A Survey of Cyber Attack Detection Systems

Shailendra Singh and Sanjay Silakari,

Rajiv Gandhi Technological University, Bhopal INDIA

Summary

In the recent years, number of attacks on networks has exponentially increased therefore; interest in cyber attack detection has increased among the researchers. The tremendous opportunities for information and resource sharing that this entails comes a heightened need for information security, as computing resources are both more vulnerable and more heavily depended upon them before. This paper provides a review on current trends in cyber attack detection together with a study on technologies implemented by some researchers in this area. This will help to predict, pointing towards a number of areas of future research in the field of cyber attack detection and response.

Key words:

*Cyber attack detection, networks, information security***.**

1. Introduction

The information security research that has been the subject of much attention in recent years is that of cyber attack detection systems. As the cost of information processing and internet accessibility falls, organizations are becoming increasingly vulnerable to potential cyber threats such as network cyber attacks. So, there exists a need to provide secure and safe transactions through the use of firewalls, Cyber Attack Detection Systems (CADSs), encryption, authentication, and other hardware and software solutions. Many CADS variants exist which allow security managers and engineers to identify attack network packets primarily through the use of signature detection; i.e., the CADS recognizes attack packets due to their well-known fingerprints or signatures as those packets cross the network's gateway threshold. On the other hand, anomaly based ID systems determine what is normal traffic within a network and reports abnormal traffic behavior. CADS are made so they can reliably detect Probe, DoS, U2R, R2L and data attacks with low false alarm rates. However, for most systems, complete attack prevention is not realistically attainable due to system complexity, Configuration and administration errors and abuse by authorized users. For this reason, attack detection has been an important aspect of recent computer security efforts [1] The aim of this paper is to review the current trends in Cyber attack detection system and to analyze some current problems that exist in this research area. In comparison to some mature and well settled research areas, CADS is a young field of research. However, due to its mission critical nature, it has attracted significant attention towards itself. Density of research on this subject is constantly rising and everyday more researchers are engaged in this field of work. The threat of a new wave of cyber or network attacks is not just a probability that should be considered, but it is an accepted fact that can occur at any time. The current trend for the CADS is far from Reliable protective system, but instead the main idea is to make it possible to detect novel network attacks. One of the major concerns is to make sure that in case of an attack attempt, the system is able to detect and to report it. However, no part of the CADS is currently at a fully reliable level, even though researchers are concurrently engaged in working on efficient approach for detection. A major problem in the CADS is the guarantee for the cyber attack detection. This is the reason why in many cases CADSs are used together with a human expert. In this way, CADS is actually helping the network security officer and it is not reliable enough to be trusted on its own. The reason is the inability of CAD systems to detect the new or altered attack patterns. Although the latest generation of the detection techniques has significantly improved the detection rate, still there is a long way to go

2. Cyber Attacks

Cyber attacks are actions that attempt to bypass security mechanisms of computer systems. So they are any set of actions that threatens the integrity, availability, and confidentiality of a network resource. These properties have the following explanations:

- **Confidentiality** – means that information is not made available or disclosed to unauthorized individuals, entities or processes;

Manuscript received May 5, 2009
Manuscript revised May 20, 2009

- **Integrity** – means that data has not been altered or destroyed in an unauthorized manner;
- **Availability** – means that a system or a system resource that ensures that it is accessible and usable upon demand by an authorized system user. Availability is one of the core characteristics of a secure system.

In the 1998 DARPA cyber attack detection evaluation [2] program, an environment was setup to acquire raw TCP/IP dump data for a network by simulating a typical U.S. Air Force LAN. The LAN was operated like a true environment, but being blasted with multiple attacks. For each TCP/IP connection, 41 various quantitative (continuous data type) and qualitative (discrete data type) features were extracted among the 41 features, 34 features are numeric and 7 features are symbolic. The data contains 24 attack types that could be classified into four main categories:

1.1 Denial of Service Attacks (DOS)

Denial of service (DOS) is class of attack where an attacker makes a computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate user access to a machine. At least that way, when the main entrance is blocked, you can use the emergency exit to maintain at least minimal communications such as email. There are many varieties of DoS attacks. Some DoS attacks (like a mailbomb, neptune, or smurf attack) abuse a perfectly legitimate feature. Others (teardrop, Ping of Death) create malformed packets that confuse the TCP/IP stack of the machine that is trying to reconstruct the packet (apache2, back, syslogd)

1.2 Remote to Local (User) Attacks (R2L)

A remote to local (R2L) attack is a class of attacks where an attacker sends packets to a machine over network, then exploits the machine’s vulnerability to illegally gain local access to a machine. It occurs when an attacker who has the ability to send packets to a machine over a network but who does not have an account on that machine exploits some vulnerability to gain local access as a user of that machine. There are many possible ways an attacker can gain unauthorized access to a local account on a machine. The Dictionary, Ftp-Write, Guest and Xsnoop attacks all attempt to exploit weak or misconfigured system security policies. The Xlock attack involves social engineering in order for the attack to be successful the attacker must successfully spoof a human operator into supplying their password to a screensaver that is actually a Trojan horse.

1.3 User to Root Attacks (U2R)

User to root (U2R) attacks is a class of attacks where an attacker starts with access to a normal user account on the system and is able to exploit vulnerability to gain root access to the system in which the attacker starts out with access to a normal user account on the system (perhaps gained by sniffing passwords, a dictionary attack, or social engineering) and is able to exploit some vulnerability to gain root access to the system. There are several different types of U2R attacks where the most common is the buffer overflow attack. Buffer overflows occur when a program copies too much data into a static buffer without checking to make sure that the data will fit.

