Host Based Intrusion Detection Architecture for Mobile Ad Hoc Networks

Prabhudutta Ray, Center for Development of Advanced Computing, Noida, India; E-mail: mtechray@yahoo.com

ABSTRACT

Mobile ad hoc network is a collection of mobile hosts, which can communicate with each other using wireless interfaces and can also dynamically form a network topology where each node can act as router to forwarding the packets to other nodes. These networks are in high demand due to the ease and speed in setting up such networks. Due to the inherent vulnerabilities of wireless medium and node mobility make such network highly susceptible to malicious attacks. Things are getting worst when some nodes getting hijacked or compromised and make this network to stop from the smooth workings. This paper proposes the host based intrusion detection architecture to identify the malicious node and provide security support to continue the smooth workings of this network.

Keywords: HAR, ACM, ARP, CM, ADM, MDM, HDD, SCM etc.

1. INTRODUCTION

Mobile ad hoc network (MANET) has become an exciting and important technology in recent years because of the rapid development of wireless devices. MANETs are highly vulnerable to attacks due to the open medium, dynamically changing network topology, lack of centralized monitoring and management point and lack of clear line of defense. Since mobile nodes are autonomous devices that are ready to capable of roaming independently and due to roaming, network topology changes dynamically. The nature of the mobile nodes makes the network very vulnerable to an adversary's malicious attacks. First of all the use of wireless links renders this network susceptible to attacks ranging from passive eavesdropping to active interfering. Second, the nodes with inadequate physical protection are receptive to being captured, compromised and hijacked. Since identifying a particular mobile node in a large scale network cannot be done easily, and attacks by a compromised node from inside the network are far more damaging and much harder to detect. Therefore, all the nodes in this network must be prepared to provide its own security to operate in a mode that does not have any centralized administration and trust no peer. Due to decentralized nature of decision-making, many network algorithms rely on the cooperative participation of all the other nodes in the network, which creates a great problem for this network. Since any adversaries can capture any node to exploit this vulnerability for new types of attacks designed to break the cooperative algorithms. Further packet routing creates vulnerability in the ad hoc network, because most of the ad hoc routing protocols are also co-operative in nature. Since the nodes are acting as router, unlike with a wired network, where firewall and extra protection can be placed on routers and gateways to provide extra security. So an adversary who hijacks an ad hoc mobile node could paralyze the entire wireless network by injecting false routing information and intentionally dropping the packet so that false routing information conclude in messages from all the nodes being fed to the compromised node and it can dropping the packet to waste the valuable resource of this network. In summary, history of security research for mobile ad hoc network provide intrusion prevention measures, such as encryption and authentication, can be used to minimize the intrusion, but cannot eliminate them. For example, above measures cannot defend against compromised mobile nodes, which act as master for several slaves in a clustered network architecture, which carry the private keys of other slaves in that cluster. The dynamic nature of the ad hoc network also means that trust between the nodes in the network is virtually non-existent. Without trust, preventive measures are unproductive and measures that rely on a certain level of trust between nodes are susceptible attacks themselves. Further no matter how many intrusions prevention measurers are inserted in a network there are always some weak links that one could exploit to break in. Intrusion detection presents a second wall of defense and it is a necessity in any high-survivability of this type of network.

2. SURVEY OF INTRUSION DETECTION ARCHITECTURE

Since fixed network based computer system there are several points where the monitoring activity can be performed to protect the devices which becomes the target of an intruder. An intrusion can be defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource", when it takes place, intrusion prevention techniques, such as encryption and authentication are usually the first line of defense. But the scalability and complexity of the ad hoc network address exploitable weakness in the system due to design and programming practice of various autonomous nodes. Such as vulnerabilities like buffer overflow, static buffer flows and memory leakages can waste significant amount of electrical power and intensive processing drains. So we have to avoid the situation whereby the device has to do more routing in the ad hoc network. The primary assumptions of intrusion detection are the node activity in terms of user and program activities are observable via system auditing mechanism during a particular session of the node activity and differentiate between normal and intrusion activities. So intrusion detection therefore involves capturing audit data of the session and reasoning about the evidence in the data to determine whether the system is under attack. Based on the session audit data of the host, which supplied by the operating system or maintaining the audit data by special mechanism, IDS can analyze and monitor the events to find that whether the activity is belonging to any normal behavior or not. Though each node in the network act as router but this paper does not consider any network level examination of the packet.

