process to ensure secure email communication. One should understand the following design scenarios for secure and effective email communication.

a. Internet facing Email service

If you are providing access of email through internet then it requires special consideration as it will be readily available to everyone on the internet. In such scenarios it is better to adopt multi tier security model and special security measures.

b. Campus-wide email service

It is common belief that internal accesses are more secure than accesses from internet, but most Email Security[4] compromise happens via internal systems[4] only. Internal systems are usually given unrestricted access to the email service and are not guarded by firewalls and similar security mechanisms.

2.2 UNDERSTAND RESOURCE AND IT INFRASTRUCTURE

Understanding the IT resources and identifying the conformance matrix of resource with the needs of the organization is an important step in ensuring availability and security of the email. It should be understood that Email Security [4] does not only call for security of email systems from virus and other malicious attacks but also includes in its scope availability, traceability and accountability of the service. Hence resource planning and its optimal utilization should also be understood. Following is the process model for understanding IT infrastructure and resource requirement for secure email design[3].

a. Identify the users Resource planning is governed by the number of users.

More is the number of users more is processing, storage, security requirements and hence the number of users and probable growth in number of users for next 5 years should be considered while planning IT resource.

b. Identify the type of access

Emails can be accessed using various protocols including POP3 & Secure POP3, IMAP & Secure IMAP, http & https. Depending upon the type of access organization provides it to its user, the hardware requirement will vary. If your organization is providing an access of email using https, then it requires a hardware and software that can handle multiple https connection concurrently and if access is through POP3 or IMAP. Then user local system must be configured for such accesses and should have sufficient disk space to store emails[3].

c. Identify security aspects

One should clearly understand the security aspects associated with each type of access. POP3 on one hand will download entire mailbox content on local system making it difficult for administrator for central management and compliance. On other hand access over http or https requires secure mechanism to be deployed to combat web based threats and vulnerability.

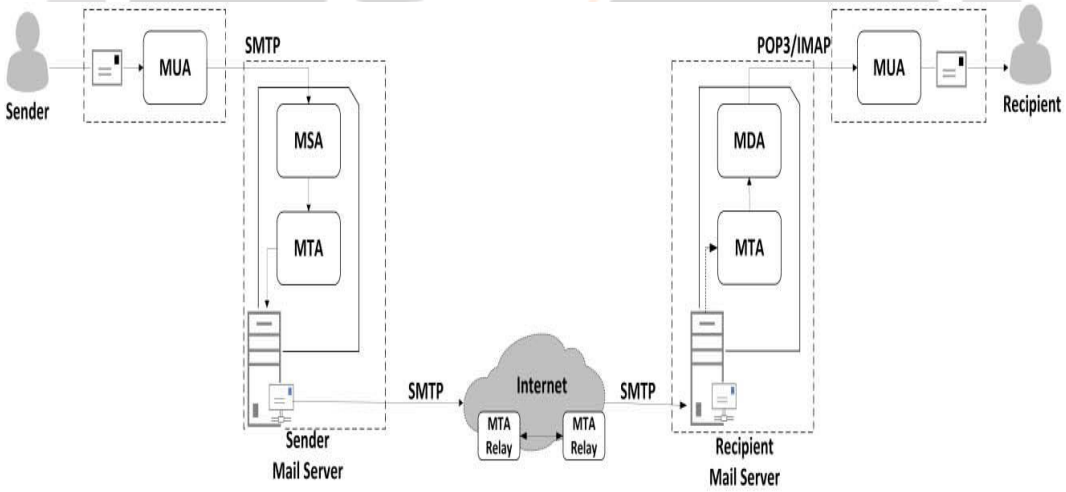

Fig- 2: End-to-end architecture of email systems and their communications protocol[1]

d. Identify network access parameter and Network Security:

IT administrator should clearly understand the network access requirements for secure email infrastructure design. As explained previously there

should be an isolation of clients and servers. Email servers should be guarded against various types of attacks and hence devices with capabilities of IDS and IPS, Antivirus & Anti-mal ware should be

deployed. IT administrators may choose to deploy email service in intranet or internet or mix of both. Organizations may choose to deploy software or hardware based solutions or mix of both to provide multi tier security[3].

e. Identify email software requirements

It is very important to understand the system requirements for the email software. All email software includes User Agent (MUA) and mailbox database. Organizations must choose right software for right needs. The software with limited scalability should not be deployed for an organization with dynamic user growth in the organization. On identifying the correct software, IT team should plan the resources to meet the minimum hardware requirement for the software and future growth and scalability should also be considered during design process.

f. Identify Hardware Requirements

Hardware must be properly sized and estimated before deploying email infrastructure. Organization having multiple geographical offices, the hardware must be planned for branch offices as well . Hardware must be planned by taking into consideration scalability and high availability of the systems[3].

