Developing a Model to Detect E-mail Address Spoofing using Biometrics Technique

A. S. Zadgaonkar, Suresh Kashyap, Murari Chandra Patel

Abstract ***Email changed the way we communicate in today's highly technical world. Its usage increased tremendously in the last few years and millions of user's world wide joined this technological revolution that made the world look so small and at our disposal. 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.***

Index Terms— threats. Viruses, worms, Security, Internet, Email.

I. INTRODUCTION

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.

Email spoofing is a technique frequently used by perpetrators of all manner of email hoaxes to hide their identities and point the blame at somebody else. It is a favorite with spammers and also used by hackers. Spoofing received some media coverage recently when a 12-year-old was able to demonstrate how he apparently sent an email purporting to come from the UK Prime Minister to the Chancellor of the Exchequer. Most e-mail systems that send mail over the Internet use simple mail transfer protocol (SMTP) to send messages from one server to another. The messages can then be retrieved with an e-mail client using either post office protocol (POP) or Internet message access protocol (IMAP). SMTP is also generally used to send messages from a mail client to a mail server in "host based" (or Unix-based) mail systems, where a simple mbox utility might be on the same system [or via Network File System (NFS) provided by Novell] for access without POP or IMAP. SMTP is a simple email protocol. It is usually only used for outbound emails such as email notifications sent by your Iomega network device. By default, this protocol uses UDP port 123.

Different security protocols offer different levels of security to insecure Simple Mail Transfer Protocol. These protocols vary considerably in degree of efficiency and adaptability. Therefore E-mail system not only suffers from various well known messages integrity problems like spamming, phishing, sender spoofing, etc., but it also experiences a lesser know problem of date spoofing. This paper briefly appraises date spoofing and threats it can cause to e-mail and other e-systems. It also illustrates processes to send and receive date spoofed e-mail messages. Further, it lists solutions to the problem of date spoofing and proposes a model including necessary algorithms to detect and stop transmission and reception of date spoofed e-mail messages.

Manuscript received on May 8, 2013

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

Suresh Kashyap, Asst. Prof., Dr. C.V.Raman University, Kargiroad, Kota, Bilaspur,India.

Murari Chandra Patel, Research scholar, Dr. C.V.Raman University, Kargiroad, Kota, Bilaspur(C.G.),India.

II. 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.

III. PROBLEM STATEMENT

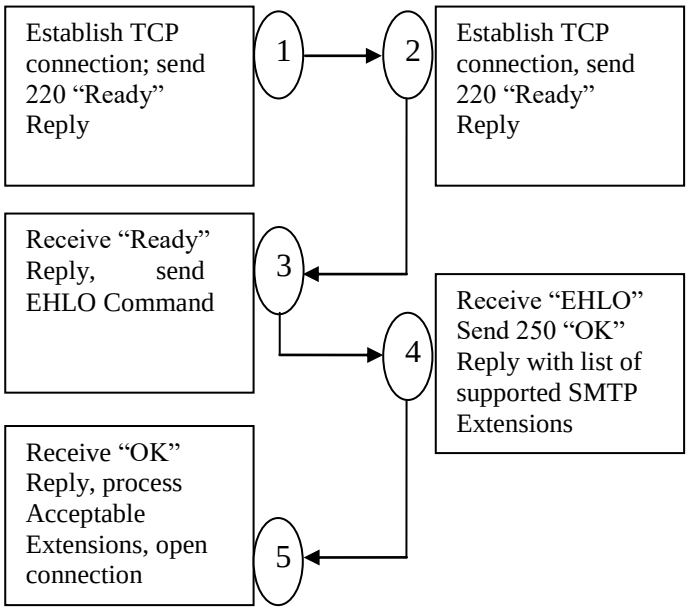
Address spoofing aids spamming by increasing chances of opening spam e-mails and impediments its countermeasures due to increase in false positives. The problem of date spoofing is not only limited to spamming, it can cause manifold of problems, more serious than spamming. Permitting submission, transmission or reception of either pre-dated or post-dated email messages can not only lead to confusions and wastage of time of their recipients but also can inflict threats to several other electronic services and systems that use e-mail for communication, record and reference. These include ecommerce, e-tendering, e-evaluation, e-transactions, etc. In these, e-mail before or after a particular date and time is in acceptable as response within some stipulated time is mandatory. A user may trick these systems by sending response after the expiry of deadline by sending pre-dated e-mail. As a consequence, a dispute over the correctness of date can cause a protracted legal battle between the contending parties.