3. CATEGORIZATION OF IDS MODEL

intrusion detection model can be categorized into misuse detection and anomaly detection. Misuse detection model: - detection is performed by looking for the exploitation of known weak points in the system, which can be described by a specific pattern or sequence of events or data (the" signature" of the intrusion).

Anomaly detection model: - detection is performed by detecting changes in the patterns of utilization or behavior of the system. This is the type of intrusion detection described in [1]. It is performed by building a statistical model that contains metrics derived from system operation and flagging as intrusive, if any observed metrics that have a significant statistical deviation from the model. Conceptually, an intrusion detection model, i.e., a misuse detection rule or a normal profile, has major two components:

- The features extraction (or attributes, measures), e.g. "the number of failed login attempts", "the number of opening of Vi editor", the manipulation of bash_profile file ", etc, that altogether describe a logical event, e.g. user manipulation of system files and environment variables.
- The modeling algorithm, e.g. rule –based pattern matching, that uses the features to identify intrusion.

The main advantage of misuse detection is that it can accurately and efficiently detect instances of known attack that is already specified in the system but unable to detect newly (truly innovative) attacks. Anomaly detection systems, for example, IDES [2], flag observed activities that deviate significantly from the established normal usage profiles as anomalies, i.e. possible intrusions. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusion, but it may not be able to describe what the attack is and may have high false positive rate. Since defining a set of

predictive features that accurately capture the representative behaviors of intrusive or normal activities and extracting abnormal features from the data that quickly identify the intrusive activity in the system is the most important step in building an effective intrusion detection model which can be independent of the design of modeling algorithms.

4. PROBLEMS OF THE EXISTING IDS TECHNIQUES AND ITS LIMITATION

Since ad hoc networks neither have any centralized administration, nor have any traffic concentration points where the IDS can collect audit data for the entire network. Therefore, at any one time, the only available audit trace will be limited to communication activities taking place within the radio range, and the intrusion detection algorithms must be made to work on this partial and localized information [3].

A scenario of this problem can be seen in the following. Suppose IDS on a mobile ad hoc network are communicating with a certain encryption algorithm. Once an attacker compromises the security of one node in the network, it can send a message to all of the neighboring nodes conveying the need to change the encryption algorithm because due to an attack the attacker gain control of the network. Since the compromised node is communicating with the authorized encryption algorithm, the other nodes in the network trust the compromised nodes decision, and change the encryption algorithm for the network. This could lead to a type of availability attacks on the network. Since the nodes are busy trying to change the encryption keys by using intensive processing power, the IDS takes up a lot of the communication bandwidth between nodes, making the other, regular communication between nodes very slow. Further scalability is limited because distributed data collection can also cause problems with excessive data traffic in the network. Further it is also difficult to reconfigure or add capabilities to the IDS when network is fully operational. In summary, it must be needed to answer the following research questions in developing an ideal intrusion detection system for the mobile ad hoc networks

1. What architecture of the system is necessary for developing intrusion detection and response systems that fits in the mobile nodes and run continually with minimal supervision?
2. What are the suitable appropriate points to collect audit data of the nodes?
3. How to find out anomalies which depends on the partial, local audit traces –if they are the only acceptable audit sources?
4. How do we impose a minimal overhead on the system where it is running, so as to not interfere with its normal operation and run independently?
5. What is a good model of activities in a wireless communication environment that can separate anomaly when the nodes under attacks from the normalcy?
6. Finally due to resources constraints on the mobile nodes, IDS should not consume too much resource including power, processing time; therefore IDS should increase the run-time efficiency?

