Volume 3 Issue 1 | March 2015 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

A Review on Enhancement of Security in IPv6

Mukta Bhatele
Professor and Head of Department
Department of Computer Science and Engineering
Jai Narain College of Technology,
Bhopal (M.P.)India
Email: mukta_bhatele@rediffmail.com

Ayushi Arzare
M.Tech. Research Scholar
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email: ayushi.arzare@gmail.com

Prof B.L. Rai
Assistant Professor
Department of Computer Science and Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email: blrai_08_76Yahoo.com

Raghvendra Singh Tomar
Assistant Professor
Department of Computer Science and Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email: raghvendra_tomar@rediffmail.com

Abstract**—***Denial of Service is an attack which makes an information or data unavailable to its Intended hosts. There are various methods to carry out these attacks. The underlying aspect would be to choke victim's network and thus make it inaccessible by other client. However, there are also different ways of making service unavailable rather than just dumping it with abundant IP packets. The victim could also be attacked at various loopholes making it unstable which depends on the nature of the attack.*

Today, serious challenges arise when IPv6 needs to be established globally and transition from version 4 to version 6 has to be done. IPv6 introduces six optional headers like Routing header, Authentication header etc [5]. In spite of providing better security with authentication, encryption and encapsulation techniques, IPv6 also brings out serious complications. In this paper, we implement two types of Denial of Service attacks with the help of IPv6.

Keywords:**—***Denial of service, IPv6.*

1. INTRODUCTION

Denial of Service attack is generally carried out with large number of systems attacking a specific martyr. Such as attacking network is called the Botnet. A Botnet is formed by thousands of slave systems usually termed as the Zombies. The attacking systems are much controlled and manipulated by a remote attacker who makes use of these compromised machines. Most of the times, the real owner of a compromised machine is not aware of the malicious activities

Denial of Service is an attack which makes an information or data unavailable to its Intended hosts. There are various methods to carry out these attacks. The underlying aspect would be to choke victim's network and thus make it inaccessible by other client. However, there are also different ways of making service unavailable rather than just dumping it with abundant IP packets. The martyr could also be attacked at various loopholes making it unstable which depends on the nature of the attack.

There are also attacks that could be carried out at application level, hindering the normal functioning of a service. There are attacks that are designed to blast a web browser, email application or even a media player. When a specific application is disturbed and when normal functioning is blocked, it is called the Application level Denial of Service.

Denial of service attacks are further classified into many categories according to the style with which it is implemented. Now, we are discussed few of the most well known categories of DOS.

1. Distributed Denial of Service:

Distributed Denial of service has the cohesive strength of many compromised systems working towards a single cause. The first stage of this attack is to built its platform with many host systems that can work under remote commands. The attacker group would first scan networks to hunt for vulnerable systems that are weak in security features. According to researchers there are millions of host machines that are vulnerable without secure patches and proper updates that often fall victims to these attackers

2. Low-rate TCP targeted Denial of Service:

Unlike the Distributed Denial of Service, low-rate TCP targeted attacks does not used numerous packets to downpour the network. Instead, it exploits the working mechanism of TCP timers thus bringing the throughput of a system to almost zero. These low-rate attacks are crafted to generate packets only periodically in very minimal quantity. Thus the attacking packets can easily disguise with the legitimate packets and escape from the Anti-Dos traffic monitoring systems. The attacks carried out this way exploiting the TCP timers are coined with the term Shrew attacks. It is also indispensable to understand the TCP working procedure before discussing this attack.

During congestion in TCP, the congestion window is gradually reduced until the network is clear. Thus during congestion the sender rate is reduced which apparently reduced the potential throughput. The TCP interval for the Retransmission Time Out (RTO) to expire after which the data is sent again. When the congestion is more, the RTO timer is doubled after which the packets are retransmitted. Hence, during a low rate attack, when packets are lost, TCP enters RTO. When an attacker is able to calculate this RTO time and sends attacking packets to create packet concussion and loss, the attacker can push the TCP into waiting state. Hence, there is no need for inundation the network with packets, but only send packets when the timer is about to expire and push it again into the RTO waiting time. This type of attack can effortless escape the traffic monitors due to its low traffic rate and is a serious challenge for the security.

