A Survey on Anomaly-Based Network Intrusion Detection Systems

Neeraj Shukla, Anjali Vishwakarma,
Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

ABSTRACT

The significance of system security has become enormously and various gadgets have been acquainted with enhance the security of a system. System Intrusion Detection Systems (NIDS) are among the most broadly sent such framework. Prevalent NIDS utilize an accumulation of marks of known security dangers and infections, which are utilized to sweep every parcel's payload. Most IDSs do not have the capacity to identify novel or beforehand obscure assaults. An uncommon sort of IDSs, called Anomaly Detection Systems, create models taking into account typical framework or system conduct, with the objective of recognizing both known and obscure assaults. Oddity location frameworks face numerous issues including high rate of false alert, capacity to work in online mode, and versatility. This paper shows a specific study of incremental methodologies for recognizing abnormality in ordinary framework and system activity.
Keywords : Computer networks, Network security, Anomaly detection, Intrusion detection

I. INTRODUCTION

The field of intrusion detection has received increasing attention in recent years. One reason for this is the explosive growth of the Internet and the large number of networked systems that exist in all types of organizations. The increase in the number of networked machines has lead to an increase in unauthorized activity, not only from external attackers, but also from internal attackers, such as disgruntled employee and people abusing their privileges for personal gain.

Security is a big issue for all networks in today's enterprise environment. Hackers and intruders have made many successful attempts to bring down high-profile company networks and web services. Many methods have been developed to secure the network infrastructure and communication over the Internet, among them the use of firewalls, encryption, and virtual private networks. Intrusion detection is a relatively new addition to such techniques. Intrusion detection methods started appearing in the last few years. Using intrusion detection methods, you can collect and use information from known types of attacks and find out if someone is trying to attack your network or particular hosts. The information collected this way can be used to harden your network security, as well as for legal purposes. Both commercial and open source products are now available for this purpose. Many vulnerability assessment tools are also available in the market that can be used to assess different types of security holes present in your network.

II. METHODS AND MATERIAL

A. Classification of Intrusion Detection System

All the classification of intrusion detection system is described below as shown in Figure 1.

Statistical Models

1) Operational Model/ Threshold Metric

The count of events that occur over a period of time determines the alarm to be raised if fewer then "m" or more than "n" events occur. This can be visualized in Win2k lock, where a user after "n" unsuccessful login attempts here lower limit is "0" and upper limit is "n". Executable files size downloaded is restricted in some

organizations about 4 MB. The difficulty in this sub-model is determining m and n (Faizal *et al*., 2009).

2) Markov Process or Marker Model

The Intrusion detection in this model is done by investigating the system at fixed intervals and keeping track of its state a probability for each state at a given time interval *Is*. The change of the state of the system occurs when an event happens and the behavior is detected as anomaly if the probability of occurrence of that state is low. The transitions between certain commands determine the anomaly detection where command sequences were important.

3) Statistical Moments or Mean and Standard

Deviation Model: In statistical mean, standard deviation, or any other correlations are known as a moment. If the event that falls outside the set interval above or below the moment is said to be anomalous. The system is subjected to change by considering the aging data and making changes to the statistical rule data base. There are two major advantages over an operational model. First, prior knowledge is not required determining the normal activity in order to set limits; Second, determining the confidence intervals depends on observed user data, as it varies from user to user. Threshold model [2] lacks this flexibility. The major variation on the mean and standard deviation model is to give higher weights for the recent activities.
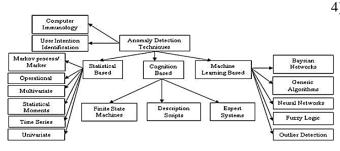

Figure 1: Classification of Intrusion Detection System

Multivariate Model: The major difference between the mean and standard deviation model is based on correlations among two or more metrics. If experimental data reveals better judicious power can be achieved from combinations of related measures rather than treating them individually.

1) Time Series Model

Interval timers together with an event counter or resource measure are major components in this model. Order and inter-arrival times of the observations as well as their values are stored. If the probability of occurrence of a new observation is too low then it is considered as anomaly. The disadvantage of this model is that it is more computationally expensive.

Cognition Models

Finite State Machine: A Finite State Machine (FSM) or finite automation is a model of behavior captured in states, transitions and actions. A state contains information about the past, i.e., any changes in the input are noted and based on its transition happens. An action is a description of an activity that is to be performed at a given moment. There are several action types: entry action, exit action, and transition action.

