Survey and Analysis of Attacks via Email Infrastructure

Lavkush Singh
Department of Computer Science and Engineering
NIIT University
Neemrana, India
lavkush.singh@st.niituniversity.in

Deverapally Viharika
Department of Computer Science and Engineering
NIIT University
Neemrana, India
deverapally.viharika@st.niituniversity.in

Pendyala Revanth
Department of Computer Science and Engineering
NIIT University
Neemrana, India
p.revanth@st.niituniversity.in

***Abstract*—Email Security is a most sensitive issue in the domain of cyber and information security. Since Emails are used in everyday life as an integral part of communication, they are required to be secured against the malicious users outside. The email infrastructure is well secure enough, still they are used to deploy a variety of attacks on user. With the revolution in the technology, various solutions and different standards levels have been designed and implemented complying with the security requirements. The most basic thing which we follow today is various email filtering systems as the defense against attacks using email. This paper aims to review the different kinds of attacks which happens by the use of email. This paper also discusses briefly about different types of attacks and the counter measures which are used to deal with them. Finally, our paper will also describe several techniques to counter those attacks.**

Keywords—component, formatting, style, styling, insert *(key words)*

I. Introduction

The Email protection is the important tool for enterprise and communique, that are used greater day by day. The Email is used for sending textual content, documents and statistics of tables at paintings and at domestic. Because of being the information transmitting is pretty delicate method, the guarantee of those records is questionable and this represented a trouble due to the fact the contract details of the competitive corporations are unlimited, and the more serious, there are competencies for fraud Emails. It is very important that the email data stays confidential otherwise it can cause serious damage to the enterprise and communique. Data exposure via email communication has now turned into a problem of greater magnitude. A single wrong-click can expose top secret information, make known private financial statements, and expose sensitive negotiations. Owing to such reasons it has become extremely vital to go in for email encryption.

II. EMAIL Technology and its working

A. What is an email?

Email is the short of Electronic mail, which refers to the digital mode of communication wherein an electronic letters are send across a sender and receiver using email id. AN email ID is identical to a unique identifier, which identifies the individual to send or receive emails. It can be used with either web applications or computer programs or with mobile applications. Now a days, due to its high reliability and fastest mode of transmission, emails have become an integral part of our lives.

B. How Email Works?

Email systems comprises of message processing and storing computer servers of the users who connect to the email infrastructure.

The two major components are:

a. Email servers

b. Email Clients.

Email Servers are basically entities which are responsible for functions like to store, to receive and to forward the emails coming from user and to the intender user. These messages are communicated to servers and exchanged via protocols like SMTP and mail agents, often called as Mail Transfer Agents (MTAs) like Postfix, Sendmail etc. Servers are therefore used to store the messages for the access by the user to view in email clients or to download for the offline use.

Servers receive the email if the delivery can happen else a negative acknowledgement or the delivery failure message is sent to the sender. This helps to ensure the integrity that the email is either received or is failed, It does not vanish in between.

Three major types of email servers are:

i. SMTP servers

ii. POP servers

iii. IMAP servers

When a message is framed, it is sent by the sender to the receiver, the email hops through multiple places to reach to the destination. An email is composed using a identifier called the email address.

Here is the step wise illustration of how email works:

1. A user X composes the message, and hits the 'Send' button. This connects him to his configuration based on his Mail User Agent (MUA) or email client to Simple Mail Transfer Protocol (SMTP) server.

2., Mail Transfer Agent (MTA) located the recipient address on the SMTP server domain is resolved to find the receiver's address.

3. Then after DNS or Domain Name System is queried for the corresponding the Mail exchanger (MX) associated to the domain name of the recipient.

4. Then message will be sent by the SMTP server to that found server via the SMTP protocol.

5. The message will be stored by the receiving server which in turn will make it available to the intended recipient who will be able to view and access via any desired from, be it POP or WEB or IMAP.

III. Review of Literature

Author of [1] presents a survey on students in Croatia about how much they're aware of social engineering and phishing attacks. The survey was conducted in the form of graphical questionnaire. A real practical phishing were made to happen on the students which meant to identify what kind of scams or attacks were successful against students. This paper also discusses the security measures against phishing attempts. Although there were certain limitations such as fewer sample space of the target, the violation of cyber laws, 'testwares' instead of the real malwares and few others, still the results were discussed. The results were that roughly about 59% students fell in the trap of those phishing emails. The paper concluded that students require information, awareness and guidelines to safeguard themselves against these attacks. Students with no or minimal theoretical knowledge were the easier target and were more in number in the result set.

