International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-2, Issue-11, November 2014

Emphasizing On E-Mail Privacy

Dhawal Dighe, Nayna Bhardwaj, Parvez Khan, Saloni Agrawal

***Abstract*— E-mail security is the major issue for personal communication and business. E-mail is highly prone to various kind of attacks. The most common attack would be detected as Masquerading, Modification, Phishing, Denial of Service (DOS) and Spoofing. In order to provide security against these attacks, there are a number of tools have been proposed like Privacy Enhancement Mail (PEM), Pretty Good Privacy (PGP) and GnuPG, this tools are reportedly provide various security features like Data Integrity, Non-Repudiation, Encryption. But somewhere these features still fails to provide higher authentication and confidentiality. This paper is totally focused over the security issues that are still to be overcome after using the highly authenticated tools as mentioned above or any existing E-mail privacy tool.**

***Index Terms*— Authentication, confidentiality, data integrity, masquerading**

I. INTRODUCTION

Securing the E-mail from an unauthorized access is the major issue now a days.

E-mail is most widely used on smartphones among the user under the age of 18 to 44. It has observed that 33% of E-mails recipient opens the E-mail based solely on the subject line [1]. Today business is terrificallyran on electronic mails to correspond with client and colleagues. The E-mail servers are accepts, forward, deliver and store messages [2]. Neither the user nor their computers are supposed to be online simultaneously. When an E-mail messages is sent between two distant sites, it will be transit through dozens of machines on its way. Any of those machines can read the messages and could be record that for the future use. The internet is a vast network of computers, many of which are unprotected against malicious attacks from the time when it was composed to the time when it would be read. The protection of E-mail from unauthorized access and inspection is known as electronic privacy.

II. PROBLEM DOMAIN

E-mails are vulnerable to both i.e. passive attack and active attacks as well. Passive threats include release of message contents, and traffic analysis while active threats includes modification of message contents, Masquerade, replay and Denial Of Services (DOS). Actually all the mentioned threats are applicable to the traditional E-mail protocols. [3]

Today, life can't be imagine without internet and E-mail is the most famous and useful feature of this technology, as it is used by various organization for their business affairs, we can say that it is used by almost every student and educational organization for transferring the information, regarding notes and any other personal affair. But this service mainly carries a problem i.e. Security and Privacy. E-mail is most popularly used over internet, hence greatest prone to attacks, even with the best designed E-mail filters. The intruders attack to access the private information of individuals.

There are two types of attacks [1]:-

1) **Passive Attack**: Here data is used by the intruder, but there is no harm done to network, it has two types :
   a) Releasing message.
   b) Traffic analysis.
2) **Active Attack:** It is very dangerous as intruder affect the information by changing the content, modification and etc.

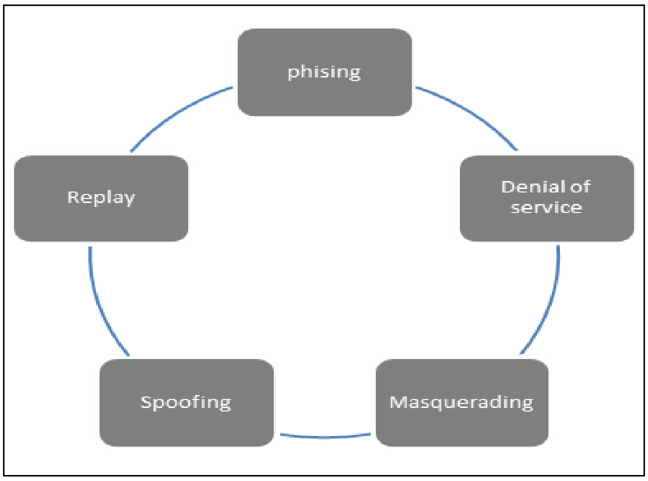

Fig 1.1 Shows various attacks on E-mail

E-mail in general completely insecure, the security issues include:

- Invasion of privacy
- Message Modification
- Repudiation
- False Messages
- Identity Theft

- **Modification Attack**: In this type of attack, the intruder makes changes and modifies the content. Then this content is send to the sender.
- **Masquerading Attack:** Masquerading occurs when one person uses the identity of another to gain access to a computer. This can be done by a person or remotely.[2]

Manuscript received November 19, 2014.

Dhawal Dighe, Nayna Bhardwaj, Parvez Khan, Saloni Agrawal, Student, BE, Department of Information Technology, Swami Vivekanand College of Engineering, Indore, Rajiv Gandhi Technical University, Bhopal, India.

