ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

Survey on ROQ attacks

Seema Gulati[1], Amandeep Dhaliwal[2]

Student, CSE, RIMT-IET (PTU), Mandi Gobindgarh, India[1]
Assistant Professor, CSE, RIMT-IET (PTU), Mandi Gobindgarh, India[2]

Abstract: Reduction of Quality (ROQ, pronounced as Rock attack) of attacks is a new category of attacks that target the adaptation mechanisms of the current internet systems. Unlike its ancestral Denial of Service Attacks these attacks don't aim to completely shut down the services of a server or a network, instead these aim to depreciate the Quality of the targeted network(s). The main objective of these attacks is to degrade the Quality of the systems, due to this reason they are also termed as low rate DDOS or DOS or shrew attacks. The users of the system experience a considerably degraded response from the network. These attacks are orchestrated while keeping a low profile, to evade the current detection systems and hence are more difficult to detect, yet they cause a serious damage to the system. This paper aims to look into the current research in the field and what all techniques have been discussed so far to mitigate the impact of this attack on the current internet systems.

Keywords: ROQ, DDOS, Shrew, RTO, RTT, TCP time-out.

I. INTRODUCTION

Network is an integral part of our lives, current systems rely on the internet therefore its security is a critical issue. Network security aims at preventing and monitoring unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. There are a number of DOS attacks (main focus of this paper) which are launched on the networks in order to completely shut down the services or deny services to the users who are the intended users of the particular system. Attacks on the networks could be internal or external. Internal attacks are made by the users of the system to harm the system, mostly the attacks are external and are made from outside the system and are not the users (generally). The main goal is to bring the system and its services to a halt state for some time or permanently.

II. DOS ATTACKS

The detection systems try to detect and prevent such (DOS) attacks in order to provide good quality i.e. fast and secure services to the users of the systems. Perpetrators of DOS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. The most common method is to overwhelm the server by sending too many requests to the server, when the server saturates it becomes incapable of catering to the requests of the legitimate senders, ultimately the system either attains a halt or becomes so slow that it nears a halting state. Thus such attacks lead to a server overload. In simpler words we can say that Dos attacks are implicated by forcing the target to consume its resources so that it cannot provide its services to the intended users or by barricading the communication between the legitimate users and the media, so that they are unable to enter into a proper communication.

A. Methods of launching DOS Attack:

a. Consumption of the resources like the bandwidth, the CPU time and cycles, disk space
b. Tampering with the configuration information such as the routing information.
c. Modification of the state information such as the unauthorized resetting of TCP sessions.
d. Barricading the communication medium between the authorized or intended users and the victim
e. Damaging physical components.

B. DOS Attack types:

Pulsing attack: An attacking node sends packet to a victim node which is randomly selected node, and the attacking period and the size of the packets is randomly selected.

Flooding attack: In beginning of a flooding attack the victim is forced to decrease its reception and transmission with other nodes in the network and gradually the system enters a non-performing or DOS state.

Packet drop attack: also called a Black-hole attack is a DOS attack in which a router which should relay the packets drops them, due to the router becoming compromised from a

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

number of reasons like the launch of a DOS attack with the help of DDOS tool.

SYN flood: this attack renders a system in-operation or at times a system crash. This attack is launched by flooding the server with TCP/SYN requests with a spoofed IP address; the server treats them as connection requests and thus keeps waiting TCP/SYN acknowledgement from the sender, which is never received.

ICMP flooding attack: this attack is launched by a sending in bulk- echo-reply packets to the victim from an intermediary node, thus causing congestion in the network or outages. Smurf, Ping flood, Ping of death are examples of ICMP attack.

Teardrop attack: it involves sending tangled fragments of IP which have an overlapping and over-sized payloads, to the target machine. Therefore, most operating systems crash, since an error is determined in their TCP/IP fragmentation reassembly code.

