SECURITY OF THE NETWORK BASED ON DURATION OF ATTACKS

Sneha Vinod Kumar, Yashashwini V, Anusha Pai G, Dr.Yuvaraju B.N

snehavinokumar@gmail.com

pravesaya@gmail.com

anushapaig@gmail.com

yuvarajubn@gmail.com

Department of CSE, NIE

Mysore.

---***---

Abstract - *The growth of the computer networks and internet demands a high level of security against the unauthorized access and invasion. Though there are many tools and softwares to check the security, in this paper, we try to alert the administrator about the attack considering time as one of the most important aspects. All this is done in the physical layer. This method initially monitors the network, captures the packets on the network. In the next step data is extracted, parsed and then based on the duration of attack, an alert is made to the administrator or system. This method is not enough to judge the total criteria of network security but it does cover one of the major aspects of security i.e. time. It is expected that these methods can be used as a base for further experiments and enhancements to build a stronger security against attacks.*

Key Words: **Network security, Duration of attack, Data extraction, Packet sniffing, Flood attack.**

1. INTRODUCTION

Since the growth of computer networking, internet related activities etc. are having a rapid growth in today's world. It is always not a safe place to store or transmit important data through the internet as there may be malicious attacks that affect our data or disturb the system's functionality. One such type of attacks can be grouped as the cyber-attacks which is a major issue in the field of networks [1]. Another way in which the attacks are found is by using different kinds of tools and softwares that causes threat to the network. These tools are designed in such a way that they are launched to capture, visualize and find defects in different fields with respect to their requirements and goals.

The main cause that allows the scope of unauthorized access and threats, solely depend upon the complexity of the attackers' algorithm, defects in the design of the network and even poor understanding or knowledge about attacking tools and software algorithms. Before these weaknesses are found out by the attackers, the administrators must analyze and tighten the security. One way of preventing defects is to perform multiple tests and estimate different methodologies before the actual implementation of the design.

Yes of course, attacks are always complex in nature and guessing the exact method for preventing it is quite complex too though comparing it with different attacking algorithms may give us an idea in finding out an appropriate method sometimes.

Although intruders may obtain complex tools and software algorithms and high knowledge about the network structures for attacking, one of the most important concepts during attacking is time, because these complex tools and softwares take time to run their algorithms [2].

In this paper, we present a new method of looking into these complex algorithms. Even though algorithms and their tools change according to the latest design modules or structures of networks the only concept that remains the same is time. This is done using the physical layer. Initially, monitoring is done on the network and packets are captured accordingly. The information is extracted from each of these packets and parsed accordingly. A list is maintained depending on the required content. Time is checked for a given threshold value and a check is made for packet flooding. The type of attack is determined and an alert is made to the administrator.

The paper is organized as follows. In Section 2, a review on current network security design is provided. Section 3 introduces the actual working of this system, different modules it uses for this particular method, what are the benefits and limitations etc. In Section 4, suggestion for improvisation of this method is given. Finally discussions and conclusions are given in Section 5 of the paper. Section 6 contains the papers that can be referred.

2. LITERATURE SURVEY

Different security measures have been implemented against attacks. Different methods on how analysis is made on security are mentioned here. Since an overall security cannot be provided for attacks it is best said to use different realistic models to analyze security. Some methods use probabilistic models; some use graphs to measure the patterns of attacks, and a few of them use transitional models to determine the system's states [3]. All these are done on the basis of some information that was got during the previous design defects. All these work solely depends on the individual's skill set. Attacks depend on classes of attacks also [4].

Network intrusion systems are very good at listening to traffic and comparing them against known attacks in its database. In this paper we present a new method for preventing attacks using time as the main parameter. It compares the time of the packets captured with the threshold time and attacks are determined. Before all this is done, some of the preliminary steps are as follows.

The sniffer technology was created to perform different tasks, but that doesn't mean that you cannot use this tool for things other than what it was created for. Sniffer and its robust engine capture traffic as well as the performing the following capabilities:

A. Filtering

Sniffer has a powerful filtering capability. The filtering capability allows a network administrator to have a focused visibility on the network, right down to the bit level. A network administrator can quickly zoom down to a specific problem by defining a filter for it.

B. Capturing

Sniffer not only examines every packet on the wire it also saves and captures the packets into the trace files. Forensic techniques, when combined with the captured trace files, can provide enough evidence to identify the attacker or security events that have occurred [5].

C. Extraction

In this division data is extracted according to the requirement and its fields such as the version, header length, TTL, source, destination etc. are parsed and these data are stored. If the time duration is found to exceed the threshold time then it detects the attack else keeps updating the time record which it had stored previously.

