Email Security: The Challenges of Network Security

Ms.Priyanka S. Kamthe

Ms.Sonal P. Nalawade

ASM Institute of Management & Computer Studies (IMCOST), Thane, Mumbai
University Of Mumbai
kamthe.priyanka05@gmail.com
snalawade93@gmail.com

Abstract: Now a day's, network security has become very important. For those securities Simple Mail Transport Protocol is the most widely used protocol for e-mail delivery. But, it lackssecurity features like privacy, authentication and integrity of e-mail message. To make e-mail communication secure and private,e-mail servers adopted one or more security features. The security protocolsprovide a most security but it also has several limitations.
This paper discusseslimitations of e-mail security protocols, analyses and evaluates theireffectiveness in e-mail servers, as well as outlines the various attack methods which are used, and various defencemechanisms against them.

Keywords: E-mail Security, E-mail Security Protocols,S/MIME, SMTP Security Issues,SPAM.

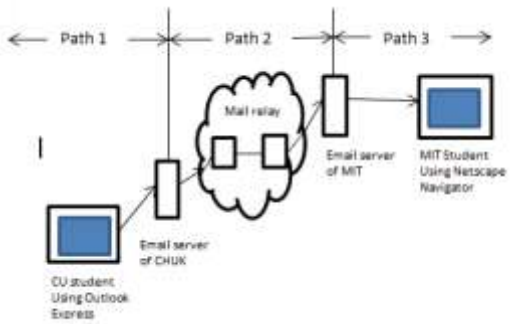
*****

I. INTRODUCTION

Now a day's email is become more adequate in industry so the importance of email security become more significant. Security contains management of email storage, data recovery. When data is large then managing and storage takes lots of time that will impact the user and lost productivity.
Email security becomes more important in organization, business, government and every field. Email security refers to protecting from various attacks. The architecture of network is main part while securing email. Many organization uses firewall to prevent the attacks. To understand the email security research first we need to understand its background.

Simple Mail Transport Protocol (SMTP) was designed for a smaller community of users. Now a day's several technology and policies changes were made to SMTP server powerful to make email secure. It does not contain incompatibility between older and newer systems.

II. HOW E-MAIL WORKS?



In this figure, Bob (a CU student) sent an e-mail from his PC to Jack (a MIT student) through the Internet.
Path 1 - First the e-mail is transmitted to the e-mail server of CUHK.
Path 2 - The e-mail server of CUHK forwards the e-mail to other Internet mail servers called Mail Relays.
Path 3 - The e-mail is forwarded to the e-mail server of MIT. Jack uses his e-mail program to check the e-mail from the e-mail server of MIT.

From above diagram anyone can easily understand the email communication as well as sender and receiver addresses. In Internet e-mail communication, the standard/protocol used for sending/transferring e-mail is SMTP (Simple Mail Transfer Protocol), while the standards/protocols used for receiving e-mail are POP (Post Office Protocol) and IMAP (Internet Message Access Protocol).

III. SECURITY ISSUES IN INTERNET E-MAIL:

Secrecy:
The content of email is in plain text format. While it is transmitting it never decrypted so data can be easily revealed if one can get access of your mailbox and one can knows how to tap network and flow.

Integrity:
Integrity means changes the original data. Email is mainly stored in plain text and also transmitted in plain text. So anyone can easily hack the way of email transmission and change the original data without being noticed by sender and receiver.

IV. SECURITY ISSUES IN SMTP

Security in information technology is defined as to protect information against unauthorized revelation as well as unauthorized modification. User needs to take care about

possibility of malicious and fraudulent attacks by hackers as well as impact of viruses and denial-of-services attack. Some of approaches that is useful for security of your system includes:

A. Authentication

Techniques can be used to identify and verify if anyone is seeking to access unauthorised system.

B. *Access control*

Users can be restricted to ensure they only access data and services for which they have been authorised.

C. Encryption

Techniques that scramble data is used to protect information while transmitted data over network.

D. Firewall

Firewall is mainly used to differentiate the internal and external information access. Firewall prevents the outsiders to access information within organization.

E. Intrusion detection

Techniques that monitor the system and network to check whether anyone is trying to access network without authentication.

F. *Anti-virus software*

Can detect viruses and prevent access to infected files.

