Investigations on Intrusion Discovery Methods in Wireless Adhoc Networks

Brajendra Pratap Singh[1], Dr. Brij Bhusan[2]

[1]Research Scholar, Mewar University, Gangarar Chittorgarh, Rajasthan
[2]Professor, Mewar University, Gangarar, Chittorgarh, Rajasthan

Abstract

As the recent denial-of-service attacks on several major Internet sites have shown us, no open computer network is immune from intrusions. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Many of the intrusion Discovery techniques developed on a fixed wired network are not applicable in this new environment. How to do it differently and effectively is a challenging research problem. In this paper, we first examine the vulnerabilities of a wireless ad-hoc network, the reason why we need intrusion Discovery, and the reason why the current methods cannot be applied directly. We then describe the new intrusion Discovery and response mechanisms that we are developing for wireless ad-hoc networks.

Keywords: *Investigations, Intrusion, Discovery, Wireless Adhoc Networks, techniques.*

1. INTRODUCTION:

An Intrusion Discovery Method (IDM) would be device be able to or a software and additionally hardware based system that screens network traffic and screens for suspicious movement and alarms the framework or network administrator of a security rupture, strategy infringement or other trade off that may unfavorably influence the overseer's information technology network. It goes about as the principal line of guard against network attacks (Zhimin et al 2010).

Intrusion Discovery methods monitor and examine a network's activities, break down its arrangements and vulnerabilities and evaluate record respectability. They are fit for perceiving normal attack patterns, investigating unusual movement examples and following client arrangement infringement.

Intrusion Discovery methods are created to handle the regularly expanding number of attacks on real locales and networks. However because of the advancements of attack ending up especially refined and with an exposed measure of specialized learning by the attacker, the Discovery systems turn useless.

As specified by Rouse (2014), ordinarily, IDS takes after a two-step process. They can either act in a latent mode by being host based and observing the framework's setup records for Discovery of helpless settings, unsafe passwords and policy violations. They can likewise act in a dynamic mode by being network based altogether to monitor the Discovery mechanisms set up to recognize the attacks and keep up the log reports.

Intrusion attempt or a risk can be characterized as the likelihood of a purposeful or unapproved endeavor to get to or control the data as well as render a system unreliable or unusable.

Interruptions can be comprehensively named

- Attempted break-ins and masquerade attacks, which are identified by atypical conduct profiles or violations of security constraints
- Penetration of the security monitoring system,
- Information Leakage, which gets saw by atypical utilization of assets in the framework.
- Denial of administration, which gets found by unusual requests set in from other systems

- Malicious use, which is seen by an adjustment in conduct profiles, security requirement infringement and utilization of special privileges.

Intrusion Discovery

The process of observing the occasions happening in a computer system or network, breaking down them for indications of security problems is alluded to as Intrusion Discovery. Intrusion Discovery (ID) is a procedure of dealing with the security for computers and networks. It gathers and breaks down the gathered data from different regions inside a computer or from a network trying to distinguish the vulnerabilities. It utilizes a vulnerability evaluation strategy called 'filtering' to discover the security of a computer system or network.

The various categories of Security attacks (Kartit et al 2012) are: Interruption, Interception, Modification and Masquerade. Intrusion Discovery functions (Asmaa Shaker & Sharad 2011) include:

i) Monitoring and analyzing both user and system activities

ii) Analyzing system configurations and vulnerabilities

iii) Assessing system and file integrity

iv) Ability to recognize patterns typical of attacks

v) Analysis of abnormal activity patterns

vi) Tracking user policy violations

The primary assumption in the Discovery process of Intrusion is that user and program activities can be monitored and modeled.

2. REVIEW OF LITERATURE:

A Port Scan is a technique for deciding if specific administrations are accessible on a host or a system by watching reactions to association endeavors. In light of how filtering is performed, port sweep systems can be characterized into two general classes: single-source port outputs and disseminated port outputs. Single source port outputs examine numerous goal has from one source hub. Then again, circulated port sweeps can be checking the ports of single goal have from many source hubs or filtering the ports of numerous goal has from numerous source nodes. (Bhuyan et al 2010).

Kim et al (2004) proposed this technique which means to identify arrange port sweeps utilizing oddity Disco very. To start with, the technique performs measurable tests to dissect movement rates and after that, it influences utilization of two dynamic chi-to square tests to identify irregular bundles. It demonstrates arrange movement as a stamped point process and presents a general port sweep show. The creators exhibit reenactment results to identify 10 pernicious vertical outputs with genuine positive rate more prominent than 90% and false positive rate littler than 15% for both the static and dynamic tests utilizing the port sweep display and factual tests.

