Email Spoofing

Kunal Pandove
Project Assistant
CSRC, PEC,
Sector 12, Chandigarh.

Amandeep Jindal
Project Assistant
CSRC, PEC,
Sector 12, Chandigarh.

Rajinder Kumar
Research Associate
CSRC, PEC,
Sector 12, Chandigarh.

ABSTRACT
Email spoofing is referred to as malicious activity in which the origin details have been altered so as to make it to appear to origin from a different source. Sending fake emails is usually used to convince the receiver so that he stays unaware of the real sender. Email spoofing may be effectively used to launch phishing attacks on the receivers. The attacker may also use the attack with some amplification and in addition use mass mailer to spam mail users. Infections may be propagated by the means of spoofed emails to attack victims. There are a variety of attackers who do email spoofing. The list starts from people trying to just have fun by sending spoofed messages to users. Other serious attacks are done by wrong doers to make damages to the systems.

Causes of email spoofing include compromised account information from where emails are sent. Sometimes user browsers are infected so as to use them to send spoofed emails. Email service providers versatility may be attacked by misusing the SMTP protocol.

Proper management and deterrence steps that are always recommended should be used to avoid falling into spoofing attacks. Mostly administrators need to follow guidelines to prevent email spoofing in their domains. Once email spoofing is been detected or reported, it should be properly handled. There are a certain set of instructions to react to attacks and also to provide deterrence against spoofing attacks.

Implementation of security relies on usage of physical medium like smart cards. The end users may also implement verification for the originators of email to prevent them from falling into the attacks of spoofed emails. Digital signatures and certificates are also recommended to ensure that the emails are genuine.

The recommended implementation of security does not come without limitations. These mostly include cost factors, providing training to users and implementation at both the client as well as the server ends.

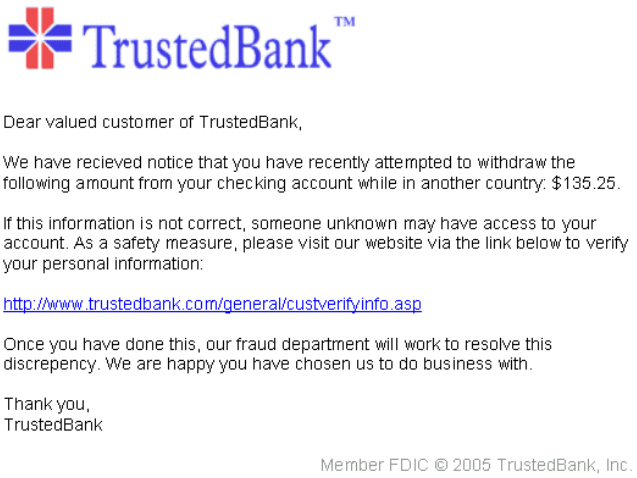
Keywords
Email Spoofing, Phishing, SSL/TLS, PGP

1. INTRODUCTION
E-mail spoofing is a term used to describe (usually fraudulent) e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source [1]. Email spoofing finds a wide variety of victims who may be attacked for a multiple reasons. These multitudes of reasons have been listed in Section II. It is an art in itself to make measures to prevent such attacks on hosts. There are certain measures of prevention that may be used to keep a check on spoofing attacks. These have been listed in section III. The very next section suggests reactions to email spoofing. Section V points out the security mechanisms. Section VI describes the causes of email spoofing. Section VII gives suggestions of implementation of security and the very next following section VIII lists out the barriers that exist to hinder implementation of security. The conclusion has been derived in Section IX.

2. ATTACKERS AND VICTIMS
Email spoofing attacks may be launched by some mischievous users just to do poking into other user accounts to simply have fun. Out of sake of mischief usually friends send spoofed emails to their friends to make fun. This category is though not considered to be criminal, but the attacker should avoid doing such activities because faking identity is in itself a wrong doing which should not be done. Such practices are not widely discouraged. However, spoofing anyone other than yourself is illegal in some jurisdictions [2]. Email spoofing attacks may be launched with simply having an email account and any email client like Outlook. The technique to spoof the identity of the sender is to change the display name for the sender and send emails from the client. Such attacks are launched within an organization to surprise the receivers. Both the above stated categories are treated as innocent since they are not intended to cause damage to the victim. More kinds of severe attacks are possible when the attackers have much more malicious intent. In such cases the attackers may cause some serious damages to the victim.

The most famous and frequently used attack that is done by the means of email spoofing is phishing attack. The attackers in this case are usually interested in the information regarding the particular user.

An example of a phishing e-mail, disguised as an official e-mail from a (fictional) bank. The sender is attempting to trick the recipient into revealing confidential information by "confirming" it at the *phisher'*s website. Note the misspelling of the words *received* and *discrepancy*. Such mistakes are common in most phishing emails. Also note that although the URL of the bank's webpage appears to be legitimate, it actually links to the phisher's webpage [3].