IV. MAIL TRANSFER PROCESS

The process of sending e-mail from the senders client to the senders server or its transmission from senders SMTP server to recipients SMTP server consists of a) connection establishment, b) mail transactions and c) connection termination which are illustrated below.

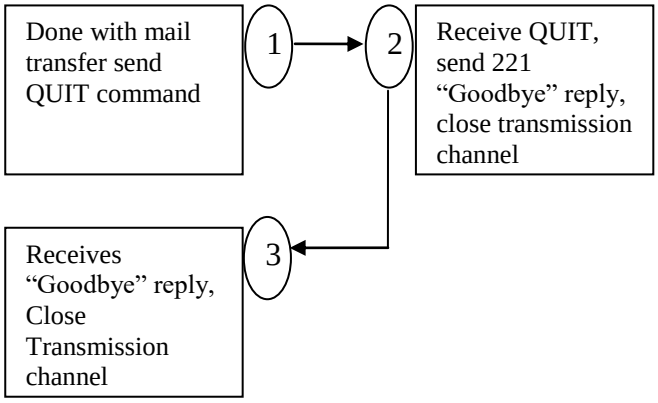
1. Connection establishment:

SMTP Sender TCP SMTP Receiver



2. Connection termination:

SMTP Sender Quit SMTP Receiver



Connection is established by the creation of a TCP connection on an ephemeral TCP port. The receiver sends connection acceptance reply using a code 220. The response also includes server information including full server name and the version of the SMTP server software. The client on receiving the connection ready reply issues HELO/EHLO in case of ESMTP which also includes the domain name of the client. The SMTP server after receiving the HELO/EHLO command, responses with service code 250 along with the supported ESMTP extensions. In case, the receiver does not support extensions, it replies with a service code 500

V. PROPOSED METHODOLOGY

We present a new approach to email security that uses fingerprint recognition to authenticate users and provide them with a transparent process of signing and verifying email messages. The idea is to enroll a user fingerprint, associate the fingerprint with a record that is unique to that user, and finally use the user's fingerprint and unique record to authenticate the user,

sign the user's email message, and verify other users' email messages. Our approach was implemented as an email client called SEFR. To accomplish the proposed solution the following methodology will be adapted:

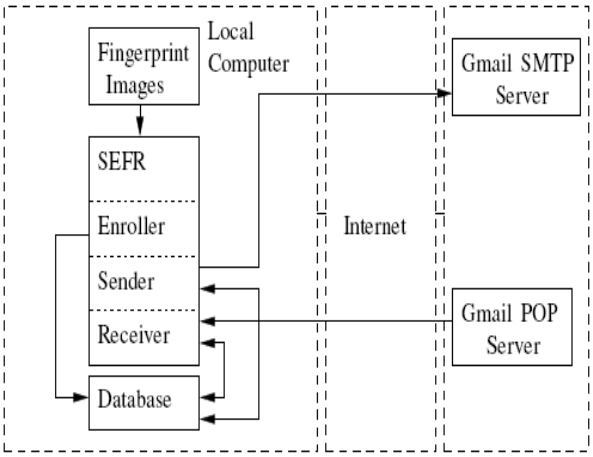


Fig1: Proposed Model

1. Enroller with their account information (username and password), and the path to their fingerprint image. Enroller acquires the information correctly.

2 Downloads the email message from Gmail's POP server using the commands described in the POP RFC document.

3 Parses the email message and retrieves the email address in the "To:" and "From:" fields of the email message.

4. Strips the tabs, spaces, line feeds, form feeds, and carriage returns from the email body.

5. Computes the hash of the stripped message using SHA-1

6. Checks if the retrieved email address has the hash value associated with it in the database. If yes, then the verification status is set to Success else it is set to Failure.

