Journal of Computer Science, 9 (2): 271-276, 2013
ISSN 1549-3636

doi:10.3844/jcssp.2013.271.276 Published Online 9 (2) 2013 (http://www.thescipub.com/jcs.toc)

A Proficient Traceback Approach Using Provincial Locality Aspects to Eliminate Denial of Service Attacks

[1]S. Periyasamy and [2]K. Duraiswamy

[1]Department of Information Technology, K.S.R. College of Engineering,
[2]Department of CSE, K.S.Rangasamy College of Technology,
Tiruchengode, Namakkal, Tamilnadu, India

Received 2012-11-17, Revised 2013-03-19; Accepted 2013-04-12

ABSTRACT

A Denial-of-Service (DoS) attack, a menace to the availability of resources and service to the intended user, is usually by augmenting the traffic in the communication medium. These attacks originate in either ways, internal or external to a network with the aim to suspend the legitimate user from getting his/her service. The DoS attacks have been countered through various approaches, yet this problem remains stable in field. The traceback mechanisms of the attacker necessitate a large amount of valuable information which is usually hidden by the attacker or not documented in the network. Moreover the network has strict constraints over the usage of memory resources by the nodes and routers, equivalent to an empty memory nature. The amount of data reasonably required for computation would increase the processing delay which is usually unexpected. The counter measures proposed tried to detect the network under attack or to track the attacker with some degree of information available. Nowadays these attacks have evolved to break out from all those detection approaches with greater immunity to not reveal their identity. This study works with the physical zone addresses to detect and traceback the identity of the attacker. The packet sent from the attacker carries merely the part of its identity. Yet the Provincial Assessment Attributes (PAA) possesses the geographical locality aspects in terms of Continent Code, Country Code, State Codes and the Area Codes along with its IP address. Accepting the factor that IP is spoofed in most cases, the routers in the path are still able to keep track of these PAA prospects irrespective of the faked IP. Hence this mechanism could be implemented with minimal computation, leading to the attacker with considerable and fruitful results in identifying the same. Besides, this method takes deep care to authenticate and not to affect the traffic of legitimate users.

Keywords: Network Security, Dos Attack, Traceback, Security, Provincial Attributes

1. INTRODUCTION

The internet services have been the only source of fast and accurate references for every uncertainty of the mankind. Repository of the internet comprises the detailed information of almost every field on earth and beyond. The absolute open framework of the internet service provides easy access to the requester from each nook and corner of the world. Apart from the regular users, there exists a category of users working to disturb the amenities of internet service. Internet services are greatly affected by the Denial-of-Service attacks. The attacker performs many functions to alter the customary request and response between the user and the internet. The security of the internet services is questioned by these attacks and despite the remedial options; the attacks remain stable. Preventive approaches have been proposed by diagnosing the entry points of attacks in the architecture. Yet the attackers always tend to find a new way for their objective.

Corresponding Author: S. Periyasamy, Department of Information Technology, K. S. R. College of Engineering, Tiruchengode, Namakkal, Tamilnadu, India