1.4 Probing

Probing is class of attacks where an attacker scans a network to gather information or find known vulnerabilities. An attacker with map of machine and services that are available on a network can use the information to notice for exploit. The purpose of port scanning is to determine what ports are open, and hence what services that may be running on a system are available to the attacker. This result is utilized for good by network and system administrators as a part of network security audits, and for evil by attackers who wish to compromise a box by using an exploit for one of the discovered running services on its open port. Port scanning's additional applications can also tell us what hosts are up on a network and various other network topological details, such as IP addressing, MAC addressing, router and gateway filtering, firewall rules, IP-based trust relationships, etc. Worms and viruses: they are replicating on other hosts. Compromises: they obtain privileged access to a host by known vulnerability [3].

3. Cyber Attack Detection

Cyber attack detection has been defined as “the problem of identifying individuals who are using a computer system without authorization (crackers) and those who have legitimate access to the system but are abusing their privileges (insider threat)” [4]. We add to this definition the identification of attempts to use a computer system without authorization or to abuse existing privileges. Therefore, our working definition of cyber attack matches the one given by Heady et al [5]. All modern cyber attack detection systems monitor either host computers or network links to capture cyber attack data.

3.1 Host Intrusion Detection Systems (HIDS)

Host intrusion detection refers to the class of intrusion detection systems that reside on and monitor an individual host machine. There are a number of system characteristics that a host intrusion detection system (HIDS) can make use of in collecting data including:

File System - changes to a host's file system can be indicative of the activities that are conducted on that host.

Network Events - An intrusion detection system can intercept all network communications after they have been processed by the network stack before they are passed on to user-level processes.

System Calls - with some modification of the host's kernel, an intrusion detection system can be positioned in such a way as to observe all of the system calls that are made. This can provide the intrusion detection system with very rich data indicating the behavior of a program.

A critical decision in any HIDS is therefore choosing the appropriate system characteristics to monitor. This decision involves a number of tradeoffs including the content of the data that is monitored, the volume of data that is captured, and the extent to which the intrusion detection system may modify the operating system of the host machine

3.2 Network Intrusion Detection Systems (NIDS)

A network cyber attack detection system (NCADS) monitors the packets that traverse a given network link. Such a system operates by placing the network interface into promiscuous mode, affording it the advantage of being able to monitor an entire network while not divulging its existence to potential attackers. Because the packets that a NCADS is monitoring are not actually addressed to the host the NCADS resides on, the system is also impervious to an entire class of attacks such as the “ping-of-death” attack that can disable a host without ever triggering a HCADS. A NCADS is obviously of little value in detecting attacks that are launched on a host through an interface other than the network. Network data has a variety of characteristics that are available for a NCADS to monitor: most operate by examining the IP and transport layer headers of individual packets, the content of these packets, or some combination thereof. Regardless of which characteristics a system chooses to monitor, however, the positioning of a NCADS fundamentally presents a number of challenges to its correct operation.

4. Analysis Approach

Currently there are three basic approaches to cyber attack detection. The CADS uses its analysis engine to process this data in order to identify cyber attacks. Modern systems primarily employ three approaches to perform this analysis: misuse, anomaly [6] and specification [7].

4.1 Misuse Detection

Misuse (signature) detection is based on the knowledge of system vulnerabilities and known attack patterns. Systems generally contain design and implementation flaws that result system vulnerability. Misuse detection is concerned with finding intruders who are attempting to break into a system by exploiting some known vulnerability. Ideally, a system security administrator should be aware of all the known vulnerabilities and eliminate them. The term cyber attack scenario is used as a description of a known kind of cyber attack. It is a sequence of events that would result in a cyber attack without some outside preventive intervention. A cyber attack detection system continually compares recent activity to known cyber attack scenarios to ensure that one or more attackers are not attempting to exploit known vulnerabilities. A less fortunate ramification of this architecture results from the fact that a misuse detection system is incapable of detecting cyber attacks that are not represented in its knowledge base. Subtle variations of known attacks may also evade analysis if a misuse system is not properly constructed. Therefore, the efficacy of the system relies heavily on the thorough and correct construction of this knowledge base, a task that traditionally requires human domain experts

4.2 Anomaly Detection

It assumes that a cyber attack will always reflect some deviations from normal patterns. Anomaly detection may be divided into static and dynamic anomaly detection. A static anomaly detector is based on the assumption that there is a portion of the system being monitored that does not change. Usually, static detectors only address the software portion of a system and are based on the assumption that the hardware need not be checked. The static portion of a system is the code for the system and the constant portion of data upon which the correct functioning of the system depends. For example, the operating systems, software and data to bootstrap a computer never change. If the static portion of the system ever deviates from its original form, an error has occurred or an intruder has altered the static portion of the system. Therefore static anomaly detectors focus on integrity checking.

Dynamic anomaly detection typically operates on audit records or on monitored networked traffic data. Audit records of operating systems do not record all events; they only record events of interest.

4.3 Specification based Detection

A recently introduced approach is the specification based cyber attack detection approach. Some reported works emphasize only on the misuse based and anomaly based cyber attack detection approaches [6]. However, there are others who talk about all three of the approaches. The specification constraint in this approach is used for reducing the number of FP alarms [7]. The specification constraints are extracted by the human expert manually. Although specifying critical resources of the system and their utilization may improve the security, there might always be some points missing in this process that may affect the system utilization. Specification based is not just applicable to the host systems but they can also be applied on the users as well.

