Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey of Intrusion Detection Techniques

Karamjeet Kaur* , **Er. Navdeep Singh**

Department of Computer Engineering,
University College of Engineering,
Punjabi University, Patiala, Punjab, India

Abstract— Intrusion detection is an alternative to the situation of the security violation.Security mechanism of the network is necessary against the threat to the system. There are two types of intruders: external intruders, who are unauthorized users of the machines they attack, and internal intruders, who have permission to access the system with some restrictions. This paper describes a brief overview of various intrusion detection techniques such as fuzzy logic, neural network, pattern recognition methods, genetic algorithms and related techniques is presented. Among the several soft computing paradigms, fuzzy rule-based classifiers, decision trees, support vector machines, linear genetic programming is model fast and efficient intrusion detection systems.

Keywords- Introduction, intrusion detection methods, misuse detection techniques, anomaly detection techniques, genetic algorithms.

I. INTRODUCTION

Intrusions are the activity that violates the security policy of system. Intrusion detection is the process used to identify intrusions. Intrusion detection system is a pattern discovers and pattern recognition system. The pattern (rule) is the most important part in the intrusion detection system.

- Pattern (rule) expression.
- Patterns (rule) discover.
- Pattern matching and pattern recognition.

Intrusion detection is a process of monitoring and analysing the events occurring in a computer and/or network system in order to detect signs of security problems.

A. Intrusion detection approaches

- Define and extract the features of behaviour in system
- Define and extract the rules of intrusion.
- Apply the rules to detect the intrusion.

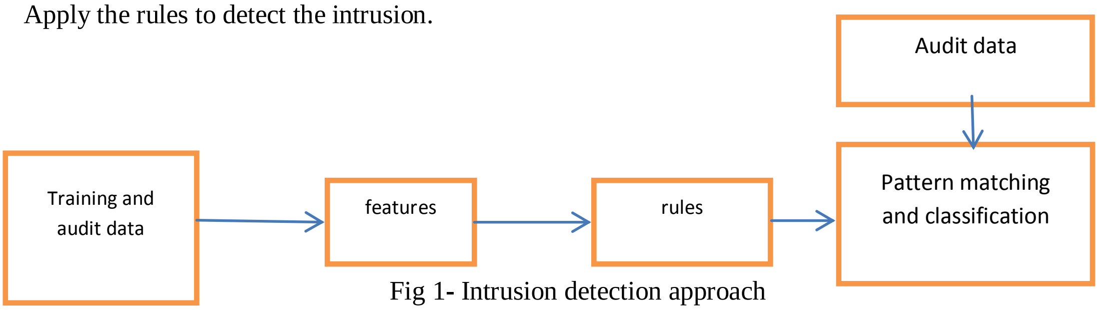


Fig 1- Intrusion detection approach

The most popular way to detect intrusions has been using the audit data generated by operating system. An audit trail is a record of activities on a system that are logged to a file in chronologically sorted order. Audit trails are particularly useful in establishing the guilt attackers. They are often the only way to detect unauthorized but subversive user activity.

B. Characteristics

- Intrusion detection monitors a whole system or just a part of it.
- Intrusion detection occurs either during an intrusion or after it.
- Intrusion detection can be stealth or openly advertised.
- If suspicious activity occurs it produces an alarm and keeps logs that can be used for reports on long term development.
- Human (administrator) needed for alarm processing.
- Intrusion detection produces an alarm and or produces an automated response.
- An intrusion detection system does not usually take preventive measure when an attack is detected.
- It is a reactive rather than a proactive agent.

II. INTRUSION DETECTION SYSTEM

A. *Host based IDs*

Get audit data from host audit trails and detect attack against a single host. It works in switched network environments. It operates in encrypted environments and detects and collects the most relevant information in the quickest possible manner. It requires the use of the resources of a host server – disk space, RAM and CPU time. It does not protect entire infrastructure

B. *Distributed IDs*

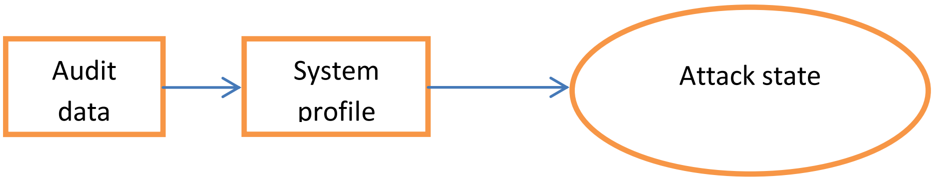
It gathers audit data from multiple hosts and possibly the network that connects the host. It detects attacks involving multiple hosts.