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Phishing attacks are aimed at obtaining the confidential information regarding the user. Such emails take the user to a URL which is a fake website hosted by the attacker and pretending to be the genuine one so as to gain some personal information from him.

Examples of spoofed email that could affect the security of your site include:

- email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not do this
- email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information

Another kind of attack that is popular amongst the attackers is spamming from spoofed origin. Spam mails are usually done to populate the inboxes of users to use up server space. The spam is intended at flooding the server space and cause after effects of sluggishness.

Finally, expert attackers also use spoofing as a means to propagate infections through the internet. Maliciously designed scripts may be embedded into the emails which cause harm to the recipient machines. Spoofed emails ensure that such infections reach their destination and cause the desired harm to the receiver.

3. PREVENTION

Managing how we choose to email is the first step towards preventing spoofing related attacks. Spam attacks are common when the users use one email account which is shared between trusted and untrusted contacts. The implication of this is that a user should try to obtain more than one email accounts if he chooses to stay in contact with users that he may not rely on completely. Spam attacks usually have embedded infections in them, therefore it has been recommended to clear scam and not keep it for a long time. In addition to this the browser should also be configured to not allow malicious scripts in emails and should be closed after logging out of email. In case the user has used a public terminal the cache needs to be cleared fearing phishing. It should be ensured that account of email used is not insecure. Sometimes alternate options are suitable rather than emailing and may be used.

Sometimes the receiver has to be careful regarding the origins of emails so that they are not wrong. The sender may use bcc field so that users may not contact each other and cause spam with copy fields. In other cases the victims should be careful of not forwarding or replying to suspicious material.

Another issue in spread of infection is in backups of emails. Taking backups of suspicious emails may lead to spread of malicious programs. Additional care is required when the access is in mobile devices, since there is danger of device malfunction. Care needs to be taken while deleting suspicious emails so that they are not just simply moved into the deleted items folder from where they may become active again.

The users of emails should also be aware regarding how to tackle with fraudulent emails. One should not believe in claims like 'you have won a lottery' or such similar titles. Also the users should try to recognize the phishing attacks in emails and avoid to follow links in them. It should be avoided to send personal and financial information in emails over insecure channels. User should avoid falling into the traps like unsubscribe to a newsletter that he hasn't ever subscribed to.

Another precautionary prevention step is to avoid malware in the emails. Sometimes users become careless if the email comes from a trusted source, ignoring the fact that it may be spoofed. It is considered better to delete spam than to blacklist it. It is better to have an email filter enabled than not using it. One should not fail to scan all attachments as most of viruses and trojans stay in the attachments.

Users should also be proficient in keeping hackers not know their personal information. Any account information that is shared should be done securely and it should be kept in mind that someone may not steal it and use for spoofing. Keeping easy to break passwords lets hackers use user's account. All the Emails that are sending confidential misusable information should be secured by encryption using say PGP. The network connections that may be wireless also should be encrypted so that credentials are not stolen. The sender may also use digital signatures to provide assurance to the receiver regarding authenticity of email.

4. REACTION

An administrator may be alerted about the spoofed emails by either users or logs of bounced emails. Once it is reported, the fault should be reviewed. Mostly the examination is conducted in the header of the email. Any mischievous activity should also be reported to the other sites involved in the activity, if they can be determined. They should be taken into confidence and alerted to determine the original source of the email. Now just to make sure to get as much information as possible, the logging of the mail server should be increased. The matter ends at a revelation that the it may not be possible to obtain the origin of every spoofed email.

5. SECURITY AND DETERRENCE

There are certain lists of measures that are helpful in providing security against spoofing attacks. Cryptographic signatures may

be used to exchange authenticated email messages. Pretty Good Privacy (PGP) or other encryption technique may be used. Authenticated emails also ensure that the emails are from the users that they appear to be and not altered in transit. In addition the sites may also use SSL/TLS for security in their mail transfer software.

Mail delivery daemon should be configured so as to prevent someone from directly connecting to SMTP port to send spoofed emails to someone. It should also be logging the details so as it is made easy to track any mischievous emails.

The server should consider to implement single point of entry for the site. This will also provide centralized logging.

The administrators should educate their users from being social engineered into disclosing any information. If such activity is observed by them, they should alert the administrator immediately.

6. CAUSES

The users of email accounts are also susceptible to being misused by attackers. If an attacker gets to somehow obtain the credentials of a user of email, then he may use it to propagate mass emails to produce spam attacks on other users. The email user may not even make out that his account is compromised and being used for bad purposes.

Hackers may also infect browsers with malware to compromise their security and misuse them to send spoofed emails.

It is easy to spoof because the protocol that is used called SMTP lacks authentication. If the site server is configured to allow SMTP connections then the attackers may exploit this and issue commands to send some emails that may appear to originate from choice of the attacker. This email address may be either of two – a correct email address or any address that is of the choice of the attacker that is correctly formatted.