5. Analysis Approach

Individual systems take differing approaches to the problem of cyber attack detection. There exist, however, a number of common issues that plague the range of detection strategies. This section examines a number of these issues and some of the ways in which researchers have attempted to improve them.

5.1 Embedded Programming Approach

In this method some parts of the processing is performed prior to the CADS. This preprocess will significantly reduce the processing load on the CADS and consequently the main CPU. Otey et al. [8] have reported a similar work by programming the Network Interface Card (NIC). This approach can have many properties including lower computational traffic and higher performance for the main processor. Implementing this approach will make it easier to detect variety of attacks such as Denial of Service (DoS) attack. This is because the NIC is performing the major part of the processing while the main processor only monitors the NIC operation.

5.2 Agent based Approach

In this approach, servers can communicate with one another and can alarm each other. In order to respond to an attack, sometimes it can be sufficient enough to disconnect a subnet. In this type of system in order to contain a threat, the distributed CADS can order severs, routers or network switches to disconnect a host or a subnet. One of the concerns with this type of system is the extra workload that the CADS will enforce on the network infrastructure. There are two approaches in implementing an agent based technology. In the first approach, autonomous distributed agents are used to both monitor the system and communicate with other agents in the network. A Multi-agent based system will enjoy a better perception of the world surrounding it. Zhang et al. [9] report implementing a multi-agent based CADS where they have considered four types of agents: Basic agent, Coordination agent, Global Coordination agent and Interface agents. Each one of these agents performs a different task and has its own subcategories. Foo et al. [10] report a CADS development work [11]. Luo et al. [12] introduce a new Mobile Agent Distributed Intrusion Detection System (MADIDS). Authors address number of deficiencies that exist in distributed IDSs.

5.3 Software Engineering Approach

The programming language with its special components will improve the programming standard for the CADS code. CADS developers can enjoy the benefits of a new language dedicated to the CADS development. Such a language will improve both the programming speed and the quality of the final code. In a paper by Vigna et al. [13] the main attention is focused on the software engineering aspect of the CADS. Issues such as object-oriented programming, component reusability and the programming language for the CADS are discussed in this paper. A new framework called State Transition Analysis Technique (STAT) is introduced in this paper. In their implemented framework, propose a type of state machine system called STAT that follows the state transition of the attack patterns. This framework is for developing signature based CADSs. These approaches could help the CADS to perform the cyber attack detection in a more successful and non-intrusive

5.3 Artificial Intelligence Approach

Researchers have proposed application of the fuzzy logic concept into the cyber attack detection problem area. Works reported by Ajit Abraham et al. [14], Bridges et al. [15] and T.S. Chou et al. [16] are examples of those researchers that follow this approach. Some researchers even used a multi disciplinary approach, for example, Gomez et al. [17] have combined fuzzy logic, genetic algorithm and association rule techniques in their work. Cho [18] reports a work where fuzzy logic and Hidden Markov Model (HMM) have been deployed together to detect cyber attacks. In this approach HMM is used for the dimensionality reduction. Due to its nature, the data mining approach is widely appreciated in this field of research. This algorithm is some-times used for the clustering purposes as well. Reported works from researchers such as Bulatovic et al. [19], Barbara et al. [20] and Bilodeau et al. [21] are examples of this approach. Researchers such as Zanero et al. [22], Kayacik et al. [23] and Lei et al. [24] find the Artificial Neural Network (ANN) approach more appealing. These researchers had to overcome the curse of dimensionality for the complex systems problem. A suitable method is the Kohonen’s Self Organizing features Map (SOM) that they have proposed. Liberios et al. [25] The main goal of using the ANN approach is to provide an unsupervised classification method to overcome the curse of dimensionality for a large number of input features. Since the system is complex and input features are numerous, clustering the events can be a very time consuming task. Using the Principle Component Analysis (PCA) or Singular Value Decomposition (SVD) methods can be an alternative solution [26]. In the computer networks cyber attack detection problem area, the size of the feature space is obviously very large. Once the dimensions of the feature space are multiplied by the number of samples in the feature space, the result will surely present a very large number. This is why some researchers, Srilatha Chebrolu et al. [27], Gopi K.Kuchimanchi et al. [28] and S. Selvan et al. [29] either select a small sampling time window or reduce the dimensionality of the feature space. Since the processing time is an important factor in the timely detection of the cyber attack, the efficiency of the deployed algorithms is very important. Time constraint may sometimes force us to have the less important features pruned (dimensionality reduction). However, the pruning approach is not always possible. Implementing data mining methodology, some researchers have proposed new data reduction approaches.

