Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 8, August 2013, pg.201 – 205

REVIEW ARTICLE

A Review of ROQ Attacks in Internet

Shaina Pundir[1], Naveen Kumari[2]

[1]Computer Science Engineering, Punjabi University Regional Center Information Technology and Management, Mohali, India

[2]Computer Science Engineering, Punjabi University Regional Center Information Technology and Management, Mohali, India

Abstract— Today secure network is the primary aspects in the network. Internet is the primary medium which is used by number of users around the across the networks. Network resources such as bandwidth, throughput, response time are affected most by these ROQ attacks. In this paper we have discussed ROQ attacks, its detection and mitigation of these attacks.

Key Terms: - ROQ; QOS; DOS; CPU; TCP; RTO; AQM

I. INTRODUCTION

The DOS is defined that the normal user can't get the service because the hacker seized the service using some different attack methods which can destroy the system and network and it can occupy the computer resources such as CPU, ram, buffer, and network bandwidth. The DOS Attacks has further various types, one of the major types of attacks is ROQ attacks [3].

Reduction of Quality (RoQ) attacks is a new breed of attacks that target adaptation mechanisms employed in current computing systems and networks. RoQ attacks keep an adaptive mechanism oscillating between over-load and under-load conditions, all the time. Instead of refusing the clients from the services completely, these ROQ attack throttle the TCP throughput heavily and reduce the QOS (Quality Of Service) to end systems [4].

RoQ attacks different from DoS attacks:

Denials of Service (DoS) attacks rely on overwhelming the victim with load that constantly exceeds its capacity. RoQ attacks, on the other hand, optimize the attack traffic to produce the maximum damage, while keeping a low profile to avoid detection. RoQ attacks do not necessarily result in a complete denial of service [6].

RoQ attacks different from Shrew attacks:

Shrew attacks exploit the timeout mechanism of TCP resulting in a complete denial of service. RoQ attacks do not target this specific protocol setting, but they are a general class of dynamic exploits that target adaptation mechanisms wherever they are present (transport layer, application layer, mac layer, etc,...). Also, RoQ attacks aim to maximize the attack potency [3].

Amey Shavetkar et al have proposed router-based technique to mitigate the stealthy reduction of quality (RoQ) attacks at the routers in the Internet. The RoQ attacks have been shown to impair the QoS sensitive VoIP and the TCP traffic in the Internet. It is difficult to detect these attacks because of their low average rates. They have also shown that their generalized approach can detect these attacks even if they employ the source IP address spoofing, the destination IP address spoofing, and undefined periodicity to evade several router-based detection systems [1].

Methodology used to assess the impact of RoQ attacks

We used a control-theoretic model to underline the complex interplay between the efficiency-load behavior of a resource and the adaptation mechanisms of both the resource and its consumers. The adaptation is modelled as an optimization process driving the system to a quiescent stable operating point. An optimized RoQ exploit would then keep the system oscillating between different states, in presence and absence of the attack traffic. We developed associated metrics to quantify the system's vulnerabilities. We present numerical and simulation results, which we validate with observations from real Internet experiments [2].

II. INTERNET ATTACKS OVERVIEW

The current architecture of Internet carries many security holes in it, which creates opportunities for attacker to launch a successful attack.[11] Before going through the detail about ROQ attacks, it is useful to have an overview and classification over internet attacks. An attacker uses a tool to exploit a vulnerability to perform an action on a target in order to achieve an unauthorized result. Thus, attack is an assault against a computer system or network as a result of deliberate, intelligent action.[10]