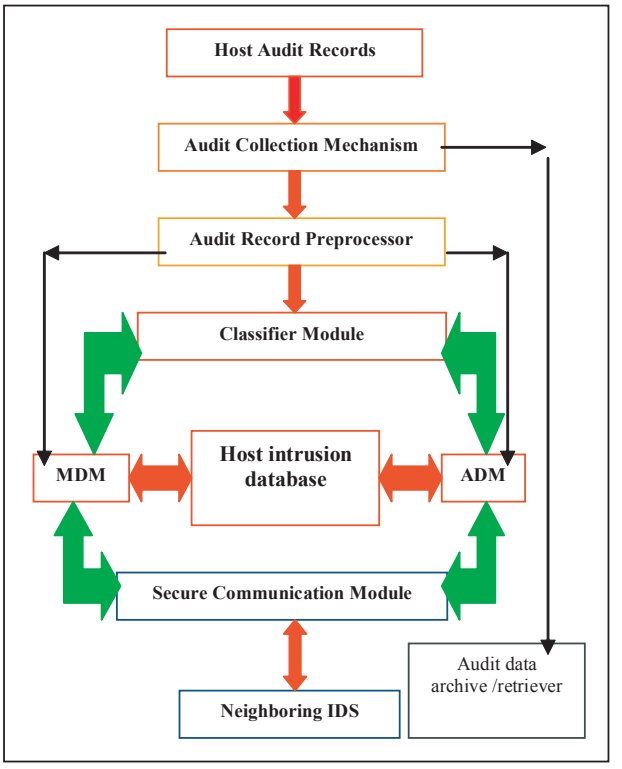
Considering the above all issues it can be found that if the design of IDS architecture are standalone for each host then they can detect attacks independently to decrease the co-operation between nodes and also takes the major decision locally. In order to provide protection to the individual nodes in the ad hoc networks it is required to constantly monitor the activity performed on the individual host so that unnecessary communication with other nodes can be minimized.

5. PROPOSED ARCHITECTURE

Host based system architecture are concerned with what activity is happening on each host. This architecture is ideal if it is able to detect actions and other activities with high confidence. In order to function properly, IDS has to be installed on every node in the network to processes and perform analysis on the audit data gathered locally, at the expense of the already limited resources on the hosts. The below architecture takes care to ensure that the IDS running on each host does not drain resources more than necessary. Here all the modules work collectively at the same time to provide the necessary support for the intrusion detection in the network.

The proposed architecture has eight parts, a) Host Audit Records (HAR), b) Audit Collection Mechanism (ACM), c) Audit Record Preprocessor (ARP), d) Classifier Module (CM), e) Anomaly Detection Module (ADM), f) Misuse Detection Module (MDM), g) Host Intrusion Database (HID) and h) Secure Communication module (SCM).

Figure 1. Graphical representation of a proposed host based IDS



a) Host Audit Records (HAR)

each operation of a host should be recorded to check that whether an intrusion is taking place. The local host audit record will consist of specific items out of the network traffic as well as user commands of the node. HAR is responsible for collecting useful information to minimize the volume of the audit data, responsible for gathering and storing not to processing it.

b) Audit Collection Mechanism (ACM)

This module usually passes the audit records to both the modules, one is Audit data archive/retriever, for the session duration storage, and to the Audit Record Preprocessor. The audit data archive /retriever can support as a simple buffer that writes the session oriented raw audit data into audit files or as sophisticated as a custom database management system used to store and retrieve audit data.

c) Audit Record Preprocessor (ARP)

This refers to one or more individual preprocessors used by IDS to isolate and format certain audit records prior to inputs into the other modules. Some records of the ongoing activity of the users must be maintained to provide as input to the intrusion detection system. In this module detection specific audit records are created from the host audit records. Each record contains the fields like subject, actions, object, exception-condition, resource-usage, time-stamp etc. This formatted audit records are providing structured and system specific useful information, which are passed below to the three individual module (MDM, CM, ADM) of the IDS. These individual modules are independently process the each audit records to determine any new intrusion has occurred or any malicious activity is performed by the host or not [4].