Table 1: Summary of cyber attack detection approach

Researchers	***Approach***	***Model representation***	***Search algorithm***
Fan et al 2000	Misuse Detection	Ordered Associative rule	FAST rule induction
Neri 2000a	Misuse Detecion	Associative rule	Genetic Algorithm
Lane 2000	Anomaly detection	Hidden Markov Model(HMM)	Baum-Welch algorithm
Dasguta et al 2001	Misuse detection	Classifier on statistics of attributes	Genetic Algorithm
Portnoy et al 2001	Anomaly detection	Outliers from clusters	Fixed width clustering
Bloedorn et al 2001	Anomaly detection	Outliers from clusters	K-mean clustering
Eskin et al 2002	Anomaly detection	Outliers from clusters	K-nearest neighbor
Staniford et al 2002	Misuse Detection	Bayes network	Simulated annealing
R. Sekar et al 2002	Specification based detection	State Machine	Specification Language
Mukkamala et al 2003	Misuse detection	Support Vector Machine (SVM)	SVM algorithm
Me-Ling Shyu et al 2003	Anomaly detection	Principle Component Ananlysis(PCA) feature reduction	Principal Component Algorithme
Gopi K. Kuchimanchi et al 2004	Misuse detection	PCA,Neural Network Feature reduction	Decision tree
Ajit Abraham et al 2005	Misuse detection	Decision tree feature selection	Fuzzy rule
Liberios et al 2006	Anomaly detection	Self Organizing Map (SOM)	Neural Network SOM
S.Selvan et al 2007	Misuse detection	PCA feature reduction	LAMSTAR Neural Network
T.S.Chou, et al 2007	Misuse detection	Fast Correlation based Filter feature redcuction	Fuzzy-Neural Network

6. Cyber Attack Detection Systems

Cyber attack Detection System (CADS) is software that automates the cyber attack detection process and detects possible cyber attacks. Cyber attack Detection Systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsider cyber attack.

6.1 Haystack

The Haystack [30] was developed for the detection of cyber attacks in a multi-user Air Force computer system, then mainly a Unisys (Sperry) 1100/60 mainframe running the OS/1100 operating system. This was the standard Air Force computing platform at the time. To detect cyber attacks the system employs two methods of detection: anomaly detection and signature based detection. The combination of these two methods solves many of the problems associated with the application of any one of them in cyber attack detection systems.

6.2 MIDAS. Expert systems in cyber attack detection

MIDAS (Multi Intrusion Detection and Alerting System) [31] was designed and written to perform rule-based cyber attack detection. For developing, compiling, and debugging the rules, MIDAS uses the Production-Based Expert System Toolset (P-BEST) that is a forward chaining, LISP based development environment. The P-BEST compiler produces primitive LISP functions that embody the semantics of the rules. The MIDAS rule base grew to be very large, so it was subdivided by the type of cyber attack for which each rule was designed to detect.

6.3 IDES/NIDS.A real-time intrusion detection expert system

Initially, IDES [32] was designed with a simple rule-based system to detect cyber attack attempts using cyber attack scenarios described by rule sets. The rule-based component was based on the same Production-Based Expert System Toolset (P-BEST) that MIDAS used. The rule base was divided into two parts for easier maintainability and understanding. NIDES [33] is the successor to the IDES project Like its predecessor it is very well documented, and there are many more references available than the two given here. Therefore, the model-based approach gains both efficiency and improved maintainability. The target hosts collect audit data from various host-based logs. There is a provision to utilize TCP WRAPPER [34], viz. host-based network traffic logs convert them into the canonical NIDES format, and transmits them to the NIDES host. The SSO interacts with the system through the NIDES host

6.4 Wisdom & Sense Detection

W&S [35] is another seminal anomaly detection system. Development began as early as 1984, with the first publication in 1989. W&S is unique in its approach to anomaly detection: it studies historic audit data to produce a forest of rules describing `normal' behavior, forming the `wisdom' of the title. These rules are then fed to an expert system that evaluates recent audit data for violations of the rules, and alerts the SSO when the rules indicate anomalous behavior, thus forming the `sense'. W&S reads historic audit records from a file.

6.5 NADIR An automated system for detecting network attack and misuse

NADIR [36], [37] was developed at the Los Alamos National Laboratory, for use by the laboratory in its internal computer security.2 Thus NADIR was conceived with the problems and organizational needs of the Los Alamos National Laboratory in mind. NADIR is implemented on a Sun SPARCstation II using the Sybase relational database management system. NADIR collects audit information from three different kinds of service nodes. Each audit record entered into NADIR pertains to a specific event. NADIR produces several sets of reports about system activity that the SSO can inspect for indications of intrusive behavior.

6.6 Hyperview. A neural network component for cyber attack detection.

Hyperview [38] is a system with two major components. The first is an `ordinary' expert system that monitors audit trails for signs of cyber attack known to the security community. The second is a neural network based component that learns the behavior of a user adaptively and raises the alarm when the audit trail deviates from this already `learned' behavior. The decision to attempt to employ a neural network for the statistical anomaly detection function of the system stemmed from a number of hypotheses about what the audit trail would contain. The fundamental hypothesis was that the audit trail constitutes a multivariate time series, where the user constitutes a dynamic process that emits a sequentially ordered series of events. The authors acknowledged that this would make for a simple model that could be easily trained, for example. However, since there were a number of problems with this approach the authors decided on a different tack. The authors chose to connect the artificial neural network to two expert systems.

6.7 DIDS Distributed Intrusion Detection Systems

DIDS [39] is a distributed cyber attack detection system that incorporates Haystack and NSM in its framework. DIDS is made of up of three main components. On each host, a host monitor performs local cyber attack detection, as well as summarizing the results and parts of the audit trail for communication to the DIDS director. Furthermore each network segment houses its own LAN monitor that monitors traffic on the LAN, and reports to the DIDS director. Finally, the centralized DIDS director analyses material from the host monitors and the LAN monitors that report to it, and communicates the results to the SSO. The expert system is an ordinary rule-based expert system. It is implemented in CLIPS, a C language expert system implementation from NASA.