Low rate DOS attack/Reduction of quality attack: These attacks target the TCPs Retransmission Time Out (RTO) mechanism to strangulate the TCP throughput and thus degrading the Quality of Service in the network. By keeping the profile low and causing maximum damage.

Round Robin Attack: Multiple attacking nodes chosen randomly send attack packets to the chosen victim in a round-robin manner, with again a randomly selected sending rate and a random packet size to evade detection systems.

Permanently Denial of Service (PDOS) attack: at times also loosely called flashing. These attacks target the loop holes in the security mechanisms of the system, and allow remote administration on the management interfaces of the victim's hardware, such as routers, printers, or other networking hardware. The attack damages to an extent that replacement of hardware is needed.

TCP reset: The attacker listens to the TCP connections of the victim; a fake TCP RESET packet is sent by the attacker to the victim, it results into termination of TCP connections inadvertently.

III. REDUCTION OF QUALITY ATTACKS

Reduction of Quality attack is an important attack launched on the MANETS or wireless networks. The DOS or DDOS flooding attacks are characterized by bursts sent to the victim. Recently new category of attacks called Low-rate DDOS attacks or Reduction of Quality attacks have been identified.

The ROQ attacks reduce the quality of service of end systems gradually. These attacks while sending attack traffic at sufficiently low average rate, try to deny bandwidth to the legitimate flows. Low profile is kept so that the attacking nodes can evade the detection by the counter DOS mechanisms. These attacks reduce the QoS by strangulating the TCP throughput heavily instead of completely refusing the clients of the services. Like the DOS attacks the ROQ attacks don't limit the steady state capacity, instead these target the systems adaptive behavior. Both source and destination IP address spoofing is used by the ROQ attacks. Dissimilar periodicity helps the attack packets to evade the filtering mechanism. The ROQ attacks are launched through multiple zombies and the one attack controller controls these zombies. The zombies spoof header information so that they can easily avoid the detection trace-back techniques.

The ROQ attacks targets the TCPs time-out mechanism which uses two time-scales. The first is the Round Trip Time (RTT), and the second is the Retransmission Time Out (RTO). When the packet is sent by the source node, the packet is received at the destination node, the destination sends an acknowledgement to the receiver; the total time spent in this round trip is the Round Trip Time. The TCP operates on RTT, which ranges from 10's- 100's of msec. when the network is severely congested TCP works on RTO. RTO includes the RTO and the delay in incurred during the round trip. When the network is congested, TCP will wait for a period of RTO and retransmit the packets if the acknowledgement is not received during this time.

A. TCP Time-Out Mechanism:

Whenever a TCP stream is sent the sender is acknowledged by the destination on successful transmission of packets at the receiver. If a stream is not successfully delivered at the destination node, ACK (acknowledgement packet) will not be sent to the source. The source shall wait for a period of RTT and the TCP now enters a TIME-OUT state. On entering a Time-out state, the TCP waits for a period of RTO and then retransmits the stream of packets. The TCP at this point of time senses that some congestion in the network is present and to counter to this congestion in the network the TCP connections reduce their sending rate, and increase their RTO period. The sending rate is reduced multiplicatively, generally to one packet, thus the congestion window is set to one packet; whereas the RTO is doubled from one second to two seconds. This mechanism is termed as Additive Increase and Multiplicative Decrease (AIMD). The following figure (fig 1) explains the behavior of TCP retransmission timer.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

