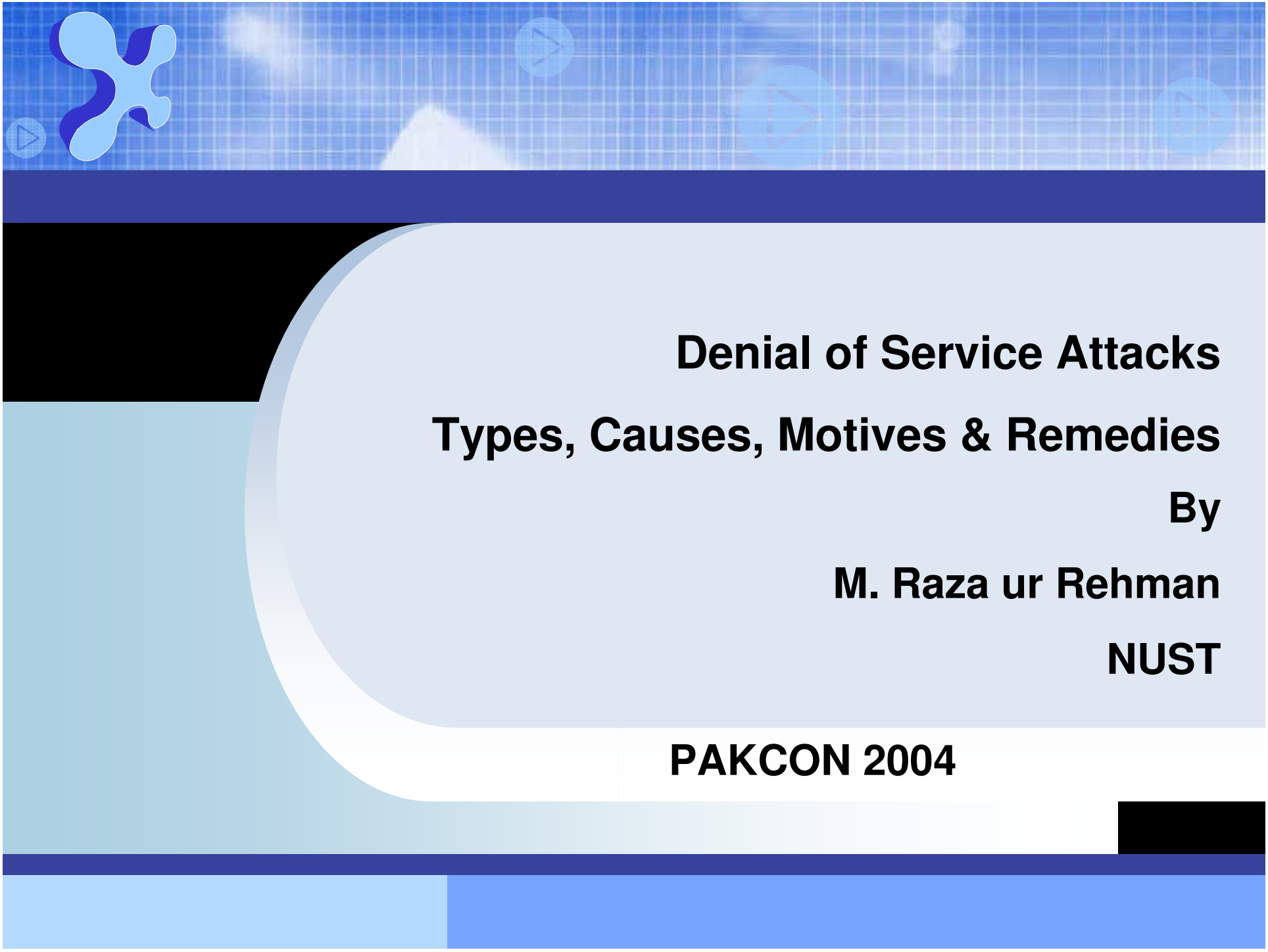
