Vol. 4, No. 10 October 2013 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

The Assessment of Employing Computational Intellection in Intrusion Detection Systems

[1] Murtaza Hussain Shaikh, [2] Ievet S.Karlson
[1] Member IEEE, Oslo, Norway
[2] Department of Computer Science, University of Bristol, Bristol BS8 1TH, United Kingdom
[1] Murtaza.Shaikh@ieee.org, [2] Ievet.K@bristol.ac.uk

ABSTRACT

Computer systems of today are subject to many attacks and it can be anticipated that these problems will increase in the future era. One way of protecting the systems is to use better authentication and other categories of preventive security mechanisms. These mechanisms do not offer good enough protection in most cases and they should therefore be complemented with monitoring and detection mechanisms. Intrusion detection over the network is indeed an important field of the information security. Although many intrusion detection systems are widely available today, the technology is still young and the combat against threats from both internal and external sources seems to be an endless. Intrusion detection systems have turn out to be a significant factor in security toolbox. Nevertheless, numerous security specialists are still in the gloomy about intrusion detection phenomena and hesitant about what intrusion detection systems tools do; how to utilize them, or why they are a compulsory. In this article we will present a succinct overview of intrusion detection systems, including a sketch; the functionalities and the diverse techniques of intrusion detection that could provide work for.

Keywords: *Availability; Authenticity; Detection; Expansion; Intrusions; Sensitive; Denial of Service.*

1. INTRODUCTION

Before we start to answer this important question asked from everyone in every network age that "Why we need network security?" we have to take a deep look about our current running systems. As Internet expanded, so did the opportunities for its misuse, the result of a host of security flaws. For instance, e-mail was easy to spoof, passwords were transmitted in clear and connections could be hijacked. Nevertheless, most users had no real interest in security failings until the 1980`s Internet worm case, which provided a glimpse of how damaging these defects [1]. At the moments, as billions of usual citizens are by means of networks for banking, shopping, and network security is intimidating on the perspective as a potentially massive dilemma. The concept of security is defined as a continuous process of protecting an object from attack. That object may be a person , an organization such as a business , or property such as a computer system or a file [6]. Network security can be defined as a process of securing network assets from internal and external threats. It also can be defined as protecting data that are stored on or that travel over a network against either accidental and intentional unauthorized disclosure or modification [2]. Many people view network security as having 3 main goals are described in fig 1. Availability is a characteristic that ensures that our information, service or asset is accessible and can provide the service it is designed for, when it is needed. There are several processes in networking such as redundancy, backups; that can offer a higher level of system availability [5]. The denial of service attacks are aimed to harm availability of the system. Integrity is a characteristic about the insurance of software or data completeness and accuracy as well as its authenticity. When we talk about the network integrity it has the purpose to provide and ensure that data must be protected from unauthorized modification and destruction.

It can be achieved by cryptography. Confidentiality is a characteristic of protecting sensitive information from manipulation in a form of disclosure and interception. Cryptography is also used here to provide confidentiality [2].

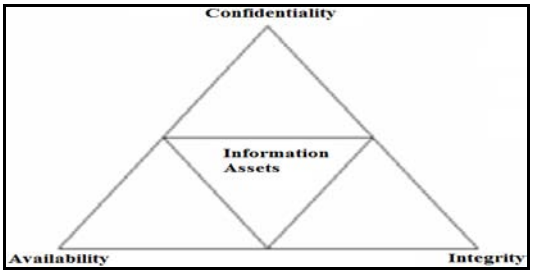

Fig 1: Network security trinity [2]

The importance of those characteristics varies depending on the company's business. Furthermore, all characteristics are connected among themselves and cooperate to provide an adequate level of security . Based on everything we know , this truly seems to be the golden age of hacking this statement is true for many reasons we will explain this as follows;

1.1 Easy to be cracked

The Internet grew so quickly that few gave any thought to security. Attackers have the upper hand and it will take a while before companies secure their systems. The other thing that makes matters worse is how companies have built their networks. In late 80`s, companies hired programmers to customize their applications and systems, so if an attacker wanted to break into the network, he had to learn a lot about its secure environment. The information did not help the attacker when he tried to break into another company's network, because its systems were totally different [7]. Now every

company uses the same equipment with the same software. If an attacker learns Cisco and he can break into practically any system on the Internet; because networks are so similar, and software and hardware are so standardized, the attacker's job is much easier [7].

1.2 Easy to be Attacked and Exploit

Not only are systems easy to break into, but the tools for automating attacks are very easy to obtain on the Internet. Even though an attacker might have a minimal amount of sophistication, he can download tools that allow him to run very sophisticated attacks. The ease at which these tools and techniques can be obtained transforms anyone with access to the Internet into a possible attacker [7].

