UACEE International Journal of Advances in Computer Networks and its Security – IJCNS
Volume 3 : Issue 2 [ISSN 2250 – 3757]
Publication Date : 05 June 2013

FRAMEWORK FOR CHOOSING BEST INTRUSION DETECTION AND PREVENTION SYSTEM FOR AN ORGANIZATION

Bilal Maqbool Beigh

Prof.Mushtaq Ahmad Peer.

Abstract*—In today's world, where every organization relay on computer systems and stores it's all critical information on the computer systems via online and off-line systems. Critical information is being sent via network. But in recent time's computer system are facing problems in the form of malicious data which can cause different problems such as denial of services, information theft, information lost etc. Till date many detection and prevention techniques are available in market, but how an organization will choose the best security policy for it remains a big issue for researchers and security professionals. In order to solve this issue we are devising a framework in terms of guidelines for choosing best intrusion detection system for your organization. The results of current research are very useful for educational purpose and organization who are interested in intrusion detection systems (IDSs).

Keywords:Intrusion, Malicious, Attack, challenge, critical, information, computer systems, network, denial of service, security, policy, guidelines.

I. Introduction

The tremendous growth in communication technology brings number of good things to human society, but it also makes us re-lay on information systems [1].As the information is increasing in digital format day by day, the vulnerabilities are also increasing in the form of cyber threats, attacks and mis-identification of trusted users. There are lots of intrusion attacks in today's digital world, According to recent survey by CERT/CC [2][3], the rate of intrusion attacks almost doubles every year. The Computer Emergency Response Team (CERT) reported 3734 incidents in 1998, 9859 in 1999 and 8836 in the first 6 months of 2000. In a recent audit of U.S. federal agencies by the GAO [7] investigators were able to pierce security at nearly every system they tested. The cause of these attacks are either complexity of the system itself or increasing number of hackers day by day or market competitors or software development companies itself etc. Therefore along with these tremendous opportunities for sharing important information and resource especially used for some critical operation like military , space, nuclear etc. It has become very much important to protect these special and important resources and information against such attacks [4]. For protecting the same, we have the concept called "Information security" thus we can say that information security is such area which protects our information / resources from theft or misuse. But still this field of research is in its infancy days. This research started in early 90's and so far little has been done in this field. This research field comprises of many subfield such as system side security, network side security etc. One subset of information security that has been the area of much more attention in recent years is intrusion detection system [4].Therefore intrusion detection system can be defined as the process of monitoring events occurring in a system and signaling responsible parties when interesting (suspicious) activity (compromises the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network) occurs [5]. At this instant of time, there are many intrusions detection systems available in market with different features and uses, but it is very difficult for a user or organization to choose best Intrusion detection system for him or for his organization [6]. As there is no such guideline provided by any agency/ organization to choose the security policy therefore there is a need of guidelines for the purpose.

In this paper, we will provide a brief introduction of different intrusion detection systems and then challenges and issues faced in intrusion detection system and finally will provide a framework for choosing best possible intrusion detection system for you and your organization. The distribution of the paper will be as Section II will discuss about different

Bilal Maqbool Beigh
University of Kashmir
India.
Bilal.beigh@gmail.com

Prof.M.A.Peer
General Admin. Department
Govt. of J&K , India
drpeerma@gmail.com

intrusion detection systems available and discuss them briefly, Section III will discuss issues and challenges faced will using intrusion detection systems, Section IV discusses the framework for choosing intrusion detection systems and in final section i.e. Section V conclusion will be there.

II. Intrusion Detection System?

Intrusion may be defined as a process of interrupting someone without permission or in terms of computers we can say that it is an act of attempting access to someone's system/computer without proper privileges [8]. In order to detect this unauthorized access to some one's resources, we have a concept called "Intrusion detection system". Thus intrusion detection system is a system through which we can monitor, detect and block or mitigate the attacks made on a particular network or system.

A. *ARCHITECTURE OF ID&PS.*

It is important to understand the processing or working of intrusion detection system. Generally the architecture of intrusion detection and prevention systems depends upon number of things starting from data gathering to actions taken on detection of intrusion. The general structure of intrusion detection and prevention systems is depicted in figure 1 below [9].

