Current Design Trends in Intrusion Detection System: A Review on Technologies Implemented by Researchers

Parvathi Devi.Karumanchi [1], Y.A.Siva Prasad[2], Navya Dhulipalla[3]

Department of computer science and engineering, KL University
Green Fields, Vaddeswaram, Guntur
[1]parvathidevik@hotmail.com
[2]sivaprasady@gmail.com
[3]navya.dhulipala@gmail.com

Abstract— An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies distrustful patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. With modern advances in network based technology and increased reliability of our everyday life on this technology, assuring reliable operation of network based systems is very important. During recent years, number of attacks on networks has significantly increased and leads to an interest in network intrusion detection among the researchers. This paper provides a review on some current design trends of IDS together with a study on technologies implemented by some researchers in this research area.

Keywords— Intrusion detection, IDS design, False Positive (FP).

I. INTRODUCTION

In the past two decades with the rapid progress in the Internet based technology, new application areas for computer network have emerged. At the same time, wide spread progress in the Local Area Network (LAN) and Wide Area Network (WAN) application areas in business, financial, industry, security and healthcare sectors made us more dependent on the computer networks. All of these application areas made the network an attractive target for the abuse and a big vulnerability for the community. A fun to do job or a challenge to win action for some people became a nightmare for the others. In many cases malicious acts made this nightmare to become a reality. One of the major concerns is to make sure that in case of an intrusion attempt, the system is able to detect and to report it. Once the detection is reliable, next step would be to protect the network (response). In other words, the IDS system will be upgraded to an Intrusion Detection and Response System (IDRS). However, no part of the IDS is currently at a fully reliable level. Even though researchers are concurrently engaged in working on both detection and respond sides of the system. A major problem in the IDS is the guarantee for the intrusion detection. This is the reason why in many cases IDSs are used together with a human expert. In this way, IDS is actually helping the network security officer and it is not reliable enough to be trusted on its own. The reason is the inability of IDS systems to detect the new or altered attack patterns. Although the latest generation of the detection techniques has significantly improved the detection rate, still there is a long way to go.

A. Intrusion Detection

The first step in securing a networked system is to detect the attack. Even if the system cannot prevent the intruder from getting into the system, noticing the intrusion will provide the security officer with valuable information. The Intrusion Detection (ID) can be considered to be the first line of defense for any security system. Some of the researchers are more interested in applying rule based methods to detect the intrusion. Data mining using the association rule is also one of the approaches used by some researchers to solve the intrusion detection problem. Researchers such as Barbara et al. [1, 2], Yoshido [3] and Lee et al. [4] have used these methods. Others have proposed application of the fuzzy logic concept into the intrusion detection problem area. Works reported by Dickerson et al. [5], Bridges et al. [6] and Botha et al. [7] are examples of those researchers that follow this approach. Some researchers even used a multidisciplinary approach, for example, Gomez et al. [8] have combined fuzzy logic, genetic algorithm and association rule techniques in their work. Cho [9] reports a work where fuzzy logic and Hidden Markov Model (HMM) have been deployed together to detect intrusions. In this approach HMM is used for the dimensionality reduction. Due to its nature, the data mining approach is widely appreciated in this field of research. Some researchers have tried to use the Bayesian methodology to solve the intrusion detection problem. The main idea behind this approach is the unique feature of the Bayesian methodology. For a given consequence, using the probability calculations Bayesian methodology can move back in time and find the cause of the events. This feature is suitable for finding the reason for a particular anomaly in the network behavior. Using Bayesian algorithm, system can somehow move back in time and find the cause for the events. This algorithm is sometimes used for the clustering purposes as well. Reported works from researchers such as

Bulatovic et al. [10], Barbara et al. [11] and Bilodeau et al. [12] are examples of this approach. Although using the Bayesian for the intrusion detection or intruder behavior prediction can be very appealing, however, there are some issues that one should be concerned about them. Since the accuracy of this method is dependent on certain presumptions, distancing from those presumptions will decrease its accuracy. Usually these presumptions are based on the behavioral model of the target system. Selecting an inaccurate model may lead to an inaccurate detection system. Therefore, selecting an accurate model is the first step towards solving the problem. Unfortunately due to the complexity of the behavioral model within this system finding such a model is a very difficult task.