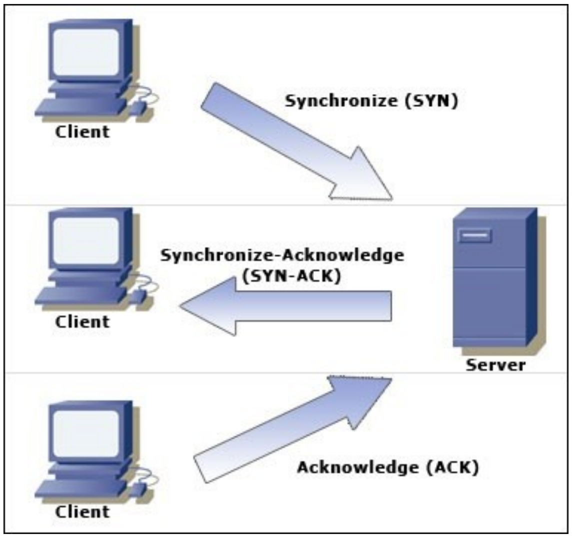

Figure.1: Denial-Of-Service Attack

Security Issues Related to IPv6

The transition from IPv4 to IPv6 is under way as more network and content providers embrace IPv6. As the amount of IPv6 traffic (and IPv6-based threats) increases in your network, it's essential that you deploy a network security solution that can deliver the same level of protection for IPv6 content as IPv4. Organizations of all sizes need to understand the security implications of IPv6, which include:

1. IPv4 security devices cannot inspect IPv6 traffic Although there are work-around measures to enable IPv4 network and security devices to

forward IPv6 packets, IPv4 devices cannot inspect those packets for malicious content. This lack of visibility enables a simple evasion technique to avoid detection by legacy security devices--send malicious content via IPv6. This allows old threats to bypass policies that may have been in place for years. And, as long as the victim system can process IPv6, the attack will reach its intended target.

2. IPv6 is likely in your network today, as many systems (such as Windows 7) natively support IPv6 and ship with IPv6 support enabled Many systems ship today with IPv6 support enabled by default. And, unless that support is specifically disabled, these devices will be vulnerable to threats transported via IPv6.

3. Some legacy security devices will never support IPv6 and will need to be replaced Many network security devices require recently released versions of their operating systems to support IPv6. Unfortunately, not all devices can support the most recent releases due to lack of memory or other hardware-based limitations, requiring an upgrade to the latest hardware device. Without replacing the device, the network segments protected by these legacy systems will be blind to threats embedded within IPv6 traffic.

4. Many security vendors have limited support for IPv6 today, leading to potential gaps in protection Supporting IPv6 with a dual-stack architecture is not a trivial development exercise; it requires a significant allocation of development resources to build a new stack and incorporate it with the existing IPv4 stack. Many vendors have only recently committed development resources to supporting IPv4, choosing to wait until demand for IPv6 support increased before allocating the necessary resources. One result of the delayed investment is that they will not be able to offer feature parity with their IPv4 devices, which has the potential to lead to years of gaps in IPv6 policy enforcement, as these vendors will struggle to make all key IPv4 features functional in IPv6.

5. IPv6 support is often at much slower performance In addition to reduced functionality in their IPv6 support, many vendors rely on software only to filter traffic to detect threats. As stated above, the implementation of IPv6 support in a network security device is not a trivial exercise. It requires significant investment and, like any other new technology, several product releases to deliver stable, mature functionality. One way to accelerate the speed with which they can bring IPv6 support to market, vendors of devices that utilize custom processors will release IPv6 support in software only. The advantage is that a software-only approach reduces the amount engineering effort required to bring the functionality to market. The disadvantage is that the performance of a software-only approach is significantly slower than a hardware-accelerated approach

I. LITERATURE REVIEW

Interconnected systems, such as Web servers, database servers, cloud computing servers etc, are now under threads from network attackers. As one of most common and aggressive means, Denial-of-Service (DoS) attacks cause serious impact on these computing systems. In this paper, we present a DoS attack detection system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Our MCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition. This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA. The effectiveness of our proposed detection system is evaluated using KDD Cup 99 dataset, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined. The results show that our system outperforms two other previously developed state-of-the-art approaches in terms of detection accuracy. The overview of our proposed DoS attack detection system architecture is given in this section, where the system framework and the sample-by-sample detection mechanism are discussed.