2.3 UNDERSTAND SECURITY BY DESIGN PRINCIPLE

Security by design principle should be understood before designing any system or critical subsystem. Security by design principle states that design of a processor service should be carried out by considering the worst case access scenarios and deployment plans. If services are designed using this principle, then most of the inherent problems associated with security aspects of the service can be eliminated. Following are the most common practices in designing email services architecture.

a. DNS Security

DNS plays a vital role in email transaction as the email is designed with close associability with DNS. It should be properly understood before initiating email architecture planning. The IT administrators should al so ensure that reverse DNS
for a domain are also properly configured. This will help in preventing email spoofing attacks.

b. Sender Policy Framework:

Sender policy framework (SPF [5][6]) is email validation method designed to combat increased spam. SPF [5][6] defines a resource record in the DNS.

2.4 UNDERSTAND SECURITY AND AVAILABILITY

Security and availability of the service are closely associated with each other. Availability service is badly affected during denial of services or DDOS Attacks. Design process should include the process of ensuring availability of service. All the services to maximum extent possible should be made high available. High available systems should be load balanced as well in order to defend against of denial of service attacks[3].

3. ANALYSIS OF CURRENT EMAIL ECOSYSTEM

Email systems facilitate the exchange of information between interested parties whereby one sender can communicate a message to one or more recipients. The communication functionality offered by email systems involves a scalable and distributed architecture over the Internet, which is illustrated in Figure 2 and is discussed in what follows along with the relevant communication protocols.

A. Email systems architecture

The *sender* is the initiator of the email communication exchange. For senders to send an email to another user or a number of other users they need to utilise a dedicated software program, i.e. the *Mail User Agent* (MUA) that can be standalone programs or web-based ones, namely web mail. Conversely, the *recipient* of the email is the person or persons with whom the sender wishes to communicate, who also makes use of a MUA to receive emails. Mail User Agents have a *Message Submission Agent* (MSA) and *Mail Delivery Agent* (MDA) associated with them in order to handle respectively the transmission and reception of mails to/from *Mail Transfer Agents* (MTA). The mail server is at the heart of the email system's architecture. Its functionality comprises two main activities, namely managing

users' mailboxes and implementing the delivery of email messages between users. The mail server is at the heart of the email system's architecture. Its functionality comprises two main activities, namely managing users' mailboxes and implementing the delivery of email messages between users.
When the mail servers of the client and the recipient are not directly connected, MTA relays are utilised to store email messages and forward them towards the intended destination, whereas even in the case that the recipient's mail server is temporarily offline such a mechanism can be used to enforce robustness in mail delivery by making repeated attempts to deliver the mail on behalf of the server.

B. Email communication protocols

The core components of mail systems, i.e. the MTA clients and servers, communicate using standard protocols, the foremost of which is SMTP [7]. In addition, protocols such as POP3 (Post Office Protocol v3) [8] or IMAP (Internet Mail Access Protocol) [9] are used for the communication between MUAs and MDAs. When webmail systems are utilized, senders and recipients interact with them over HTTPS, whereas in the background SMTP and POP3/IMAP are employed as before. These interactions are highlighted in Figure 2 SMTP is used for the communication between the sender and the mail server, as well as between the sender's and the recipient's mail servers. SMTP is a communication protocol that defines the exchange of messages between these entities using DNS. The SMTP protocol is based on the exchange of commands and responses between the involved parties. Originally being ASCII-based and thus having limited functionality, SMTP was subsequently updated to allow for binary content to be exchanged with the introduction of MIME (Multipurpose Internet Mail Extensions) [10], [11], as well as to support advanced features. This was achieved with the introduction of a flexible service extension model that led to Extended SMTP (ESMTP) [14], [16]. The extension model complements the originally limited functionality scope of SMTP. For example, authentication was introduced as a service extension [16] enabling the server to inform the client on the supported authentication mechanisms.

4. EMAIL SECURITY

Email communications were originally built on the
principle of simplicity, however the need to enhance the provided functionality and to address emerging concerns such as those involved with security have both led to a plethora of add-ons and extensions. There exist standardised protocols and techniques capable of enhancing the security of email communications but they are not always used or they are not implemented properly in practice. We summarize here common existing threats .

A. Communication channel

The SMTP protocol did not originally ensure the confidentiality of the communications. STARTTLS [10] was proposed as an extension to SMTP to encrypt the otherwise clear text exchange of messages, whereas similar capabilities exist for IMAP and POP3 [21]. STARTTLS utilizes TLS to encrypt all SMTP traffic, thus additionally promoting authentication between the interacting mail servers and hindering potential Man-in-The-Middle (MiTM) attacks. To further promote compatibility between providers, SMTP servers are configured so as not to require the mandatory use of STARTTLS for their operation. This fact can be exploited by malicious users to break the security of SMTP by means of downgrade attacks [5].

