Intrusion Detection and Prevention System: Issues and Challenges

Bilal Maqbool Beigh
Kashmir University
Srinagar, India.

Uzair Bashir
Mewar University
Rajasthan, India

Manzoor Chachoo
Kashmir University
Srinagar, India

ABSTRACT

In In spite of the tremendous growth of technologies in computer networking and information technology, still we lack in preventing our resources from theft/attacks. This problem is very big as far as industry/ companies are concerned. As maximum of the organizations are facing an increasing number of threats every day in the form of viruses and attack etc. Since many different mechanisms were opted by organizations in the form of intrusion detection and prevention system to protect its organizations for these kinds of attacks, still there are many security breaches in every organization. In order to understand the security risks and IDPS, we will first survey about the common security breaches and then after discuss what are different opportunities and challenges in this particular field. In this paper we made a survey on the overall progress of intrusion detection systems. We survey the existing types, techniques and architectures of Intrusion Detection Systems in the literature. Finally we outline the present research challenges and issue.

Keywords

Security, IDPS, Virus, Attack, Detection, System, Architecture, Prevention, Risk, deployment, IDS, intrusion, testing, challenges.

1. INTRODUCTION

In today’s world, the whole system is going digital which mean that the information is being stored digitally instead of traditional storage. Thus all the communities either business or individuals depend on the computers for their information storage and if they want to share their valuable assets / secret information with anybody in any corner of the world, they rely on computer networks. Thus it became very much mandatory that we should keep the information / assets and network safe from the hackers/ attackers/ intruders [1][2]. In order to have our network safe from these black hats, a new field has emerged in computer science and information security we called that as Intrusion detection and prevention system. Actually this was developed in early 90’s to generate the report of attacks. Later it emerges as the tool for detecting different attacks and simultaneously prevents them. According to Bilal& peer [3], the intrusion detection may be defined as a process of denying permission on some data to someone who does not have valid permission to access the same data. Thus we can say that intrusion is act of attempting access to some other’s information/data without proper authorization or it is collection of actions on the network which violates security aspects (confidentiality, integrity, availability and authenticity) of a network‘s data/ information [4] and on the other hand intrusion detection system is a process which detects these actions / violations of security on network data. The main purpose of the intrusion detection and prevention system is to review, control, analyze and produce reports from the system activates. Even though a lot of research is done in this particular field still there are numbers of issues and challenges in the system. The research communities are working very hard but it is big research field and thus needs more research attention. The researchers have generally categorized the attackers into three different categories - insider, outsider and unknown [10] [11]. Also according to the report by University of PEREAUS, the total numbers of insider attacks are 34 %, while as for outsider attacks are 37% and rest 29% are unknown[4]. Here in this paper, we are not going to propose or develop anything new but we are going to identify the different kind of issues and challenges which are being faced by today’s intrusion detection and prevention system. The paper consists of four sections , first section will give the introduction towards the intrusion detection systems as we have above, second section will discuss the need of intrusion detection and prevention system , the third section will discuss the core part of this paper i.e. issues and challenges in today’s intrusion detection and prevention system. In Section four, we suggest some remedies or proposals for resolving the issues and challenges based on previous section and final section will consist of final conclusion.

2. NEED FOR INTRUSION DETECTION SYSTEM

As discussed in above section of this paper that intrusion can be defined as a process of accessing someone’s personal property or data or information without proper access. Since the data or information is widely available online through websites or computer programs, this method of storing data increases the security risks in huge quantity. According to Symantec report , around 60,000 websites are available online, thus a person on longer need to be a gem in hacking, just download / run the hacking program, make some settings and you are done [6]. In order to secure the companies or individual’s data/ information, firewalls are being installed, but they do not serve the purpose of defending the data from attacks or intruders. The main aim of the firewall is to filter the traffic but they cannot block all the traffic. Also once the traffic passed through the firewall there is no such mechanism available that traffic will be monitored inside the network for rest processing. Also firewall only detects external traffic coming to it, but doesn't detect the internal attacks. By using intrusion detection system, we can monitor or do the following things:

- Monitors network traffic.
- Continuously monitors servers/ network for misuse actions or abuse policy.
- Attack / breach alerting, response and reporting.
- Countermeasures.

Thus it became very much important for an organization to install both firewall and intrusion detection system to secure their assets / information for hackers / attackers.

3. APPROACHES OF INTRUSION DETECTION SYSTEM

In intrusion detection process, there are number of approaches by which an intrusion can be detected. In general, the intrusion detection policies can be as [7]:

- Anomaly based detection policy.
- Mis-Use based detection policy.
- Hybrid detection policy.