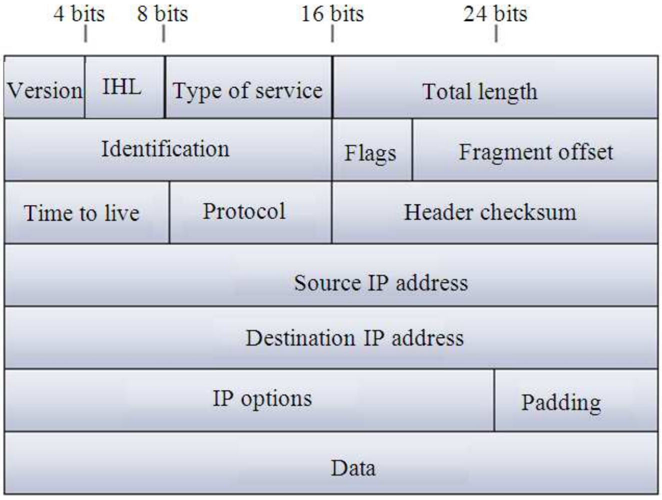

Fig. 1. IP header diagram

Fig. 2. Regions marked with individual colors for differentiation

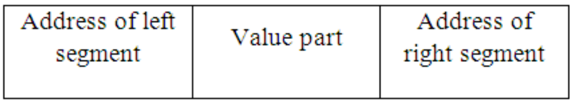

Fig. 3. Traceback mechanism

The prominent way of perturb the service is by a Denial-of-Service attack. The attacker would act on the network communication channel by sending meaningless packets to cause congestion (Ghazali and Hassan, 2011). The intended users would sense the medium to be free before they start to transmit their packets. On sensing the busy state, the node waits till the network channel is freed. Unaware that the medium is under attack, the node waits for infinite time still hoping for its turn. The attacker succeeds by making the intended user to suspend the transmission activity.

The IP Header is depicted above in **Fig. 1** for the traceback process and the possibilities with parameters in it. The **Fig. 2** describes the differentiation of the countries by their individual colours. Similarly, using the fact of individuality, the locations of the countries can be used for a security reason. With the available space in the IP header, the notations of provincial values can be incorporated into the segments of the packet along with the original values. **Figure 3** indicates the information to be stored in the packet during transmission.

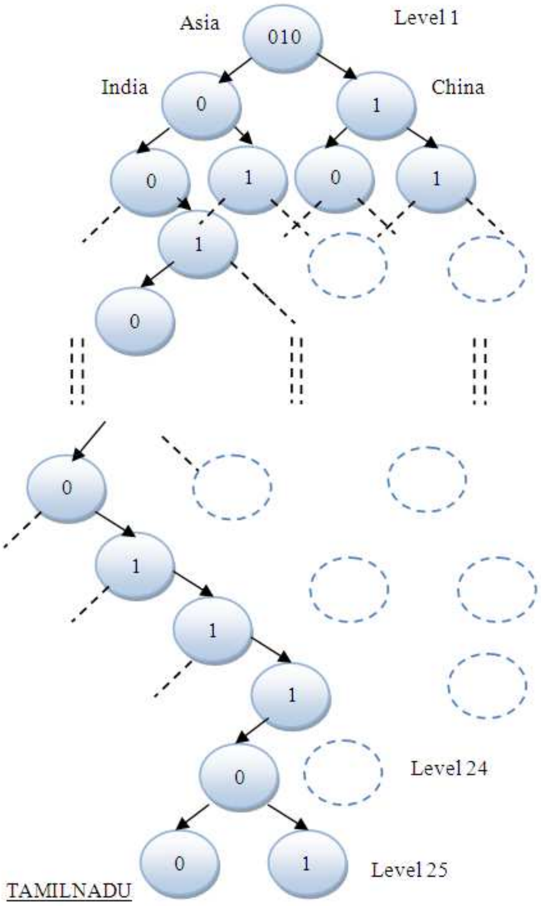

Fig. 4. Traceback mechanism

The countermeasures can be designed to prevent the network from attacks, to detect the network under attack or to identify the attacker. There are approaches to traceback the attacker with the available information in the routers and the packet itself. In most cases the IP address of the attacker is spoofed (altered) or the present information is not vital enough for tracing back to the attacker. Every packet is updated with the information of the routers it crossed. Each packet contains separate spaces for holding the information of the source address, destination address, the space for the data and other spaces including the information of the routers it has to bypass for reaching the destination. Every router in turn indicates that the packet has reached its checkpoint (decrements the value by one) and adds the next hop information. But conditions for a long path (32 hops) do not facilitate the updating of the flow. Moreover the space provided in the header field is limited and cannot be depended on for proper identification. Traditional approaches of the traceback mechanism check the upstream routers for the origin, or packet marking techniques authenticate the originality of the packets differentiating them from attack packets. Every countermeasure introduced a new way of DoS attack since the mechanism is quite easy to predict.

A factor that needs immediate attention is that the more time spent to detect the attack results in more serious consequences over the resources of the network. The countermeasure should be fast enough to mitigate the attacks as soon the attack is detected. The attacker is capable of evading the detection mechanisms for a considerable large time to take control over the resources. The changes or effects are irreversible in most cases of the attacks.