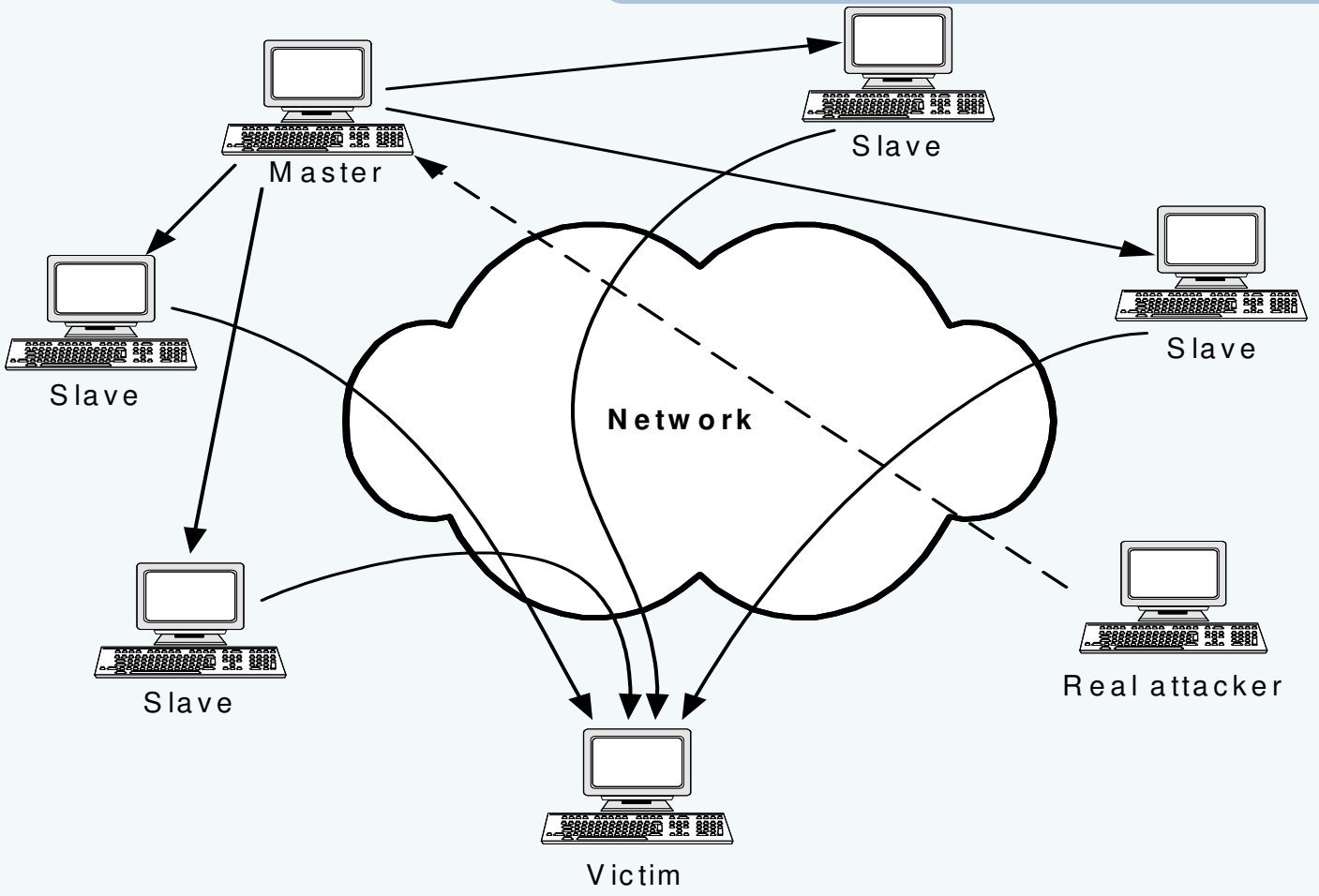