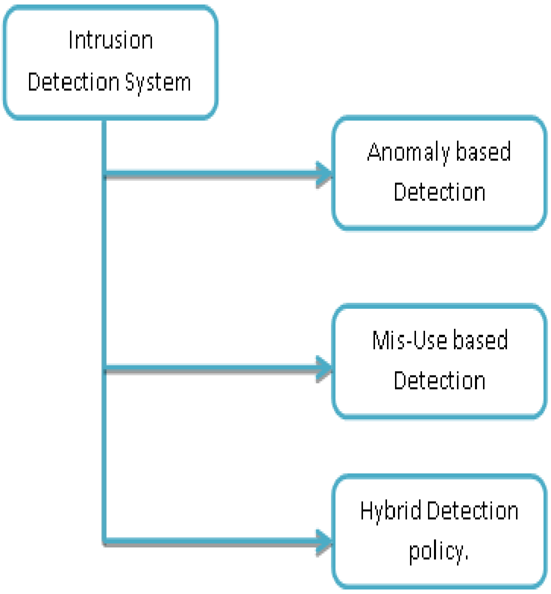

Figure 1: Approaches to intrusion Detection system

3.1 Anomaly Based Detection

In this approach, intrusion is measured as a degree of deviation from normal behavior. In other sense, we can say that any such action or work that diverts from the normal behavior of execution, it is detected as intrusion. We have different techniques which follow the anomaly detection policy [2][7].

- Statistical models.
- Machine learning and data mining models.
- Computer Immunological approaches. Etc.

these guidelines have been set. The goal is to have a 9-point text, as you see here. Please use sans-serif or non-proportional fonts only for special purposes, such as distinguishing source code text. If Times Roman is not available, try the font named Computer Modern Roman. On a Macintosh, use the font named Times. Right margins should be justified, not ragged.

3.2 Mis-Use based detection

Please In this approach, the intrusion is detected based on pattern matching. Here in this scenario, intrusion can be detected based on knowledge available on attacks or we can say that it looks for the events or actions that match with already stored events which describe a known attack. Some of the intrusion detection system which follows mis-use detection scheme is as:

- RUSSEL
- P-BEST
- State Transition
- Colored Petri Automata etc.

3.3 Hybrid detection policy

Another approach which came in existence is known as hybrid detection scheme. This technique takes the best features of both the techniques used for detection purpose i.e. anomaly and mis-use based techniques. This combined approach gives existence to a single intrusion detection system for monitoring the attacks.

4. Issues and Challenges in IDS

Today intrusion detection system is still in infancy and need lot of research work to be done to make the intrusion detection even more successful. There are a huge number of issues and challenges in current intrusion detection system which needs the immediate and strong research attention. In this paper, we have identified some important issues and challenges which need to be addressed by research communities. The issues and challenges are as:[16]

- Deficiency or incomplete Data set.
- Detection Algorithms.
- Integration of multiple formats of data.
- Platform dependencies.
- Poor Design.
- Testing/ Evaluation of IDS.

We will discuss all the issues and challenges in detail as under:

4.1 Data Set

Data set can be defined as a collection of all the data or information during the survey which needs to be analyzed. Since in intrusion detection system, the data sets play important role in accuracy of results. Thus it became very much important to have datasets which are almost near to real time system. Now a days, the researchers are using data set DARPA 98, 99, New Mexico university immune system etc. but being outdated, we are not able to mitigate those attacks which are very much new. Thus it became very much important that attack models should be tested in updated data sets [8] [9]. Therefore this problem needs to be addressed in order to have most accurate and simplified results. Some popular data sets which are used by researchers for the purpose of experimentation but are outdated are as : [12] [17]

- MIT Lincoln laboratory -- DARPA intrusion detection and Evaluation.
- University of Mexico -- Computer immune system.
- University of California –UCI knowledge discovery in databases (KDD) Archive.
- University of Minnesota – MINDS
- Prude University –CERIAS Group.
- Naval Postgraduate school – intrusion Defense.
- University of Virginia – Application Intrusion Detection.
- University of California – State Transition Analysis Technique.

4.2 Detection policy

Detection policy –this is the main part while find whether the packet/ information come is attack or the useful information which the user needs to implement the process or jobs. The detection algorithm should be competent enough that it should match all the case in small time and also should match the terms efficiently. The detection policy may be either anomaly or mis-use based. In anomaly based detection, the behaviour is identified and if behaviour is identified as reverse of normal, it is declared as attack and in another scenario, the pattern is matched using some pattern matching algorithm for known attacks and if pattern matches fully with some suspicious data, it is declared as attack. But there are also drawbacks that there are no rules for new attacks to be matched, hence new attacks are not detected or if it makes some changes in data so that it cannot match the pattern, the attack is detected. Hence we are in need of good and fast algorithm which will detect the pattern thoroughly and fast to match the most of the attacks.

