Developing a Model to Enhance E-Mail Authentication against E-Mail Address Spoofing using Application

A. S. Zadgaonkar, Vikas Chandra Pandey, Pratap Singh Pradhan

Abstract: ***E-mail is one of the most commonly used communication mechanisms. Most of the recipients and senders desire secure e-mail exchange. Senders want to make sure that the recipient is really the intended recipient, and the message arrives to the recipient confidentially. On the other hand, recipients want to make sure that the sender is the entity who it claims to be, and the arrived message has not been maliciously modified and examined during transmission. These requirements can be satisfied by the e-mail applications that use public key cryptosystem (PKC) as the security base, such as S/MIME and PGP. The main handicap behind the deployment of applications that use PKC is the problem of public key distribution with a legitimate binding with its owner. Moreover, public key management features, such as update, delete operations must be performed in a secure way.***

Index Terms—MIME, PKC, threats, attack, Internet, Spam, software.

I. INTRODUCTION

The widespread use of email caused the number of warnings being made about the dark side our technological revolution to increase and we are becoming uniquely vulnerable to many mysterious and malicious threats. Viruses, worms, and other forms of malicious software started targeting our email inboxes to propagate. Spam and other forms of unsolicited bulk electronic commerce started filling our email inboxes and invading our privacy. Phishing and other forms of fraud attacks have been using email as their primary communication channel to trick users into giving out their credentials. Email could have been a killer application for the Internet if none of the problems mentioned above exist.

II. E-MAIL SPOOFING

E-Mail plays a vital role in information communication and exploiting the vulnerabilities of it may cause hazardous effects such as spam, phishing and confidential data leakage etc. Vulnerabilities in the email system occur in both client applications and with email protocols Email spoofing is a technique used by hackers to fraudulently send email messages in which the sender address and other parts of the email header are altered to appear as though the email originated from a source other than its actual source.

Manuscript received on May 3, 2013

Dr. A.S. Zadgaonkar, vice chancellor, Dr. C.V.Raman University, Kargiroad,Kota, Bilaspur(C.G.),India

Vikas Chandra Pandey, Asst. Prof., Dr. C.V.Raman University, Kargiroad,Kota, Bilaspur(C.G.),India

Pratap Singh Pradhan, Research scholar, Dr. C.V.Raman University, Kargiroad,Kota, Bilaspur(C.G.),India

1. Email Client Vulnerabilities: SMTP and early email clients were designed for sending and receiving only text-based emails. Email clients have become more feature-rich as well, supporting scripting languages, address books, and integration with other desktop applications. Although certainly useful, these additional functions have also introduced vulnerabilities into mail clients that have been exploited by viruses, worms, and other forms of malware.

2. Protocol Vulnerabilities: A number of vulnerabilities in SMTP is that users are not authenticated and it trusts them in message exchanges. The open relay configuration is an example. The servers do not verify the origin of a message as a part of trust assumption. The sending server can put any origin address in the message and send it. The receiving server accepts this address and continues to handle this message which allows spammers to substitute fake addresses (*spoofing*) and hide the true identity of the sender. Spoofing is when an e-mail message appears to come from a legitimate source but in fact is from an impostor. E-mail spoofing can be used for malicious purposes such as spreading viruses, crawling for sensitive business data and other industrial espionage activities. Spoofed email may lead to phishing attacks. The major reason for spoofed email is due to lack of SMTP authentication.

Due to its un-authenticated nature, anybody can send an email with a *From* field equal to. A spoofed e-mail is when the header is changed for the e-mail appears to be from a legitimate and authorized sender in an attempt to trick the user into believe the email content forcing them to reveal their personal information or attempting to view the fraudulent websites to obtain their data failing which may cause lock or loose of their accounts. It is easy to spoof e-mail because Simple Mail Transfer Protocol (SMTP) lacks authentication.

III. PROBLEM STATEMENT

Recently, email is indispensable for life. Because the Web-based free mail offered by Yahoo! and Google, etc. can be acquired free of charge, and can be exchanged with other users anywhere in the world if you have an environment that can access to the Internet, it is being used by a lot of people. However, “sniffing”, “manipulation”, and “spoofing” by the third party become problems as email becomes an important infrastructure. Recently, free mail by ””spoofing” is used for the phishing to aim at these account takeovers on the portal site such as Yahoo! because various services are consolidated in one

ID and password and being provided.

