A Hybrid Approach for Detecting, Preventing, and Traceback DDoS Attacks

ALI E. EL-DESOKY[1], MARWA F. AREAD[2], MAGDY M. FADEL[3]
Department of Computer Engineering
University of El-Mansoura
El-Gomhoria St., Mansoura, Dakahlia, 35516
EGYPT
Email: adesoky@mans.edu.eg[1]
Email: engineer_m_a@yahoo.com[2]
Email: mfares73@yahoo.com[3]

Abstract: The main objective of this study is to design a hybrid technique to defend against the DDoS attack. Distributed Denial of Service (DDoS) attacks constitute one of the major threats and among the hardest security problems in today's Internet. With little or no advance warning, a DDoS attack can easily exhaust the computing and communication resources of its victim within a short period of time. A network simulation program NS2 will be applied to test the efficiency of the proposed technique in filtering out all the attack packets, and traceback them to their sources. Many criterias will be used to prove the efficiency of the proposed technique, one of them is the ratio of the dropped packets, the second is the ratio of the passed legal packets, and finally, the accuracy of determining the actual source of the attack packets. Applying these techniques will enhance and increase the efficiency in preventing the success of these DDoS attacks.

Key-Words: DDoS attacks, Firewall, Bloom filter, Packet marking, Packet logs, Packet tracing.

1 Introduction

Today, the Internet is an essential part of our everyday life and many important and crucial services like banking, shopping, transport, health, and communication are partly or completely dependent on the Internet. As the Internet was originally designed for openness and scalability without much concern for security. Unfortunately, it is not possible to reliably determine the source of received IP packets, as the protocol does not provide authentication of the packet based on the source address field, which can be easily faked (IP spoofing). Furthermore the Internet routing infrastructure also does not keep information about forwarded packets. Malicious users can exploit these design weaknesses of the internet to wreak havoc in its operation. Incidents of disruptive activities which have raised the most concern in recent years are the denial-of-service (DoS) attacks [1] whose sole purpose is to reduce or eliminate the availability of a service provided over the Internet, to its legitimate users. This is achieved either by exploiting the vulnerabilities in the software, network protocols, or operation systems, or by exhausting the consumable resources such as the bandwidth, computational time and memory of the victim. The first kind of attacks can be avoided by patching-up vulnerable software and updating the host systems from time to time. In comparison, the second kind of DoS attacks is much more difficult to defend. This works by sending a large number of packets to the target, so that some critical resources of the victim are exhausted and the victim can no longer communicate with other users.

In the distributed form of DoS attacks (called DDoS), the attacker first takes control of a large number of vulnerable hosts on the internet, and then uses them to simultaneously send a huge flood of packets to the victim, exhausting all of its resources. There are a large number of exploitable machines on the internet, which have weak security measures, for attackers to launch DDoS attacks, so that such attacks can be executed by an attacker with limited resources against the large, sophisticated sites. The attackers in DDoS attacks always modify the source addresses in the attack packets to hide their identity, and making it difficult to distinguish such packets from those sent by legitimate users. This idea, called IP address spoofing has been used in major DDoS attacks in the recent past.

These recent DDoS attack used highly sophisticated and automated tools which ironically are readily available over the Internet, to be downloaded and used by anyone, even computer novices, to attack any Web site. Network worms have been developed and are available for the automatic scanning, exploitation, deployment, and propagation process of the attack tools.

The devastating effects of the DoS and DDoS attacks have caused attention of scientists and researches, leading to various mechanisms that have been proposed to deal with them. However, most of them are ineffective against massively distributed DoS attacks involving thousands of compromised machines. It was observed, that there is no single approach that can defend against (D)DoS attacks effectively by itself; there should be a combination among various schemes with different merits. A proposal for a new technique named "a hybrid packet track and traceback mechanism for IP traceback" will be introduced in this paper to defend against the most harmful and difficult to detect DDoS attacks - those that use IP address spoofing to disguise the attack flow, this proposed scheme is composed of two kinds of IP traceback techniques.

The first one is marking-based detection and filtering scheme to defend massively distributed DoS attacks. It based on a firewall that can distinguish the attack packets (containing spoofed source addresses) from the packets sent by legitimate users, and thus filters out most of the attack packets before they reach the victim. Unlike the other packet-marking based solutions [1, 2], this technique has a very low deployment cost, since it requires the cooperation of only about 20% of the Internet routers in the marking process.

