ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY ON EMAIL BASED TRUST MANAGEMENT SYSTEM

Jinkal Gajera
Master of computer engineering, Parul Institute of Engineering and Technology, India

ABSTRACT

Spoofing is a very common security threat to email applications. Several powerful techniques have been developed to counteract spoofing, but most of them are server-oriented and transparent to the user. Making up for the vast majority of emails transmitted, spam is an annoyance and potential security issue for users, and moreover a superfluous burden to the internet. Despite the maturity of today's email infrastructure, it is difficult to ensure the authenticity of a sender address for inbound mails. This shortcoming is used by spammers to bypass existing spam protection systems and furthermore poses a security risk to users. Due to this a vast majority of spam emails today are sent from botnets with forged sender addresses. This has attracted researchers over the years to develop email sender authentication mechanism as a promising way to verify identity of the senders. Therefore an urgent need to new mechanisms to circumvent the spoofing threat.

KEYWORDS:Email Security,Spoofing

INTRODUCTION

Ensuring email security is not a small task. Lots of mail servers and many millions of users are on the Internet today. Any system exposed to the Internet it must be able to handle a large volume of traffic and also must have a significant set of security risks. All of these factors highlight the importance of taking a more holistic approach to email security to filter viruses, spam, and other unwanted. Spammers continue to exploit the email infrastructure to compromise the security features such as privacy, authentication, integrity, non-repudiation and consistency of email.[11]

Security loopholes in the email communication enable cybercriminals to misuse it by forging its headers or by sending it anonymously for illegitimate purposes, leading to email forgeries. Simple Mail Transfer Protocol is the primary protocol for transferring email messages worldwide. However, despite being a powerful asset for most competitive businesses, it must along with some security threats which, if not addressed properly, it can be harmful. Email technology is subject to vulnerabilities such as phishing attacks, spamming, email spoofing and spreading of malware and viruses.[11]

Importance of E-mail Security

Email security is very important to protect confidential documents against misuse of the system.

There are number of drawbacks that arise if Email security is not launched such as:

1. Violation of Confidentiality: Every business has some information that is required to be kept confidential from other competitors and even from their own employees.

2. Damaging Data: Data is an important and valuable asset for any company or sole proprietor as it is the core of what your information is based on. Therefore backup scripts are also set for the data to be stored on other available media. If the data is damaged by any means, then the victim will face severe loss and can cripple the business severely.

When considering email security, it must be noted that the whole email network should be secure. Email security does not only about the security in the email content at each end of the communication channel. When transmitting data, the communication channel should not be easier to attack. A possible hacker could target the communication channel, obtains the data, and can misuses it. Securing the email content is just as important as securing the communication channel.

When developing a secure email, the following need to be considered.[11]

Access–authorized users are provided the rights to communicate.

Confidentiality – Information in the network remains private.

Authentication – Ensure the users of the network are authenticated or not.

Integrity – Ensure the message has not been modified in transit.

Non-repudiation – Ensure the user does not refute that he used the network

The types of attacks on email is also be studied to identify them and protect against them. Intrusion detection systems are developed based on the types of attacks most frequently used. Intruders generate problems on email for the following reasons:

- To consume resources uselessly
- To interfere with any system resource’s
- To gain system resources or knowledge that can be exploited in later attacks

LITERATURE SURVEY

Email Communication

The below figure shows a typical sequence of events that takes place when Alice composes a mail using her mail user agent (MUA).She enters the email address of her correspondent, and press the "send" button.

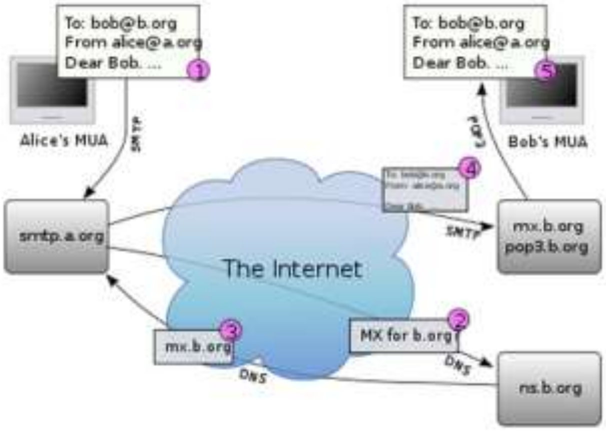

Figure 1 flow of email communication[12]