1.3 Boundless Nature of Internet

Another issue is the ease in which a user connected to the Internet can travel across local, state, and international boundaries. Accidentally, typing one wrong number in an IP address can be the difference of connecting to a machine across the room and connecting to a machine across the world [10]. When connecting to a machine outside this country, international cooperation is required to trace the connection [4]. Based on the ease of connecting to a machine anywhere in the world, attackers can hide their path by hopping through several computers in several countries before attacking a target machine. In many cases, picking countries that are not allies can almost eliminate the possibility of a successful trace. So to trace this attacker couple of things is needed. First, it takes a lot of time, and second, it requires timely cooperation among all the regions, which would be difficult at best [7].

1.4 No Policing

Currently, because there is no one policing the Internet, when problems occur, there are not clear lines over who should investigate and what crime has been committed. Most countries are trying to take conventional laws and apply them to the Internet. In some cases, they apply, but in other cases they do not adapt well. Even if there were an entity policing the Internet, it would still be difficult because people are committing the crimes virtually [7].

So need to computer network is not an option during the present days, it became a must and the question should not be whether to secure network or not; but it must be how to secure it [3]. An intrusion detection system can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity[14].

2. DRIVING FACTORS OVER IDS

Concept of intrusion detection is not a new one, but it has been discussed more than thirty years ago and from that time many researchers addressed it. Originally, the first step in intrusion detection was done by system administrators they performed intrusion detection by sitting in front of a console and monitoring user activities. They might detect intrusions by noticing, for example, that a vacationing user is logged in locally or that a seldom used printer is unusually active [1]. Although effective enough at the time, this early form of intrusion detection was ad hoc and not scalable. The subsequently step in intrusion detection involved audit logs, which system administrators reviewed for evidence of unusual or malicious behavior. In late 80`s, administrators typically printed audit logs on fan-folded paper, which were often stacked four to five feet high by the end of an average week. Searching through such a stack was obviously very resource consuming. With this overabundance of information and only manual analysis, administrators mainly used audit logs as a forensic tool to determine the cause of a particular security incident after the fact. There was little hope of catching an attack in progress [9]. As storage became cheaper, audit logs moved online and researchers developed programs to analyze the data. However, analysis was slow and often computationally intensive and, therefore, intrusion detection programs were usually run at night when the system's user load was low. Therefore, most intrusions were still detected after they occurred. In early 90`s, researchers developed real time intrusion detection systems that reviewed audit data as it was produced. This enabled the detection of attacks and attempted attacks as they occurred, which in turn allowed for real time response, and, in some cases, attack preemption [13]. More recent intrusion detection efforts have centered on developing products that users can effectively deploy in large networks.

a) **Threat:** A prospect of deliberate not permitted try to manipulate information, render a system unusable [19].

b) **Risk:** A violation of operations integrity due to malfunction of hardware [19].

c) **Vulnerability:** A flaw in hardware / software design or operation of a system that exposes information to accidental revelation [19].

d) **Attack:** A precise formulation of an arrangement to carry out a threat [19].

e) **Penetration:** An ability to get unauthorized access to control state of a system [10], [19].

In article [15] it was proposed that audit trials should be used to monitor threats and all protection methods were focused on denying access to sensitive data. Later in [2] it was intended a concept of intrusion detection as a key to the problem of providing a sense of security in computer systems. The basic idea is that intrusion behavior involves abnormal usage of the system. The model is a rule based pattern matching system. Some models of normal usage of the system could be constructed and verified against usage of the system and any significant deviation from the standard usage flagged as abnormal usage. Statistical approaches compare the recent behavior of a user of a computer system with observed behavior and any significant deviation is

considered as intrusion. This approach requires construction of a model for normal user behavior . Predictive pattern generation uses a regulation base of user profiles defined as statistically weighted event sequences [20]. This method of intrusion detection attempts to predict future events based on events that have already occurred. State transition analysis approach constructs the graphical representation of intrusion behavior as a sequence of alterations that direct from a preliminary secure state to targeted state. Using the audit trail as input, an analysis tool can be developed to compare the state changes produced by the user to state transition diagrams of known penetrations [1],[4]. Keystroke monitoring technique utilizes a user's keystrokes to determine the intrusion attempt. The main approach is to pattern match the sequence of keystrokes to some predefined sequences to detect the intrusion. A proper model based approach attempts to model intrusions at a higher level of abstraction than audit trail records. This permits administrator to generate their representation of the penetration abstractly, which shifts the burden of determining what audit records are part of a suspect sequence to the expert system. This technique differs from the rule based expert system technique, which simply attempt to pattern match audit records to expert rules [5], [6]. A pattern match technique encodes the intrusion signatures that are matched against audit data. Intrusion signatures are classified using structural interrelationships among the elements of the signatures. The patterned signatures are matched against the audit trails and any matched pattern can be detected as an intrusion [11], [12]. During recent years, several data mining approaches have been also used to construct IDS.

