A Rate-Limiting System to Mitigate Denial of Service Attacks
Overall information

Intents and scope

The Rate-Limiting System

Tests and results

Analysis

Areas of application, future research
DoS Attacks

- Attackers aim to disrupt the normal operation of their targets' services. Flooding attacks aim to exhaust resources on the target. Logic attacks rely on intelligent exploitations of software bugs.

- Attacks are distributed (DDoS) when they are carried out using a (large) set of compromised hosts.

- Flooding DoS attacks resemble legitimate traffic, their patterns vary a lot and change quickly (attackers use random addresses and port numbers).
Means of Defense

- Applying security patches.
- Manual and long investigation process involving everyone on the attack path.
- ID Ses, blocking
- CITRA [1], ACC [2]

No complete solution!
Intents

- Automated, early-warning defense mechanism that mitigates DoS attacks. [3, 4]
- Using rate-limiting instead of blocking
- Using IDSes and QoS capabilities

Question:
Is rate-limiting a viable defense mechanism?
Scope

- Traffic is packet-loss tolerant.
- The attack bandwidth is low.
- The probability of attack is low.
- The attack is non-destructive.
- False-positives are too frequent to use blocking.
Building blocks of the Rate-Limiting System

- RLS messages:
  - Rate-Limit
  - Cancel

- Build/delete attack queues
- Build/delete filters

Defended network

QoS capable router
**Effects of the RLS on traffic**

Discarded Packets

- **Incoming traffic:** Legitimate + attack traffic
- **Defended network:** QoS capable router

**Outgoing traffic:** no packet discard
**QoS operations**

- **QoS support**: The RLS-AQM enforces rate-limiting by randomly discarding packets.

- **Flow identification**: The scheduler processes packets by identifying legitimate traffic queues.

- **Attack queues**: RLS-AQM enforces rate-limiting by randomly discarding packets.

- **Legitimate traffic queues**: AQM processes legitimate traffic.

- **Discarded packets**: Packets marked as attack are discarded.

- **No packet discard**: Packets that are not marked as attack are forwarded.
Dropping probability function of the RLS-AQM

Packet discard probability

\[ R + P(1-R) \] when average queue size < first threshold

\[ R + p(1-R) \] when first threshold < average queue size < second threshold \( P = \max(p) \)

1 when second threshold < average queue size
Dropping probability function of the RLS-AQM

Packet discard probability

$R + P(1 - R)$

Average queue size

$R$ when average queue size $<$ first threshold

The queue does not get full:

- The RLS is intended to work with low-bandwidth attacks.
Main tests

- Validating the RLS-AQM behavior
- FTP-uploading / downloading with rate-limiting
- Web-browsing with rate-limiting
Layout of the test network and the RLS implementation
Experienced packet loss ratios using the RLS-AQM compared to configured values
FTP-upload rates for different packet discard probability values.
FTP-downloading rates for different packet discard probability values.
Analysis

➲ Uploading: data packets are discarded. Every lost data packet has to be retransmitted.

➲ Downloading: ACKs are discarded. A lost ACK does not necessary need to be retransmitted: following ACKs can recover the information.

➲ The theoretical model only takes into account the loss of data packets. [5]
Areas of application

➲ Test HTTP: handle up to 55% packet discard
Test FTP-downloading: up to 40% packet discard

➲ HTTP and FTP-downloading are the two most common services offered by websites.

➲ Flooding DoS attacks (i.e. TCP SYN flooding, ICMP Echo Request flooding) are the most common DoS attacks and very often aim well-known websites (e.g. Yahoo!, eBay, Amazon, CNN... shut down by the same attack in February 2000).
Future Research

- Designing a complete system

- More exhaustive and precise tests, including more realistic network conditions

- Managing several attack and legitimate queues according to the characteristics of traffic flows

- Finding the right communication protocols between components
Kysymyksiä?

Questions?
Congratulations

➲ Read aloud:
  ● "Bravo"
  ● "Viva"
  ● "Bis"

➲ Applause, make a stand-up ovation

➲ You can throw:
  ● Roses
  ● Hats
  ● Wallets
References