- Her MUA formats the message in email format and uses the Submission Protocol (a profile of the Simple Mail Transfer Protocol (SMTP),to send the message to the local mail submission agent (MSA), in this case smtp.a.org, run by Alice's internet service provider (ISP).
- The MSA looks at the destination address provided in the SMTP protocol (not from the message header), in this case bob@b.org. An Internet email address is a string of the formlocalpart@exampledomain. The part before the @ sign is the local part of the address, often the username of the recipient, and the part after the @ sign is a domain name or a fully qualified domain name. The MSA resolves a domain name to determine the fully qualified domain name of the mail server in the Domain Name System (DNS).
- The DNS server for the b.org domain, ns.b.org, responds with any MX records listing the mail exchange servers for that domain, in this case mx.b.org, a message transfer agent (MTA) server run by Bob's ISP.
- smtp.a.org sends the message to mx.b.org using SMTP.

The server may need to forward the message to other MTAs before the message reaches the final message delivery agent (MDA).

1. The MDA delivers it to the mailbox of the user bob.
2. Bob presses the "get mail" button in his MUA, which picks up the message using either the Post Office Protocol (POP3) or the Internet Message Access Protocol (IMAP).

Email Spoofing

In email system email spoofing is one type of attack in which email users who are sent emails from email addresses that are fake or altered.

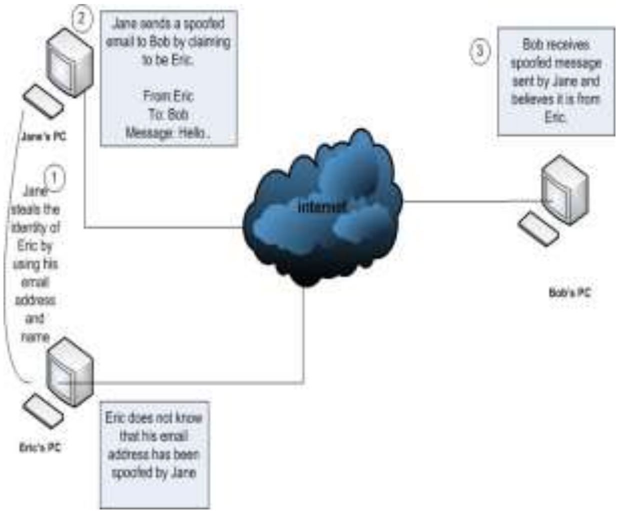
2
Jane sends a spoofed email to Bob by claiming to be Eric.
From Eric
To: Bob
Message: Hello..
Jane's PC
1
Jane steals the identity of Eric by using his email address and name
internet
3
Bob receives spoofed message sent by Jane and believes it is from Eric.
Bob's PC
Eric's PC
Eric does not know that his email address has been spoofed by Jane

Figure 2 Spoofing scenario [2]

Email spoofing is the illegal stealing of someone’s identity to send emails containing viruses and other malwares or cause other forms of damage. In this way spammers and spoofers can send malicious emails to specific recipients by falsely claiming that the email is actually from the trusted source.

Methods of generating of Spoofed Email

The spoofing entities include the legitimate sender’s identity and certifying authorities. Spoofed emails can be generated by using different techniques like

Telnet or configuring web servers or through services offered by some websites.[7]

1.Telnet

Telnet used to send spoofed emails by establishing a connection with SMTP server. This involves making a TCP connection to port 25 of the MTA. Sending the contents of the mail includes SMTP commands/replies between a client and server such as HELO, MAIL FROM, RCPT TO, DATA and QUIT as illustrated in below Figure[7].

