Oriental Journal of Computer Science & Technology Vol. **2**(1), 69-74 (2009)

Techniques of Wireless Intrusion Detection System: T-WIDZ

RAJSHEKHAR M. PATIL[1], MAMITHA R. PATIL[2] and K. V. RAMAKRISHNAN[3]

[1]Computer Science and Engineering Department,
[2]BHSFGC Vijaya College, Bangalore, (India).
[3]Department of Electronics and Communication, CMRIT, Bangalore (India).

(Received: February 10, 2009; Accepted: April 30, 2009)

ABSTRACT

Recently data mining methods have gained importance in addressing network security issues, including network intrusion detection-a challenging task in network security. Intrusion detection systems aim to identify attacks with a high detection rate and a low false alarm rate.

Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS) in computer network security are real-time software assessment by monitoring for suspicious activity at the network and system layer. Software scanner allows network administrator to audit the network for vulnerabilities and thus securing potential holes before attackers take advantage them.

The network traffic datasets provided by the DARPA 1998 offline intrusion detection project are used in our empirical investigation, which demonstrates the feasibility and promise of unsupervised learning methods for network intrusion detection using UML diagrams. The goal of this paper is to place some characteristics of good IDS and examine the positioning of intrusion detection as part of an overall layered security strategy and a review of evaluation criteria for identifying and selecting IDS.

Keywords: IDS- Intrusion Detection System, IPS-Intrusion Prevention Systems, WIDZ- Wireless Intrusion Detecting System.

INTRODUCTION

Information held by IT products or systems is a critical resource that enables organizations to succeed in their mission. Additionally, individuals have a reasonable expectation that their personal information contained in IT products or systems remain private be available to them as needed, and not be subject to unauthorized modification[1].

It is very important that the security mechanisms of a system are designed to prevent unauthorized access of a system are designed to prevent unauthorized access to system resources and data. However, completely preventing of security appears, at present, unrealistic. However, we can try to detect these intrusion attempts so that action may be taken to repair the damage now or later. This field of research is called Intrusion Detection. The goal of an Intrusion Detection System are designed to prevent unauthorized resources or services. File Integrity Analyzers (FIAs) are a class of related tools that automatically verify the content of security-critical files frequently referred to as tripwires, they attempt to detect if files have been modified in unauthorized ways. Once suspicious modifications are detected by triggering the tripwire, the analyzer may alert a security administrator or invoke some type of automated response. There are two ways to handle subversion attempts one way is to prevent subversion itself by building a completely secure system[4]. Network administrator could, for example, require all users to identify and authenticate themselves; administrator could protect data by various cryptographic methods and very tight access control mechanisms. However this is not really feasible because:

1. In practice, it is not possible to build a completely secure system because 2 Bug

free software is still a dream. No one wants to make the effort to try to develop. In addition, designing and implementing a totally secure system is thus an extremely difficult task.

2. The vastly installed base of systems worldwide guarantees that any transition to a secure system (if it is ever developed) will be long incoming.
3. Cryptographic methods have their own problems. Passwords can be cracked, users can lose their passwords, and entire crypt systems can be broken.
4. Ever a truly secure system is vulnerable to abuse by insiders who abuse their privileges. We thus see that we are stuck with systems that have vulnerabilities for a while to come. An IDS does not usually take preventive measures when an attack is detected, it is a reactive rather than pro-active agent[5,6]. It plays the role of information rather than a police officer.

It is thus more important than ever before that since it seems obvious that administrators cannot prevent subversion, they should at least try to detect it and prevent similar attacks in the future. An IDS requires human intervention and specialized training to implement the proper remediation behavior. These shortcomings limit the effectiveness of IDS solutions as the first line of security defense.

The paper is organized as follows: Section 2 presents some definitions and technical details related to the intrusion detection systems. Section 3 introduces the classification of intrusion detection. Section 4 emphasizes on some attack against intrusion detection systems. Section 5 presents intrusion detection system character discussion about good characteristics. Section 6 includes the summary and conclusion of that work.

Intrusion Detection Systems

IDS are the process of detecting and identifying unauthorized or unusual activity is also defined as the process of evaluating suspicious on the system. ID is also defined as the process of evaluating suspicious activity that occurs in corporate network.

Concepts

By using the audit records, the intrusion detection system should identify any undesirable activity. Such a scheme requires specification of what constitutes an undesirable activity and a means of automatically detecting such activity as it occurs. For example, consider a sales agent who logs into the data base during office time and odd time to maintain his record.

