Development of Security in Intellectual Networks

T.Kishore Babu[1], Dr.GuruPrakash.C.D[2]
[1, 2] CSE Department
[1] Andhra Loyola Institute of Engineering and Technology, Vijayawada.
[2] Sri Siddhartha Institute of Technology, Maraluru, Tumakuru.

Abstract- *There are security coercions in compromised machines which is used to spread malware and junk... The spamming doings and malware undertakings are the key to recruit cooperated machines, an effective Spamming and malware discovery system is generated to detect any cooperated machine on the network. RTOSP is called Part test of Sequential Possibility. The spam detection system monitors the departing messages which has error rates which can be bad and progressive. The detailed methodology has been discussed which captures the ip address of cooperated machines and detect the level of junk on the basis of their corresponding threshold values. Hence forth, we also achieve various security mechanisms verification, privacy, reliability, non-repudiation, and obtainability and contact services.*

Keywords- RTOSP, Junk, zombies, security, virus, malware, Cooperated machine.

I. INTRODUCTION

The most complex task is to work on uncompromised machines on network. The machines that are used spread various attacks such as spreading malware, virus and spamming which makes the hacker or attacker to use various machines on the internet, spotting and cleaning the threat on time is the most crucial task on the internet. RTOSP is used to detect the compromised machines on the network RTOSP is used to detect the threat machine Ratio test of Sequential Probability.RTOSP needs number of observations.Spam net is considered to be the most crucial threat. [1-2] Spam hunter has been created to capture all kinds of spam which includes various threats that includes virus worms and malware. These Spam net has been considered as a threat to attributes of information security. Due to increase of spam net congestion has been increased in the network. In existing system there is no mechanism which can detect the spam net in the cognitive network Based on the drawbacks of existing system a new framework has been proposed which includes six different modules which will detect the spam and mark them as compromised machines[3-6]. Based on the compromised machines the ip address have been recorded of the compromised machines and is considered as threat.

After detection RTOSP detection system compares the machines threshold level. Henceforth various attributes of information security have been applied on the RTOSP module [7-8].

In this research paper we develop a Spamming and malware detection system, named RTOSP, which monitors the outgoing messages. RTOSP is a statistical model called Ratio test of Sequential Probability (SPRT which has error rates that are positive and negative .In this system architecture different modules have been created. In RTOSP module firstly the IP address of different machines have been compared. Based on which there is a spam filter which filters the data either as spam or not spam [15]. The spam have been recorded as compromised machine which have been separated from Uncompromised machine. In the last module machines have been compared .The threshold activity is maintained in compromised machines. After the results that have been generated based on the analysis. These results have been analyzed on various attributes of information security [9-10]. The attributes of information security includes the following:

X Authentication x	Confidentiality x	Availability x
Access Services x	Non Repudiation x	Integrity

In this paper, Section II represents the proposed mechanism and the Corresponding results are compared in Section III. Section IV concludes the paper.

II. PROPOSED MECHANISM

***Module 1:** Interface-Interaction ModuleIn Interface-Interaction Module we create a system for end user login. In order to forward messages to other user all the machines have to logon to the network.

***Module 2:** RTOSP Module in the RTOSP Module all the IP address of each machine which sends a message is recorded and whenever a machine sends a spam messages continuously then it is considered as threat machine.

*** Module 3:** Poll-Count Module (P-C) Poll Count Module is used to record the number of spam messages sent by each machine based on their IP address over a particular network.

*** Module 4:** Percentage (PM) Module In this Percentage module we find the compromised machines based on the proportion of all the spam messages that are recorded and their corresponding machines.

*** Module 5:** Spamming and malware Detection ModuleThe spamming and malware detection module detects the compromised machine and compare their threshold levels.If they exceed the threshold levels they are considered as spam. After all the results are being analyzed on various attributes of information security which includes confidentiality, accessibility, integrity, authentication access control& non repudiation.

The detailed methodology to be followed is:

Stage 1: In this account is login with email id and password and email is composed to different receivers
Stage 2: Then the email sent to different receivers are analyzed using RTOSP module.
Stage 3: The IP address are captured and passed through spam filter to differentiate between compromised and uncompromised machines.
Stage 4: Then Compare RTOSP module are done using CT(Compare threshold) and UT(Uncompromised threshold) which compares the threshold values of the spam mail.The results are passed through compare CT(Compare threshold) and UT(Uncompromised threshold) which compares the threshold values of the spam mail.If the threshold value is n and output comes as n+1 or n+2 etc it is a spam mail if the threshold value comes n-1 or n-2 etc it is not a spam mail.In this way the ip address of compromised machines are stored and are blocked for future communication.
Stage 5: These modules have been analyzed on the basis of attributes of security which includes confidentiality, integrity, authentication, accessibility, non-repudiation and access control.

III. ANALYSIS OF RESULTS

In the research paper a machine is involved in keeping a track of all spam messages. Any new machine which enters into the network is monitored by RTOSP. The main machines considered as a server machine, it monitor all the spam messages. RTOSP detection system can detect compromised machines very quickly and efficiently. It also reduces the number of observations in the system.System administrators can automatically detect the compromised machines as shown in Table I and Table II.