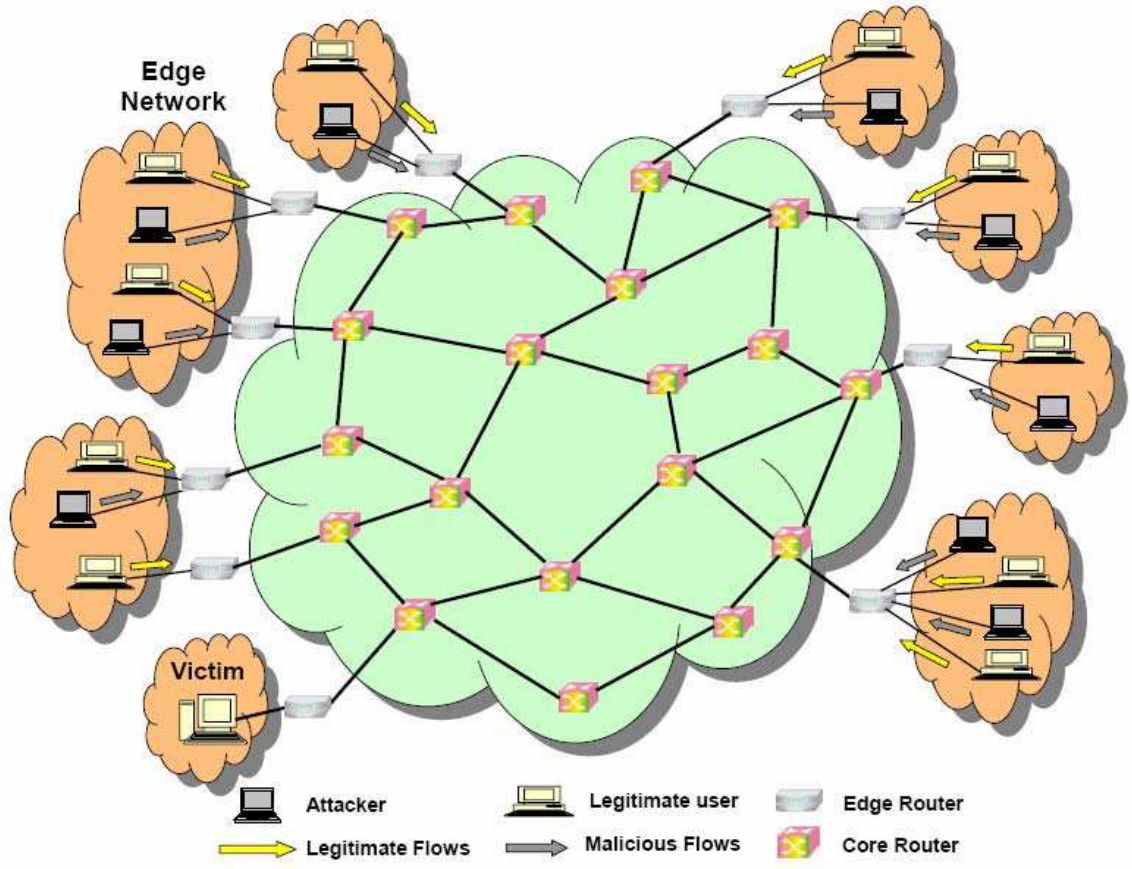

Fig.1 Reduction of quality attack on internet

General Attack Classification

A possible attack classification of internet attacks according to unauthorized result could be [dos review paper]

1) Increased Access: An unauthorized increase in the domain of access on a computer or network.

2) Disclosure of Information: Dissemination of information to anyone who is not authorized to access that information.

3) Corruption of Information - Unauthorized alteration of data on a computer network. This may result in loss of information.

4) Denial of Service: Intentional degradation or blocking of computer or network resources. Its main goal is to disrupt the services to legitimate user.

5) Theft of Resources: Unauthorized use of computer or network resources [15].

III. DOS AND ROQ OVERVIEW

According to the WWW Security FAQ, a DoS attack can be described as an attack designed to render a computer or network incapable of providing normal services, A DoS attack is characterized by an intentional attempt by malicious users/attackers to completely disrupt or degrade availability of services/resources to legitimate/authorized users[2]. Hence, legitimate users are deprived of available services/resources they would normally expect to have. These attacks do not necessarily damage the data directly or permanently, but they deliberately compromise availability of the resources and thus, can cost the target a great deal of time and money [3].

By the high rate or high volume, the typical DDoS flooding Attacks are characterized. An alternative of DDoS attacks has been identified recently which is too complex to detect which are called as shrew attacks or Reduction of Quality (RoQ) attacks. Instead of refusing the clients from the services completely, these RoQ attacks throttle the TCP throughput heavily and reduce the QoS to end system gradually [8].

The transients of systems adaptive behaviour is targeted by the RoQ attacks instead of limiting its steady state capacity. The RoQ attacks can use source and destination IP address spoofing, and they do not have distinct periodicity, and may not filter the attack packets precisely. In order to escape from being caught by the trackback techniques, RoQ attacks often launch attacks through multiple zombies and spoof header packet information. But, it is important to control the frequency domain characteristics of attacking flows. In order to throttle the TCP flows efficiently, the attacking period has to be close to the Retransmission Time Out (RTO). Using traffic spectrum, the energy distribution pattern will give up such malicious flow detection mechanism even if the source IP address are carried in packet header are falsified[10].

Network Adaptation Mechanisms and Vulnerabilities:

End system protocols (*e.g.*, TCP) rely on feedback mechanisms to adapt their sending rates to match their "fair share" of network resources. Buffer management schemes play an important role in the effectiveness of transmission control mechanisms as they constitute the feedback signal (by marking or dropping packets) to which such mechanisms adapt. Active Queue Management (AQM) techniques have been developed that try to maintain the queue size at a target level and employ probabilistic dropping. Stabilizing the queue at a low target guarantees efficiency while minimizing jitter and round trip time in general[12].

