International Journal of Scientific Research & Engineering Trends
Volume 3, Issue 5, Sept.-2017, ISSN (Online): 2395-566X

Attack over Email System: Review

Anuradha Kumari
Computer Science & Engineering
NRI Institute of Information Science & Technology, Bhopal, India
Email: anuradhagupta622@gmail.com

Nitin Agrawal
Computer Science & Engineering
NRI Institute of Information Science & Technology, Bhopal, India
Email: seonitin79@gmail.com

Umesh Lilhore
Computer Science & Engineering
NRI Institute of Information Science & Technology, Bhopal, India
Email: umeshlilhore@gmail.com

Abstract – **Email has become an integral part of our life. Email is reliable and authentic method for exchanging message. But Email systems are facing increasing security threats from local and distributed unethical elements. Keeping the email system secure is of supreme importance to every organization whether running its own emails system or using email services from internet service provider (ISP). Denial of service (DoS) attacks is more prevalent on email system. Various DoS attacks on email system are Chain bombs, error message bombs. Zip bombs and mass mailing bombs. In this paper email architecture and their security issue is discuss and explain their vulnerability with counter measure .**

Keywords – **Email, Web Mining, Dos Attack, Email Bombing, Mass Mailing.**

I. Introduction

Web technology is used to implement the “Web or www” portion of Web Services. Web servers and web browsers are communicating client-server computer programs for distributing documents and information, generally called web data, over the Internet. Web data are marked up in the HTML language for presentation and interaction with people in web browsers. Each web server uses an IP address or domain name as well as a port number for its identification [6]. People use web browsers to send data requests to web servers with the HTTP protocol, and the web servers running on server computers either retrieve the requested data from local disks or generate the data on-the-fly, mark up the data in HTML, and send the resulting HTML files back to the web browsers to render. Apache, Tomcat and IIS are popular web server programs, and IE and Firefox are popular web browsers.

Email is one of the most common applications used daily by millions of people world-wide. Email is transmitted over internet by email transmission Protocol such as Simple Mail Transport Protocol (SMTP) or Secure/Multipurpose Internet Mail Extensions (MIME). SMTP according to [1] defines the message format and SMTP server (mail transfer agent) stores and routes message throughout the internet. Mail Transfer Agents (MTA) uses the Simple Mail Transfer Protocol (SMTP) for relaying emails. MTA is commonly a target of planned or unplanned DoS attacks. A few emails may totally load an email server resulting in a Denial of Service (DoS) condition. In SMTP DoS the delivery procedure is harmed so much that the legitimate e-mails are affected with a non-tolerable delay [2]. Email bombing is one form of SMTP denial of service attack that floods an inbox and mail server with messages. The email bomb may also damage in the form of loss of internet connectivity and many more [3]. These cases may result in more serious problems especially if one is using internet connection for business purposes. E-mail bombs have one key objective: flood the mail server so that mail server becomes occupied or is unserviceable [3]. Mass e-mail attacks also used to fake the identity of the intruder, degrade the accessibility of communications systems, damage the integrity of institution, or secretly share out illegitimate material.

II. Architecture of Email System

The first uniform architecture for email defined an email system into user world and transfer world as shown in the figure 1. User world is defined as Mail User Agents (MUA), and the transfer world, as Mail Handling Service (MHS) [8]. Mail Handling Service is composed of Mail Transfer Agents (MTAs). The MHS accepts an email from one sender and delivers email to other users. MHS predefine a virtual MUA-to-MUA exchange environment [8]. Sender-to-receiver Internet Mail exchange is performed by using a uniform infrastructure. Mail exchange system has four components namely Email Object, Global Addressing, Point-to-Point Transfer Mechanisms, No requirement for Author, Originator, or Recipients to be online at the same time.