2) Description Scripts

Numerous proposals for scripting languages, which can describe signatures of attacks on computers and networks, are given by the Intrusion Detection community. All of these scripting languages are capable of identifying the sequences of specific events that are indicative of attacks.

3) Adept Systems

Human expertise in problem solving is used in adept systems. It solves uncertainties where generally one or more human experts are consulted. These systems are efficient in certain problem domain, and also considered as a class of Artificial Intelligence (AI) problems. Adept Systems are trained based on extensive knowledge of patterns associated with known attacks provided by human experts.

Cognition Based Detection Techniques Cognition - Based (also called knowledge-based or expert systems) Detection Techniques work on the audit data classification technique, influenced by set of predefined rules, classes and attributes identified from training data, set of classification rules, parameters and procedures inferred.

4) Boosted Decision Tree

Boosted Tree (BT), that uses ADA Boost algorithm to generate many Decision Trees classifiers trained by different sample sets drawn from the original training set,

is implemented in many IDS successfully. All hypotheses, produced from each of these classifiers, are combined to calculate total learning error, thereby arriving at a final composite hypothesis.

5) Support Vector Machine

Support Vector Machines (SVM), reliable on a range of classification tasks, are less prone to over-fitting problem, and are effective with unseen data. The basic learning process of the SVM includes two phases: (1) Mapping the training data from the original input space into a higher dimensional feature space, using kernels to transform a linearly non separable problem into a linearly separable one, (2) Finalizing a hyper plane within the feature space, with a maximum margin using Sequential Minimal Optimization (SMO) or Osuna's method.

6) Artificial Neural Network

Artificial Neural Network (ANN) architectures [1] (popular one being , Multilayer Perceptron (MLP), a layered feed-forward topology in which each unit performs a biased weighted sum of their inputs and pass this activation level through a transfer function to produce their output), are able to identify not readily observable patterns, however MLP is ineffective with new data. For general signal processing and pattern recognition problems, another branch of ANN that makes use of radial basis function, called The Modified Probabilistic Neural Network [3] (related to General Regression Neural Network (GRNN) classifier and generalization of Probabilistic Neural Network (PNN)), was introduced by Zaknich. It assigns the clusters of input vectors rather than each individual training case to radial units.

7) Machine Learning Based Detection Techniques

Machine learning techniques Reuters News Service (2005) to detect outliers in datasets from a variety of fields were developed by Gardener (use a One-Class Support Vector Machine (OCSVM) to detect anomalies in EEG data from epilepsy patients) and Barbara (proposed an algorithm to detect outliers in noisy datasets where no information is available regarding ground truth, based on a Transductive Confidence Machine (TCM)) [4]. Unlike induction that uses all data points to induce a model, transduction, an alternative, uses small subset of them to estimate unknown attributes of test points. To perform online anomaly detection on time series data in, Ma and Perkins presented an algorithm using

support vector regression. Ihler *et al.* present an adaptive anomaly detection algorithm that is based on a Markov-modulated Poisson process model, and use Markov Chain Monte Carlo methods in a Bayesian approach to learn the model parameters [5].

B. Common Attacks and Vulnerabilities and Role of NIDS

Current NIDSs requires substantial amount of human intervention and administrators for an effective operation. Therefore it becomes important for the network administrators to understand the architecture of NIDS, and the well-known attacks and the mechanisms used to detect them and contain the damages. In this section, we discuss some well-known attacks, exploits, and vulnerabilities in the end host operating systems, and protocols.

Attack Types

Confidentiality: In such kinds of attacks, the attacker gains access to confidential and otherwise inaccessible data.

Integrity: In such kinds of attacks, the attacker can modify the system state and alter the data without proper authorization from the owner.

Availability: In such kinds of attacks, the system is either shut down by the attacker or made unavailable to general users. Denial of Service attacks fall into this category.

Control : In such attacks the attacker gains full control of the system and can alter the access privileges of the system thereby potentially triggering all of the above three attacks.

Attacks Detected by a NIDS

A number of attacks can be detected by current generation of NIDS. Some of these are listed and described below.

