Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants)

Aleksandar Kuzmanovic and Edward W. Knightly. In ACM SIGCOMM'03

Presented by Fengwei Zhang

Outline

- Introduction
- Background
- Shrew Attack
- Defense Mechanisms
- Conclusions

Outline

- Introduction
- Background
- Shrew Attack
- Defense Mechanisms
- Conclusions

Introduction

- Denial of Service (DoS) attack

> «A denial of service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory bandwidth, and disk space.»
>
> (from: NIST Computer Security Incident Handling Guide, source: Stallings/Brown (2012), p.244)

- Examples
  - A YouTube video (https://www.youtube.com/watch?v=9qmyX9DgqG4)

Outline

- Introduction
- Background
- Shrew Attack
- Defense Mechanisms
- Conclusions

Background

- Traditional DoS attacks
  - Consuming the resource (CPU, Memory, Disk, Bandwidth) of the target systems
  - Example: Distributed Denial of Service (DDoS) attack, SYN flooding
- Defense
  - Attacking traffic has a high rate
  - Monitoring the traffic using statistics

Background

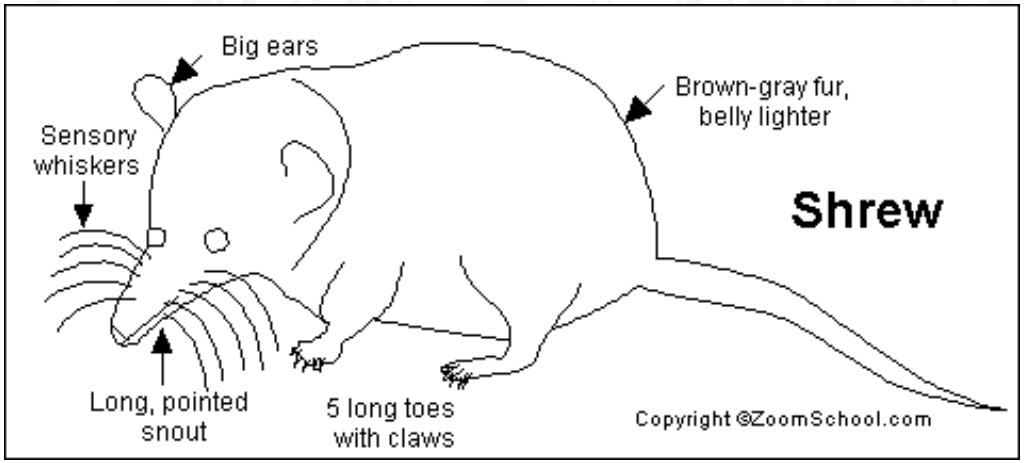
- Transport Control Protocol (TCP)
  - Providing reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network
  - Applications such as the World Wide Web, email, and file transfer
  - User Datagram Protocol (UDP) provides a connectionless datagram service that emphasizes reduced latency over reliability

Outline

- Introduction
- Background
- Shrew Attack
- Defense Mechanisms
- Conclusions

What is Shrew

- A shrew is a small but aggressive mammal that ferociously attacks and kills much larger animals with a venomous bite



Shrew Attack

- Low-rate TCP-targeted attacks
- Cannot detect by counter-DoS approaches such as traffic analysis
- Able to severely deny service to legitimate users

TCP Congestion Control

- Cwnd: Congestion Window
- RTT: Round Trip Time
- AI: Additive Increase
- MD: Multiplicative Decrease