Author of [2] talks about the wireless sensor networks and the spoofing attacks. Sensor networks are essential because they record and analyses the sensitive information. Therefore their security cannot be ignored. The author describes their working mechanisms and analyses the different defense mechanisms against the spoofing attacks along with their advantages and disadvantages. Few preventive measure of spoofing includes Forge Resistance Relationship with Rate, Change – Point Detection Method, Trace route and Cooperation with Trusted Adjacent Nodes Based Method, Analysis (FRR-RA) Method and many others. Since wireless sensor networks are distributed in ad-hoc manner, author concludes that there is no such ideal solution as such. With increasing security, the cost becomes significant.

Author of [3] studies the 'Wannacry Ransomeware' in great details and talks about it. Although author admits that a malware analysis is time consuming, the paper aimed at exploring behavioral indicators and further extracting the indicators of compromise. Analysis were performed using 'Yara' tool and formulation of cyber threat intelligence into structured formation using the collected information. The paper conducted in depth analysis to understand process, registry, file system, and network activities and suggested the application of malware database synchronization will provide protection against the subsistence growth of threats against ransomware.

The email communication are integral part of our lives, Authors of [4] presents the detailed survey on email attacks and talks about the threats and the threat avoiding counter measures. Author covered a variety of attacks like Eavesdropping, Identity theft, Spoofing, Emails used for sending threats and etc. Then Security is discussed, Email Security via different techniques such as Using Encryption and Compression, Secure Server Verification by Using RSA Algorithm and Visual Cryptography and others. Paper also suggests that since there is no comprehensive solution to the Email security attacks, however, combined methods should be adopted in order to secure ourselves from attacks based on the requirements.

Author of [5] highlights the analysis of Ransomware threat and its consequences. Paper reveals that across the globe, people are intensively subjected to extortion, in a very large scale. This paper describes what exactly is ransomware, its different kinds, working and preventive measures. It can spread via zip file, SMS, emails and many different modes. The paper suggests different counter measures to mitigate this ransomware attacks. Stating a few like using antivirus, updated firewall, keeping regular interval backups at remote locations etc.

Author of [6] throws light upon phishing attacks in depth. It's a type of attacks which aims at collecting victim's sensitive information. Like passwords, financial, personal etc. Authors have implemented Linkguard Algorithm in Windows XP which they claimed that experiments verified that they were able to detect roughly 96% of the phishing links. Since phishing attacks are characteristic based, their proposed algorithm is successful in detecting unknown phishing attacks too.

Author of [7] presents the literature survey on social engineering attack, particularly the phishing attack. It also highlights the ways in which phishing attack can be harmful, the personal impact in can have in the lives of people. The paper describes Trojan horse, Tab-napping, spoofing emails etc. along with ways to avoid them. Different techniques have also been discussed by the author to detect them and then to deal with them. This paper is a detailed and throughout analysis of Phishing with their cause and effects

IV. ATTACKS THROUGH EMAIL COMMUNICATION

A. *Man in the Middle Attack*

In email communication, an email can have malware attached to an attachment. If the recipient of the email opens the attachment and the malware is released onto their computer, the attacker can gain access to the user's web browser. He can, for example, see the data that is sent and received during financial transactions and conversations. To prevail over the Man in the middle attack, encryption services can be employed.

B. *Identity Theft*

Identity theft can be committed through e-mail (phishing) or other means, such as regular mail, fax or telephone, or even by going through someone's trash. Identity theft occurs when someone uses your personal information such as your name, Social Security number or other identifying information without your permission to commit fraud or other crimes. Typically, identity thieves use someone’s personal data to empty the victim’s financial accounts, run up charges on the victim’s existing credit cards, apply for new loans, credit cards, services or benefits in the victim’s name, file fraudulent tax returns or even commit crimes. To counter the identity theft, enhancing of user skills can be used.