Design

Intrusion detection design consists of two basic steps. The first step is the creation of audit records. The second step is checking the audit log against the intrusion thresholds. Finally, the system administrator or investigators to generate an intrusion detection report for review potential IDS.

Classification of Intrusion Detection System

According to its assumptions and components IDS is classified as follows Fig. 1:

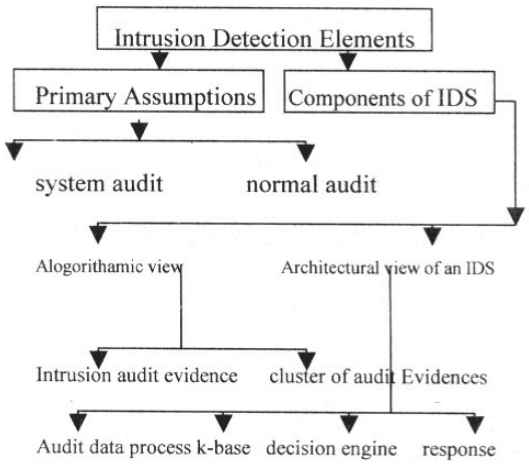

Fig. 1: Tiny parts of an intrusion detection system

IDS components are classified from an algorithmic perspective and from a system architecture perspective point of views as shown in figure 2 using UML diagram. IDS are classified into features algorithms, which capture intrusion evidences, and models algorithms, which collect piece evidences together. IDS components from system architecture perspective may consist of audit

data processor, knowledge base, decision engine, alarm generation and responses.

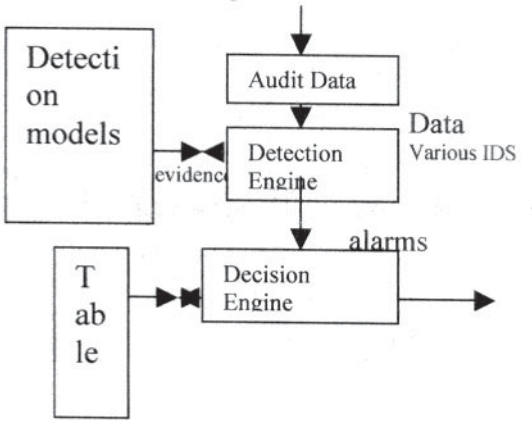

Fig. 2

Also, IDS that monitor computer systems and networks, analyze them for signs of security policy violation and respond accordingly, is based on one of the following approaches:

1. Anomaly detection systems.
2. Misuse detection systems.

Anomaly detection systems

Anomaly detection (Sub) systems flag observed activities that deviate significantly from the established normal usage profiles as anomalies, i.e., possible intrusions. For example, the normal profile of a user may contain the averaged frequencies of some system commands used in his or her login sessions. If for a session that is being monitored the frequencies are significantly lower or higher, then an anomaly alarm will be raised. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions.

Misuse detection systems

Misuse detection systems use patterns of well-known attacks or weak spots of the system to match and identify known intrusions. For example, a signature rule for the guessing password attack can be there are more than 4 failed login within 2 minutes the main advantage of misuse detection is that it can accurately and efficiently detect instances of known attacks. The main disadvantage is that it lacks the ability to detect the truly innovative (i.e., newly invented) attacks. The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected[6]. This means that these systems are not unlike virus detection systems, they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods.

An interesting point to note is that anomaly detection systems try to detect the complement of bad behavior but misuse detection systems try to recognize known bad behavior. These main issues in misuse detection that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activity.

Attacks against IDS

An attacker targeting a network IDS has many Potential objectives. The most likely of these is simply to attack a machine that the IDS are watching without the IDS noticing it, any of the attacks system may allow an attacker to do this. Another possible goal is to spoof attacks from fake addresses, framing other people for attacks. An attacker can also create fake attacks in order to trigger a reaction from the IDS, causing it to cut network connectivity for a legitimate service.

Table 1: Advantages and disadvantages of misuse detection systems

Advantages	Disadvantages
High detection accuracy	Building the signatures rules base is a difficult and a time consuming process.
Very low false alarm rate	They cannot detect Unknown intrusion.

We outline here three different attacks that can be employed by an attacker to compromise a network IDS. The first two aim to reduce the accuracy of the system, causing it to see something other than what is actually happening on the network. The third tries to completely disable the IDS.

