International Journal of Technology and Engineering System (IJTES)
Vol 7. No.5 2015 Pp. 478-483
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

Implementation of a Differential Equation based Analytical Model for Analyzing the Malware Behaviour in E-mail

P.Deepa[1] , S.Latha[2], E.Karpagam[3]
Associate Professor[1] PG Student[2,3]
[1, 2, 3] Department of M.C.A., Panimalar Engineering College, Chennai.
mca_deepa@yahoo.com[1] , aslatha54@gmail.com[2], karpagam12691@gmail.com[3]

ABSTRACT

In the modern world various kind of email malware is spreading easily through various modes like spreading by clicking vulnerable link and direct malware spread from untrusted person. The main objective of this concept is to detect the malware mail and to avoid such kind of files. In the existing system spam mail is detected only after it reaches the receiver that too done after reaching the receiver mail box. In such situation it is necessary that the mail should get stored in receiver space which reduces the efficiency of the mail server and occupies valuable space in server. The user needs to read each and every unwanted mail in order to remove it which also becomes an overhead to the user. To provide solution for this problem user by themselves train the spam words to the database. According to the user specification mail will be classified in the server itself and only normal mail will be sent to the receiver where as if a mail contains any spam word either in the body of the mail or in attachment then those kind of mail got block and return back to the sender which increases efficiency and storage space of the receiver. It is mandatory to find out the misbehaved users in order to provide better service to the user. Here we follow two way of blocking one is if only a specified user misuses then we will block them by using their mail ID. If the entire user from an IP misuses the application then we will block all the users by simply blocking their IP.

Keywords: Differential Equation, Malware, email, IP, Analytical Model

I. Introduction

In the real world, email is a basic service for computer users, while email malware poses critical security threats. For a number of years, the propagation of email malware has followed the same modus operandi. A viral email is sent to the victim and appears as though it was sent by somebody the recipient trusts. The subject is also related to the recipient's business area. Once the victim is tricked into either clicking the malicious hyperlinks or opening the attachments inside such an email, the computer will be compromised. Then, the compromised computer will start to infect new targets found in its email address lists immediately. To prevent email malware, scientists have spared no effort to dissuade people from opening unexpected hyperlinks and email attachments. However, the success of recent new email malware, such as "Here you are", indicates that those education measures are not very successful.

A key reason is because social engineering is a tried-and-true technique in the context of security. For example, by convincing computer users that the received emails with malicious hyperlinks and attachments were from a trusted source, the technique of email-borne malware will be highly effective and is still widely adopted by current malware authors. Current research on email malware focuses on modeling the propagation dynamics which is a fundamental technique for developing countermeasures to reduce email malware's spreading speed and prevalence. There are a few works reported to model email malware propagation. Previous works assume that a user can be infected and send out malware copies only once, no matter whether or not the user visits a malicious hyperlink or attachment again. Real instances are those early email malware like Melissa in 1999 and Love letter in 2000 , which will check whether a victim has been compromised before the infection.

However, modern email malware is far more aggressive to spread in network than before by introducing two new propagation features. First feature is "reinfection", i.e., an infected user sends out malware copies whenever this user visits the malicious hyperlinks or attachments. Second feature is "self-start", i.e., an infected user sends out malware copies when certain events (like PC restart) are triggered. Researchers stated that a user can be infected multiple times. However, their model assumes that an infected user could send out only one malware copy each time the user checks emails, even if the user visits more than one malicious hyperlinks or attachments.

II. 2.RELATED WORK

In the existing system once the victim is tricked into either clicking the malicious hyperlinks or opening the attachments inside such an email, the computer will be compromised. Then, the compromised computer will start to infect new targets found in its email address lists immediately. To prevent email malware, scientists have spared no effort to dissuade people from opening unexpected hyperlinks and email attachments**.** However, their model assumes that an infected user could send out only one malware copy each time the user checks emails, even if the user visits more than one malicious hyperlinks or attachments. In short, previous works did not take the two new features into account, and hence, cannot accurately.