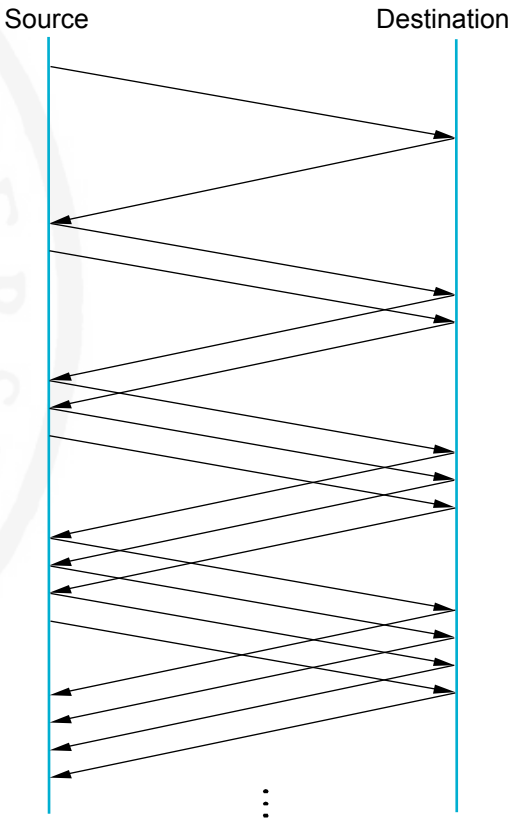


Figure source: [3]

TCP Timeout Mechanism

- TCP's retransmission timeout (RTO)
  - Detects packets loss
  - Waits for a period of retransmission timeout to expire, reduces its congestion window to one packet and resends the packet
  - RFC2988 recommends minRTO = 1 sec

Shrew Attack

- TCP congestion control: AIMD

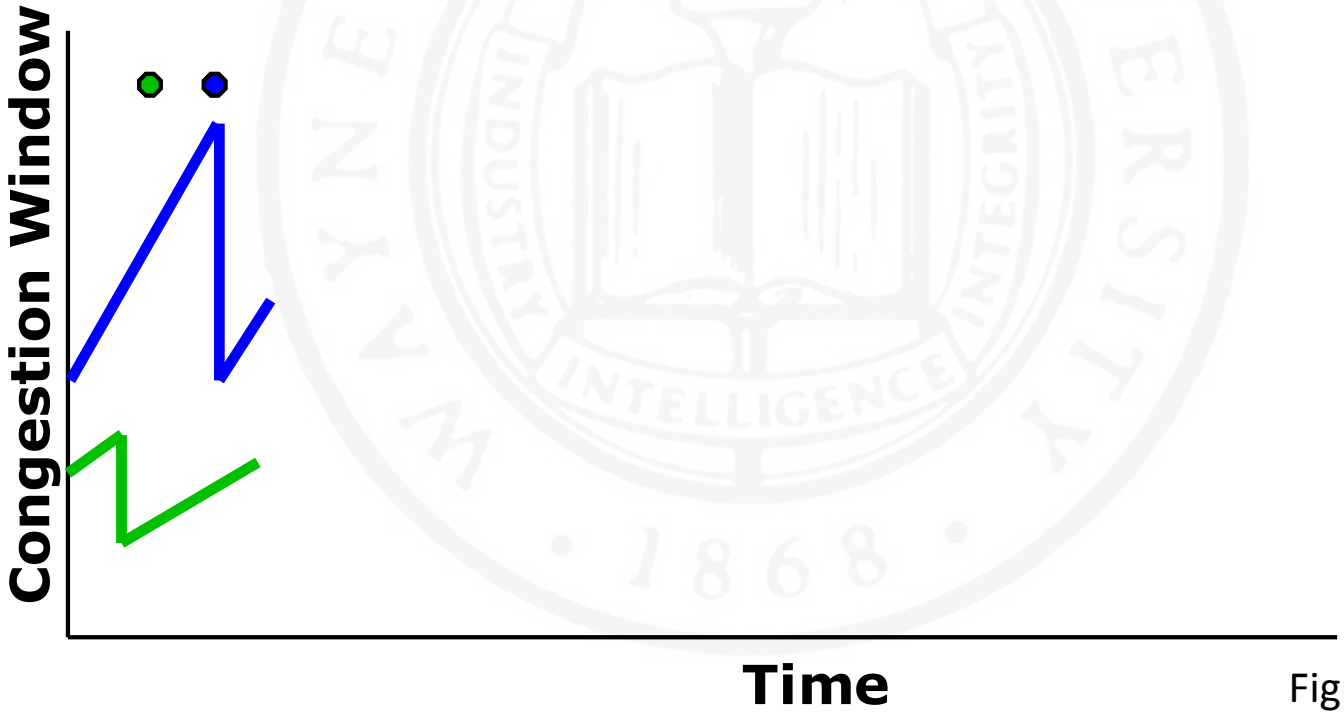


Figure Source: [1]