6.8 ASAX Architecture and rule based language for audit trail analysis

The paper outlining ASAX [40] only describes a suggested prototype of the system, and hence it cannot be fully surveyed. ASAX is a rule-based cyber attack detection system with a specialized, efficient language (RUSSEL) for describing the rules. ASAX first converts the underlying operating system's audit trail into a canonical format. named NADF by the authors and then processes the resulting audit trail in one pass by evaluating rules in the RUSSEL language. The RUSSEL language is a declarative, rule-based language that is specifically tailored to audit trail analysis. The authors state that: `a general purpose rule-based language should not necessarily allow encoding of any kind of declarative knowledge or making a general reasoning about that knowledge.

6.9 USTAT State transition analysis

USTAT [41] is a mature prototype implementation of the state transition analysis approach to cyber attack detection.

State transition analysis takes the view that the computer initially exists in a secure state, but as a result of a number of penetrations modeled as state transitions. it ends up in a compromised target state. USTAT reads specifications of the state transitions necessary to complete an cyber attack, supplied by the SSO, and then evaluates an audit trail in the Another intruder who is difficult to detect is the masquerader. However, if that masquerader then goes on to attempt any one of a number of cyber attacks to gain greater privileges; state transition will have a chance to catch him.

6.10 DPEM Distributed program execution monitoring

The authors note that previous work on the detection of the exploitation of previously known cyber attacks has focused on the patterns of use that arise from these exploitations [42] [43]. Instead they suggest that the opposite approach be taken, and that the cyber attack detection system should focus on the correct security behavior of the system, or more particularly a security privileged application that runs on the system as specified. The authors have designed a prototype. the distributed program execution monitor (DPEM) that reads the security specifications of acceptable behavior of privileged. DPEM prototype, as its name suggests, monitors programs executed in a distributed system. This is accomplished by collecting execution traces from the various hosts, and where relevant distributing them across the network for processing. DPEM consists of a director, a specification manager, trace ispatchers, trace collectors, and analysers that are spread across the hosts of the network.

6.11 IDIOT An application of Petri-nets to cyber attack detection

IDIOT [44] [45] is a system that was developed at COAST (now the Center for Education and Research in Information Assurance and Security (CERIAS). The basic principle behind IDIOT is to employ colored Petri-nets for signature based cyber attack detection. The authors suggest that a layered approach should be taken when applying signature based techniques to the problem of cyber attack detection. The authors argue that of the many available techniques of pattern matching, colored Petri-nets (CP-nets) would be the best technique to apply since it does not suffer from a number of shortcomings common in other techniques. The latter do not allow conditional matching of patterns, and do not lend themselves to a graphical representation. The patterns play a major role in IDIOT.

6.12 GrIDS. A graph based intrusion detection system for large networks

The authors suggest a method for constructing graphs of network activity in large networks to aid in cyber attack detection [46]. The graphs typically codify hosts on the networks as nodes, and connections between hosts as edges between these nodes. The choice of traffic taken to represent activity in the form of edges is made on the basis of user supplied rule sets. The graph and the edges have respectively global and local attributes, including time of connection etc., that are computed by the user supplied rule sets. The authors argue that these graphs present network events in a graphic fashion that enables the viewer to determine if suspicious network activity is taking place.

6.13 CMS Co-operating security managers

The authors of co-operating security managers [47] note that as networks grow larger, centralized cyber attack detection will not scale up well. To alleviate this problem they suggest that several cyber attack detection agents, one at each computer connected to the network, co-operate in a distributed fashion, where the computer from which a user first entered the system is made responsible for all that user's subsequent actions. This, the authors claim, results in the load being evenly distributed among the co-operating entities

6.14 Janus. A secure environment for entrusted helper applications

Janus [48] is a security tool inspired by the reference monitor concept that was developed at the University of California, Berkeley. While it is not a cyber attack detection system per se, it shows many interesting similarities with specification based cyber attack detection. Furthermore, its high degree of active influence over running applications makes it an interesting case-in-point when studying active response. Janus is a user-space, per application reference monitor intended to supervise the running of potentially harmful web-browsing helper applications.

6.15 JiNao Scalable cyber attack detection for the emerging network infrastructure

The authors have developed a prototype implementation of JiNao [49], a network cyber attack detection system that aim to protect the network infrastructure itself, rather than the individual hosts on that network. The threat model assumes that certain routing entities in a network can be compromised, causing them to misbehave or stop routing altogether. The authors state that cyber attack detection in

JiNao is operated using three different paradigms: misuse based detection, anomaly based detection, and protocol based (misuse) detection.

6.16 EMERALD Event monitoring enabling responses to anomalous live disturbance

EMERALD [50] [51] is intended as a framework for scalable, distributed, inter-operable computer and network cyber attack detection. The authors begin by describing a situation in which large, organic computing and network resources provide critical and costly service to their operators. These large computing resources typically contain commercial off the-shelf (COTS) components, as well as non-COTS components and legacy systems integrated with current technology. These infrastructures clearly need to be protected, and yet there is little in the way of widely available, robust tools to detect and track intruders. It is intended that EMERALD will contain components to enable the system to respond actively to the threats posed, principally by an attacker external to the organization or at least external on some level. However, the proposed architecture does not preclude the detection of internal attackers.

6.17 Bro

Bro [52] is, in the words of its authors, `A stand-alone system for detecting network intruders in real-time by passively monitoring a network link over which the intruder's traffic transits. The cyber attack detection system would have to operate in an environment in which it could come under attack. The construction of resilient security systems has attracted little research, so the designers chose to simplify matters by assuming that only one of two systems communicating would be subverted. The authors note that this assumption would cost practically nothing, since if the intruder had both systems under his control, he could establish intricate covert channels between them, and hence avoid detection anyway. Bro is realized as a single-point, network monitoring, policy based system, that contains both default deny and default permit elements in its detection. It is capable of monitoring the full data stream of an Internet access point consisting of an FDDI interface.