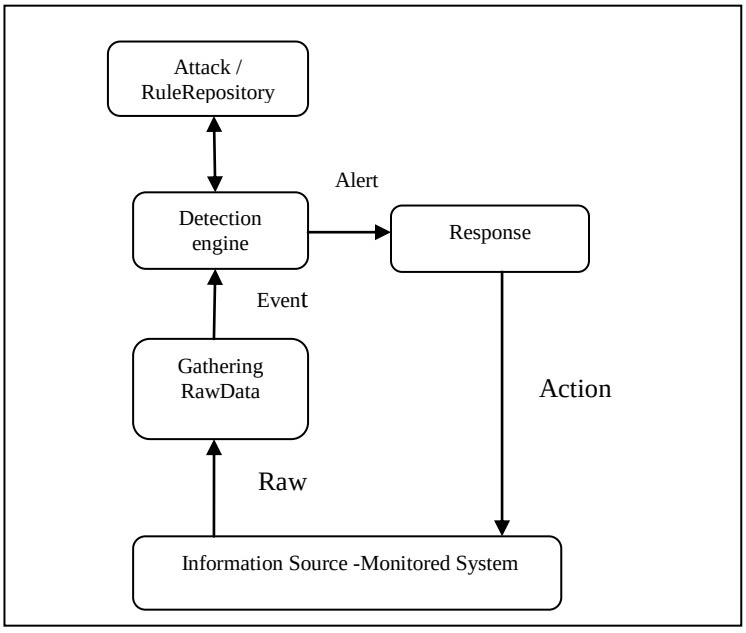

Figure 1: Basic Architecture of Intrusion detection and Prevention System.

- Gathering Raw Data- This is one of the basic step of intrusion detection system. The responsibility of this step is to gather the data from network or individual. Sensors are responsible for collecting the data from the monitored system.

- Detection engine-In this step, the intrusion detection system analyzes the collected data from sensors to identify the intrusion activity. This analysis is based on different algorithms used for the purpose.

- Repository-It contains knowledge base / data collected by different sensors, but in preprocessed format (e.g. knowledge base of attacks and their signatures, rules for attack signatures, filtered data, data profiles, etc.). This information is usually provided by network and security experts.

- Response-This step determines the action to be taken when an intrusion is detected. These responses can either be automated (active) or involve human interaction (inactive).

B. *Characteristics of ID&PS*

There are much desired characteristics for good intrusion detection system regardless of what mechanisms techniques it is based on. The characteristics which are enlisted for good intrusion detection systems as under [10][11][12]:

- The intrusion detection and prevention systems must run automatically and continuously without any manual effort. The system must be flexible enough, so that the ID&PS can be run in the background of other system applications.
- It should not be a "black box" as its internal working should be examinable from outside.
- The system (ID&PS) must be competent enough to sustain from different type of attacks thus must be dependable, robust and resistant towards the attacks and should have capability to recover fast from successful attacks and should provide security services from your system continuously.
- The ID&PS must make minimum overhead on the system.
- The accuracy characteristic of ID&PS is very important. For attaining this characteristics,

the intrusion detection and prevention system should satisfy two criteria:

- The system must identify intrusion correctly.
- The system must not identify normal traffic as intrusion.

- It must have the adaptability as the system technology is changing over rapidly.
- Finally the system (ID&PS) must not be difficult to implement.

C. *Intrusion Detection System Types:*

As discussed in the above sections intrusion detection systems are ment for security purpose, but it will not accomplish full security for an organization. In order to implement such security there are various types of intrusion detection systems available, as discussed under:

- Host Based Intrusion Detection System.
- Network Based Intrusion Detection System.
- Hybrid Based Intrusion Detection System.

Host Based Intrusion Detection System-- In this type of intrusion detection system, the attacks (unauthorized access, illicit and anomaly behavior) are detected at host level or on specific device on which intrusion detection system is installed. In other words, we can say that HIDS works with software agent at host. The modern day HIDS is actually derived from log analyzer .These types of IDS are applications running in the background of presumed critical, sensitive hosts, such as Mail Servers, DNS Servers, web servers, database servers, etc. [13].

Network Based Intrusion Detection System-- These type of intrusion detection system are platform independent i.e. they can be installed anywhere in the network depending upon to suitable position for acquiring maximum data/traffic for analyzing attacks/ intrusions on network. NIDS monitors multiple hosts by gaining access to network traffic through switch / hub. Sensor installed at different points captures all network traffic and analyze the contents of individual packets for malicious attacks [14].

Hybrid Based Intrusion Detection System-- In this type of intrusion detection system, the best features of different type of intrusion detection i.e. host based and network based intrusion detection systems are combined to give rise to a new type of intrusion detection system called hybrid intrusion detection system. The main motives behind developing these types of intrusion detection systems are getting better efficiency [14].