3. TRAITS OF IDS

Our existing computer systems which are supposed to provide assurance against DOS (denial of service), however, due to improved connectivity and vast scale of financial potential that are opening up; more systems are subject to attack by hackers [17]. These treason attempts try to take advantage of defects in the operating system as well as inside main apps of system. This may rise another important question "How we can handle subversion attempts?" There are two possibilities of this subversion. One possible way is to avoid subversion is by construction of a secure system (e.g. require all users for authentication). We could guard data by cryptographic methods and tight access control protocols. Therefore, designing and implementing a bug free system is extremely difficult task [6], [7]. If there are attacks, we would like to trace them immediately. This is exactly what IDS based system`s job. Intrusions could be divided in six main types;

a) Attempted break-ins which can be detected by violations of system constraints [16].
b) Masquerades are attacks which can be detected by violations of internal security limitations [16].
c) Penetration of security control which are detected by monitoring of specific activity [16].
d) Leakages which are could use the system resources if an attack is launched [16].
e) Denial of service which is detected by use of system supplies [16].
f) Malicious services use which is detected by violations of special privileges [16].

Intrusion detection systems can be classified according to different criteria such as information sources, detection techniques, and response options. A common means to classify IDS is to cluster them by an information sources. Various IDS analyze network packets. A number of commercial IDS`s are network-based system. Snooping on network switch, one network-based ID system can monitor network traffic of multiple hosts that are associated with that specific switch [8]. Network-based IDS`s often consists of a set of hosts assembled at different positions in network. These divisions monitor network traffic, performing local analysis of the traffic and exposure attacks to a central management console [15]. The main objective of network security is to ensure that protected applications and information used as input and generated as output by these applications are not compromised by malicious security breaches [13]. As a result, it is possible to define the major basic network security functional elements that are needed to build a network security system, in terms of the following well known security services needed for secure message exchanges: authentication, message integrity, and non-repudiation [20].

4. ASSOCIATED VIEWS

Commonly known, host based IDS (HIDS) and network based IDS (NIDS) are two types of IDS as defined in table 1, fluctuate considerably from each other. The architecture of host is actually an agent-based, which means that software agent exists in each host. In addition, IDS are capable of collecting system audit trails in real time, thus distributing both CPU utilization provides a flexible means of security administration [14]. It would be beneficial to integrate IDS network, such that it would filter alerts in an identical manner to host-based portion of the system. This provides an effective means of supervising both types of intrusion detection.

Table 1: Differences in NIDS and HIIDS

NIDS	HIDS
Broad scope (watches all network activities)	Narrow scope (watches specific host activities)
Easier setup	Complex setup
Enhanced for detecting attacks outside	Enhanced for detecting attacks inside
Low-cost to implement	Expensive to implement

NIDS	HIDS
Detection is based on recorded system on entire network	Detection is based on what single host can record
Determination of packet headers	No determination of packet headers
Real-time response	Responds after suspicious log entry
OS-independent	OS-specific
Detects network attacks as payload is analyzed	Detects local attacks before they hit the network
Detects unsuccessful attack attempts	Verifies success or failure of attacks

Most internal threats come from two sources: employees and accidents. Employee threats may be intentional or accidental as well. We will not stress on threats occurred by accidents. In most cases, employees know more about a network and the computers on it than any outsider. At the very least, they have legitimate access to user accounts [15]. Intentional employee security threats include the following;

i. Person who employ hacking techniques to upgrade their legitimate access to root/administrator access, allowing them to reveal trade secrets, steal money, and so on for personal or political gain [10].
ii. Person who take advantage of legitimate access to reveal trade secrets, steal money, and so on for personal or political gain.
iii. Family members of employees who are visiting the office and have been given access to company computers to occupy them while waiting.
iv. Person who breaks into secure machine rooms to gain physical access to mainframe and other large system consoles.

5. DETECTION TECHNIQUES & FURTHER RESPONSE

Detection techniques can be classified according to misuse detection and anomaly detection. Misuse detection is used by mostly commercial systems. While anomaly detection looks for abnormal patterns of activity.

