International Journal of Information Technology and Knowledge Management
January-June 2012, Volume 5, No. 1, pp. 79-83

EXISTING TRENDS IN INTRUSION DETECTION - A COMPARATIVE ANALYSIS

Manish Shrivastava[1] and Shubha Mishra[2]

ABSTRACT: One of the recent advances throughout this decade has been the evolution of various intrusion detection modes and the way they are used. Since a lot of work has already been done and there is still much more to do, we are focusing here on what we have currently in this area, particularly the techniques and a comparative study to highlight the prominent features to provide support for computer network security. This review paper is based upon the currently existing trends in the relevant context.

Keywords: Intrusions, Clustering, Anomaly-based.

1. INTRODUCTION

The need for flow of information across the world led to the emergence of intelligent networks which are capable of exchanging or transporting bulk of insensitive and sensitive information all over the world. But to efficiently manage and transfer this information, specializing techniques are adopted to make the network safe, secure and free from data tracking , misusing, corrupting and all such attempts. A rather important concern is to be able to identify it whenever there is an attempt to disclose the data integrity, confidentiality and privacy. The attempt to do so by what are regarded as unfair means by the regulatory authority is termed as intrusion technically and the measures adopt to look after such attempts is known as intrusion control mechanism.

The intrusion control system includes two important phases-intrusion detection and intrusion prevention. Intrusion detection is the effort made to identify the possibilities that could lead to an attack and focuses on the methods to reduce the frequency of those possibilities, whereas intrusion prevention targets on techniques used to protect the network from malicious activities.

This combined operation of detecting and preventing a network against any intrusion requires a tremendous, constant effort including analyzing the parameters that could lead to a successful intrusion in any network plus the ways to bring back the data authenticity.

There is a wide classification available of the various existing and recently known techniques to intrusion detection. This growth, particularly in the field of intrusion detection is the result of the realization of the fact that the detection of an attempt towards the unauthorized access of data is more vital and should receive more attention than the means adopted to remove them once such access is made. Three types of data are used by IDSs- network traffic data, system level test data and system status files. This paper is organized as follows - history and types of IDSs are covered in literature survey, techniques adopted to use detection measures is covered under mechanisms of applied technologies, a comparison among the available strategies so far is made in the next section and finally the conclusion and future enhancement in the relative field has mentioned.

2. LITERATURE REVIEW

Broadly, the first classification includes very important techniques upon which all the recent work is in progress. Among them, one is the anomaly detection (behavior based) approach based on identification of intrusion by calculating a deviation from the normal system operational behavior. They build statistical models to describe the normal behavior of the network, and flag any behavior that significantly deviates from the normal as attack.[2] Higher false alarm rates are often related with anomaly based detection systems.

The other one called signature based (knowledge based) detection identifies intrusion based on known attack characteristics or signatures. A characteristic trait of the intrusion is developed offline, and then loaded in the. Intrusion database before the system can begin to detect this particular intrusion which yields good results in terms of low false positives. The examples of signatures are-an email with a subject of “free pictures”! and an attachment filename of “freepics.exe”, which are characteristics of a known form of malware. It is the simplest detection method as it just compares the current unit of activity to a list of signatures.

[1,2] Department of Information Technology LNCT, Bhopal (MP) India, E-mail: maneesh.shreevastava@yahoo.
E-mail: com,mis.shubha@gmail.com

The next classification could be based upon the types of systems that support these approaches. Among them, one is the HIDS-Host based IDS, in which anti-threat applications like firewall, anti-virus or spyware programs are installed on every network computer that has a two-way access to the outside environment such as the internet. The other is the NIDS- Network based IDS in which the anti-threat applications are installed in the single server and not in individual systems.

One more classification is based on the centralized and distributed approaches in the IDS. In the centralized approach, various SOC (security operation centre) boxes are placed inside a centralized server which analyzes and monitors the network traffic against any attack. On the contrary, in distributed approach, there are more than one SOC boxes attached dynamically at various nodes to gather the information and to categorize the attack from it. With DSOC, on any network site, a local detection engine analyzes the data collected by one or several collection boxes to find intrusion patterns. Then all the generated alerts are processed by a global intrusion detection engine to find more complex intrusions. One more type is the one combining the best possible combination of both HIDS and NIDS techniques, known as the hybrid technique. SOC boxes gathers data from a wide range of sources (IDS, IPS, firewall, router, workstation etc). [1] This provides for global security architecture for intrusion detection systems.