IV. LITERATURE REVIEW

- **Mina Guirguis et al. [3]** have explained what ROQ attack is, and how is it different from other attacks like traditional Brute force, high rate DoS attacks, as well as recently proposed attacks that exploit specific protocol settings such as TCP timeouts. They have also developed control theoretic models and associated metrics to quantify these vulnerabilities of common adaption mechanisms.
- **Mina Guirguis et al. [4]** have developed a control theoretical model for assessing the impact of ROQ attacks on end system's admission controller. They have quantified the damage inflicted by an attacker through deriving appropriate metrics. They have also studied the ROQ attacks on Internet end systems.
- **Wei Ren et al. [7]** have explained in detail congestion based ROQ attacks in mobile ad-hoc networks. They have classified these attacks into four categories: pulsing attack, round robin attack, self-whisper attack and flooding attack. Then they have proposed a defense scheme that includes both the detection and response mechanisms. They have used extensive ns2 network simulations to demonstrate the existence of high goodput and delay jitters under the pulsing attack mode.
- **Yu Chen et al. [9]** in their paper explore the energy distribution of Internet traffic flows in frequency domain. Normal TCP traffic flows present in periodicity because of protocol behaviour. The results reveal that normal TCO flows can be segregated from malicious flows according to energy distribution properties. The combining flow level spectral analysis with sequential hypothesis testing, the have proposed a novel defense scheme against ROQ attacks.

V. ATTACK DETECTION SYSTEMS

Detection system architecture and logic- The ROQ attacks cause fluctuations in the queue size and congestion levels at the router during the ON period of the Attack. They can incur an increase in the instantaneous packet loss. It is important that the detection system should be "OFF" when there is no attack. The network administrator can also invoke the detection system by using the congestion signal from the active queue management (AQM) system. Amey et al have used a congestion signal from the adaptive virtual queue (AVQ) algorithm to invoke the detection system [1].

Intelligent attacker- the only way an attacker can evade detection is if the attack flows are classified as the benign flows. This can be staged if an attack flow sends packets for more than 2s, and then uses the same flowid to launch a low rate DoS and RoQ attack. The time difference approach relies on computing the time difference between the consecutive packets of a flow. The time difference approach [10] relies on computing the time difference between the consecutive packets of a flow. It was shown in[10] that only DoS and RoQ attack flows exhibit periodicity in the time difference, while other legitimate traffic flows lack this characteristic periodicity in the time difference , while other legitimate traffic flows lack this characteristic periodicity of the property of the low rate DoS and RoQ attack. The time difference technique can be easily integrated in the current detection system as it only requires the following per-flow information, the created time, the last accessed time, and per-flow system. The per flow system is configured to provide each packet arrival time as one of the flow fields, and just has to be record the timestamp when it samples a packet belonging to a particular flow for this requirement. If a particular flow is found to be an attack flow by using the time difference technique, it can be easily blocked by filtering traffic coming from that IP address [1].

Trace evaluation- To confirm that the thresholds proposed in the previous subsection will work for the Internet traffic, A. Shevtekar et. al. have evaluated the strategy by analysing the OC48 (2.5Gbps) traces provided by CAIDA [27].[8] Using the Coralreef[28] software, they have first obtained the expired flow statistics<Source IP address, Destination IP address, Source IP port, Destination IP port, Packetcnt, Bytecnt, Createdtime, and Last accessed time>, which are similar to the ones that have been proposed to collect for all the flows. The attack detection algorithm runs using the flow information obtained by the coral reef software to observe the characteristics of the sum variable in the absence of the low rate DoS and RoQ attack. The attack with ON period greater than 2s can certainly be detected by this approach, but they can be easily detected by RED-PD and many other existing AQM schemes too. They have highlighted that in a short period of 1-2s the sum variable does not exceed the proposed thresholds in the absence of the low rate DOS and RoQ attack, the sum will exceed the proposed thresholds [1].