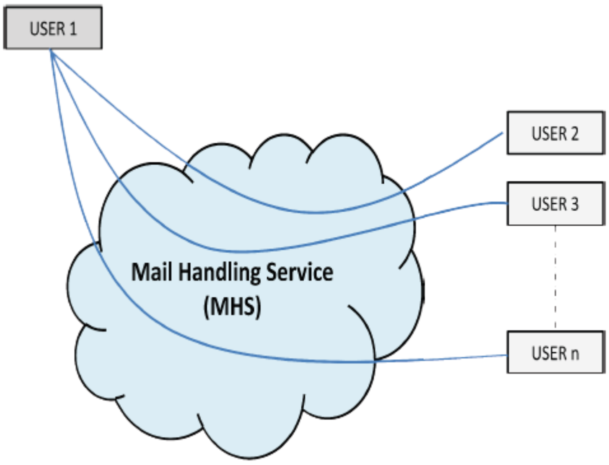

Fig.**Ошибка! Текст указанного стиля в документе отсутствует.**. Architecture of Network Email

Mail Handling Service (MHS)

The Mail Handling Service (MHS) as shown in the figure 2 accomplish a sender-to-receiver transfer of mail. Transfers of email are performed using one or more Relays. Email services in organization typically have only one Relay [8].

Relay

TheRelay accomplishes routing of email from sender to receiver, by transmitting or retransmitting the email as shown in figure 1-3. The Relay appends routing information [RFC2505]. Relay does not alter the message content or information on message envelop. Relay may alter message content type, like binary to text as per the suitability of the next node in the MHS [8].

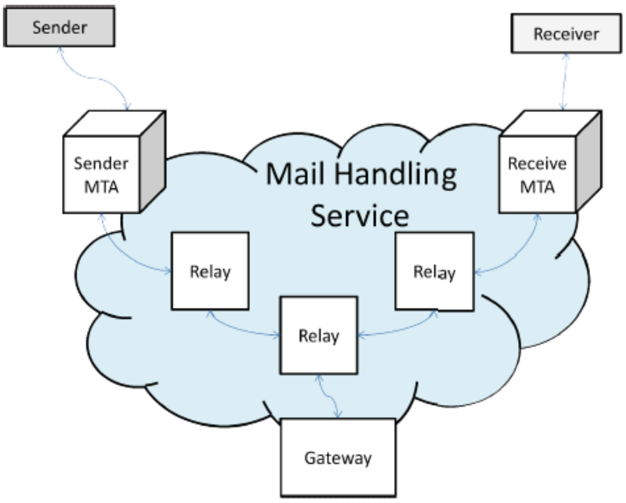

Fig.2. Email Architecture with Relay

The Internet Mail architecture composed of six basic types of components as shown in the figure 1-4; all components are needed to perform a store-and-forward operation of email [8].

1. Message
2. Mail User Agent (MUA)
   a. Sender's Mail User Agent (S-MUA)
   b. Receiver's Mail User Agent (R-MUA)
3. Message Submission Agent (MSA)
   a. Sender's Message Submission Agent (S-MSA)
   b. MHS's Message Submission Agent (H-MSA)
4. Message Transfer Agent (MTA)
5. Message Delivery Agent (MDA)
   a. MHS's Message Delivery Agent (MDA)
   b. Receiver's Message Delivery Agent (R-MDA)
6. Message Store (MS)
   a. Sender's Message Store (S-MS)
   b. Receiver's Message Store (R-MS)

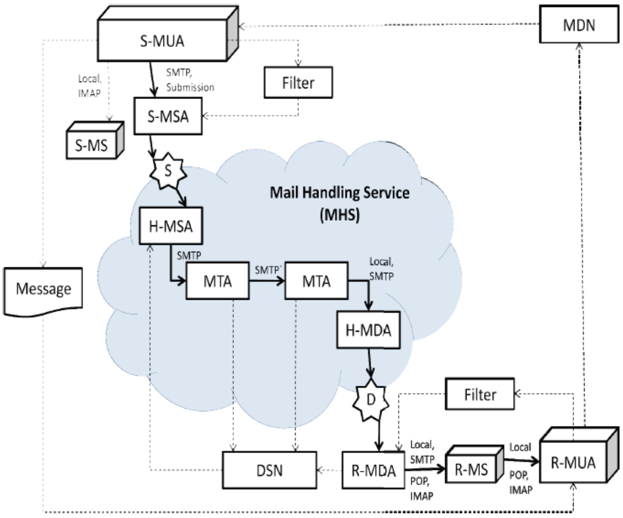

Fig.3. Main Components of Email System

In addition to main components shown in figure above, a few notification and filtering components are present in Internet mail architecture:

Delivery Status Notification (DSN)

A Delivery Status Notification (DSN) is a notification message. DSN may be generated by the MHS components like MSA, MTA, or MDA. MDA and MTA are sources of DSNs and S-MSA is its recipient. DSNs provide notification about message transfer, such as errors in email transfer or successful delivery [8].

Message Disposition Notification (MDN)

A Message Disposition Notification (MDN) is a notification. MDN gives information related to post-delivery processing, such as representing that the email has been displayed. MDN may be originated by an R-MUA and is received to the S-MUA [8].

Message Filter (MF):

Message Filter is a scripting language to state conditions for handling of mail, typically at the time of delivery. Scripts may be used in a variety of ways, as a MIME part. Message filter script operates from the R-MUA to the MDA. However, message filtering is done at many points along the transfer path [8].

Message Data

The purpose of the Mail Handling Service (MHS) is to send the message from its originator to its recipients. A message is composed of a route-information envelope and the message content. The envelope contains details used by the MHS. The message content is parted into a header part and the body part. The header part comprises route information and body part comprises sender's message contents. The body may be lines of text or attachments [8].

Mail User Agent (MUA)

The Sender's MUA (S-MUA) generates a message and performs submission of message into the Mail handling service through a Mail Submission Agent (MSA). S-MSA may arrange messages in many ways. The common way of arranging messages is in "folders". Folder method creates a folder for messages under development known as Drafts.

Draft is a folder for Queued or Unsent messages waiting to be sent. Messages that have been posted are kept under Sent folder [8]. The Recipient MUA (R-MUA) works on Recipient's side to receive and process email. Processing at receiver side includes generating user-level control messages, displaying the received message, replies and forwarding new messages.

Message Store (MS)

An MUA make use of a Message Store (MS). MS may be on a server or on the local machine as the MUA. An MS gets email from an MDA either from a local method or by means of POP or IMAP [6].

Mail Submission Agent (MSA)

Mail Submission Agent (MSA) uses SMTP and TCP for submitting mail to Mail Handling Service (MHS). MSA imposes different requirements, such as access permission. A Mail Submission Agent (MSA) gets the emails submitted by the S-MUA and make mail to adhere to the Internet standards. MSA is divided into two subcomponents, S-MSA and H-MSA, respectively [8].S-MSA appends header fields, such as Message-ID and Date and alters portions of the email according to local Internet environment, such as transforming an address to its proper representation. The MSA prepares emails for submission to MHS, via H-MSA. The H-MSA is responsible for a message to adhere to the receiver's Internet environment and to local site standards.

Mail Transfer Agent (MTA)

A Mail Transfer Agent (MTA) relays mail from host to host (hop). It works similar to network router, to move the email towards the Recipient. Email relaying is done by a series of MTAs, until the email reaches at destination MDA. On comparison to the packet payload messages are larger in size, sender-to-destination transfer time is more. Hence, an MTA performs both sender and receiver MTA functionality. An MTA also adds trace information. Internet Mail deploys SMTP, Batch SMTP [RFC-2442] and ODMR [RFC-2645]. The Internet Mail SMTP provides a basic level of reliability, providing retransmission facility in case intermediate transfer failure. Internet Mail MTAs are store messages in a proper way that gives recovery while service interruptions. Main routing means for Internet email is the Domain Name Service - MX record [RFC-1035]. DNS-MX records specify an MTA via which the required domain may be reached.