1.1. The Strategy of Using Provincial Assessment Attributes

The proposed approach handles the concept of tracing back the attacker with the physical zonal details (Chen *et al*., 2007; Gao and Ansari, 2005). Every node in the network possesses a location either stationery or dynamic. The locality metrics are not subjected to change even in case of a mobile user. A mobile user said to change his locality every one hour or so, still requires the function of the routers to establish a communication link over the destination node. Even if the routers are dynamic, they should always be a part of a boundary which is assigned with a Provincial Assessment Attribute (PAA). The paths of the packets from every node are routed through the intermediate nodes in between the source and destination. Hence instead of using the IP address of the particular node for traceback process, the physical location of the node is considered which cannot be altered.

The identities of the places over the world are denoted by individual names. The provinces of the world on the whole are represented by the names of Continents, Countries, States, Districts, Areas and finally villages. The conceptual model of the Provincial Assessment Attributes (PAA) introduces the same methodology. The provinces are identified by a two digit value. The above shown **Fig. 4** comprises of the values of Asia, leading to India and China with the next corresponding values. The fourt digit in the sequence denotes India and the entire sequence will definitely identify the specific region in Indis. Further allocations of the values are made to the states and districts. To eliminate the difficulties in naming almost every user in the locality, this strategy limits the concept to provide the value to the most prominent physical locations. When a packet is transmitted from node A to a destination node, the provincial attribute values of the routers are updated into separate sub-spaces of the 16 bit information field of the IP header.

The areas of the continents are:

- Asia-17,139,445 square miles (44,391,162 square km)
- Africa-11,677,239 square miles (30,244,049 square km)
- North America-9,361,791 square miles (24,247,039 square km)
- South America-6,880,706 square miles (17,821,029 square km)
- Antarctica-About 5,500,000 square miles (14,245,000 square km)
- Europe-3,997,929 square miles (10,354,636 square km)
- Australia-2,967,909 square miles (7,686,884 square km)

Largest Continents in Population:

- Asia-4,055,000,000 (Over 4 billion)
- Africa-1,108,500,000 (Over 1 billion)
- Europe-729,871,042 (including all of Russia)
- North America-522,807,432
- South America-379,919,602
- Australia-20,434,176

Antarctica-No permanent residents but up to 4000 researchers and personnel in the summer and 1000 in the winter.

The information of these physical locations cannot be altered by the attacker in real time. These predefined values to the routers needs to be assigned based on the province it resides in. Each province in a country of a particular continent carries the values of the area of origin of the attack.

The further sub-net of the particular locality could be derived with the available router information. When the routers are traced back, the first information would be the value of the previous router from a certain province. Leading back to all the routers in the path would lead to the location of the attacker. Even if the IP address of the node is spoofed, the location could be identified or the packets from the specific locality could be blocked to mitigate the DoS attack (Chen *et al*., 2007). When the packets are found to be dispatched from the same locality and if the number exceeds a normal level, then the network considers the packets as an attack and alarms the detection algorithm.

Every region of the different countries is distinguished by different colors. Each color represents a unique PAA. These assignments are made accordingly such that there are no collisions or repetitions between the different regions of the same locality. Differentiations are marked by the boundaries of each area and the entry and exit routers residing on the boundary. Obviously there are no possibilities of possessing a network in regions of no human existence. Hence the impractical conditions for humans would be considered to limit the allocation of PAA metrics to those regions.

Considering the limitless extendibility and the infinite routes of the internet services as a prime factor, the Provincial Locality Attributes (PAA) is assigned. Packets from Asian continent irrespective of the number of thousands are marked by the Asian PAA. Similarly to every continent is differentiated by the PAA. The country codes are unique and thus the area codes. Ultimately the routers through which the packets from an organization enter and exit would be marked with the PAA. Once found to exceed the threshold value, the routers are ordered to block the function of transmitting the packets in and out of the network. Preventing the entry of the attack packets is achieved at the router after detection of the attack.

