International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 3 (2014), pp. 279-284

http://www. irphouse.com /ijict.htm

Comparative Analysis of SYN Flooding Attacks on TCP Connections

Priyanka Kalra, Kamlesh Pandey and Ankit Varshney

Centre for Development of Advanced Computing, Noida (U.P.), INDIA.

Abstract

SYN flooding attacks are very common types of attacks in IP (Internet Protocol) based networks. It is a type of Denial of Service Attack in which attacker sends many SYN request with spoofed source address to a victim’s machine. Each request causes the targeted host to allocate data structures out of a limited pool of resources. After some time the targeted host goes out of resources and cannot accept further incoming SYN requests thus denying the service. This paper is about analysis SYN flooding attacks in IP (Internet Protocol) based networks with TCP connection establishment and also gives brief introduction about IP (Internet Protocol) and connection establishment in IP (Internet Protocol) based networks. This paper also discusses existing and proposed countermeasures.

Keywords: SYN, SYN flooding, IP (Internet Protocol), TCP, Denial of Service Attack.

1. Introduction

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN request to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. The Internet was designed for the minimal processing and best-effort forwarding of any packet, malicious or not. For cyberat-tackers motivated by revenge, prestige, politics, or money- this architecture provides an unregulated network path to victims. Denial-of-service (DoS) attacks exploit this to target mission-critical services. In SYN flooding attacks sends many SYN request with spoofed source address to a victim’s machine. IP spoofing, or called source IP address spoofing, refers to the technique of lying about the return address (i.e., source address) of a packet. With IP spoofing, attackers can gain unauthorized access to a computer or a network by making it appear that a message has come from a certain trusted machine by "spoofing" the IP address of that machine. DoS attacks, which come in many forms, are explicit attempts to block legitimate users' system access by reducing system availability. Here, we survey various approaches for detecting DoS flooding attacks — a network-based attack in which agents intentionally saturate system resources with increased network traffic. The malicious workload in net-work-based DoS attacks comprises network data-grams or packets that consume network buffers, CPU processing cycles, and link bandwidth. When any of these resources form a bottleneck, system performance degrades or stops, impeding legitimate system use. Overloading a Web server with spurious requests, for example, slows its response to legitimate users. This specific DoS attack type doesn't breach the end (victim) sys- tem, either physically or administratively, and requires no other pre-existing conditions except an Internet connection.

2. General Types of Attacks

To keep our discussion manageable, we've generalized it based on the exploited weakness, dividing the network based DoS attack space into vulnerability attacks and flooding attacks. In a vulnerability attack, malformed packets interact with some network protocol or application weakness present at the victim. This type of vulnerability typically originates in inadequate software assurance testing or negligent patching. The malformed attack packets interact with installed software, causing excessive memory consumption, extra CPU processing, system reboot, or general system slowing. Popular examples are the land attack, Neptune or Transmission Control Protocol synchronization (TCP SYN) flag, the ping o' death, and the targa3 attacks.Flooding attacks our focus here sends the victim a large, occasionally continuous, amount of network traffic workload. As a result, legitimate workloads can become congested and lost at bottleneck locations near or removed from the victim. Such an attack requires no software vulnerability or other specific conditions. To saturate network links, queues, and processors with workload any-where in the network, the attack can use a range of protocols, including Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), and TCP, through tools such as stream2, synhose, synk7, syn send, and hping2. Under continued attack-related congestion, flow-controlled applications will continue to increase their back-off time between retransmissions. From the users' perspective, their workload isn't being processed; a DoS situation has occurred.

3. Attack Detection

Vulnerability-attack workloads use common at-tributes to exploit software weaknesses. A TCP SYN attack, for example, requires repetitive use of specific TCP flag fields. Once the exploit is identified, adequate vendor support ensures the vulnerability is short-lived and unlikely to return. Vendors can address TCP SYN attacks using syn cache, syn cookies, and synkill mechanisms, for example. Although vendors can address vulnerability attacks by correcting protocol or application weaknesses, these types of attacks can remain problematic. If their volume is sufficient enough to cause resource depletion and subsequent performance degradation, they can be reclassified as flooding attacks. For this reason, flooding attacks are especially difficult because even the best-maintained system can become congested, thus denying service to legitimate users.