d) Classifier Module (CM)
Classification algorithms have attracted considerable interest both in the machine learning and data mining research areas [5]. In this architecture the classifier module basically concentrates on the decision tree approach. Objective is to use learning algorithm such that it is good if it produces hypotheses that do a good job of predicting the classification of unseen attacks. Audit record preprocessor (ARP) module provides structured and system specific set of records. Each record has the structure, consisting of a number of attribute value pairs. One of these attributes represents the category of the record. Basic approach is to determine a decision tree that on the basis of answers to questions about the non category attributes predicts correctly the value of the category attributes which takes only the values {attack, Don't attack}. From the tree construction, this module in the IDS properly does classification and finding new attacks. The use of the decision tree-learning algorithm is to test the "most important" attribute first, which makes the most difference to the classification of an example. That way, it can be hoped to get to the correct classification with a small number of tests, meaning that all paths in the tree will be short and the tree as a whole will be small so that it will provide faster approach to detect attacks on the node.

e) Anomaly Detection Module (ADM)
Each ADM is responsible for detecting a different type of anomaly. There can be many ADM modules based on the complexity of the IDS architecture. Each working separately or co-operatively with other ADM modules based on the processing load, e.g. .one is looking for file access frequency, while another might watch user input speed. In this architecture ADM will analyze data, compare with known profile which already defined, run the statistical analysis to determine if any deviation is significant, and flag the events as a true attack state, false attack state, or normal state. If it finds a false positive, then profile must be updated to reflect the results. Since in that case it making bridge with the classifier module (CM) to identify new types of attack occurred in the node. ADM's activity is to update profiles and checks for anomalous behavior whenever an audit record is generated or a session terminates. If abnormal behavior is detected, an anomaly record is generated having three components <Event, Time-stamp, and Profile>[6]. These generated records are compared with the audit record preprocessor input to conclude for an attack and then matches with the classifier module. If an ADM can identify an anomaly based on the data in the Host intrusion database, then it can initiate a local and global response to the intrusion. An example of a local response could be to stop communication to the identified node, rendering it useless to an attacker. A possible global response would be to use the secure communication module to alert other nodes in same cluster or in the other cluster, allowing them to configure a new network topology by excluding the designated compromised node. If the amount of data in the HID and CM is not sufficient to determine if the present activity should be as an intrusion, then it is possible for ADM to use the secure communication module to query the other nodes in the network to get help in identifying an intrusion [7].

f) Misuse Detection Module (MDM)
Detection is performed by looking for the exploitation of known weak points in the system, which can be described by a specific pattern or sequences of events or the data (the "signature" of the intrusion). Here the collections of signatures (representative patterns) define the known attacks [8]. The primary purpose of MDM is only to identify the known patterns of attacks that are specified in the local intrusion database. It also gathering sufficient information from the CM module about the specification of new attacks, accordingly it can update the rule sets. MDM takes the audit data for analysis and compares the data to HID for attack signatures. The attack signatures are normally specified as rules with respect to timing information and are also referred to as known attack patterns. If any comparison made between ADM and MDM, then it can be find that MDM'S job is to only identify known patterns of attacks that are specified in the host intrusion database. If MDM needs more information from the other neighboring nodes then it should use the Secure Communication Module to interact with them. Using the information provided by neighboring nodes IDS, then MDM might be able to predict an intrusion with more accuracy.

g) Host Intrusion Database (HID)
HID is a database maintaining in the nodes that warehouses all the information necessary for the IDS, such as the signatures of known attacks, the established patterns of users and resource usage and the normal volume of data flow in the network. The ADM and MDM communicate directly with the HID to determine if an intrusion is taking place.

h) Secure Communication Module (SCM)
SCM is providing necessary communication with other IDS on the network. It will allow the MDM and ADM to use co-operative algorithms to detect intrusion [9]. This module initiates a global response when an IDS of a node or a group of IDS of several nodes detects an intrusion. Basically, to provide security in a wireless medium it is required any communication that must be occurred from one node to another will use the SCM. Since Buttyan et.al. [10] discuss the problems regarding any public-key based security system to make each user's public key available to others in such a way that its authenticity is verifiable. In ad hoc networks, this problem becomes even more difficult to solve because of the absence of centralized services and possible network partitions [11]. Since data communication via SCM will need to be encrypted in order to ensure the data received by another IDS is accurate and has not been modified in any way. This module is only used by the IDS to exchange security related information between nodes and also share the necessary bandwidth that mobile devices uses for normal data transmission. So it is required to be efficient and fast, and can only use the amount of bandwidth it needs when transmission required. Efficiently managing the bandwidth for normal data transmission for mobile devices is another issue for IDS design also [12].