Scanning Attack

In such attacks, an attacker sends various kinds of packets to probe a system or network for vulnerability that can be exploited. When probe packets are sent the

target system responds; the responses are analyzed to determine the characteristics of the target system and if there are vulnerabilities. Thus scanning attack [1] essentially identifies a potential victim. Network scanners, port scanners, vulnerability scanners, etc., are used which yields these information. Once the victim is identified, the attacker can penetrate them in a specific way. Scanning is typically considered a legal activity and there are a number of examples and applications that employ scanning. The most well-known scanning applications are Web search engines. On the other hand independent individual ay scan a network or the entire Internet looking for certain information, such as a music or video file. Some well-known malicious scanning include Vertical and Horizontal port scanning, ICMP (ping) scanning, very slow scan, scanning from multiple ports and scanning of multiple IP addresses and ports. NIDS signatures can be devised to identify such malicious scanning activity from a legitimate scanning activity with fairly high degree of accuracy.

Denial of Service (DoS) Attacks

A Denial of Service attack attempts to slow down or completely shut down a target so as to disrupt the service and deny the legitimate and authorized users can access. Such attacks are very common in the Internet where a collection of hosts are often used to bombard web servers with dummy requests. Such attacks can cause significant economic damage to e-commerce businesses by denying the customers an access to the business. There are a number of different kinds of DoS attacks [6], some of which are mentioned below.

Flaw Exploitation DoS Attacks

In such attacks, an attacker exploits a flaw in the server software to either slow it down or exhaust it of certain resources. Ping of death attack is one such well known attack. A ping of Death (POD) [7] is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size (or 84 bytes when IP header is considered); many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size can crash the target computer. Some limitations of the protocol implementation also lead to vulnerability which can be exploited to implement DoS attacks Jelena Mirkovic et

al., (2005) such as DNS amplification attack which uses ICMP echo messages to bombard a target. For these attacks, a signature can be devised easily, such as to determine a ping of death attack a NIDS needs to check the ping flag and packet size.

Flooding DoS Attacks

In a flooding attack, an attacker simply sends more requests to a target that it can handle. Such attacks can either exhaust the processing capability of the target or exhaust the network bandwidth of the target, either way leading to a denial of service to other users. DoS attacks are extremely difficult to combat, as these do not exploit any vulnerability in the system, and even an otherwise secure system can be targeted. A more dangerous version of DoS attack (Reuters News Service (2005), is called Distributed Denial of Service attack (DDoS), which uses a large pool of hosts to target a given victim host. A hacker (called botmaster) can initiate a DDoS attack by exploiting vulnerability in some computer system, thereby taking control of it and making this the DDoS master. Afterwards the intruder uses this master to communicate with the other systems (called bots) that can be compromised. Once a significant number of hosts are compromised, with a single command, the intruder can instruct them to launch a variety of flood attacks against a specified target.

Penetration Attacks

In penetration attack [8], an attacker gains an unauthorized control of a system, and can modify/alter system state, read files, etc. Generally such attacks exploit certain flaws in the software, which enables the attacker to install viruses, and malware in the system. The most common types of penetration attacks are:
User to Root: A local user gets the full access to every component of the system.
Remote to User: A user across the network gains a user account and the associated controls.
Remote to Root: A user across the network gains the complete control of the system.

Remote Disk Read: An attacker on the network gains access to the inaccessible files stored locally on the host.
Remote Disk Write: An attacker on the network not only gains access to the inaccessible files stored locally on the host, but can also alter them.

SSH Attack

SSH attacks are a main area of concern for network managers, due to the danger associated with a successful compromise. The fact that the number of people using and relying on the Internet is increasing rapidly makes breaking into and compromising systems an ever more lucrative activity for hackers. One popular class of attack targets is that of Secure Shell (SSH) daemons. By means of SSH (Alex Lam 2005), a hacker can gain access to and potentially full control over remote hosts. Once compromised, a hacker can sabotage not only the host it, but also use it for attacking other systems. The detection of intrusions, especially in the case of SSH, is therefore crucial for preventing damage to hosts and networks.

III. RESULTS AND DISCUSSION

Intrusion Detection Systems

Intrusion Detection System (IDS) is software that automates the intrusion detection process and detects possible intrusions. IDS serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. An IDS is composed of several components:

Sensors [9] which generate security events; Console to monitor events and alerts and control the sensors Central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received.

In many simple IDS implementations [10] these three components are combined in a single device or appliance. More specifically, IDS tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection.

