Asian Journal of Information Technology 9 (3): 154-158, 2010
ISSN: 1682-3915
© Medwell Journals, 2010

A Survey of Routing Instability with IP Spoofing on the Internet

[1]D. Srinath, [2]J. Janet and [3]Jose Anand
[1]St. Peter's University, Chennai, India
[2]Vel Tech Engineering College, Chennai, India
[3]Jaya Engineering College, 602024 Chennai, India

Abstract: The Internet has experienced a tremendous growth in its size and complexity since its commercialization. Internet hosts are threatened by large-scale Distributed Denial-of-Service (DDoS) attacks. DDoS attacks typically rely on compromising a large number of hosts to generate traffic to a single destination, the severity of DDoS attacks will likely increase as greater numbers of poorly secured hosts are connected to high-bandwidth Internet connections. In this study we present the routing instability in the Internet due to the IP Spoofing and analyzed a survey of possible attacks and controlling mechanism available.

Key words: Attacks, DDoS, internet, IP Spoofing, routing protocols, security

INTRODUCTION

The Internet consists of rapidly increasing number of hosts interconnected by constantly evolving networks of links and routers. Internet connects thousands of Autonomous Systems (ASs) operated by many different administrative domains such as Internet Service Providers (ISPs) companies and universities (Gao, 2001). Routing within an AS is controlled by intra domain protocols such as Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS) and Routing Information Protocol (RIP).

IP Spoofing has often been exploited by DDoS attacks to conceal flooding sources and dilute localities in flooding traffic and coax legitimate hosts into reflectors, redirecting and amplifying flooding traffic (Wang *et al*., 2007). IP Spoofing is also known as IP address forgery and is a hijacking technique in which the hacker masquerades as a trusted one to get the access to a network. Spoofing is a process whereby one entity masquerades as another.

IP Networks are vulnerable to source address into packet headers. DDoS block legitimate access by either exhausting victim server's resources or saturating stub networks access links to the Internet. By masquerading as a different host an attacker can hide its actual identity and location, rendering source-based packet filtering less effective. Many popular attacks use IP Spoofing and require the ability to forge source addresses. DDoS attacking tools spoof IP addresses by randomizing the 32-bit source address field in the IP header Dietrich (2000) which conceals attacking sources and dilutes localities in attaching traffic. IP Spoofing remain popular for number of reasons like as it makes isolating attack traffic from legitimate traffic header: packets with spoofed source address may appear to be from all around the Internet and also it presents the attacker with an easy way to insert a level of indirection (Duan *et al*., 2008).

While DdoS attack the attacker increases the amount of illegitimate traffic originating from the systems under the users control (Snyder *et al*., 2007). This results in a positive increase by some ratioα where $0 \leq \alpha \leq 1$ relative to the traffic that was present in the system to begin with The attacker is analyzed into four kinds as follows:

Random: Ratio of attack traffic for each division of the attack dimension is a randomly chosen normalized distribution.

Base: Attack traffic is spread so that it matches the distribution for divisions in the base traffic distribution for the attack dimension.

Uniform: Attack traffic is spread evently amongst the divisions in the attack dimensions.

Loaded: Attacker directs all of the attack traffic at initial division of the attack dimension.

In order to analyze all possible moves for attacker and defender a sensitivity matrix was generated in all the four kinds of attacker.

RELATED WORK

Attackers may insert arbitrary source address into IP packets and are not able to control the actual paths that the packets take the destination. Park and Lee (2001)

Corresponding Author: D. Srinath, St. Peter's University, Chennai, India

proposed the route-based packet filters as a way of mitigating IP Spoofing which has single-path $P_{(s,d)}$ routing between the source node s and the destination node d.

Yaar *et al*. (2003) proposed the path identification in which each packet along a path is marked by a unique Path Identifier (P_i) of the path and the victim node can filter packets based on the P_i carried in the packet header.

Cheng *et al*. (2002) proposed Hop-Count Filtering (HCF) in which each end system maintains a mapping between IP address aggregates and valid hop counts from the origin to the end system Packets that arrive with a different hop count are suspicious and are therefore discarded or marked for further processing.

Chen and Song (2005) proposed that the attack can be most effectively detected at the victim end where all the attacked packets can be observed readily so that the attack detection module is placed near the victim and the packed filtering module is placed as close to the attack source as possible.