B. Data mining approach for IDS

In the data mining approach, Lee et al. [13] report a work based on data mining concept where initially two main usual classes of IDS are described and compared. Later, authors have explained their way of solving problems with the system and bringing it up to where it is now. Their approach is a rule-based approach (using machine learning techniques). In the report [14] authors say: “Anomaly detection is about establishing the normal usage patterns from the audit data”. Their viewpoint seems to be the following: Anomaly detection is to detect any known anomaly (or a famous anomaly pattern) in the network. However, we are not necessarily agreed with them on the known anomaly or the signature based approach and would rather to use any automatically detected intrusive anomaly detection approach. Adaptability of their reported system requires that someone always keep the system rule sets up to date. It could be a big challenge to include an automated adaptation feature in the IDS.

II.DESIGN TRENDS IN IDS

Before getting started with describing trends in the IDS design, it should be noted that IDS has a classifier kernel. The kernel of the IDS is responsible for classifying the acquired features into two groups namely normal and anomaly, where the anomaly pattern is likely to be an attack. Nevertheless, there are occasions where a legitimate use of the network resources may lead to a positive classification result for the anomaly or signature based intrusion detection. As a result of this wrong classification, IDS will wrongly raise the alarm and will signal an attack. This is a common problem with the IDS and is called False Positive (FP). One of the parameters to measure the quality of IDS is the number of its FP alarms. The smaller is the number of false positives, the better is the IDS.

A. Signature Based, Anomaly Based and Specification Based IDS

Signature based intrusion detection (misuse detection) is one of the commonly used and yet accurate methods of intrusion detection. Once a new attack is launched, the attack pattern is carefully studied and a signature is defined for it. The signature can be a name (in characters) within the body of the attack code, the targeted resources during the attack or the way these resources are targeted (attack pattern). Studying the attack pattern, security specialists can design a defense against that attack. Later on, using the proposed defense method, the IDS is updated accordingly to recognize the new attack patterns and to response to them. This approach is very efficient for the known attacks and produces small number of FP alarms. However, as the main short coming of this approach, it is not capable of detecting novel attacks. Once the attack pattern is slightly altered, this approach will not detect the altered versions of the old attacks. Thus, this approach is only efficient in detecting previously known attacks. There is another approach for detecting the novel and unseen attacks that follows. Another widely used ID method is the anomaly detection approach [15, 16]. The basic idea behind this approach is to learn the usual behavioral pattern of the network. Consequently the attack is suspected (detected) once the network behaves out of its regular way(Anomaly). However, network regular behavior is not similar for different networks. The network behavior is dependent on the date or the working conditions in the organization where the network is installed. The regular behavior model for the network can be variable. Considering these working conditions, the degree of freedom for the problem is large. One way to solve this problem is to make the IDS adaptable to the network environment where it is going to be installed. To do so, IDS will start to monitor and record the network behavior just after its deployment. Assuming the recorded pattern as the regular pattern for the network, IDS will use it as the normal behavior of the network and will set a baseline. Once the network pattern deviates from this baseline pattern by more than a threshold value, it denotes an anomaly. As it was mentioned earlier, not every anomaly indicates an intrusion. This is especially true in this case, where the system is very dynamic. Thus, it is not clear if the detected anomaly should be assumed to be an intrusion or not.

As a direct result of this uncertainty, anomaly based IDS will produce high FP alarms. As a remedy to this problem there should be a pruning system to detect FP alarms and cancel them. Keeping this shortcoming in mind this approach has a big benefit, that is, it is capable of detecting novel attacks or new releases of the old attacks .One of the problems in this field of research is finding either the right features or the right relation between certain features to monitor. May be sometime in future, the anomaly detection methodology becomes mature enough not to require a baseline anymore. Currently many commercial ID systems use a hybrid approach where anomaly based intrusion detection is used together with the signature based intrusion detection method. Using the signature based ID methods system can accurately identify the Known attacks with low FP alarms. If any unknown intrusions occur then anomaly detection based ID methods can detect the intrusion and raise the alarm. Using the anomaly detection based ID, the signature based methods can also be used to refine the FP alarms raised by this method. This approach will result in increasing the accuracy and reliability of the IDS while keeping the number of FP alarms low. A recently introduced approach is the specification based intrusion detection approach. Some reported works emphasize only on the signature (misuse) based and anomaly based intrusion detection approaches [5, 9]. However, there are others who talk about all three of the approaches. The specification constraint in this approach is used for reducing the number of FP alarms [18, 17]. Implementation of the anomaly based IDS requires in depth knowledge of the system. The specification constraints are extracted by the human expert manually. Although specifying critical resources of the system and their utilization may improve the security, there might always be some points missing in this process that may affect the system utilization. Specification based is not just applicable to the host systems but they can also be applied on the users as well. A legitimate user is expected to behave in a certain way, or it can be specific that a user should behave in this manner. This decision will improve the security but with the expense of a less attractive user interface. Limiting the user actions and freedom may lead to making the application look less appealing to some users. It is expected to get better results by applying specification based ID methods on the system itself.

