International Journal of Electronics, Communication & Soft Computing Science and Engineering
ISSN: 2277-9477, Volume 2, Issue 3

Intrusion Detection Technique in Standard Network

Mamitha R Patil, Shivu G Raj, Siddharth Jain, Prof. Rajshekhar M

Abstract — Intrusion detection is a significant focus of research in the security of computer systems and networks. This paper presents an analysis of the progress being made in the development of effective intrusion detection systems for computer systems and computer networks. The technologies which are discussed are designed to detect instances of the access of computer systems by unauthorized individuals and the misuse of system resources by unauthorized system users. A review of the foundations of intrusion detection systems and the methodologies which are the focus of current development efforts are discussed. The results of an IDS in network security and network professionals are discussed to offer a real-world view of Intrusion Detection System in Networks.

Index Terms—*Computer* & Network Security **(CNS),** Intrusion Detection System **(IDS),** Anomaly Detection (AD), Misuse detection (MD).

I. INTRODUCTION

Intrusion Detection as is an approach to counter the computer and networking attacks and misuses. Intrusion Detection is implemented by an intrusion Detection System using any network connectivity and its user data in a network and today there are many commercial Intrusion Detection Systems available. In general, most of these commercial implementations are found to be insufficient, which gives rise to the need for research on more dynamic Intrusion Detection Systems. Generally an intruder is defined as a system, program or person who tries to and may become successful to break into an information system or perform an action not legally allowed. We refer intrusion as any set of actions that attempt to compromise the integrity, confidentiality,
or availability of a computer resource .The act of detecting actions that attempt to compromise the integrity, confidentiality, or availability of a computer resource can be referred as Intrusion Detection. An intrusion detection system is a device or software application that monitors network and/or system activities for malicious or policy violations and produces reports of the current research and development efforts to detect internal and external penetrations of computer systems and networks. The area of intrusion detection is central to the concept of computer security. The first three components of security systems identified are:

1. Prevention.
2. Preemption, and
3. Deterrence,

are primarily based on passive measures which decrease the likelihood of a successful attack on a system. These components address the policy related issues of information security and those elements which can be incorporated into a system with minimal effort. Examples of these include the establishment of organizational security guidelines, security education and training, and the posting of warning notices on the initial screens of a system.

The last three components, deflection, detection, and countermeasures, are more active measures designed to protect the critical elements of a system. Of the six components as shown in fig1, the accurate detection of a system intrusion is the most critical. While additional measures may be very effective at preventing an eventual penetration of the system, all security measures rely on the accurate identification of an attacker prior to the employment of defensive measures.