Chen *et al*. (2007) proposed Attack Diagnosis (AD) a novel attack mitigation scheme that combines the concept of Pushback and packet marking to thwart DDoS attacks. Attack Diagnosis takes a divide and conquer strategy in the sense that it consists of a repetitive process of isolating an attacker and the filtering its traffic.

Mahajan *et al*. (2002) proposed an attack detection module near the victim and also execute the packet filtering close to the attack sources. The scheme adopts hop-by-hop transmission of control messages to coordinate packet filtering. The Time-To-Live (TTL) field present in the packet ensures authentication to the control message packets. The proposed scheme uses the Aggregate-based Congestion Control (ACC) module for local congestion detection and high-bandwidth traffic throttling.

Dean *et al*. (2002) proposed the utilization of probabilistic packet marking for IP trace back. The 16-bit identification field in the IP header of each packet will be marked with partial path information. So the entire information regarding the path can be recovered after receiving many packets. But this approach is vulnerable to packet markings forgery.

Liu *et al*. (2006) proposed packet passport method for Spoofing elimination and are used to verify the source of a packet by attaching a sequence of marks. Each mark is created using a secret shared between the source and one AS on the path to the destination. It cannot properly validate packets during route changes or multi-path routing and only requires extensive secret sharing when deployment is large. Sung and Xu (2003) utilized an attack detection model to differentiate attack traffic from legitimate traffic and use a packet filtering module to filter attack packets. Shen *et al*. (2008) presented a signature and verification based IP Spoofing prevention method named Automatic Peer-to-Peer based Anti-Spoofing (APPA) method. APPA has two levels named Intra-AS level and Inter-AS gateway level.

In an Intra-AS level, the end host tags a one-time key into each outgoing packet and the gateway ate the AS border verifies the key. In an Inter-AS level, the gateway at the AS border tags a periodically changed key into the leaving packet and the gateway at border of the destination AS verifies and removes the key.

Fadlallah and Serhrouchni (2006) proposed a signaling architecture for tracing anonymous IP packets back towards their source where specialized signaling entities exchange through a simple security-oriented signaling protocol, reliable signaling information can be used for a simple and efficient trace back.

Lin *et al*. (2008) proposed to monitor the traffic pattern in order to alleviate distributed denial of service attacks. In this method, a bandwidth allocation policy is adopted to assign normal users to a high priority queue and suspected attackers to a low priority queue. The simulations conducted in the network simulator shows that its effectiveness in blocking attack traffic while maintaining constant flows for legitimate traffic.

Santiraveewan and Permpoontanalarp (2004) proposed a new methodology for verifying the vulnerability of firewall configurations to IP spoofing attack and for synthesizing IP spoofing-free configurations. The methodology is based on graph theory which provides a simple and intuitive approach to the vulnerability analysis of the attack.

From the perspective of fair resource allocation a client has to consume some of its own resources to compute the solution and the number of resources that a client needs to commit is commensurate with the puzzle difficulty (Feng *et al*., 2005). Another method for fair resource allocation is max-min server centric router throttles Yau *et al*. (2005). This scheme enables a server under attack to contact a perimeter of upstream routers to install router throttles where each router only forwards the max-min fair share of the traffic that is allowed by the server.

DDoS ATTACKS

DDoS attack presents a very serious threat to the stability on the Internet. In this, a large number of hosts are amassed to send useless packets to jam a victim or its Internet connections (Song and Manjkopoulos, 2006). There are two reasons that are why defending against DDoS attacks is challenging. First, very large number of attackers is involved in DdoS attack. Even if the volume of traffic sent by a single attacker might be small, the volume of aggregated traffic arriving at the victim host is overwhelming. Secondly, it is very difficult to trace the attack traffic back to its sources, since attackers usually spoof their IP address (Chen *et al.*, 2007).

DDoS attacks can be considered into two distinct approaches named router-based approach and host-based approach. In case of router-based approach the required defense mechanisms are installed inside the IP routers. This is used to trace the source of attack or to detect and block the attacking traffic.

Rather than router support but also coordinates different routers and networks which results in wide spread deployment. In host-based approach an Internet server is used as resource management schemes or by significantly reducing the resource consumption to withstand the flooding traffic.

DDoS attack can be categorized into four classes named prevention, detection, mitigation and response. Among this mitigation techniques can be categorized into two. First is a resource allocation problem which employ techniques such as client puzzles, max-min server centric router throttles or differentiated service to allocate network or server resources to clients in a fair fashion thus preventing attackers from consuming an excessive amount of network resources. Secondly attacks by filtering or rate-limiting attack packets that consist of two modules named an attack detection module and a packet filtering module.

