ISSN: 2393-8528

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 4 Issue 3; May-June-2017; Page No. 11-14

EFFICIENT AUTHENTICATION SCHEME TO DETECT THE SPOOFER LOCATION USING PASSIVE IP TRACEBACK TECHNIQUES

Ms. A. Sheela Rini

Assistant Professor, Department of computer Science

KG College of Arts and Science, Coimbatore.

Received 20 March 2017; Accepted 28 April. 2017

ABSTRACT

Internet plays a vital role in the modern world. As the internet grows day by day the security problem also arises. Intruders spoof the packets by using their spoofed IP addresses. Nowadays installing Intrusion Detection Systems (IDS) coupled with firewalls, and monitoring networks enables us to quickly detect and react to unauthorized access. However, even if these tools can detect illegitimate activities, their sources cannot be identified. Denial of service and Distributed denial-of-service (DDoS) attacks present an Internet-wide threat. In Denial of service attacks huge amount of un-wanted packets are sent by the attacker to the IP address which they want to attack. The same attack is take place in DDos also but in a distributed manner. The reason is that denial of service (DoS) attacks, which have recently increased in number, can easily hide their sources and forge their IP addresses [1].

Keywords: Computer network management, computer network security, denial of service (DoS), IP traceback.

Introduction

1. SOURCE ADDRESS FORGERY AND ITS DANGERS

Communication in the Internet works by conveying packets from one place to another. Each packet, like a post card, contains a source address and a target address. The Internet fulfills the role of the post office, distributing packets to their particular destination addresses. It is interesting to observe that only the destination address is used to deliver the packet. In most cases, however, the sender wants the destination to reply. The source address is used by the destination to address the reply. Unfortunately, significant mischief can be caused by sending packets with wrong source addresses. First, it is extremely expected that those sending such unwanted messages would also like to avoid being notorious by the recipients. Even worse, a beneficiary who believes the forged source address will charge the owner of that address for the unwanted message. Some of the most horrible attacks today involve sending packets that cause automatic replies. Normally, in this case, neither the party that obtains the original packet nor the party that obtains the reply would object to a few such packets, but the attacker disposes for them to get huge numbers.

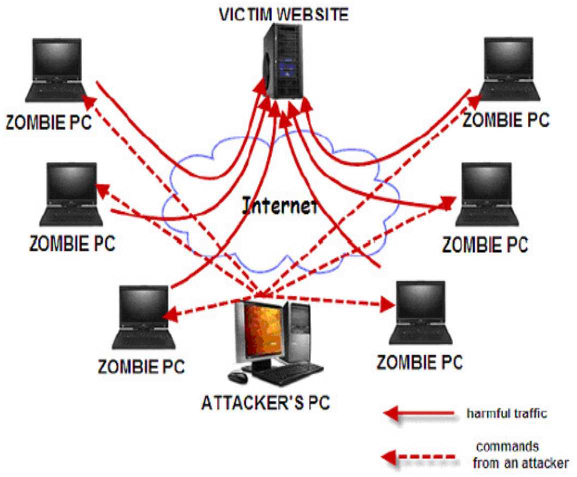

Figure 1:

Both feels like the other is attacking him. Alternatively, a large number of places are sent a smaller number of packets and the replies all converge on a victim who sees an attack that appears to come from a large number of places.[2] Even if the attack is coming from a large number of places that number can be made to appear much larger by reflecting the packets off many innocent intermediaries.

*Corresponding author: Ms. A. Sheela Rini | E-mail: sheelarini.a@gmail.com

2. PROACTIVE TRACING

This prepares information for tracing while packets are in transit. In a case where packet tracing is required, the target of the attack refers information and identifies the source of the packets.

3. REACTIVE TRACING

This "reactive tracing" starts tracing when necessary. I have selected reactive tracing that does not enlarge network traffic at normal times and generates traffic for tracing only when actual tracing is required.
Commonly reactive tracing methods trace the attack path from the target back to the source. The challenges involved in this type of method are traceback algorithm and packet matching technique.