IDSs use policies to define certain events that, if detected will issue an alert. In other words, if a particular event is considered to constitute a security incident, an alert will be issued if that event is detected. Certain IDSs have the capability of sending out alerts, so that the administrator of the IDS will receive a notification of a possible security incident in the form of a page, e-mail, or SNMP trap [12]. Many IDSs not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event. Such a response might include logging off a user, disabling a user account, and launching of scripts. IDSs are an integral and necessary element of a complete information security infrastructure performing as "the logical complement to network firewalls". Simply put, IDS tools allow for complete supervision of networks, regardless of the action being taken, such that information will always exist to determine the nature of the security incident and its source. Ideally the team's network is separated from the outside world by a well-designed firewall. The outside world includes the team's host organization. Firewalls protect a network and attempt to prevent intrusions, while IDS tools detect whether or not the network is under attack or has, in fact, been breached. IDS tools thus form an integral part of a thorough and complete security system. They don't fully guarantee security, but when used with security policy, vulnerability assessments, data encryption, user authentication, access control, and firewalls, they can greatly enhance network safety. IDS can also be used to monitor network traffic [11], thereby detecting if a system is being targeted by a network attack [12] such as a DoS attack. IDSs remain the only proactive means of detecting and responding to threats that stem from both inside and outside a corporate network.

Intrusion detection tools use several techniques to help them determine what qualifies as an intrusion versus normal traffic[13]. Whether a system uses anomaly detection, misuse detection, target monitoring, or stealth probes, they generally fall into one of two categories:

- Host-based IDSs (HIDS) – examine data held on individual computers that serve as hosts. The network architecture of host-based (Reuters News Service, 2005) is agent-based, which means that a software agent resides on each of the hosts that will be governed by the system.

- Network-based IDSs (NIDS) – examine data exchanged between computers (Reuters News Service, 2005). More efficient host- based intrusion detection systems are capable of monitoring and collecting system audit trails in real time as well as on a scheduled basis, thus distributing both CPU utilization and network overhead and providing for a flexible means of security administration.

IDSs can also be categorized according to the detection approaches they use [14]. Basically, there are two detection methods: misuse detection and anomaly detection. The major deference between the two methods is that misuse detection identifies intrusions based on features of known attacks while anomaly detection analyzes the properties of normal behavior. IDSs that employ both detection methods are called hybrid detection-based IDSs. Examples of hybrid detection-based IDSs are Hybrid NIDS using Random Forests and NIDES [11]. The following subsections explain the two detection approaches.

Misuse Detection

Misuse detection catches intrusion in terms of the characteristics of known attacks. Any action that conforms to the pattern of a known attack or vulnerability is considered as intrusive. The main issues in misuse detection system are how to write a signature that encompasses all possible variations of the pertinent attack. And how to write signatures that do not also match non-intrusive activity. Block diagram Figure 2a of misuse based detection system is as following. Misuse detection identifies intrusions by matching monitored events to patterns or signatures of attacks. The attack signatures are the characteristics associated with successful known attacks the major advantage of misuse detection is that the method possesses high accuracy in detecting known attacks. However, its detection ability is limited by the signature database. Unless new attacks are transformed into signatures and added to the database, misuse-based IDS cannot detect any attack of this type. Deferent techniques such as expert systems, signature analysis, and state transition analysis are utilized in misuse detection.
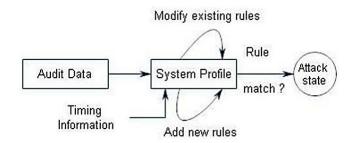

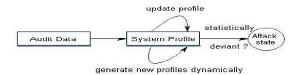
Figure 2a: Misuse Detection System

Figure 2b: Anomaly Detection System

Anomaly Detection System

It is based on the normal behavior of a subject (e.g., a user or a system). Any action that significantly deviates from the normal behavior is considered as intrusive. That means if we could establish a normal activity profile for a system, then we can flag all system states varying from established profile. There is a important difference between anomaly based and misuse based technique that the anomaly based try to detect the compliment of bad behavior and misuse based detection system try to recognize the known bad behavior. In this case we have two possibilities: (1) false positive: Anomalous activities that are not intrusive but are flagged as intrusive. (2) False Negative: Anomalous activities that are intrusive but are flagged as non-intrusive. The block diagram Figure 2b of anomaly detection system is as following:

Anomaly detection assumes that intrusions are anomalies that necessarily differ from normal behavior. Basically, anomaly detection establishes a profile for normal operation and marks the activities that deviate significantly from the profile as attacks. The main advantage of anomaly detection is that it can detect unknown attacks [12]. However, this advantage is paid for in terms of a high false positive rate because, in practice, anomalies are not necessarily intrusive. Moreover, anomaly detection cannot detect the attacks that do not obviously deviate from normal activities. As the number of new attacks increases rapidly, it is hard for a misuse detection approach to maintain a high detection rate. In addition, modeling attacks is a highly qualified and time- consuming job that leads to a heavy workload of maintaining the signature database. On the other hand, anomaly detection methods that discover the intrusions through heuristic learning are relatively easy to maintain.