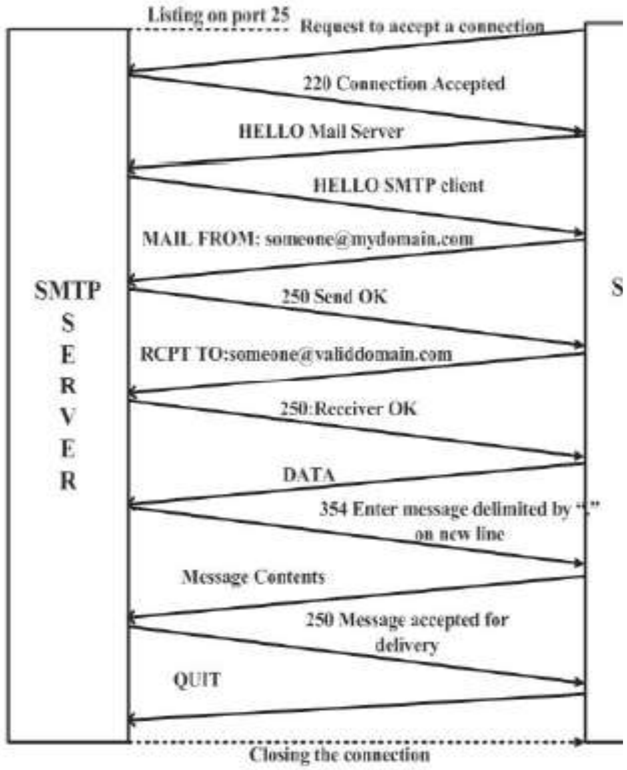
Listing on port 25
Request to accept a connection
220 Connection Accepted
HELLO Mail Server
HELLO SMTP client
MAIL FROM: someone@mydomain.com
250 Send OK
RCPT TO:someone@validdomain.com
250:Receiver OK
DATA
354 Enter message delimited by "." on new line
Message Contents
250 Message accepted for delivery
QUIT
Closing the connection
SMTP SERVER
S

Figure 3 Steps involved in SMTP handshake

Once the HELO command is received, the server responds with a 250 reply code containing its domain name. When the command is successful, both the client and the server get ready for further SMTP commands. The MAIL FROM command is the first command in the mail transaction. The address that is provided with this command is used to populate the "reverse path:" header in the email headers. The server validates the domain name of the sender by checking whether the domain exists. To issue a RCPT TO command, the MAIL FROM command must be successful. There can be several RCPT TO commands for one mail transaction. The client uses a DATA command to send the actual mail content. The end of the message is indicated through a single dot on a line by itself. The QUIT command is issued by the sender after delivering the data. This command terminates the established connection.[7]

The "from" or "Reply-to" header is easily adopted to spoofing. Doing an SMTP handshake, the MAIL FROM command can take any mail address since it is not checked in the complete transaction. It is evident from the above example that the mail server does not authenticate the sender email ID and it may be duplicated. Sending fake emails from SMTP server is therefore a common.[7]

2 configure accounts in a web server that has hosted PHP

A web server that allows hosting of PHP scripts may be used to send spoofed emails to any email user. This type of attack uses the mail method provided in PHP to launch spoofing attack. A html page is used as index to fetch the details of fake email which is to be used. The data is pushed onto the php script which executes the sending of the fake email.[7]

The scripts to launch this attack is as follows:

```
<?php
$toemail = $_POST['toemail'];
$fromname = $_POST['fromname'];
$fromid = $_POST['fromid'];
$subject = $_POST['subject'];
$message = $_POST['message'];
$headers = "From: $fromname <$fromid>";
mail($toemail,$subject,$message,$headers);
echo "Mail Sent!";
exit();
?>
```

A web server that allows hosting PHP may be used for uploading this script. When the para-meters are passed, the mail method of php sends email to any email address and posing from any email address.[7]

Details of Existing Systems

Sender Policy framework (SPF), Sender ID and DKIM (Domain Keys Identified Mail) have been implemented to short out this issue.[2]

1 Sender Policy framework (SPF)

SPF is an IP-based sender authentication scheme that work with SMTP envelope (MAIL FROM:) to block

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

forgeries at SMTP time.

