[NC-Rase 18]
DOI: 10.5281/zenodo.1485323

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

INFO SECURITY TO E-MAIL: AN OVERVIEW

Prof. N. N. Kasliwal[*1], Srushti G.Waghmare[2] & Shreya A. Pathak[3] & PrachiV. Gawande[4]
[*1]Department of Computer Science and Engineering, MGI-COET Shegaon
[2,3&4]Student of Computer Science and Engineering, MGI-COET Shegaon

ABSTRACT

E-mail security becomes a vital issue to analysis community within the field of data security. Several solutions and standards are designed consistent with the recent security needs in order to boost e-mail security. A number of the prevailing enhancements specialize in keeping the exchange of information via e-mail in assured and integral means. Whereas the others specialize in authenticating the sender and prove that, he will not repudiate from his message. This paper can survey varied e-mail security solutions. We tend to introduce completely different models and techniques accustomed to solve and enhance the security of e-mail systems and appraise each from the reading purpose of security.

I. INTRODUCTION

Nowadays, most people and organizations use the e-mail for different needs to exchange information between users. The e-mail application is the important network applications. It is significant when business, health, and educational communities use it for the exchange of critical information such as business information, health patient record and so on. Usually, the authentication systems rely upon some elements of data (password), the property of the individual (biometrics), or some derived property (tokens). The user is taken into account documented if the authenticating system will verify that the shared secret key was conferred properly. This shared secret secrets required to be encrypted to supply confidentiality that secures it from being sniffed by hackers. Moreover, a message digest ought to be performed conjointly to reassuring the integrity of the message's contents. When both confidentiality and integrity are combined, non-repudiation is assured. so as to secure the info transmission method, the protection of the authentication method ought to be discovered and certify the info is encrypted and decrypted within the correct manner as a result of there are several malware attacks which may infect the system Targeted attacks that exploit vulnerabilities in widespread software package so as to compromise specific target sets are becoming progressively commonplace. These attacks are not machine-driven and indiscriminate nor they conducted by timeserving amateurs.

These pc intrusions are staged by threat actors that sharply pursue and compromise specific targets. Such attacks are usually a part of broader campaigns, a series of failing and fortunate compromises, by specific threat actors and not isolated attacks. The target of the attacks is to obtain sensitive information. Such attacks are sometimes a region of broader campaigns, a series of failing and lucky compromises, by specific threat actors and not isolated attacks. The target of the attacks is to obtain sensitive data. Emails became one in all the foremost oft-used strategies for cyber-attacks. The foremost worrying email-based attack is Targeted Malicious Email (TME) [1] [2]. In TME, attackers send malicious emails to sure individuals targeted in a company, like executives of huge corporations, high-level government personnel, military officials and even known researchers, so as for the attackers to get valuable counseling and latest analysis of the targeted individuals. In TME, Associate in the Nursing email usually has Associate in Nursing attachment with malicious codes which will be put in mechanically upon gap while not the victims realizing it. In some cases, the victims' pc will become the rear door for the attackers United Nations agency successively have the authority to enter the network of the targeted persons and so steal counseling.

The objective of this paper is to discover the malicious spam emails in order that general users may be shielded from being re-directed to malicious websites. For this purpose, we have a tendency to propose Associate in Nursing autonomous on-line system for police work malicious spam emails. In general, it is rough to gather spam emails from individual persons as a result of it is not usually allowed to access personal email spools. Thus within the

planned system, we have a tendency to collect double-bounce spam emails that area unit delivered to unknown users. From the collected spam emails information, a classifier model is employed to learn and classify the malicious spam emails. The updated affiliation weights of the classifier model area unit sent to a user's mailer computer code to boost the malicious spam email detection ability. Jungsuk [3] points out that the live amount of malicious URLs is usually terribly short, typically, among some days; therefore, it has expected that introducing incremental learning to malicious spam email detection are going to be effective. The system will learn from the recent spam emails in order that the spam email detection system is often up so far.

