A Survey of Email Service - Attack, Security Method and Protocols

Sanjukta Mohanta¹, Shriti Banerjee², Shivani Awasthi³ Shivani Awasthi⁴

¹ Dept. of Computer Science & Engineering, Arya College Of Engg. & Research Centre, Jaipur, Rajasthan
² Dept. of Computer Science & Engineering, Arya College Of Engg. & Research Centre, Jaipur, Rajasthan
³ Dept. of Computer Science & Engineering, Arya College Of Engg. & Research Centre, Jaipur, Rajasthan
⁴ Dept. of Computer Science & Engineering, Arya College Of Engg. & Research Centre, Jaipur, Rajasthan

Abstract—Electronic-mail is one of the most important and common method of communication today. It is the main resource of enterprise’s communication on the internet. Many files such as audio, video, messages, documents are sending through email. Cyber criminals are misuse of it. Any person can send threads, spam mail, phishing e-mail and many more criminal activities. So in this paper I represent that, it is necessary to safe yourself on the own-level by secure your email and avoid the scam email which are send by the criminals. And also set a strong password such that anyone cannot access your e-mail without your permission.

Keywords—E-mail Security, Protocol, Attack, Password protection, 2-step Verification.

I. INTRODUCTION

Now one day cyber criminals are everywhere. We want to stop your criminal activities, but we can not. Because everyone has their own mind, their own thinking. We can not change our minds if they do not want that. They continue to carry out their criminal activity for fun or for any other reason and we have very important documents, personal data and many more. So, we need to ensure all this from the attackers. Although we have many security processes, such as the technique of encryption and decryption of data, secure communication protocols, secure databases to store data. But even cybercriminals have access to our data or information, bank account details, etc. and the improper use of that. Many fraud activities happen in our daily lives due to our lack of awareness of digital security. We need to secure our personal data at our own level. We do not need to trust anyone in our laptops / PCs, mobile phones or any electronic device where our data or information is stored.

Email one of the popular modes of communication. And many important documents are sent by email. So, we need to protect email, therefore, nobody can access our email account without our permission. And we should avoid that kind of fraudulent email. Set a secure password, which is a mix of numbers, symbols and letters.

II. TYPES OF ATTACK

A. Active Attack:

Active attack is method in which the attacker makes a contact with the target system. The attacker sends data to both sender and receiver or sometimes completely cut off the data stream. For e.g. Mirroring website: download all available content for offline analysis. Tools- Teleport pro, iMiser, HTTrack website copier.

Email tracking: examine email processing path. Tools- email Tracker Pro, MSGTAG, Polite Mail, zendio etc.

In this attack Active attack has some properties:

a. Interruption: Interruption means, Attacker prevents the original sender to access the site.

b. Modification: Modification means the attacker can change the data or Information during transmission because the data is in form of plain text.

c. Fabrication: Create false account or items without any permission of that person.
B. Passive Attack:
Passive attack is method in which the attacker never makes any contact with the target system. For example - google search, whose queries, DNS lookup, social networking sites etc.

Some properties of Passive Attacks:

a. Interception: It involves accessing the data of an e-mail and making it available to someone other than the sender or receiver. It also called “Man in the middle” attack.

b. Traffic analysis: This technique that look like communication pattern between entities in a system.

C. DOS Attack
In network security, the DOS attack is a major problem. If someone has basic security knowledge, then you can easily launch the attack on the network. Other attacks take more time, but this attack does not take more time and plans to work. The DOS attack is very powerful and can be a closed network of the company. The main task of this attack is to check the availability and send the request continuously through the network. Triton is a network tool that is available online. It is mainly used to attack any network. The bandwidth, the TCP connection, the CPU cycle is the main part of the network for the attack. The zombies are a network of multiple users in the same network where this attack begins. The computer is infected by these attacks, but users are not aware of this.

III. EMAIL ARCHITECTURE AND WORKING
Email architecture consists of two parts. One is User Agent (UA) and another is Message Transfer Agent (MTA). User agent allows people to read and send mail and Message Transfer Agent (MTA) allows moving the message from source to destination.
B. Post Office Protocol (POP)
Most email clients support either POP3 or IMAP to receive messages. Few Internet Service Products (ISPs) support IMAP.

C. Internet Mail Access Protocol (IMAP)
Support for the internet standard protocols allows other email clients to access these servers. Allows clients to be used with other server. E.g. Qualcomm’s Eudora or Mozilla Thunderbird.

IV. HOW TO PROTECT EMAIL
Do not download any files which are send by the unknown persons. These attached document may contain malicious virus which are not good for our devices and also our data.

For that we can use two-step verification which have two step of verification the e-mail. One is our choose password and another is one time password (OTP) which is dynamic. We get this OTP of our mobile number when we want to log-in the e-mail account of devices. Once we done the OTP verification then you can access your e-mail messages of your devices. For this process some steps are available. I represent all this steps with screenshots.

Step 1:
Step 2:
Step 3:
Step 4:

Step 5:

Step 6:

Step 7:

Step 8:
Step 9:

Confirm that it works

Google just sent a text message with a verification code to 095219 16750.

Enter the code

Didn't get it? Resend

Step 10:

Step 11:

Figure 4: Step by Step Screenshots of 2-Step Verification

Do not share your OTP password with anyone without knowing that persons. OTP password is dynamic password which is used for user authentication. If you share your OTP with anyone then it may happens that your accounts social media bank details etc are accessed by anyone with your permission but you don’t know that person.

Figure 5: OTP Process
V. HOW TO IDENTIFY AND AVOID SCAM EMAIL

One more important thing that is, scam e-mail. Cyber criminals cannot stop their criminal activities. They continuous send you the scam messages. If you open or download these unnecessary files or messages which are send by the cyber criminals then, it is possible that your devices or data crashed or loss. So, do not open scam e-mail and don’t download any files.

VI. PASSWORD PROTECTION

One last thing that cyber criminals accessed your account in many way. They can guess your password and also can find your encrypted password and decrypt it. So you should more secure your password. Do not choose any password like name, surname, date of birth, birth place, any dictionary based word etc. choose a password which is a mixture of letters and at least one number. Change your password after 7 days or 15 days and new password never same as your old password.

VII. CONCLUSION

Email system is system which is mostly used and has complex architecture, agents, services etc. And also have more secure protocols. But still user faced many problems, scam mail etc. So we need to secure our account at ourselves and more aware of the digital security. Further there is also need to update our password after 7 days or 15 days and set a strong password such that, anyone cannot decrypt our encrypted password easily.

References