4.3 Integration of Multiple formats

As we are well aware of the fact that the incoming frames or data may be in different formats. So there is need that different formats shall be integrated on a single intrusion detection system. I.e on the fly it should check for the formats and check the stream for intrusions.[18]

4.4 Platform Dependence

In current technological world, we have different / number of intrusion detection system available some are free source while other are commercial. While implementing these available in the market. The comparative study is the tubular form. We have chosen some parameters on which the comparative study will be carried out. The parameters are in the table below:

Table 1: List of parameters with explanation for comparative analysis.

Parameter	**Description**
Name	The name of the intrusion detection system
type	The type of tool, or category in which this tool belongs, e.g., “Web Application Scanning
Platform	The operating system(s) on which the tool runs. If the tool is an appliance, this field will contain a “not applicable” symbol (N/A) because the operating system is embedded in the tool.
License	The type of license under which the tool is distributed, e.g., Commercial, Freeware, GNU Public License
Based on	The technology on which IDS is based on i.e, Rule based , pattern matching etc.
Suitability	On what kind of networks or systems it will be best implemented.

intrusion detection systems all of them have system requirement to implement the intrusion detection software. Therefore needs some platform for implementation. As we do have different platforms, we need a intrusion detection software which may be platform independent so that we can implement the same intrusion detection software on all the platforms.

4.5 Poor design

The design of all the intrusion detection systems are compact i.e if a user want to change some part of the intrusion detection system, we have to stop the intrusion detection system, then made the changes as desired and re-deploy it again. Hence the design of the intrusion detection system must be like as mentioned below [13]:

- It should have two parts, one core part which consists of detection algorithm and second part will be the part associated with pattern matching. This part should be updated on the fly. I.e it should not affect the detection process of the system but only updates the other parts without touching core part of the system. Thus every update should be added on the fly without stopping the intrusion detection system.

4.6 Testing and evaluation of IDS

As discussed in the paper, data is growing enormously and IDS has now become a standard for securing large network. Companies are investing huge amount in IDS technologies, but there is no such scientific methods to test the effectiveness of these IDS. Even though some quantitative measurable methods have been design to test the effectiveness, but they do not evaluate the effectiveness on same scale. These methods consider coverage or probability of false alarm or probability of detection or resistance to attacks directed at IDS or ability of handling bandwidth and traffic or ability to identify attacks etc. Hence are not sufficient enough to figure out effectiveness of IDS. Also there should be common scale for evaluating or testing the effectiveness of IDS. The different issues are as [14] [15]:

- Collecting script and victim softwares.
- Different requirements for testing different types of IDS.
- Testing with different parameters.

5. Theoretical Study of Different Intrusion Detection System.

Here in this paper, we have made an attempt to carry out the comparative study of different intrusion detection technique

Attacks Detected	What kind of attacks is detected by the system?

The comparative studies based on the parameters discussed in table 1 are shown in below mentioned table2 in details.

Table 2: Comparative analysis of Different intrusion detection techniques available on some selected parameters

Name	Type	Platform	License	Based On	Suitability	Attacks Detected
AIDE—Advanced Intrusion Detection Environment	HIDS	Linux 2.6, Solaris 10/ Open Solaris, FreeBSD2.2.8,3.4, UnixWare 7.0.1, BSDi 4.1, OpenBSD2.6,3.0, AIX 4.2, TRU64 4.0x, HP-UX 11i, Cygwin	Open Source	Rule Based	Suitable for checking integrity of file & directory, mainly useful for security purposes and can be used in small, medium, large scale organizations, is suitable in Linux and Unix based system	File & Integrity Checker
CSP Alert-Plus	HIDS	Windows	Commercial	Rule Based	Suitable for checking integrity of file & directory. Mainly useful for security purpose and can be used in large scale organizations	Intrusion, file and integrity checker
Snort	NIDS	Linux	Open Source	Rule based	Suitable for checking intrusion or attacks for large or small organizations	DOS & CGI (Common Gateway Interface) Attacks, Intrusion Attacks, port Scans, SMB (Server Message Block) probes layer3 and above attacks.
Bro	NIDS	LINUX	Open source	Pattern matching	Suitable for checking intrusion in the system for known attacks	Signature inspection method.
AAFID	NIDS	Windows NT, Linux, FreeBSD, Open BSD	Open source	Statistical based	Suitable for checking intrusion or attacks for large or small organizations	DOS, File System Attacks
DTK	HISD	Free BSD, Open BSD Linux, MAC OS	Open source	Statistical based	Works as a deception to attackers and is suitable in Linux and Unix based systems. It suits in single user environment.	Resources Exhaust, Port Scanning
ImSafe	NIDS	Free BSD, Open BSD Linux, MAC OS	Open source	Statistical based	Suitable for buffer overflow attacks and react in real time, for monitoring sequences of system calls, in Linux and Unix based platforms. It suits in small scale organization.	Buffer Overflow Attack

