

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

A System for Mac Convention Misconduct Location

R.Ilakkiya¹, M.Maheshwari², D.R.Nandhini³ and K.Tamilarasi⁴

U.G. Student, Department of Computer Science Engineering, Velammal Institute of Technology, Chennai,
Tamil Nadu, India.¹

U.G. Student, Department of Computer Science Engineering, Velammal Institute of Technology, Chennai,
Tamil Nadu, India²

U.G. Student, Department of Computer Science Engineering, Velammal Institute of Technology, Chennai,
Tamil Nadu, India.³

Assistant Professor, Department of Computer Science Engineering, Velammal Institute of Technology, Chennai,
Tamil Nadu, India.⁴

ABSTRACT: The most common issue in mail server is delivery of spam mails. Most of the modern spam filtering techniques is deployed only in the receiver side. It is good at filtering spam for end users but spam messages still keep wasting Internet bandwidth and the storage space of mail servers. This work is therefore intended to detect and nip spamming bots in the bud. Bro intrusion detection system is used to monitor the SMTP sessions. The spam mails are detected and blocked in the sender side. This reduces storage space of mail servers and utilizes the Internet bandwidth efficiently. This is implemented in the Network layer. Bloom filter is used to track the number and the uniqueness of the recipients email addresses in the outgoing mail messages from each individual internal host. Due to the huge number of email addresses observed in the SMTP sessions, Bloom filters are used to store and manage them efficiently. In the existing system, IP address is used for blocking email malware which can be reconfigured. Here, MAC address is blocked as it is unique for a system and this is implemented in the Data Link layer using bloom filter.

KEYWORDS: spam mail, bloom filter, email malware, spamming bot.

I.INTRODUCTION

Wireless networks are computer networks that are not connected by cables of any kind. The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. The basis of wireless systems is radio waves, an implementation that takes place at the physical level of network structure. The benefits of a wireless network are convenience, mobility, easy setup, scalability, security, etc.

With the increase in number of Internet users, email is becoming the most extensively used communication mechanism. In recent years, the increased use of emails has led to the emergence and further escalation of problems caused by spam and phishing emails [1]. An automatic email classifier is a system that automatically classifies emails into one or more of a discrete set of predefined categories. For instance, in email management, one can benefit from a system that classifies an incoming email into official or personal, phishing or normal, and spam [1]. Spam is defined as unsolicited commercial email or unsolicited bulk email [2]. Spam zombies are referred as detection of the compromised machines in a network that are used for sending spam messages. Spam bots are computer program designed to assist in the sending

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

of spam.. Spam bots usually create accounts and send spam messages with them. It has become the major problem for email users. A Spam email causes serious problems such as network bandwidth consumption, system resource utilization, time of users, usage of limited mailbox space. To deal with these problems, efficient spam email filtering mechanism to be implemented [2].

The email classification process is divided into three distinct levels [1]:

i) Pre-processing/Data cleansing:

An email dataset should be collected. Then email is converted into token of words. This level also eliminates unnecessary words or stop words to reduce the amount of data that needs to be examined for their dispositions. Stemming and lemmatization are performed on token of words to convert them into their rootforms.

ii) Learning:

Features (a measurement of some aspect of a given user's email activity or behaviour) sets are developed and features are extracted. It is essential in making the learning task efficient and more accurate. After feature extraction, the most discriminative features are selected for the classification to enhance classifier performance in terms of accuracy and efficiency.

iii) Classification:

A classifier is constructed and saved to classify future incoming emails. Finally, a constructed classifier is used to classify an incoming email into a specific class, such as ham, spam, phishing, etc.

The rest of the paper is organized as follows. Section 2 discusses Literature Review. Section 3 then describes how spam mails are detected and blocked in sender side. Section 4 shows the results. Section 5 concludes the whole paper.

II. LITERATURE REVIEW

In 2017, Chih-Ning Lee, Yi-Ruei Chen and Wen-Guey Tzeng proposed an online subject-based spam filter built upon an extended version of weighted naive Bayesian (WNB) classifier. The spam filter checks email subjects only. It is faster than spam filters that scan whole body of emails and useful even spam senders temper email bodies to avoid filtering. This classifier is immune to the spams with malicious campaigns beyond contemplation [3].