VI. CONCLUSION

This research is centered on "An Model to Detect E-mail Address Spoofing". The outcome of the proposed work will likely to yield expected result and fulfill the following objective:

1. Secure email access.
2. Prevent email spoofing.
3. Prevent against man-in-the-middle attacks

REFERENCES

1. S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair. A comparison of machine learning techniques for phishing detection. In Proceedings of the eCrime Researchers Summit, 2007.
2. Anti-Phishing Working Group. Phishing activity trends - report for the month of December 2007, 2008. http://www.antiphishing.org/reports/apwg report oct 2007.pdf, accessed on 28.04.08.
3. Bank Austria. Faq mobile TAN, 2008. http://www.bankaustria.at/de/19825.html, accessed on 25.01.08.
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. B. Biggio, G. Fumera, I. Pillai, and F. Roli. Image spam filtering using visual information. In ICIAP '07: Proceedings of the 14th International Conference on Image Analysis and Processing, pages 105–110, Washington, DC, USA, 2007. IEEE Computer Society.
6. D. M. Blei, A. Y. Ng, and M. I. Jordan. Latent Dirichlet allocation. Journal of Machine Learning Research, 3:993–1022, 2003.
7. A. Bratko, G. V. Cormack, B. Filipic, T. R. Lynam, and B. Zupan. Spam filtering using statistical data compression models. Journal of Machine Learning Research, 6:2673–2698, 2006.
8. L. Breiman. Random forests. Machine Learning, 45(1):532, 2001.
9. B. Byun, C.-H. Lee, S.Webb, and C. Pu. A discriminative classifier learning approach to image modeling and spam image identification. In CEAS 2007 Fourth Conference on Email and Anti-Spam, August 2-3, 2007, Mountain View, California USA, 2007.
10. R. Cattoni, T. Coianiz, S. Messelodi, and C. Modena. Geometric layout analysis techniques for document image understanding: a review. Technical report, IRST, Trento, Italy, 1998.
11. M. Chandrasekaran, K. Narayanan, and S. Upadhyaya. Phishing email detection based on structural properties. In Proceedings of the NYS Cyber Security Conference, 2006.
12. Commtouch. Commtouch q3 spam statistics: Spam problem reaches new peak, expands in every dimension, 2008. http://www.commtouch.com/Site/News Events/pr content.asp?news id=767&cat id=1, accessed on 11.05.08.
13. G. V. Cormack and R. N. Horspool. Data compression using dynamic markov modelling. The Computer Journal, 30(6):541–550, 1987.
14. R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems, pages 581–590, 2006.
15. A. Emigh. Phishing attacks: Information flow and chokepoints. In M. Jakobsson and S. Myers, editors, Phishing and Countermeasures, pages 31–64. Wiley, 2007.
16. I. Fette, N. Sadeh, and A. Tomasic. Learning to detect phishing emails. Technical report, School of Computer Science Carnegie Mellon University, CMU-ISRI-06-112, 2006.
17. I. Fette, N. Sadeh, and A. Tomasic. Learning to detect phishing emails. In Proceedings of the International World Wide Web Conference (WWW), pages 649–656, 2007.
18. G. Fumera, I. Pillai, and F. Roli. Spam filtering based on the analysis of text information embedded into images. Journal of Machine Learning Research, 7:2699–2720, 2006.
19. Gartner. Gartner survey shows phishing attacks escalated in 2007; more than $3 billion lost to these attacks. http://allpaynews.com/node/3820 retrieved on April 27th, 2008, 2007.
20. J. Goodman, G. V. Cormack, and D. Heckerman. Spam and the ongoing battle for the inbox. Communications of the ACM, 50:25–33, 2007.
21. M. Gupta. Spoofing and coutermeasures. In M. Jakobsson and S. Myers, editors, Phishing and Countermeasures, pages 65–104. Wiley, 2007.