Host-S entry	HIDS	Linux, Free BSD	Open Source	Statistical based	Suitable for detecting login anomaly detection, trace suspicious user activity, monitors interactive login sessions, and reports or reacts in real time in Linux. It suits in environment where authentication and authorization is main concern.	Unknown user Logins, Suspicious User Activity, Suspicious login Domain

6. CONCLUSION AND FUTURE SCOPE

Intrusion detection is used for the purpose of securing the assets or information of a company. Companies are investing huge amount of money for securing their valuable assets or information. But there are number of issues and challenges present in today's intrusion detection system. In this paper, we are discussing the objectives behind using the intrusion detection system or in other words we can say we discuss the need of intrusion detection system. Also we discussed some important issues in current intrusion detection system, which needs to be addressed by research communities. We also provide a brief comparative study of different intrusion detection system based on some parameters. In future, we are going to mitigate some issues first by proposing theoretical model and then implement the same. Also we will make attempt to implement some of the techniques discussed in above table and make empirical analysis.

7. REFERENCES

[1] Abadeh, M. Saniee, Jafar Habibi, and Caro Lucas. "Intrusion detection using a fuzzy genetics-based learning algorithm." Journal of Network and Computer Applications 30.1 (2007): 414-428.

[2] Beigh, Bilal Maqbool, and M. A. Peer. "Intrusion Detection and Prevention System: Classification and Quick." (2011).

[3] Bilal maqbool and M.A.Peer "frame work for choosing best intrusion detection and prevention system for an organization " appears in the Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

[4] Mir, Suhail Qadir, S. M. K. Mehraj-ud-din Dar, and Bilal Maqbool Beig. "INFORMATION AVAILABILITY: COMPONENTS, THREATS AND PROTECTION MECHANISMS." Journal of Global Research in Computer Science Journal of Global Research in Computer Science 2.3 (2011).

[5] Bace, Rebecca, and Peter Mell. NIST special publication on intrusion detection systems. BOOZ-ALLEN AND HAMILTON INC MCLEAN VA, 2001.

[6] Garcia-Teodoro, Pedro, et al. "Anomaly-based network intrusion detection: Techniques, systems and challenges." computers & security 28.1 (2009): 18-28.

[7] Ning, Peng, and Sushil Jajodia. "Intrusion detection techniques." The Internet Encyclopedia (2003).

[8] Stiawan, Deris, Mohd Idris, and Abdullah Hanan Abdullah. "Classification of Habitual Activities in Behavior-based Network Detection." Journal of Computing 2.8 (2010): 1-7.

[9] Dantu, Ram, Prakash Kolan, and Joao Cangussu. "Network risk management using attacker profiling." Security and Communication Networks 2.1 (2009): 83-96.

[10] Beigh, Bilal Maqbool, et al. "Performance Evaluation of Pro-Active Routing Protocols with Fading Models: An Empirical Evaluation using Ns-2." International Journal of Engineering Science 3 (2011).

[11] Beigh, Bilal Maqbool, and M. A. Peer. "Performance evaluation of geographical routing protocols: An empirical study." Computer Communication and Informatics (ICCCI), 2012 International Conference on. IEEE, 2012.

[12] IDRIS, MOHD YAZID, KAMARULNIZAM ABU BAKAR, and ABDUL HANAN ABDULLAH. "INTRUSION PREVENTION SYSTEM: A SURVEY." (2005).

[13] Richharya, Vineet, et al. "Design of Trust Model For Efficient Cyber Attack Detection on Fuzzified Large Data using Data Mining techniques." IJRCCT 2.3 (2013): 126-130.

[14] Mell, Peter, et al. "An overview of issues in testing intrusion detection systems." (2003).

[15] Puketza, Nicholas J., et al. "A methodology for testing intrusion detection systems." Software Engineering, IEEE Transactions on 22.10 (1996): 719-729.

[16] Corona, Igino, Giorgio Giacinto, and Fabio Roli. "Adversarial Attacks against Intrusion Detection Systems: Taxonomy, Solutions and Open Issues." Information Sciences (2013).

[17] Hoque, Mohammad Sazzadul, et al. "An implementation of intrusion detection system using Genetic Algorithm." arXiv preprint arXiv:1204.1336 (2012).

[18] Kandeeban, S. Selvakani, and Rengan S. Rajesh. "Integrated Intrusion detection system using soft computing." International Journal of Network Security 10.2 (2010): 87-92