WHITE PAPER

DDoS Detection, Mitigation and Prevention Strategies: An Analysis of Selected Current Techniques

June 23

2014

This white paper presented by SDV INTERNATIONAL is a primer that focuses on selected techniques to detect, mitigate and prevent Distributed Denial of Service (DDoS) attacks. A focus on cloud datacenter environments is incorporated. By R. Jason Roys

.:. SDV INTERNATIONAL, LLC .:.
.:. Phone: (202) 455-6554 .:.
.:. Email: info@SDVInternational.com .:.
.:. Website: www.SDVInternational.com .:.

INTRODUCTION

Denial of Service (DoS) attacks can be disruptive to information systems and highly problematic for the people who depend on them. DoS attacks attempt to overwhelm network resources and aim to take them offline. Some attacks may be traced back to a particular person, such as someone using the Low Orbit Ion Canon (LOIC), and or they may be traced back to thousands of unknowing botnet computers (Sauter, 2013). Damages caused by DoS attacks vary, and have been known to shut down major websites such as MasterCard.com, preventing users from accessing or administering accounts for some period of time (Olson, 2011).

The study of detecting, mitigating and preventing DoS attacks is a worthy effort. This paper provides an analysis of three peer-reviewed, scholarly journal publications that identify DoS detection, mitigation and prevention techniques. These three journal publications were selected for analysis based on relevancy to the subject of DoS attacks, recency of publication, and because they offer different approaches to solving the same type of problem (i.e. DoS attack). In total, this paper provides a collection of nine total techniques (three from each publication), including analysis of the potential for each being practically implemented and strengths and/or weaknesses (i.e. limitations).

Description of Techniques

The first research paper, *Detection of DDOS Attacks Using IP Traceback and Network Coding Technique*, focuses on attacks against network routers and introduces the concept of: 1) IP traceback, which allows data to get to an intended destination when a particular router is overwhelmed by a distributed denial of service (DDoS) attack (mitigation technique); 2) network coding (mitigation technique), which enables a receiver to assemble data received from multiple sources, and; 3) RC4 algorithm overlay (mitigation technique), which may be utilized to segment and encrypt data in transit.

The second research paper, *An Enhanced Entropy Approach to Detect and Prevent DDoS in Cloud Environment,* focuses on DDoS attacks in a cloud environment and introduces the concept of: 1) analysis of heuristic data (detection technique), which provides a dynamic measurement of traffic behavior; 2) classification of traffic (detection technique), which includes entropy measurement, and; 3) a trust mechanism using credits (mitigation technique), which creates an adaptable and accurate method for mitigating DoS attacks over time. The analysis of present-day cloud environments is particularly relevant and important because more data centers are implementing cloud solutions to reduce infrastructure cost and provide a more scalable platform for customers. In addition, a successful DDoS attack on a cloud datacenter might not only harm one victim, but might also provide access to other potential victims that share the same virtualized environment; possibly leading to data corruption or loss.

The third research paper, *Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks,* focuses on various DDoS detection, mitigation and prevention techniques, among which this paper highlights the following: 1) disabling IP broadcast (prevention technique); 2) hybrid signature-anomaly based response (detection technique), and; 3) Hadoop based defense (mitigation technique). This publication is relevant to this paper because it provides a comparison of several DDoS architectures and attack methods, real world examples of how DDoS attacks have caused damages, as well as a timeline of the evolution of DDoS countermeasures.

Analysis of Techniques

This paper provides an analysis of nine total techniques, including strengths, weaknesses, and practicality of being implemented.

First Peer-Reviewed Scholarly Publication

The first research paper, *Detection of DDOS Attacks Using IP Traceback and Network Coding Technique*, features the following techniques and corresponding practicalities and strengths and/or weaknesses.

1. *Technique #1 – IP traceback (mitigation technique)*

   IP traceback follows a packet all the way back to its source through interconnected autonomous systems (i.e. other routers) by utilizing logs and data mining techniques. Moreover, IP traceback is made practical by marking and logging packet information in routing tables, which can be mined at some point in the future (Lonea, Popescu, & Tianfield, 2013). In the context of DoS attacks, this technique may allow for identification and filtering of traffic from the attack source, which is a clear strength (Yulong, & Rui, 2014). A possible weakness is that an IP traceback is not possible if all autonomous systems (i.e. other routers) do not allow does not support IP traceback.