In 2015, Warinda Kiatdherarat, Chayakorn Netramai proposed that reduction of the bandwidth usage of the Bloom Filter based SNMP by means of an additional compression scheme. Zip compression and zip decryption techniques are used for zip encryption and zip decryption of the Bloom Filter. The experiment with compression ratio showed that the SNMP bandwidth is reduced, compression time became small and negligible and SNMP information still retain its 100% correctness. [4].

In 2012, Frederic Massicotte, Mathieu Couture; Hugues Normandin, Frederic Michaud proposed a Dynamic Malware Analysis System (D-MAS), often called a sandbox, is a controlled environment in which malicious software (malware) is executed in order to identify the actions it is performing when infecting computer systems [5].

In 2006, Z. Duan, K. Gopalan, and X. Yuan analyzed emails received at a large US university campus network and characterized the spammer behavior at both the mail server and the network levels and proposed that spam mails sent by a large portion of spammers are received at mail server level and only negligible amount of spam mails are received at network level [6].

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

In 2006, M. Xie, H. Yin, and H. Wang proposed a simple and effective technique called DB Spam which is used to on-line detect and break spam laundering activities inside a customer network. One salient characteristic of proxy-based spamming activities, namely packet symmetry, by analyzing protocol semantics and timing causality is revealed. [7]

In 2004, J. Jung, V. Paxson, A. Berger, and H. Balakrishnan proposed that Network Intrusion Detection Systems (NIDS) are attempted to detect attackers who routinely performed ports cans of IP addresses and flagged these port scanners as malicious. Balancing the goals of promptness and accuracy in detecting malicious scanners is a delicate and difficult task [8].

III. PROPOSED SYSTEM

DESCRIPTION:

In Proposed System, spam filtering techniques are deployed on the sender side itself. This reduces the usage of internet bandwidth and memory storage. Encrypted files, .exe files, prank links and unwanted advertisements are blocked at the sender side itself. Bloom filter is used to track the REAs. Large number of REAs can be handled. The lists of spamming bots are reported to the network administrators in the computer center for them to investigate and crack down the hosts. World Net dictionary and short message technique is used to find the encrypted format text and to find the spam. An automated report of blocked spam messages is generated. When the fixed count for sending spam messages is exceeded, the particular MAC id is blocked. Fig. 1 shows the system design.

SYSTEM DESIGN:

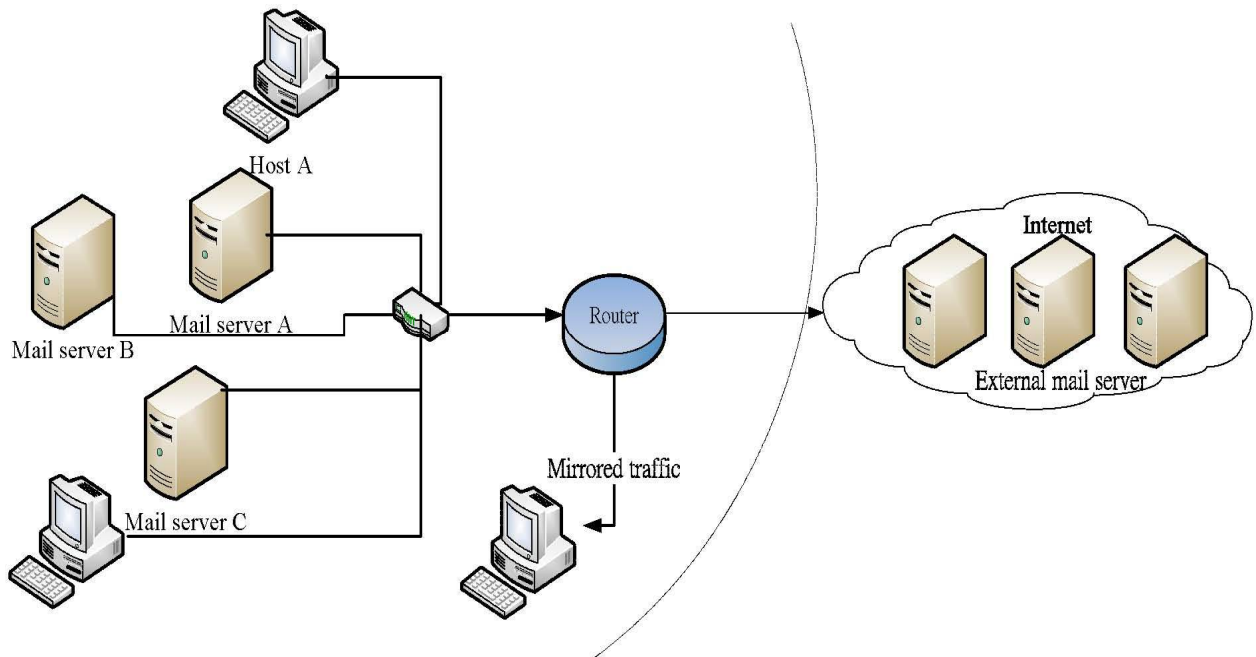


Fig.1 shows System design

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

SUBSYSTEMS:

A. Users profile:

The email user can register by signing up with their user name (e-mail id) and a secured password along with date of birth, mobile number and favorite hobby. The user can login by providing email id and respective password. If the user id (email id) and password matches the user will be permitted to login the mail. If the user forgets the user name or password, they can login by providing their date of birth, mobile number and favorite hobby.

B. Message composition, delivery and report generation:

Message composition and delivery:

Mail containing only positive words and attachments without virus files are successfully delivered where as mail containing negative words, prank video links, '.exe' files and unnecessary marketing advertisements are blocked in the sender side.

Automated report generation:

The sender can view the report of blocked messages with REA and its subject. By clicking to a particular message the user can view the details of the message. It contains the reason for blocking mails from sending.

C. Network Monitoring and blocking:

Network Monitoring:

It contains the list of MAC address from which the user has received message. It also contains the count of message.

Blocking:

It contains the message, message count, blocking status and message details. By clicking the details, detailed report can be viewed by the admin.

D. REA monitoring:

It contains the recipient email address and the message count of respective REAs. Blocking status contains three status namely blocked, unblock and waiting count to block REA. The REA will be blocked once the fixed count is reached. A compromised user may send malware email copies to neighbors every time the user visits those malware hyperlinks or attachments. Malware emails are also sent when certain events like computer restart are triggered. Thus, at an arbitrary time t , a user may receive multiple malware email copies from an identical neighboring user who has been compromised.

IV. RESULTS

Fig. 2- 7 shows how mails containing spam messages such as negative words, prank links, .exe files, unwanted advertisements are blocked from sending and report of blocked mails are generated automatically. It is monitored by monitoring Network and REA.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018



Fig. 2 shows sending prank video link

Prank links are considered as spam. Thus mails containing these are blocked from sending.



Fig. 3 shows sending .exe files

Executable files and shortcut files are considered as spam. Thus mails containing these sorts of files are blocked.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018



Delete	To	SUBJECT	TIME
<input type="checkbox"/>	nandhini@gmail.com	spam message	2018-02-21 21:46:10.0
<input type="checkbox"/>	nandhini@gmail.com	prank link	2018-02-21 21:53:47.0
<input type="checkbox"/>	nandhini@gmail.com	exofiles	2018-02-21 22:01:37.0

Fig. 4 shows automatic report generation.

This report contains details of blocked messages with REA and its subject.



Hi ilakkiya !

View Reports Message

[Back to Reports](#)

Your Subject or Message Containing this Encrypted Spam Word - '!#\$%&*()_(*&^\$#%&*())(*&'

To : nandhini@gmail.com
SUBJECT : spam message
MESSAGE : !#\$%&*()_(*&^\$#%&*())(*&
TIME : 2018-02-21 21:46:10.0
IP : 38-B1-DB-EC-41-EA

Fig. 5 shows the reason for blocking the message.

