Novel Architecture for Intrusion-Tolerant Distributed Intrusion Detection System using Packet Filter Firewall and State Transition Tables

Dr. S.G. Bhirud
Member of AICTE

Vijay Katkar
Dep. of Computer Engineering,
MPSTME, NMIMS University Mumbai

ABSTRACT

Tremendous efforts have been taken over many years to secure the network against attacks; still attackers are successful with painful frequency. Experienced attackers try to disable the Intrusion Detection System (IDS) before launching attack. Therefore there should be some mechanism in IDS for uninterrupted detection of intrusion even though failure in IDS has occurred due to attacks. This paper presents the design and implementation of Novel Intrusion-Tolerant Distributed Intrusion Detection System using Packet Filter Firewall and State Transition Tables. Proposed architecture is immune to both, failure of IDS components and compromised IDS components. This architecture is capable of restricting the effect of network attacks like DoS, DDoS and Probing to a subset of network. Experimental results prove the usefulness and efficiency of this architecture.

General Terms

Firewall, Intrusion-Tolerance, DoS attack, NIDS, Distributed IDS

1. INTRODUCTION

Firewall is a widely used and useful tool for securing network from attacks. Firewall is normally installed at entry point of the network and configured with pre-defined policies and rules. The administrator defines rules to protect the network against known attacks. It is useful tool for preventing basic intrusion. But the need of detecting attacks on network so that administrator can define new rules to protect network against attacks, results in the development of IDS.

IDS is widely used tool for detection of unauthorized use, misuse, and abuse of computers as well as resources of computer network. Many researchers [9][10][11][12] have proposed architecture and framework for developing IDS. Depending on the placement of the IDS, there are two types of IDS. If IDS is installed to analyze traffic of the whole network, then it is called as Network-based IDS (NIDS). If IDS is installed on computer to analyze activities going on that computer only, then it is called as Host-based IDS (HIDS).

Security provided by Firewall has many limitations, such as it cannot prevent network from interior attacks. Intrusion Detection System (IDS) also has many limitations, such as it does not have response mechanism against attack. But if firewall and IDS are integrated together then this integration can enhance the network security. IDS can monitor the network for detection of interior and exterior attacks and automatically informs Firewall about attacks. By using this information Firewall can dynamically alter the rules to prevent network resources from attack. Many researchers [6][7][8] have proposed security mechanisms based on integration of IDS and Firewall.

Distributed IDS (DIDS) is consisting of many IDS to monitor a network or group of networks and all of these IDS communicate with each other or central coordinator to exchange information. Due to continuous expansion of network scale and the complexity of novel attacks DIDS has come into existence. Distributed processing, decentralized collection of IDS and centralized management of IDS can satisfy security requirements of large-scale and high-speed network [5].

Now a day’s hackers are using viruses and worms for attacking the security applications to get into the system without any problem. But currently used security applications are also not able to detect and prevent unknown attacks against them. Therefore, in order to strengthen the security of security applications, a concept called Intrusion Tolerance has emerged.

Due to the increasing importance of IDS in network security, IDS may become a primary target of attackers. Experienced attackers try to disable the IDS before launching attacks. Therefore there should be some mechanism in IDS for uninterrupted detection of intrusion even though failure in IDS has occurred due to attacks. Intrusion-tolerant IDS is a special case of IDS that has inbuilt intrusion-tolerant mechanism to protect IDS from attacks. Intrusion-tolerant mechanism protects the IDS instead of the network monitored by IDS.

Currently two methods are used by many researchers for implementation of Intrusion-tolerance system. First method is known as attack response. In this method, when it detects fault in the system or detect high probability of attack against the system, it goes for reallocation of system resources and system structure adjustment to make system more immune to attacked. Second method is known as attack mask. In this method, when attack took place, the system tries to mask the impact of attack with the help of redundancy, Byzantine agreement or other method.

A recent trend used by attackers is to create zombie machines in the organization and then use these zombie machines to launch the attack against the organization itself. Thus Intrusion-Tolerant IDS must be able to deal with such kind of attacks.

2. RELATED WORK

Liwei Kuang, Mohammad Zulkernine [1] have proposed an intrusion-tolerant mechanism for NIDS using multiple independent components which work together. The tolerance mechanism continuously monitors the distributed detection units and as soon as it detects the failed component it creates a new copy of that component and replaces it with failed component. Due to the use of dynamic redundancy of components, this mechanism does not require any duplicate component. The major drawback of this mechanism is that, it depends on configuration files for detection of failed components. An attacker may change the configuration file and fool the Intrusion Tolerance mechanism. Their proposed IDS is not immune to Compromised components.