III. *Issues and Challenges in ID&PS.*

In IDS there are many issues and challenges which are yet to be resolved by the researchers and need some more attention towards the resolving of these issues and challenges. The issues and challenges which need attention are as under [15] [16]:

- The main motive behind the intrusion detection system are to analyze the data for some malicious or intrusion. While detecting for malicious data, there are chances that the system will detect the normal data as malicious i.e. false alarm. The challenge is to reduce the number of false alarms.

- As there are different types of intrusion detection systems available in the market but there are no guidelines available which will provide some procedure about choosing a particular intrusion detection system for his organization.

- No such intrusion detection system are designed that will detect all the intrusions correctly. There should be an attempt to integrate the best features of all the intrusion detection systems available in the market and make a full-fledged security model.

- There should be attempt towards making some updates in the data sets and rules for the same attacks, as during the test old data set and rules are used by researchers. So there is need for making new entry in the data set and rules already available (i.e. DARPA Data Set 1998 and 1990).

IV. Framework for Choosing Intrusion Detection System

Choosing an intrusion detection system is a delicate task, as the whole company security responsibility lies on the shoulders of the intrusion detection system i.e. to detect the attack made on the organization system, to mitigate them if possible or to alert the administrator about the attack happened [17]. Currently there are many intrusion detection systems available within the market but it is difficult to choose the best intrusion detection system for an organization. In order to choose the same, we have devised a

framework that will help an organization to choose the best intrusion detection and prevention system. The framework consists of steps and must be followed. The steps involved in choosing best intrusion detection are as:

- Risk Analysis.
- IDS Category.
- Free/ Commercial IDS.
- Platform dependencies.
- Deployment Issues.
- Cost Benefit Analysis.
- Detection Rate.
- Updates/ Patches available.

The steps above mentioned must be followed as shown in the diagram shown below to incorporate you to choose best ID&PS.

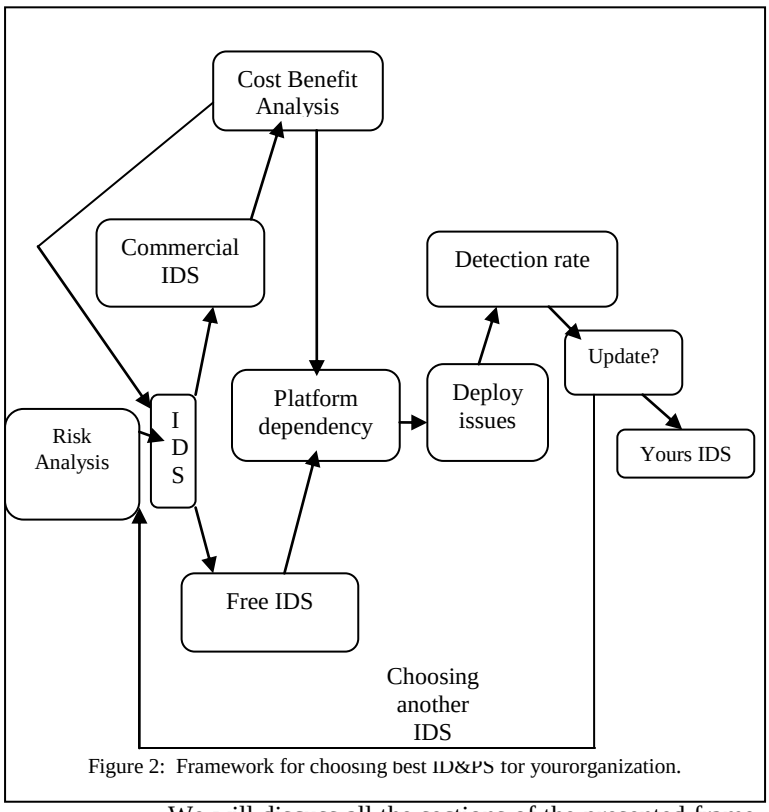

Figure 2: Framework for choosing best ID&PS for yourorganization.

We will discuss all the sections of the presented frame work in detail.

A. *Risk Analysis*

This step is the most important for choosing intrusion detection and prevention system for an organization. The risk analysis can be considered as a tool for risk management, which is helpful for identifying security issues i.e. vulnerabilities, threats and unauthorized access. As every security professional knows that dealing with securing the organization is very big task. In order to accomplish the same, the organizations have to make a team for risk assessment (Let Us call it RAG "Risk Assessment group) whose responsibility will be [18][19][20][21]:

- Identify important information of organization and their values for organizations,
- Identify different threats and vulnerabilities for the identified information/assets.