2. *Technique #3 – Network coding (mitigation technique)*

Network coding enables a receiver to assemble data received from multiple sources, which may be necessary when chunking down data into smaller segments and sending the data segments simultaneously through multiple routes when using alternate paths while a particular router is disabled due to a denial of service attack (Yin, Wang, Li, Wang, Zhao, & Xue, 2014). Network coding can be applied to collected and reassemble data that is segmented during transmission, and has come to be known as a practical approach to managing network traffic (Yin, 2014).

The benefit of this technique in a DoS scenario is that when a router is overwhelmed by an attack, the normal traffic can send smaller segments of the data through multiple routes to get to the destination, and the data can be reassembled at the destination. Network coding increases network throughput and minimizes delay by utilizing intermediate forwarders, as opposed to conventional packet forwarding technology. It's application in networks includes, but is not limited to file distribution, data transmission in industrial control systems, multimedia streaming on P2P overlay networks (Lonea, 2013). Network coding is common and practical to implement.

This technique is strong in the context of a DoS attack, however, a weakness of this technique's explanation in this publication is that it does not address the possibility of a solution to lost data.

3. *Technique #3 – RC4 algorithm overlay for traffic segmentation and encryption (mitigation technique)*

The RC4 cryptographic cypher may be utilized to segment and encrypt data in transit. This is relevant to a DoS attack because data transmitted with the RC4 algorithm can be retrieved by a destination by using multiple routers rather than a singer router, which may come under a DoS attack and be taken offline. There is the added benefit of encryption being added to the data when it is segmented by RC4, which increases confidentiality protection. This is a practical technique, and in fact, the RC4 algorithm is often used for WEP, WPA and TLS (Chen, & Miyaji, 2013).

The strength of this approach lies in RC4's ability to rapidly and efficiently segment and encrypt the data, and does not slow traffic. However, a weakness to this technique is that key collision may occur using a brute force key attack, and therefore different keys may have the same encryption and decryption effects, which would render the aforementioned confidentiality benefit null (Chen, 2013).

Second Peer-Reviewed Scholarly Publication

The second research paper, *An Enhanced Entropy Approach to Detect and Prevent DDoS in Cloud Environment,* features the following techniques and corresponding practicalities and strengths and/or weaknesses.

1. *Technique #1 - Analyze heuristic data (detection technique)*

   Analysis of heuristic data provides a dynamic measurement of traffic behavior through self-education and improvement through successive iterations (Dzemyda, & Sakalauskas, 2011). As suggested by the publication's title that contains the term entropy, or uncertainty of an outcome, analysis of heuristic is not a 100% solution. Moreover, analysis of heuristic data about incoming traffic is the first step in this publication's recommendation list, and as more determinations are made about the accuracy of preceding analyses, the better subsequent heuristic data analyses may become. Implementation of this technique is practical, but requires a network traffic analyzer and a strong algorithm.

   In contrast to signature-based DoS detection techniques that require large signature databases that are updated regularly, analysis of heuristic data is behavior-based and requires much less data to detect DoS attempts (Dzemyda, 2011). Limitations include a lack of heuristic assumptions during initial implementation, which may be mitigated by importing a recent update of the algorithm from a similar established cloud environment implementation. Establishing a pre-live trial phase whereby known the analyzer processes packets, allowing it to 'learn' before going live, may also mitigate this limitation.

2. *Technique #2 – Classify traffic (detection technique)*

   Classification of traffic as described in this publication includes the use of entropy measurement. The authors suggest this technique should follow the preceding technique when abnormal traffic is suspected. Further, they describe an entropy measurement technique that utilizes Hellinger Distance, which is a measure of predicting variation between two probable variables (Sengar, Wang, Wijesekera, & Jajodia, 2008). In this case, the variables include: 1) packets collected and grouped as a dataset during a trial phase, and; 2) incoming packets that are monitored and logged into a second buffer. This probability difference is based on the Hellinger Distance measurement of predicting variation or distance and is known as the entropy value.

It is practical to develop an entropy measurement using a Hellinger Distance, although implementation will require a risk analysis that determines whether the Hellinger Distance coefficient would be set closer to 0 (treat all traffic as threatening) or 1 (treat all traffic as non-threatening). Strengths of the entropy measurement include the ability to improve detection accuracy by calculating overload conditions that are relevant to detection, as well as a synergistic effect of working in concert with the aforementioned heuristic data analysis approach.