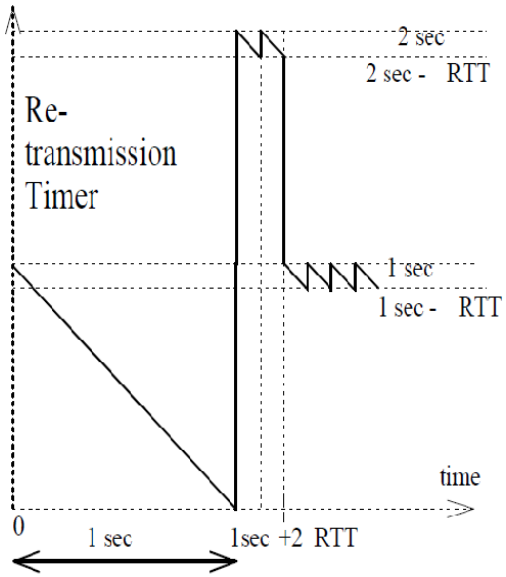

Fig 1: TCP retransmission timer

When the TCP transmits a packet at t=0 taken as reference time, also a retransmission timer of one second is set in the beginning when the packet is transferred over the network. If the packet is dropped by the network the stream enters a time-out when the timer expires at t=1 second. At this point, the source node or the sender enters an exponential back-off phase, and the AIMD mechanism is started. The congestion window is reduced to one packet; the RTO value is doubled from 1 sec to 2 seconds, packets which had not been acknowledged is retransmitted and resets the retransmission timer with the new RTO value.

In case the packet is lost again, the exponential back-off phase is continued, the sender waits until the 2-sec RTO completes to receive an ACK. The RTO is again doubled, now RTO equals to 4 seconds and the process is repeated. But here in the diagram at t=3 seconds the packets are successfully delivered and the acknowledgement is received at the source. Therefore the sender quits from the exponential back-off state and now it gets into a slow start state, the window size is doubled from one to two and new packets (next two) with a new RTO, instead of 2 seconds RTO.

B. ROQ Attack construction and difference between ROQ and Shrew Attacks:

The DOS attacks are a great threat to the internet systems and services. The attacks first publicly exposed by A. Kuzmanovic and E. Knightly in the year 2003[1] were identified these attacks as low rate TCP denial of service attacks and termed them as Shrew Attacks. The ROQ attacks do-not attempt to bring the legitimate flows to a halting state, rather they attempt to degrade the quality of services of the legitimate flows. Therefore it becomes much more difficult to detect these attacks. These low rate DOS attacks can be represented by a square wave, as shown in the figure below (fig 2).

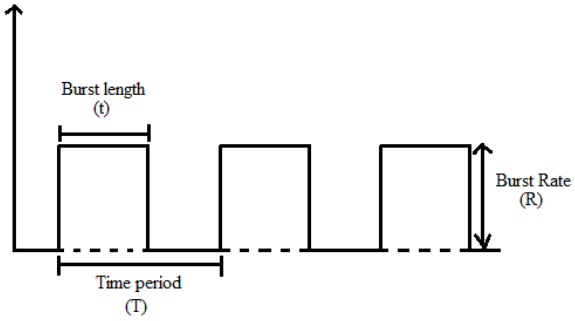

Fig 2: Attack Parameters

A low rate DOS attacks have 3 parameters:

a) Burst Rate: is the amount of traffic (burst) sent to the targeted victim.

b) Burst length: is the time for which the attack traffic is to be sent.

c) Burst time or time period: is the time period after which the attack is repeated.

The TCP targeted attacks called the Shrew attacks exploit the exponential back-off algorithm and the minimum RTO property of the TCP protocol. These attacks launch by selecting a target victim and sending burst of traffic to the victim. The attack traffic is greater than the capacity of the victim for a very short time period such as 20-200 ms every 1s. This results in overwhelming at the victim router and the legitimate TCP connections experience packet loss, which ultimately causes a time-out. The legitimate connections try to resend the packets after the fixed minimum RTO, which are again hampered due to the attack traffic. They then work on the exponential back-off algorithm, and then retransmit the lost packets, the retransmission time is a multiple of 1s, simultaneously the attack traffic is sent at the victim and again the TCP flows are denied of the services. Thus, giving a lethal blow to the long lived legitimate TCP flows.

Whereas the ROQ attacks try to only depreciate the quality of service offered to the end systems. These try to make the bandwidth unavailable for the legitimate flows, by occupying a large share of the available band width. Unlike the shrew attacks, the ROQ attacks work on longer timescales. Burst of traffic is sent to occupy the bandwidth of the legitimate flows. High bursts are sent periodically, but for a longer time. Thus causing instability of the queues, and the queue management techniques find it hard to manage, due to the long and random sending period. Since the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

periodicity is not well defined in a ROQ attack, the attackers can easily surpass the detection mechanisms by keeping a relatively low average attacking traffic.