5.1 Misuse Detection

Misuse detectors analyze system activity and those particular events that match with predefined patterns. Since the pattern corresponding to known attack is called signature, misuse detection is commonly called signature-based detection. It is also known in literature as rule-based detection. This method is similar to method of detection new viruses where an appropriate signature or pattern should be known in advance [16]. A lump diagram of typical misuse detection is shown in Fig 2.

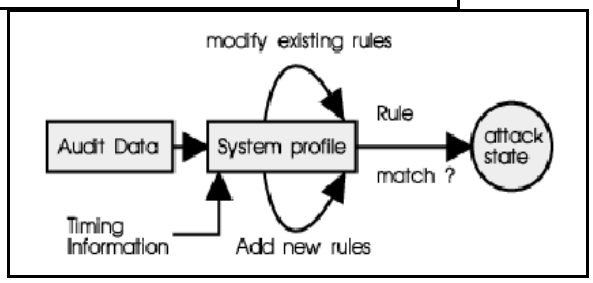

Fig 2: A misuse detection system

5.2 Anomaly Detection

Anomaly detectors are designed to track abnormal behavior of patterns as illustrate in fig 3. For example, a user logs on and off of a system 20 times in a day instead of normal 1 or 2 times. Anomaly detection can investigate user patterns, such as profiling the executed tasks.

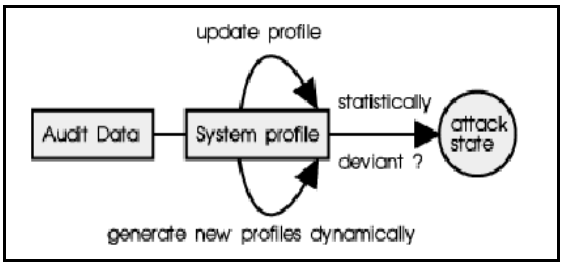

Fig 3: An Anomaly detection system

5.3 Response Options for IDS

Once IDS have recorded event information, it to find symptoms of attacks, they create responses. Some of responses entail reporting results to a specified location. Though networking researchers are tempted to undervalue the importance of good response functions in IDS [18]. Commercial IDS support a wide range of response options, often categorized as active responses, passive responses. Active responses are the automated actions taken when intrusions are detected [3].

5.4 Alarms and Notifications

The alarms are generated by IDSs to inform users when attacks are detected. Mostly commercial IDS allow users a great deal of latitude in determining when alarms are generated and display [2].

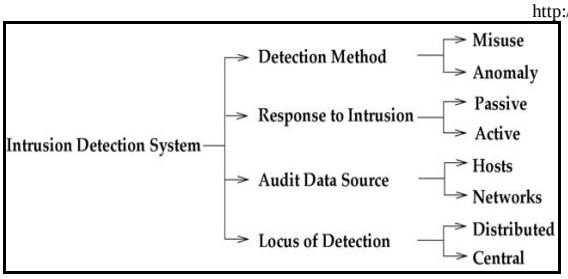

Fig 4: Distinctive misuse detection system

Commonly form of alarm is an onscreen alert in operating system. The information provided in alarm message varies from a notification to a detailed message outlining the IP addresses of the source [5]. Another set of options are of utility to distributed organizations involving remote alerts and some products also recommend email services as effective notification channel [5].

6. FEATS AGAINST INTRUDERS

The most innocuous, an active response is to collect additional information about a suspected attack. Each one of us has probably done the equivalent of this when awakened by a strange noise at night. The first thing one does in such a situation is to listen more closely, searching for additional information that allows deciding whether to take action [17]. In the IDS case, this might involve increasing the level of sensitivity of information sources as shown in fig 4. Collecting additional information is helpful for several reasons. The additional information collected can help resolve the detection of the attack. Another active response is to halt an attack in progress and then block subsequent access by the attacker. Typically, IDS do not have the ability to block a specific user access, but instead block IP addresses from which the attacker appears to be coming. Passive IDS responses provide information to system users, relying on humans to take subsequent actions based on that information [20]. Many commercial IDS rely solely on passive responses and some who follow intrusion detection, especially in cyber warfare theme, believe that an active response is to taken against the intruder. The aggressive form of this response involves launching attacks against the attacker's host. Due to legal ambiguities about civil liability, this option can represent a greater risk that the attack it is intended to block [19]. A reason for approaching this option with a great deal of caution is that it may be an illegal step.