Feng Zhao, Qing-Hua Li1, Li Jin [2] have proposed an intrusion-tolerant intrusion detection method based on sequence forecast for network stream. They are trying to discover the network events' key features and then apply linear regression technique of Data Mining to discover normal behavior and use it to differentiate between intrusive behavior and normal behavior. They have proposed different strategies for IDS to behave in different attack cinereous. But the drawback of their proposal is that, this IDS is not immune to component failure or compromised Components as well as their proposed Intrusion Tolerant mechanism is not immune to IP Spoofing.

Paulo Sousa, Alysson Neves Bessani, Miguel Correia,Nuno Ferreira Neves, Paulo Verissimo [3] have proposed a combined approach of proactive recovery and reactive recovery. Authors guarantees that, in this architecture at any moment of time there will be sufficient amount of system replicas to ensure system's correct operation. Proactive recovery is used with services that enable replicas to react and recover replicas which are compromised.

Hui Zhao, Shanhong Zheng ,Wanlong Li, LiJuan Zhang [4] have proposed real-time unsupervised network intrusion-tolerant system using improved adaptive theory. They have developed a different intrusion tolerance mechanism which is based on triggering. Similar to [2] their architecture is not immune to component failure.

[1][2][3][4] Have common drawback that, if DDoS attack it launched against organization using zombie machines of the organization itself, then this will affect the network of entire organization.

The major focus of the Paper is on making the IDS Intrusion Tolerant, thus we have implemented NIDS for detecting DDOS attacks only.

3. PROPOSED ARCHITECTURE

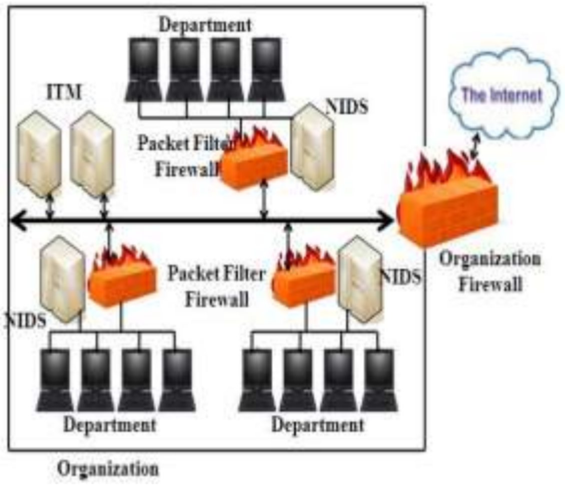

Figure: 1

If the size of the organization is too large then it increases the load on the NIDS as it monitors the traffic of entire network. As the number of machines in the network increases or as number of high-speed machines in the networks increases it increases a burden on NIDS a lot. This makes analysis of every packet of the network almost impossible for NIDS. Every Organization is divided into departments and each department has its own LAN. Thus separate NIDS can be placed at every department. Each NIDS monitors the traffic of that department only and communicate with remaining NIDS, Central Controller i.e. Intrusion Tolerant Mechanism (ITM). This reduces the burden on the NIDS drastically and provides Intrusion Tolerant capability. There are always two or more instances of ITM.

ITM is placed at point where it is accessible to all NIDS in the Organization. Responsibilities of ITM are:

- Detection and restoration of Failed NIDS
- Detection and restoration of Compromised NIDS
- Synchronization among different NIDS
- Detection and restoration of Failed ITM
- Detection and restoration of Compromised ITM
- Sending Alert to Administrator indicating Hardware and unhandled failure

NIDS and ITM are linked with each other for implementing Intrusion Tolerance. While detecting intrusion NIDS goes through different and predefined states with proper sequence, say packet capture, packet analysis, rule comparisons, alert generation. As NIDS goes through each state, it sends corresponding message to ITMs. ITM uses this message along with State Transition Table to maintain the state of every NIDS.