Shrew Attack

- Pulsing introduces **outage**
- multiple packet losses force TCP to enter RTO

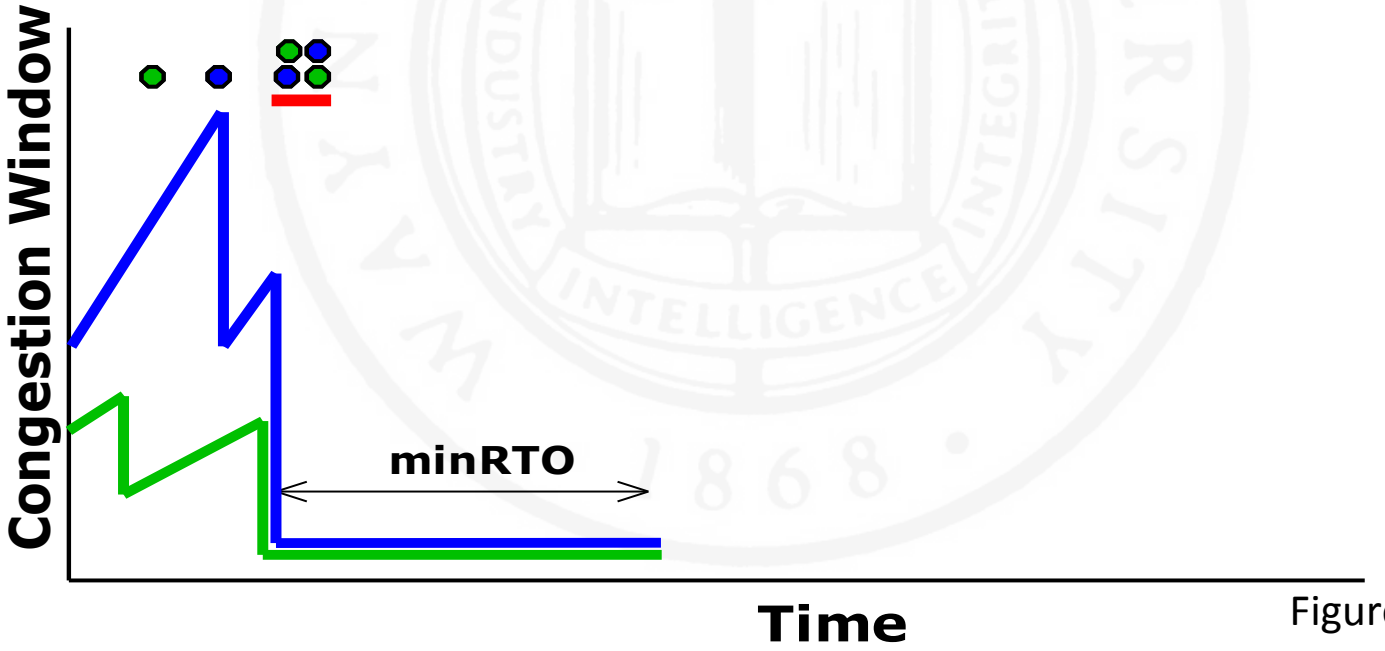


Figure Source: [1]

Shrew Attack

- Timeout makes TCP enter slow-start
- Attackers pulse, force packet losses, and TCP enter retransmission again