The second one is a log-based traceback [3] packet logs are kept throughout the network, ideally one per segment. The SPIE architecture (Source Path Isolation Engine) [4] is a log-based traceback that allows the path of a packet to be traced. The logs are not kept by the routers themselves, but by a packet monitor that listens to a router interface. The set of packet monitors form an overlay network that allows the source of individual IP packets to be determined. The general goal of log-based traceback is to build an attack graph, given an IP packet, its approximate time of receipt and its destination, which is usually called the victim. The attack graph consists of vertices that represent nodes (routers and hosts) that have processed the packet, and the links through which the packets were transmitted. False positives are the nodes of the attack graph that have not really processed the packet. This technique improves the precision and efficiency of traceback, by returning an attack graph that precisely identifies the route traversed by a given packet allowing the correct identification of the attacker.

The reset of the paper is organized as follows: section 2 discusses the existing approaches for defending DDoS attacks and argues why they are not adequate by themselves, and there should be a combination among various schemes with different merits. In section 3 we give an overview of a marking-based detection and filtering (MDADF) scheme. Section 4 presents and analyzes an existing precise and efficient log-based IP traceback scheme. Section 5 outlines our suggested hybrid scheme that makes a combination between the two schemes presented in sections 3, and 4. And explains how this hybrid technique not only synthesizes the advantages but also compromises the disadvantages of the above two methods. Finally we conclude our work in section 6.

2 Approaches for Defending DoS/DDoS Attacks

Current DoS/DDoS defenses can be classified into three categories: preventing mechanisms, reactive mechanisms, and source-tracking mechanisms.

2.1 Preventive Defenses

The preventive schemes aim at improving the security level of a computer system or network; thus preventing the attack from happening, or enhancing the resistance to attack.

A proactive server roaming scheme [5] belongs to this category. This system is composed of several distributed homogeneous servers and the location of active server changes among them using a secure roaming algorithm. Only the legitimate users will know the server's roaming time and the address of new server. All connections are dropped when the server roams, so that the legitimate users can get services at least in the beginning of each roaming epoch before the attacker finds the active server out again. Such solutions are generally costly and difficult to really prevent attacks.

2.2 Reactive Solutions

The reactive measures for DDoS defense are designed to detect an ongoing attack and react to it by controlling the flow of attack packets to mitigate the effects of the attack.

One of the proposed reactive schemes, given by Yaar et al. [6] uses the idea of packet marking for filtering out the attack packets instead of trying to find the source of such packets. This scheme uses a path identifier (called Pi) to mark the packets; the Pi field in the packet is separated into several sections and each router inserts its marking to one of these. Once the victim has known the marking corresponding to attack packets, it can filter out all such packets coming through the same path.

The success of the reactive schemes depends on a precise differentiation between good and attack packets.

2.3 Source Tracking

The source-tracking schemes, on the other hand, aim to track-down the sources of attacks, so that punitive action can be taken against the attacker and further attacks can be avoided. The existing solutions fall into three groups: packet marking, message traceback, and logging.

Many different packet marking schemes have been proposed, for encoding path information inside IP packets, as they are routed through the internet. The idea is first put forward by Savage et al. [1], called probabilistic packet marking (PPM), in which the routers insert path information into the Identification field of IP header in each packet with certain probability, such that the victim can reconstruct the attack path using these markings and thus track down the sources of offending packets. Belenky and Ansari [2] propose a deterministic marking approach (DPM), in which only the address of the first ingress interface a packet enters instead of the full path the packet passes (as used in PPM) is encoded into the packet.

In the message traceback method [7], routers generate ICMP traceback messages for some of received packets and send with them. By combining the ICMP packets with their TTL differences, the attack path can be determined. Some factors are considered to evaluate the value of an ICMP message, such as how far is the router to the destination, how quick the packet is received after the beginning of attack, and whether the destination wishes to receive it.

Another method called logging [4] is to record packet information at routers. The path to the attacker can be determined by the routers exchanging information with each other.

A common problem existing in these solutions is that the reconstruction of attack path becomes quite complex and expensive when there are a large number of attackers (i.e. for highly distributed DoS attacks). Also, these types of solutions are designed to take corrective action after an attack has happened and cannot be used to stop an ongoing DDoS attack.

