A router-based technique to mitigate reduction of quality (RoQ) attacks

Abstract

We propose a 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. We also show that our 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. The detection system operates in two phases: in phase 1, the presence of the RoQ attack is detected from the readily available per flow information at the routers, and in phase 2, the attack filtering algorithm drops the RoQ attack packets. Assuming that the attacker uses the source IP address and the destination IP address spoofing, we propose to detect the sudden increase in the traffic load of all the expired flows within a short period. In a network without RoQ attacks, we show that the traffic load of all the expired flows is less than certain thresholds, which are derived from real Internet traffic analysis. We further propose a simple filtering solution to drop the attack packets. The filtering scheme treats the long-lived flows in the Internet preferentially, and drops the attack traffic by monitoring the queue length if the queue length exceeds a threshold percent of the queue limit. Our results show that we can successfully detect and mitigate RoQ attacks even with the source and destination IP addresses spoofed. The detection system is implemented in the ns2 simulator. In the simulations, we use the flowid field available in ns2 to implement per-flow logic, which is a combination of the source IP address, the destination IP address, the source port, and the destination port. We also discuss the real implementation of the proposed detection system.

Introduction

The CSI/FBI 2006 [1] survey showed that the denial of service (DoS) is still an issue leading to a significant revenue loss for many organizations. The low rate DoS attack poses a new threat to the Internet [2], [3], [4], [5], [6], [7], [8]. The low rate DoS attack was first publicly known from the work of [2], referred to as the Shrew attack. The RoQ attack [3] does not try to shut down the legitimate flows, but tries to reduce the quality of service experienced by them. Thus, it is even harder to defend against RoQ attacks. All these low rate types of DoS attacks can be defined by a general periodic waveform as shown in Fig. 1. A low rate type of DoS attack is characterized by three parameters, the attack period (T), the burst period or the burst length (t), and the burst rate (R). The Shrew attack [2] exploits the minimum RTO property and the exponential backoff algorithm of the TCP protocol. It works by sending a burst of attack packets with a rate greater than the target capacity for a short period like 20–200 ms at the target router every 1 s. This leads to packet drops of legitimate TCP connections, which subsequently enter timeout; as these connections attempt to retransmit lost packets after the minimum RTO of 1 s, they are again hampered by the attack traffic at the router. The connections now use the exponential back off algorithm to retransmit lost packets, attempting to retransmit packets at 2^n seconds, where n is an integer. These times are multiples of 1 s during which the attack traffic is present at the router, thereby continuously denying service to the legitimate TCP connections. Typically, the Shrew attack was shown to be lethal to the long-lived TCP flows in the Internet.

On the contrary, the RoQ attack targets to dampen QoS experienced by the TCP traffic by keeping the time period high. It tries to occupy the share of the legitimate network traffic by sending high rate bursts on longer timescales. For instance, by sending the periodic bursts of attack packets to a router, the attacker does not allow the queue to stabilize such that the QoS sensitive Internet traffic experiences degradation of quality [6]. In particular, the periodicity is not well defined in an RoQ attack, thereby allowing the attacker to keep the average rate of the attack traffic significantly low to evade the adaptive queue management techniques like RED and RED-PD [9]. The RoQ attack exploits the AIMD algorithm of the TCP protocol; it achieves this by intermittently sending the attack traffic during which the legitimate packets are dropped, and TCP reduces the current congestion window by half and enters the slow start phase. Since the attack time period is high, the legitimate TCP traffic regains some of the lost congestion window size slowly following the AIMD mechanism, and thus only suffering from reduction of quality. We consider the RoQ attack and the low rate DoS attack model in our study. To distinguish the two attacks, we classify an attack with time period greater than or equal to 5 s as a RoQ attack, and an attack with time period less than 5 s as a low rate DoS attack. It was suggested in [3], though not explicitly specified, to set a higher time period, but the time period value of 5 s is empirically found to perform well for our proposed attack filtering algorithm.

In our earlier work [10], the detection system can detect the stealthy low rate DoS and RoQ attack by using a simple time difference method. The time difference technique uses a per-flow approach to store arrival times of the packets belonging to each flow, and computes inter-arrival times between the consecutive packets to detect periodicity. The attacker using IP address spoofing can easily deceive this simple per-flow approach as the time difference approach will not be able to detect periodicity in the attack flow, which is no longer a single flow. In this paper, we consider an attacker that will use the IP address spoofing to fool the per flow detection system. The approach presented in this paper works in conjunction with our previous approach, which can easily detect low rate DoS attack that do not use IP address spoofing, to provide a complete solution against these attacks. Traditional approaches to mitigate the IP address spoofing such as IP traceback are useful when an end-host is attacked [11], [12]. On the contrary, the RoQ attack targets network elements, and so packets may not even reach the end host.