Gates et al (2006) devised a method which analyzes Cisco Net Flow data for port scan attacks. The method extracts the events for each source and the flows in each event are then sorted according to destination IP and destination port. It attempts to calculate six characteristics for each event based on statistical analysis of port scans. It estimates a probability using logistic regression with these six characteristics as input variables to predict whether t he events contain a scan or not. The main disadvantage of this technique is that it is non-real time.

Udhayan et al (2009) suggested a heuristic approach for detecting port scan attacks. One possible solution to curb a zombie army or a malicious botnet attack is by detecting and blocking or dropping reconnaissance scans, i.e., port scans. They derive a set of heuristics for their Discovery, some quite crafty. It is written into the firewall and is triggered immediately after a port scan is detected, to drop packets with the IP address of the source of port scan for a pre-determined period.

Gyorgy et al (2005) proposed a model known as off-the-shelf classifier based on the data mining approach. Initially, it transforms network trace data into feature dataset with label information. Then, it selects Ripper, a fast rule based classifier, which is capable of learning rules from multi-model datasets and the results provided by it are easy to interpret. The authors successfully demonstrate that data mining models can enclose expert knowledge to create an adaptive algorithm which can outperform the heuristic based scan Discovery in both precision and recall. Also, this technique is capable of detecting the scanners at an early stage.

Haan (2005) presents a conceptual model of ports can Discovery and uses it to analyze the possibility of scan Discovery based on network layer header data only. The model uses different features based on the IP header list: source and destination IP addresses, datagram size, transport layer protocol field, fragmentation information, and the checksum. This model has been shown to be effective and robust in terms of size of the datasets and Discovery rate.

Rong-sheng et al (2004) proposed this approach which uses a new mechanism termed Port Scan Discovery (PSD) and is based on TCP packet anomaly evaluation. By learning the port distribution and flags of TCP packets arriving at the protected hosts, PSD can compute the anomaly score of each packet and effectively detect port scans including the slow scans and stealthy scans. It shows that PSD has high Discovery accuracy and low Discovery latency.

El-Hajj et al (2008) report on a fuzzy logic based port scan attack Discovery approach in their paper. They design a fuzzy logic controller and integrate it with SNORT. The new method, known as Fuzzy-Based SNORT (FB-SNORT) enhances the functionality of port scan Discovery. The authors use fuzzy logic for Discovery because: (i) Clear boundaries do not exist between normal and abnormal events, and (ii) Fuzzy logic rules help in smoothing the abrupt separation of normality and abnormality i.e., anomaly. Their method shows that applying fuzzy logic for scan Discovery adds to the accuracy of determining bad traffic and it gives a rank for each type of port scanning attack.

Liu et al (2008) suggested a method known as Naive Bayes Kernel Estimator (NBKE) which is used to identify flooding attacks and port scans from normal traffic. The method represents all known attacks in terms of traffic features. This method achieves high accuracy in the Discovery of flooding attacks and port scan attacks. The authors show that the Kernel based Estimator can provide improved accuracy of 96.8% over the simple Naive Bayes estimator.

Shafiq et al (2008) report a comparative study of three classification schemes for automated port scan Discovery. These include a simple Fuzzy Inference System (FIS) that uses classical inductive learning, a Neural Network that uses the back propagation algorithm and an Adaptive Neuro Fuzzy Inference System (ANFIS) that also employs the back propagation algorithm.

3. INTRUSION DISCOVERY SYSTEM:

An Intrusion Discovery System (IDS) can be device or a software and/or hardware based system that monitors network traffic and monitors for suspicious activity and alerts the system or network administrator of a security breach, policy violation or other compromise that may adversely affect the administrator's information technology network. It acts as the first line of defence against network attacks.

Intrusion Discovery systems monitor and analyze a network's activities, analyze its configurations and vulnerabilities and assess file integrity. They are capable of recognizing typical attack patterns, analyzing abnormal activity patterns and tracking user policy violations.

Intrusion Discovery systems are developed in order to tackle the ever increasing number of attacks on major sites and networks. However due to the technologies of attack becoming very much sophisticated and with a bare amount of technical knowledge by the attacker, the Discovery systems turn futile.

As mentioned typically, IDS follows a two-step process. They can either act in a passive mode by being host based and monitoring the system's configuration files for Discovery of vulnerable settings, unsafe passwords and policy violations. They can also act in an active mode by being network based in order to monitor the Discovery mechanisms set in place to identify the attacks and maintain the log reports.