4. Survey of Detection Approaches

A detector's main goal is to detect and distinguish malicious packet traffic from legitimate packet traffic. If, for example, many clients all want Web service and a DoS attack maliciously floods many Web session requests as well, how can the Web server discriminate between the requests? Clearly, legitimate user activity can be easily confused with a flooding attack, and vice versa. When large amounts of expected or unexpected traffic from legitimate clients suddenly arrive at a system, it's called a flash event. One way to predict such events and thus distinguish them from DoS attacks is for service providers to be aware, a priori, that adding new content might trigger large request volume.5 Unpredictable and legitimate Web activity is also possible, however (as with the Slashdot effect, in which a newly posted link on a popular news or information site results in numerous Web requests). Because there is no innate Internet mechanism for performing malicious traffic discrimination, our best alter-native is to install attack detectors to monitor real-time traffic, rather than rely on static traffic load predictions. DoS attack-detection approaches can be in-stalled locally, thus protecting a possible victim, or remotely, to detect propagating attacks. Although detecting propagating attacks is desirable, IT departments generally focus on protecting their own networks and therefore choose local detection approaches.

4.1 Activity Profiling

Monitoring a network packet's header information offers an activity profile. Loosely defined, this activity profile is the average packet rate for a net-work flow, which consists of consecutive packets with similar packet fields (such as address, port, and protocol). The elapsed time between consecutive matching packets determines the flow's aver-age packet rate or activity level. We can measure total network activity as the sum over the average packet rates of all inbound and outbound flows. To analyze individual flows for all possible UDP services, we would have to monitor on the order of 264 flows, and including other protocols, Such as TCP, ICMP, and Simple Network Management Protocol (SNMP) greatly com-pounds the number of possible flows. To avoid high-dimensionality issues, we can cluster individual flows with similar characteristics. Each cluster's activity level is the summation of constituent flows. For this abstraction, an attack is indicated by increasing activity levels among clusters, which can indicate a few attacking agents increasing their attack-generation rate; or an increase in the overall number of distinct clusters, which can represent many distributed attacking agents (as in a DDoS).

4.2 Sequential Change Point Detection

Change-point detection algorithms isolate a traffic statistic's change caused by attacks. These approaches initially filter the target traffic data by address, port, or protocol and store the resultant flow as a time series. The time series can be considered a time-domain representation of a cluster's activity. If DoS flooding attack begins at time T, the time series will show a statistical change either around or at a time greater than T.One class of change-point detection algorithms operates on continuously sampled data and requires only low amounts of memory and computational resources. An example here is cumulative sum (Cusum) algorithms. To identify and localize a DoS attack, the Cusum identifies deviations in the actual versus expected local average in the traffic time series.8–10 If the difference exceeds some upper bound, the Cusum's recursive statistic increases for each time-series sample. During time intervals containing only normal traffic, the difference is below th is bound, and the Cusum statistic decreases until reaching zero. Using an appropriate threshold against the Cusum statistic, the algorithm identifies an increasing trend in the time-series data, which might indicate a DoS attack's onset. Through the settings of the threshold and upper bound, the Cusum algorithm can trade off detection delay and False alarm rates. Other researchers have extended this detection method to identify the typical scanning activities of network worms.