Therefore, the sender domain authentication technology is used to detect whether sender's mail address is not pretend other domains. This is divided two. One is an electronic signature-based "DomainKeys" and other is the Internet Protocol (IP) address-based "SPF". DomainKeys is used in Yahoo! and Gmail.

Address Spoofing: -address spoofing emerged as an e-mail spoofing trick, wherein a spammer sends spam e-mails that contain forged send date to recipients. It keeps e-mails listed on top in recipient mailbox, thereby maximizing the chances of immediate attention by the recipient. The "address" header field in a address spoofed e-mail may contain a address which is different from actual address it was sent. It is easy to spoof email because SMTP (Simple Mail Transfer Protocol) lacks authentication. If a site has configured the mail server to allow connections to the SMTP port, anyone can connect to the SMTP port of a site and (in accordance with that protocol) issue commands that will send email that appears to be from the address of the individual's choice; this can be a valid email address or a fictitious address that is correctly formatted.

In the case of my spoofed email address, the message has no ("Unknown") subject and the body of the email contains only URLs of some sites. As such, I suspect that the spamming activity is a handiwork of some bad entities offering site visitors to clients (bloggers in many instances) for a fee.

Free mail: The free mail service is service that the mail account can be acquired free of charge if we input a necessary item (mail address and password, etc.) even if we do not join the Internet access service. Such a mail account is called a free mail. A lot of companies that are offering the portal site are providing this service. Many of mail accounts of such mail use the Web mail. Because many of mail accounts of such mail use the Web mail, we can exchange email from anywhere if we have an environment that access to the Internet. However, anonymity and the danger of crime and mischief, etc. rise because we can easily acquire mail account even if the personal identification is not done. The security of the free mail of the major company that provides the free mail service can put trust of some degree. But we need to take heed of its use because the fishing site exists to acquire ID and the password of the free mail illegally. Also, the following three risks exist in the free mail.

1. Sniffing: When we send the message with email, we send it with the sender address attached on the head of the message as address. By way of many computers, this message reaches the recipient. To look at the message in email by the operator of the computer that passeson the way of this.

2. Manipulation: To change the content of the sniffed email and send a different message.

3. Sender spoofing: To send an email that pretended sender address by writing another mail address in sender address. The free mail is used for the phishing in recent years and the damage has been increasing. The portal sites which provide the free mail are prevents spoofing by using the electronic signature-based and IP address-based authentication technology.

IV. RELATED WORKS

1. Domain Keys: Domain Keys [1] is the electronic signature-based sender domain authentication technology, and it is used by the Yahoo! mail and the Gmail, etc. Because the electronic signature is added to the header of email when mail is sent from the server corresponding to Domain Keys, we can judge on the receiving side whether email is sent from which server. Therefore, it is used to prevent the spam mail and the phishing that pretended ender address. Process of Domain Keys is shown in Fig.1.

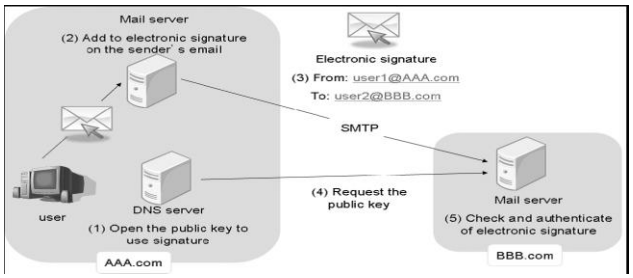

Fig. 1. Process of Domain Keys

1. In AAA.com, The public key used to sign is opened with the DNS (Domain Name System) server in advance.
2. The mail server of AAA.com gives the electronic signature based on the text and the header of the sent mail.
3. Email is sent to BBB.com by SMTP.
4. The mail server of BBB.com refers to DNS server of domain part AAA.com of "From:" for the public key.
5. The electronic signature is checked by the public key acquired from AAA.com, and the authentication succeeds if the electronic signature corresponded.