Mail Delivery Agent (MDA)

A transfer of message from the Mail Handling Service to a Recipient's mailbox is known as "delivery" (D). Message delivery occurs from MHS-oriented Mail Delivery Agent (H-MDA) to the Recipient oriented MDA component (R-MDA) [8]. The MHS portion (H-MDA) acts like a server SMTP engine. H-MDA's additional goal is to re-direct the email to an alternative address, as specified by recipient addressee's preferences. The work of the recipient side of the MDA (R-MDA) is to carry out any delivery work specified by the Recipient. Email transferred to MDA is performed by a normal MTA transfer method. Transfer from an MDA to an MS is done through an access protocol, like as POP or IMAP.

Gateways

A Gateway does the basic transfer and routing work of email relay. Gateway is allowed to alter address, content, structure, or other attributes. Modifications are needed to send the email into a messaging environment under different internet standards or mismatched policies. The critical difference between a Gateway and an MTA is that former may make essential changes to a message required to transfer the message [8].

III. Vulnerabilities in Email System

Vulnerability is a weakness or flaw in the system. Vulnerability allows an attacker to reduce a system's security. Vulnerability is the combination of three things: a system has flaw, attacker access to the flaw, and attacker has ability to exploit the flaw. In order to launch an attack on a mail service, the attacker will need to select and focus on a section of the mail flow to exploit. Existing mail service attacks focus on ways to allow for malicious attackers to send more mail traffic through the Internet while evading responsibility by making the messages difficult to trace through techniques such as spoofing.

While spamming does not represent a direct attack on any piece of the mail flow infrastructure, it instead depicts an abuse of it. Spammers profit by utilizing other companies, resources, and systems to funnel their unwanted e-mail messages out to the world. Depending on the end goal, different attacks target mail services in varied ways. If we break down the mail flow into key architectural components, it may be summed up to include the following attack points [8]:

Messaging Servers

Messaging servers are the most commonly attacked component of the mail architecture. Attacks that may be targeted at messaging servers include DoS attacks, mail relay attacks, buffer overrun attacks, mail loops, SMTP Auth attacks, spam, and viruses [8].

Addressing

Every e-mail message that goes out into the Internet for delivery must be addressed with recipient information. E-mail messages may contain various types of addresses, such as To, From, Carbon Copy , and Blind Carbon Copy. Attackers may choose to manipulate addresses in an e-mail message in a number of ways, all ending in the changes being made to assist them achieve the message routing behavior desired. Attackers may choose to manipulate source or destination information. However, changing source information may have purpose, such as in a Non Delivery Report attack (NDR). Spoofing is the term used to describe the manipulation of address information, and many attacks utilize some form of spoofing as part of their attack approach. Examples of attacks that include spoofing to some degree are NDR attacks, DoS, mail loops, phishing and spam [8].

System Users

Attacks that target users include phishing and social networking and are much more difficult for messaging administrators to defend against [8].

Infrastructure Services

Exchange depends on infrastructure services such as Active Directory (AD) and Domain Name Services (DNS) to function properly. An attack may seek to disable messaging in an organization, or instead may prefer to redirect, or simply disrupt it. By attacking AD or DNS, have the ability to indirectly impact Exchange if successful. Some of the common AD attacks include Denial of service (DoS) attacks. A DoS attack may also be issued against an e-mail server directly, but by targeting AD, the attacker has the potential to cause problems for many applications, instead of causing problem purely for Exchange [8].

IV. ATTACKS ON EMAIL SYSTEM

Email system has multiple attack points, which make it vulnerable to various attacks like Directory harvest Attacks, SMTP Auth Attack, Mail Relay attacks etc and some other attacks performed with certain modification to these attacks.