If attacker targets the NIDS and successfully disables it, then no message will be sent by NIDS to STT module of

ITM and absence of message from NIDS will be detected as failure of NIDS within mean time. After detection of failure one of the ITM performs following steps:

```
i.   Send a Message of another NIDS (Say NIDS_Temp) to
     analyze the data of Failed NIDS (Say NIDS_Failed) and
     generate alerts
ii.  Remotely enable the Failed NIDS
iii. If(Successfully Enabled the NIDS)
         Send Message NIDS_Temp to stop analyzing the
         data of NIDS_Failed
     Else
         Send High Priority Alert to the Administrator
         Indicating Failed NIDS
```

If attacker targets the NIDS and successfully Compromise it, then NIDS will not follow the predefined sequence. This change is easily determined by STT module of ITM. Now one of the ITM performs following steps:

```
i.   Send Message of another NIDS (Say NIDS_Temp) to
     analyze the data of Compromised NIDS (Say
     NIDS_Compromised) and generate alerts
ii.  Remotely terminates the instance of Compromised NIDS
iii. If(Successfully terminate NIDS)
         1) Remotely creates new instance of NIDS to
            replace the compromised NIDS
         2) Send Message NIDS_Temp to stop analyzing the
            data of NIDS_Compromised
     Else
         Send High Priority Alert to the Administrator
         indicating Compromised NIDS
```

Similar to NIDS; ITM also periodically sends messages to every ITM and NIDS. These messages then can be used by ITM and NIDS to determine whether ITM is alive or not. If attacker targets the ITM and successfully disables it, then no message will be sent by ITM to STT module of remaining ITM and absence of message from ITM will be detected as failure of ITM within mean time. Now one of the ITM performs following steps:

```
i.   Remotely enable the Failed ITM
ii.  If(Unable to enabled ITM)
         Send High Priority Alert to Administrator
         indicating Failed ITM
```

If attacker targets the ITM and successfully Compromise it, then ITM will not follow the predefined sequence. This change is easily determined by STT module of remaining ITM. Now one of the ITM performs following steps:

```
i.   Remotely Disable Compromised ITM
ii.  If (Successfully terminate Compromised ITM)
         Remotely create a new Instance of ITM
     Else
         Send High Priority Alert Message to
         administrator indicating Compromised ITM
```

If attacker successfully disables or Compromises the every available ITM, then NIDS sends High Priority Alert to the Administrator, who can restart ITM so that it can function properly. Until every NIDS detect that ITM is properly working again, every NIDS sends its own State Message to remaining NIDSs instead of ITM. NIDS uses these messages to ensure the proper functioning of remaining NIDSs and sends the state information (Working/ Disabled/ compromised) of every NIDS to Administrator. This information then can be used by Administrator to take the necessary steps.

Packet Filter firewall is installed at the entry point of every department so that secure isolation between LAN of different departments can be achieved. When NIDS detects that DoS/DDoS/Probing attack is being launched from the department network monitored by it, it instructs the packet filter firewall to drop the packets of systems from which attack is being launched. This limits the effect of attack to the subset of network.

4. EXPERIMENTAL RESULTS

NIDS and ITM units are developed using Java 1.6 for the sake of development simplicity. Packet filtering firewall is implemented using VC++ 6.0 as it can’t be developed in Java. Two different versions of NIDS and ITM are developed for testing the proposed architecture. First version of NIDS and ITM is developed to work as described in proposed architecture section. Second version of NIDS and ITM are developed as Compromised NIDS and Compromised ITM. Compromised version of NIDS and ITM are developed in such a way that they do not follow the normal flow of execution.

Experimental Setup for performing experiments has 3 departments. Each department has 3 desktop computers. NIDS is present on separate computer. Different departments are connected through router; firewall is present between router and departmental LAN. Proposed architecture is tested for six different scenarios. For testing each scenario new installation of NIDS and ITM is done.

4.1 Scenario 1: Failure of NIDS

After successful and working installation of the system, one instance of the NIDS is terminated using Windows task manager. Within few seconds a new working instance of NIDS is started by ITM.

4.2 Scenario 2: Compromised NIDS

This time while installing a system, one instance of Compromised NIDS is used in one department and remaining instances of NIDS are of normal NIDS. Within few seconds ITM terminates the Compromised NIDS and starts normal version of NIDS

4.3 Scenario 3: Failure of ITM

This time after successful and working installation of the system, one instance of the ITM is terminated using Windows task manager. Within few seconds a new working instance of ITM is started by second ITM.

