How to protect from DoS in internet enviroment?

Petri Suvila

Detect and limit DoS Attacks

A Collection of procedures to prevent DoS attacks:

- **Monitor for attacks**
- **Limit the rate to or from one host**
- **Limit ICMP floods**
- **Limit concurrent flows of one type**
- **Detect pseudo-address attacks**
- **Detect portscan attacks**
- **Disrupt virus attacks**

Monitor for Attacks

The following techniques are different ways to check whether a denial-of-service attack has occurred:

- **Monitor Class Hits**
  - Class hits let you know the number of times flows match a class. By monitoring class hits regularly, you'll know what constitutes a normal number of hits in a class and an abnormally high number of hits will be apparent.

Spot a huge increase on an ignored traffic class.

Monitor for Attacks

- **Monitor TCP connections**
  - Track the number of new TCP connections and which the server never responded

Establish baselines for TCP connections in a normal, non-attack setting.

Use automatic warning abnormal situations

Monitor for Attacks

The following measures are more proactive ways to detect and limit DoS attacks:

- **Look for Unwelcome Hosts**
  - Potential attacks is to look for abnormal hosts
- **Look Flood Attacks**
  - It appers a large number of illegitimate connections, consuming bandwidth and overwhelming hosts

Decrease DoS attack impact

- **Limit the rate of new traffic to or from one host**
  - Set limit on the number of flows per minute that can be initiated by any client or received by any server.
- **Limit the amount of ICMP and UDP traffic**
  - Many DoS attacks use the ICMP or UDP protocol
  - Normally ICMP traffic uses a only tiny portion of bandwidth

Decrease DoS attack impact

- **Detect Pseudo-Address Attacks**
  - Monitor class hits to notify if anyone has tried to send traffic with an incorrectly trusted source.
- **Prevent spoofing and LAND attacks by filtering**
- **Detect Portscan Attacks**
  - IDS would alert before DoS attacks occur and would isolate impact of attacks
- **Disrupt Virus Attacks**
  - Ristrict and track well-known virus traffic flows

How Company works at DoS?

- Identifies DoS traffic flow
  - Resolve destination of DoS (IP, port, traffic type)
  - Source addresses are usually spoofed
- Block DoS at firewall or router
- Isolate other critical systems
- Try to route other traffic flows different backup connection (E-mail)
- Call ISP and give detailed description of attack

How ISP works at DoS?

- Identifies traffic flow
- Blocks traffic at router by hop by hop
- If DoS attacks comes another AS
  - Inform exchange place and other AS operator
  - Revent customer IP addresses publicity to world