6.18 RIPPER

RIPPER [53] is tool inspired by data mining for the automatic and adaptive construction of cyber attack detection models. The central idea is to utilize auditing programs to extract an extensive set of features that describe each network connection or host session, and to apply data mining programs to learn rules that accurately capture the behavior of cyber attacks and normal activities. These rules can then be used for signature detection and anomaly detection. Data mining generally refers to the process of extracting descriptive models from large stores of data. The data mining field has utilized a wide variety of algorithms, drawn from the fields of statistics, pattern recognition, machine learning, and databases. Several types of algorithms are particularly useful for mining audit data: The authors concur that in order to detect new or novel cyber attacks; anomaly detection has to be employed. RIPPER as a signature detection tool does not produce signatures of a sufficiently general nature.

6.18 Honey Pot

HP is mainly a heuristic approach and is based on the concept of bait and trap. Nevertheless, industry sector is very attracted to this concept. There are a number of products available that use the HP to trap undetected intrusion attempts. Generally speaking, HP is a deception based approach to detect actions of a deceitful enemy (the intruder). Khattab et al. [54] propose roaming HPs for service level DoS attacks. The proposed mechanism allows the HP to randomly move its position within a server pool. Interesting beneficial features in this work are the filtering effect and connection-dropping. The filtering effect is when the idle server that is acting as a HP detects addresses of the attackers and filters them out or blacklists them.

7. Conclusion

The study of cyber attack detection systems is quite young relative to many other areas of system research and it stands to reason that this topic offers a number of opportunities for future exploration. Cyber attack detection systems vary in the sources they use to obtain data and in the specific techniques they employ to analyze this data. Most systems today classify data either by misuse detection or anomaly detection: each approach has its relative merits and is accompanied by a set of limitations. It is likely not realistic to expect that a cyber attack detection system be capable of correctly classifying every event that occurs on a given system. Desired features for the cyber attack detection system depend on both the methodology and the modeling approach used in building the cyber attack detection system. These features are usually numerous. Thus considering the volume of data, processing all of them will take quiet awhile. In order to speed-up the process, these features are usually preprocessed to reduce their size, while increasing their information value. There are numerous approaches reported in this area but still needs to implements new methodology to reduce the input feature of the network data without degrading the accuracy of the system. In future we would like to investigate the efficient technique for feature reduction of the input dataset.

References

[1] SANS Institute Staff, Intrusion Detection and Vulnerability Testing Tools: What Works? 101Security Solutions E-Alert Newsletters.2001.

[2] KDDCup99datasetAugust2003http:// kdd.ics.uci.edu/database//kddcup99/kddcup99.html

[3] Marinova-Boncheva, V. Applying a Data Mining Method for Intrusion Detection. – In: International Conference on Computer Systems and Technologies CompSysTech'07, 14-15 June 2007.

[4] Biswanath Mukherjee, Todd L. Heberlein, and Karl N. Levitt. Network intrusion detection. IEEE Network, 8(3):26–41, May/June 1994

[5] R. Heady, G. Luger, A. Maccabe, and M. Servilla. The Architecture of a Network Level Intrusion Detection System. Technical Report CS90-20, University of New Mexico, Department of Computer Science, August 1990

[6] N. Ye, "A markov chain model of temporal behavior for anomaly detection," in Proceedings of the 2000 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, June 2000.

[7] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, and S. Zhou, "Specification-based anomaly detection: a new approach for detecting network intrusions," in Proceedings of the 9th ACM conference on Computer and communication security, pp. 265–274,Washington D.C., USA, Nov. 2002. ACM Press.

[8] M. Otey, S. Parthasarathy, A. Ghoting, G. Li, S. Narravula, and D. Panda, "Towards nic based intrusion detection," in Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 723–728. ACM, ACMPress, NY, USA, Aug. 2003. Poster Session: Industrial/government track.

[9] R. Zhang, D. Qian, C. Ba, W. Wu, and X. Guo, "Multi-agent based intrusion detection architecture," in Proceedings of 2001 IEEE International Conference on Computer Networks and Mobile Computing,pp. 494–501, Oct. 2001.

[10] Simon Y. Foo and M. Arradondo, "Mobile agents for computer intrusion detection," in Proceedings of the Thirty-Sixth Southeastern Symposium on System Theory, pp. 517–521. IEEE, IEEE, 2004.

[11] Mitsubushi Corporation. "Concordia mobile agent development kit,". Software, 1999.

[12] G. Luo, X. L. Lu, J. Li, and J. Zhang, "Madids: A novel distributed ids based on mobile agent," ACM SIGOPS Operating Systems Review, vol. 37, pp. 46–53, Jan. 2003.

[13] G. Vigna, F. Valeur, and Richard A. Kemmerer, "Designing and implementing a family of intrusion detection systems," in Proceedings of the 9th European software engineering conference held jointly with 10th ACM SIGSOFT international symposium on Foundations of software engineering, pp. 88–97, Helsinki, Finland, 2003. Source: ACM Portal.

[14] Ajit Abraham, Ravi Jain, Johnson Thomas, Sang Yang Han " D-SCIDS: Distributed softcomputing intrusion detection system" Journal of Network and Computer Applications, Elsevier, 2005.