2. SPF (Sender Policy Framework): SPF [2] is the IP address-based sender domain authentication technology. It can detect whether sender's mail address is not pretend other domains. This is set on to the basis of assumption that the spoofing of IP address is difficult, and can complete the authentication only by acquiring information described on DNS server. Process of SPF is shown in Fig. 2.

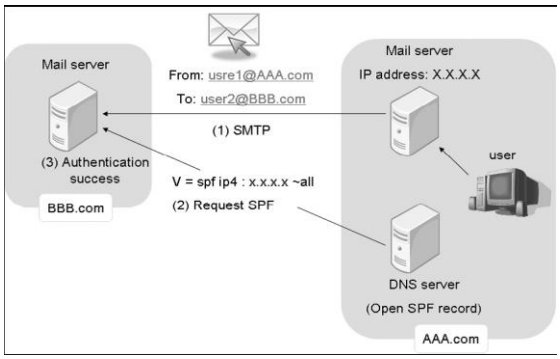

Fig. 2. Process of SPF

1. The SMTP communication is begun from the mail server of AAA.com to the mail server of BBB.com.
2. The mail server of BBB.com refers to the SPF record for the DNS server of AAA.com based on the domain part of the mail address described in "From:"
3. The authentication succeeds if the mail server of the sending side is included in the list of IP address shown on the SPF record of AAA.com.

3. Email sender address spoofing:

Email sender address spoofing by the free mail: The following free mail has the function that changes mail address in "From" field into another mail address.

– Gmail
– Yahoo! mail
– Windows Live Hotmail (Hotmail)
– @nifty WEBMAIL

In Gmail, we can send email by using another address instead of the Gmail address and easily manage two or more accounts from the Gmail interface by using "Addressor" originally set ourselves. The mail address and the password of the added account are needed to add the new address. If we use this function, it is possible to show like sending mail from the mail address except for the Gmail. Then, we investigate how it is displayed in the "From" field or another fields on the receiving side when we send email by actually using this function.

Email sender address spoofing by TELNET: In our research, we consider email sender address spoofing. Here, we use Gmail as receiving side. The protocol named SMTP (Simple Mail Transfer Protocol) is used for the transmission of mail. It is a protocol used to send email. SMTP client accesses to SMTP server and sends SMTP command. We examine doing actually when email is sent by using the command prompt.

1. HELO: (Establishment of access, 250 (Requested mail action okay, completed) is returned)
2. MAIL: (Specification of sender, 250 (Requested mail action okay, completed) is returned)
3. RCPT: (Specification of recipient, 250(Requested mail action okay, completed) is returned)
4. DATA: (Sending of text, 354 (Start mail input; The end of input sends the line only of ".") is returned)
5. QUIT: (Processing termination, 221 (Service closing transmission channel) is returned)

In email sending ahead, we add the "From" column and the "To" column to the header. Then, the place that transmits sender mail address to SMTP server becomes two (the character string given following "MAIL FROM" that is SMTP command and the character string following the "From" field that exists in the header of email). Also, the place that transmits recipient mail address to SMTP server becomes two (the character string given following "RCPT TO" that is SMTP command and the character string following the "To" field that exists in the header of email). Here, recipient mail address is correct (exist) because we consider email sender address spoofing. Here, Gmail receives as Fig. 3 even if sender mail address is rewritten another mail address and it is transmitted.

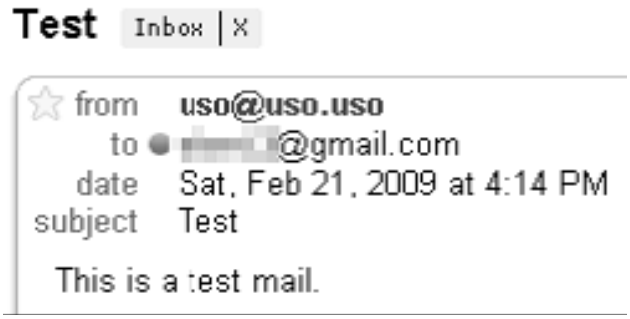

Fig 3: receiving of email sender address spoofing

In receiving side of email, it is possible to impersonate by rewriting mail address written in the "From" field because the part where general user refers to sender's mail address is only here. If this is used, spoofing is possible because these settings are freely actually decided in the sending side. It is possible because sender's mail address check in SMTP server look at whether domain name only exist, and it do not completely examine whether the account name of ahead of "@" exist or user who sent email is really an owner of the account.