4.4 Scenario 4: Compromised ITM

This time while installing a system, one instance of Compromised ITM is used and Second instance of ITM is of normal ITM. Within few seconds ITM terminates the Compromised ITM and started normal version of ITM

4.5 Scenario 5: Failure of all ITM

This time after successful and working installation of the system, all instances of the ITM are terminated using Windows task manager. Within few seconds All NIDS sent a High Alert Message to Administrator.

4.6 Scenario 6: Launching DDOs attack from one department

Two machines of one department were used to launch the DDoS attack within the organization. After detection of DDOs attack by NIDS, no packet from these two machines was detected in remaining two departments.

5. CONCLUSION AND FUTURE WORK

Use of Firewall within the organization network along with IDS is very effective away of implementing a security. Distribution of NIDS among different departments makes it more immune to Intrusion and avoids the problem of single point of failure. Distributed nature of NIDS results in early Detection of attacks launched from organizations against organization itself. DoS/DDoS/Probing attack launched from the organization can't affect the entire organization as it gets detected and blocked at NIDS of the Department itself.

Future work is to develop intelligent ITM, so that it can dynamically take preventive steps against all kinds of Intrusive behavior.

6. REFERENCES

[1] Liwei Kuang, Mohammad Zulkernine, "An Intrusion-Tolerant Mechanism for Intrusion Detection Systems", The Third International Conference on Availability, Reliability and Security, ISBN: 0-7695-3102-4, IEEE 2008

[2] Feng Zhao, Qing-Hua Li1, Li Jin, "An Intrusion-Tolerant Intrusion Detection Method Based On Real-Time Sequence Analysis", Fifth International Conference on Machine Learning and Cybernetics, Dalian, ISBN: 1-4244-0060-0, IEEE 2006

[3] Paulo Sousa, Alysson Neves Bessani, Miguel Correia,Nuno Ferreira Neves, Paulo Verissimo, "Resilient Intrusion Tolerance through Proactive and Reactive Recovery", 13th IEEE International Symposium on Pacific Rim Dependable Computing, ISBN: 0-7695-3054-0, IEEE 2007

[4] Hui Zhao, Shanhong Zheng ,Wanlong Li, LiJuan Zhang, "A Network Intrusion-Tolerant System Based on Adaptive Algorithm", 5th International Conference on Wireless Communications, Networking and Mobile Computing ISBN: 978-1-4244-3693-4, IEEE 2009

[5] Xiaohong Qu, Zhijie Liu , Xiaoyao Xie, "Research on Distributed Intrusion Detection System Based on Protocol Analysis", IEEE 2009

[6] Senda Hammouda, Lilia Maalej, Zouheir Trabelsi, "Towards Optimized TCP/IP Covert Channels Detection, IDS and Firewall Integration", ISBN: 978-2-9532443-0-4, IEEE 2008

[7] Hamed Salehi, Hossein Shirazi, Reza Askari Moghadam, "Increasing overall network security by integrating Signature-Based NIDS with Packet Filtering Firewall", International Joint Conference on Artificial Intelligence, ISBN: 978-0-7695-3615-6, IEEE 2009

[8] Zongpu Jia, Shufen Liu, Guowei Wang, "Research and Design of NIDS Based on Linux Firewall", 1 st International Symposium on Pervasive Computing and Applications, IEEE 2006

[9] Duanyang Zhao, Qingxiang Xu, Zhilin Feng, "Analysis and Design for Intrusion Detection System Based on Data Mining", Second International Workshop on Education Technology and Computer Science, ISBN: 978-0-7695-3987-4, IEEE 2010

[10] Mohammad Akbarpour Sekeh, Mohd. Aizaini bin Maarof, "Fuzzy Intrusion Detection System via Data Mining Technique With Sequences of System Calls", Fifth International Conference on Information Assurance and Security, ISBN: 978-0-7695-3744-3, IEEE 2009

[11] Ming-Yang Su, Kai-Chi Chang, Hua-Fu Wei, and Chun-Yuen Lin, "A Real-time Network Intrusion Detection System Based on Incremental Mining Approach", ISBN: 1-4244-2415-3, IEEE 2008

[12] Mrs. P. Kola Sujatha Dr. A. Kannan S. Ragunath K. Sindhu Bargavi S. Githanjali, "A Behavior Based Approach to Host-Level Intrusion Detection using Self-organizing Maps", First International Conference on Emerging Trends in Engineering and Technology, ISBN: 978-0-7695-3267-7, IEEE 2008