There are email service providers that may be vulnerable to attacks of forged or spoofed emails.

If in case there are a lot of bounced emails , one should be alert and analyse the logs to make proper remedial measures. However, if your email address is being spoofed, you may experience large numbers of messages appearing in your inbox that have bounced back because the original spam message was undeliverable to the intended recipients. These messages are referred to as "backscatter." [6].

7. IMPLEMENTATION OF SECURITY

The websites of e-commerce or e-banking may issue physical authentication media such as smart cards to their users who are legitimate. Thus if a user compromises data due to phishing may still be doubly sure against misuse since the attacker would not be able to procure the physical media. The drawbacks of this approach are investing in user education and infrastructure setup.

In addition the receiver's end may implement authentication of mail server. The implementation uses domain name verification to ensure that the origin of certain emails are valid. This makes it difficult for the attackers to be anonymous. The email service providers need to implement verification procedure and allow verification of every email that is sent from its usage. The downside of this approach is to implement both at the sender's and receiver's gateway.

Another approach to provide security against spoofing is to use digital signatures and verification mechanisms. If an email arrives at a receiver that does not contain signature or has a signature that may not be verified, then the user may become aware that the email is not genuine and a duplicate. The verification of signatures may be done at either of the following – at the client of the user or at the gateway which acts as relay from which the emails are routed.

8. HINDERENCES IN EMAIL SPOOFING SECURITY

PGP is a technique that is used for email security. The problem with PGP is complexity and it becomes difficult training people to implement and use PGP. In addition PGP is a technique that should be implemented at both the sender and receiver making it cumbersome. Another issue is that of key management, where keys may get lost or corrupted. In some cases compromised keys may lead to email attacks.

TLS/SSL need a requirement of stateful connection which renders it weak in versatility. Not all the implementations of TLS/SSL have implemented client and server authentication and also it becomes tedious to get almost all the users to start using it. TLS/SSL becomes expensive in case it has been used in tunnel mode.

TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS [8].

To deny connecting directly to the SMTP service may become annoyance to users who prefer remote logins. To provide a single point of entry into a domain should make the system sluggish and mostly burden a single interface.

To educate users regarding measures to counter email spoofing is a tedious task. Multitude of users are using the Internet and providing training to all the email users may almost be next to impossible. Sending training material to the users against spoofing also poses strong challenges. It may not be easy to understand by the users. In some of cases attackers may follow it with feedback request to get confidential information.

Disadvantages of computer mediated communication include: e-mail is a limited symbolic representation system void of oratory and graphic appeals and thus open to misunderstanding, some learners prefer speaking to writing, e-mail is limited to certain kinds of learning, computer anxiety may be a barrier to participation, and cost and access to technology may also be barriers [9].

To issue physical authentication media requires costs in addition to standard investment. Customers have to make installations on their infrastructure. Third party certifying authorities may need to be involved for certificates issued on behalf of business for authentication.

To implement mail server authentication additional implementations need to be accommodated. The email relays need to lookup for the email envelope and compare with sender domain name. The sender enterprises from where the emails originate have to register their IP address with DNS.

In the case of digital signature methodology, it needs to be implemented at both the client and server gateways. Also it doesn't prevent valid signatures to have misleading addresses which take the user to fake site.

9. CONCLUSION

Email spoofing is referred to activity of sending emails using someone else's identity. The attackers may vary from innocent mischievous users seeking fun , to malicious attackers who seek more serious damages to the users. These attacks may be used to launch phishing attacks so as to get information from users. In addition these may be used to spam the users with emails. Spoofed emails are also used to carry infections like trojans to do harm to victim systems.

Administrators need to take a variety of measures to prevent , detect and provide remedial measures to email spoofing attacks.

The causes of email spoofing have been described in the preceding sections.

Implementation of security also takes on importance when there is commerce that is involved in the email communication. If there is some leakage in such communications then it becomes undesirable. Various techniques which require economic investments in implementation have been suggested that ensure that secure email communication is possible.

The implementations of security have own set of drawbacks and hindrances that have been listed in the end of this work.

10. REFERENCES

[1] http://en.wikipedia.org/wiki/E-mail_spoofing

[2]http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci840262,00.html

[3] http://en.wikipedia.org/wiki/Phishing

[4]http://www.windowsecurity.com/whitepapers/25-Common-Mistakes-Email-Security.html

[5]http://www.cert.org/tech_tips/email_spoofing.html

[6] http://www.umt.edu/it/email/spoofing.aspx

[7]http://www.ehow.com/list_5924278_disadvantages-pgp-encryption_.html

[8]http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci343029,00.html

[9]http://www.eric.ed.gov/ERICWebPortal/custom/portlets/recordDetails/detailmini.jsp?_nfpb=true&_&ERICExtSearch_SearchValue_0=ED415834&ERICExtSearch_SearchType_0=no&accno=ED415834