D. Alert system

After the detection of attack, an alert is send to the administrator and the admin can decide what he wants to do with it.

3. METHODOLOGY

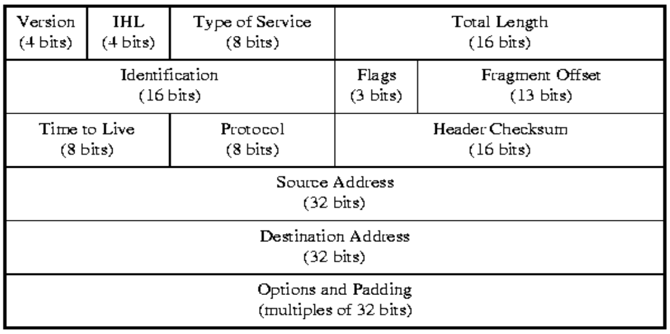
Here the actual way of doing the process is described as follows:

A. Packet capturing

In this step data is intercepted across the network and it is captured and stored in a byte array.

B. Packet analyzer

In this step, packet that is captured is analyzed. It also decodes the packet's raw data, showing the values of various fields in the packet, and analyzes it. The raw data extracted are version, header length, type of service identification etc. as shown in the figure these raw data extracted are stored in the form of a structure. The validity of the packet is also looked out.



<table>
<tr><td>Version
(4 bits)</td><td>IHL
(4 bits)</td><td>Type of Service
(8 bits)</td><td colspan="2">Total Length
(16 bits)</td></tr>
<tr><td colspan="3">Identification
(16 bits)</td><td>Flags
(3 bits)</td><td>Fragment Offset
(13 bits)</td></tr>
<tr><td colspan="2">Time to Live
(8 bits)</td><td>Protocol
(8 bits)</td><td colspan="2">Header Checksum
(16 bits)</td></tr>
<tr><td colspan="5">Source Address
(32 bits)</td></tr>
<tr><td colspan="5">Destination Address
(32 bits)</td></tr>
<tr><td colspan="5">Options and Padding
(multiples of 32 bits)</td></tr>
</table>

Fig -1: IP header.

C. Packet parsing

Parsing is done based on the protocol we use like UDP, TCP/IP etc. For example if we take identification field, there will be two segments like fragment and do not fragment where 0 indicates fragment and 1 indicates do not fragment.

For these extracted data a data type is declared. After parsing is done filtering of the content is done [6].

D. Administrative dashboard module

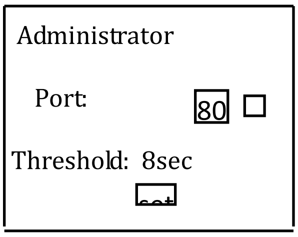
After capturing ,analyzing, parsing the data obtain from these process are stored and dashboard is made to admin this dashboard may contain IP address, type of service, connected time, elapsed time etc. as shown in the figure service, connected time, elapsed time etc. as shown in the figure.

IP	SERVICE	PORT	CONNECTED - TIME	
			TIME-ELAPSED	
192.168. - -	Http - -	80 - -	10:34:12 - -	15 2 sec - -

Fig -2: Dashboard Diagram.

E. Threshold value

For each connection there will be a threshold time, which is set i.e., a fixed time for that connection to check whether the connection duration is more than the provided threshold value. To check this, a table is maintained with IP addresses and their initial time connection. Then operations like delete/update are performed as to add on the time if the connection is from the same IP address again. If the time exceeds, a note is made for that IP address as shown in the figure.



Administrator

Port: 80 □

Threshold: 8sec

Fig -3: Setting threshold values.

F. Backtracking:

If the connection time exceeds the threshold time then backtracking is done using the IP address and the intruder is detected.

G. Flood attack:

When packet arrives at an instant of time and its the server is flood attack. When flood attack occurs IP address is noted that packets get rejected [7].

H. Alert to admin:

Whenever an intruder is detected an alert is given to the admin and the intruder's IP address, time, type of attack etc. are displayed.

3.1 Algorithm for Random Early Detection (RED)

The packets arriving when queue is full are dropped and also sometimes the packets at the front (head) of queue are dropped. To keep throughput high and delay low and also provide room for the packets on network RED algorithm is used. This algorithm randomly marks the packets to be dropped. It also assumes that the source responds to the lost packets.