3 An effective protection scheme

Generalizing from the various defense mechanisms, a good protection scheme against DDoS attacks should be based on continuous monitoring, precise detection and timely reaction to attacks. The following characteristics are desirable:

The scheme should be able to control or stop the flow of attack packets before it can overwhelm the victim. The timely detection and immediate reaction to an attack is essential, to prevent the depletion of resources at the victim location. The suitable place to deploy defense scheme are the perimeter routers or the firewall of a network.

In stopping the flow of attack packets to the victim, the scheme must ensure that packets from legitimate users are successfully received so that the service to the legitimate users is not denied or degraded. Any degradation in service would signify a partial success for the denial of service attack.

The implementation cost should be low. Unless most internet users fully recognize the threats posed by DoS/DDoS attacks, it is difficult to get cooperation from them in defending such attacks, especially when the investment required is costly. Therefore, any viable DDoS defense scheme should require minimal participation of third party networks or intermediate routers on the internet.

A good defense mechanism should be able to precisely distinguish the attack packets from the legitimate packets. What makes it difficult to control or stop the DDoS attacks is the use of spoofed IP address [8].

If we can distinguish the packets which have spoofed IP addresses, then these packets can be selectively filtered out by a firewall to stop most attacks.

3.1 Distinguishing the attack packets

In this section, an overview of a packet marking method which will help in distinguishing DDoS attack packets from packets sent by legitimate users will be presented.

Though source IP addresses can be spoofed by attackers, the paths packets take to the destination are totally decided by the network topology and routers in the Internet, which are not controllable by

the attackers. Therefore, the path of a packet has taken can really show the source of it. By recording the path information, the packets from different sources can be precisely differentiated, no matter what the IP addresses appeared in the packets. Packet marking, which is firstly proposed by Savage et al. in the PPM scheme [1], is a good method to record path information into packets.

To indicate the path packet traverses, the simplest way is to add all the routers' IP addresses into the packet. The number of hops a packet passes through in the Internet is about 15 on average and mostly less than 31. Since the length of a path is uncertain, it is difficult to reserve enough space in the packet to put all the addresses, and the packet size increases as the length of the path increases.

In order to avoid the increase in packet size, a possible method is to but all information into a fixed space. A router puts its IP address into the marking space of each packet it receives; if there is already a number in that space, it calculates the exclusive-or (XOR) of its address with the previous value in the marking space and puts the new value back. This method ensures that the marking does not change its length when a packet travels over the Internet, so the packet size remains constant.

In order to make the marking scheme fast and efficient, part of the header in an IP packet will be used as the marking field. The 16-bit Identification field in IP header has been commonly employed as the marking space [1, 2, 6].

In this marking scheme, each cooperating router on the path of an IP packet would insert a mark on the ID-field of the packet. The generated marking should be such that two packets reaching the victim through different routers are guaranteed to have distinct markings.

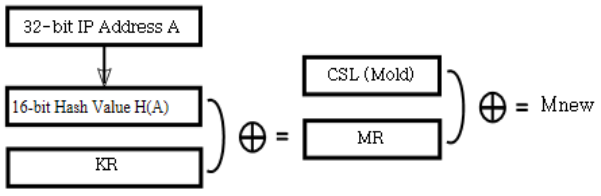

Fig.1: The marking scheme

The mark made by a router would be a function of its IP address. To fit the 32-bit IP address A of a router into the ID field, we employ a hash function H that converts A to a 16-bit value.

Since attackers can easily know the routers' IP addresses, they can spoof the marking on a packet if they know the hash function used by each router. We cannot expect every router in the Internet to participate in the marking scheme and mark all packets passing through it. If a packet with such a spoofed marking passes through a route where there are no co-operating routers, this packet is impossible to be identified as an attack packet.

To avoid such spoofing of the marking, each router R uses a 16-bit key K_R (which is a random number chosen by the router) when computing its marking. The marking for a router R is calculated as $M_R = H(A)$ XOR K_R, where A is the IP address of the router. After receiving a packet the router computes the marking $M = M_R \oplus M_{old}$, if an old marking Mold exists in that packet, and replaces M_{old} with M.

3.2 Inserting Order Information

One possible drawback with the scheme mentioned above is that the marking on a packet depends only on the routers it passes through, but not on the order passing them. This means that the packets which pass the same routers on two different paths have the same marking.

To make the marking scheme more effective, each router will perform a Cyclic Shift Left (CSL) operation on the old marking M_{old} and compute the new marking as $M = CSL(M_{old}) \oplus M_R$. In this way, the order of routers influences the final marking on a packet received by the firewall. Figure 1 shows the complete marking scheme.