II. METHODOLOGY

Background

The email system is a way of transferring an important information or data in the form of a message from one person to other. Earlier days the email system was very simple, easy to use and it includes the only basic function and less security [4] [5]. Nowadays email becomes an important way of communication. Email security is an important issue of concern. Different people, organization send crucial information through email. There are different filters used for providing security to the Email system. Due to increase in popularity of email as an attack vector, it is critical for the enterprises and individual entities take measures to secure their email accounts for defending common attacks as well as attempts to unauthorized access to accounts for communications [6]. Due to different attacks, Spoofing, Phishing it needs to secure Email system so that crucial information should not be used by unauthorized person or entity. There are different methods are used to provide security to the Email system.Most popular of them are End-to-End encryption techniques and digital signature.

Different techniques for Providing Security to Email

Biometric Authentication:-

Biometric authentication is one of the processes for authentication using physiological or biological impression [7] [8]. As stated methodology in [7], a complete biometric-based end-to-end security system prototype has been explained in plaintext e-mail message for providing security. This system is divided into two parts 1.Hardware 2.Software.The hardware used is a thumbprint reader module to read thumbprint expressions and computer system for internet connection. The software used is to take biometric thumb impression, which extracts the features of thumb impression. These features are then used for encryption and decryption at the sending and receiving end respectively.

[NC-Rase 18]
DOI: 10.5281/zenodo.1485323
ISSN 2348 – 8034
Impact Factor- 5.070

Encryption /Decryption Technique

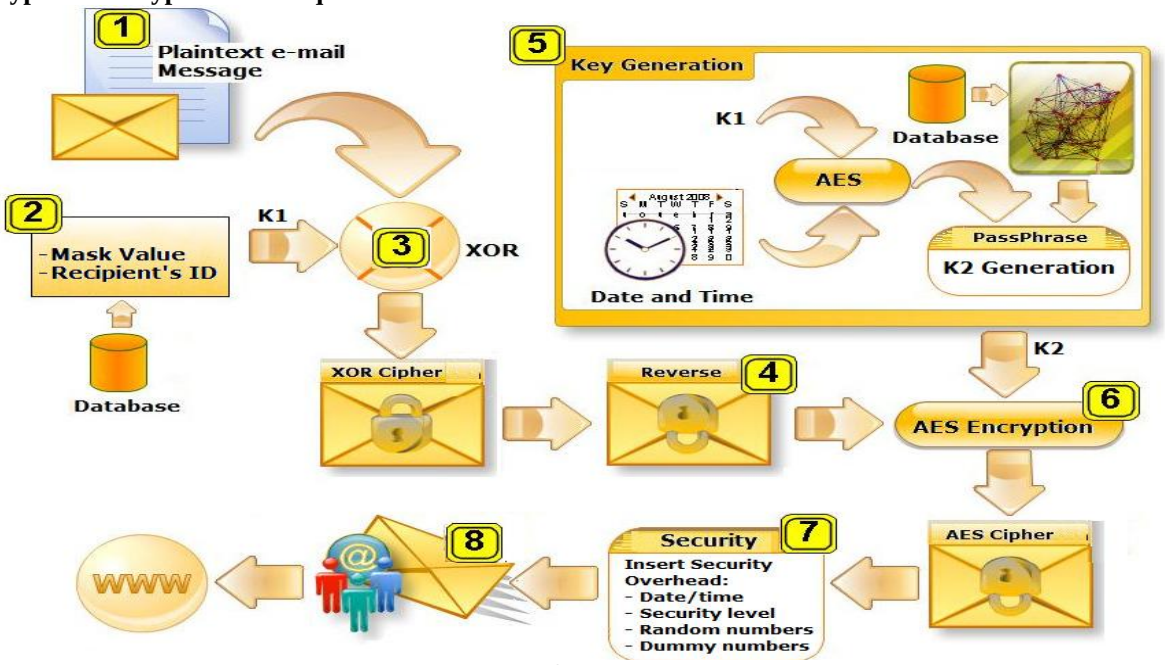

Fig. Block diagram for encryption process [7]