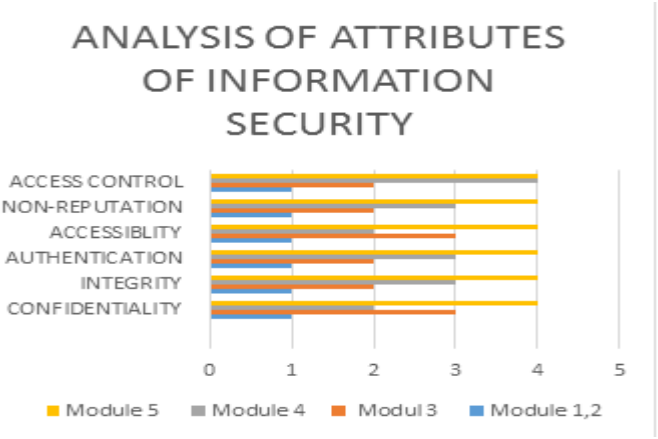
Table 1. Analysis Of Different Modules

degree	Module 1&2	module 3	module 4	module 5
confidentiality	low	medium	moderate	high
integrity	low	moderate	medium	high
authentication	low	moderate	medium	high
accessibility	low	medium	moderate	high
non-reputation	low	moderate	medium	high
access control	low	moderate	medium	high

4=High Security
3=Medium Security
2=Moderate Security
1=Low Security

Module A: Interface-Interaction Module
Module B: RTOSP Module
Module C: Poll-Count Module
Module D: Percentage (PM) Module
Module E: Spamming and malware Detection Module

TABLE 2.



COMPARISON OF ATTRIBUTES OF INFORMATION SECURITY

IV. CONCLUSION

In this research paper, an effective zombie system has been detected RTOSP which monitors all the outgoing messages. RTOSP is an efficient and statistical tool named Ratio test of Sequential Probability to detect the compromised machines that are occupied in any spamming activities. RTOSP has devised a system which has both rates positive and negative. It also decreases the number of required observations to detect a Spamming and malware. Based on which security has been enhanced by monitoring various attributes of information security.

REFERENCES

[1] L. Yang, L. Cao, and H. Zheng, "Proactive Channel Access in Dynamic Spectrum Network," Proc. Int'l ICST Conf. Cognitive Radio Oriented Wireless Networks (CROWNCOM '07), July 2007.

[2] Q. Zhao, L. Tong, A. Swami, and Y. Chen, "Decentralized Cognitive Mac Opportunistic Spectrum Access in Ad Hoc Networks: A Pomdp Framework," IEEE J. Selected Areas in

[3] Comm., vol. 25, no. 3, pp. 589- 600, Apr. 2007

[4] R. Tandra, S.M. Mishra, and A. Sahai, "What Is a Spectrum Hole and What Does It Take to Recognize One?" Proc. IEEE, vol. 97, no. 5, pp. 824-848, May 2009

[5] W. Stallings, Cryptography and network security: principles and practice: Prentice Hall, 2010.

[6] P. Kruus, C. Scace, M. Heyman, M. Mundy,A Survey of Steganographic Techniques for Image Files,Advance Security Research Journal,vol. 05,pp 41-52,2011

[7] Ross J. Anderson,A Security Policy Model for Clinical Information Systems, vol. 08,pp 33-42,2012.

[8] Yogesh Kumar, Lecturer in CSE Deptt, BPR College of Engg Gohana (Sonipat), Rajiv Munjal, lecturer in CSE Deptt., CBS Group of institution (Jhajjar), Harsh Sharma, Lecturer in CSE Deptt, BPR College of Engg Gohana (Sonipat), 2011, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", IJCSMS International Journal of Computer Science and Management Studies.

[9] Manish Singh, Shailender Gupta and Bharat Bhushan, YMCA University of Science and Technology, Faridabad, 2012, "Comparison of symmetric and asymmetric key cryptography: A study", Proceeding of the National Conference "Science in Media 2012" Organized by YMCA University of Science and Technology, Faridabad, Haryana (India).

[10] Karimi, R. , Dept. of Comput., Islamic Azad Univ., Qazvin, Iran ,

[11] Kalantari, M.,2011, "Enhancing Security and Confidentiality in Location- Based Data Encryption Algorithms",Roedunet International Conference(RoEduNet)

[12] Shraddha D.Ghogare, Swati P. Jadhav, Ankita R. Chadha, Hima C. Patil, 2012 "Location Based Authentication: A New Approach towards Providing Security" International Journal of Scientific and Research Publications.

[13] C. Ko and T. Redmond,Detecting Race-condition Attacks Using Noninterference,Advance Security Research Journal,vol. 05,pp 77- 85,2013

[14] Lalit Singh, Dr. R.K. Bharti (C.S.E) BTKIT Dwarahat, 2013, "Comparative Performance Analysis of Cryptographic Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering Research Paper.