In Sample-by-sample Detection Jin et al. [2] systematically proved that the group-based detection mechanism maintained a higher probability in classifying a group of sequential network traffic samples than the sample-by-sample detection mechanism. Whereas, the proof was based on an assumption that the samples in a tested group were all from the same distribution (class). This restricts the applications of the group-based detection to limited scenarios, because attacks occur unpredictably in general and it is difficult toobtain a group of sequential samples only from the same distribution. To remove this restriction, our system in this paper investigates traffic samples individually. This offers benefits that are not found in the group-based detection mechanism. For example, (a) attacks can be detected in a prompt manner in comparison with the group-based detection mechanism, (b) intrusive traffic samples can be labeled individually, and (c) the probability of correctly classifying a sample into its population is higher than the one achieved using the group-based detection mechanism in a general network scenario. To better understand the merits, we illustrate them through a mathematical example given in [2], which assumes traffic samples are independent and identically distributed [2], [3], [4], and legitimate traffic and illegitimate traffic follow normal distributions $X1 \sim N(\mu1, \sigma21)$ and$X2 \sim N(\mu2, \sigma22)$ respectively. In “A system for Denial of Services Attack Detection Based on multivariate Correlation Analysis” by Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda and Ren Ping Liu, presents a threshold-based anomaly detector, whose normal profiles are generated using purely legitimate network traffic records and utilized for future comparisons with new incoming investigated traffic records. The dissimilarity between a new incoming traffic record and the respective normal profile is examined by the proposed detector. If the dissimilarity is greater than a pre-determined threshold, the traffic record is flagged as an attack. Otherwise, it is labeled as a legitimate traffic record. Clearly, normal profiles and thresholds have direct influence on the performance of a threshold-based detector. A low quality normal profile causes an inaccurate characterization to legitimate network traffic. Thus, we first apply the proposed triangle area-based MCA approach to analyze legitimate network traffic, and the generated TAMs are then used to supply quality features for normal profile generation.

In a Distributed Denial of Service has the cohesive strength of many compromised systems working towards a single cause. The first stage of this attack is to build its platform with many host systems that can work under remote commands. The attacker group would first scan networks to hunt for vulnerable systems that are weak in security features. According to researchers there are millions of host machines that are vulnerable without secure patches and proper updates that often fall victims to these attackers.

In a Low-rate TCP targeted Denial of Service targeted attacks does not employ numerous packets to flood the network. Instead, it exploits the working mechanism of TCP timers thus bringing the throughput of a system to almost zero. These low-rate attacks are crafted to generate packets only periodically in very minimal quantity. Thus the attacking packets can easily disguise with the legitimate packets and escape from the Anti-Dos traffic monitoring systems. The attacks carried out this way exploiting the TCP timers are coined with the term Shrew attacks. It is also indispensable to understand the TCP working procedure. When an attacker is able to calculate this RTO time and sends attacking packets to create packet collision and loss, the attacker can push the TCP into waiting state. Hence, there is no need for flooding the network with packets, but only send packets when the timer is about to expire and push it again into the RTO waiting time. This type of attack can effortlessly escape the traffic monitors due to its low traffic rate and is a serious challenge for the security.

2. PROBLEM FORMULATION

Today, serious challenges arise when IPv6 needs to be established globally and transition from version 4 to version 6 has to be done. IPv6 introduces six optional headers like Routing header, Authentication header etc [5]. In spite of providing better security with authentication, encryption and encapsulation techniques, IPv6 also brings out serious complications.

Here I describe DDOS attack in IPV6. These all attack we describe through the some steps and diagram i.e.