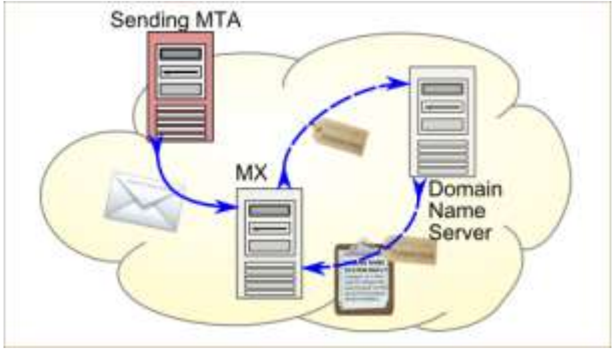

Figure 4 SPF Mechanism[2]

It allows the domain administrators to publish the range of IPs or IPs for their valid server on DNS Server in simple text format referred to as SPF record. Figure mechanism of SPF. [2]When the email exchange begins, the receiving side can query the DNS for sender's SPF record to validate if sender's IP is listed in the address range specified by the sender's domain. If majority of spamming domains will adopt SPF over time, SPF would become useless. return path is edited during forwarding, the receiver will treat the message as forgery for not coming directly from its listed sender. [2]

2 DKIM (Domain Keys Identified Mail)

Domain Keys was designed by Mark Delany of Yahoo in 2004. This former tool was implemented to prevent email threats by analyzing the Domain Name System (DNS) of a received email and therefore authenticate the sender. Many email providers such as Yahoo and Gmail are now using this form of strong encryption to prevent spoofing attacks. Below Figure the mechanism of DKIM.[2]

The steps shown in below Figure are described as follows: [2]

1. A user sends an email which passes through the mail server.

2. The mail server using DKIM tool, encrypts the message using a private key and publishes the public key through the DNS server.

3. The message is then forwarded to the destination email server

4. The receiving email server retrieves the public key of the message through the DNS server and matches it with the private key.

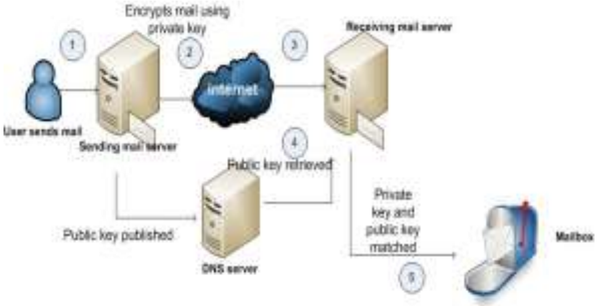

Figure 5 DKIM Mechanism.[2]

5. If the keys are matched, the message is decrypted and then forwarded to the appropriate mailbox.

3 Sender-ID

Sender-ID operates on purported responsible address (PRA) of a message, which the sender given in the header of a message. As with SPF, recipients can check if the purported sender's IP address matches one that is published on the DNS. [2]

4 PGP and S/MIME

Pretty Good Privacy (PGP) and S/MIME both cryptographic approaches that operate on the message body using public-key cryptography and append the signature on body.PGP, keys are stored in end-user key rings or in public key-servers. Key management uses a peer-to-peer web-of trust architecture. In S/MIME, key management follows a hierarchical model like SSL and keys are signed by a certificate authority(CA). PGP and S/MIME are not widely used. Majority of the mail user agents uses /MIME by default, still majority of email sent out is not signed. According to some experts average users don't sign their outgoing email because they find it inconvenient to manage keys and enter pass phrases.[3]

5 Identity Based Email Sender Authentication for Spam Mitigation(iSATS)

iSATS is a crypto-based email sender authentication system that operates on the SMTP envelop, on MAIL FROM: command, to perform domain level authentication.[3]

iSATS leverages identity based signature (IBS) using identity-based public key cryptography (IBC) to authenticate the identity of an email sender. iSATS requires establishment of a trusted authority (TA) also known as private key generator (PKG), responsible for issuing the secret key (SK) and system parameters. The TA is responsible to verify the identity of a domain before issuing the SK.[3]