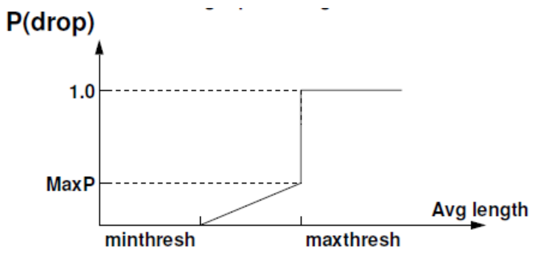


Fig -4: Concept of Random Early Detection.

Marking probability (pb) based on queue length and is given by

$$Pb = maxp\ (avg - minth)\ /\ (maxth - minth)$$

maxth set to twice the minth.
History of unmarked packets is given by

$$Pb = Pb\ /\ (1 - count\times Pb)$$

Where count is the number of unmarked packets that has been arrived since the last marked packet.

Apart from this, RED algorithm compares the new packet with the dropped packet and drops it if it is from the same flow.

3.2 Advantages

1. Since the proposed system is based on attack duration, it covers one of the most important aspects that is time, which is irrespective of the protocol or type of message used by the intruder.
2. This concept based application reduces the complexity of determining the possible attacks.

3. Gives the details of attackers as well as type of attack, duration that it lasted etc., within a single application.
4. Ensures network security in an efficient manner by determining flood attack.
5. After determining the packets of the attackers causing the flood, they are removed from the network which in turn reduces the network traffic.
6. Time can be made as a flexible factor so that it can be changed according to the application.

3.3 Limitations

7. This paper describes about detecting the threats caused by an intruder but doesn't provide the actual security i.e. stopping the attacks.
8. Only time cannot judge the overall security of the network but it is an important parameter for network's security.

4. FUTURE ENCHANCEMENTS

Until now this paper talks about the classification of the packets that are on the network based on duration of the packets and hence, attacks are determined only on the basis of the packet arrival time. So for further improvement, denial of services can be done. An application can be developed which can determine the attack duration for particular services. Time is set for browser, FTP applications or other services in a similar manner to that of the packet. This can limit the access based on the requirements of different services separately, hence limiting malicious intruders.

Another different way of enhancing security can be done by configuring the application so that it runs in router in such a way that the packets entering the router are checked for intrusion before it is allowed to be passed across it, hence limited threats can be made.

5. CONCLUSIONS

This paper presented a new concept on the security of the networks by introducing time as the main concept because even though there are different means for attacking, one important and common factor is time as attacker's algorithm is more complex in nature.

As we proceed further, in the first step packet capturing is done. Later information is extracted, analyzed and parsed. All this is done for each of the packets. Information is stored in a hash table and threshold value is set. If any of the IP addresses exceed their connection time beyond the threshold value, an alert is made to the administrator. If a particular IP address sends excess packets on the network, it is determined by a flood graph and the packets are dropped along with alerting the administrator. This provides an easy and alternative method for determining the attackers in spite of their complex tools and algorithms.

This concept does not cover the entire security for a network but provides an important concept that can list the attackers in a different fashion. We hope that this presented paper will become a helpful guideline for organizations and researchers who are working on the security issues.

6. REFERENCES

[1] Gan B, Brendlen Jr JH. Nuclear power plant digital instrumentation and control modifications. In: Nuclear science symposium and medical imaging confer-ence, conference record of the 1992 IEEE; October, 1992. p. 730–732.

[2] Shahab Forghani, Navid Habibi, Mohsen FiroozbakhtDepartmentofComputerEngineering,Islamic Azad University, South TehranBranch,Tehran,Iran,St_sh_forghani@azad.ac.ir,St_n_habibi@azad.ac.ir, Firoozm@azad.ac.ir

[3] D.J. Leversage, E. James, Estimating a system's mean time-to-compromise, IEEE Sec. Priv. 6 (1) (2008) 52–60. March 16–19.

[4] B.Z. Moayedi, M. Abdollahi Azgomi, A game theoretic framework for evaluation of the impacts of hacker's diversity on security measures, Reliab. Eng. Syst. Safety 99 (1) (2012) 45–54.

[5] Kai Guo, The design and implementation of the packet capturing system based on Winpcap, Xidian University, pp. 3, 2013.

[6] M. Attig, G. Brebner, "400 gb/s programmable packet parsing on a single fpga", *Architectures for Networking and Communications Systems (ANCS) 2011 Seventh ACM/IEEE Symposium on*, pp. 12-23, oct. 2011.

[7] M. Bellaiche and J.-C. Gregoire, "Syn flooding attack detection based on entropy computing," in Global Telecommunications Conference, 2009.