Our objective is to address the following question: can an individual router detect spoofed packets used in the low rate DoS and RoQ attack, and alleviate/mitigate the RoQ attack? Our solution provides both detection and mitigation against the RoQ attacks. We propose a scalable technique that passively detects the low rate DoS and

RoQ attacks. After having confirmed the onset of an RoQ attack, we enable our filtering algorithm to separate long-lived legitimate flows at the router, and subsequently to drop the RoQ attack packets. The filtering algorithm is best suited for RoQ attacks; furthermore, we briefly discuss the problem of filtering low rate DoS attack packets using our approach.

The rest of the paper is organized as follows. Section 2 describes the problem in detail. Section 3 presents the detection system. Section 4 discusses the hardware implementation issue. Section 5 presents the ns2 simulation results and relevant discussion. Related works and comparisons with the proposed detection system are described in Section 6, followed by concluding remarks in Section 7.

Section snippets

Problem description

The MIT Spoofer project [13] has reemphasized the detrimental effect of the IP address spoofing. The subnet IP address spoofing [14] is easily orchestrated, as the ingress IP address filtering cannot contain the spoofing. To illustrate the subnet IP address spoofing, consider an attacker in the subnet, 12.28.34.0–12.28.34.100; an attacker can easily use any address in this range for spoofing a source IP address inside this subnet. The IP address of every outgoing packet can be easily spoofed by

Detection system architecture and logic

The low rate DoS and 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. The packet loss observed in our experiments [6] was greater than 2%. It is important that the detection system should be “OFF” when there is no attack. Note that for the RoQ attack, the packet loss might not increase, and so the network administrator can also invoke the detection system by using

Implementation discussion

Internet security is vital to facilitate e-commerce transactions, and there has been continued research effort to provision network traffic monitoring at high speeds. The hardware capabilities achieved by some other approaches like the deep packet inspection [29], [30], at relatively low speeds show that our proposed approach can be realizable. That the fast memory, i.e., SRAM, is exorbitantly costly, and the cheap memory, i.e., DRAM, is too slow to work at the high speed line rates, are the

Simulation results and discussion

We used the ns2 simulator [35] to demonstrate the performance of the proposed detection scheme. The topology used in our experiment is shown in Fig. 8. We used the PackMime [36] HTTP traffic generator, which was developed by using the real traces of the Internet traffic. It is the most recent work about the modeling of the HTTP traffic that improves over the previous HTTP traffic models. We have adopted the PackMime traffic model in our study because the HTTP traffic interaction with the

Related works

We briefly review some of the countermeasures proposed in the literature to mitigate the low rate DoS and RoQ attacks in the Internet although none of them has made a comprehensive attempt to address such attacks that can use IP address spoofing or botnets. In [26], an autocorrelation and dynamic time warping algorithm is proposed to detect the low rate DoS attacks. The paper proposes deficit round robin algorithm to filter the attack flows, which will fail to drop attack packets when the

Concluding remarks

We have proposed a router-based approach to detect the stealthy low rate DoS and RoQ attacks which use IP address spoofing or botnets. This work addresses the IP address spoofing and botnet problem in the context of the low rate DoS and RoQ attacks, and proposes an effective and realizable solution to defend against RoQ attacks. The effectiveness of the proposed approach has been demonstrated via extensive experiments. At the time of writing this paper to best of our knowledge, there is no

Acknowledgement

This work has been supported in part by the National Science Foundation under Grants 0435250 and 0726549.

Amey Shevtekar received the B.S. degree in Electronics and Telecommunications Engineering from University of Mumbai, India, and the M.S. degree from the New Jersey Institute of Technology (NJIT) in Telecommunications. He is pursuing his doctorate in Computer Engineering at New Jersey Institute of Technology (NJIT), focusing on network security, Low Rate DoS Attacks, DDoS Attacks, and computer networks.

References (45)

- CSI/FBI Computer Crime and Security Survey. <http://www.gocsi.com/>, 2006,...
- A. Kuzmanovic, E. Knightly, Low-rate TCP-targeted denial of service attacks (The Shrew vs. the Mice and Elephants), in:...
- M. Guirguis, A. Bestavros, I. Matta, Exploiting the transients of adaptation for RoQ attacks on Internet resources, in:...
- S. Ebrahimi-Taghizadeh, A. Helmy, S. Gupta, TCP vs. TCP: a systematic study of adverse impact of short-lived TCP flows...
- X. Luo, R.K.C. Chang, On a new class of pulsing denial-of-service attacks and the defense, in: NDSS 2005,...
- A. Shevtekar, N. Ansari, Do low rate dos attacks affect QoS sensitive VoIP traffic? in: IEEE ICC 2006, 2006, pp....

- R. Chertov, S. Fahmy, N. Shroff, Emulation versus simulation: a case study of TCP-targeted denial of service attacks,...
- M. Delio, New Breed of Attack Zombies Lurk. <http://technews.acm.org/articles/2001-3/0514m.html#item2>,...
- Y. Xu *et al.*
  On the robustness of router-based denial-of-service (DoS) defense systems
  ACM Computer Communications Review
  (2005)
- A. Shevtekar *et al.*
  Low rate TCP denial-of-service attack detection at edge routers
  IEEE Communication Letters
  (2005)