Identifying important information and their Values **–** Identifying the values of the organization's important information is the very first step for risk analysis. In this step the risk assessment group will point out / identify the most important assets of organization and will estimate the cost associated and damage resulted if some intrusion/ attack happed on an organization or we can say the group will analyze the loss made by losing the information to some other company. While identifying the assets following things must be kept in consideration.

- Cost of assets/ information that may be lost if intrusion happen.
- Role and usage of assets / information.

Identifying threats and Vulnerabilities **–**After pointing out the important information/assets, the responsibility of the group is to identify the vulnerabilities and threats for assets/ important information as identified in the prior step. Also they have to keep an order of threats i.e. which threat may damage/ theft more information according to the percentage of damage done by these threats and vulnerabilities.

Thus in general, the RAG will gather the following information.

Loss of assets / information in total at the initial stage, if not prevented and total threats and vulnerabilities that can cause these losses.

B. *Choosing an ID&PS*

Here in this frame work , step 2 to 6 are recursive process until the RAG will met the conditions laid down by them in risk analysis step. In this step the company/ security professionals assigned by organization will choose the type of ID&PS depending upon the requirement i.e host based, network based or hybrid intrusion detection and prevention system.

C. *Type of ID&PS*

In this step, the decision is up to the security professionals or organization whether they want to go with free ware or with commercial intrusion detection systems. But the criteria are that the selected intrusion detection and prevention system will at least fit for the requirement made by the RAG. This step wholly

depends on the choice of organization or security professionals.

D. Cost Benefit Analysis

After analyzing the risks of the organization, it is very important to perform cost benefit analysis. This is one of the most important factor in deciding to choose commercial intrusion detection system. The step of risk analysis will give a real cost associated with assets under threat. [22]Thus it will be a bit easier for the cost benefit analysis group to decide the final cost of assets and cost to be surfed for purchasing intrusion detection and prevention system to protect their assets. The cost benefit group consists of IT development, finance, budget and statistics [23][24]. They will put up all the analysis and will conclude with a decision to deploy the same intrusion detection system for his organization or they want to find out new. If the cost benefit group found that the ID&PS which they are currently analyzing is not up to the mark, they have to start again from step 2. But next time it will be easy to analyze the second or another intrusion detection system.

E. Platform and deployment Issues

After calculating and finalizing the cost for ID&PS, we have to check the issues of platform dependencies and deployment issues related to chosen ID&PS.i.e. the intrusion detection and prevention system shall be flexible enough in term of platform and deployment related matters. The intrusion detection and prevention system must run on any platform, if the organization changes the technology in future and must be easy to deploy.

F. Detection rate

This is the main point while choosing intrusion detection and prevention systems for any organization. In this step, the responsibility of security professional is to develop a detailed report about the detection rate, false positive alarm, false negative alarms and no detection. This step is very important in respect of the assets / information to be secure. The main criteria for choosing the ID&PS on rate are as

- There should be high detection rate while analyzing the traffic for attack. This process is very important while securing the assets/ information.
- There should be less alarm while detecting right/ normal traffic as intrusion or attack.
- The system must detect most of the malicious traffic.

If the criteria above discussed does not met the best practice then it has to be done in recursive manner again starting from step 2.

G. Update?

The organization needs to check whether patches or new updates in terms of rules for attack detection etc are readily available or not. If such updates are provided by some agencies, at what cost they will provide the same .If not what will be the development / maintenance cost,if organization will develop itself.

If all the criteria are matched enough, so that the organization is well satisfied by the matches. Then thisis the best intrusion detection and prevention system for your organization.

V. Conclusion

The current research is focused on the research so far done on framework for choosing ID&PS, challenges and Issues in ID&PS. As discussed above, choosing intrusion detection and prevention system is a very tough job. In this paper, we have given a framework for choosing best intrusion detection system for an organization. The framework is the form of flowdiagram, when followed strictly will yield a solution for choosing best intrusion detection and prevention system for an organization. The steps mentioned in framework appears to be a simple exercise but are basically important/ critical steps for getting best of ID&PS for an organization . But ultimately the choice depends upon company. Also in future we will make an attempt for providing standard benchmark for intrusion detection and prevention systems.

Acknowledgment

I would like to thank my mentor, my guide Prof.M.A.Peer for his valuable support and suggestions. Also I would like to thank head of department Dr.S.M.K.Quadri for supporting me during this research work. Last but not least, I would be very much thankful to my family and friends who stood beside me at every time.