B. Identity spoofing and spam

Malicious users commonly try to masquerade themselves as legitimate ones by faking their source email addresses as part of phishing or spamming campaigns. Those attacks, known as spoofing attacks, are possible because of the security shortcomings related to transferring and routing of email messages between mail servers.
The Sender Policy Framework (SPF) DNS Resource Records was recently introduced to detect email identity spoofing [13] by defining for a particular domain the hostnames of its computers that are allowed to send emails. The receiver SMTP server can then quickly check against the listing to decide to accept an email or not, based on whether the sending host is in the SPF record or not.

C. Protecting DNS communications

The aforementioned security mechanisms increase the trust one can have in a sender mitigating the risks of email identity spoofing and spamming. DNS plays a central role in the email infrastructure acting as a trusted anchor that glues the several protocols together. As a matter of fact, it is crucial to secure the DNS communications and the DNS records to preserve the security brought by the other protocols.

Accordingly, the DNSSEC protocol, described in the proposed standard RFC 6840 [23], has been developed to address the lack of security in the DNS protocol that not only weakens the email ecosystem but more broadly the entire Internet.

5. CONCLUSIONS

Email is one of the most common and widespread forms of digital communications, amassing an enormous user base that daily utilize it to exchange information. Protecting and securing this means of communication is therefore of more importance in order to promote user privacy and ensure the integrity and authenticity of the exchanged information. Largely based on SMTP, email was not originally designed with security as one of its main requirements, hence the various solutions that
have arisen over the past few years to address its security related shortcomings.

Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work Conclusion related your research work

6. REFERENCES

[1] Malatras, Coisel and Sanchez Technical Recommendations for Improving Security of Email Communications, MIPRO 2016, May 30 - June 3, 2016, Opatija, Croatia

[2] Neeta Wadhwa, Syed Zeeshan Hussain and S.A.M Rizvi "A Combined Method for Confidentiality, Integrity, Availability and Authentication (CMCIAA)" WCE 2013, July 3 - 5, 2013, London, U.K

[3] Dharmendra Choukse Umesh Kumar Singh Lokesh Laddhani Rekha Shahapurkar ," Designing Secure Email Infrastructure"

[4] M.Tracy,W.Jansen,K.Scarfone,J.Butterfield Guidelines on Electronic Mail Security- Recommendations of National Institute of Standards and Technology- NIST Special Edition 800-45 Version 2 Feb 2007

[5] P. Hoffman, "SMTP service extension for secure SMTP over Transport Layer Security", RFC 3207, RFC Editor, February 2002. http://www. rfc-editor.org/rfc/rfc3207.txt.

[6] Let's Encrypt, Linux Foundation collaborative projects. 2016.

[7] Klensin, "Simple Mail Transfer Protocol", RFC 5321, RFC Editor, October 2008. http://www.rfc-editor.org/rfc/rfc5321.txt.

[8] J. G. Myers, and Marshall T. Rose, "Post Office Protocol –version 3", STD 53, RFC Editor, May 1996. http://www.rfceditor. org/rfc/rfc1939. txt.

[9] M. Crispin, "Internet Message Access Protocol -version 4rev1", RFC 3501, RFC Editor, March 2003. http://www.rfceditor. org/rfc/rfc3501. txt.

[10] N. Freed and N. S. Borenstein, "Multipurpose Internet Mail Extensions (MIME) part one: format of internet message bodies", RFC 2045, RFC Editor, November 1996. http://www.rfceditor. org/rfc/ rfc2045.txt.

[11] N. Freed and N. S. Borenstein "Multipurpose Internet Mail Extensions (MIME) part two: media types", RFC 2046, RFC Editor, November 1996. http://www.rfc-editor.org/rfc/rfc2046.txt.

[12] J. Klensin, "Simple Mail Transfer Protocol", RFC 2821, RFC Editor, April 2001. http://www.rfc-editor.org/rfc/rfc2821.txt.

[13] J. Klensin, N. Freed, M. T. Rose, E. A. Stefferud, and D. Crocker, "SMTP service extensions", STD 10, RFC Editor, November 1995. http://www.rfc-editor.org/rfc/rfc1869.txt.

[14] C. Newman, "Using TLS with IMAP, POP3 and ACAP", RFC 2595, RFC Editor, June 1999. http://www.rfceditor. org/rfc/rfc2595.txt.

[15] Z. Durumeric, D. Adrian, A. Mirian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. Bailey, and J. A. Halderman, "Neither snow nor rain nor MITM...: an empirical analysis of email delivery security", in proceedings of the 2015 ACM Conference on Internet Measurement Conference, IMC '15, pages 27–39, New York, NY, USA, 2015.

[16] S. Kitterman, "Sender Policy Framework (SPF) for authorizing use of domains in email, version 1", RFC 7208, RFC Editor, April 2014. http: //www.rfc-editor.org/rfc/rfc7208.txt

[17] S. Weiler and D. Blacka, "Clarifications and implementation notes for DNS security (DNSSEC)", RFC 6840, RFC Editor, February 2013. http: //www.rfc-editor.org/rfc/rfc6840.txt.