C. *Email Header Spoofing*

Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a tactic used in phishing and Spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation. Email spoofing is possible because the Simple Mail Transfer Protocol (SMTP) does not provide a mechanism for address authentication. SPF protects domains from email spoofing by defining the IP addresses that can send emails from that domain. DKIM implements automatic email signing. A DKIM signature protects the integrity of the email, preventing the content from tampering before it is delivered. DKIM uses DNS TXT records to publish the public keys, so anyone can check an email’s validity.

D. *Account Enumeration*

A clever way that attackers can verify whether e-mail accounts exist on a server is simply to telnet to the server on port 25 and run the **VRFY** command. The **VRFY** command makes a server check whether a specific user ID exists. Spammers often automate this method to perform a directory harvest attack, which is a way of gleaning valid e-mail addresses from a server or domain for hackers to use. The **SMTP** command **EXPN** might allow attackers to verify what mailing lists exist on a server. You can simply telnet to your e-mail server on port 25 and try **EXPN** on your system. Disable **VRFY** and **EXPN** unless you need your remote systems to gather user and mailing list information from your server. If you need **VRFY** and **EXPN** functionality, check your e-mail server or e-mail firewall documentation for the ability to limit these commands to specific hosts on your network or the Internet.

E. *SMTP Relay*

SMTP relay lets users send e-mails through outside servers. Open e-mail relays aren’t the problem they used to be, but you continue to need to test for them. Spammers and hackers can use an email server to send unsolicited mail or malware through e-mail under the guise of the unsuspecting open-relay owner. Some of the counter measures against SMTP relay can be disable SMTP relay on your e-mail server. Enforce authentication if your e-mail server allows it.

F. *Denial of Service Attack*

Denial of Service attacks can prove extremely damaging, as they can render the whole service out-of-commission for long periods of time. This can have double costs in remediation as well as lost reputation and customer loyalty. To prevent DoS attacks, you need to limit the amount of both general overtime and simultaneous connections to the SMTP server. Other ways to protect the server from large quantities of Send messages include Mail Relay and Reverse DNS.

G. *Non-Delivery Report (NDR) Attacks*

As a first Step, Spam email is created with the intended Spam victim's address in the sender field and a random, fictitious recipient, at your domain, in the To: field. And next, Your mail server cannot deliver the message and sends an NDR email back to what appears to be the sender of the original message, the Spam victim. The return email carries the non-delivery report and possibly the original Spam message. Thinking it is email they sent, the spam victim reads the NDR and the included Spam.

H. *Phishing Attacks*

Phishing attacks refers to the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication. Its main intention is to gather personal information using deceptive e-mails and websites. Through email, a link or a deceptive add can be sent to the victim which makes him believe that the email is genuine and he clicks on it. He then is redirected to any of the legitimate-looking malicious cite which collects his information to exploit him.

There are different types of phishing attacks depending upon how they are crafted. For example Spear phishing, where attackers try to craft a message to appeal to a specific individual, Clone phishing, where an attachment or link within the email is replaced with a malicious version and then is sent to the victim to target and Whaling, which is a special type of Spear phishing attacks, directed specifically at senior executives and other high-profile targets of any company or organisation, also sometimes called as Business Email Compromise (BEC).

I. *Malware*

Software which is specifically designed to disrupt, damage, or gain authorized access to a computer system tricks you into installing software that allows scammers to access your files and track what you are doing exploits target system vulnerabilities, such as a bug in legitimate software (e.g., a browser or web application plugin) that can be hijacked. A malware attack is a piece of malicious software which takes over a person’s computer in order to spread the bug onto other people’s devices and profiles.

V. Vulnerabilities in Email Communication.

A. *Identity Spoofing*

Identify spoofing is one of the primary vulnerabilities inherent to the layout of the e-mail machine. In an perceive spoofing assault an adversary is capable of impersonate the identity of a valid electronic mail user and ship emails to third events on his behalf. In most of the assault situations the legitimate person will in no way realize that a person has impersonated his/her identification.

Even a basic identification spoofing assault could be very hard to locate by means of the common consumer, due to the fact that the e-mail appears to be indistinguishable from what will be a valid one. However, very superior users and protection specialists could decide that the source e-mail deal with turned into spoofed through analysing the email headers inserted by using the SMTP servers involved inside the communication.

Detecting more complex email spoofing assaults is often infeasible until specific security features, inclusive of the ones a good way to be defined inside the subsequent bankruptcy, are installed region.