4. HASH-BASED TRACEBACK APPROACH

This is arguably the most promising approach to packet tracking and tracing described in the research literature. It demonstrates the feasibility of tracking and tracing single packets, which has long been considered impractical.

A major disadvantage of this technique is that the storage interval at each router is very short, in the order of a minute or a few minutes at best for high-speed routers. The high bandwidth and high traffic levels of today's Internet mean that hashes based on new traffic quickly fill storage and push out the old. The problem is most rigorous for routers in or near the high-speed core of the Internet.

5. INGRESS FILTERING

One way to address the problem of anonymous attacks is to eliminate the ability to forge source addresses. One such approach, frequently called ingress filtering, is to configure routers to block packets that arrive with illegitimate source addresses, this requires a router with sufficient power to examine the source address of every packet and sufficient knowledge to distinguish between legitimate and illegitimate addresses, consequently, ingress filtering is most fusible in customer networks or at the border of ISP.

6. LITERATURE REVIEW

Basic features are produced from ingress network traffic to the interior network where protected servers exist in in and are used to form traffic records for a well-defined time interval. Monitoring and analyzing at the destination network lessen the overhead of detecting malicious behavior by concentrating only on relevant inbound traffic. This also facilitates our detector to offer shelter which is the best fit for the targeted internal network because valid traffic profiles used by the detectors are developed for a smaller number of network services. The detailed process can be found.

Drawbacks

Existing system process is the counter measurement and distance of the request from the client or DOS attackers. Different type of attacker can't control when they change their route.

7. PROPOSED METHODOLOGY

Basic features are generated from ingress network traffic to the internal network where protected servers exist in and are used to form traffic records for a well-defined time interval This also enables the detector to provide guard which is the best fit for the targeted internal network because valid traffic profiles used by the detectors are developed for a smaller number of network services.

The detailed process can be found. Multivariate correlation investigation, in which the "triangle area map generation" component is applied to extort the correlations between two distinct features within each traffic record coming from the first step or the traffic record normalized by the "feature normalization" module in this step. The occurrence of network intrusions origin changes to these correlations so that the changes can be used as indicators to identify the intrusive activities.

Advantages

Location based time measurement is take notice. Traceback routing protocol is used to find the normal packet. It detects and avoids the request from the clients.

8. IMPLEMENTATION PLAN

Step 1. Over-Provision Bandwidth to Absorb DDoS Bandwidth Peaks
This is one of the most common measures to improve DDoS attacks, but it is also possibly the most expensive, particularly since DDoS attacks can be ten times or even one hundred times greater than standard Internet traffic levels. An alternative to over-provisioning Internet bandwidth is to use a security service to scale on-

demand to soak up and strain DDoS traffic. DDoS protection services are designed to stop enormous DDoS attacks without troubling business Internet connections.

Step 2. Monitoring Application and Network Traffic

The best way to detect when you are under an attack is by observing application and network traffic. Then, you can find out if poor application performance is due to service provider outages or a DDoS attack. Monitoring traffic also permit organizations to differentiate legal traffic from attacks. Ideally, security administrators should evaluate traffic levels, application performance, abnormal behavior, protocol destruction, and Web server error codes. Since DDoS attacks are almost always executed by botnets, application tools should be able to differentiate between standard user and bot traffic.

Step 3. Detect and Stop Malicious Users

There are two primary methods to recognize DDoS attack traffic: recognize malicious users and recognize malicious requests. For application DDoS traffic, repeatedly recognizing malicious users can be the most proficient way to moderate attacks.