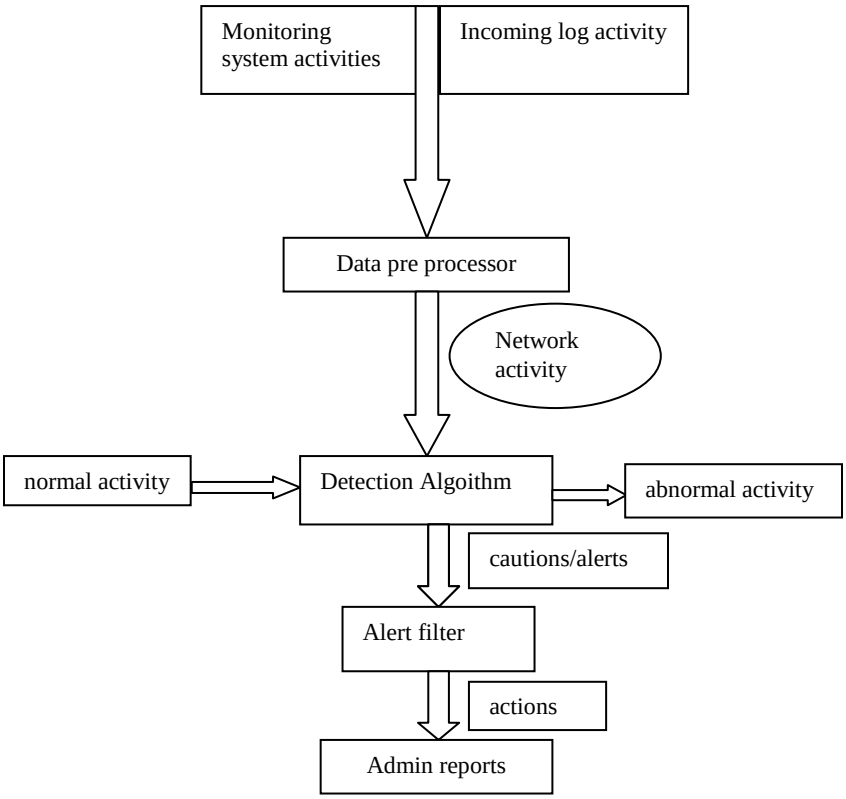


Fig.1 Components of IDS

II. Related Works

Some import applications of soft computing techniques for Network Intrusion Detection is described in this section. Several Genetic Algorithms (GAs) and Genetic Programming (GP) has been used for detecting intrusion detection of different kinds in different scenarios. Gas used to select required features and to determine the optimal and minimal parameters of some core functions in which different AI methods were used to derive acquisition of rules. There are several papers related to IDS which has certain level of impact in network security. The effort of using GAs for intrusion detection can be referred back to 1995, when Crosby and Safford applied the multiple agent technology and GP to detect network anomalies. For both agents they used GP to determine anomalous network behaviors and each agent can monitor one parameter of the network audit data. The proposed methodology has the advantage when many small autonomous agents are used but it has problem when communicating among the agents and also if the agents are not properly initialized the training process can be time consuming.

Li described a method using GA to detect anomalous network intrusion. The approach includes both quantitative and categorical features of network data for deriving classification rules. However, the inclusion of quantitative feature can increase detection rate but no experimental results are available.

The data described is based on network users to classify all types of smurf attack using the training dataset with false positive rate is very low (at 0.2%) and detection rate is almost 100%. Lu and Traore used historical network dataset using GP to derive a set of classification. They used support-confidence framework as the fitness function and accurately classified several network intrusions. But their use of genetic programming made the implementation procedure very difficult and also for training procedure more data and time is required Xiao et al. Used GA to detect anomalous network behaviors based on information theory. Some network features can be identified with network attacks based on mutual information between network features and type of intrusions and then using these features a linear structure rule and also a GA is derived. The approach of using mutual information and resulting linear rule seems very effective because of the reduced complexity and higher detection rate. The only problem is it considered only the discrete features. Gong et al presented an implementation of GA based approach to Network Intrusion Detection using GA and showed software implementation. The approach derived a set of classification rules and utilizes a support-confidence framework to judge fitness function. Abdullah et al. Showed a GA based performance evaluation algorithm to network intrusion detection. The approach uses information theory for filtering the traffic data.

III. Classification of IDS

Intrusion Detection is traditionally divided into two categories, that is., misuse detection and anomaly detection. Misuse detection mainly searches for specific patterns or sequences of programs and user behaviors that match well-known intrusion scenarios. While, anomaly detection develops models of normal network behaviors, and new intrusions are detected by evaluating significant deviations from the normal behavior. The advantage of anomaly detection is that it may detect novel intrusions that have not been observed yet. While accuracy is the essential requirement of an Intrusion-Detection System , its extensibility and adaptability are also critical in today's network computing environment. Currently, building effective IDS is an enormous knowledge engineering task. Therefore mainly classification of IDS is as shown in below fig2.

Anomaly detection

Anomaly detection is the general category of intrusion detection which works by identifying activities which vary from established patterns for users, or groups of users. Since masquerading as a legitimate user is a very powerful method for an attacker to gain access to system resources, this type of approach looks for the variations in behavior which might indicate a masquerade. Anomaly detection typically involves

the creation of knowledge bases which contain the profiles of the monitored activities.

Misuse Detection

The second general approach to intrusion detection is misuse detection. This technique involves the comparison of a user's activities with the known behaviors of attackers attempting to penetrate a system. Misuse detection also utilizes a knowledge base of information. The misuse knowledge bases include specific metrics on the various techniques employed by attackers when the knowledge base was created.