For E-mail security, Simple Mail Transfer Protocol (SMTP) is the first protocol which is used for security purpose.
In E-mail messaging, security contain
i) Privacy,
ii) Sender authentication,
iii) Message integrity,
iv) Non-repudiation,
v) Consistency

i. Privacy guarantees confidentiality of a message transmitted over network otherwise it can be altered.
ii. Sender authentication is the verification of the identity of the sender
iii. Message integrity refers to policies that ensure security against fake mail which includes policies to stop transmission of spam e-mails.
iv. Non-repudiation means sender should not refuse an emails sent by him.
v. Consistency means uniformity of data from source to destination.

V. LIMITATIONS OF SECURITY PROTOCOLS

For privacy and authentication of sender SMPT provide lack of security. Using many intermediaries like routers, and mail servers we can pass Email from sender to recipient which is in plain text format. Thus it is very difficult to both physical and virtual malicious attackers who can access to email & can read it. Even when these are deleted by the users from their mailboxes E-mail Service Providers (ESPs) have capabilities to store copies of e-mail messages.
It is possible to send spam and phishing e-mails because there is no such mechanism to authentication and not even have security feature for message integrity. There may be several problems because of Spam like misuse of storage space, computational resources, network conjunction, legal issues, financial losses and other related attacks like spread of viruses, worms and Denial of Services attacks.
To make communications secure and private, SMTP servers incorporate one or more security features but it has several limitations.
There are many encryption techniques for e-mail security, some of them are Secure Multi-purpose Internet Mail Extensions (S/MIME), Privacy-Enhanced Mail(PEM), Pretty Good Privacy (PGP) etc. which are based on Cryptography.
The use of PEM is very negligible because it lacks flexibility and also it requires a single Certificate Authority (CA). Use of PGP is occasional and it is based on PKI scheme and limited to a smaller user community. To add cryptographic security services to emails we can use S/MIME protocol.
We need not to make any S/MIME change in the sending and receiving MTAs or the e-mail transmission process since this functionality is already added at client software which is at sending and receiving client.
Since S/MIME uses encryption and digital signatures in basic form by making use of sender authentication, non-repudiation of sender, message integrity. Security service allow us to send signed messages, received sign messages, encrypted messages. As compared with other protocol this is most widely used protocol even though it has several disadvantages.

VI. DIFFERENT TYPES OF SECURITY ATTACKS

A. Passive Attacks

Passive attacks break the whole system using observed data. For Example, sender and receiver both have plain text of data which is already known to the attacker. Some properties of Passive Attacks:

I. Interception: It involves accessing the data of an e-mail and making it available to someone other than the sender or intended recipient. It also called “Man in the middle” attack.
II. Traffic analysis: This technique that look like communication pattern between entities in a system.

B. Active Attacks

In this attack the attacker sends data to both sender and receiver or sometimes completely cut off the data stream.
Active attack has some properties:

I. Interruption: Attacker prevents the original sender to access the site. It attacks the availability called DOS attack.
II. Modification: Information is transmitted in plain text. Attacker mostly changes data during transmission.
III. Fabrication: Without authentication attacker create false account or items.

C. DOS Attack

In network security DOS attack is major issue. If anyone has basic knowledge of security then he can easily launch the attack on network. Other attacks take more time but this attack does not take more time and plan to execute. DOS attack is very powerful it can be shutdown company network. The main task of this attack is checking availability and continuously sends the request over network. Triton is network tool which is available on internet. It is mainly used for attack any network. Bandwidth, TCP connection, CPU cycle is main part of network for attack. Zombies are a network of multiple users in a same network where this attack is initiated. Computer is infected by these attacks but users are unaware of this thing.

VII. WHAT ARE THE THREATS TO EMAIL SECURITY

A. Viruses

Email security contains multiple issues. Virus is most high risk issue in network. Virus has capability to destroy whole data at a time. When virus found in any email it can be bring down entire mail system and it often in large amount in a single mail.
Many issues are affects system but virus is stronger than any other. Virus is staying long and destroys data immediately. It does not remove by any antivirus product. Virus leaves its impact for long time and recovery takes large amount of money, resources and efforts as well as lost computer information.

B. SPAM

SPAM is another major issue in network security. Viruses and SPAM is goes hand in hand. Spam is also known as junk email. SPAM mail contains malicious code which affects mail system immediately. SPAM mail contains virus which down the entire system. Users cannot request any mail but them getting number of mails of unintended user which can be a SPAM mail. Mail filtering cannot filter legitimate email from SPAM. Virus and SPAM have negligible difference.