Denial of Service Attacks
Types, Causes, Motives & Remedies
By
M. Raza ur Rehman
NUST
PAKCON 2004

Denial of Service Attacks

- Attempts to prevent or disturb legitimate access to co mputer resources
- Resources like bandwidth, services etc.
- The most common way:Network Flooding
- Alter the Configurations so that configurations have to be fetched again and again

Distributed DoS Attacks



Common DoS Attacks

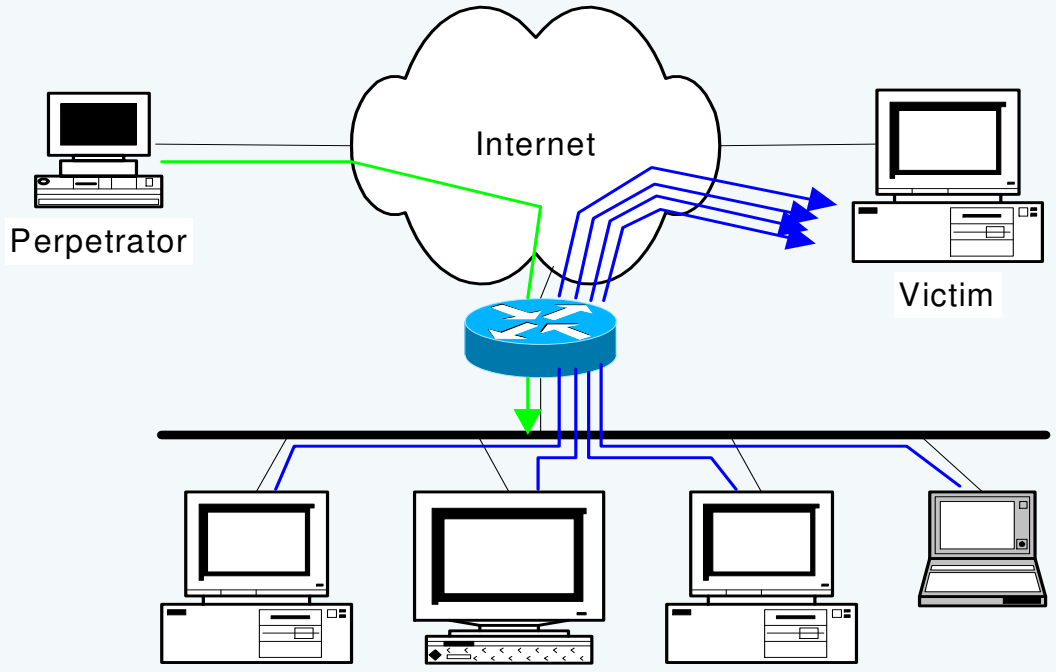
- Smurf Ping of Death Attack
- SYN Flooding
- UDP Flooding (Fraggle)

Etc…

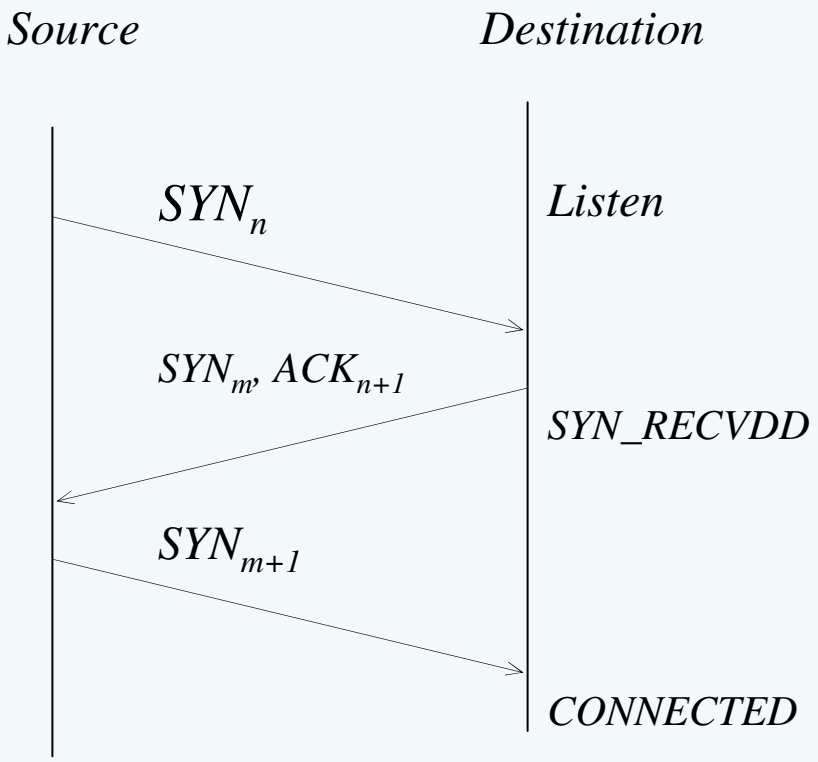
Smurf (Ping of Death Attack)

ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

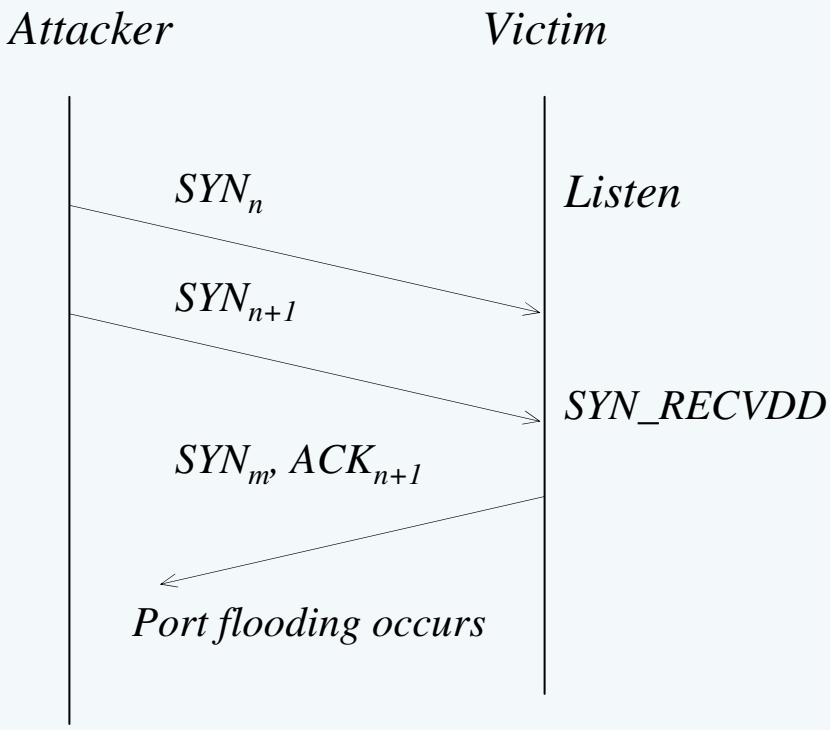
ICMP echo reply



SYN Flooding



Normal TCP Connection Establishment



SYN Flooding

UDP Flooding (Fraggle)

- Similar to SMURF Attacks
- UDP Echo Request expects UDP Reply messages

Causes of DoS Attacks

- Flaws in the core Internet Protocols.
- Lack of Security Concerns amongst masses
- Distributed nature of Attacks
- Nature of Internet

Motives

Political Reasons

- India Pakistan Cyber Warfare (YAHA Worm) 2002

http://www.vnunet.com/News/1133119

- Attacks on Brazil Government sites 2000

http://www.computeruser.com/newstoday/00/03/18/news1.html

- DDoS Attacks on Aljazeera 2003

http://www.infoworld.com/article/03/03/26/HNjazeera_1.html

- SCO Website down by DDoS

http://www.infoworld.com/article/03/08/25/HNscoweb_1.html

Motives

Economic Reasons

- British Telecom (2000)

  "This is my payback to BT for ripping this country off."
  http://www.theregister.co.uk/content/1/12097.html

  CNN, Yahoo, E-Bay Down by Ddos Attacks

  (2000)

- Cloud Nine (A British ISP)doomed by Dos Attacks (2002)

  http://www.wired.com/news/business/0,1367,50171,00.html

- Attack on Microsoft.com (2003)

  http://www.informationweek.com/story/showArticle.jhtml?articleID=12808118

Motives

Other Reasons

- Attack on Gibson Research—Revenge by Script Kiddies (2002)
- DoS Attacks on DALNet IRC Servers..