3. *Technique #3 – Trust mechanism using credits (mitigation technique)*

A trust mechanism, as described in this publication, is a system for recognizing legitimate traffic rapidly. The paper describes an adaptable and accurate method for mitigating DoS attacks by adding trust credits following successive legitimate behavior, and subtracting trust credits based on successive aggressive behavior. This trust mechanism acts as a three-way handshake, validating trusted sources of traffic rapidly utilizing previously established acceptability ratings. Further, the credit system allows both the sender and the receiver to utilize certificates to identify one another, allowing both to have a high level of trust, and possibly reduce DoS security system workload caused by analysis and classification (Omar, Challal, & Bouabdallah, 2012).

Implementation of this system in a cloud environment is practical, but would require a traffic analyzer, load balancer, entropy measurement and parsing engine, certificate engine, and trust credit manager. While this technique is not a 100% solution for preventing DoS attacks, it is a strong mitigation technique because it enables handshake enfranchisement. This system is limited during initial implementation because of the time it could take time to establish and trust certificates on a large scale, but this limitation would diminish over time. A possible weakness could exist if trust certifications were spoofed, or if the trust certificate generation system were otherwise unsecure (Omar, 2012).

Third Peer-Reviewed Scholarly Publication

The third research paper, *Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks,* features the following techniques and corresponding practicalities and strengths and/or weaknesses.

1. *Technique #1* – Disabling IP broadcast (prevention technique),

   Various DDoS attacks take advantage of IP broadcasts based on the ICMP protocol's echo packets that respond to ICMP calls. This kind of attack is effective insofar as the attacker may have a low-cost, low-bandwidth architecture, but may cause damage to a high-cost, high-bandwidth information system because the ICMP requests cause a target router as well as every host behind the target router to respond with an IP broadcast. The hosts behind the target router multiply the ICMP protocol's echo packet requests, and therefore the workload on a system increases, possibly leading to a slowdown or crash (Bogdanoski, & Risteski, 2011).

   Disabling IP broadcast is a practical solution on smaller networks, and is common. The solution is strong with regard to its effectiveness, but its weakness is that all host computers behind the target router will also have to disable IP broadcast, which might not be practical for larger networks. In addition, IP broadcast is very helpful when troubleshooting routers, and disabling ICMP unreachables, which is useful for troubleshooting, may hinder options available to network administrators (Anbar, Manasrah, & Manickam, 2012).

2. *Technique #2* – Hybrid signature-anomaly based response (detection technique)

   A hybrid signature-anomaly based response is a detection technique that combines known signatures of attacks, such as those collected and utilized by intrusion detection systems (e.g., SNORT), and unusual traffic behavior (Dabbour, Alsmadi, & Alsukhni, 2013).

   It is practical to implement a hybrid signature-anomaly based response, such as by using the SNORT intrusion detection system, but comes at the price of software and hardware acquisition and management personnel. What makes the hybrid response so strong, is that is takes advantage of known threat signatures, and detects deviations from normal traffic patterns at the same time; this reduces the rate of false positives and false negatives. A limitation that is inherent in both of the underlying signature and anomaly responses is the requirement for the signature database to be current and comprehensive, and for the anomaly algorithm to have a strong baseline for what is considered normal network behavior, respectively (Dabbour, 2013).

3. *Technique #3* - Hadoop based defense (mitigation technique)

   Hadoop is an open source Apache Software Foundation implementation of the MapReduce framework. It is Java-based, and it is capable of processing vast amounts of data rapidly, i.e. big data (Xianfeng, & Liming, 2014). As a countermeasure to DDoS, the Hadoop countermeasure relies on three variables related to DDoS attacks that strain network resources: 1) threshold, which indicates frequency of events, such as requests; 2) time interval, which is the time it takes for packets to be analyzed, and; 3) unbalance ratio, which indicates the anomaly ratios of responses for pages requested between specific servers and clients.

   This technique is practical to implement because its complexity is low (Tripathi, Gupta, Almomani, Mishra, & Veluru, 2013). Further, this technique is strong because it can help the label traffic that crosses acceptable levels of the aforementioned metrics as malicious. The possible limitation to this approach is that its threshold determination has to be set, and the publication expressed uncertainty about how to determine an appropriate threshold value. However, this limitation may be bridged by utilizing a Hellinger Distance that determines how to treat traffic based on a measurement of normal traffic as compared to a value of malicious traffic during a trial or implementation phase (Jeyanthi, 2013).