When there is an intruder who has no idea of the legitimate user's activity patterns, the probability that the intruder's activity is detected as anomalous

should be high. Four possibilities in such a situation, each with a non-zero probability.

- Intrusive but not anomalous: An IDS may fail to detect this type of activity since the activity is not anomalous. But, if the IDS detect such an activity, it may report it as a false negative because it falsely reports the absence of an intrusion when there is one.
- Not intrusive but anomalous: If the activity is not intrusive, but it is anomalous, IDS may report it as intrusive. These are called false positives because an intrusion detection system falsely reports intrusions.
- Not intrusive and not anomalous: These are true negatives; the activity is not intrusive and should not be reported as intrusive.
- Intrusive and anomalous: These are true positives; the activity is intrusive and much is reported as such.

IV. CONCLUSION

In this paper, we review IDS tools are becoming increasingly necessary. They round out the security arsenal, working in conjunction with other information security tools, such as firewalls, and allow for the complete supervision of all network activity. It is very likely that IDS capabilities will become core capabilities of network infrastructure (such as routers, bridges and switches) and operating systems. In future we would like to find out how data mining can help improve intrusion detection and most of all anomaly detection. For that purpose we have to understand how an IDS work to identify an intrusion. By identifying bounds for valid network activity, data mining will aid an analyst to distinguish attack activity from common everyday traffic on the network. This will require, I believe, combination of multiple complicated methods to cover all of the difficulties will make it even more time consuming.

V. REFERENCES

[1] Alex Lam (2014), "New IPS to Boost Security, Reliability and Performance of the Campus Network", Newsletter of Computing Services Center.

[2] Pfahringer B (2013), "Winning the KDD99 Classification Cup: Bagged Boosting", In SIGKDD Explorations.

[3] Barbara D, Domeniconi C and Rogers J (2014), "Detecting Outliers Using Transduction And Statistical Testing", Association for Computing Machinery.

[4] Dasgupta D(2011),"AnArtificialImmune System AsAMultiagent Decision Support System", IEEE International Conferenceon Systems, Manand Cybernetics, pp. 3816-3820.

[5] Reuters News Service (2005), FBI Agents bust 'Botmaster', November 4.

[6] Jelena Mirkovic, Sven Dietrich, David Dittrich and Peter Reiher (2005), Internet Denial of Service: Attack and Defense Mechanisms, Prentice Hall PTR, ISBN 0131475738.

[7] Ma J and Perkins S (2003), "Online Novelty Detection on Temporal Sequences", ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), Washington, DC.

[8] Levin (2000), "KDD-99 Classifier Learning Contest: LLSoft's Results Overview", SIGKDD Explorations.

[9] LI Yongzhong, YANG Ge and XU Jing Zhao Bo (2008,) "A New Intrusion Detection Method Based on Fuzzy HMM", IEEE, Vol. 2, No. 8.

[10] Ihler A, Hutchins J and Smyth P (2006), "Adaptive Event Detection with Time-varying Poisson Processes", ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining (KDD), Philadelphia, PA.

[11] Sharma S K, Pandey P and Tiwar S K (2012), "An Improved Network Intrusion Detection Technique Based On k-means Clustering Via Naïve Bayes Classification", IEEE, Vol. 2, No. 2.

[12] Tarem Ahmed, Boris Oreshkin and Mark Coates (2007), "Machine Learning Approaches to Network Anomaly Detection", in Workshop on Tackling Computer Systems Problems with Machine Learning Techniques, McGill University Montreal, QC, Canada.

[13] Vaughn Randal and Evron Gadi (2007), "DNS Amplification Attacks".

[14] Zhenglie Li (2011) "Anomaly Intrusion Detection Method Based on K-Means Clustering Algorithm with Particle Swarm Optimization", Springer, Vol. 4, No. 2.