INTRUSION DETECTION SYSTEM WITH COLLOBORATIVE NETWORK SYSTEM

M.Kanneeswari[1](B.Tech IT), R.Preethi[2](B.Tech IT),S.Ragini[3](B.Tech IT), M.S.Vijaykumar[4](Assistant Professor –IT)
Tejaa Shakthi Institute of Technology for Women, Coimbatore.

Abstract: ***With the development of Internet cooperation, collaborative intrusion detection environments have been developed, which allow Intrusion Detection System nodes to collect information and learn experience from others. This project frame work for an adaptive intrusion detectionsystem*** *using* ***Bayesian network project is also called as IDS system which is developed control malicious behavior of packets that will effect network and its resources. There are many Parameters which are part of intrusion detection which have effect on network. In order to control unwanted packets decision making is important. A signature-based IDS (or rule-based IDS) detects a potential attack by comparing incoming events with its stored signatures, where a signature is a kind of description that defines an attack or an exploit by means of expert knowledge. In this project we use this tool based on signature recognition. Main objective of BN model tool is to check signature of attacks with the existing signatures and compare to take decision. Problem with this system is as the signature changes need to update regularly to comparison. The developed IDS using BN which will update these changes regularly.***

I. Introduction

NETWORK intrusions such as worms, Trojans and DDoS attacks are a big threat for computer networks and have already become more sophisticated to detect and defend. For instance, McAfee's threat prediction report indicates that intrusions over the Internet would still be prevalent in future years. The potential damage of these intrusions could be significant if they are not detected timely.To address this problem, intrusion detection systems (IDSs) have been implemented at large with the purpose of defending against various attacks and they have become an indispensable component with respect to current defense mechanisms .These detection systems usually identify an intrusion through comparing observable behaviour against suspicious patterns. In particular, based on different detection methodologies, an IDS can be typically classified as signature-based IDS and anomaly-based IDS. A signature-based IDS (or rule-based IDS) detect a potential attack by comparing incoming events with its stored signatures, where a signature is a kind of description that defines an attack or an exploit by means of expert knowledge. On the other hand, an anomaly based IDS tries to identify great deviations between current events and its pre-established normal profile. A normal profile often represents a normal action or a normal

Network connection through monitoring the normal behaviour for a long period. In addition, based on the deployed locations and target events, an IDS can be classified as host-based IDS (HIDS) and network-based IDS (NIDS). The former like often resides on a local system and tracks changes made to important files and directories, while the latter like usually places on the network with the purpose of analyzing network traffic for malicious patterns.

1. ACK implementation:

ACK is basically an end – to – end acknowledgment scheme .It is a part of co-operative scheme aiming to reduce the network overhead when no network misbehavior is detected.The basic flow is if Node A sends an packet p1 to destination Node D, if all the intermediate node are cooperative and successfully receives the request in the Node D. It will send an ACK to the source (Node A) , if ACK from the destination get delayed then it S-ACK process will be initialized.

2. Secure Acknowledgment (S-ACK):

In the S-ACK principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

3. Misbehavior Report Authentication (MRA):

The MRA scheme is designed to resolve the weakness of watchdog with respect to the false misbehavior report. In this source node checks the alternate route to reach destination. Using the generated path if the packet reaches the destination then it is concluded as the false report.

4. Digital Signature Validation:

In all the three parts, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect mis-behaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

Disadvantages Of Existing System

Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping. The lack of any infrastructure added with the dynamic topology feature of make these networks highly vulnerable to routing attacks such as blackhole and grayhole (known as variants of blackhole attacks).In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

II Proposed System

In fact, many of the existing IDS adopt an acknowledgment-based scheme. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to

guarantee that the acknowledgment packets are valid and authentic. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced. In the proposed system, a mechanism [so-called cooperative bait detection scheme (CBDS)] is presented that effectively detects the malicious nodes that attempt to launch grayhole/collaborative blackhole attacks. In this scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike previous works, the merit of CBDS lies in the fact that it integrates the proactive and reactive defense architectures to achieve the aforementioned goal.

III Advantages of Proposed System

The proposed approach is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again. This function assists in sending the bait address to entice the malicious nodes and to utilize the reverse tracing program of the CBDS to detect the exact addresses of malicious nodes. Documentation carefully. The stateful inspection feature typically assists in mitigating the risk posed by network reconnaissance and IP spoofing.

IV CONCLUSION

Overhead network packets are a big challenge for an IDS, where constructing a packet filter is a promising solution. With the advent of collaborative intrusion detection environments like CIDNs, it is found that the previously designed trust-based packet filter is not effective, as the process of trust computation could be easily compromised by insider threats, e.g., betrayal attacks, where trusted nodes suddenly become malicious

REFERENCES

[1] A.V. Aho and M.J. Corasick, "Efficient string matching: an aid to bibliographic search," Communications of the ACM, vol. 18, no. 6, pp. 333-340, 1975.

[2] R.S. Boyer and J.S. Moore, "A fast string searching algorithm," Communications of the ACM, vol. 20, no. 10, pp. 762-772, 1977.

[3] A. Bremler-Barr and Y. Koral, "Accelerating multipattern matching on compressed HTTP traffic," IEEE/ACM Transactions on Networking, vol. 20, no. 3, pp. 970-983, 2012.

[4] Y.-K. Chang, M.-L. Tsai, and C.-C. Su, "Improved TCAM-based Pre- Filtering for Network Intrusion Detection Systems," In: Proceedings of the 22nd International Conference on Advanced Information Networking.and Applications (AINA), pp. 985-990, 2008.