B. *Alteration of Email Content*

Similarly to the state of affairs of the identity spoofing, an attacker can also abuse the lack of safety of the integrity of the facts to alter the content of legitimate emails which can be dispatched or acquired by customers.

Even if no identification spoofing is achieved and the e-mail received with the aid of the user became virtually sent via the recipient, it is still viable for its content to have been modified with the aid of an attacker. Moreover, this holds proper both for the content of the email, in addition to for any viable attachments that the e-mail would possibly include, which include a PDF file.

C. *Confidentiality of Email Communications*

The email system assumes that all the users involved in the communications, as well as the communication links can be trusted and are secure. In reality this is different. For example, the communication between SMTP servers for email delivery takes place through the public Internet and it is susceptible to be intercepted by third parties. In real world, absence of security measures, such as end to end encryption, encryption with PGP etc. There is no certainty that communication is secure and private.

VI. Attack Vectors

A. *SMTP-SMTP Server Communication*

The communication between two SMTP servers is considered to be more vulnerable component of email infrastructure. The Original SMTP Protocol was built under assumption that SMTP servers trust each other, so no additional security features were initially built-in into the design of the protocol. Consequently, while a SMTP server contacts every other server to send a given message, there's an implicit assumption that none of the events concerned inside the communication will act in a malicious way and that the network communication channel is secure.

In Real-time communication, neither of these 2 assumptions is correct. On the one hand, the verbal exchange among SMTP servers doesn't take place via secure dedicated channels but via the Internet. On the other hand, the identification of the SMTP servers isn't always at the same time authenticated and the emails requested to be added, each for the content and related metadata, are assumed to be legitimate. An attacker could also employ active means in order to perform a Man-in-The-Middle attack at network level to change the flow of communications to his/her advantage and be able to monitor the communication. Another possible attack can be email identity spoofing, In order to perform this attack, the attacker isn't always required to tamper with the network communications of a valid e-mail delivery of every other SMTP server. Internet IP connectivity and a simple TCP connectivity are sufficient to execute the assault, furnished no additional measures are used by the recipient's SMTP.

B. *User to Server Communication*

The user to server communication can also be attacked with a purpose to send emails with a spoofed identity, eavesdrop or alter the content of dispatched and acquired emails.

In the absence of implicit or specific SSL, the emails retrieved over POP3 and IMAP protocols can be passively eavesdropped. An attacker able to reveal the IP conversation between the person email client and the POP3/IMAP4 server may be capable of retrieve the entire content material of the emails retrieved by using the person. Furthermore, the attacker would additionally be capable of retrieve the user name and password of the user that is transmitted over the community as part of the POP3 and IMAP authentication process. Once in ownership of this statistics the attacker may want to without delay connect himself to the server and absolutely impersonate the consumer. In the ones instances, inclusive of IMAP4, wherein a copy of the emails is continually stored within the server, the attacker could be able to remotely retrieve all of the emails ever received with the aid of the sufferer.

In addition to the attack vectors formerly described, the shortage of security within the SMTP and POP3/IMAP communications also can be exploited in extra extraordinary ways, together with transparent alternative of electronic mail content material or spoofed electronic mail injection without delay to the customer software because it retrieves the emails from the server's inbox.

VII. Email Privacy And Security Measures

In order to secure the email from the source it originates till it is received, we need to make it so secure that it should be authentic, shouldn't be tampered while transition to reception of email ensuring integrity. Therefore, the factors of CIA (Confidentiality, Integrity, and Authentication) principle applies to email security as well.

a. Confidentiality: The email must be encrypted while transit such that it does not gets tampered by eavesdroppers.

b. Authentication: The email must come from a genuine sender and not from spoofed address.

c. Integrity: The email must be send and should be the original as what the sender framed it initially.

A. *Email Security Using Encryption and Compression [8]*

This method as a conventional way uses a Codebook to Send Email to impart privacy. To enhance the protection of the emails across the internet transition Compression, Decompression, Encryption and Decryption algorithms are used. Although the key is defined from the receiver's user id, cipher text is formed by changing the character with different keys and the key is set to increase by one at the moment. The subsequent features are also suggested by the algorithm like to secure Email, Encryption of the messages and to counter the traffic overhead, message compression and then transmission via channel.