7. CONCLUSION

As system security threats become more frequent, IDS tools are becoming increasingly essential. They round out the working in conjunction with other security tools (e.g. firewalls for the supervision of network activity). These security tools use various techniques to determine what verifies an intrusion versus a normal traffic of network. Whether a system uses anomaly or misuse detection, they usually come into different categories that are described in this article. Each category has its strong and weak points that should be counter measure against the requirements. Preferably, the effective IDS tool combines mutual approaches under one system management console. A user gets comprehensive coverage against countless threats, whether it`s host-based or network-based. Intrusion detection supported on computational intelligence is recently attracting considerable interest from the network research community. Its uniqueness such as fault tolerance, towering computational speed and fits the requirement of building a good IDS platform.

REFERENCES

[1] An Architecture for Intrusion Detection using Autonomous Agents, Jai Sundar, et al., 2004, COAST Technical Report 19/05, COAST Laboratory, Purdue University,USA.

[2] Loyall, J. et. al., Building Adaptive and Agile Applications Using Intrusion Detection and Response. Network and Distributed System Security Symposium (NDSS) (Jan. 2008) San Diego CA,USA.

[3] L. Spitzner, Honeypots- Tracking Hackers, Indianapolis, IN: Addison-Wesley, 2008, pp. 242-261.

[4] W. Stallings, Network Security Essentials, Upper Saddle River, NJ: Prentice Hall PTR, 2009, p. 322.

[5] E. Skoudis, Counter Hack, Upper Saddle River, NJ: Prentice Hall PTR, 2009, p. 47.

[6] Korba, J. 2010. Windows NT attacks for the evaluation of intrusion detection systems. Master's Thesis. Massachusetts Institute of Technology, Cambridge, MA,USA.

[7] Zonghua Zhang , Hong Shen, M-AID: An adaptive middleware built upon anomaly detectors for intrusion detection and rational response, ACM Transactions on Autonomous and Adaptive Systems (TAAS), v.4 n.4, p.1-35, November 2009.

[8] Lee, W. 1999. A data mining framework for building intrusion detection models. In Proceedings of the 1999 IEEE Computer Society Symposium on Research in Security and Privacy (Berkeley, CA, May). IEEE Computer Society Press, Los Alamitos, CA, 120-132.

[9] Stolfo, S. J., Lee, W., Chan, P. K., Fan, W., & Eskin, E. (2006). Data mining-based intrusion detectors: an overview of the columbia IDS project. ACM SIGMOD Record, 30(4), 5-14, Italy.

[10] Stephen G. Eick, Joseph L. Steffen, and Jr. Eric E. Sumner. Seesoft-a tool for visualizing line oriented software statistics. IEEE Transactions on Software Engineering, 18(11):957–968, 2005, USA.

[11] Tetsuji Takada and Hideki Koike. Tudumi: Information visualization system for monitoring and auditing computer logs. In Proceedings of Information Visualization, pages 570–576, July 2009. Sixth International Conference, Finland.

[12] Hideki Koike and Kazuhiro Ohno. Snortview: Visualization system of snort logs. In ACM, editor, VizSEC/DMSEC'09, Washington DC, USA.

[13] H. Debar and A. Wespi. Aggregation and correlation of intrusion detection alerts. In Recent Advances in Intrusion Detection (RAID), pages 85–103. Springer-Verlag, 2007.

[14] A.Boukerche, K. R. Lemos Juc, J. B. Sobral, and M. Sechi Moretti Annoni Notare, "An artificial immune based intrusion detection model for computer and telecommunication systems", IEEE Parallel Computing, vol. 30, issues 5-6, pp. 629-646, 2009.

[15] W. Lee, S. Stolfo, and K. Mok, "A data mining framework for building intrusion detection models", in proceedings of the IEEE Symposium on Security and Privacy, pp. 120-132, 2001, United Kingdom.

[16] Dorothy E. Denning, "An intrusion detection model", IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 118-131, 2005.

[17] Phil Baskerville, " Intrusion Prevention Systems: How do they prevent intrusion?", Master's thesis, University of Otago, Dunedin, New Zealand, March 2010.

[18] W. H. Chen, S. H. Hsu, and H. P. Shen, "Application of SVM and ANN for intrusion detection", Computers & Operations Research, vol. 32, issue 10, pp. 2617-2634, 2009, China.

[19] C. Zhang, J. Jiang, and M. Kamel, "Intrusion detection using hierarchical neural networks", Pattern Recognition Letters, vol. 26, issue 6, pp. 779-791, 2007, China.

[20] Carl Endorf, Eugene Schultz, and Jim Mellander, "Intrusion Detection & Prevention", 2008, McGraw-Hill Publishing, ISBN: 0-07-222954-3, USA..