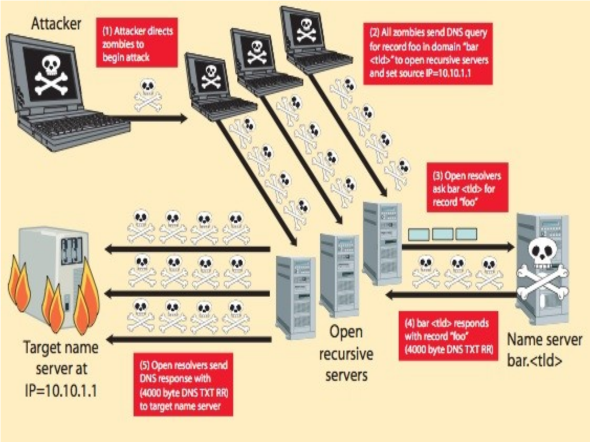
Attacker
(1) Attacker directs zombies to begin attack
(2) All zombies send DNS query for record foo in domain "bar <tld>" to open recursive servers and set source IP=10.10.1.1
(3) Open resolvers ask bar <tld> for record "foo"
(4) bar <tld> responds with record "foo" (4000 byte DNS TXT RR)
(5) Open resolvers send DNS response with (4000 byte DNS TXT RR) to target name server
Target name server at IP=10.10.1.1
Open recursive servers
Name server bar.<tld>

Figure 2 : DDOS attack in IPV6

Step 1: Firstly attacker attacks in some proxies' server which followed by client for the sending message to server. These attacks are called zombies attack.

Step 2: All zombies send DNS query for record too in domain to open recursive server and set source IP.

Step 3: Open recursive server send to message packet to the resolver.

Step 4: Resolver responds to open recursive servers.

Step 5: Open resolver send DNS to attacker so, here DNS are leaked.

3. PROPOSED WORK

Today, serious challenges arise when IPv6 needs to be established globally and transition from version 4 to version 6 has to be done. IPv6 introduces six optional headers like Routing header, Authentication header etc Dr Nick zakhleniuk IP NETWORKING AND APPLICATION. In spite of providing better security with authentication, encryption and encapsulation techniques, IPv6 also brings out serious complications. The following two types of Denial of Service attacks could be implemented if IPv6 is used.

Routing Header Denial of Service

Experts say DDoS attacks could be strengthened 88% more in IPv6 when compared to the IPv4. In IPv4, the path taken by the attack packets can be either one way (TCP, UDP and other attacks) or two ways (ICMP traffic). But in IPv6, the attack packets could be made to oscillate between the routers endlessly. Thus the network would be constantly occupied by these forged packets and can lead to a powerful DDoS attack. Routing header is an extension header that dictates a packet to visit the compulsory routers on path. Attackers can easily forge this Routing header (RH0) and make a packet wander back and forth between two routers.

Denial of Service attack exploiting IPv6 mobility

IPv6 has come out with a revolutionary idea of mobile IP that was not possible in the former versions. Regular IP is designed to serve only the stationary users. A user is forced to change his IP address when he changes his geographical network. But with the advent of IPv6, user can change his geographical location moving to different networks and can still hold to a single IP address. This is attaining by the extension headers provided in IPv6. The original IPv6address is stored in the extension header whereas an additional temporary address is held in the IP header. The temporary address keeps changing when the user is mobile but the original IP address remains unchanged. An attacker can easily change this temporary IP address and carryout spoof attacks.

Since IPv4 is in the verge of extinction and is getting replaced by IPv6, the future work should focus on stopping DDoS in IPv6. In spite of having additional headers and options for enhanced security in IPv6, it is still prone to various flavors of Denial of Service attacks. Thus, additional research work should be emphasized on IPv6 security and proper mitigation techniques should be introduced for existing vulnerabilities.

To overcome zombie DDOS attack in IPV6, we proposed the new technique which is called mitigation technique. This method is adopted by most of the data providers as it proves to be extremely effective and saves the network components from permanent denial of service. However this cannot be an ideal solution as it still permits controlled traffic from attacking system as well.