III. Proposed System

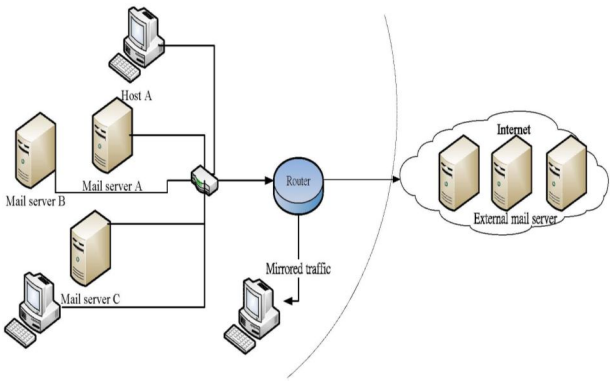
We proposed a new analytical model to capture the interactions among the infected email users by a set of difference equations, We introduce a new concept of virtual nodes to address the underestimation in previous work, which can represent the situation of a user sending out one more round of malware copies each time this user gets infected. We perform empirical and theoretical study to investigate why and how the

proposed SII model is superior to existing models.

3.1Advantage

These observations become the motivation of our work to develop a new analytical model that can precisely present the propagation dynamics of the modern email malware. Since the spreading procedure can be characterized by an susceptible-infected-immunized (SII) process, we name our proposed model as SII.

3.2.System Architecture



IV. Module Description

The proposed system can be broadly divided into seven modules, namely

Modules

- ✓ Spam word classification
- ✓ Mail drafting
- ✓ Server monitoring
- ✓ Virus mail scanning
- ✓ Mail History
- ✓ IP address wise blocking
- ✓ Email id wise block

4.1 SPAM Word Classification

Email marketing has become one of the popular ways of advertisement. In such situation users will receive a bulk irrelevant message which becomes an overhead to the application user. In order to overcome this admin will add a spam words to the application to monitor the mails which send by the sender. By implementing this we can avoid spam mail spreading across the application which in case improve our user experience

4.2 Mail Drafting

If a user logs in to the application they will have access to various categories like inbox, outbox, spam and compose mail. In this a user will compose a mail to forward it to the receiver. If they initiate sending a mail then it will reach the server. In server it will check for spam word in the composed body and attachment. In case if any spam found then those mail will not forwarded to the receiver rather it will be redirected back to the sender spam box.

4.3 Server Monitoring

Each and every mail come out from the sender will be monitored by the server if any vulnerability found in that mail or not. So server plays an important role here. Admin will give the rights to the individual users to attain some membership in the application for file sharing purpose. After that admin can able to monitor the users files and Spam files individually.

4.4 Virus Mail Scanning

In most of the application virus file is detected based on the extension of file. In our application if a sender attaches a vulnerable kind of file then it is scanned by the server and automatically vulnerable will get removed and only normal contents will get forward to the receiver. An efficient mail application will always scan the file by using its behaviour

4.5 Mail History

Admin maintains history of normal mail and spam mail send by the sender. Each and mail will be tracked by the mail for the application security and efficiency purpose.

4.6 IP Address Wise Blocking

If a mail send by the sender contains spam word then those mail will be taken into count. If more number of spam count trigged for the mail id’s

from same IP address then such kind of vulnerable persons will be completely blocked by using their Ip address rather than blocking them by using their mail id

4.7 Mail Wise Blocking

Once user noticed more number of spam files it they have access to block the particular user and unblock the blocked user. Once the user's i.p.address will regularly intimating spam files admin will block the I.p.address to restrict the access. Admin have the access to block and unblock the user. If more number of spam send by the sender then they will get blocked by the admin.