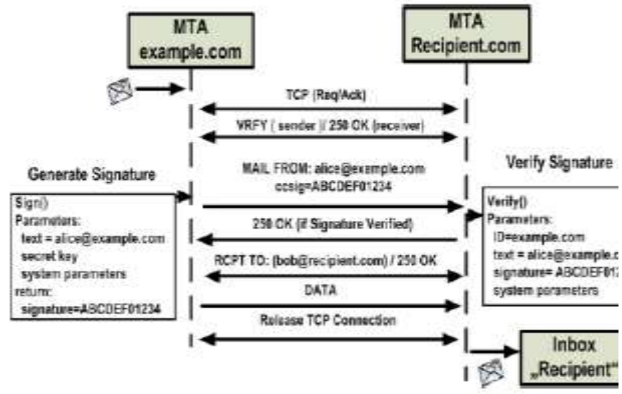

Figure 6 Email Processing with iSATS

On receiving side MTA will verify the signature. For verification the MTA will use the public system parameters, signature (which is extracted from MAIL FROM:), signed text i.e. sending user's email address from MAIL FROM: and the domain name of the sender as the public key (see above Fig.). The entire verification process is completed before replying to command MAIL FROM:, which give the option to recipients to reject the message before its content is sent.[3]

Comparison Table of Existing Methods

There are several sender authentication protocols have been proposed, and the comparison is as follows:

Table 1 Comparison Table of Existing Methods

Method Name	Operates on	Limitations
DKIM[2]	Email headers and body	- Packets from Spoofed IP address is not identified
Sender ID[2]	purported responsible address (PRA)	- Can not authenticate the message at SMTP time.
PGP and S/MIME	Operate on the message body	- Average users don't sign their outgoing email because they find it inconvenient to manage keys and enter pass phrases.
SPF[2]	SMTP envelope (MAIL FROM:)	- Message forwarding - return path is edited during forwarding, the receiver will treat the message as forgery

Limitations of the Existing System

Existing email infrastructure was not actually designed to verify the authenticity of sender address. There are several sender authentication protocols have been implemented, however, it is still possible to spoof emails easily using certain programs

CONCLUSION AND FUTURE ENHANCEMENT

Email spoofing is the harmful threat to email in these days, some techniques and measurement has already been introduced to mitigate it, but the problem still lies there. however, it is still possible to spoof emails easily using certain programs. Therefore an urgent need to new mechanisms to circumvent the spoofing threat. Our proposed mechanism is for protect the unauthorized source email (SPOOFED Email)

Future work will be dependent on the information and susceptibility gathered from scanning more types of attacks. If we equip our strategy with such highly developed and glassy information our approach can work more efficiently. In future, the proposed work should be implemented in real environment to countermeasure the Spoofed email.

REFERENCES

1. Laurent Cailleux , Ahmed Bouabdallah, Jean-Marie Bonnin," A confident email system based on a new Correspondence Model ",ICACT 2014
2. D. Mooloo and T.P. Fowdur , "An SSL-Based Client-Oriented Anti-Spoofing Email Application ", IEEE-2013
3. Sufian Hameed , Tobias Kloht , Xiaoming Fu ," Identity Based Email Sender Authentication for Spam Mitigation", IEEE-2013
4. Dharmendra Choukse, Umesh Kumar Singh ,Lokesh Laddhani, Rekha Shahapurkar "Designing Secure Email Infrastructure", IEEE-2012.
5. M. Tariq banday," Effectiveness and limitations of e-mail security protocols", international journal of distributed and parallel systems (ijdps) vol.2, no.3, may 2011
6. Dijiang Huang ,"Email-based Social Network Trust",IEEE-2010
7. Kunal pandove, Amandeep , Jindal," Launching Email Spoofing Attacks ", IJCA-2010
8. Mohsen Toorani "SMEmail–A New Protocol for the Secure E-mail in mobile environm-ent",IEEE-2008
9. Alexander W. Dent,"Flaws in an E-Mail Protocol of Sun, Hsieh, and Hwang",IEEE-2005
10. H.-M. Sun, B.-T. Hsieh, and H.-J. Hwang, "Secure email protocols providing perfect forward secrecy," IEEE Commun. Lett., vol. 9, pp. 58– 60, Jan. 2005.
11. Hathai Tanta-ngai, Tony Abou-Assaleh, Sittichai Jiampojamarn , and Nick Cercone, Fellow ,"Secure Mail Transfer Protocol (SecMTP)" , IEEE
12. M. Tariq Banday, Jameel A,Nisar A. Shah, "A Practical Study of E-mail Communica-tion through SMTP"