C. *Network based IDs*

It uses network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services. It detects attack from network.NIDS uses a passive interface to capture network packets for analyzing. NIDS sensors placed around the globe can be configured to report back to a central site, enabling a small team of security experts to support a large enterprise.NIDS systems scale well for network protection because the number of actual workstations, servers, or user systems on the network is not critical – the amount of traffic is what matters .Provide better security against DOS attacks.

III. Misuse Detection Techniques

This can detect only known attacks. The concept behind the misuse detection system is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. MDSs can detect many or all known attack patterns, but they are of little use for unknown attack methods.



Modify existing rule

Fig 2- Misuse detection

Advantages:

- Easy to implement, deploy, update and understand
- Low rate of false positives
- fast

Disadvantages:

- Cannot detect previously unknown attacks
- Constantly needs to be updated with new rules
- As good as the database of attack signatures

A. *Types of misuse detection method*

1) *Expert system*- These are modelled in such a way as to separate the rule matching phase from the action phase. For example NIDES.NIDES follows a hybrid intrusion detection technique. The expert system misused detection component encodes known scenarios and attack patterns.

2) *Model based intrusion detection* – This states that certain scenarios are inferred by certain other observable activities.The model based scheme consists of three important modules

The ***antcipator*** uses the active models and the scenario models to try to predict the next step in the scenario that is expected to occur.

The ***planner*** then translates this hypothesis into a format that shows the behavior as it would occur in the audit trail.

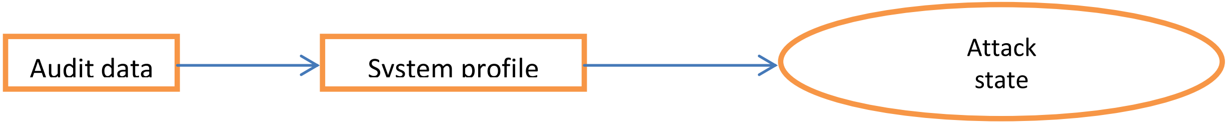
The ***interpreter*** then searches for this data in the audit trail.

3) *Pattern Matching*-This model encodes known intrusion signatures as patterns that are then matched against the audit data. The implementation makes transitions on certain events called labels, and Boolean variables called guards can be placed at each transition.Advantages:

- Multiple event streams
- Portability
- Real-time capabilities

IV. ANOMALY DETECTION TECHNIQUES

Anomaly based IDS are based on tracking unknown unique behavior pattern of detrimental activity.



Generate new rules dynamically

Fig 3- Anomaly detection

Advantages:

- May catch novel attacks we have not seen before
- Disadvantages:
- Current implementations do not work very well (too many false positives/negatives)
- Cannot categorize attacks very well
- Difficult to train in highly dynamic environments
- The system may be gradually trained by intruders

A. *Fuzzy logic*

Fuzzy logic has rapidly become one of the most successful of today's technologies for developing sophisticated control system. The reason for which is very simple. Fuzzy logic addreses such applications perfectly as it resemble human decision making with an ability to generate precise solution from certain or approximate information. Fuzzy logic is a superset of Boolean logic that has been extended to handle the concept of partial truth value between "completely true" and "completely false".

Fuzzy control, which directly uses fuzzy rules is the most important application in fuzzy theory. A fuzzy control system can also be described as based on fuzzy logic i.e. a mathematical system that analyses analog input value in terms of logical variables that take on continuous value between 0 and 1,in contrast to classical or digital logic , which operates on discrete values of either 1 or 0 (true or false respectively). Three steps to create a fuzzy controlled machines

1) *Fuzzification:* The objective of fuzzification is to define input variable as well as input membership functions for each input variable.

2) *Inference engine and knowledge base:* The inference engine categorize each input according to the membership values such as low,medium and high. The knowledge base stores the fuzy if then rules. The knowledge base consists of a brief rules defined as follow:

If((illegal firewall access=true)>M) then (unauthorized user).

3) *Defuzzification (mapping)*: This step maps the two graphs i.e. Template graph and user action graph. The template graph incudes all output membership functions and all membership functions are maximized when all output membership functions have a "high" fuzzy value. The user action graph includes various audit logs and user profiles. The defuzzification step will calculate the absolute value if matching is found between these two graphs.