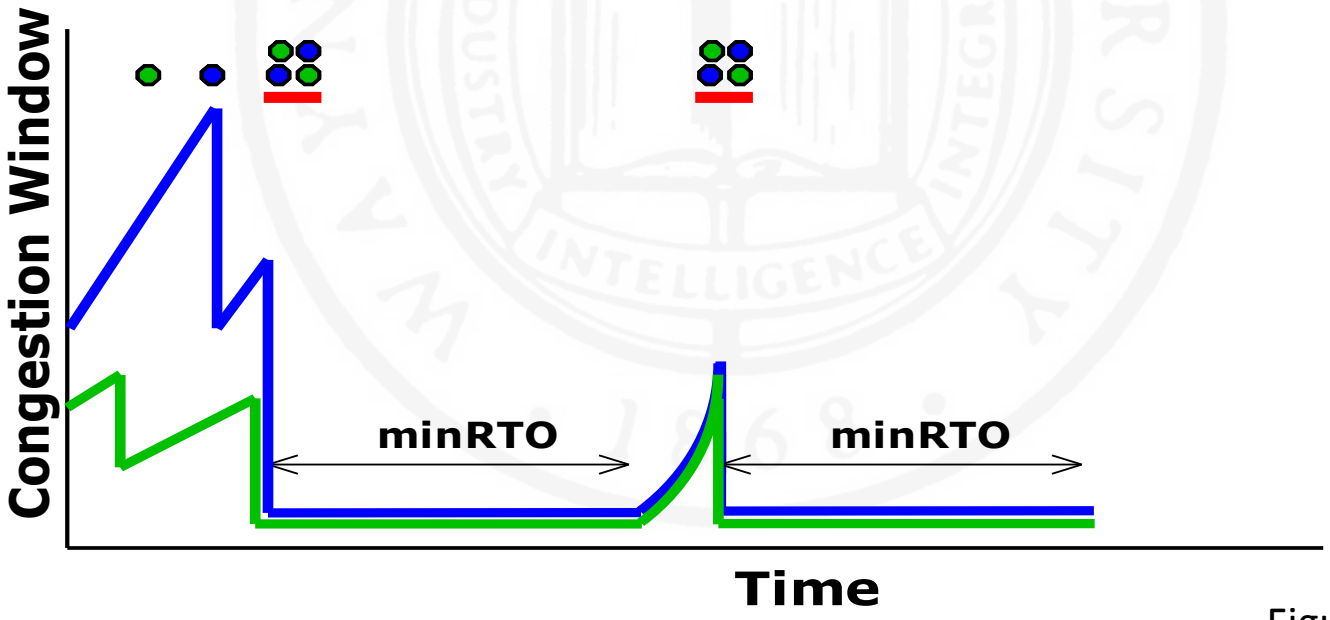


Figure Source: [1]