4.3 Wavelet Analysis

Wavelet analysis describes an input signal in terms of spectral components. Although Fourier analysis is more common, it provides a global frequency description and no time localization. Wavelets provide for concurrent time and frequency description, and can thus determine the time at which certain frequency components are present. For detection applications, wavelets separate out time-localized anomalous signals from background noise; the input signal contains both. Ideally, the signal and noise components will dominate in separate spectral windows. Analyzing each spectral window's energy determines the presence of anomalies. Paul Barford and his colleagues12 define anomalies as network failures or misconfigurations, attacks (DoS or other), flash events, and other "measurement" events. They decomposed traffic data into distinct time series of average IP/HTTP packet sizes per second, flows per second, and bytes per second. They then applied wavelet analysis to each time series, resulting in time-localized high and mid-band spectral energies. They considered low-frequency content to be daily or weekly activity, and thus not an onset of an abrupt attack. To identify anomalies, they weighted a combination of high- and middle-spectral energies, and then threshold its variability. Wavelet energies in the high-band spectral window can also identify change points within an input signal. To enhance a Cusum change-point detection approach's performance, Richard Brooks and his colleagues used discrete wavelet analysis to post process the Cusum statistic's response. The signed magnitude of the high-band wavelet energy is proportional to the abruptness of an increasing Cusum statistic. Thresholding the high-band spectral energies quantifies the Cusum's abruptness, which is a potential indicator of an abrupt flooding attack.

5. Detection Method Results

Surveying each detection method's validation reveals disparate uses of test data, different attack types, and a wide range of reported results. In most cases, researchers provided quantitative true detection results, but didn't provide false positives, missed detections, and detection delay results. Table 1 summarizes the testing conditions and noteworthy detection test results.

References

[1] Kavisankar L., Chellappan C., "A mitigation model for tcp syn flooding with IP spoofing", Department of CSE, IEEE International Conference on Recent Trends in Information Technology, ICRTIT 2011

[2] Schuba Christoph L., Krsul Ivan V., Kuhn Markus G., Spafford Eugene H., Sundaram Aurbindo, Zamboni Deigo, "Analysis of denial attack on tcp", Department of Computer Sciences.

[3] Zhanh Yi, Liu Qiang, Zhao Guofeng, "A real time ddos attack detection and prevention system based on per-ip traffic behavioral analysis", Chongqing University of Posts and Telecommunications, 978-1-4244-5540-9/10 © 2010 IEEE.

[4] Dalia Nashat, Xiaohong Jiang, Susumu Horiguchi, " Detacting syn flooding agents under any type of ip spoofing", IEEE International Conference on e-Business Engineering.

[5] Guiyi Wei, Ye Gu, Yun Ling, " An early stage detecting method against syn flooding attack" , College of Computer and Information Engineering, International Symposium on Computer Science and its Applications, 978-0-7695-3428-2/08© 2008, IEEE, DOI 10.1109/ CSA.2008.18.

[6] Chen Wei, Yeung Dit Yan, "Defending against tcp syn flooding attacks under different types of ip spoofing", Department of Computer Science, Proceedings of the International Conference in Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06), 0-7695-2552-0/06 © 2006 IEEE.

[7] Gregg Donna M., Blackert William J., Heinbuch David V., Furnanage Donna, " Assessing and quantifying denial of service attacks", The Johns Hopkins University Applied Physics Laboratory (JHU/APL), 0-7803-7225-5/01 © 2001, IEEE.

[8] Chen Xiuzhen, Li Shenghong, Ma Jin, Li Jianhua, "quantitative threat assessment of denial of attacks on service availability", School of Information Security Enginnering, Department of Electronics Engineering, 978-1-4244-8728-8/11 © 2011, IEEE.

[9] Fu Zhang, “Mitigating distributed denial - of - service attacks:application – defence and network – defence methods”, Department of Computer Science & Enginnering, 2011 Seventh European Conference on Network Defence, 978-0-7695-4762-6/12 © 2012, IEEE, DOI 10.1109/ EC2ND.2011.18.

[10] Behera H.S, Patel Simpi, Panda Bijayalakshmi,” A new round robin and SRTN algorithm with variable original time slice for soft real time systems” Internatsional Journal of Computer Applications volume 16- No.1, February 2011.

[11] Hofmann Stefan, Louizi Mohamed, Stoll Dieter, “A novel approach to identify denial of service attacks against transport network resources.”, Alcatel – Lucent Deutschland AG, Nurnberg.