ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2 Issue 10, October 2013

Anomaly Detection & Prevention by Using Users Fingerprints

Nitin Y. Suryavanshi , Dinesh D. Puri , Atul V. Dusane

***Abstract*-According to the latest National Opinion Poll, as of January 2007, almost half of UK citizens still harbor a "deep mistrust" of the Internet due to security concerns. The House of Lords Select Committee on Science and Technology, meanwhile, is currently orchestrating a major enquiry into personal Internet security. Their Lordships observed wisely that "With the ever growing use of home computers, the spread of broadband and the rise in internet banking and commerce the importance of proper internet security measures has never been greater." In Network Security concern network access control and security assurance is a major issue to secure the private or public network from abnormal user. In this paper we are presenting the design and implementation of anomaly prevention through packet filtering model which is used to detect the anomalies using IP Gray Space analysis and preventing the network from such anomalies using UDP packet filtering.**

Index term: **Anomalies Detection System, Anomalies Prevention System**

I. INTRODUCTION

To handle all issues related the network security must consider the behavior of the users from the internet which may cause the harm to the network and becomes anomalous users or abnormal user. The challenge of detection and prevention from anomalous host is accepted by anomaly detection and prevention system [1]. Intrusion Detection technique is classified in to two categories : Signature based misuse detection in which identification of normal user is given to server through the database and second is anomaly detection & Anomaly based detection by identifying the activities of user it classify into the normal and abnormal user[2][3] To overcome limitation of signature based misuse detection the concept of anomaly detection was introduced in the work of Denning [5]. Anomaly detection systems can observe activities that deviate significantly from the established normal usage profiles as anomalies. Our APTPF system detects of anomaly from network and preventing it which under consideration. In this paper we consider IP gray space analysis [1], identifying an anomalies from large area network and UDP packet filtering for the prevention purpose we present an APTPF model which is used to detect and prevent the network anomalies using IP Gray Space analysis and UDP Packet filtering. This methodology is working in two phases first phase is identification phase and second phase is prevention phase. In identification phase it is detecting the abnormal behaviors using the concept of unassigned IP addresses viz Gray IP and in second phase it is preventing the network by using the concept of UDP packet filtering by user cooperation.

II. NETWORK ANOMALY

Anomaly is a behavior based system which detects normal and abnormal users in system anomaly detection system establishes baseline for all users and depends on it decides anomaly .Network anomaly is an abstraction of existing intrusion detection techniques to the network level allowing us to simultaneously monitor the security of multiple nodes as well as the network infrastructure. Network anomalies typically refer to circumstances when network operations deviate from normal network behavior. The anomalies can arise due to various causes such as malfunctioning network devices, bad configuration in network services and operating systems, Network overload, malicious denial of service attacks, ill advised applications installed by users, high level users' effort to discover network and gather information about it and its devices These anomalous events will disrupt the normal behavior of some network data

III. IP GRAY SPACE AND IP ACTIVE SPACE ANALYSIS

In networks often have many unassigned IP addresses that collectively form IP gray space within the address blocks of such networks [1]. In network there are number of IP Addresses all these addresses are called as IP space that IP space is divided into two address blocks one is IP gray space and other is IP active space. All IP addresses are not likely to be assigned to "active" hosts (i.e., actual machines such as servers, desktops, lap- tops, etc.) at any given time period. We refer to these IP addresses within the campus network that are not assigned to any host throughout a given time period, say, an hour or a day, as "inactive" or gray IP addresses. In contrast, the IP addresses within the same address blocks that are assigned to hosts at any point within the time period are referred to as active IP addresses. The inactive IP addresses collectively forms IP gray space [1] within the address blocks, while active addresses the active space.

By definition, IP gray and active space within a campus or any network are time dependent in other words, they are not fixed and vary over time. In IP Gray space analysis we will identify IP gray space if any outside host if try to access that gray IP address we will trap him/her and after trapping he/she will be the anomalous host in our campus network.

IV. PACKET FILTERING

Packet filtering is a network security mechanism that works by controlling what data can flow to and from a network. To transfer information across a network, the information has to be broken up into small pieces, each of which is sent separately. Breaking the information into pieces allows many systems to share the network, each sending pieces in turn. In IP networking, those small pieces of data are called packets.All data transfer across IP networks happens in the form of packets. Client Communicate with the server. In this system client send the information about himself in the form of the message in the UDP Packet. This is the UDP client for the communication it uses the User datagram protocol (UDP) only, because UDP is connection less protocol.