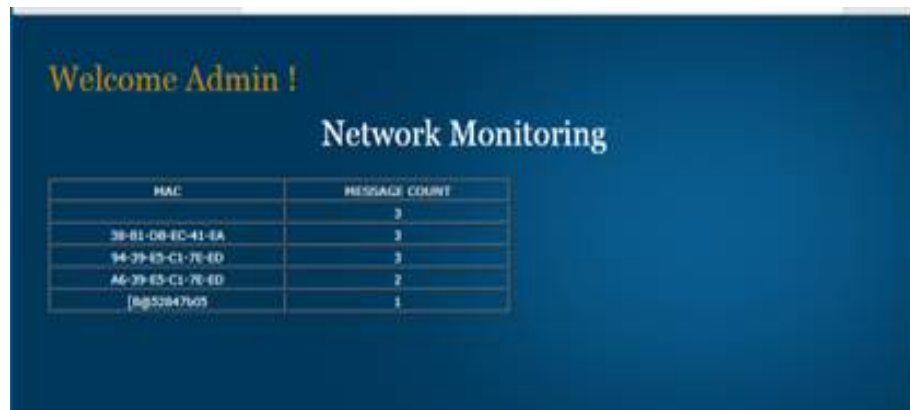
By clicking a particular message the user can view the details of the blocked message.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018



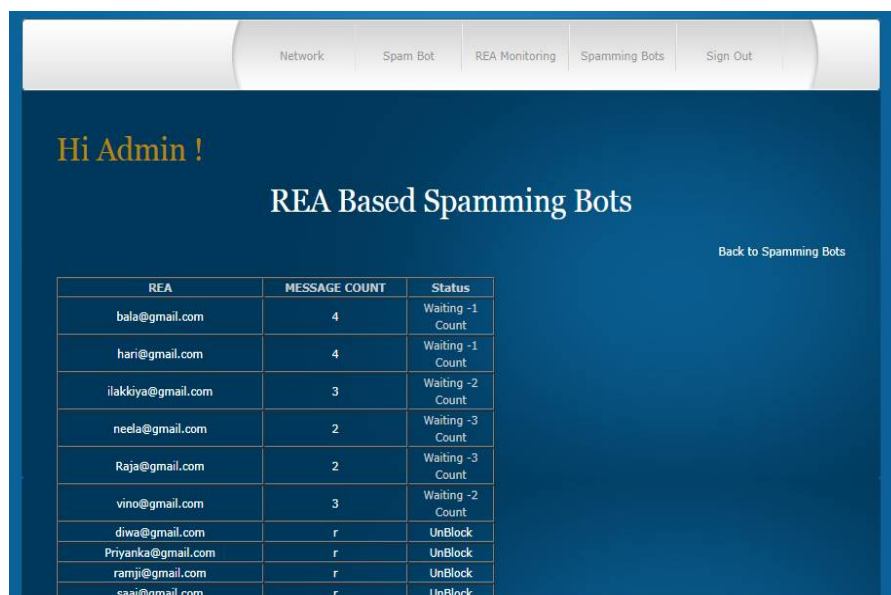
Welcome Admin !

Network Monitoring

MAC	MESSAGE COUNT
	3
38-81-08-EC-41-EA	3
94-39-85-C1-7E-ED	3
A6-39-85-C1-7E-ED	2
1a@52847605	1

Fig. 6 shows Network monitoring

It contains list of Mac address with message count.



Hi Admin !

REA Based Spamming Bots

Back to Spamming Bots

REA	MESSAGE COUNT	Status
bala@gmail.com	4	Waiting -1 Count
hari@gmail.com	4	Waiting -1 Count
ilakkiya@gmail.com	3	Waiting -2 Count
neela@gmail.com	2	Waiting -3 Count
Raja@gmail.com	2	Waiting -3 Count
vino@gmail.com	3	Waiting -2 Count
diwa@gmail.com	r	UnBlock
Priyanka@gmail.com	r	UnBlock
ramji@gmail.com	r	UnBlock
saai@gmail.com	r	UnBlock

Fig. 7shows REA monitoring

It contains lists of the Recipients email address with message count and blocking status

V.CONCLUSION

This paper tries to summarize how spam mails are detected and blocked in the sender side using MAC address. Bloom filter technique is used to detect and block the spamming bots. Large number of REAs can be handled. The spam messages are filtered at the sender side itself. This reduces the usage of internet bandwidth. MAC address is used to block the spamming bots. When the fixed count for sending spam messages is exceeded, the particular MAC id is

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

blocked. Prank links, .exe files and mails containing negative words are blocked. Marketing advertisements are considered as spam messages and hence it is blocked. An automated report of blocked spam messages is generated.