Directory Harvest Attacks

The purpose of a directory harvest attack [9] is to collect a key piece of information from your directory services, namely valid e-mail addresses. By knowing which e-mail addresses in an organization are valid, spammers may target messages at legitimate user accounts without generating as much negative attention. Directory harvest attacks are often performed by submitting large numbers of e-mail addresses with very little content to an organization. The e-mail messages are randomly generated, but commonly used e-mail aliases. If the e-mail message is not returned in a Non Delivery Report (NDR), then the message must have been delivered, making it a valid address. Individuals or entities that specialize in generating and propagating spam may collect these directory harvest lists as a precursor to launching a spam attack. With a listing of valid e-mail addresses, the penetration rate of the attacks is much higher amongst the target audience for the spam message. One feature of Exchange Server, which specifically combats against directory harvest attacks, is called tarpitting. Tarpitting is the practice that involves delaying the response back to a connected SMTP server. Tarpitting forces a delay between the time a recipient is submitted for acceptance to the SMTP server and the time when the response is sent back. The time delay has nothing at all to do with the responsiveness of the directory server. Regardless of the time that it takes to receive the response back from the directory server, the SMTP server imposes a preconfigured delay before delivering the “Recipient OK” or the “User unknown” response. This delay does cause a directory harvest attack to become cumbersome to execute due to the shear duration required to extract information.

Cache Poisoning Attack

Cache poisoning attacks [9] function by intentionally causing a DNS server to cache misrepresented information, such as the wrong Internet Protocol (IP) address for a particular domain name. When a query is issued to determine the MX record for a target domain name, the DNS server responds with the wrong address due to the poisoned cache in it. Since the mail server is unaware that it has been given misinformation, mail server connects to the resolved address and delivers the e-mail messages. In this manner, cache poisoning may allow an attacker to redirect e-mail messages to an unauthorized messaging server.

Non-Delivery Report (NDR) Attacks

Some attacks utilize other attacks’ methods in order to achieve their end results. NDR attacks [9] are good example of this since actually depend on address spoofing to accomplish their goal. An NDR is an e-mail message generated by a messaging system indicating that the destination e-mail address does not exist and the e-mail message may not be delivered as shown in figure 3. The NDR is generated and forwarded to the sender of the message, indicating that even though the e-mail message arrived successfully at the target messaging system responsible for the domain name, the username indicated on the mail message does not exist in the target mail infrastructure, addressed to fictional addresses in a target enterprise. The messages arrive at the target, and since the addresses do not exist in the environment, the messaging system will generate an NDR, typically with the original message attached, to be directed back to the source for each of the fictional target mail messages. This does not seem like anything out of the ordinary until source address is analyzed carefully. The sneaky part of an NDR attack is that the source address on each of the original messages has been spoofed to represent a legitimate e-mail address existing on some other mail infrastructure. So the outcome of the scenario is that when the NDRs are generated by the target system will then be transmitted to the spoofed sending address and each NDR, containing the original spam message as an attachment, will be delivered to an unsuspecting user.

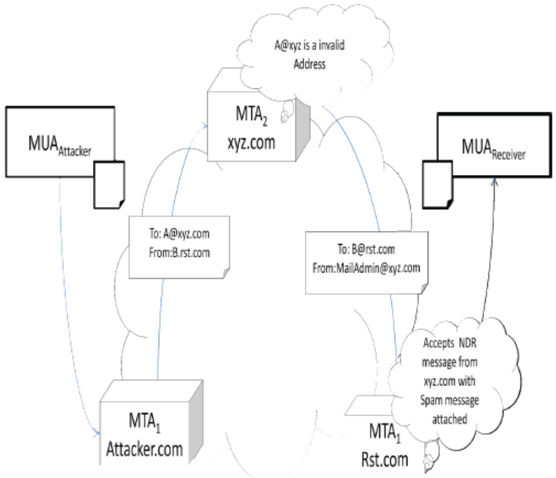
A@xyz is a invalid Address
MTA$_2$ xyz.com
MUA$_{Attacker}$
MUA$_{Receiver}$
To: A@xyz.com From:B.rst.com
To: B@rst.com From:MailAdmin@xyz.com
Accepts NDR message from xyz.com with Spam message attached
MTA$_1$ Attacker.com
MTA$_1$ Rst.com

Fig.4. Non Delivery Report Attack

The users may mistake the NDR as being a response to one of their own messages and proceed to open it, thereby achieving the goal of presenting the users with the spam message without it being traceable back to the source. In many ways, NDR attacks are similar to mail relay attacks, albeit ancillary.