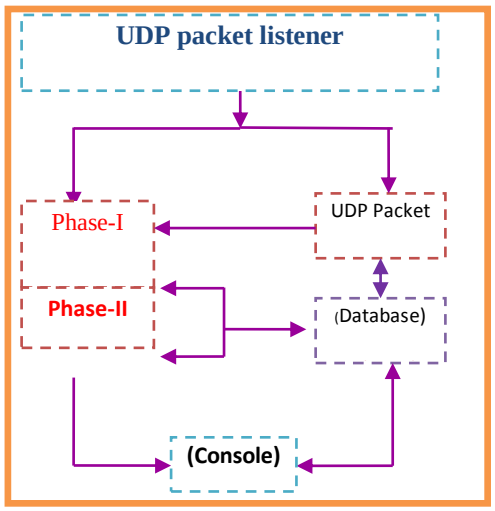

Fig. 1 APTPF Model

Offset (Bits)	0-15	16-32
0	Source Port Number	Destination Port Number
32	Length	Checksum
64+	ProcessorID@MAC@ Username	

Fig. 2 Datagram of UDP

V. PROPOSED METHODOLY

In proposed methodology we are designing and implementing a APTPF model used to detect and prevent the network from anomalies this model will work in two phase

Phase-I Detection of Anomalies using IP Gray Space Analysis

This work involves the development of two step methodology naming As H-NADS Model
Identifying and tracking anomalous hosts by correlating traffic towards both IP gray and active spaces of a network. In the first step we set an IP active threshold range that range is called as IP active space. Such a threshold setting is called as association rule generation [5] for supervised learning .If source IP Address of communication host is comes from IP. Active Space (198.162.51.1 to 198.162.51.254) and IP gray space if any host crosses that threshold of IP active space he/she is an anomalous host.

Phase-II-Prevention of Network from Anomalies using UDP Packet filtering

This phase processed the result of first phase. Once APTPF model detect network anomalies then the working of this phase starts. If any anomalous host interfaces out defended network then it becomes necessary to protect the network from such users. In this phase the model will captures the MAC address and Processor-ID of each outsider interfacing host and by using that knowledge this phase will denial all services of anomalous host by masking the source IP of given anomalous host .

APTPF Algorithm

1. User sends one UDP packet with Processor Id, MAC & user name in datagram.
2. Server accepts UDP packets through the UDP listener analyze as existing work store in Input table.
a. Make IP Validation by using IP gray space analysis.
b. Identify physical system through the MAC and Processor ID
3. Take a Turing test through the user ID
a. If communicated IP and Associated MIC in white table to allow the access.
b. If IP is matched but its associated MIC not match with white List then give message as invalid user & IP snooper & Make entry in black list of MIC
c. If IP is not in White List or not active IP but MIC in White List, it treated as masking user and denies access.
d. If MIC & IP is not white list & its active IP Then It is new user Administrator decided the action
4. Added to White List & allow the access Else add in Black List to denies the access

VI. DISCUSSION

In result we identified various anomalies using IP Gray Space and prevent the network using UDP datagram Filtering. In External Host Interface we are using username Turing Test for the identification of human and machine.

VII. CONCLUSIONS AND FUTURE WORK

Anomaly detection is a major issue in network security, so by considering this myth we develop and implement a two phase approach for preventing from anomalous host by considering IP Gray Space and UDP packet Filtering which is connection less protocol. In future we will try to implement a proposed method develop for detect anomalies by using support vector machine technique.

VIII. REFERENCE

[1] Yogendra Kumar JAIN, Sandip S. PATIL "*Design of Hybrid Network Anomalies Detection System (H-NADS) Using IP Gray Space Analysis*" International Journal of Informatica Economică vol. 13, no. 2/2009 110

[2] K. Jackson, *Intrusion Detection Systems* (IDS): Product Survey, Los Alamos National Laboratory,

[3] H. Debar, M. Dacier, and A. Wespi, *Towards a Taxonomy of Intrusion Detection Systems*, Computer Networks, 31(8):805-822, April 1999

[4] Wei Lu, Mahbod T. and Ali A." *Detecting Network Anomalies Using Different Wavelet Basis Functions*", Communication Networks and Services Research Conference 978-0-7695-3135-9 IEEE August, 2008 .

[5] D.E.Denning, "An Intrusion Detection Model." IEEE Transactions on software engineering, 2:222

AUTHOR

Mr. Nitin Y. Suryawanshi is currently working as Assistant Professor in Shram Sadhana Bombay Trusts College of Engineering & Technology, Jalgaon. He has received his M.E. degree in Computer science and engineering from North Maharashtra University, Jalgaon in the year 2012 and. He has published 8 research papers in reputed journals, International and National conferences. His research interest includes Analysis and design of system and network security.

Mr. D.D Puri is currently working as Assistant Professor in Shram Sadhana Bombay Trusts College of Engineering & Technology, Jalgaon. He has received his M.Tech degree in Computer technology from Dr. Babasaheb Ambedkar Technological University, Lonere in the year 2010 and and B.E degree in Computer Science & Engg. from walchand College of Engineering Sangali under Shivaji University in 2004. He has published many research papers in reputed journals, International and National conferences. His research interest includes Software Engineering, Computer networking, Pattern Recognition and Knowledge Discovery & Management.

Mr. A.V. Dusane currently working as Assistant Professor in Shram Sadhana Bombay Trusts College of Engineering & Technology, Jalgaon. He has received his M.E degree in Computer technology from North Maharashtra University in 2012 and B.E degree in Computer Science & Engg. from Shram Sadhana Bombay Trusts College of Engineering & Technology, Jalgaon NMU University in 2009. He has published many research papers in reputed journals, International and National conferences. His research interest includes Software Engineering, Image Processing.