Wireless Intrusion Detection

The networking basic defenses deployed and maintained, technical teams can shift their attention to the subject of defending the network from attacks. Attacks can come in a variety of forms, and in many cases can even be unintentional. Wireless LANs by their very nature provide a way of accessing the network through walls and physical barriers that normally protect business assets. Add this to the fact that most WLANs are not properly secured, and it is no wonder that an intruder would look to the wireless network as the ideal place to begin an attack[16]. For several years now the industry has been developing hardware and software to support the 802.11 environment. The Wired Equivalent Privacy (WEP) protocol, 64 bit encryption, was introduced with a number of flaws in its security mechanisms and industry took a hard look at implementation of wireless environment based on the fears associated with the security flaws. The WEP protocol is being replaced by the new WPA (Wi-Fi Protected Access), 128-bit encryption security standard introduced last year. Additionally, a number of companies began to produce products to assist in overcoming the flaws inherent in WEP and to define standards for implementation and use of wireless tools to support the secure day-to-day business of large and small organizations. The Wi-Fi alliance provides a list of products that have been released with the WPA standard several that provide alternative security solutions like VPN and other mobile security measures and there are several other tools which meet the criteria established by the FIPS 140-1 and 140-2 guidelines for encryption and are discussed in brief in this article.

Rogue Problem Experimental

The problem of rogue access points has garnered more attention in the industry than any other security issue, and for good reason. A rogue access point is any access point in your network that was intentionally deployed by your network staff. They can come from well-meaning employees who bring in devices from home, they can be devices used by attackers for malicious purposes, or they can be neighboring devices that simply overlap with your wireless network. These devices can have may effects and none of them are good in terms of network security. The most common rogue AP scenario involves devices introduced by employees. In this case, the employee brings in an unsecured access point, plugs it in to an available wired port and now has wireless access to the larger wired network. Unfortunately, so does anyone else within range of the access point including the wireless lurker in the parking lot. This provides virtually unchecked access to the entire enterprise network (Fig. 3).

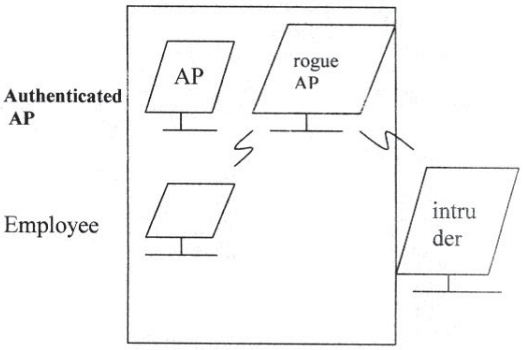

Fig. 3: Unsecured rogue access point allows anyone to connect to the network[10]

RESULT AND DISCUSSION

IDS Characteristics

The beginning of making the most of an investment starts with the right investment. In this environment of savvy marketing and thickly fielded markets, is can be difficult to analyze and compare performance metrics. The greater challenge could be making sure that the metrics being proposed are valid. The most popular metric for IDS is the number of packets dropped- or how many packets the IDS was not able to analyze. But, that is not the reason An IDS is built or purchased. If routers and firewalls, being inline devices, drop packets, they block traffic, and for these devices, the metric is

appropriate. IDS cannot be categorized with routers and firewalls because it is radically different in the following two ways:

1. IDSs are passive devices and connect to the network with a bTQ connection so it cannot block traffic.
2. IDSs are not access control devices so dropped packets cannot result in blocked transmissions.

The key to using the right metric is being certain about what your are buying the IDS to do. The goal of the IDS is to correctly identify an attack regardless of the complexities of network saturation. The correct metric for IDS is battack detection Q at varying levels of network saturation, for 10 Mbs, 100 Mbs, and Gigabit segments also from wired network to wireless network. Testing og IDS algorithms can be performed either in a real environment or in an experimental environment. The advantages and disadvantages of each method are discussed below.

CONCLUSION

Undoubtedly, network attacks present a serious problem in the field of information technology and challenge its rate of growth and wide acceptance by the public government and businesses. In this paper, we tried to achieve a clear view of the IDS and attacks against it. Having this clear view of the problem, our thinking is clarified and this way we can find effective solutions to IDS problems. These core problems lead to the existence of three attacks that can be used against a network IDS insertion attacks, evasion attacks and complex attacks, which allow an attacker to fool the IDS into incorrectly reconstructing information from network packets, and denial-of-service attacks, which can be exploited to stop the IDS from working outright. In the next section of this paper, the system must take a look at each of these attacks, and present examples that real ID systems are vulnerable today. One great advantage of the development of IDS classifications is that effective communication and cooperation between researchers can be achieved so that additional weaknesses of the IDS field can be identified. These classifications need to be continuously updated and expanded as new attacks signatures, behaviors and defense mechanisms are discovered.

