A Survey of Challenges in E-Mail Security

Priya. R¹ & Malathi. M²

¹PG and Research Department of Computer Science, Government Arts College (Autonomous), Salem-7.
²Assistant Professor, M.C.A., M.Phil., PG and Research Department of Computer Science, Government Arts College (Autonomous), Salem-7.

Abstract: E-mail is currently the most widely used communication system in daily life. The main reason for using e-mail is probably the convenience and speed with which it can be transmitted, irrespective of geographical distances. This paper discusses the threats to electronic mail system security such as phishing, spam, virus, spyware, and malware. E-mail security goals of confidentiality, message integrity, authentication, and non-repudiation from original and how to ensure the safety and security of corporate e-mail environment, detailing threats that should be able to avoid them, and tools that should be used to mitigate them.

Keywords: E-mail Security, SPAM, Virus, Phishing.

INTRODUCTION

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

HOW E-MAIL WORKS

A user (Alice) sends an e-mail message and connect to SMTP (Simple Mail Transfer Protocol) Server as configured in her e-mail client or Mail User Agent(MUA). On the SMTP Server, a Mail Transfer Agent (MTA) looks at the recipient address and looks ups the domain part of the address to determine its destination. The main components of an e-mail system that facilitate sending and receiving of e-mails on the Internet are,

- An e-mail client
- An e-mail server (SMTP server)
- POP and IMAP servers.

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).

A. THREATS OF EMAIL SECURITY

1) viruses: One of the most publicized and high risk of all the issues is viruses. Viruses are so dangerous, they often deliver a highly fatal load, destroying data, and dropping down entire mail systems. Most of the viruses that were responsible for actual disasters during that time were either Internet worms or mass mailer viruses. To make matters worse, both of these virus types staying around longer than other types, even after anti-virus products have included protection against them.

2) 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.

3) **Phishing**: Phishing (identity theft), is a newer threat to email security. Phishing is the process where identity thieves target customers of financial institutions, using common spamming techniques to generate huge numbers of emails with the intent of luring customers to spoofed web sites and Trapping them into giving personal information such as passwords.

Phishing is the most common methods of attack. Some of the threat and defenses are as follows masquerading: an attacker pretends to be someone else. In such situation, a criminal can set up a storefront and collect thousands or billions of credit card numbers from unsuspecting consumers.

4) **The man in the middle**: The man in the middle attack and session hijacking attack occurs when an attacker inserts Itself between two parties and pretends to be one of the parties.

5) **Eavesdropping**: Eavesdropping happen when attacker listens to a private communication. The attacker views information as it is sent over the network.

6) **Data Diddling**: Data diddling attack happened when an attacker changes the data while it routing between communication parties.

7) **Dictionary attacks**: a dictionary attack happen when an attacker uses large set likely combinations to guess a secret. aka, an attacker may choose one widely used password and try them all until the password is discovered.

8) **Denial of service (DoS) attack**: denial of service attack occurs when an attacker floods the Email with hundred or even million of messages. Though the attacker does not benefit, service is denied to legitimate users. This is one of the most difficult attacks to thwart.

9) **Spyware Threats**: A serious computer security threat, spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information. We’ve amassed a wealth of knowledge that will help you combat spyware threats and stay safe online.

10) **Hackers**: People, not computers, create computer security threats and malware. Hackers are programmers who victimize others for their own gain by breaking into computer systems to steal, change or destroy information as a form of cyber-terrorism.

11) **Viral Web Sites**: Users can be enticed, often by email messages, to visit web sites that contain viruses or Trojans. These sites are known as viral web sites and are often made to look like well known web sites and can have similar web addresses to the sites they are imitating. Users who visit these sites often inadvertently download and run a virus or Trojan and can then become infected or the subject of hacker attacks.

12) **Spyware, Adware and Advertising Trojans**: Spyware, Adware and Advertising Trojans are often installed with other programs, usually without your knowledge. They record your behaviors on the Internet, display targeted ads to you and can even download other malicious software on to your computer. They are often included within programs that you can download free from the Internet or that are on CDs given away free by magazines. Spyware doesn’t usually carry viruses but it can use your system resources and slow down your Internet connection with the display of ads. If the Spyware contains bugs (faults) it can make your computer unstable but the main concern is your privacy. These programs record every step that you take on the Internet and forward it to an Ad Management Centre which reviews your searches and downloads to determine your shopping preferences. The Ad Management Centre will build up a detailed profile of you, without your knowledge, and can pass this on to third parties, again without your knowledge. Some Spyware can download more serious threats on to your computer, such as Trojan Horses.

13) **Bluesnarfing**: The act of stealing personal data, specifically calendar and contact information, from a Bluetooth enabled device.

**DIFFERENT TYPES OF SECURITY ATTACKS**

**A. Passive Attacks**

The attacker tries to learn something from the data or information from the system. 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:

1. **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 looks like communication pattern between entities in a system.

B. Active Attacks

In this attack in which the attempts are made to alter, modify, delete or the attacker sends false 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, an attacker creates false account or items.

C. DoS Attack

In network security, DOS attack is a 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 a network. The main task of this attack is checking availability and continuously sends the request over the 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 the network for attack. Zombies are a network of multiple users in the same network where this attack is initiated. The computer is infected by these attacks but users are unaware of this thing.

Some of the approaches that are useful for security of your system includes:

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

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

III. Encryption: Techniques that scramble data is used to protect information while transmitted data over the network.

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

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

VI. 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 contains,

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 e-mails sent by him.

V. Consistency: means uniformity of data from source to destination.

DEFENCE AGAINST E-MAIL SECURITY ATTACKS

Now a day’s in a 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, the 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, the confirmation process, Bayesian filtering, open relay protection, size and bandwidth control, and encryption.

**Sender Policy Framework**

There is first technology invented to authenticate the sender of email is Sender Policy Framework. The developer of this method is Meng Wong who’s main aim is to identify original sender or receiver of an e-mail message.

**Caller ID**

For Sender authentication, there is also another method known as Caller ID which is developed by Microsoft. Caller ID is a similar method as SPF just the difference is Caller ID method uses Purported Responsible Address (PRA) record, instead of SPF record. The difference between two methods is the use of algorithms to check the authenticity of address. SPF based on a most visible address of sender but PRA based on most recent sender to check records.

**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 allows those mail to enter the network because firewall prevents these attacks. It takes more time for processing as well as reduces speed at which data can be sending.

I. Don’t forward or send e-mail containing pornographic images.

II. The attachment should be of 5MB in size.

**Prevent data loss via e-mail**

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.

6) Copy sensitive messages, both internal and external.

**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.

**Conclusion**

In this we conclude the different types of e-mail threats and its solution. 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.

**References:**

[1] SANS Institute InfoSec Reading Room Securing E-mail


[3] SANS Institute InfoSec Reading Room “Email Security Threats”


Imperial Journal of Interdisciplinary Research (IJIR)