Shrew Attack

- Attackers periodically repeat the pulse

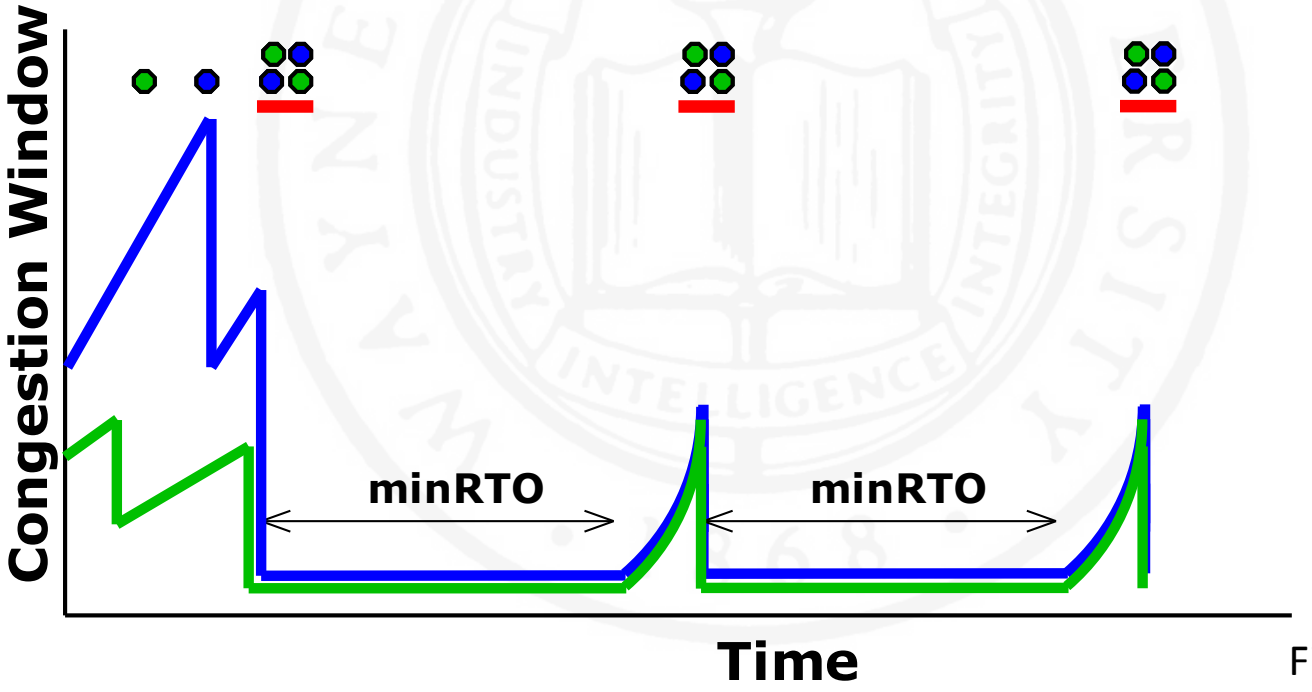
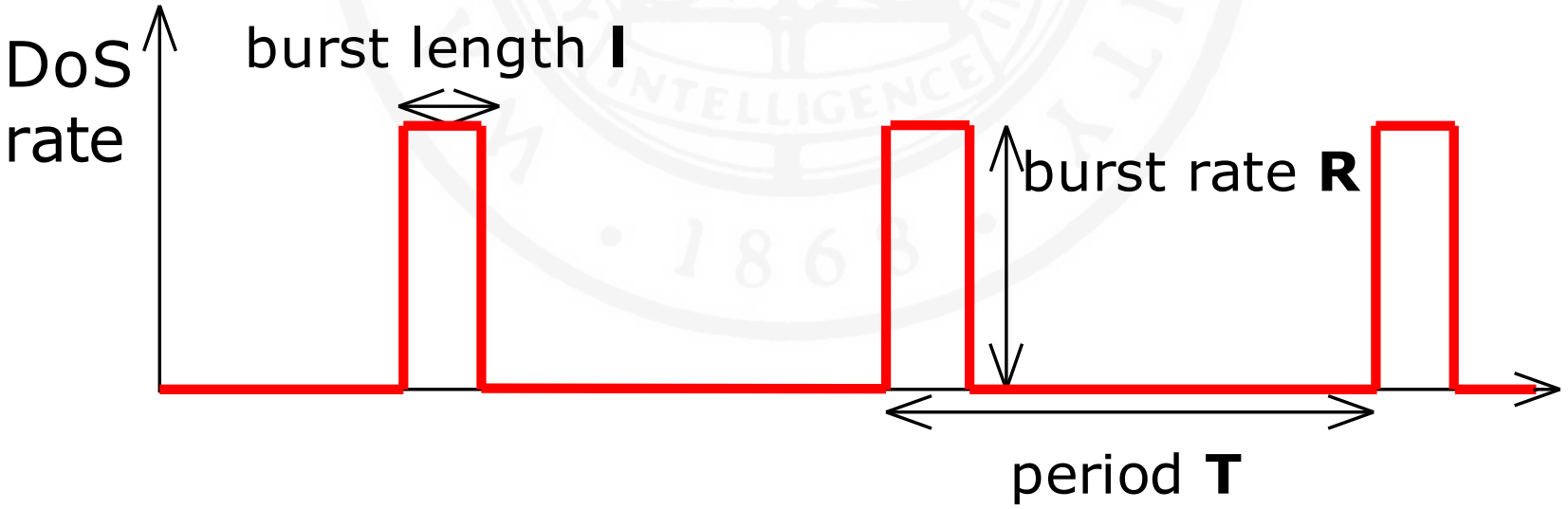


Figure Source: [1]