Evaluation of SPF: Next, we explain how SPF is evaluated when email is actually received as an example of Gmail. There is an area where various information that was called a header fields was described in email besides the text.

First, when email is sent from the mail server that does not specify the SPF record at all, the following two lines are found in the header field.

Received-SPF: neutral (google.com: xxx.x.xx.xx is neither permitted nor denied by best guess record for domain of uso@uso.uso) client-ip=xxx.x.xx.xx;
Authentication-Results: mx.google.com;
spf=neutral (google.com: xxx.x.xx.xx is neither permitted nor
denied by best guess record for domain of ***@***.com)
smtp.mail=***@***.com

The part of "***@***.com" is sender's mail address and as the result of the evaluation of SPF it is "neutral". "?all" is defined in the end of the record like "v=spf1 ?all" for instance, and when it does not match to other conditions and it is match to "?all", the SPF record of the sender domain becomes "neutral". SPF should not immediately refuse the receiving of email even if the result is "neutral". On the other hand, when email is sent from the mail server that the SPF record is appropriately set, evaluation of SPF becomes the following two lines, and the result of it is "pass".

Received-SPF: pass (google.com: domain of ****@yahoo.co.jp designates xxx.xx.xxx.xx as permitted sender) client-ip=xxx.xx.xxx.xx;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of *****@yahoo.co.jp designates xxx.xx.xxx.xx as permitted sender) smtp.mail=*****@yahoo.co.jp; domainkeys=pass (test mode) header.From=*****@yahoo.co.jp

This is the case that IP address in the sending side matches to the SPF record and succeeds in the authentication. Email is processed according to the evaluation of the sender domain because it is valid.

V. PROPOSED METHODOLOGY

Much information is described in the header field, and the header field is described in shape of "field name: field value".When MTA (Mail Transfer Agent) forwards email, the content of the work is recorded in "Received:". "Received" is added whenever the server's passing. "Received:" with the header field most below passed first is a server near the sender and "Received:" with the header field most up passed at the end is a server near the recipient. In addition, information of "Received: from X by Y" means "Mail was sent from the server of X to the server of Y".

However, because SMTP server automatically acquires other party's IP address as data while communicating SMTP, the IP address written its next cannot be misrepresented. Sender host's information can be obtained by watching here. Then, we propose the check technique of the "Received:" field shown in Fig.4. There is a research [3] to distinguish the spam mail as a technique for evaluating the message of email by checking the "Received:" field on such a user side. To accomplish the proposed solution the following methodology will be adapted**:**

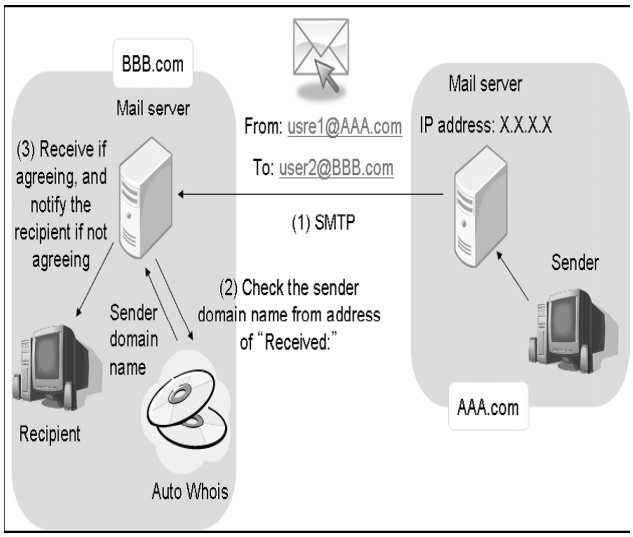

Fig. 4. Sender domain authentication

1. SMTP begins from the mail server of AAA.com to the mail server of BBB.com

2. The mail server of BBB.com obtains a sender domain name by using Auto Whois from IP address described "Received" of the most below header field.

3. A sender domain name obtained by using Auto Whois, domain name below @ in the mail address written in "Received:", and "From:" is compared. The authentication succeeds if they all agree, and recipient is notified if they don't agree.