In Figure 1, the IDS responds to anomalous or malicious traffic by taking action such as blocking the user or source Internet Protocol (IP) address from accessing the network.

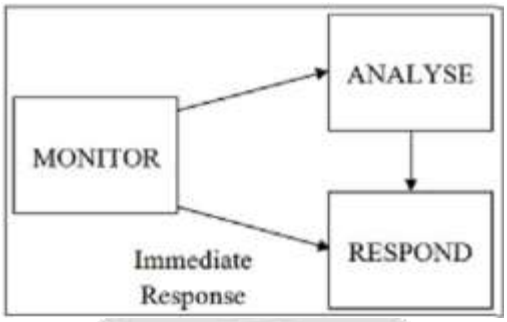

Figure 1 Process of Intrusion Discovery System

Steps in Intrusion Discovery System: The various steps performed by a typical Intrusion Discovery system are:

i) Monitoring and analyzing traffic

ii) Identifying abnormal activities

iii) Assessing severity and raising alarm

Goals of Intrusion Discovery System: The goals of any Intrusion Discovery system would be to:

i) Detect wide variety of intrusions

ii) Detect intrusions in timely fashion

iii) Present analysis in simple, easy-to-understand format

iv) Accuracy

v) Minimize false alerts i.e., false positives & false negatives

Network based Intrusion Discovery System: Network-based Intrusion Discovery System (NIDS) possess the capability to analyze the data traffic that travel through the network. The NIDS are strategically placed at premeditated places within the network so that they can monitor the traffic on the network effectively. Ideally the best option is to scan all incoming and outgoing traffic; however on doing it would affect the overall speed of the network. The packets captured are analyzed and compared with empirical data for their identification as malicious. Software or hardware lies in one or more machines connected to a network to analyze the incoming traffic. Network based IDS uses packet sniffing techniques to pull data from Transmission Control Protocol/Internet Protocol (TCP/IP) or other protocol packets travelling along the network.

Limitations in Network Intrusion Discovery Systems: Network intrusion Discovery systems analyze traffic passing through the network segments at the network layer. Attacks can be identified at this level as their Discovery would prove to be difficult by observing at an application level. However, there can be instances where the attack traffic passes through the network without being completely visible to the NIDS. This is due to the use of secure encrypted tunnels and Virtual Private Network (VPN). Attacks launched through Secure Sockets Layer (SSL) traffic over Hyper Text Transfer Protocol Secure (HTTPS) based connections can go unidentified by Discovery systems. The major limitation to NIDS arises due to increasing bandwidth rates of the network as NIDS has to keep up with the high data rates. (Information Assurance Tools Report 2009).

4. WIRELESS ADHOC NETWORKS:

A Wireless Ad-hoc Network is a decentralized type of Wireless Networks. The network is called ad-hoc since it does not depend on any preexisting infrastructure such as routers or access points. Further, each and every node in

ad-hoc network extends their participation in the process of routing by forwarding the data from one node to the other. Ad-hoc networks also use flooding mechanism to forward data whereby the participating node forwards the incoming data to all outgoing links except to the link through which it received the data. In Ad-hoc network all nodes have equal status and are free to associate with any other Ad-hoc network within the link range. Ad hoc network often refers to a mode of operation of Institute of Electrical and Electronics Engineers (IEEE) 802.11 wireless networks.

Intrusion Discovery in Wireless Adhoc Networks: Since, Wireless Adhoc Networks are decentralized and infrastructure less network, the nodes in the Wireless Adhoc Network are very much susceptible to malicious attacks as the attacker does not need a physical access to gain entry into the node. Further a compromised node is very vulnerable as it proves too difficult to identify it. Hence Intrusion Discovery in such a scenario proves to be a challenging and much needed task.

Challenges in Intrusion Discovery in Wireless Adhoc Networks: The major challenges involved in the intrusion Discovery in Wireless Adhoc Networks include:

i) High data rate & false alerts – The enormous amount of network traffic poses a great challenge in the identification of intrusion as intrusive packets can go unnoticed by the IDS if the traffic rate is high. This eventually produces false alerts.

ii) Rule set size of IDS – Since the data rate is high the scanning rate of the intrusion Discovery algorithm should also be high. However the ever increasing rule set of the heuristic IDS poses a great challenge as all these rules need to be checked to detect the intrusion.

iii) Processor Architecture & Processor speed – The processor architecture i.e., single-core or multicore, multithreading support and processor speed also plays a major role in the intrusion Discovery process. Multicore processor architectures offer the advantage of software parallelism i.e., the intrusion Discovery algorithm can be parallelized to run in multicores thereby scanning the data at faster speeds.