Shrew Attack

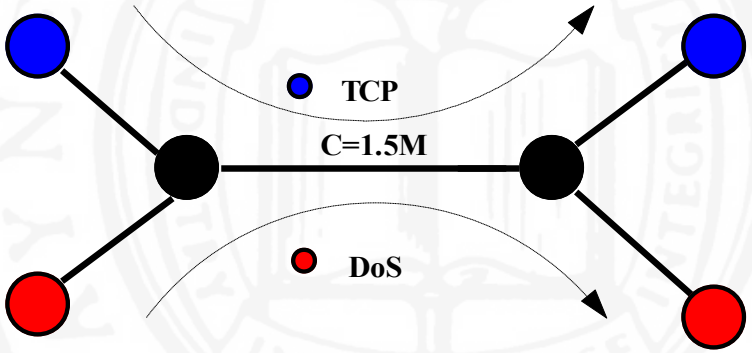
- Optimal case: square-wave stream
  - **l** is RTT and **T** is minRTO
- Low-rate "TCP friendly"
  - DoS defense mechanisms tuned for high rate attacks
  - Very hard to detect

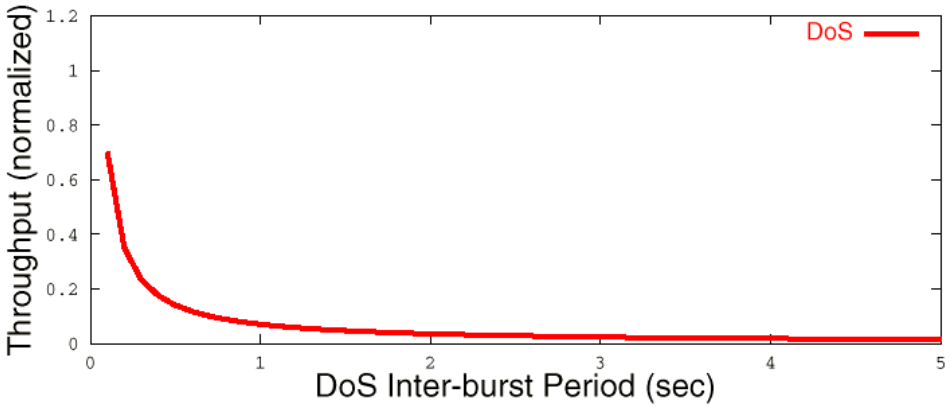
Figure source: [1]



Shrew Attack Example [1]

- **DoS** stream: **R=C=**1.5Mb/s; **l**=70ms (~TCP RTT)





Outline

- Introduction
- Background
- Shrew Attack
- Defense Mechanisms
- Conclusions

Defense Mechanisms

- Router-Assisted Mechanisms
  - Though having low average rate, attackers do send high-rate bursts for short time intervals
  - Identify traffic pattern by smart routers
- End-point minRTO Randomization
  - Attacking pulses need to be synchronized
  - RFC sets minRTO = 1 sec, so that attackers can predict the packets retransmission
  - Moving target defense: randomization

Other Low-rate DoS Attacks

- Slowloris attack against web server
  - Holds the connection open by sending valid but incomplete HTTP requests
  - Sends a bit more information just before the connection time out
  - Eventually all the connections will be used up and no other server will be able to connect
  - A YouTube video (https://www.youtube.com/watch?v=G2PMqeJMCfU)
- Reduce of Quality (RoQ) Attacks
  - Low-rate DoS is a type of RoQ attack
  - Active research area

Outline

- Introduction
- Background
- Shrew Attack
- Defense Mechanisms
- Conclusions

Conclusions

- Shrew attack
  - Exploits the TCP retransmission mechanism
  - Low-rate, TCP-friendly
  - Very hard to detect
  - Open research (DARPA XD3 Program)

References

- [1] http://www.cs.northwestern.edu/~akuzma/rice/doc/shrew.ppt
- [2] http://www.cs.northwestern.edu/~akuzma/rice/doc/shrew.pdf
- [3] http://web.cs.wpi.edu/~cs3516/b09/slides/tcp-cong-control.ppt

Paper Discussion

- Zhenyu Ning,
- CSC 6991 – Advanced Computer System Security
-
- Low-Rate TCP-Targeted Denial of Service Attacks
- In contrast to well-known high-rate DoS attacks, this paper presents a class of low-rate Dos attacks which can evade from be detected by routers or counter-Dos mechanisms easily. After experiments based on different environments and different attack parameters, the author concludes that this kind of attack is a realistic threat to our Internet and, more seriously, is hard to defend while keeping high system performance.