6. CONCLUSION
This paper has discussed several new issues and ideas that must be addressed when designing intrusion detection systems for mobile ad hoc networks. Even if the prevention schemes are perfect and implemented correctly, there are still internal and insider attacks that utilizes software vulnerability. A compromised node is an insider, with all the necessary cryptographic keys, and if it elected as a cluster head then it can launch many attacks. Thus, intrusion detection system should be designed in such a way that it can provide a necessary level of protection to the node and network and work independently without minimum human supervision. Through continuing investigation, it can be shown that this architecture is well suited for better intrusion detection in wireless ad hoc network that are distributed and co-operative in nature. Furthermore, the modular characteristics of the architecture allow it to be easily extended, configured and modified, either by adding new components, or by replacing components when they need to be updated. Such as it is possible to modify the audit record preprocessor module to provide more structured format of output. Application of this architecture might prove helpful in networks that are dynamic in nature, such as a group of tanks roaming in the desert, emergency response teams, and law enforcement etc.

7. FUTURE WORK
Future work includes implementation of such IDS architecture and testing its effectiveness in mobile ad hoc networks environments. Further enhance the capability of classifier module, so that it detect the attacks with minimal amount of time and provide useful information to the ADM and MDM module, to increase the effectiveness and scalability of this proposed architecture.

8. REFERENCES
1). Dorothy .E. Denning. An Intrusion- Detection Model. IEEE transaction on software Engineering, 13 (2); 222-232, February 1987.
2). T. Lunt, A. Tamru, F. Gilhan, R. Jagannathan, P. Neumann, H. Javitz, A. Valdes and T. Garvey. A real-time intrusion detection expert system (IDES) –final technical report, computer science laboratory SRI International, Menlo Park, California, February 1992.
3). Zhang, Y. W. Lee, 2000 Intrusion detection in wireless ad hoc networks. In proceedings of the sixth international conferences on Mobile computing and networking (Mobicom 2000). Boston, MA. August 2000.
4). Lee, W., S. Stolfo. A framework for constructing features and modules for intrusion detection systems. In processdings of the 1999. IEEE symposium on security and privacy.
5). J.R. Quinlan, C4.5: programs for machine learning, Morgan Kaufmann, san mates, CA 1993.

6). Andrew .B. Smith, An examination of an Intrusion Detection Architecture for wireless Ad hoc networks, department of computer science, Mississippi state university, MS.39762.

7). Z. Hou, L., J. Zygmunt 1999. Securing ad hoc networks. IEEE networks November /December 1999.

8). K. Ilgun, R.A Kemonerer and P.A Porras , State transition analysis : A rule based Intrusion detection Approach , IEEE transaction on software engineering , vol .21 .no 3. March 1995. Pages 181-199.

9). Wu, H., S. Yang, Y. Lin 2000. The sharing session key component (SSKC) algorithm for End-to-End secure wireless communication. In Proceedings of the IEEE 34th annual International Carnahan Conference on the security Technology. Pp.242-250.

10). S. Capkun. Levente Buttyan. Self-organized Public key management for mobile ad hoc networks, IEEE Transactions on mobile computing, vol.2.No.1: 52-64; January –March 2003.

11). Y. hung and W. lee, A. cooperative Intrusion Detection System for Ad hoc networks.

12). Y. Zhang and W. Li, An Integrated environment for testing mobile ad hoc networks. In proceedings of the Third ACM international symposium on mobile ad hoc networking and computing (Mobihoc ’02), Lausanne, Switzerland, June 2002.