B. Network Based IDS and Host Based IDS

As it was mentioned earlier in the introduction section of this article, network based and host based systems are two categories of the IDSs. The network based IDS is responsible to protect the entire environment of the network from the intrusion. This task asks for full knowledge of the system status and monitoring both the components of the network and the transactions between them. Agent technology plays a key role in this strategy. Network is the infrastructure for a distributed system. Therefore, agents are a natural choice for this approach. Collecting information within the network and processing them, responding to the requests and commands of the kernel of the IDS or working as an individual, all can be accomplished using agent based technology. The network based IDS is capable of accessing the network routers and instructing them to perform tasks. Using this feature, system can ask the router to disconnect a terminal or a subnet that has become a security threat.

In a paper by Luo et al. [19] a new Mobile Agent Distributed IDS (MADIDS) has been introduced. Paper reports that one of the main goals of the system is to improve the performance of the IDS in regard to speed and network traffic. MADIDS consist of four parts: Event Generation Agent, Event Analysis Agent, Event Tracking Agent and Agent server. Data is transferred by the Generalized Intrusion Detection Object (GIDO). Event generators are responsible for collecting data and converting them to the appropriate format. Event analyzers are responsible for analyzing the events and generating GIDOs. Response units will process GIDOs. Events and GIDOs are store in event servers (databases). Distributed computing on different computers will significantly improve MADIDSs processing performance.

The host based IDS is only installed on a single host/terminal and is responsible for monitoring the status of that terminal/server only. This type of IDS is responsible for the security of its host and will monitor all the network activities in that host [20]. One of the problems with the host based IDS is the high processing overhead that they impose on their host. This overhead wills slowdown the host and therefore it is not welcomed. This approach is quite popular among the researchers.

C.Different Approaches to IDS Design

Active IDS will provide a predefined response to the detected intrusions. The passive IDS is only responsible for monitoring the system and to inform the administrator once an intrusion occurs or to produce an advance warning. The response concept is related to the active IDS. This response can be a reaction to a security breach in the system or a preemptive response to avoid a security breach. One of the main goals of any active IDS is to prevent the security breach and not just to respond to the threat.

Continuing their earlier work [21], Cabrera et al. [22] report a more advanced work where the feasibility of their approach is studied. Authors use the Simple Network Management Protocol (SNMP) to build an IDS system. In this report, authors report that the idea of proactive IDS is about predicting the intrusion attack before it actually reaches to its final stage. Proactive IDS is a system that reacts to the imposed threats, and in response it will apply predefined defensive routines within the system.

There are two types of product lines in the commercial IDS industry. In one type of production, the IDS is
Produced in the form of a software package. In order to protect a host, the IDS software has to be installed on that host. Once the IDS is installed, it will access the network modules/ports of that host and will gain control over them. Later on, using its control over the system, IDS will monitor the network transactions and will respond to the threats. Although it can be used for the distributed IDS as well, this approach is more suitable for the host based IDS than the network based IDS.

However, industry has shown a great interest in another approach as well. In this approach, the whole IDS product is included in one box (IDS appliance). Both the hardware and the software modules are inside that box. Other hosts/servers can communicate with the IDS using the network infrastructure. Network administrator can update the IDS with new policies using a terminal with a network connection. Products from companies such as CISCO (CISCI IDS Sensors) and Mazu (Mazu Enforcer) are examples of this type of approach.

The reason for the IDS appliance approach being attractive to the market and consequently to the IDS industry, is its ease of installation and flexible deployment. At the same time, administrators do not need to worry about the high computing overhead exerted on the host machines by the IDS. Once a network is targeted, the first attack is aimed on the IDS itself. Thus, in the case of the host based IDS, both the host and the IDS will go under attack. This situation will increase the computing overhead on the host machine at the same time will reduce its response time. With the appliance IDS this problem is solved. Another benefit of this approach is for the manufacturer. Producing the IDS in the form of an appliance will improve the security measures for the product reengineering as well. It is easy to crack a software and make illegal copies out of it, however, following this approach wont be feasible for the appliance IDS. The hardware implementation of the appliance will make it harder and more expensive to make a copy of it. The drawback for this approach is the cost of production. Using the hardware components will increase the production cost and consequently the price of the product. Another benefit of this approach is the guarantee for the optimum hardware setup and performance for the IDS. This is because, the hardware platform and the software setup is already completed and tested by the manufacturer that is familiar with the system.