VIII. DEFENCE AGAINST EMAIL SECURITY ATTACKS

Now a day's in market variety of email security products are available. They come in the form of special software that you can load on an existing mail server or on a dedicated mail gateway platform, or in the form of a hardware appliance that acts as an email gateway. There is another option for companies is to outsource the mail security to an outsource service provider. All of these products offer same feature set but actually it different from each other.
Today in market some common features of all products in mail security are antivirus, Script removal, antispam, HTML tag removal, block of attachments by file type, scanning of inappropriate content and confidentiality checks.
In all above products mostly antispam methods supported by products include real-time blackhole lists (RBL), heuristics, confirmation process, Bayesian filtering, open relay protection, size and bandwidth control, and encryption.

A. Sender Policy Framework

There is first technology invent to authenticate sender of email is Sender Policy Framework. Developer of this method is Meng Wong who's main aim is to identify original sender or receiver of email message.

I) How does it work?

Every domain has its own sender and receiver. Now a days to know everybody about what machine receive mail for their own domain or not, all domain send MX records to DNS on internet. Only because of this record mail server come to know that where to send mail at which destination. In SPF same functionality is achieved but it is in reverse order of MX record which also specifies which machine sends mail from which domain.
When receiver gets mail, it will get check from SPF record to know where this mail is come from. The FROM is get checked with the column of FROM of SPF record. So, if user get mail from xyz_address@domainName.com then "domainName.com" is get checked from SPF record. Then IP address which is contain in header is cross check with domain ip address. If matches successfully them it's a trustable user or else we can say it is a fake user & email may contain spam or virus.
SPF used by envelop sender who uses "MAIL FROM" not "FROM" as a return path of their email. So we can say that SPF is used to authenticate return path security. We can use cryptographic techniques such as PGP,S/MIME for header.

B. Caller ID

For Sender authentication there is also another method known as Caller ID which is developed by Microsoft. Caller ID is similar method as SPF just the difference is Caller ID method uses Purported Responsible Address (PRA) record, instead of SPF record. Difference between two methods is the use of algorithms to check authenticity of address.SPF based on most visible address of sender but PRA based on most recent sender to check records. So as we can say that PPRA specify most recently mails come from where as SPF specify initially emails comes from. Microsoft announces this year that they are going to proposing a hybrid specification for Caller ID that is they are going combine Caller ID technology with SPF. And it will know as Sender ID Framework.

C. Encryption

Encryption methods are used to prevent hackers from listening data. To prevent MAN in the middle attack during data transmission various methods are used like HTTPS and SHTTP. These techniques are also preventing sniffing of data. Data is transmitted in the encrypted format. For encryption Virtual Private Network is used. VPN is mainly used for improving user's privacy. Many mails contain

malware and viruses but encryption allow those mail to enter the network because firewall prevent these attacks. CPU provides processing power to encrypted data. It takes more time for processing as well as reduces speed at which data can be sending.

D. Defence against DOS Attacks

There are many technologies have been developed to prevent DDoS attack such as intrusion detection systems (IDSs), firewalls, and enhanced routers. Between internet and server all above things are used. They protect the network by monitoring all incoming and outgoing connections. Traffic analysis, redundancy contain in them. There is a log maintain for incoming and outgoing connection by IDSs. To detect potential Dos attack these log is compared to the baseline traffic. Alert system of Dos attack such as TCP SYN flooding is available if there is high traffic in on-going data. Every network have its own firewall system for prevent attack. If certain mail contain wrong port number, IP address or packets then firewall will prevent these mail to entering in network.
Firewall works on real time evaluation.
Even if Dos attacks takes place in the internal network user can protect it by employing security measures in routers which can create another defence line. Service provider is mainly increase the service quality of infrastructure. Dos attack effect is negligible when backup server is in use. Dos attacks are prevent by only those service provider who can able to distribute heavy traffic of Dos attack over a network.

E. Establish clear rules about email usage

Email is the perfect communications tool for an organization. Today's day to day life is dependent on Email for both internal and external communication. It is very important setting out the rules for how it should be used is essential.