1. Identify known attack sources, such as malicious IP addresses that are actively attacking other sites, and recognizing anonymous proxies and TOR networks. Known attack sources report for a large percentage of all DDoS attacks. Because malicious sources continuously change, organizations should have the latest list of active attack sources.
2. Identify known bot agents; DDoS attacks are almost always achieved by an automated client. Many of these client or bot agents have exclusive characteristics that differentiate them from regular Web browser agents. Tools that recognize bot agents can immediately stop many types of DDoS sources.
3. Perform validation tests to find out whether the Web visitor is a human or a bot. For example, if the visitor's browser can accept cookies, carry out JavaScript calculations or understand HTTP redirects, then it is most likely a real browser and not a bot script.
4. Restrict access by geographic location. For some DDoS attacks, the majority of attack traffic may begin from one country or a specific region of the world. Blocking requests from objectionable countries can be a simple way to stop the huge majority of DDoS attack traffic.

Step 4. Detect and Stop Malicious Requests

Because application DDoS attacks impersonate regular Web application traffic, they can be difficult to detect through classic network DDoS techniques. However, using a mixture of application-level controls and abnormality detection, organizations can recognize and stop malicious traffic.

9. CONCLUSION AND FUTURE WORK

Once the DoS attack has been recognized, the incoming packet commence the following pushback process to recognize the locations of attack, the victim first identifies which of its upstream routers are in the attack tree based on the flow entropy deviations it has accumulated, and then submits requests to the associated immediate upstream routers. The upstream routers identify where the attack flows came from based on their local entropy deviations that they have monitored. Once the immediate upstream routers have predict the attack flows, they will forward the necessities to their immediate upstream routers, respectively, to identify the attacker sources further; this procedure is repetitive in parallel and distributed fashion until it reaches the attack source(s) or the discrimination limit between attack flows and legitimate flows is satisfied.

The former technique extracts the geometrical correlations concealed in individual pairs of two distinct features within each network traffic record, and offers more accurate characterization for network traffic behaviors. The latter technique assists the system to be able to differentiate both known and unknown DoS attacks from legitimate network traffic.

Future work is to make a technique for detecting application DoS attack by means of a new constraint-based group testing model. Theoretical analysis and preliminary simulation results demonstrated the outstanding performance of this system in terms of low detection latency and false positive/negative rate.

9. References

1. Pritish Deshpande, Virandra Patil, Mahesh Talekar, Swapnil Tapkir, Dhanajay khade, and Nitin Humbir, "Forensic spoofer location detection using passive IP traceback techniques," International Research Journal of Advanced Engineering and Science, Volume 1, Issue 2, pp. 40-43, 2016.
2. M. T. Goodrich, "Efficient packet marking for large-scale IP traceback," in Proc. 9th ACM

Conf. Comput. Commun. Secur. (CCS), 2002, pp. 117–126.

3. D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback," in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 2. Apr. 2001, pp. 878–886.

4. Yaar, A. Perrig, and D. Song, "FIT: Fast internet traceback," in Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 2. Mar. 2005, pp. 1395–1406.

5. J. Liu, Z.-J. Lee, and Y.-C. Chung, "Dynamic probabilistic packet marking for efficient IP traceback," Comput. Netw., vol. 51, no. 3, pp. 866–882, 2007.

6. K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack," in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 1. Apr. 2001, pp. 338–347.

7. M. Adler, "Trade-offs in probabilistic packet marking for IP traceback," J. ACM, vol. 52, no. 2, pp. 217–244, Mar. 2005.

8. Belenky and N. Ansari, "IP traceback with deterministic packet marking," IEEE Commun. Lett., vol. 7, no. 4, pp. 162–164, Apr. 2003.

9. ICANN Security and Stability Advisory Committee, "Distributed denial of service (DDOS) attacks," SSAC, Tech. Rep. SSAC Advisory SAC008, Mar. 2006.

10. C. Labovitz, "Bots, DDoS and ground truth," presented at the 50th NANOG, Oct. 2010.

11. G. Yao, J. Bi, and A. V. Vasilakos, "Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, 2015.

12. Pritish Deshpande, Virandra Patil, Mahesh Talekar, Swapnil Tapkir, Dhanajay khade, and Nitin Humbir, "Forensic spoofer location detection using passive IP traceback techniques," International Research Journal of Advanced Engineering and Science, Volume 1, Issue 2, pp. 40-43, 2016.