Network-Based Denial of Service Attacks

Trends, Descriptions, and How to Protect Your Network

Craig A. Huegen <chuegen@cisco.com>

Cisco Systems, Inc.

NANOG 13 -- Dearborn, MI -- June 9, 1998

Cisco Systems

980609_dos.ppt

Trends

- **Significant increase in network-based Denial-of-Service attacks over the last year**
  - Attackers’ growing accessibility to networks
  - Growing number of organizations connected to networks
- **Vulnerability**
  - Most networks have not implemented spoof prevention filters
  - Very little protection currently implemented against attacks

Profiles of Participants

- **Tools of the Trade**
  - Anonymity
  - Internet Relay Chat
  - Cracked super-user account on enterprise network
  - Super-user account on university residence hall network
  - “Throw-away” PPP dial-up accounts
- **Typical Victims**
  - IRC Users, Operators, and Servers
  - Providers who eliminate troublesome users’ accounts

Goals of Attacks

- **Prevent another user from using network connection**

  "Smurf" and "Fraggle" attacks, "pepsi" (UDP floods), ping floods

- **Disable a host or service**

  "Land", "Teardrop", "NewTear", "Bonk", "Boink", SYN flooding, "Ping of death"

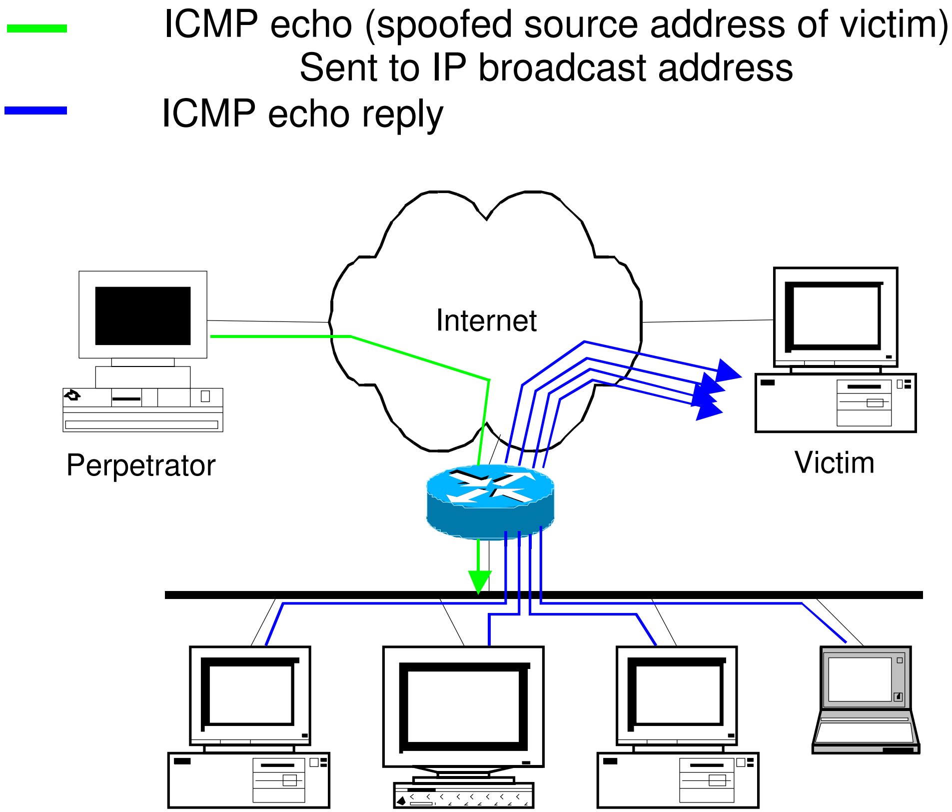
- **Traffic monitoring**

  Sniffing

“Smurf” and “Fraggle”

- **Very dangerous attacks**
  - **Network-based, fills access pipes**
  - **Uses ICMP echo/reply (smurf) or UDP echo (fraggle) packets with broadcast networks to multiply traffic**
  - **Requires the ability to send spoofed packets**
- **Abuses “bounce-sites” to attack victims**
  - **Traffic multiplied by a factor of 50 to 200**
  - **Low-bandwidth source can kill high-bandwidth connections**
- **Similar traffic content to ping, UDP flooding but more dangerous due to traffic multiplication**

“Smurf” (cont’d)


ICMP echo (spoofed source address of victim)
Sent to IP broadcast address
ICMP echo reply
Internet
Perpetrator
Victim

Prevention Techniques

- **How to prevent your network from being the source of the attack:**
  - **Apply filters to each customer network**
  - **Apply filters to your upstreams**
- **This removes the possibility of your network being used as an attack source for many attacks which rely on anonymity (source spoof)**

Prevention Techniques (cont'd)

- **How to prevent being a "bounce site" in a "Smurf" or "Fraggle" attack:**
  - **Turn off directed broadcasts to networks:**
    - Cisco: Interface command "no ip directed-broadcast"
      - As of 12.0, this is default (CSCdj31162)
    - Proteon: IP protocol configuration "disable directed-broadcast"
    - Bay Networks: Set a false static ARP address for bcast address
    - 3Com: SETDefault -IP CONTrol = NoFwdSubnetBcast
  - **Use access control lists (if necessary) to prevent ICMP echo requests from entering your network**
  - **Configure host machines to not reply to broadcast ICMP echos**

Prevention Techniques (cont'd)

- **Unicast RPF checking & CEF**
- **Inter-provider Cooperation**

  Network Operations Centers should publish proper procedures for getting filters put in place and tracing started

  IOPS working group

References

- **Detailed "Smurf" and "Fraggle" information**

  http://www.quadrunner.com/~chuegen/smurf/

- **Ingress filtering**

  RFC 2276

- **Other DoS attacks**

  See expanded presentation at http://www.quadrunner.com/~chuegen/smurf/980513_dos

Author

Craig Huegen

<chuegen@cisco.com>

Questions?