Other Developments

- **DDoS Vulnerabilities in IPv6 protocols**
  http://www.packetstormsecurity.org/

Detection and Prevention

Difficulties Associated

- Harder to Detect
- Easier to Commit and easier to perpetrate
- Difficult to Isolate from Normal Traffic
- Difficult to track the origins

Prevention Techniques

Some general measures

- Software patches
- Secure host computer from hacking, trojan horse, virus, back door, …
- Configure router to deny spoofed source address
- Reduce time-out of half-open connections
- Increase resources for half-open connections (backlog)
- Close unused TCP/UDP port
- Firewall

Prevention Techniques

SYN Cache

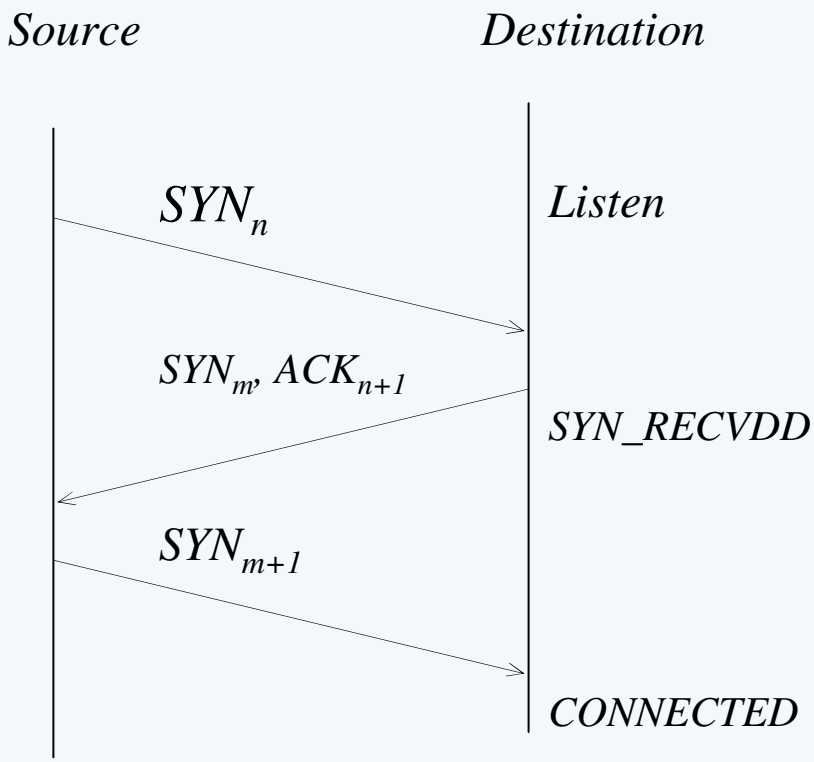
- Replaces the per-socket linear chain of incomplete queued connections with a global hash table.
- Hash Table provides two forms of protection against choking up of server resources
- Total no of entries in the hash table provides an upper bound on the memory Syn Cache can take
- The latter limit bounds the amount of time that the machine needs to spend searching for a matching entry, as well as limiting replacement of the cache entries to a subset of the entire cache

Prevention Techniques

SYN Cookies

- **Does not allocate Resources on SYN Request**
- **Send back its initial sequence no (m)as a function of client properties**
- **Client has to send back**

  Sequence no as (m+1)



Conclusions

- Present State of Affairs in the Control of DoS Attacks.
- Network Bandwidth congestion still unavoidable problem

Q & A