Fuzzy controller are very simple conceptually. They consist of an input stage, a processing stage, and an output stage.

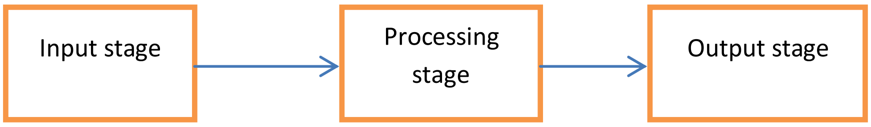


Fig 4- Fuzzy controller

The input stage maps sensors or other inputs such as switches and so on, to the appropriate membership functions and truth values. The processing stage invokes each appropriate rule and generates a result for each, then combines the results of the rules. Finally the output stage converts the combined result back into a specific control output value.

B. *Neural networks*

A neural network in the case of artificial neurons called as artificial neural network(ANN). Neural network is an interconnected group of artificial neurons that uses a mathematical model for information processing and intrusion detection. Neural networks are useful for pattern recognition or data classification through a learning process. Neural network maps a set of input nodes to a set of output nodes.

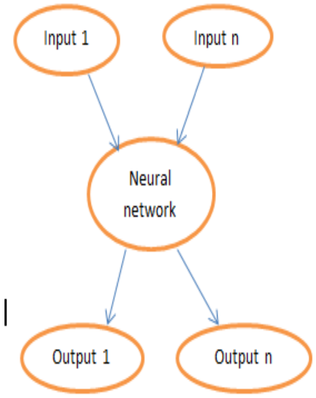


Fig 5- Neural network

Self-organising map (SOM) method used as a intrusion detection based on neural network. SOM was used to cluster and then graphically display the network data for the user to determine which clusters contained attacks.

V. Genetic Algorithm

Genetic algorithms are search procedures often used for optimization problems. Genetic algorithm is based on the principles of evolution and natural selection of chromosomes. An initial population of chromosomes is generated randomly where each chromosome represents a possible solution to the problem (an set of parameters).The evaluation function is used to calculate the “goodness” of each chromosome. In evaluation , two operators, crossover and mutation, are used to generate the new population or rules.Then ,the best individual or chromosome is selected as the final result once the optimization criteria in met. The genetic algorithm works by slowly “evolving” a population of chromosomes that represent better and better solutions to the problem.

VI. Conclusion

In this paper , several soft computing techniques are explained that compromise the confidentiality, integrity, authentication and resource availability. Soft computing consists fuzzy logic, neural networks, genetic programming or algorithms. Soft computing is very useful in intrusion detection because the techniques used in soft computing give accurate result with high speed and with good efficiency.

References

[1] Sundaram, *An introduction to intrusion detection*, 1996.

[2] K. Ilgun and A. Kemmerer, *State transition analysis: A rule-based intrusiondetection approach*, IEEE Transaction on Software Engineering 21(3): 181-99 (1995).

[3] Yao JT, Zhao SL, Saxton LV, *A study on fuzzy intrusion detection.data mining, intrusion detection, information assurance, and data networks security*, 2005.

[4] Balasubramaniyan JS, Garcia-Fernandez JO, Isaco D, Spatford E, Zamboni D, *An architecture for intrusion detection using autonomous agents*, In: Proceedings of 14th annual computer security applications conference, 1998.

[5] H. Ishibuchi, T. Nakashima, T. Murata, *A fuzzy classifier system that generates fuzzy if–then rules for pattern classification problems*, in: Proceedings of 2nd IEEE International Conference on Evolutionary Computation, Perth, Australia, 29 November–1 December 1995, IEEE, vol. 2, 1995.

[6] SanieeAbadeh, M., Habibi, J., & Lucas, C. (2007).*Intrusion detection using a fuzzy genetics-based learning algorithm. Journal of Network and Computer Applications*, 2007.

[7] Crosbie M, Spafford E. *Applying Genetic Programming to Intrusion Detection*, *Proceedings of the AAAI 1995 Fall Symposium, 1995.*

[8] Ryan, J., Lin, M., and Mikkulainen,R , “*Intrusion Detection with Neural Networks,” Advances in Neural Information Processing Systems*, vol. 10, 1998.

[9] Ypma, A., and Duin, R., “*Novelty Detection using Self-Organizing Maps,” Progress in Connectionist-Based Information Systems*, vol. 2, pp 1322-1325, 1997.