REFERENCES

- [1] GhulamMujtaba, LiyanaShuib, Ram Gopal Raj, NahdiaMajeed and Mohammed Ali Al-Garadi, "Email Classification Research Trends: Review and Open Issues", 2016.
- [2] Reshma Varghese and Dhanya.K.A, "Efficient Feature Set for Spam Email Filtering", IEEE 7th International Advance Computing Conference, 2017
- [3] Chih-Ning Lee, Yi-Ruei Chen and Wen-GueyTzeng, "An online subject-based spam filter using natural language features", Dependable and Secure Computing, 2017.
- [4]WarindaKiatdherarat and ChayakornNetramai, "Bandwidth reduction in SNMP monitoring system with bloom filter using lossless compression", International Conference on Science and Technology(TICST), 2015.
- [5] Frederic Massicotte, Mathieu Couture, HuguesNormandin and Frederic Michaud, "A Testing Model for Dynamic Malware Analysis Systems", SoftwareTesting, Verification and Validation, 2012.
- [6] Z. Duan, K. Gopalan, and X. Yuan, "Behavioral Characteristics of Spammers and Their Network Reachability Properties," Technical Report TR-060602, Dept. of Computer Science, Florida State Univ., 2006.
- [7] M. Xie, H. Yin, and H. Wang, "An Effective Defense against Email Spam Laundering", Proc. ACM Conf. Computer and Comm. Security, Oct./Nov. 2006.
- [8] J. Jung, V. Paxson, A. Berger, and H. Balakrishnan, "Fast Portscan Detection Using Sequential Hypothesis Testing," Proc. IEEE Symp. Security and Privacy, May 2004.
- [9] J. Robertson, "E-mail Spam Goes Artisanal", Bloomberg Technology, Jan. 2016
- [10] A. Almomani, B. Gupta, S. Atawneh, A. Meulenber, and E. Almomani, "A survey of phishing email filtering techniques," Communications Surveys & Tutorials, IEEE, vol. 15, pp. 2070-2090, 2013.
- [11] S. Yadav, A. K. K. Kumar, K. Reddy, A. L. Reddy, and S. Ranjan, "Detecting algorithmically generated malicious domain names," in Proc. ACM Internet Meas. Conf., Melbourne, VIC, Australia, Nov. 2010.
- [12] Z. Chen, C. Chen, and C. Ji, "Understanding Localized-Scanning Worms," Proc. IEEE Int'l Performance, Computing, and Comm. Conf. (IPCCC '07), 2007.
- [13] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "BotHunter: Detecting Malware Infection through Ids-Driven Dialog Correlation," Proc. 16th USENIX Security Symp, Aug. 2007.
- [14] G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," Proc. 15th Ann. Network and Distributed System Security Symp. (NDSS '08), Feb. 2008.
- [15] N. Ianelli and A. Hackworth, "Botnets as a Vehicle for Online Crime," Proc. First Int'l Conf. Forensic Computer Science, 2006.
- [16] J.P. John, A. Moshchuk, S.D. Gribble, and A. Krishnamurthy, "Studying Spamming Botnets Using Botlab," Proc. Sixth Symp. Networked Systems Design and Implementation (NSDI '09), Apr. 2009.
- [17] J. Klensin, "Simple Mail Transfer Protocol," IETF RFC 2821, Apr. 2001.
- [18] Leo Hatton and Alan John, "Delivering Genuine Emails in an Ocean of Spam", Wireless networking, June 2017.
- [19] Y. W. Wang, Y. N. Liu, L. Z. Feng, and X. D. Zhu, "Novel feature selection method based on harmony search for email classification," Knowledge-Based Systems, vol. 73, pp. 311-323, Jan 2015.
- [20] D. Anstee, A. Cockburn, G. Sockrider, and C. Morales, "Worldwide infrastructure security report," Arbor Netw., Burlington, MA, USA, Tech. Rep., Jan. 2014, vol. 9.