Filtering logic- Amey S. et al have propose a filtering scheme to mitigate the RoQ attack detection algorithm provides information on how frequently the attack bursts are instigated from which one may determine the attack type(i.e. RoQ attack). To filter the RoQ attack packets, which are using the spoofed IP addresses, they have proposed a non- deterministic approach because it is difficult to know which IP address an attacker will use in future bursts. Thus, it is futile to store the Attack IP addresses seen in the old bursts [11]. Thus, it is futile to store the attack IP Addresses seen in the old bursts. We have developed a simple method to address this problem. As mentioned before, they separate the long-lived flows in the benign flow table, and they are treated preferentially. On the arrival of the packets belonging to these flows, and the buffer is full, they are enqueued in the queue and are passed normally. Special attention is needed while identifying a new benign long lived flow when the attack filtering mode is ON by verifying that the difference mode createdtime and last accessed time should be close to the inspection time to classify the flow as a non-expired, legitimate, and long-lived flow. The detection algorithm also considers special attack scenarios before classifying the flow as a non-expired, legitimate and long lived flow. Packets, which belong to the new flows and are not present in the benign flow table, are enqueued in the queue, and the current queue length is then computed. The current queue length is checked if it is greater than a% of the queue limit. If so, the enqueued packet is dropped immediately, otherwise, the enqueued packet is treated normally.[10] Their strategy is a preemptive strategy to prevent the attack packets from gaining access to the legitimate bandwidth. It can be empirically confirmed that the point after which the queue length exceeds a% of the queue limit will occur only during the attack epochs as the legitimate bandwidth, and the packets out of the queue once the occurrence of the attack is confirmed by the proposed attack detection algorithm. Nevertheless, under no attack during congestion, the legitimate flows can force other legitimate packets to be dropped, but in the RoQ attack case, we know that the most likely, these packets are RoQ attack packets, and hence we drop these packets. The filtering is also activated at the approximate time instants for 1s when attack packets start arriving at the queue [1].

ACKNOWLEDGEMENT – This work has been supported in part of M.Tech thesis from Punjabi University, Patiala. It is my immense pleasure to express my deep sense of gratitude and indebtedness to my highly respected and esteemed Ms Naveen Kumari, and Upasna Sen Gupta HOD (CSE). Their invaluable guidance, inspiration, constant encouragement sincere criticism and sympathetic attitude could make this paper possible.

REFERENCES

[1] Amey Shevtekar and Nirwan Ansari (2007), A router based technique to mitigate reduction of quality (ROQ) attacks [online], Available: http://www.sciencedirect.com.
[2] Jatinder Singh, Dr. Savita Gupta and Dr. Lakhwinder Kaur "A MAC Layer based Defense Architecture for Reduction-of-quality(ROQ) Attacks in wireless LAN", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.
[3] Mina Girguis , Azer Bestavros and Ibrahim Matta, "Expoliting the aspects of adaption for ROQ Attacks on Internet Resources", Tech report BUCS-TR-2004-005, CS Dept, Boston University, 2004.
[4] Mina Girguis , Azer Bestavros and Ibrahim Matta, "Reduction of Quality (ROQ) attacks on Internet End-Systems", CS Dept, Boston University, 2005.
[5] Mursel Yildiz, Ahmet Cihat Toker, Fikret Sivrikaya, Seyit Ahmet Camtepe and Sahin Albayrak, "User Facilitated Congestion And Attack Mitigation", DAI-Labor/ Technische Universitat Berlin, Germany, 2011.
[6] 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), Vol 21- No.1, May 2011.
[7] Wei Ren, Dit-Yan Yeung, Hai Jin and Mei Yang, "Pulsing ROQ Attack and Defense Scheme in Mobile Ad Hoc Networks", International Journal of Network Security, Vol.4, No.2, PP.227-234, Mar. 2007.
[8] Wentao Liu, "Research on DOS Attacks and Detection Programming", Third International Symposium on Intelligent Information Technology Application, 2009.
[9] Yu Chen and Kai Hwang, "Spectral Analysis of TCP Flows for Defense against Reduction Of Quality Attacks", University of Southern California, Los Angeles, USA, 2007.
[10] CSI/FBI Computer Crime and Security Survey.http://www.gocsi.com/>, 2006, online.
[11] A. Kuzmanovic, E Knightly, Low-rate TCP- targeted denial of service attacks(The Shrew vs. the Mice and Elephants), in: ACM SIGCOMM 2003, pp.75-86.
[12] X. Luo, R.K.C. Chang, On a new class of pulsing denial-ofservice attacks and the defense, in NDSS 2005, 2005.
[13] A. Shevtekar, N. Ansari, Dolowrate dos attacks affect QoS sensitive VoIP traffic? In: IEEE ICC 2006, pp.2153-2158
[14] Z. Gao, N. Ansari, Tracing Cyber-attacks from the practical perspective, IEEE Communication Magazine 43(5)(2005) 123-131.
[15] Ruiliang Chen, Jung-Min Park and Randolph Marchany, "A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks", IEEE Transaction on Parallel on Distributed Systems, Vol. 18, No. 5, May 2007.
[16] Jeevaa Katiravan, C. Chellappan and J. Gincy Rejula, "Detecting the Source of TCP SYN Flood Attack using IP Trace Back", European Journal of Scientific Research ISSN 1450-216X Vol.71 No.1, pp. 78-84,2012.