By creating spam messages that contain completely falsified address information, an NDR attack uses one legitimate mail system to deliver spam to another legitimate mail system by way of NDR messages. Essentially, servers are used as a dispatch point.

Mail Relay Attacks

One of the most common attacks attempted today is the mail relay attack. Mail relay attacks [9] allow mail servers to be utilized to deliver mail traffic originating from some other location, which usually consists of spam and other unwanted, unsolicited, or even illegal mail. Mail relay attacks may impact your environment in multiple ways.

The first obvious impact is on the performance of your mail servers. Often times, once a malicious attacker has discovered this vulnerability or mis-configuration in mail systems, your servers may be used to transmit millions of additional e-mail messages a day.

The primary purpose behind mail relay attack executions is to disperse spam messages out onto Internet servers and into unsuspecting user mailboxes. Many defensive systems today track trends over time, and many of them use metrics based on source IP address in order to determine the probability of spam when screening e-mail traffic.

Since the malicious attacker is utilizing mail servers to send out spam e-mail, the systems that utilize tracking mechanisms based on IP address will start to document a spam trend originating from legitimate source IP addresses. It may lead to legitimate systems becoming blacklisted and mail servers will no longer be trusted, which would potentially cause legitimate e-mail messages from your environment to be rejected or dropped.

In order to assist with combating the amounts of spam that are forwarded around on the Internet each and every day administrators should consider implementing the usage of Sender Policy Framework (SPF) records in DNS. SPF records in DNS are a method used for validating that only authorized servers are senders of e-mail messages from a particular domain. By utilizing SPF records as a verification mechanism, administrators may reduce the amount of spam messages processed since only trusted entities would be allowed to submit mail for delivery.

It Implement in two-step process, including configuring mail system’s Internet facing services to utilize SPF records in order to validate the source of received messages, and the second part consists of configuring organization’s SPF records so that other enterprises may validate e-mail stream.

Mass Mailing Attack

POP3 and IMAP4 are the protocols used to retrieve e-mail messages from an e-mail server, and implementations of each have had documented vulnerabilities in the past. Since these protocols are used to access e-mail, the services are listening for client connections, which makes them viable targets for attacks such as a denial of service (DoS) or buffer overrun attacks as shown in figure 4.

DoS attacks occur when an attempt is made by an attacker to overwhelm a target system and cause it to fail [9]. Most of these attacks include sending a flood of requests to the target system, scaled well beyond what the system is design to handle. If the attack is successful, the target system is incapacitated and therefore unavailable to service valid client connections.

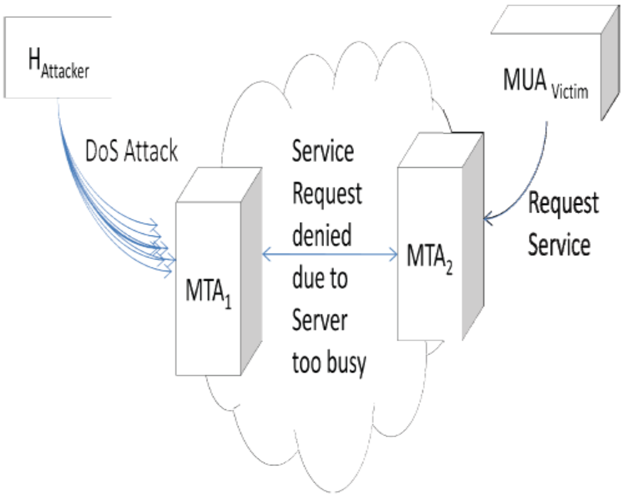

Fig.5. Mass Mailing Attack

Buffer overrun attacks attempt to achieve the same end result, but the approach is different. Buffer overrun attacks often execute code on the targeted system, which cause the system to overrun its memory buffer and write data inappropriately into random access memory. The impact may include errors in program execution and conflicts with other system components, ultimately incapacitating the target system.

