



Advanced Networking Laboratory
Department of ECE, NJIT

Low-Rate Denial of Service Attack Detection and Prevention



REU Site for
Computer Networking
and Security

John Cosgrove Stille

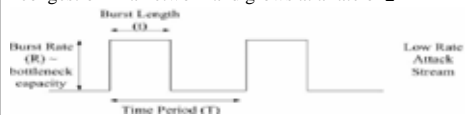
Mentors: Amey Shevtekar, Dr. Nirwan Ansari
Advanced Networking Laboratory

Abstract

Low rate denial of service attacks present a unique challenge to QoS sensitive traffic and TCP traffic on the internet. This research focuses on the detection and mitigation of the attack on an internet router. The mechanisms proposed minimize the effects of stealthy attacks against legitimate TCP flows. Studies are done through the use of DETERLab and NS2.

Introduction

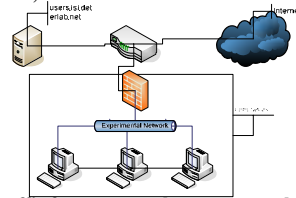
- Low rate denial of service attacks are characterized by a pulsing attack pattern.
- Low average throughput makes aggregate traffic appear minimized
- The TCP timeout/exponential back off mechanism is taken advantage of to prevent throughput of "good" flows.
- Exponential back off exists as a way to reduce congestion in a network and grows at a rate of 2^n



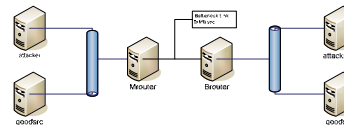
- **Burst Length** - Amount of time UDP traffic is sent through the bottleneck link at a rate greater than or equal to the bottleneck capacity.
- **Burst Rate** - The throughput achieved or sought to be sent through the bottleneck link greater or equal to the speed of the bottleneck link.
- **Time Period** - Total time between start of one attack and the start of the next.
- DETERLab provides an emulation test bed for security research and is based on Emulab.
- DETERLab is located at USC Information Sciences Institute and The University of Utah.
- NS2 is a network simulation tool provided by USC for network topology experiments.

Methodologies

- Experiments are setup on the DETERLab test bed, allowing full control of network topology, characteristics, and runtime execution.



- Generate traffic from an attacker to an attack traffic sink on the other side of a router implementing the proposed detection technique. The following topology was used for initial testing.



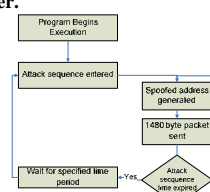
- Traffic was generated using an IP spoofing packet sender created for this experiment. It generates a complete low rate denial of service attack against any router.

Burst Rate $\approx 12\text{MB/s}$

Burst Length - .5 sec

Time Period - 1 sec

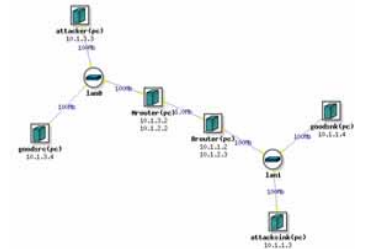
Sequences - 180



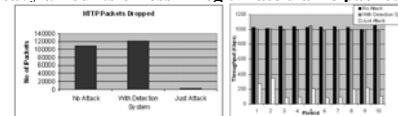
- TCP traffic is generated from the "good" source to the "good" traffic sink. This traffic should emulate standard internet traffic and be representative of "good" flows.

Methodologies/Results on NS2

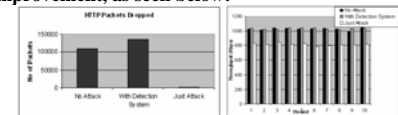
- Using RED queues we can detect when the packet rate has placed a strain on the bottleneck link, creating a backup in the queue. At this time we turn the detection system on.
- During the attack detection execution we will verify against a benign flow table. The short flow table will be updated if it does not exist as a benign flow in the system. We will check against expired flows and flows that reach a tuneable low rate denial of service threshold.
- In the following emulated topology we placed the detection system on Mrouter:



- Figures below show that the detection mechanism allows for very comparable average throughput when the attacker chooses one spoofed address throughout the entire attack, while not incurring heavy amounts of loss in legitimate traffic packets.



- Similar patterns are found when every packet is spoofed from a destination source. Although this detection is more difficult, results do show improvement, as seen below:



Discussion and Further Work

- Utilizing fast memory we can read the legitimate flow information off of the router at line rate. After reasonable amounts of time we will transfer the data to slow memory.
- A more recent work has shown [2] that by tuning the sampling probability the short flows can be estimated using an array of 32bit counters without using sophisticated architectures like the space code bloom filter. This type of sampling would help generate more information on short flows, rather than just long flows.
- A software implementation is being worked on for the Click Modular Router, as a fully functioning example of this algorithm.
- The use of emulated traffic and scenarios will give confidence in results that have been found.

Conclusion

A methodology for detection and mitigation of low rate denial of service attacks results in better overall performance of legitimate flows while under attack, as opposed to an alternative scenario where no detection mechanism is in place. This system allows for a hardware implementation to exist, while utilizing reasonable resources in the current market.

References

- [1] A. Shevtekar and N. Ansari, "Do Low Rate DoS Attacks Affect QoS Sensitive VoIP Traffic?," Proceedings of IEEE ICC 2006, Istanbul, Turkey, June 2006, pp. .
- [2] A. Kumar and J. Xu, "Sketch Guided Sampling - - Using On-Line Estimates of Flow Size for Adaptive Data Collection," Proceedings of IEEE Infocom 2006, Barcelona, Spain, April 2006, pp. .
- [3] Emulab Documentation [Online] Available: <http://www.isi.deterlab.net/tutorial/docwrapperr.php?docname=tutorial.html>
- [4] A. Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Communication Letters, Vol. 9, No. 4, April 2005, pp.363-365.