This proposed strategy introduced the conceptual model of assigning a unique attribute of identifying the attacker, beyond the existing marking terminologies. Location attributes are stable and consistent beyond the political changes on the boundaries of each nation. Evaluation of the strategy includes the assignment of different and non overlapping values to the available areas enabling the user to differentiate and locate the router or the source from which every packet originated. Initializing the values to the widespread network is the most challenging factor now. Mechanism to traceback the attacker has to be discussed indeed.

1.2. Traceback Mechanism

The messages sent from a source to a destination node needs to be segregated into smaller packets for easier and faster transmission process (Ghazali and Hassan, 2011). Each packet is assigned to a route or path from the source via a number of nodes and routers and at most of 32 hops in case of an internet service. The routers are themselves nodes which act as the intermediate to forward a packet to the destination registered in every individual packet of the broken message. The packet is entered with the information on the type of packet, the message type, the size of the packet, source and destination information, the IP addresses of the source and destination along with the path information. Beyond the stated level of hops in the medium, the quality of the small sized packet is considerably weak and would be discarded. Every packet needs to be acknowledged by the receiver node upon the reception of the right packet in terms of quality and content. This is the benign process of transmission of packets in a wireless communication.

At the receivers end, all the segregated packets (Al-Duwairi and Govindarasu, 2006; Burch and Cheswick, 2000) are acknowledged to receive the corresponding packets and collected sequentially or in any random order. If a packet has failed to be received, it is requested to b retransmitted again. This proves that without the whole set of divided packets cannot constitute the meaningful message. After collecting, the packets are grouped together. Understanding that the subsets of the segregated packets may be transmitted and received in any order for a security reason, the receiver side waits until all the packets are transmitted and reported.

Along with the standard information, the Provincial Assessment Attributes (PAA), values which represent the locality of the nodes are added. This PAA would be marked by the protocols and standards of the layers responsible for transport of the packet to the destination. This conditions that the node itself cannot alter the mechanism of appending the PAA with the message packet. After appending, the message packets are allowed to be transmitted and follow the procedure of hopping the medium. With every hop it crosses, the information of the PAA is updated without disturbing the initial or the source address

At the receiver's end, the verification of PAA attributes commences with ensuring the unaltered representations and further additions. Validation of these PAA metrics is carried out in a renowned methodology and theoretical model of a binary search tree. A binary search tree categorizes the input values in its place after comparing with its disparity from that of its root node. If the input is found to be greater than the value of root node, it is then placed on the descending arm on its right side. Otherwise the new value occupies a left arm position. Similarly the input value is evaluated with every other node with the same criteria. Considering the same case in tracing back the initiator in this study, implementing a binary digit for representing the continents, countries and to specific regional spaces facilitates the correctness with very minimal effort. Evaluation by this strategy becomes even simpler since the attributes are mere 0s and 1s.

The process can be understood easier with the help of the following example. Assigning the PAA metric of Asia as 010 and in bound countries with their respective PAA metrics following the first three continent denoting binary digits is the first step (Keromytis *et al*., 2002; Snoeren *et al*., 2001; Xiang *et al*., 2008). Tracing back is needed only if the node initiating the packets needs to be identified. Hence the computation is not a primary process which is mandatory along with all other operation. The continents, only limited to seven, are determined without the need for any computation. Secondly, the continent code is taken as the root value.

The sample algorithm for tracing the source of attack can be as follows:

```
/* Number of elements in the "FixedValue" array to the
number of subspace of Globe"G" */
begin
Continents_val=allocated_memory1
If(Continents_val==001) begin
Continent_set=1;
Subspace(continent_set,remaining_bit)
end
Else If(Continents_val==010)
 begin
Continent_set=2;
Subspace(continent_set,remaining_bit)
end
else If(Continents_val==100)
begin
Continent_set=3;
Subspace(continent_set,remaining_bit)
end
else If(Continents_val==110) begin
Continent_set=4;
Subspace(continent_set,remaining_bit)
end
If(Continents_val==101)
begin
Continent_set=5;
Subspace(continent_set,remaining_bit)
end
If(Continents_val==111) begin
Continent_set=6;
Subspace(continent_set,remaining_bit)
end
Else
Continent_set=7;
Subspace(continent_set,remaining_bit)
end
End
Subspace(int location, int bit[22])
Begin
*ptr=bit[3];
I=3;
```

```
Recursiveofsub(ptr)
begin
if(bit[i]==0)
begin
ptr=ptr->left;
recursiveofsub(ptr);
end
else
ptr=ptr->right
recursiveofsub(ptr);
end
end main
```