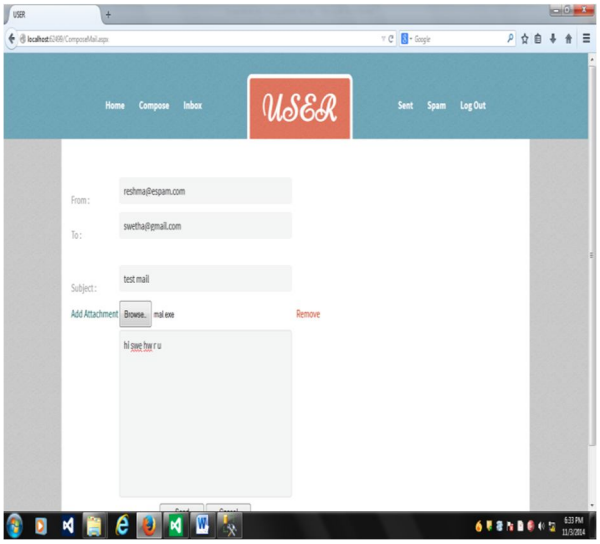
V. Implementation

The implementation of our work is organized in the following steps:

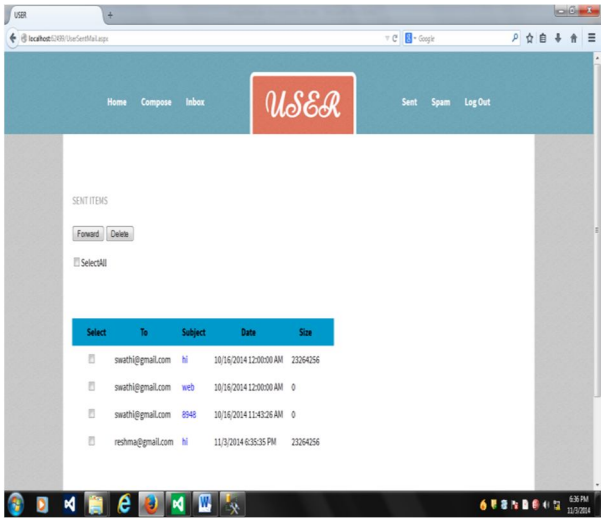
5.1 Registration

5.2 Login

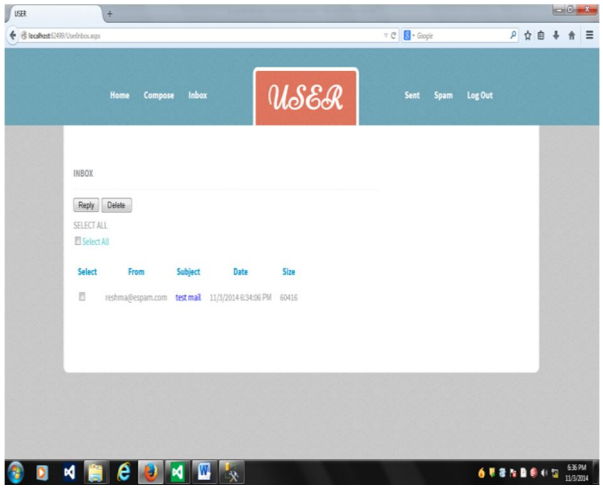
5.3 Compose Mail



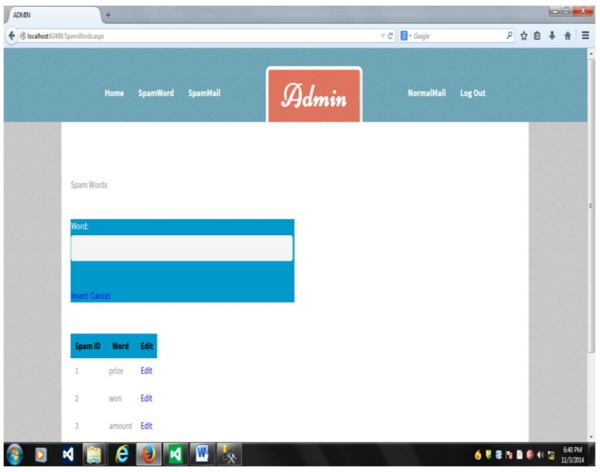
5.4 Sent Mail



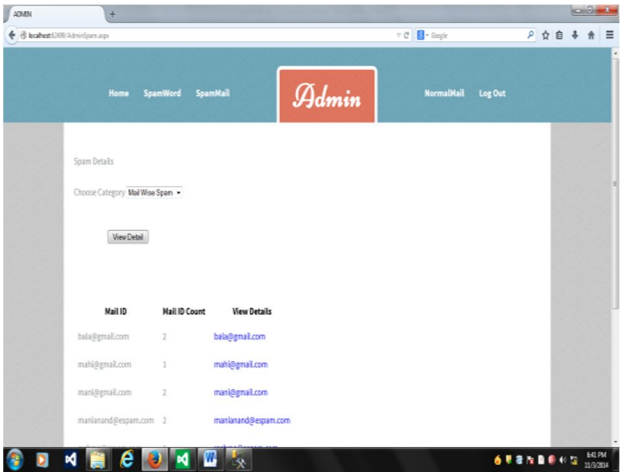
5.5 Inbox Mail



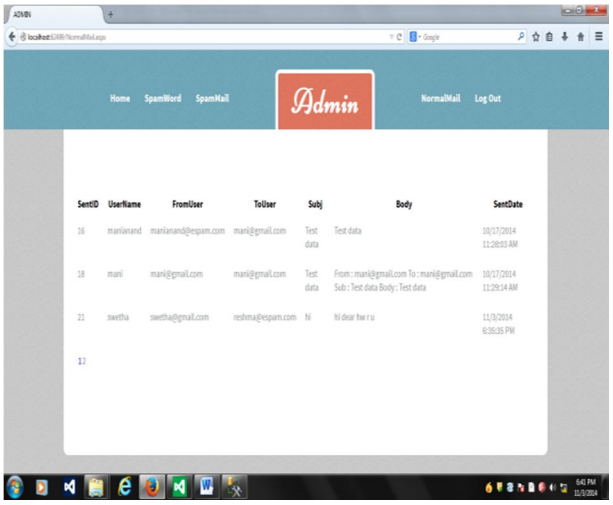
5.6 Spam Word



5.7 Spam Mail Details:



5.8 Normal Mail Details



VI. Conclusion

In this paper, we have proposed a novel SII model for the propagation of modern email malware. This model is able to address two critical processes unsolved in previous models: the reinfection and the self-start. By introducing a group of difference equations and virtual nodes, we presented the repetitious spreading processes caused by the reinfection and the self-start. The experiments showed that the result of our SII model is close to the simulations.

There are also some problems needed to be solved, such as the independent assumption between users in the network and the periodic assumption of email checking time of users.

VII. References

1. M. Fossi and J. Blackbird, “Symantec Internet Security Threat Report 2010,” technical report Symantec Corporation, Mar. 2011.