5. CONCLUSION:

Intrusion Discovery can complement intrusion prevention techniques (such as encryption, authentication, secure MAC, secure routing, etc.) to improve the network security. However new techniques must be developed to make intrusion Discovery work better for the wireless ad-hoc environment. Through our continuing investigation, we have shown that architecture for better intrusion Discovery in wireless Adhoc networks should be distributed and cooperative. A statistical anomaly Discovery approach should be used. The trace analysis and anomaly Discovery should be done locally in each node and possibly through cooperation with all nodes in the network. Further, intrusion Discovery should take place in all networking layers in an integrated cross layer manner. Currently, we are continuing our investigation in the architecture issues, the anomaly Discovery model, and the multilayer integration approach. For architecture study, we are refining its design and plan to implement it and study its performance implications. For anomaly Discovery model, we are studying the effectiveness and scalability of our approach for building anomaly Discovery models for ad-hoc routing protocols and for other layers of wireless networking. In particular, we will first focus on two questions about ad-hoc routing: what information a routing protocol should include to make intrusion Discovery effective, and what is the best anomaly Discovery model for a given routing protocol. Finally, we will study the effectiveness gain (i.e., in Discovery rate) with the multi-layer integration approach, as well as its performance penalties.

6. REFERENCES:

1. Zhimin, Z, Zhongwen, C, Tiecheng, Z & Xiaohui, G (2010), 'The Study on Network Intrusion Discovery System of SNORT', Proceedings of the second international conference on networking and digital society, vol. 2, pp. 194-196
2. Rouse, M (2014), Intrusion Discovery Systems. Available from: [27 Oct 2014].
3. Kartit, A, Saidi, A, Bezzazi, F, El Marraki, M & Radi, A (2012), 'A New Approach to Intrusion Discovery System', Journal of Theoretical and Applied Information Technology, vol. 36, no. 2, pp.284–289.
4. Asmaa Shaker, A & Sharad, G (2011), 'Importance of Intrusion Discovery Systems (IDS)', International Journal of Scientific & Engineering Research, vol. 2, no.1, pp. 1–4.

5. Bhuyan, M H, Bhattacharyya, D K & Kalita, J K (2010), 'Surveying Port Scans and Their Discovery Methodologies', The Computer Journal, vol. 54, no. 10, pp. 1565-1581.
6. Kim, H, Kim, S, Kouritzin, M A& Sun, W (2004), 'Detecting Network Portscans through anomaly Discovery, Proceedings of SPIE, pp. 254- 263.
7. Gates, C, McNutt, JJ, Kadane, JB & Kellner, M (2006), 'Scan Discovery on very large networks using logistic regression modeling', Proceedings of IEEE Symposium on Computers and Communication, pp. 402–408.
8. Udhayan, J, Prabhu, MM, Krishnan, VA & Anitha, R (2009), 'Reconnaissance scan Discovery heuristics to disrupt the pre-attack information gathering', Proceedings of conference on Network and Service Security, pp. 353-365.
9. Gyorgy, JS, Hui, X, Eric, E & Vipin, K (2005), 'Scan Discovery: A data mining approach', Proceedings of SIAM International Conference on Data Mining, pp. 118-129.
10. Haan, GHK (2005), 'Discovery of portscans using IP header data', Proceedings of Technology Business Research Centre.
11. Rong-sheng, S, Xiao-yong, L & Jian-hua, L (2004), 'An adaptive algorithm to detect port scans', Journal of Shangai University (English Edition), vol. 8, no. 3, pp. 328-332.
12. El-Hajj, W, Aloul, F, Trabelsi, Z & Zaki, N (2008), 'On detecting port scanning using fuzzy based intrusion Discovery system', Proceedings of IWCMC'08, pp.105–110.
13. Liu, D, Zhang, M-W & Li, T (2008), 'Network traffic analysis using refined Bayesian reasoning to detect flooding and port scan attacks', Proceedings of ICACTE'08, pp.1000 – 1004.
14. Shafiq, MZ, Farooq, M & Khayam, SA (2008), 'A comparative study of fuzzy inference systems, neural networks and adaptive neuro fuzzy inference systems for portscan Discovery', Proceedings of Applications of Evolutionary Computing, LNCS, Springer, vol. 4974, pp. 52-61.