The attack detection module is used to extract the characteristics of attack packets or attack signatures such as source IP address or marked IP header values. After that this information is used by the packet filtering module to filter malicious packets. The attack detection module is placed near the victim and packet filtering module is placed as close to the attack as possible (Chang, 2002).

Instead of subverting services, DDoS attacks limits and block legitimate user's access by exhausting victim server's resources or saturating stub networks access links to the Internet (Venkatesu *et al.*, 2008) Attackers often spoof IP addresses by randomizing the 32 bit source address field in the IP header to conceal flooding sources and localities in flooding traffic.

Each spoofed packet with the victims IP address is masquerade with the source IP address to network attacks. Because of the stateless and destination based routing of the Internet, it is difficult to counter IP Spoofing. The IP Protocol lacks the control to prevent a sender from hiding the origin of its packets and destination based routing does not maintain state information on senders and forwards each IP packet toward its destination without validating the origin of the packet.

CONTROL MECHANISM

Because of DDoS attacks IP Spoofing was exploited to conceal flooding sources and localities in flooding traffic and amplifying flooding traffic. The ability to filter spoofed IP packets near victims is essential to their own protection as well as to their avoidance of becoming involuntary attacks. An attack can forge any field in the IP header that falsify the number of hops an IP packet takes to reach its destination. Basically there are two different control approaches for preventing the DDoS attacks. First is a router-based controlling mechanism and second is a victim-based controlling mechanism. The router-based approach makes improvements to the routing infrastructure while the victim-based approach enhances the resilience of Internet servers against attacks.

The router-based control mechanism installs defense mechanisms inside IP routers to trace the origin of attack or to detect and block attacking traffic. This approach not only requires router support but also coordination among different routers and networks and wide-spread deployment to reach their potential. Inside a router both the off-line analysis of flooding traffic and on-line filtering of DDoS traffic was performed in router-based control approach.

The off-line IP trace back attempts to establish procedures to track down flooding sources but help pinpoint locations of flooding sources. It also does not keep sustain service availability during an attack (Savage *et al.*, 2000). To detect abnormal traffic patterns and foil DDoS attacks on-line filtering mechanisms rely on IP router enhancements. For efficient prevention coordination among different routers network and its wide spread deployment other than router support is needed.

Implementation of security mechanism in the host is provided in the victim-based control approach (CERT, 2000). To deploy defense mechanisms than network service providers a potential victim has a much stronger incentive. This approach uses sophisticated resource management schemes which provide accurate resource accounting and fine grained service isolation and differentiation.

So victim-based filtering that detects and discards spoofed traffic without any router support is essential to protecting against DDoS attacks. Due to resource depletion caused by spoofed IP packets the victim-based approach is unlikely to be able to sustain service availability under intense attacks. Moreover this mechanism cannot prevent the victim server from consuming CPU resource in servicing interrupts from spoofed IP traffic as this mechanism work at the transport-layer.

CONCLUSION

Despite the fact that Spoofing based attacks have severe consequences and are wide-spread much of the present day Internet. To trace back the origin of an Internet attack, strategic importance is given to cyber space security.

From the survey it is analyzed that each method has certain features that make it more suitable to implement in one situation than another. The routing instability in the Internet due to the IP Spoofing is depicted in this study and a survey of possible attacks and controlling mechanism available are made.

RECOMMENDATION

By introducing a filter function on the forwarding path of the packets, the cost can be analyzed. Also research can be done on the AS relationship and routing information which improves the performance of the IP Spoofing. For Internet security it is essential to trace back to the original source of the attacks. IP Spoofing makes it difficult for the victim to determine the IP packets origin.

As a result, there is a need for a mechanism that could rapidly trace back to the origin of attacks for the victim. Trace back can be performed by Intelligent Techniques to get better performance.

REFERENCES

CERT, 2000. Advisory CA-96.21. TCP SYN flooding and IP spoofing. http://www.cert.org/advisories/CA-1996-21.html.

Chang, R.K.C., 2002. Defending against flooding-based distributed denial-of-service attacks: A tutorial. IEEE Commun. Magaz., 40: 42-51.

Chen, C. and Q. Song, 2005. Perimeter-based defense against high bandwidth DDoS attacks. IEEE Trans. Parallel. Distrib. Syst., 16: 526-537.

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.