- The attack is mainly based on TCP timeout mechanism, which using RTT and RTO to achieve high performance and robustness in most network conditions. RTO is a variable used to manage packet resend timeout. If error occurs when a packet is sending, the packet will be resent after RTO. And if error occurs again during resending, RTO will double itself to be the next resend timeout. After a packet is sent successfully, RTO will decrease periodically to the original value. RTT is a dynamically measured value which helps to determine an appropriate RTO. Shrew attack attempts to trigger outages in duration approximating with RTOs, which may cause packet resending failed again and again and thus to keep the TCP flow stay in timeout state.

- Shrew attack is hard to detect due to its low rate. To detect such kind of low rate attack, current DoS attack detect mechanisms may suffer from much high false positives. And also, RTO randomization helps a litter since both decrease the lower edge value or increase the higher edge value will degrade TCP performance. But as this paper was published more than 10 years ago, I believe there must be some excellent ideas in recent researches to detect such kind of DoS attack with much lower cost.

Paper Discussion

- Hitakshi Annayya
-
- **Low-Rate TCP-Targeted Denial of Service Attacks**

- The paper "Low-Rate TCP-Targeted Denial of Service Attacks" investigates the low-rate denial of service attack also called as **"shrew attacks"**, which consume resources in networks, server clusters, or end hosts, with the malicious objective of preventing or severely degrading service to legitimate users. The DOS attacks are difficult for routers and counter-DoS mechanisms to detect. DOS attacks typically consumes the resources such as network bandwidth, server or router CPU cycles, server interrupt processing capacity, and specific protocol data structures.

- Ex: DoS attacks include TCP SYN attacks that consume protocol data structures on the server operating system.

- The paper discusses by using a combination of analytical modeling, simulations, and Internet experiments, show that maliciously chosen low-rate DoS traffic patterns attempt to deny bandwidth to TCP flows while sending at low average rate to escape detection by counterDoS mechanisms.

- The experiments conducted through counter-DOS techniques such as Router-assisted detection and throttling and end-point based randomization, TCP exhibits null frequencies when multiplexed with a maliciously chosen periodic DoS stream. The experiments concludes low-rate DoS attacks are successful against both short- and long-lived TCP aggregates and thus represent a realistic threat to today's Internet and both network-router (RED-PD) and end-point-based mechanisms can only mitigate, but not eliminate the effectiveness of the attack.

Paper Discussion

- Lucas Copi
- CSC 6991

- DOS Attacks

- *Low-rate TCP-Targeted Denial of Service Attacks* discusses using low-rate denial of service attacks to remain undetected by system monitors. The paper details how DOS attacks can utilize TCP timeout mechanisms to force synchronization of TCP flows and force near zero throughput.

- Low-rate DOS attacks (shrew attack) attempt to trigger bottlenecks and outages in conjunction with RTO which increases the timeout period before each packet is resent after each bottleneck. The results from experiments conducted show both the effectiveness of the attacks as well as the plausibility of remote attacks.

- The paper demonstrates the effectiveness of shrew attacks as the well as the capability to avoid detection by transmitting at a small average rate. Although shrew attacks manipulate the RTT and RTO mechanisms of TCP preventing such attacks would have too much cost to be feasible.

Paper Discussion

- Sharani Sankaran
- CSC 6991 Advance Computer System Security

- Low Rate TCP Targeted Denial of Service Attacks

- This paper mainly deals with low rate DoS attacks unlike the high rate attacks which are more difficult counter DoS attacks. It mainly handles shrew attacks that mainly deny bandwidth to TCP flows. It mainly works on the principle of TCP's timeout mechanism. a class of randomization techniques in which flows randomly select a value of minRTO such that they have random null frequencies.
- The synchronization has been extensively explored the avoidance synchronization many TCP flows of the windows at the same time. Even the mechanisms like RED are unable to prevent DoS-initiated synchronization.
- There is an underlying vulnerability due to tradeoff induced by mismatch of defense and attack timescales

Reminders

- Term project proposal is due a week from today (Extended to Oct 5th)

- Paper Reviews