FUTURE WORK AND CONCLUSION

This present IPv6 based on Denial-Of-Service attacks, which are two types of Denial of Service attacks could be implemented if IPv6 is used such as Routing Header Denial of Service and Denial of Service attack exploiting IPv6 mobility. Our planned to stop DDoS in IPv6. In spite of having additional headers and options for enhanced security in IPv6, it is still prone to various flavors of Denial of Service attacks. Thus, additional research work should be emphasized on IPv6 security and proper mitigation techniques should be introduced for existing vulnerabilities. This project also aims at suggesting possible solutions in mitigating this attack. These attacks should be able to save the victim and also provide access to legitimate client who would require service during an attack. The objective would be to investigate and learn subject in depth, implementing the attacks, identifying and measuring the attack and finally adopting counter measures to defend Denial of Service attack.

REFERENCES:

[1] Zhiyuan Tan, ArunaJamdagni, Xiangjian He, Priyadarsi Nanda and Ren Ping Liu, “A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:25 NO:2 YEAR 2014.

[2] S. Jin, D. S. Yeung, and X. Wang, “Network Intrusion Detection in Covariance Feature Space,” Pattern Recognition, vol. 40, pp. 2185-2197, 2007.

[3] G. V. Moustakides, “Quickest detection of abrupt changes for a class of random processes,” Information Theory, IEEE Transactions on, vol. 44, pp. 1965-1968, 1998.

[4] A. A. Cardenas, J. S. Baras, and V. Ramezani, “Distributed change detection for worms, DDoS and other network attacks,” The American Control Conference, Vol.2, pp. 1008-1013, 2004.

[5] Dr. Nick Zakhleniuk, university of ESSEX, “IP NETWORKING AND APPLICATION” IPv6 Extension

Headers (EHs) - IPv6 Security, March 2011. Huu-Jung-Lim, Tai-Myoung Chung, "The Bias Routing Tree Avoiding

[6] Technique for Hierarchical Routing Protocol over 6LoWPAN", 2009 Fifth International Joint Conference on INC, IMS and IDC, Page: 232 – 235.

[7] Volker K ̈oster, Dennis Dorn, Andreas Lewandowski and Christian Wietfeld "A novel approach for combining Micro and Macro Mobility in 6LoWPAN enabled Networks", Page:1-4,2011 IEEE Publications.

[8] Abdelkader Lahmadi, C ́Esar Brandin, Olivier Festor "A Testing Framework for Discovering Vulnerabilities in 6LoWPAN Networks" 2012 8th IEEE International Conference on Distributed Computing in Sensor Systems.

[9] Gopinath R S, Khan Imran, Suryady, zeldi "Optimized web service architecture for 6L0WPAN", 2009 IEEE international conference pages-1-Donghyuk Han; Jong-Moon Chung; Garcia, R.C., "Energy efficient wireless sensor networks based on 6LoWPAN and virtual MIMO technology," Circuits and Systems (MWSCAS), 2012 IEEE 55thInternational Midwest Symposium on, vol., no., pp.849,852 5-8Aug.2012 doi: 10.1109/ MWSCAS.2012.6292153Publication Year: 2012, Page(s): 849 – 852

[10] Kun Feng; Xiaohong Huang; Zhisheng Su, "A network management architecture for 6LoWPAN network," Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on, vol., no., pp.430,434, 28-30 Oct. 2011 doi:10.1109/ICBNMT.2011.6155971

[11] Kermajani, H.R.; Gomez, C., "Route change latency in low-power and lossy wireless networks using RPL and 6LoWPAN Neighbor Discovery," Computers and Communications (ISCC), 2011 IEEE Symposium on, vol., no., pp.937,942, June 28 2011-July12011doi: 10.1109/ ISCC.2011.5983962

[12] Bosling, M.; Redmann, T.; Tekam, J.; Weingartner, E.; Wehrle, K., "Can P2P swarm loading improve the robustness of 6LoWPAN data transfer?," Wireless On-demand Network Systems and Services (WONS), 2012 9th.