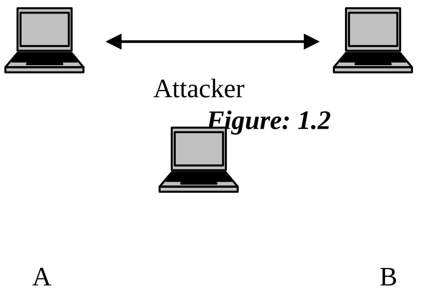

Figure: 1.2

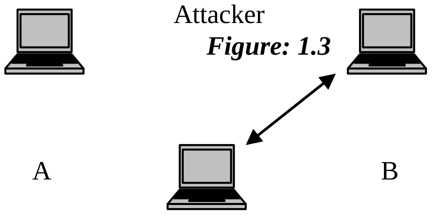

Figure: 1.3

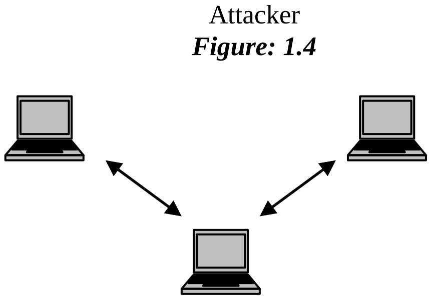

Figure: 1.4

- ✓ Figure 1.2 shows that how a normal communication occurs between two users A and B, and the **Attacker** is continuously **monitoring** it.
- ✓ Figure 1.3 shows that user B doesn’t know that he is communicating with the Attacker as he is thinking that he is communicating with the another user A.
- ✓ Figure 1.4 shows that how the **Attacker communicate** with **both the user** (A and B) and they **don’t have any clue** that they are **communicating** with someone else.

- ➢ **Denial Of Service:**A Denial of Service (DoS) attack usually either involves attackers sending messages to exploit certainvulnerabilities leading to the abnormality or paralysis of business systems, or sending a massive amount of regular messages quickly to a single node to run out the system resources resulting in business system failure.[3]
- ➢ **Distributed Denial Of Service:**A Distributed Denial of Service (DDoS) attack is a DoS attack utilizing multiple distributed attack sources. Typically, the attackers use a large number of controlled bots (also referred to as zombies) distributed in different locations to launch a large number of DoS attacks against a single target or multiple targets.[3]
- ➢ **Phishing**: Phishing is an attempt by an individual or a group to solicit personal information from unsuspecting user by employing social engineering techniques. Phishing E-mails are crafted to appear as if they have been sent from a legitimate organization or known individual.[4]

III. PROPOSED SOLUTION

The first step will be Digital Signature. [5] After that we are going to fragment the data into the size of 3KB. The minimum size of data will be of 21 kb. After fragmentation[6] the next step would be Encryption, [7] in Encryption we are going to use three algorithms i.e. – DES, 2 DES, 3DES.[8] And the last stage will be Base 64 Conversion.[9]

After using this algorithm all the issue regarding Confidentiality and Authentication will be solved and security will be more.

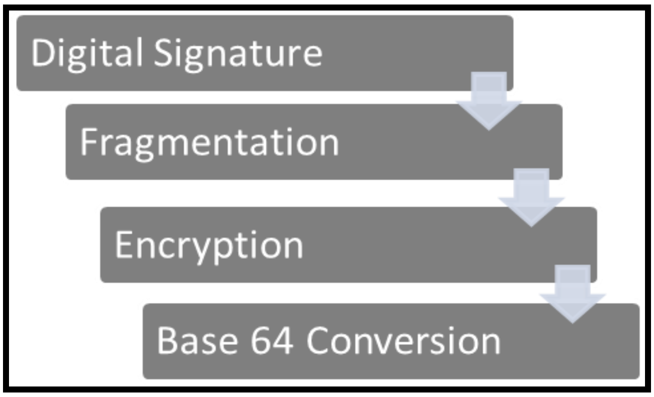

Figure: 1.5 Steps of Algorithm

IV. CONCLUSION

In this paper we proposed a new algorithm for securing Email Application by using Symmetric Key algorithms for optimising email privacy issues .Thus the various steps involved in this algorithm isto provide secure email service.

REFERENCES

[1] “Email stats” available at- http://blogs.salesforce.com/company/2013/07/email-marketing-stats.html accessed on [20/10/2014]

[2] “Email server details” available at- http://webcards.biz/ss/emails accessed on [20/10/2014]

[3] “E-mails are vulnerable” available at - http://www.flowersbyjim.com/ accessed on [20/10/2014]

[4] “Types of attacks” available at-http://www.zeepedia.com/read.php?web_security_passive_attacks_active_attacks_methods_to_avoid_internet_attacks_information_systems&b=14&c=39. accessed on [28/10/2014].

[5]”Masquerading attack” available at-http://oreilly.com/catalog/crime/chapter/cri_02.html.aaccessed on [28/10/2014].

[6]”Denial of Service and Distributed Denial of Service attack” available at-http://en.nsfocus.com/uploadfile/Product/ADS/DDoS%20FAQ/What%20is%20DDoS%20Attack.pdf. accessed on [28/10/2014].

[7]”Phishing attack” available at-https://www.us-cert.gov/report-phishing.accessed on [28/10/2014].

[8]”Digital Signature details” available at-http://office.microsoft.com/en-in/outlook-help/secure-messages-with-a-digital-signature-HP001230539.aspx. accessed on [31/10/2014].

[9]”Fragmentation details” available at-http://ccskguide.org/data-fragmentation/. accessed on [01/11/2014]

[10]“Encryption details” available at-http://windows.microsoft.com/en-in/windows/what-is-encryption#1TC=windows-7. accessed on [02/11/2014]

[11]”Triple DES details” available at-http://www.cryptographyworld.com/des.htm. accessed on [03/11/2014]

[12] “Base64 Conversion works” available at-https://www.base64decode.org/. accessed on [04/11/2014]