The corresponding PAA metrics identifying the regions of the respective continent is divided into every single bit thereafter considered for evaluation. The fourth bit is checked to be a 0 and placed in the descending arm on left side of the tree. On possession of a value 1 would place it on the right side arm. Every level on the descending arm is predefined with a regional name. The regions are named based on their distance measures, directional measures. Let us say that India would be the country with its states organized at different levels of both arms.

The destination nodes process the packets to check for the identity of the PAA to ensure the origin and route that the packets travelled. After collection and verification of all individual packets of the entire message and reassemble them to obtain the meaning. Without the right PAA values, the packets are considered to be the attack packet and made to undergo a few other standards. Those packets may be intended communicated packets of authenticated users, but transferred at a wrong time. This mechanism avoids the chances of false negatives and false positives. The appended values of the packets would determine the source and the route of the transmission path in case of attack packets. The attack packets are identified by the variations in the Provincial Assessment Attributes of some hundreds of packets meant for suspending the normal functioning of the network.

2. CONCLUSION

The study contemplates a different approach of identifying the attacker in any network with the information on the locality of the corresponding nodes. Being able to assign the attributes representing the geographical locations to the routes and nodes, it becomes a inflexible metric which could be spoofed in present cases. Spoofing eliminates the chances of directing the attacker to a great percentage as the rate of false negatives are in urge to be reduced by any efficient methodology. This study reflect the new technique for limiting the amenities of a jammer to masquerade their identity and impose a threat to the confidential networks. Constant and proficient metrics of location based entries would enhance the security level of the wireless network.

3. REFERENCES

Al-Duwairi, B. and M. Govindarasu, 2006. Novel hybrid schemes employing packet marking and logging for IP traceback. IEEE Trans. Parallel Distrib. Syst., 17: 403-418. DOI: 10.1109/TPDS.2006.63

Burch, H. and B. Cheswick, 2000. Tracing anonymous packets to their approximate source. Carnegie Mellon University, pp: 319-327.

Chen, R., J.M. Park and R. Marchany, 2007. A Divide-and-conquer strategy for thwarting distributed denial-of-service attacks. IEEE Trans. Parallel Distrib. Syst., 18: 577-588. DOI: 10.1109/TPDS.2007.1014

Gao, Z. and N. Ansari, 2005. Directed geographical traceback. Proceedings of the 3rd International Conference on Information Technology, Research and Education, Jun. 27-30, IEEE Xplore Press, pp: 221-224. DOI: 10.1109/ITRE.2005.1503108

Ghazali, K.W.M. and R. Hassan, 2011. Flooding distributed denial of service attacks-a review. J. Comput. Sci. 7: 1218-1223. DOI: 10.3844/jcssp.2011.1218.1223

Keromytis, A.D., K.V. Misra and D. Rubenstein, 2002. SOS: Secure overlay services. Proceedings of the Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, Aug. 19-23, ACM Press, New York, USA., pp: 61-72. DOI: 10.1145/633025.633032

Snoeren, A.C., C. Partridge, L.A. Sanchez, C.E. Jonesn and F. Tchakountio *et al*., 2001. Hash-Based IP traceback. Proceedings of the Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, Aug. 27-31, ACM Press, New York, USA., pp: 3-14. DOI: 10.1145/383059.383060

Xiang, Y., W. Zhou and M. Guo, 2008. Flexible deterministic packet marking: An IP traceback system to find the real source of attacks. IEEE Trans. Parall Distrib. Syst., 20: 567-580. DOI: 10.1109/TPDS.2008.132