1. The User at sender end logs on to the system by using biometric impression authentication technique and write the message, which it wants to send at the desired destination address.
2. After writing the message a mask value which is a mixture of XML safe character combined along with recipient id, which forms a non-repeated encryption key value k1.The recipient's ID is already stored in the shared and secured database which retrieved depending on the destination address.
3. This key k1 performs XOR operation with the plain text, which creates a cipher text.
4. This cipher text is then reversed to create a random combination of cipher text so that it becomes hard for an attacker to understand the original message.
5. In step five key 2 is generated for the AES algorithm. Key2 is made up of static as well as dynamic part. Key k1 along with date and time creates an output of 44 characters using the AES encryption algorithm. The key k1 is used again in step 5. The second part, which is static use for generation of K2 represented by 10 decimal numbers. This number is created on the basis of the features extracted from the template features of recipient's biometric impression which is already stored in a database same like recipient's ID in step2.
6. In step6 the output of step4 i.e. Reverse-cipher text is encrypted using the AES algorithm. This uses a K2 key as passphrase for generation of a key of 256 bits.
7. In step7 when the message is transferred via internet security overhead of 50 characters is added to provide strong security. This security overhead may be encrypted date and time, random numbers, dummy numbers.
8. All this resultant combination of a message is then transferred to the receiver side using SMTP protocol. Here only the message is transferred not the id and fingerprint of the sender. At the receiver end, an encrypted message is received, it is then decrypted. For the decryption process, the valid recipient id is needed.

Providing Privacy and Confidentiality to Email through secure proxy interactions

It is another technique for providing Confidentiality and Security to the Email System. Protection, Privacy, and security to the transaction is a subject of key interest to a user. Based on this concept Ioannis et al. [9] Suggested an Email security system which gives information about the secrecy of location from which system email is accessed,Authorized user authentication. The system provides different features in terms offriendliness, security,privacy.

ISSN 2348 – 8034
Impact Factor- 5.070

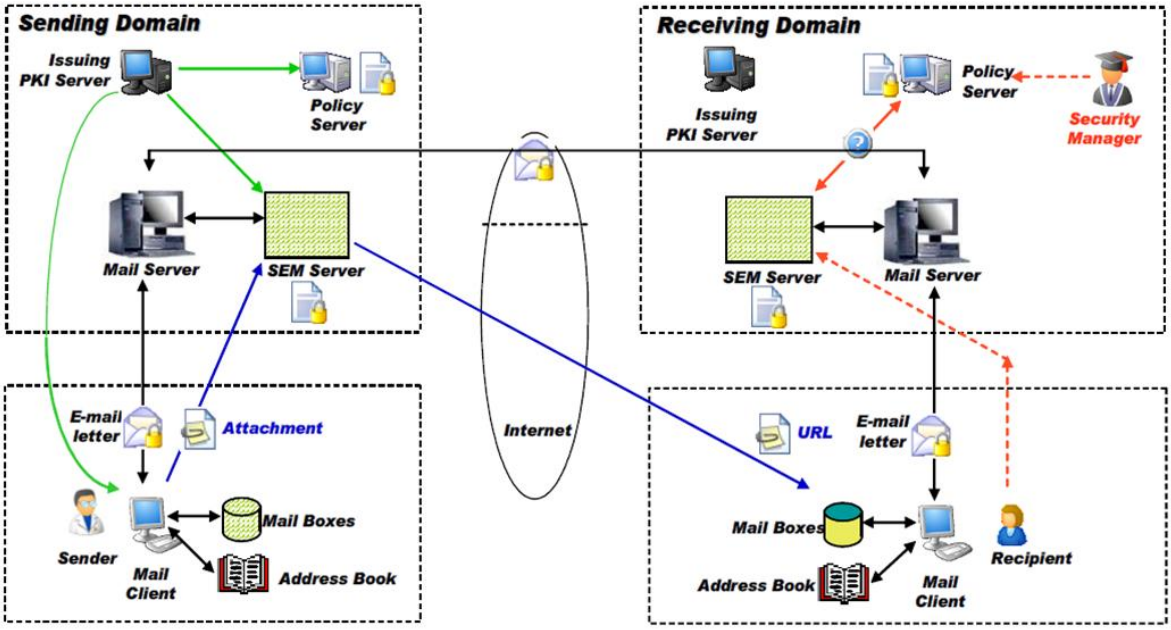

Figure 2.Secure Proxy Interactions [10].