2. P. Wood and G. Egan, “Symantec Internet Security Threat Report 2011,” technical report, Symantec Corporation, Apr. 2012.

3. C.C. Zou, D. Towsley, and W. Gong, “Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worms,” IEEE Trans. Dependable and Secure Computing, vol. 4, no. 2, pp. 105- 118, Apr.- June 2007.

4. Z. Chen and C. Ji, “Spatial-Temporal Modeling of Malware Propagation in Networks,” IEEE Trans. Neural Networks, vol. 16, no. 5, pp. 1291-1303, Sept. 2005.

5. C. Gao, J. Liu, and N. Zhong, “Network Immunization and Virus Propagation in Email Networks: Experimental Evaluation and Analysis,” Knowledge and Information Systems, vol. 27, pp. 253-279, 2011.

6. S. Wen, W. Zhou, Y. Wang, W. Zhou, and Y. Xiang, “Locating Defense Positions for Thwarting the Propagation of Topological Worms,” IEEE Comm. Letters, vol. 16, no. 4, pp. 560-563, Apr. 2012.

7. J. Xiong, “Act: Attachment Chain Tracing Scheme for Email Virus Detection and Control,” Proc. ACM Workshop Rapid Malcode (WORM ’04), pp. 11-22, 2004.

8. S. Wen, W. Zhou, J. Zhang, Y. Xiang, W. Zhou, and W. Jia, “Modeling Propagation Dynamics of Social Network Worms,” IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 8, pp. 1633- 1643, Aug. 2013.