3.3 Filtering scheme

The MDADF scheme employs a firewall at each of the perimeter routers of the network to be protected and the firewall scans the marking field of all incoming packets to selectively filter-out the attack packets, as shown in Figure 2.

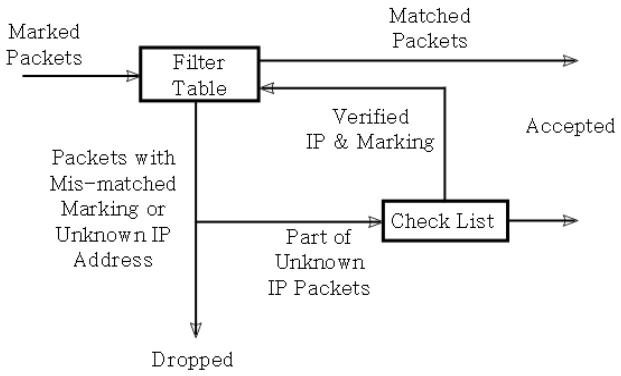

Fig.2: The filtering system structure.

On employing this scheme, when a packet arrives at its destination, its marking depends only on the path it has traversed. If the source IP address of a packet is spoofed, this packet must have a marking that is different from that of a genuine packet coming from the same address. The spoofed packets can thus be easily identified and dropped by the filter, while the legitimate packets containing the correct markings are accepted.

4 An overview of the source path isolation engine

Log-based IP packet traceback employs packet logs that are stored throughout the network, possibly one per segment. In the SPIE architecture [4] logs are kept for recently processed packets. As the amount of storage is limited, newer records overwrite older ones when necessary. If the traceback operation was requested for a given packet, e.g. by an IDS (Intrusion Detection System), the request is executed by running a distributed search throughout the network logs in order to discover the routers that processed the packet, and eventually its source.

In order to log packets processed by backbone routers, massive storage space is required, even for relatively slow links and for short time frames. Storing packets from several sources also involves privacy issues. SPIE uses Bloom filters to solve both these problems, and stores information obtained from a packet hash. A packet hash should uniquely identify an IP packet. The hash also preserves confidentiality when a search is executed across several autonomous domains. In order to compute the hash of a given IP packet, SPIE only uses the invariant portion of the packet plus 8 bytes from the payload.

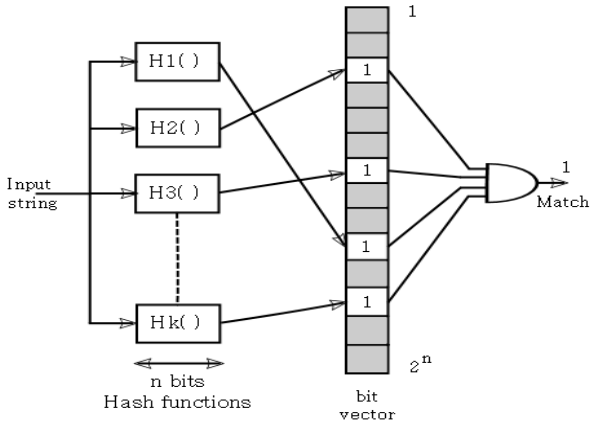

Fig.3: Bloom filter example.

A Bloom filter is a data structure used to store a set of elements allowing a fast membership-test operation. Figure 3 shows a Bloom filter using k hash functions.

The SPIE architecture for IP Packet Traceback is shown in figure 4. The three basic components of this architecture execute the set of tasks involved in determining the origin and route traversed by a packet. These components are described below.

DGA (Data Generation Agent): This component computes and stores the hash value of the router's outgoing packets. The data is stored locally on the DGA for a fixed time interval whose length depends on storage space constraints.

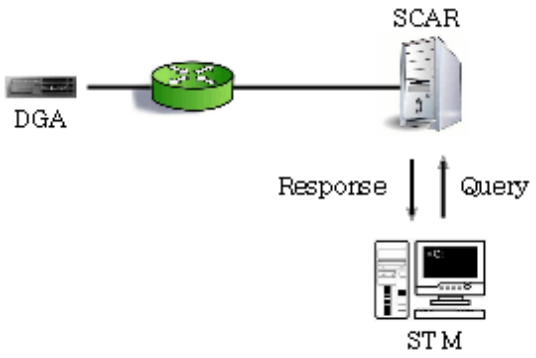

Fig.4: The SPIE architecture.