VI. CONCLUSION

This research is centered on "A Model To Enhance E-Mail Authentication Against E-Mail Address Spoofing". The outcome of the proposed work will likely to yield expected result and fulfill the following objective:

a)Secure email access.
b)Prevent email spoofing.
c)Prevent against man-in-the-middle attacks.

REFERENCES

1. M. Delany, "Domain-based email authentication using public-keys advertised in the DNS (DomainKeys)," RFC4870, IETF, May 2007. http://tools.ietf.org/html/ rfc4870
2. Mark Lentczner and Meng Weng Wong, "Sender Policy Framework (SPF) a Convention to Describe Hosts Authorized to Send SMTP Traffic," May 2004. http: //tools.ietf.org/html/draft-mengwong-spf-01
3. Yukiko Sawaya, Yutaka Miyake, "An Examination of Spam Mail Filtering with k-NN Analysis Based on Mail Header Information", The 2008 Symposium on Cryptography and Information Security (SCIS 2008), 3C2-1, 6pages, January 2008.
4. A. Bergholz, J.-H. Chang, G. Paaß, F. Reichartz, and S. Strobel. Improved phishing detection using model-based features. In Proceedings of the Conference on Email and Anti-Spam (CEAS), 2008.
5. http://en.wikipedia.org/wiki/E-mail_spoofing
6. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci840262,00.html
7. http://en.wikipedia.org/wiki/Phishing
8. http://www.windowsecurity.com/whitepapers/25-Common-Mistakes-Email-Security.html
9. http://www.cert.org/tech_tips/email_spoofing.html
10. http://www.umt.edu/it/email/spoofing.aspx
11. http://www.ehow.com/list_5924278_disadvantages-pgpencryption_.html
12. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci343029,00.html
13. http://www.eric.ed.gov/ERICWebPortal/custom/portlets/recordDetails/detailmini.jsp?_nfb=true&_&ERICExtSearch_SearchValue_0=ED415834&ERICExtSearch_SearchType_0=no& accno=ED415834.
14. RFC 2821, Simple Mail Transfer Protocol, http://www.ietf.org/rfc/rfc2821.txt.
15. Aaron Emigh, *Online Identity Theft: Technology, Chokepoints and Countermeasures.* Report of the Department of Homeland Security – SRI International Identity Theft Technology Council, October 3, 2005.
16. Adida, B., Hohenberger, S., Rivest, R. Lightweight Encryption for Email. USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI), 2005.
17. Anti-Phishing Working Group. Phishing Archive.http://www.antiphishing.org/phishing archive.html.
18. Anti-Phishing Working Group. Phishing activity trends report, June 2006.http://antiphishing.org/reports/apwg report june 2006.pdf, June 2006.

19. D. Birk, M. Dornseif, S. Gajek, and F. Grobert, "Phishing phishers—tracing identity thieves and money launderers," Horst Gortz Institute for IT Security, Ruhr University Bochum, Tech. Rep. TR-HGI-01-2006.
20. *e-mail spoofing*. internet.com, Dec 11 2003.Available from http://www.webopedia.com/TERM/E/e_mail_spoofing.html.
21. J. Callas, M. Delany, M. Libbey, J. Fenton, M. Thomas, "DomainKeys Identified Mail (DKIM)," Internet Draft draft-allman-dkim-base 01,http://mipassoc.org/dkim/specs/draftallman- dkim-base-01.txt, October 2005.
22. L. Cranor, S. Egelman, J. Hong, and Y. Zhang.Phinding phish: An evaluation of anti phishing toolbars. Technical report, Carnegie Mellon University, Nov. 2006.
23. Fette, N. Sadeh, and A. Tomasic. Learning to Detect Phishing Emails. In *Proceedings of the International World Wide Web Conference (WWW)*, Banff, Alberta, Canada, May 2007.
24. Garera, S., Provos, N., Rubin, A.D., Chew, M. A Frameword for Detection and Measurement of Phishing Attacks. In *Proceedings of the 2007 ACM workshop on Recurring malcode*, pages 1-8, 2007.
25. Jacobsson, M., & Myers, S. (2007). Phishing and Countermeasures - Understand the Increasing Problem of Electronic Identity Theft. New Jersey: Wiley.