III. CONCLUSION

In this paper, the intrusion detection products were analyzed with respect to the recent design trends . Finally we conclude that desired features for the IDS depend on both the methodology and the modeling approach used in building the IDS, One of the parameters to measure the quality of an IDS is the number of its FP alarms. The smaller is the number of false positives, the better is the IDS.

ACKNOWLEDGMENT

We like to express our gratitude to all those who gave us the possibility to carry out the paper. We would like to thank Mr.K.Satyanarayana, chancellor of K.L.University, Dr.K.Raja Sekhara Rao, Dean, and K.L.University for stimulating suggestions and encouragement. We have further more to thank Prof.S.Venkateswarlu, Dr.K.Subrahmanyam, who encouraged us to go ahead with this paper.

REFERENCES

[1] D. Barbara, J. Couto, S. Jajodia, and N. Wu, "Special section on data mining for intrusion detection and threat analysis: Adam: a test bed for exploring the use of data mining in intrusion detection," AC SIGMOD Record, vol. 30, pp. 15–24, Dec. 2001.

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

[3] Ken. Yoshida, "Entropy based intrusion detection," in Proceedings of IEEE Pacific Rim Conference on Communications, Computers and signal Processing (PACRIM2003), vol. 2, pp. 840–843. IEEE, Aug. 2003. IEEE Explore.

[4] W. Lee, Salvatore J. Stolfo, and Kui W. Mok, "Mining audit data to build intrusion detection models," in Proceedings of the Fourth International Conference on Knowledge Discovery and Data Mining (KDD '98),, New York, NY, USA, Aug. 1998.

[5] John E. Dickerson and Julie A. Dickerson, "Fuzzy network profiling for intrusion detection," in Proceedings of NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, pp. 301–306, Atlanta, USA, July 2000.

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

[7] M. Botha and R. von Solms, "Utilizing fuzzy logic and trend analysis for effective intrusion detection, "Computers & Security, vol. 22, no. 5, pp. 423–434, 2003.

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

[9] S. B. Cho, "Incorporating soft computing techniques into a probabilistic intrusion detection system," IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICSPART C: APPLICATIONSAND REVIEWS, vol. 32, pp. 154–160, May 2002.

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

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

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

[13] W. Lee, Salvatore J. Stolfo, and Kui W. Mok, "Mining audit data to build intrusion detection models," in Proceedings of the Fourth International Conference on Knowledge Discovery and Data Mining (KDD '98),, New York, NY, USA, Aug. 1998.

[14] W. Lee, Salvatore J. Stolfo, and Kui W Mok, "Adaptive intrusion detection: A data mining approach, "Artificial Intelligence Review, vol. 14, no. 6, pp. 533–567, 2000.

[15] S. Mukkamala, G. Janoski, and A. Sung, "Intrusion detection using neural networks and support vector machines," in International Joint Conference on Neural Networks IJCNN02, vol. 2, pp. 1702–1707,Honolulu, HI USA, May 2002. IEEE, IEEE. Source: IEEE Explore.

[16] F. Neri, "Comparing local search with respect to genetic evolution to detect intrusions in computer networks," in Proceedings of the 2000 Congress on Evolutionary Computation, vol. 1, pp. 238–243, Marseille, France, July 2000. IEEE, IEEE. Source: IEEE Explore.

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

[18] T. Song, J. Alves-Foss, C. Ko, C. Zhang, and K. Levitt, "Using acl2 to verify security properties of specification-based intrusion detection systems," in Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003), July 2003.

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

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

[21] J. Cabrera, L. Lewis, X. Qin, W. Lee, R. Prasanth,B. Ravichandran, and R. Mehra, "Proactive detection of distributed denial of service attacks using mibtraffic variables - a feasibility study," in Proceedings of the 7th IFIP/IEEE International Symposium on Integrated Network Management, pp. 609–622, Seattle, WA, May 2001.

[22] Joao B. D. Cabrera, L. Lewis, X. Qin, W. Lee, and Raman K.Mehra, "Proactive intrusion detection and distributed denial of service attacks case study insecurity management," Journal of Network and Systems Management, vol. 10, pp. 225–254, 2002.