[15] Susan M. Bridges and M. Vaughn Rayford, "Fuzzy data mining and genetic algorithms applied to intrusion detection," in Proceedings of the Twenty-third National Information Systems Security Conference. National Institute of Standards and Technology, Oct. 2000.

[16] T.S.Chou, K.K. Yen and J.Luo " Network Intrusion Detection Design Using Feature Selection of Soft Computing Paradigms" International Journal of Computaional Intelligence Vol. 4 Number 3, 2007

[17] J. Gomez and D. Dasgupta, "Evolving fuzzy classifiers for intrusion detection," in Proceedings of the 2002 IEEE Workshop on the Information Assurance, West Point, NY, USA, June 2001

[18] . S. B. Cho, "Incorporating soft computing techniques into a probabilistic intrusion detection system," IEEE transactions on systems, man and cybernetics, application and reviews, vol.32, pp.154-160, May 2002.

[19] D. Bulatovic and D. Velasevic, "A distributed intrusion detection system based on bayesian alarm networks," Lecture Notes in Computer Science (Secure Networking CQRE (Secure) 1999), vol. 1740, pp. 219–228, 1999.

[20] D. Barbara, N. Wu, and S. Jajodia, "Detecting novel network intrusions using bayes estimators," in Proceedings of the First SIAM International Conference on Data Mining (SDM 2001), Chicago, USA, Apr.2001.

[21] M. Bilodeau and D. Brenner, Theory of multivariate statistics. Springer - Verlag : New York, 1999.Electronic edition at ebrary, Inc.

[22] Ste. Zanero and Sergio M. Savaresi, "Unsupervised learning techniques for an intrusion detection system," in Proceedings of the 2004 ACM symposiumon Applied computing, pp. 412–419, Nicosia, Cyprus, Mar. 2004. ACM Press.

[23] H. Gunes Kayacik, A. Nur Zincir-Heywood, and Malcolm I. Heywood, "On the capability of an som based intrusion detection system," in Proceedings of theInternational Joint Conference on Neural Networks, vol. 3, pp. 1808–1813. IEEE, IEEE, July 2003.

[24] J. Z. Lei and Ali Ghorbani, "Network intrusion detection using an improved competitive learning neural network," in Proceedings of the Second Annual Conference on Communication Networks and Services Research (CNSR04), pp. 190–197. IEEE-Computer Society, IEEE, May 2004.

[25] Liberios VOKOROKOS et.al, "Intrusion detection system using self organizing map", Acta Electrotechnica et Informatica , Vol. 6 No.1, pp.1-6, 2006.

[26] M. Analoui, A. Mirzaei, and P. Kabiri, "Intrusion detection using multivariate analysis of variance algorithm," in Third International Conference on Systems, Signals & Devices SSD05, vol. 3, Sousse, Tunisia, Mar. 2005. IEEE.

[27] Srilatha Chbrolu, Ajit Abraham, Johnson P. Thomas " Featrue deduction and ensemble design of intrusion detection systems" Computer Security, Elsevier 2004.

[28] Gopi K. Kuchimanchi, Vir V. Phoha, Kiran S. Balagani, Shekhar R. Gaddam "Dimension Reduction Using Feature Extraction Methods for Real-time Misuse Detection Systems" Proceedings of the workshop on Information Assurance and Security, US Military Academy, West Point, NY,10-11 June 2004.

[29] S. Selvan, V. Venkatachalam " Performance comparision of intrusion detection system classifiers using various feature reduction techniques" International Journal of Simulation vol. 9 no.1., 2007.

[30] S. E. Smaha. Haystack: An intrusion detection system. In rroceedings of the IEEE Fourth Aerospace Computer Security Applications Conference, Orlando, FL, USA, December 1988. IEEE, IEEE Computer Society Press, Los Alamitos, CA, USA

[31] Michael M. Sebring, Eric Shellhouse, Mary E. Hanna, and R. Alan Whitehurst. Expert systems in intrusion detection: A case study. In Proceedings of the 11th National Computer Security Conference, pages 74.81, Baltimore, Maryland, 17.20 October 1988.

[32] Teresa F. Lunt, R. Jagannathan, Rosanna Lee, Sherry Listgarten, David L. Edwards, Peter G. Neumann, Harold S. Javitz, and Al Valdes. IDES: The enhanced prototype, A real-time intrusion detection system. Technical Report SRI Project 4185-010, SRI-CSL-88-12, CSL SRI International, Computer Science Laboratory, SRI Intl. 333 Ravenswood Ave., Menlo Park, CA 94925-3493, USA, October 1988.

[33] D Anderson, T Frivold, and A Valdes. Next-generation intrusion-detection expert system (NIDES). Technical Report SRI-CSL-95-07, Computer Science Laboratory, SRI International, Menlo Park, CA 94025-3493, USA, May 1995.

[34] Wietse Venema. TCP WRAPPER: Network monitoring, access control and booby traps. In Proceedings of the 3rd USENIX UNIX Security Symposium, pages 85.92, Baltimore, Maryland, 14.16 September 1992. USENIX Association.

[35] H S Vaccaro and G E Liepins. Detection of anomalous computer session activity. In Proceedings of the 1989 IEEE Symposium on Security and Privacy, pages 280.289, Oakland, California, 1.3 May 1989.

[36] Kathleen A Jackson, David H DuBois, and Cathy A Stallings. An expert system application for network intrusion detection. In Proceedings of the 14th National Computer Security Conference, pages 215.225,Washington, D.C., 1.4 October 1991. National Institute of Standards and Technology/National Computer Security Center.