Conclusion

DoS attacks attempt to disrupt information systems, and as more tools are developed to support attackers, threat volume has the potential for growth. It is important for information technology professionals to continuously develop new methods to protect information systems as a countermeasure against constantly evolving threat sources. The techniques analyzed in this paper are relevant and among the numerous ideas being shared in the forefront of the information systems security field today.

References

Anbar, M., Manasrah, A., & Manickam, S. (2012). Statistical cross-relation approach for detecting TCP and UDP random and sequential network scanning (SCANS). *International Journal Of Computer Mathematics*, *89*(15), 1952-1969. doi:10.1080/00207160.2012.696621

Bogdanoski, M., & Risteski, A. (2011). Wireless Network Behavior under ICMP Ping Flood DoS Attack and Mitigation Techniques. *International Journal Of Communication Networks & Information Security*, *3*(1), 17-24.

Chen, J., & Miyaji, A. (2013). Novel strategies for searching RC4 key collisions. *Computers & Mathematics With Applications*, *66*(1), 81-90.

Dabbour, M., Alsmadi, I., & Alsukhni, E. (2013). Efficient Assessment and Evaluation for Websites Vulnerabilities Using SNORT. *International Journal Of Security & Its Applications*, *7*(1), 7-16.

Dzemyda, G., & Sakalauskas, L. (2011). Large-Scale Data Analysis Using Heuristic Methods. *Informatica*, *22*(1), 1-10.

Higgins, J. (2007). How to Trace a DDOS Attack. Information Week Dark Reading Room. Retrieved from www.darkreading.com

Jeyanthi, N. N., Iyengar, N. N., Kumar, P., & Kannammal, A. A. (2013). An Enhanced Entropy Approach to Detect and Prevent DDoS in Cloud Environment. *International Journal Of Communication Networks & Information Security*, *5*(2), 110-119.

Lonea, A., Popescu, D., & Tianfield, H. (2013). Detecting DDoS Attacks in Cloud Computing Environment. *International Journal Of Computers, Communications & Control*, *8*(1), 70-78.

Olson, P. (2011). Anonymous Speaks. *Forbes*, *187*(2), 38.

Omar, M., Challal, Y., & Bouabdallah, A. (2012). Certification-based trust models in mobile ad hoc networks: A survey and taxonomy. *Journal Of Network & Computer Applications*, *35*(1), 268-286. doi:10.1016/j.jnca.2011.08.008

Priya, J., Ramakrishnan, M., & Rajagopalan, S. (2014). Detection of DDoS Attacks Using IP Traceback and Network Coding Technique. *Journal Of Theoretical & Applied Information Technology*, *62*(1), 99-106.

Sauter, M. (2013). "LOIC Will Tear Us Apart": the Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks. American Behavioral Scientist. Retrieved from http://abs.sagepub.com

Sengar, H., Wang, H., Wijesekera, D., & Jajodia, S. (2008). Detecting VoIP Floods Using the Hellinger Distance. *IEEE Transactions On Parallel & Distributed Systems*, *19*(6), 794-805. doi:10.1109/TPDS.2007.70786

Seung Wook, J. (2012). CAPTCHA-based DDoS Defense System of Call Centers against Zombie Smart-Phone. *International Journal Of Security & Its Applications*, *6*(3), 29-36.

Tripathi, S., Gupta, B., Almomani, A., Mishra, A., & Veluru, S. (2013). Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks. *Journal Of Information Security*, *4*(3), 150-164.

Xianfeng, Y., & Liming, L. (2014). A New Data Mining Algorithm based on MapReduce and Hadoop. *International Journal Of Signal Processing, Image Processing & Pattern Recognition*, *7*(2), 131-141. doi:10.14257/ijsip.2014.7.2.13

Yin, X., Wang, Y., Li, Z., Wang, X., Zhao, J., & Xue, X. (2014). Bounding the Advantage of Multicast Network Coding in General Network Models. *IEEE Transactions On Communications*, *62*(3), 1023-1032. doi:10.1109/TCOMM.2014.011614.130316

Yulong, W., & Rui, S. (2014). An IP-Traceback-based Packet Filtering Scheme for Eliminating DDoS Attacks. *Journal Of Networks*, *9*(4), 874-881. doi:10.4304/jnw.9.4.874-881