Their value in achieving further research and discussion is undoubtedly large. A next step in this path would be to create sets of characteristics of good IDS so that good IDS can be compared and evaluated. To maximize the value of IDS, a proper foundation needs to be laid including choosing the right metrics for product evaluation and success. Equally important is creating a policy that clearly identifies what the enterprise is trying to accomplish with IDS so that the right devices may be deployed in the right scenario to achieve the goal. According to this work, we addressed important issues in order to recognize good characteristics of IDS, regardless of what mechanism it is based on. With this, we hope to improve the capabilities for detecting attacks against both host and network resources.

ACKNOWLEDGEMENTS

The authors are grateful to Richar Lippmann and Daniel Barbara for providing data sets. This work is being supported by Oracle data Computing Research Center. The content of the work does not necessarily reflect the position or policy of the government and no official endorsement should be inferred. Access to official facilities was provided by GGITM Bhopal, MGR Research Center Chennai and Dean E. and C., Department CMRIT, Bangalore, Dr. K.V. Ramkrishnan.

REFERENCES

1. Han, J., Kamber, M.: Data Mining: Concepts and Techniques. Morgan Kaufmann Publishers, San Francisco (2000).
2. Olson, C.F.: Parallel Algorithms for Hierarchical Clustering. *Parallel Computing,* **21:** 1313-1325 (1995).
3. Dahlhaus, E.: Parallel Algorithms for Hierarchical Clustering and Applications to

Split Decomposition and Parity Graph Recognition, *Journal of Algorithms* **36:** 205-240 (2000).

4. Rajasekaran, S.: Efficient Parallel Hierarchical Clustering Algorithms. *IEEE transactions on parallel and distributed systems* **16**(6): 497-502 (2005).
5. Rasmussen, E.M., Willett, P.: Efficiency of hierarchic agglomerative clustering using the ICL Distributed Array Processor, *Journal of Documentation*, **45:** 1-24 (1989).
6. Li, X., Fang, Z: Parallel Clustering Algorithms, *Parallel Computing* **11:** 275-290 (1989).
7. Li, X.: Parallel Algorithms for Hierarchical Clustering and Clustering Validity, IEEE Trans, Pattern Analysis and Machine Intelligence 12: 1088-1092. An adaptive Parallel Hierarchical Clustering Algorithm 107 (1990).
8. Tsai, H.R., Horng, S.J., Lee, S.S., Tsai, S.S., Kao, T.W.: Parallel Hierarchical Clustering Algorithms on Processor Arrays with a Reconfigurable Bus System. *Pattern Recognition* **30:** 801-815 (1997).
9. Akl, S.G.: Optimal parallel merging and sorting without memory conflicts. *IEEE Trans, Comput,* **36**(11): 1397-1369 (1987).
10. Chen, G.: Design and analysis of parallel algorithm, Higher education press, Beijing (2002).
11. Datta, A., Soundaralakshmi, S.: Fast Parallel Algorithm for Distance Transform. IEEE Transactions on Systems, *Man, and Cybernetics,* **33**(5): 429-434 (2003).
12. Akl, S.G.: An adaptive and cost-optimal parallel algorithm for minimum spanning trees, *Computing* **3:** 271-277 (1986).
13. Li, K.L., Li, Q.H., Li, R.F.: Optimal parallel algorithm for the knapsack problem without memory conflicts. *Journal of Computer Science and Technology* **19**(6): 760-768 (2004).
14. Jun, M., Shaohan, M.: Efficient Parallel Algorithms for Some Graph Theory Problems, *Journal of Compt. Sci. and Technol.* **8**(4): 362-366 (1993).
15. Nath, D., Maheshwari, S.N.: Parallel algorithms for the connected components and minimal spanning tree problems, *Inf. Proc. Lett,* **14**(1): 7-11 (1982).
16. Chong, K.W., Han, Y.J.: Concurrent Threads and Optimal Parallel minimum Spanning Trees Algorithm, *Journal of the ACM* **48**(2): 297-323 (2001).