Cheng, J., W. Haining and G.S. Kang, 2002. Hop-count filtering: An effective defense against spoofed traffic. Proceedings of the 10th ACM Conference on Computer and Communications Security, Oct. 27-30, New York, USA., pp: 30-41.

Dean, D., M. Franklin and A. Stubblefield, 2002. An algebraic approach to IP traceback. ACM Trans. Inform. Syst. Secur., 5: 119-137.

Dietrich, S., N. Long and D. Dittrich, 2000. Analyzing distributed denial of service tools: The shaft ease. Proceedings of USENIX LISA, Dec. 3-8, New Orleans, La, USA., pp: 329-339.

Duan, Z., X. Yuan and J. Chandrashekar, 2008. Controlling IP spoofing through interdomain packet filters. IEEE Trans. Dependable Secure Comput., 5: 22-36.

Fadlallah, A. and A. Serhrouchni, 2006. PSAT: Proactive signaling architecture for IP traceback. Proceedings of the 4th Annual Communication Networks and Services Research Conference, May 24-25, IEEE Computer Society, Washington, DC, USA., pp: 293-299.

Feng, W., E. Kaiser and A. Luu, 2005. Design and implementation of network puzzles Proc. IEEE INFOCOM, 4: 2372-2382.

Gao, L., 2001. On inferring autonomous system relationships in the internet. IEEE/ACM Trans. Network., 9: 733-745.

Lin, C.H., J.C. Liu, H.C. Huang and T.C. Yang, 2008. Using adaptive bandwidth allocation approach to defend DDoS attacks. Proceedings of the International Conference on Multimedia and Ubiquitous Engineering, April 24-26, IEEE Computer Society, Washington, DC, USA., pp: 176-181.

Liu, X., X. Yang, D. Wetherall and T. Anderson, 2006. Efficient and secure source authentication with packet passport. Proceedings of the 2nd Conference on Steps to Reducing Unwanted Traffic on the Internet-Volume 2, (SRUTI'06), San Jose, CA., pp: 2-2.

Mahajan, R., S.M. Bellovin, S. Floyd, J. Joannidis, V. Paxson and S. Shenker, 2002. Controlling high bandwidth aggregates in the network. J. Comput. Commun. Rev., 32: 62-73.

Park, K. and H. Lee, 2001. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. Proceedings of ACM SIGCOMM, Aug. 27-31, San Diego, California, USA., pp: 15-26.

Santiraveewan, V. and Y. Permpoontanalarp, 2004. A Graph-based methodology for analyzing IP spoofing attack. Proceedings of the 18th International Conference on Advanced Information Networking and Application Volume 2, March 29-31, IEEE Computer Society, Washington, DC, USA., pp: 227-227.

Savage, A., D. Wetheralle, A. Karlin and T. Anderson, 2000. Practical network support for IP trace back ACM SIGCOMM Comput. Commun. Rev., 30: 295-306.

Shen, Y., J. Bi, J. Wu and Q. Liu, 2008. A two-level source address spoofing prevention based on automatic signature and verification mechanism. Proceedings of the 13th IEEE Symposium on Computers and Communications, July 6-9, Tsinghua University, Beijing, pp: 392-397.

Snyder, M.E., R. Sundaram and M. Thakur, 2007. A game-theoretic framework for bandwidth attacks and statistical defenses. Proceedings of 32nd IEEE Conference on Local Computer Networks, Oct. 15-18, IEEE Computer Society, Washington, DC, USA., pp: 556-563.

Sung, M. and J. Xu, 2003. IP traceback-based intelligent packet filtering: A novel technique for defending against internet DDoS attacks. IEEE Trans. Parallel Distrib. Syst., 14: 861-872.

Venkatesu, N., V. Deepan-Chakravarthy and D. Sathya, 2008. An effective defense against distributed denial of service in grid. Proceedings of the 1st International Conference on Emerging Trends in Engineering and Technology, July 16-18, IEEE Computer Society Washington, DC, USA., pp: 373-378.

Wang, H., C. Jin and K.G. Shin, 2007. Defense against spoofed IP traffic using hop-count filtering. IEEE/ACM Trans. Network., 15: 40-53.

Yaar, A., A. Perrig and D. Song, 2003. Pi: A path identification mechanism to defend against DdoS attacks. Proceedings of IEEE Symposium in Security and Privacy, May 11-14, IEEE Computer Society, Berkeley, CA, USA., pp: 93-93.

Yau, D.K.Y., J.C.S. Lui and Y. Yam, 2005 2005. Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles. IEEE/ACM Trans. Network., 13: 29-42.