The ROQ attacks exploit the TCP's AIMD (Additive Increase and Multiplicative Decrease) mechanism of congestion control, when the attacker sends the bursts to the router the legitimate TCP connection time-out and then TCP starts the AIMD algorithm. The AIMD algorithm counters the congestion in the network by decreasing the sending rate (the congestion window) to half and increasing the RTO to double, when the network converges from the congestion the sending rate is increased additively. Thus, when the legitimate TCP connections time-out, because of the ROQ attack traffic, the flows increase their RTO to double the current value and decrease the sending rate to half the current value. The process repeats till the attack period continues. Since the time period of a ROQ attack is quite long, the network converges after sometime and the TCP flows enter via a slow start, thereby increasing the sending rate additively in accordance to the AIMD mechanism of the TCP. Since the network converges the legitimate flows only experience depreciation in the quality of service offered to them and not a complete denial of the services.

Thus shrew attacks and the ROQ attacks operate on the same principle, but aim differently and the difference lies in time of operation and the periodicity, of the two attacks.

IV. DIFFERENT PROPOSED TECHNIQUES TO DETECT ROQ ATTACKS:

A number of techniques have been proposed to mitigate the ROQ attacks. They have been discussed in this section.

Y. Xu et al [4] had proposed a queue management technique like RED algorithm and the RED-PD algorithm. The RED (Random early detection) congestion control mechanism monitors the average queue size for each output queue using randomization.

Amey Shevtekar et al [5] proposed a detection algorithm for low rate TCP denial of service attack detection at edge routers. A new data structure was introduced to store the necessary history of the edge routers. This was a carefully designed structure and was light weighted.

Amey Shevtekar et al [6] also proposed a router based technique to mitigate the reduction of quality (ROQ) attacks. The proposed system works in two phases. Phase 1: the attack is detected at the routers with the help of the per flow information available at the routers. Phase 2: after the detection of the attack packets, the ROQ attack packets are dropped. ROQ attack packets are detected by sudden increase in the load in a short time period of all the expired flows, a simple filtering solution had been proposed to drop packets of the ROQ attacks.

Yu Chen at al [7] proposed effective detection of shrew attacks which remain an open problem. In the paper the challenge is met by proposing a new signal-processing approach to identifying and detecting the attacks by examining the frequency domain characteristics of incoming traffic flows to a server. The technique is quite effective, according to the simulation results and produces a solution in a very short period of a few seconds. Also simple technique has been used, so that it can be easily deployed in the Real network environment.

Yu Chen et al [8] have proposed a novel defense approach on the basis of the energy distributions of Internet traffic flows in the frequency domain. While exploring the energy distributions is was found that the TCP flows present a periodicity in the traffic pattern due to the TCP protocol behavior. The simulation results show that normal TCP flows can be separated from attack traffic using the energy distribution properties. Combining both the concepts of flow level spectral analysis and the sequential hypothesis testing, a new defense strategy or mechanism has been developed for the detection of low-rate DOS shrew attacks or ROQ attacks.

Jatinder Singh et al [9] proposed a defense scheme that detects the attack traffic on the basis of values obtained from the MAC layer. The scheme includes the detection and response stages. The detection stage uses three values. First is the frequency of RTS/CTS packets, second is the frequency of sensing a busy channel and third is the number of RTS/DATA transmissions. The three values are used to set a congestion bit, on the basis of this bit; the conclusion is drawn whether or not the traffic is from an attacker.