One more classification can be made based on the behavior after an attack has encountered. An Active IDS is configured to automatically block the suspected attacks without any intervention by the operator. A Passive IDS is configured only to monitor and analyze network traffic activity and to alert an operator to potential vulnerabilities and attacks. It is not capable of performing any protective or correlative functions on its own.

IDS can detect attacks such as - DoS attacks fully consume resources on target computer, starve the target computer of resources or cause critical services to fail or malfunction. The other is the threat to confidentiality where same viruses attach themselves to other files and distribute. The next includes the modification of contents and masquerade where one entity pretends to be a different entity.

IDS can be modeled by keeping in view many approaches that significantly add to the domain and enhances key functionalities of the system.

3. MECHANISM AND APPLIED TECHNIQUES

The following types of alerts are generated in an IDS system

(i) True positives: These are the alerts raised for real intrusion attempts.

(ii) False positives: Alerts raised on non intrusive behaviors.

(iii) True negatives: No alerts raised and no intrusion attempts present.

(iv) False negatives: No alerts raised when real intrusion attempts present

Any of these or a combination of such alerts helps to develop a statistics about the errors or mishaps with the data.

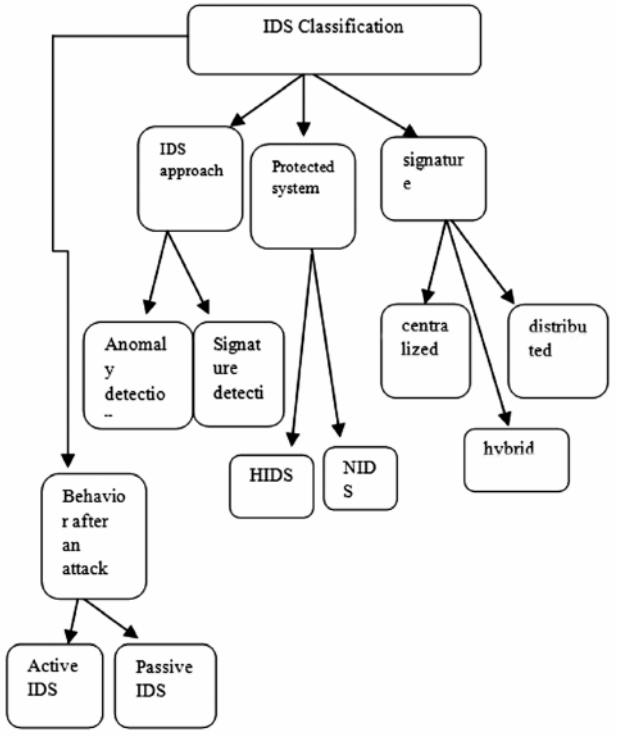

Figure 1: IDS Categorization

Current IDS have a number of significant drawbacks: current IDS are designed to detect already known service level attacks, making them vulnerable to novel and malicious attacks.

Depending upon the intrusion detection tools employed by a company and its size, there is the possibility to reach millions of records per day.

False positives: A false positive occurs when a normal attack is considered as malicious and is treated accordingly.

False negatives: This is the case where the IDS does not generate an alert when an intrusion is actually taking place [12]

The combined effort of detecting and preventing an error or an intrusive attempt can also be made using an integration of IDS and IPS techniques, collectively known as IDPS techniques. These provide for the following: Typical components-including sensor or agent, management server, database server, console etc.

Detection capabilities of IDPS includes: Threshold - a value that sets the limit between normal and abnormal behavior. They usually specify a maximum acceptable level.

Alert settings: Most IDPS technologies allow administrators to customize the alert type. Examples include specifying what information should be recorded and what notification methods (email, pager) should be used.

Code viewing and editing: some IDPS technologies permit administrators to see some or all of the detection related code. Viewing the code can help analysts to determine why particular alerts were generated, to validate alerts and identify false positives.