Combined Anomaly/Misuse detection

Intrusion Detection methodologies which combine the anomaly detection approach and the misuse detection approach .These techniques seek to incorporate the benefits of both of the standard approaches to intrusion detection. The combined approach permits a single intrusion detection system to monitor for indications of external and internal attacks.

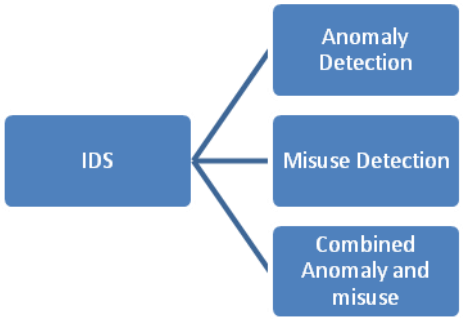


Fig.2 Classification of IDS

IV. IDS TECHNIQUE

Detection systems make four assumptions about the systems that they are designed to protect:

step1: Activities taken by system users, either authorized or unauthorized, can be monitored.

step2: It is possible to identify those actions which are indications of an attack on a system.

step3: Information obtained from the intrusion detection system can be utilized to enhance the overall security of the network.

step4: A fourth element which is desirable from any intrusion detection mechanism is the ability of the system to make an analysis of an attack in real-time. This would allow the intrusion detection mechanism to limit the adverse effects which are perpetrated on the system. An effective use of this element is probably the most difficult component of an intrusion detection system to achieve. While metrics can be developed which monitor all aspects of a user's behavior, the resulting degradation on the overall performance of the system may require that a thorough analysis be conducted off-line, thus eliminating a real-time detection capability. There are currently a variety of approaches being utilized to accomplish the desirable elements of an intrusion detection system. Two of these, anomaly detection and misuse detection, form the core of several intrusion detection techniques which currently exist. Other approaches, such as pattern recognition, are attempting to identify new methods of identifying information system attacks.

V. PROPOSED SYSTEM

A detection system capable of differentiating malicious activity from lots of background traffic collected from network traffic, to improve our understanding of user behavior, we also expanded the scope of our monitoring to explore whether we could detect malicious behavior at the level of the user's workstation in an online interview. We designed the two scenarios to be completely balanced except for the experimental variable—user intent. Both roles describe a person

1. Who has faced the hard interview times and must find difficult time to answer the questions and get good results to get placed and improve his personal morale and improve his or her financial situation. In the benign condition.

2. We gave another person an opportunity to participate in a high-profile interview team and explained that outstanding performance would likely to lead to a promotion and pay increase. In the malicious condition, we gave the person an opportunity to start a new, higher-paying job, but the offer was conditional on bringing inside information from the old company where he got placed , thereby providing a competitive advantage in a major federal acquisition. Both opportunities would mitigate the financial difficulties.

Activity: We monitored the participants using the network-based sensors and the host-based product Digital Guardian. Together, the network and the sensors monitored information-use events including file and directory reads, writes, moves, and deletes. They also monitored search-engine queries, file saves, DOC file activities like cut-and-paste functions, application launches, and URLs visited. Experimental analysis suggests that it is an effective technique of studying malicious insider behavior and identifying behaviors that appear to differentiate between the malicious and benign users.

VI. RESULTS

Table1. Network data Perceptions for Security Mechanism

NETWORK USER DATA	BENIGN (CONTROL)	MALICIOUS (EXPERIMENTAL)	TOTAL USERS
HEADERS AND FOOTERS IDENIFYING DATA AS PROPRIETRY OR SENSITIVE	3.36	3.68	3.52
INDICATING MONITORED BY POP UP WARNINGS	2.52	4.32	3.46
SOFTWARE ACTIVITY TO MONITOR YOUR COMPUTER	2.61	4.16	3.41
AGREEMENT WITH COMPANY	2.90	3.52	3.22
BEING IN A PUBLIC ENVIRONMENT WHILE USING YOUR LAPTOP	3.05	3.12	3.09
SECURITY POLICY	2.96	3.16	3.00
ORGANIZATIONAL ETHICS AND CODE OF CONDUCT	2.87	3.24	2.98
RECENT EMPLOYEE INFORMATION COMPANY RULES AND ITS VOILATIONS	2.50	3.04	2.78
TRAINING ON MAINTAINING PROPRIETARY INFORMATION	2.50	3.04	2.78