B. A Uniform Approach for Multilevel Email Security Using Image Authentication, Compression, OTP & Cryptography [9]

For Email files security, this technique identifies novel Email security multilevel design structure. The proposed design deals with three security standard that is model matching, pressure & cryptography in light of characteristic through confirmation of picture. The messages transit in the middle of sender and receiver can be a real challenge to security. So many programming adjustments has been proposed to resolve these issues.

C. Design of Fully Deniable Authentication Service for Email Applications [10]

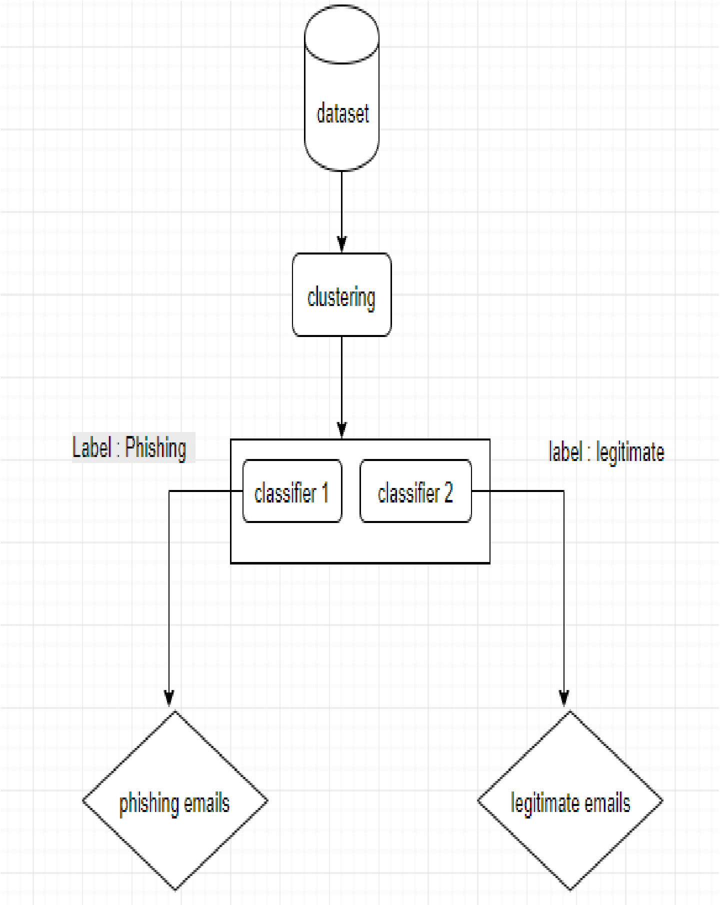
In this method, Email authentication service will be a full deniable. It can be easy fused the work described into the already existing Secure/ Multipurpose Internet Mail Extensions(S/MIME) and Pretty Good Privacy (PGP) to provide message authentication without nonrepudiation proof. The aim of this method may be a distinct message receiver to message authentication. Also this technique allows the user composing the message to be able to refuse message generation. This saves the privacy of the personal message as an advantage.

D. New Secure E-mail Scheme Based on Elliptic Curve Cryptography Combined Public Key [11]

This method supplies strong perfect security for example data integrity, authentication, data confidentiality and nonrepudiation of origin. To prepare the third online certificate agent becomes optional and not necessary if compared with other Email like S/MIME or PGP protocols to secure the email. Therefore as an added advantage, it takes lower capability of computing and is easier than other systems of Email Security. For Private networks and for the implementation in intranet environment, the proposed method is appropriate and desirable.

E. Multi-Classifier Integration Approach for Phishing Email Detection

Three algorithms will be used to build the Multi- classifier version Logistic regression,
Decision Tree, the two algorithms will take a look at the email synchronization whether or not it's phishing or legitimate then analyze the result.