Prevention capabilities include variation by IDS technology type. Also, management is a crucial step in this regard that covers the aspects such as implementation, operation and maintenance. [5]

Now, talking about the techniques that have been applied so far, the following approaches or a set of combined approaches can be used to detect the system vulnerability and the amount of intrusion and ways are designed to optimize the data -

A new mobile agent based IDS can be designed using distributed sensors which comprises three major components: network intrusion detection component, the mobile agent platform, and distributed sensors residing on every device in the network segment.[3]

Another way could be to devise an intelligent detection system developed to demonstrate the effectiveness of data mining techniques and also utilizing fuzzy logic. In this regard, two methods can be easily adopted - anomaly based intrusion detection using fuzzy data mining techniques and second is the misuse or signature detection using traditional rule-based expert system techniques.[4]

Application of misuse and anomaly techniques can also be in monitoring critical process systems, such as nuclear power plants to anomaly based systems. This monitoring and control is achieved by Supervisory Control and Data Acquisition System SCADA [6]. Thus they can detect a variety of common attacks.

The next application could be to integrate data by collecting it from heterogeneous environments and to create cyberspace situational awareness. It includes the parameters like multisensory data fusion for internet based intrusion detection [7].

The currently emerged and most recently developing aspect in this concern in the centralized and distributed environment set up for IDS. Alerts are made in the distributed approach which are exchanged and correlated in a cooperative fashion. So, recent developments are focusing towards algorithms with high detection rates and low false alarm rates. The ACO (Ant Colony Optimization) system achieved high detection rate and low false alarm rate in this regard with detecting the unseen attacks.[10]

From the technological views, intrusion detection is among the information classification problems. Thus, several classifications of intrusion detection methods are as follows:

Statistic Analysis: The IDS will record the status of computer general behavior and frequency of operation, then the system infer whether the user's actions are legal or not by the statistic information.

Neural Network: Whether using supervised or unsupervised learning network, all intrusion detections can be applied to misuse or anomaly method. Neural networks for intrusion detection was first introduced as an alternative to statistical techniques [12]

Rule-based Analysis: IDS judges the user profiles through the rule base. Expression of rule base includes positive and negative expressions.

Bayesian Network: To display the probability of events and behaviors [11] it is used. The key points are distribution of probability of events and feature.

Finite State Machine: Experts can define the transfer condition of intrusion as system operations can be expressed by it.

Data Mining: The association rules of data mining are also applied in intrusion detection. IDS use features of the fields to construct association rules, such as connection time of the user [8]. It usually implies the analysis of the collected data in an offline environment, other than real-time IDS. In an offline environment, all the features can be computed and detection rules can be checked one by one by assuming that all connections have finished. On the other hand, real-time IDS focus on implementation of feature selection and detection algorithms.

Genetic Algorithms: They are categorized as global search heuristics [9]. They were actually introduced in the field of computational biology. Since then, they have been applied in various fields with promising results.

Classification Techniques: In the classification task in machine learning, the task is to take each instance of the dataset.

4. COMPARISON BASED UPON THE OBSERVATIONS

Based upon the study made above, there are certain features to be highlighted that construct a base for distinction among various techniques discussed so far. Let's have a quick glance over the following study:

Table 1
Comparisons of Various IDS Techniques

IDS TYPE NAME	ADVANTAGE	LIMITATIONS	APPLICATIONS
Active IDS	Provides real time corrective action in response to attacks	As it must be placed inside a network boundary, it itself is susceptible to attack If false alarms and legitimate traffic have not been identified and filtered, authorized users will be denied access	It may be used to affect a DoS attack by intentionally flooding the system with alarms that cause it to block connections until no connection are available
PASSIVE IDS	These can be easily and rapidly Not susceptible to attack themselves	Not capable of performing any corrective function on its own	Used in situations where a response mode is preferred instead of reactive mode
NIDS	Individual node analysis takes much time	Use in signal processing	
IDS	Can focus on individual hosts more efficiently	It cant monitor entire network at a time	Analyzing system calls, Application logs, file system manipulation
Knowledge based/ signature based	Alarms are more standardized and easily understood Lower false alarm rates than behavior based IDS	New, unique, original attacks may not be wrongly classified	Currently more common and in much use
Behavior based or anomaly based	Dynamically adapt to new, original Less dependent on identifying operating system Vulnerabilities	Higher false alarm rates than knowledge based Usage patterns that may change easily	High security area with no external traffic
Centralized approach	Single control point for network, so not much updates are required	Single point of failure Communication link breaking in a multi-site network	Traditional approach used in many networks
Distributed approach	Scalable Support wide networks Highly available	Lack of coordination of local and global analyzer resulting in trouble	In distributed environments like adhoc networks and mobile networks