V. RELATED WORK

This paper focuses on Denial of Service (DoS) attack on email server, possible mail bombing techniques on email system, countermeasure to different mass mailing attacks, and various approaches to generate mail bombing attack signature.

Paper [11], discusses mail-bombing techniques, automated attack tools, and countermeasures. Author also discussed an actual Internet-based attack that was launched in 1997 on the Langley AFB SMTP e-mail infrastructure. An analysis of the cyber attack is carried out, graphs illustrating the attack volume, and a statistical e-mail bomb early warning system. Author has cited about a covert channel for the illegal distribution of pornography, hate mail, and pranks via standard operational SMTP MTAs.

In [12], author discusses the cyber-attack, a framework for defending against the attack. The countermeasure was accomplished by running the MTA in a mode which accepts and queues SMTP mail; processes the messages with a rules-based filter: and then forwards mail after filtering. It proposed a filtering framework which is simple and effective for a large subset of email bombs. Author uses prototype filter scripts. Black Hole strategy is combined with the rapid prototype and deployment of a rules-based filter and detailed knowledge of the battle space is an effective countermeasure to Internet mail bombs.

In paper [13], author proposed ISCREEN rule-based message Filtering System to screen messages effectively. It is found to effectively screen text messages received by a small group of users. It requires knowledge about the network in which it operates and requires the ability to use that knowledge flexibly in completing a number of different tasks. ISCREEN filtering systems act independently of the user, require the ability to communicate effectively in describing situations which have occurred, in describing situations which may potentially occur, and in asking for clarification of conflicting instructions. It is limited in its ability to understand the content of messages and applicable to small network only. In [14], the authors employed a testing methodology with email "traceroute" mechanism to measure email loss, latency, and errors of a fixed set of popular, random, and Fortune 500 domains. They present plausible explanations for some of experimental phenomena and hope to derive guidelines for designing future networks and more reliable email systems by understanding email traffic.

Gomes et al. [15] grouped emails traffic near a large university into three categories, namely spam, ham, and aggregate, and then they characterized each workload separately. They are aiming at identifying a signature of spam traffic, which may be used in the future for developing more effective spam-controlling techniques.

Paper [16], presented a server workload characterization aiming at detecting and controlling junk emails. Research in above three papers focused on mining logs in email server or an email gateway. As we know, mail logs only keep limited static statistics and ignore network and protocol properties of email traffic. In [17], authors presented an EFSA model for characterizing email traffic and choosing parameters, which firstly makes it possible to study traffic characterization effectively. Second, proposed methodology focuses on the network and protocol properties of email traffic. Third, main focus is on drawing insights into designing more effective abnormal email traffic identification techniques in backbone network.

Mass mailing attacks is commonly used to get access to email service or to disrupt the service. Mass mailing attacks consume valuable network resources and possibly are used as carriers for virus/worms, Trojans horse, phishing and DDoS attacks. Research is happening to tackle the problem. Researchers focus on mining logs in email server or an email gateway but mail logs only keep limited static statistics and ignore network and protocol properties of email traffic secondly it is difficult to locating the item or items of interest from the vast amount of data. To minimize the impact, an administrator needs to figure out the initial signs of attack by analyzing the recent traffic to stop the further destruction. There exists a strong requirement for a mechanism to study and disclose the abnormal email traffic in the network.

VI. EXPECTED WORK

Email systems are facing increasing security threats from local and distributed unethical elements. It seems to be that there are so many attacks has been done in web environment. In this manner we will try to make a system in order to detect and prevent the some of these attacks for better performance.

VII. EVALUATION PARAMETER

In this section there will be discussion of the parameters by which the performance of the system will be shown

- True Positive (TP) = If a URL entry is proven present in a class and the proposed model also classifies that URL in that class, the result is considered true positive.
- True Negative (TN) = If a URL entry is proven absent in a class and the proposed model also proves the absence of that URL in that class, the result is considered true negative.
- False Positive (FP) = If the proposed model indicates the presence of a URL in a class who actually does not contains that URL, the result is considered false positive.
- False Negative (FN) = If the proposed model indicates the absence of a URL in a class, who actually belongs to that class, is considered false negative.