The starting point is to define a clear and transparent framework for behaviour setting down what's acceptable and what isn't. As an example, typical clauses might be:

I. Don't forward or send email containing pornographic images.
II. Attachment should be of 5MB in size.

With the AUP in place, you can then focus on ensuring that your practices are compliant with the wide range of local that extend into email communications.

F. Prevent data loss via email

Your system may hold important business information. It must be protected carefully from accidental disclosure of confidential information to parties outside and within your organization. Some of the processes will be covered by your AUP, but new employees, leaving employees can all maliciously threaten the security of your data. It is essential to put in place an automated, centrally managed mechanism to prevent data loss regardless of intention your employees.

This solution should be:

1) Emails should be block by the file types of their attachments
2) Scan messages for keywords
3) Add denial and banners to mail in all directions
4) Encrypt messages so that only the intended recipient can read them
5) Ensure that your email system is not being abused by malicious users.

G. Maintain visibility over and access to current and past traffic

You need to aware of the email coming into, going out of and circulating around your organization. This means you must: Maintain accessible records of relevant email communications, including log information that can show who sent what to whom and when.

1) Copy sensitive messages, both internal and external.
2) Be able to intercept and re-route violating messages to those responsible for enforcement so that potentially damaging incidents can be avoided and remedial efforts can take place.

It is important that not every email contains sensitive data, so not everything needs to be encrypted. Depending on your authority, there are limits on how long you must maintain copies of email communication.

The cost of storing and accessing large volumes of email requires you to be deterministic when it comes to what needs archiving or encryption, and how long you should be storing.

H. Eliminate spam, phishing and malware

One of the main ways that virus get entered onto your computers or into your systems is through email. Spam push changes in order to attempt to avoid detection use a variety of methods to steal confidential business and personal information.
You must ensure that your email infrastructure is protected against malware, viruses, spyware and other threats to system and data integrity. For this solution is that blocks malware, spam, Denial of Service attacks, and harvesting of email addresses .By blocking threats through your internal mail servers and desktops, you will eliminate most of the external risk associated with data loss. Your AUP will go a long way toward covering the remaining internal risk.

IX. CONCLUSION

From the last few years the need of email security has also increased. Internet has become an important part of our daily life and along with that we deal with emails in our day to day work. As more and more users connect to the internet it attracts a lot of criminals. Today, everything is connected to internet from simple shopping to protect secrets so there is need of network security. Billions of dollars of transactions

happens every hour over the internet, this need to be protected at all costs.

Even a small unnoticed moral attack in a network can have very unfortunate affect, if companies records are leaked, it can put the users data such as their banking details and credit card information at risk, numerous software's such as intrusion detection have been which prevents these attacks, but most of the time it's because of a human error that these attacks occur. Most of the attacks can be easily prevented, by following many simply methods as outlined in this paper. As new and more sophisticated attacks occur, researchers across the world find new methods to prevent them.

REFERENCES

[1] http://en.wikipedia.org/wiki/Email_privacy
[2] http://www.theemaillaundry.com/content.php?cid=58
[3] http://www2.trustwave.com/rs/trustwave/images/Best_Practices_in_Email_Web_and_Social_Media_Security_Trustwave.pdf
[4] Banday, M.T., Qadri, J.A. (2010). "A Study of E-mail Security Protocols," eBritian, ISSN: 1755-9200, British Institute of Technology and E-commerce, UK, Issue 5,Summer 2010, pp. 55-60, available online at: http://www.bite.ac.uk/ebritain/ebritain_summer_10.pdf.
[5] ApuKapadia, (2007) "A Case (Study) For Usability in Secure E-mail Communication", IEEESecurity & Privacy, pp. 80-84.
[6] P. Hoffman, (2002) "SMTP Service Extension for Secure SMTP over Transport Layer Security", IETF RFC 3207.
[7] C. Moris and S. Smith, (2007) "Towards usefully Secure E-mail", IEEE technology and SocietyMagazine, pp. 25-34.
[8] J. Lyon and M. Wong, (2006) "Sender ID: Authenticating E-mail", Internet Engineering TaskForce (IETF), RFC 4406.
[9] http://www.microsoft.com/presspass/features/2004/Feb04/02-24CallerID.asp
[10] Tony Bradley(2000), CISSP-ISSAP,E-Mail Virus Protection Handbook
[11] John Wiley & Sons, ISBN : 047105318X, (1995), E-Mail Security,How to Keep Your Electronic Messages Private