Experimental analysis of responses from the study questionnaire show that participants successfully engaged in their assigned roles (malicious or benign) while completing the information search task of benign and malicious users. Malicious participants were significantly more likely to respond that they were "performing the task different from their normal behaviour." This indicates that our malicious participants approached the task differently from our control participants, as would be the case if they were taking their assigned roles seriously. Nevertheless, the scenarios were balanced to only manipulate user intent, and the task approach differences shouldn't have upset the balances.

Experiment design:

In designing the experiment, we had concerns about whether participants would take the scenarios seriously enough to exhibit behavioural differences. We designed the post-study questionnaire to let participants describe some of their experiences in comment boxes. We asked, "Did the scenario was effective in the ways in which you performed the task?" Sixty percent of the malicious-participant responses indicated that the role of "insider" was clearly ingrained in them as they performed the task. For example, malicious participants gave the following comments:

1. "Since the scenario cast this as theft of intellectual property, I believe I ended up closing my door."

2. "The scenario suggested secrecy was wise."

3. "It has been created a few dummy folders for 'hiding' the documents that I was able to find."

4. "The scenario added to this sense of 'wrongdoing."

5. "I maintained some secret information and tried to cover up my material."

Behavioral demonstrations that malicious participants took their role seriously include a resignation letter delivered on the CD, many inquiries about the ethics of the scenario role, searches on warning procedures, and participants using obscure folder names such as "Project AAA." These malicious-user responses are particularly interesting because at no point did we instruct or even recommend that they avoid detection. One final preliminary finding worth noting is highly significant that the correlation between malicious users and the use of the employee directory. Malicious users followed a distinct methodology of looking up coworkers associated with their target topic and browsing or downloading the shared folders that the SMEs owned. This might be a lower-profile method of getting at the information than performing topical search engine queries.

CONCLUSION

Most network Intrusion threats research as on today lacks a carefully controlled administrative group for real comparison and makes statistical analyses and interpretation of findings Intrusions. Although our preliminary analyses revealed interesting and significant patterns in malicious behavior, we haven't identified any one user abnormal behavior in the network. The most valuable way to tackle insider threats seems to be to cast a wide net over many behaviors and strategically evaluate those behaviors to identify misuse. We don't yet have a single technique for proactively detecting insider misuse, but we've lowered the false-alarm threshold, helped administrators to identify misuse patterns that require attention, and provided new insights for what the common operational picture could look like for all kinds of network designs.

.

ACKNOWLEDGMENT

Our sincere thanks to the expert members, my friends, colleagues, principal and management of Kensri College Bangalore and BMSIT Bangalore for inspiring me to publish this paper.

REFERENCES

1. M. Botha, R. Solms, "Utilizing Neural Networks For Effective Intrusion Detection", ISSA,2004.

2. R. Graham, "FAQ: Network Intrusion Detection Systems". March 21, 2000.

3. D. Zamboni, "Using Internal Sensors For Computer Intrusion Detection". Center for Education
and Research in Information Assurance and Security, Purdue University. August 2001.

4. K. Scarfone, P. Mel, "Guide to Intrusion Detection and Prevention Systems (IDPS)". Computer Security Resource Center (National Institute of Standards and Technology). February 2007.

5. A. Chittur, "Model Generation for an Intrusion Detection System Using Genetic Algorithms". January 2005.

6. W. Li, "Using Genetic Algorithm for Network Intrusion Detection". "A Genetic Algorithm Approach to Network Intrusion Detection". SANS Institute, USA, 2004.

7. W. Lu, I. Traore, "Detecting New Forms of Network Intrusion Using Genetic Programming". Computational Intelligence, vol. 20, pp. 3, Blackwell Publishing, Malden, pp. 475-494, 2004.

8. M. M. Pillai, J. H. P. Eloff, H. S. Venter, "An Approach to Implement a Network Intrusion Detection System using Genetic Algorithms", Proceedings of SAICSIT, pp:221-228, 2004.