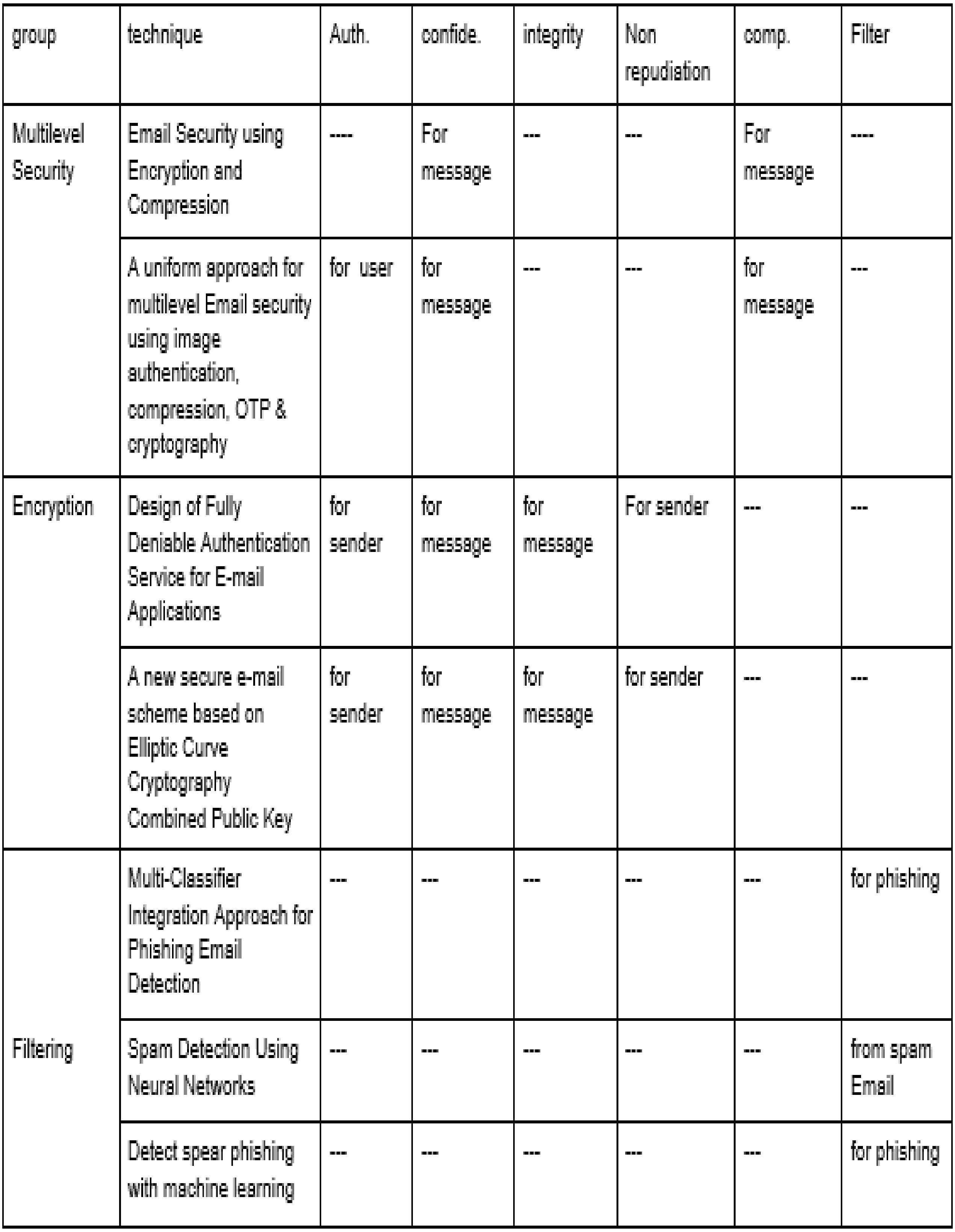
F. Spam Detection Using Neural Networks

Neural networks are powerful machine learning algorithms. They are primarily used for classification problems. In this problem, we're given a gaggle of emails (in uncooked form or in processed shape) and we also are given labels of those emails (junk mail or no junk mail). Then, we're given a hard and fast of new emails (take a look at statistics) and we should label each email within the test set as spam or no junk mail. So, based on this neural network paradigm we can classify the spam emails.

G. Detect spear phishing with machine learning

First ways that gadget getting to know can be applied to spear phishing detection is based on a "social graph" of the common place communication patterns within a corporation. For example, members of the identical department in the employer are expected to talk frequently and could have a high degree of interconnectivity. On the flip side, you do not assume the accounting department intern to be often sending emails to the CEO or vice versa.
Building a social graph of a corporation is straightforward. By gazing the records included within the headers of every e mail sent in the employer, connections may be observed while not having to read the contents of the e-mail itself. And by way of weighting connections among enterprise personnel based totally on frequency of communique, a social graph can be created.
Social graph analysis can assist stumble on this form of spear phishing attack.