Following are the step used for secure proxy interactions.

- The user with particular credentials like user id and password log on to the system through a secure email proxy.
- For each new user, proxy creates a new pair of key, which sends the public key to the server, which receives and stores user's certificate.
- Then in next step, proxy fetches e-mails from respective email server via IMAP. In which on double clicking every letter cryptographically processed and shown to the user.
- Now the user is able to send signed as well as encrypted e-mails.

I. FUTURE WORK

In the paper, we have done a survey on two techniques for providing a security to Email system from vulnerable attacks. On this basis of this survey, we can say that in future we can find new and more secured techniques for the security to the Email system in which the following features should be added.
1) The new security system can provide assurance of the identity of email's user to prevent it from a legitimate user
2) Encapsulate the messages through a different level of encryption to provide security from unauthorized user or attacker to make any modification to the message.
3) Provide client-side security system to give more restriction and security for the transaction in case of any security harm to the server.

II. CONCLUSION

Security to the Email system is a crucial issue of concern. Security to the Email system becomes an important issue when it comes to crucial information transferring, transaction. In this paper, we have done a survey for providing security to the Email system using two different encryption techniques. In Biometric, authentication technique the encryption and decryption technique are found to quite efficient for providing security to the Email system. Second technique provides security and confidentiality to the system.

ISSN 2348 – 8034
Impact Factor- 5.070

REFERENCES

1. *Vuong, T.P. and Gan, D. (2012) "A Targeted Malicious Email (TME) Attack Tool". Sixth International Conference on cybercrime, Forensics, Education and Training (CFET), Christ Church Canterbury.*
2. *Nagarjuna, B.V.R.R. and Sujatha, V. (2013) An Innovative Approach for Detecting Targeted Malicious E-Mail. International Journal of Application or Innovation in Engineering & Management (IJAIEM),*
3. *Jungsuk, S. (2011) "Clustering and Feature Selection Methods for Analyzing Spam Based Attacks". Journal of the NationalInstitute of Information and Communications Technology.*
4. *Siti-Hajar-Aminah Ali1, Seiichi Ozawa1, Junji Nakazato2, Tao Ban2, Jumpei Shimamura3"An Online Malicious Spam Email Detection System Using Resource Allocating Network with Locality Sensitive Hashing".Journal of Intelligent Learning Systems and Applications.*
5. *Study of the Security Enhancements in Various E-Mail Systems Afnan S. Babrahem1, Eman T. Alharbi1, Aisha M. Alshiky1, Saja S. Alqurashi1, Jayaprakash Kar2*
6. *Cailleux, L., Bouabdallah, A. and Bonnin, J.-M. (2014) Building a Confident Advanced Email System Using a New Correspondence Model. 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Victoria, 13-16 May 2014, 85-90.*
7. *Al-taee, M.A., Al-Hassani, H.N., Bamajbour, B.S. and Al-Jumeily, D. (2009) Biometric-Based Security System for Plaintext e-Mail Messages. Second International Conference on Developments in eSystems Engineering (DESE), Abu Dhabi, 14-16 December 2009, 202-206.5)K. Lee, and H. Park, "A new similarity measure base on intraclass statistics for biometric systems," ETRI Journal, Vol.25, No. 5, pp. 401-406, 2003.*
8. *https://digitalguardian.com/blog/what-email-security-data-protection-101*
9. *Ghafoor, A., Muftic, S. and Schmölzer, G. (2009) CryptoNET: Design and Implementation of the Secure Email System. Proceedings of the 1st International Workshop on Security and Communication Networks (IWSCN), Trondheim, 20-22 May 2009, 402-407.*
10. *Jang, J., Nepal, S. and Zic, J. (2008) Trusted Email Protocol: Dealing with Privacy Concerns from Malicious Email Intermediaries.*