Fuzzy logic: It is derived from fuzzy set theory dealing with reasoning that is approximately rather than precisely deduced from classical predicate logic.

SVM-SVM are a set of related supervised learning methods used for classification and regression. SVMs attempts to separate data into multiple classes.

Clustering and Outlier Detection: These work by grouping the observed data into clusters. A representative point is selected for each cluster, and then each new data point is classified as belonging to the given cluster.

5. CONCLUSION AND FUTURE ENHANCEMENT

Clearly, there is an urgent need to take essential measures to prevent the data from getting exploited by applying any or a set of techniques with a clear view to seize or limit the attack or intrusion attempts. The need of the hour is that we should also achieve a high level of data security in all sorts of networks, among which there is still a huge group of static networks along with growing dynamic networks. A suggested attempt in this regard is to use a hybrid IDS that involve the essential combination of IDS as well as IPS, providing a complete intrusion resistant package for a network. This can be achieved through optimizing the current results gained by applying either clustering or classification on the datasets extracted from a static or distributed network node. In the future, one should look forward to achieve intrusion detection in static networks by applying effective measures and thus optimizing the current performance of the algorithms to a more satisfactory level.

REFERENCES

[1] Abdoul Karim Ganame, Julien Bourgeois, Renaud Bidou, Francois Spies Global Security Architecture for Intrusion Detection on Computer Networks", Computers and Security 27, pp 30-47, 2008.

[2] Kingsley Leung, Christopher Leckie, "Unsupervised Anomaly Detection in Network Intrusion Detection Using Clusters" 28th Australasian Computer Science Conference , 38, January 2005.

[3] Damiano Bolzoni, Emmanuele Zambon, Sandro Etalle, Pieter Hartel, "2 Tier Anomaly-Based Intrusion Detection System" Computer Security Threat Monitoring and Surveillance, April 1980.

[4] S. Janakiraman, V. Vasudevan, "ACO Based Distributed Intrusion Detection System", International Journal of Digital Content Technology and its Applications, 3. March 2009.

[5] Tim Bass, "Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems", IRIS National Symposium Draft, April 1999.

[6] Dayu Yang, Alexander Usynin, J.Wesley Hines "Anomaly-Based Intrusion Detection for SCADA Systems", IEEE Transactions on Software Engineering, SE-13, pp 222-232, February 1987.

[7] Jeyanthi Hall, Michael Barbeau, Evangelos Kranakis, "Using Mobility Profiles for Anomaly-Based Intrusion Detection in Mobile Networks" Twentieth National Information Systems Security Conference, pp 353-365, 1997.

[8] Susan M. Bridges, Rayford B. Vaughn "Intrusion Detection Via Fuzzy Data Mining", 12th Annual Canadian Information Technology Security Symposium, June 2000.

[9] Mohamad Eid, "A New Mobile-Agent Based Intrusion Detection System Using Distributed Sensors, American University of Beirut", In Proceedings of IEEE Symposium on Security and Privacy, pp118-131, April 1986.

[10] P.Garcia-Teodoro, J. Diaz-Verdejo, G. Macia- Fernandez, E. Vazquez, "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges", Computers and Security, 28, pp. 18-28, 2009.

[11] Rung Ching Chen, Chen Chia Hsieh, "An Anomaly Intrusion Detection on Database Operation by Fuzzy ART Neural Network", Computers and Security, Vol. 22, pp 506-512, 2000.

[12] Theodoros Lappas and Konstantinos Pelechrinis, "Data Mining Techniques for (Network) Intrusion Detection Systems", Computer Networks: The International Journal of Computers and Telecommunications Networking, 44(5), pp 643-66, 2004.