SCAR (SPIE Collection and Reduction Agent): This component is responsible for searching. It maintains information about a set of DGAs in a network region. After an application generates a traceback request for a given packet, SCAR will receive a request from the STM (described below) and will then forward the request to all DGAs within its region. The DGAs send their filters to be evaluated by the SCAR. If the packet search succeeds, a partial attack graph is returned to the STM.

STM (SPIE Traceback Manager): This component is the front-end to the traceback mechanism and manages the system as whole. When a request is received, it is authenticated and validated and then dispatched to the selected SCARS. The STM then receives the resulting attack graphs from which it builds the complete attack graph which is returned.

5 Outlines of the proposed technique

In the last two years researchers working in the field of defending DDoS attacks observed that, there is

no single approach that can defend against (D)DoS attacks effectively by itself; there should be a combination among various schemes with different merits.

In Packet track and traceback mechanism [9] approach, they employ a cooperation between two DoS defending schemes, path identification (Pi) and Internet control message protocol (ICMP), as a packet track and traceback mechanism, which features rapid response and high accuracy. In this scheme, routers apply packet marking scheme and send traceback messages, which enables the victim to design the path tree in peace time. During attack times the victim can trace attackers back within the path tree and perform rapid packet filtering using the marking in each packet. The merits of this scheme is that, Traceback messages overcome Pi's limitation, wherein too much path information is lost in path identifiers; whereas path identifiers can be used to expedite the design of the path-tree, which reduces the high overhead in iTrace.

However, there are still several disadvantages in this design that limit its use. One is that the path identifier (Pi) can not be guaranteed to be globally unique; there are collisions among identifiers of different paths which could reduce the accuracy. The other one is that iTrace imposes a high traffic in the network.

So, we propose a hybrid packet marking and logging scheme for IP traceback based on the packet marking technique introduced above in section 3, and packet logging technique in section 4.

The packet marking technique introduced above is simple and feasible in deployment because it does not require any cooperation between routers, and it is rapid in responsiveness because the decision can be made on a single-packet basis.

The log-based traceback technique introduced above allows individual packets to be traced. It imposes no more traffic in the network. But it requires some storage capabilities in the routers or devices connected to the routers.

So, the proposed technique will synthesizes the advantages of the above two methods.

6 Conclusion

Depending on previous studies and techniques used to defend against DDoS attacks, we expect from this new Hybrid technique introduced in this paper that applies MDADF packet marking scheme in conjunction with SPIE traceback in log-based technique, eliminates the drawbacks in previous defending methods, represented in increased percent of collision between marks and the increased traffic in the network. In this new technique, the victim can perform rapid packet filtering and design the path-tree in peace time, then quickly find the attacker during times of attack.

References:

[1] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in proceeding of ACM SIGCOMM'00, Vol.30, No.4, 2000, pp. 295-306.

[2] A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," IEEE Communications Letters, Vol.7, No.4, 2003, pp. 162-164.

[3] M. Sung, Xu J, Li J, and Li L, "Large-Scale IP traceback in high-speed Internet: practical techniques and Information-theoretic Foundation," IEEE/ACM Transactions on Networking, Vol.16, No.6, 2008, pp. 1253-1266.

[4] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, and et al., "Single-packet IP traceback," IEEE/ACM Transactions on Networking, Vol.10, No.6, 2002, pp. 721-734.

[5] S. M. Khatab, C. Sangpachatanaruk, R. Melhem, D. Mosse, and T. Znati, "Proactive server roaming for mitigating denial-of-service attacks," in proceedings of the 1st International Conference on International Technology: Research and Education (ITRE'03), 2003, pp. 286-290.

[6] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against DDoS attacks," in proceedings of the IEEE Symposium on Security and Privacy, 2003, pp. 93-107.

[7] A. Mankin, D. Massey, C. L. Wu, S. F. Wu, and L. Zhang, "On design and evaluation of Intention-driven ICMP traceback," in IEEE International Conference on Computer Communication and Networks (ICCCN'01), 2001, pp. 159-165.

[8] Y. Chen, "A Novel Marking-based Detection and Filtering Scheme Against Distributed Denial of Service Attack," Masters Thesis, University of Ottawa, 2006.

[9] L. Li and S. Su-bin, "Packet track and traceback mechanism against denial of service attacks," Journal of China Universities of Posts and Telecommunications, Vol.15, No.3, 2008, pp. 51-58.