TABLE 1: COMPARISON AMONG THE EMAIL SECURITY



group	technique	Auth.	confide.	integrity	Non repudiation	comp.	Filter
Multilevel Security	Email Security using Encryption and Compression	----	For message	---	---	For message	----
	A uniform approach for multilevel Email security using image authentication, compression, OTP & cryptography	for user	for message	---	---	for message	---
Encryption	Design of Fully Deniable Authentication Service for E-mail Applications	for sender	for message	for message	For sender	---	---
	A new secure e-mail scheme based on Elliptic Curve Cryptography Combined Public Key	for sender	for message	for message	for sender	---	---
Filtering	Multi-Classifier Integration Approach for Phishing Email Detection	---	---	---	---	---	for phishing
	Spam Detection Using Neural Networks	---	---	---	---	---	from spam Email
	Detect spear phishing with machine learning	---	---	---	---	---	for phishing

TABLE 1: COMPARISON AMONG THE EMAIL SECURITY METHODS

CONCLUSION

Email security becomes an important since they are the integral part of life being the fastest mode of communication. Email communication is a prominent way for individuals and even organizations to communicate. But unfortunately, this facility is exploited by the malicious users to spread crime in the cyber world, for example spreading terror, virus attacks, identity theft etc. Threats are faced by people because of disturbing circumstances residing in the system. Then there it becomes a necessity to make Email system secure by eradicating the existing security flaws. This paper presented the survey and analysis of attacks via email infrastructure. This paper described various solutions to the email security but since there is no common solution to all, set of different solutions should be followed in order to enhance security as per the intensity of the security required.

REFERENCES

[1] Andrić, Jakov, Dijana Oreški, and Tonimir Kišasondi. "Analysis of phishing attacks against students." Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016 39th International Convention on. IEEE, 2016.

[2] Jindal, Keshav, Surjeet Dalal, and Kamal Kumar Sharma. "Analyzing Spoofing Attacks in Wireless Networks." 2014 Fourth International Conference on Advanced Computing & Communication Technologies (ACCT). IEEE, 2014.

[3] Kao, Da-Yu, and Shou-Ching Hsiao. "The dynamic analysis of WannaCry ransomware." Advanced Communication Technology (ICACT), 2018 20th International Conference on. IEEE, 2018.

[4] Al-Mashhadi, Haider M., and Mohammed H. Alabiech. "A Survey of Email Service; Attacks, Security Methods and Protocols." International Journal of Computer Applications162.11 (2017).

[5] Pathak, P. B., and Yeshwant Mahavidyalaya Nanded. "A dangerous trend of cybercrime: ransomware growing challenge." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5 (2016).

[6] Chen, Juan, and Chuanxiong Guo. "Online detection and prevention of phishing attacks." Communications and Networking in China, 2006. ChinaCom'06. First International Conference on. IEEE, 2006

[7] Gupta, Surbhi, Abhishek Singhal, and Akanksha Kapoor. "A literature survey on social engineering attacks: Phishing attack." Computing, Communication and Automation (ICCCA), 2016 International Conference on. IEEE, 2016.

[8] Jain, Yogendra Kumar, and Pramod B. Gosavi. "Email Security Using Encrption and Compression." Computational Intelligence for Modelling Control & Automation, 2008 International Conference on. IEEE, 2008.

[9] Nemavarkar, Apeksha, and Rajesh Kumar Chakrawarti. "A uniform approach for multilevel email security using image authentication, compression, OTP & cryptography." Computer, Communication and Control (IC4), 2015 International Conference on. IEEE, 2015

[10] Harn, Lein, and Jian Ren. "Design of fully deniable authentication service for e-mail applications." IEEE Communications letters 12.3 (2008).

[11] Zhang, Yi, Tianxi Cui, and Hong Tang. "A new secure e-mail scheme based on Elliptic Curve Cryptography Combined Public Key." 2008 IFIP International Conference on Network and Parallel Computing. IEEE, 2008.