By the help of these parameters it is possible to calculate the accuracy by the given formula.

$$\text{Accuracy} = \frac{Total\ Positive}{Total\ Assessment} = \frac{TP + TN}{P + N}$$

VIII. CONCLUSION

Email is one of the most common used network communication services. Due to enormous increase in usage of email service, attackers and hackers began to use emails in committing crimes. The simplicity of email system may be misused in numerous ways to create extraordinary and powerful e-mail bombs. These e-mail bombs may be launched in many different attack scenarios which may easily flood and shut down chains of email servers. This paper gives a bird eye over Email services and their vulnerability.

REFERENCES

[1] P. S. Bogawar and K. K. Bhoyar, "Email Mining : A Review," in IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012, pp. 429–434.

[2] C. Partridge, "The technical development of internet email," in IEEE Annals. Hist. Computer., vol. 30, no. 2, 2008, pp. 3–29.

[3] F. Lau and S. Rubin, "Distributed denial of service attacks," in Syst. Man, Cybern. 2000 IEEE Int. Conf., vol. vol.3, 2000, 2000, pp. 2275–2280.

[4] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, a. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on TCP," Proceedings. IEEE Symposium Security Privacy, 1997, Cat. No.97 CB 36097.

[5] B. Bencsáth and M. A. Rónai, "Empirical analysis of Denial of Service attack against SMTP servers," in Proceedings, 2007 International Symposium Collab. Technology Systems, 2008, pp. 72–79.

[6] Prof. Lixin Tao, (2015, January 25), "Introduction to Web Technologies", [Online]. Available: http://csis.pace.edu/ lixin/.

[7] ABS Technologies, (2015, February 5) "POP 3 Email vs. Web Based Email – Which is better ?" [Online], Available: http://www.essortment.com/pop3-email-based-email-best-28249.html

[8] Network Working Group, (2015, February 10) "Internet Mail Architecture," [Online], Available: http://http://bbiw.net/specifications/draft-crocker-email-arch-03.html.

[9] Rob Kraus, "Exchange Server- Mail Service Attacks" in Seven Deadliest Microsoft attacks, Technical edition, Syngress is an imprint of Elsevier, 2010, pp 71-91.

[10] Y. Wang, C. Lin, and Q. L. Li, "Performance analysis of email systems under three types of attacks," in Performance Evaluations, vol. 67, no. 6, 2010, pp. 485–499.

[11] T. Bass, A. Freyre, D. Gruber, and G. Watt, "E-mail bombs and countermeasures: Cyber attacks on availability and brand integrity," IEEE Networking., vol. 12, no. 2, 1998, pp. 10–16.

[12] L. Col, G. Watt, and L. Afb, "FILTERING QUEUED SMTP MAIL." in Science Applications International Corporation Center for Information Protection McLean, Virginia, 1997, pp. 16-27.

[13] R. A. Devenezia and I. Consultant, "Rule based filtering - Categorizing unwanted inputs Survey data Core Logic Core implementation," in SESUG Proceedings, March 2010, pp. 1–9.

[14] J. Zhang, Z. Du, and W. E. I. Liu, "A Behavior-Based Detection approach To Mass-Mailing Host," in Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007, pp. 19–22.

[15] M. Kim, W. James, and W. Hong, "Towards Flow-based Abnormal Network Traffic Detection Motivation : network security attack threats," in DP&NM Lab. Dept. of Computer Science and Engineering Pohang University of Science and Technology, 2004, pp. 1–12.

[16] L. Bertolotti, M. Carla, U. Pavia, and I. Pavia, "Workload Characterization Of Mail Servers." In International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010, pp. 1-16.

[17] N. Zhang, B. Fang, L. Guo, and Y. Jiang, "A new approach for detecting abnormal email traffic in backbone network," in International Conference Computer Intelligent Security ICCIAS 2006, vol. 1, 2007, pp. 586–591.