Rupa Rani et al [10] proposed a defense mechanism based on Continuous and Random Dropping (CARD) based DRDOS attack detection and prevention techniques in MANET. The scheme limits the rate and penalizes the attackers, based upon the rate limits ant load on the server. The rate limit is decreased exponentially at the victim end defense system and linear increase is made to it in accordance with attack traffic. The mechanism is discussed into three parts or phases: Detection, Prevention and Control.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

S. Venkatasubramanian et al [11] recently proposed a new detection mechanism based on flow monitoring for the ROQ attacks and then mitigate the ROQ attack in MANETS. Some monitoring nodes are selected according to some criteria. These nodes then monitor the incoming flows and examine the short lived flows. The short lived flows exceeding a threshold are added into a local black-list. All the blacklists are then sent to the master nodes, which then compare these black-lists, nodes appearing more than a certain number of times in these lists are detected as attackers and further traffic from such nodes are blocked.

V. CONCLUSION

The shrew and the ROQ attacks are though placed in the category of low rate DDOS attacks; there lies a difference in their aim and operation as discussed in the text above. These low rate attacks are quite difficult to detect and while keeping a low profile cause a lethal blow to the TCP throughput. A number of detection and defence mechanisms have been discussed, which on the basis of simulation results effectively help to detect the attack and increase the TCP throughput.

REFERENCES

[1] A. Kuzmanovic and E. Knightly, "Low-rate TCP-targeted denial of service attacks (The Shrew vs. the Mice and Elephants)", ACM SIGCOMM 2003, pp. 75–86, 2003.
[2] Mina Guirguis, Azer Bestavros and Ibrahim Matta, "Exploiting the transients of adaptation for RoQ attacks on Internet resources", IEEE ICNP 2004, pp. 184–195, 2004.
[3] Mina Guirguis, Azer Bestavros and Ibrahim Matta, "Bandwidth Stealing via Link Targeted RoQ Attacks", IEEE CCN 2004, 2004.
[4] Y. Xu, R. Guerin, "On the robustness of router-based denial-of-service (DoS) defense systems", ACM Computer Communications, Vol. 35, No. 3, pp. 47–60, 2005.
[5] Amey Shevtekar, Karunakar Anantharam, and Nirwan Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers", IEEE Communications Letters, Vol. 9, No. 4, April 2005.
[6] Amey Shevtekar and Nirwan Ansari, A router based technique to mitigate reduction of quality (RoQ) attacks, Computer Networks, Vol. 52, pp. 957–970, 2008.
[7] Yu Chen, Kai Hwang," Collaborative detection and filtering of Shrew DDoS attacks using spectral analysis", Journal of Parallel and Distributed Computing, Special Issue on Security in Grids and Distributed Systems, Vol. 66, No. 9, 2006.
[8] Yu Chen and Kai Hwang, "Spectral Analysis of TCP flows for Defense against Reduction-of-Quality Attacks", IEEE International Conference on Communications (ICC 2007), 2007.
[9] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur "A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN", International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.
[10] Rupa Rani and A.K. Vatsa, "CARD (Continuous and Random Dropping) based DRDOS Attack Detection and Prevention Techniques in MANET", International Journal of Engineering and Technology, Volume 2 No. 8, August, 2012.
[11] S. Venkatasubramanian and N. P. Gopalan, "A Flow Monitoring based Distributed Defense Technique for Reduction of Quality Attacks in MANET", International Journal of Computer Applications (0975 – 8887), Volume 21– No.1, May 2011.
[12] S. A. Arunmozhi and Y. Venkataramani, "A Flow Monitoring Scheme to Defend Reduction-of-Quality (RoQ) Attacks in Mobile Ad-hoc Networks", Information Security Journal: A Global Perspective, Vol.19, No.5, 2010, pp. 263- 272.
[13] Arunmozhi Annamalai and Venkataramani Yegnanarayanan, "Secured System against DDoS Attack in Mobile Adhoc Network", WSEAS Transactions on Communications, Issue 9, Volume 11, September 2012
[14] K. Kuppusamy and S. Malathi, "An Effective Prevention Of Attacks Using GI Time Frequency Algorithm Under DDOS", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.