References

[1] SAKURAI, Kouichi, and Tai-hoon Kim. "A Trend in IDS researches." 보안공학연구논문지제권제호년월 (Journal of Security Engineering) 5, no. 4 (2008): 8. http://www.sersc.org/journals/JSE/vol5_no4_2008/3.pdf

[2] Lazarevic, A., Ertoz, L., Kumar, V., Ozgur, A., & Srivastava, J. (2003, May). A comparative study of anomaly detection schemes in network intrusion detection. In Proceedings of the third SIAM international conference on data mining (Vol. 3, pp. 25-36). Society for Industrial & Applied.

[3] Successful Real-Time Security Monitoring, Riptech Inc. white paper, September 2001.

[4] Brown, Douglas J., Bill Suckow, and Tianqiu Wang. "A Survey of Intrusion Detection Systems." *Department of Computer Science, University of California, San Diego* (2002).

[5] Grandison, Tyrone, and Evimaria Terzi. "Intrusion Detection Technology." (2007).

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

[7] Escamilla, T. "Intrusion Detection: Network Security Beyond the Firewall." John Wiley and Sons, 1998.

[8] Anderson, James P. *Computer security threat monitoring and surveillance*. Vol. 17. Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, 1980.

[9] Lazarevic, Aleksandar, Vipin Kumar, and Jaideep Srivastava. "Intrusion detection: A survey." *Managing Cyber Threats* (2005): 19-78.

[10] H. Debar, M. Dacier and A. Wespi, Towards a Taxonomy of Intrusion Detection Systems, Computer Networks, vol. 31, 8, pp. 805-822, 1999.

[11] P.A. Porras and A. Valdes, Live Traffic Analysis of TCP/IP Gateways, In Proceedingsof the ISOC Symposium on Network and Distributed System Security (NDSS'98), San Diego, CA, March 1998.

[12] F. Provost and T. Fawcett, Robust Classification for Imprecise Environments, Machine Learning, vol. 42, 3, pp. 203-231, 2001.

[13] OSSEC (Observing System Science Executive Council) OSS. Homepage of ossec, 2011. http://www.ossec.net/. Online; accessed: 28.1.2013.

[14] Peter Scarfone, Karen; Mell. Guide to intrusion detection and prevention systems (idps). Computer Security Resource Center (National Institute of Standards and Technology), January 2010.

[15] Om, Hari, and Aritra Kundu. "A hybrid system for reducing the false alarm rate of anomaly intrusion detection system." *Recent Advances in Information Technology (RAIT), 2012 1st International Conference on*. IEEE, 2012.

[16] Wu, Shelly Xiaonan, and Wolfgang Banzhaf. "The use of computational intelligence in intrusion detection systems: A review." *Applied Soft Computing* 10.1 (2010): 1-35.

[17] Mathew, Dennis. "Choosing an intrusion detection system that best suits your organization." *GSEC Practical v1. 4b, available at: www. sans. org/reading_room/whitepapers/detection* (2002).

[18] Huang, Yi-an, and Wenke Lee. "A cooperative intrusion detection system for ad hoc networks." Workshop on Security of ad hoc and Sensor Networks: Proceedings of the 1 st ACM workshop on Security of ad hoc and sensor networks. Vol. 2003. 2003.

[19] Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. "A model for evaluating IT security investments." *Communications of the ACM* 47.7 (2004): 87-92.

[20] Banerjee, Usha, and K. V. Arya. "Optimizing Operating Cost of an Intrusion Detection System." (2013).

[21] Cohen, Gideon, Moshe Meiseles, and Eran Reshef. "System and method for risk detection and analysis in a computer network." U.S. Patent No. 8,099,760. 17 Jan. 2012.

[22] Alsubhi, K., et al. "Security configuration management in intrusion detection and prevention systems." *International Journal of Security and Networks* 7.1 (2012): 30-39.

[23] de Vries, J. A., et al. "An analysis framework to aid in designing advanced persistent threat detection systems." (2012).

[24] Kommineni, Kiran Kumar, and Adimulam Yesu Babu. "A Cost-Benefit Model for an Enterprise Information Security."

Bilal Maqbool Beigh has completed his master's with distinction from Pune university. He has completed his M.Phil. From Kashmir University in 2012 and now he is pursuing his Ph.D. from University of Kashmir. He has published more than 15 papers in national and international journals and conferences. His area of research is information security.