[37] Judith Hochberg, Kathleen Jackson, Cathy Stallings, J. F. McClary, David DuBois, and Josehpine Ford. NADIR: An automated system for detecting network intrusion and misuse. Computers & Security, 12(3):235.248, 1993.

[38] Herve Debar, Monique Becker, and Didier Siboni. A neural network component for an intrusion detection system. In Proceedings of the 1992 IEEE Computer Sociecty Symposium on Research in Security and Privacy, pages 240.250, Oakland, CA, USA, May 1992. IEEE, IEEE Computer Society Press, Los Alamitos, CA, USA.

[39] Steven R Snapp, Stephen E Smaha, Daniel M Teal, and Tim Grance. The DIDS (distributed intrusion detection system) prototype. In Proceedings of the Summer USENIX Conference, pages 227.233, San Antonio, Texas, 8.12 June 1992. USENIX Association.

[40] Jani Habra, Baudouin Le Charlier, Abdelaziz Mounji, and Isabelle Mathieu. ASAX: Software architecture and rule-based language for universal audit trail analysis. In Yves Deswarte et al., editors, Computer Security . Proceedings of ESORICS 92, volume 648 of LNCS, pages 435.450, Toulouse, France, 23.25 November 1992. Springer-Verlag

[41] Koral Ilgun, Richard A Kemmerer, and Phillip A Porras. State transition analysis: A rule-based intrusion detection approach. IEEE Transactions on Software Engineering, 21(3):181.199, March 1995.

[42] Calvin Ko. Execution Monitoring of Security-critical Programs in a Distributed System: A Speci_cation-based Approach. PhD thesis, Department of Computer Science, University of California at Davis, USA, 1996.

[43] Calvin Ko, M. Ruschitzka, and K Levitt. Execution monitoring of security-critical programs in distributed systems: A speci_cation-based approach. In Proceedings of the 1997 IEEE Symposium on Security and Privacy, volume ix, pages 175.187, Oakland, CA, USA, May 1997. IEEE, IEEE Computer Society Press, Los Alamitos, CA, USA. IEEE Cat. No. 97CB36097

[44] Mark Crosbie, Bryn Dole, Todd Ellis, Ivan Krsul, and Eugene Spafford. IDIOT. Users Guide. The COAST Project, Dept. of Computer Science, Purdue University, West Lafayette, IN, USA, 4 September 1996. Technical Report TR-96-050.

[45] Sandeep Kumar and Eugene H. Spafford. A software architechture to support misuse intrusion detection. Technical report, The COAST Project, Dept. of Comp. Sciences, Purdue Univ.,West Lafayette, IN, 47907.1398, USA, 17 March 1995.

[46] S. Stani ford Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K Levitt, C. Wee, R. Yip, and D. Zerkle. GrIDS.A graph based intrusion detection system for large networks. In Proceedings of the 19th National Information Systems Security Conference, 1996.

[47] G. White and V. Pooch. Cooperating security managers: Distributed intrusion detection systems. Computers & Security, Vol. 15(No. 5):441.450, 1996. Elsevier Science Ltd.

[48] Ian Goldberg, David Wagner, Randi Thomans, and Eric Brewer. A secure environment for untrusted helper applications (con_ning the wily hacker). In Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, USA, July 1996.

[49] USENIX, USENIX Association. Y. Frank Jou, Fengmin Gong, Chandru Sargor, Shyhtsun FelixWu, and Cleaveland W Rance. Architecture design of a scalable intrusion detection system for the emerging network infrastructure. Technical Report CDRL A005, Dept. of Computer Science, North Carolina State University, Releigh, N.C, USA, April 1997.

[50] Philip A Porras and Peter G Neumann. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In Proceedings of the 20th National Information Systems Security Conference, pages 353.365, Baltimore, Maryland, USA, 7.10 October 1997. NIST, National Institute of Standards and Technology/National Computer Security Center

[51] Phillip A Porras and Alfonso Valdes. Live traf_c analysis of TCP/IP gateways. In Proceedings of the 1998 ISOC Symposium on Network and Distributed Systems Security, San Diego, California, 11.13 March 1998.

[52] Vern Paxon. Bro: A system for detecting network intruders in real-time. In Proceedings of the 7th USENIX Security Symposium, San Antonio, TX, USA, January 1988.

[53] Wenke Lee. A data mining framework for building intrusion detection MOdels. In IEEE Symposium on Security and Privacy, pages 120.132, Berkeley, California, May 1999.

[54] Sherif M. Khattab, C. Sangpachatanaruk, D. Mosse, R. Melhem, and T. Znati, "Roaming honeypots for mitigating service-level denial-of-service attacks," in Proceedings of the 24th International Confer-ence on Distributed Computing Systems (ICDCS04),pp. 328–337. IEEE, IEEE Computer Society, Mar. 2004.

Shailendra Singh Lecturer in, Department of Information Technology at Rajiv Gandhi Technological University, Bhopal, India. He has publised 6 papers in international and national conference proceedings His research interest include softcomputing, datamining and network security.He is a life member of ISTE, Associte member of Institution of Engineers (India) and member of International Association of Computer Science and Information Technology (IACSIT).

Dr. Sanjay Silakari Professor and Head, Department of Computer Science and Engineering at Rajiv Gandhi Technological University, Bhopal, India. He has awarded Ph.D. degree in Computer Science He posses more than 16 years of experience in teaching under-graduate and post-graduate classes. He has publised more than 55 papers in international and national journals and conference proceedings.