9. M. Middlemiss, G. Dick, "Feature selection of intrusion detection data using a hybrid genetic
algorithm/KNN approach", Design and application of hybrid intelligent systems, IOS Press Amsterdam, pp.519-527, 2003.

10. Srinivas Mukkamala, Andrew H. Sung, Ajith Abraham, "Intrusion detection using an ensemble of intelligent paradigms", Journal of Network and Computer Applications, Volume 28, Issue 2, April 2005, Pages 167-182.

11. S. Peddabachigari, Ajith Abraham, C. Grosan, J. Thomas, "Modeling intrusion detection system using hybrid intelligent systems", Journal of Network and Computer Applications, Volume 30, Issue 1, January 2007, Pages 114–132.

12. M. Saniee Abadeh, J. Habibi, C. Lucas, "Intrusion detection using a fuzzy genetics-based learning algorithm", Journal of Network and Computer Applications, Volume 30, Issue 1,January 2007,Pages 414-428

13. Tao Peng, C. Leckie, Kotagiri Ramamohanarao, "Information sharing for distributed intrusion detection systems", Journal of Network and Computer Applications, Volume 30, Issue 3, August
2007, Pages 877–899

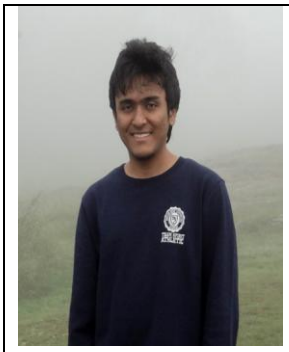
14. M. Crosbie, E. Spafford, "Applying Genetic Programming to Intrusion Detection", Proceedings
of the AAAI Fall Symposium, 1995.

15. T. Xia, G. Qu, S. Hariri, M. Yousif, "An Efficient Network Intrusion Detection Method Based
on Information Theory and Genetic Algorithm", Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC '05), Phoenix, AZ, USA. 2005.

16. Anup Goyal, Chetan Kumar, "GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System", 2008.

AUTHOR'S PROFILE

Mrs. Mamitha Patil has a vast experience of Nine years of teaching in various renowned institutions of Bangalore silicon city. Currently she is working as lecturer in the Department of computer Sciences, Kensri college, Bangalore - 24, Karnataka, India. She is also interested in research, in the computer science field. She has also published a number of research papers in various national & international journals & conferences. Her research interests are Data Mining, Computer Networks, Parallel computing, Intrusion detection systems, etc.



Mr. Shivu G Raj is studying in final year Computer Science and Engineering from BMSIT. I am compassionate, have enthusiasm to look after those less fortunate than myself. I am one among those who believe in both smart and hard working. My interest lies in technology and innovations . I am open , flexible and innovative constantly searching for new and different ways to solve problems. Also I am a workaholic person with smart personality , pleasant and cheerful nature with excellent inter personal skills and with positive attitude. My greatest strength is my willingness to understand and control everything and make sure it turns out alright. Achievements includes "Campus Brand Ambassador" for Cognizant Technology Solutions, Windows Phone Application published

	on market place and many more.

	**Mr. Siddharth Jain -** Myself Siddharth Jain, pursuing Computer Science Engineering final year in BMSIT, Bangalore. I am well motivated and energetic individual with good technical skills. I am very passionate about technology and one of my field of interests are Computer Networks. I am innovative in nature and enjoy coding and debugging. My hobbies include reading books , playing chess, travelling . Down the line in coming years i would like to see myself contributing my services for computer society under research and development. I am a flexible individual who likes challenges and solving problems. I like to lead and see what's ahead.

	**Mr. Rajashekhar M -** currently, he is working as Associate Professor in the Department of computer Science & Engg. in BMS Institute of Technology, Bangalore, Karnataka, India. He is also a research scholar in the prestigious Dr. MGR Deemed University & simultaneously doing his research work & progressing towards his Ph.D. in the computer science field. He has also published a number of research papers in various national & international journals & conferences. He has conducted a number of seminars, workshops, conferences, summer courses in various fields of computer science & engineering. His research interests are Data Mining, Computer Networks, Parallel computing, Java based programming, Intrusion detection systems, etc.