# Firewalls and Intrusion Detection Systems: Part 7

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

# References


- J. Kurose, K. Ross, "*Computer Networking: A Top Down Approach*", Sixth Edition, Pearson Education, 2012
- B.L. Menezes, R. Kumar, "*Cryptography, Network Security, and Cyber Laws*", Cengage Learning India Pvt. Ltd., 2018
- C. Kaufman, R. Perlman, M. Speciner, "*Network Security: Private Communication in a Public World*", Pearson Education, 2nd edition, 2002

# DDoS Attack Prevention and Detection

# Preventive Measures at Host

- Recall: SYN flood attack:
  - ❑ attacker(s) send a large number of TCP SYN packets, without completing the third step of the TCP three-way handshake
  - ❑ with this deluge of SYN packets, the server's connection resources become exhausted as they are allocated (but never used) for half-open connections; legitimate clients are then denied service
- One way host can defend against them:
  - ❑ host drops incoming request for TCP connection if it suspects that it is being sent by an attacker
- Host classifies source IP addresses into:
  - ❑ "almost certainly genuine", "probably spoofed", etc.
- "Almost certainly genuine" addresses are those with whom normal connections were established and terminated in the past
- Under moderate load conditions, all incoming SYN requests are served
- However, under rapidly increasing load, SYN requests with unfamiliar source addresses are discarded with high probability
- Shortcoming of above strategy:
  - ❑ SYN requests from some legitimate clients who are connecting for the first time may be dropped

# Preventive Measures at Host (contd.)

- Another defence strategy:
  - Receiver of SYN packet allocates buffers for the TCP connection request only upon completion of the three-way handshake
  - While the connection is still half-open, minimal information about it is stored in a data structure called the *SYN cache*
    - this information includes the TCP sequence numbers and source/ destination addresses and port numbers
  - This strategy reduces amount of storage required for each half-open connection
- Shortcoming:
  - A small amount of information still needs to be stored for each half-open connection, which occupies space at server
- A better solution is to use SYN cookies (discussed earlier), under which no information whatsoever needs to be stored for a half-open connection at server

# Preventive Measures Inside Network

- Above schemes help prevent memory exhaustion at the victim's machine
- However, they do not help reduce incoming attack traffic, which may cause victim's network link to saturate
- Next, we investigate approaches that seek to throttle attack traffic near source or in core of network
  - ❑ well before it enters victim's network

# Egress Filtering

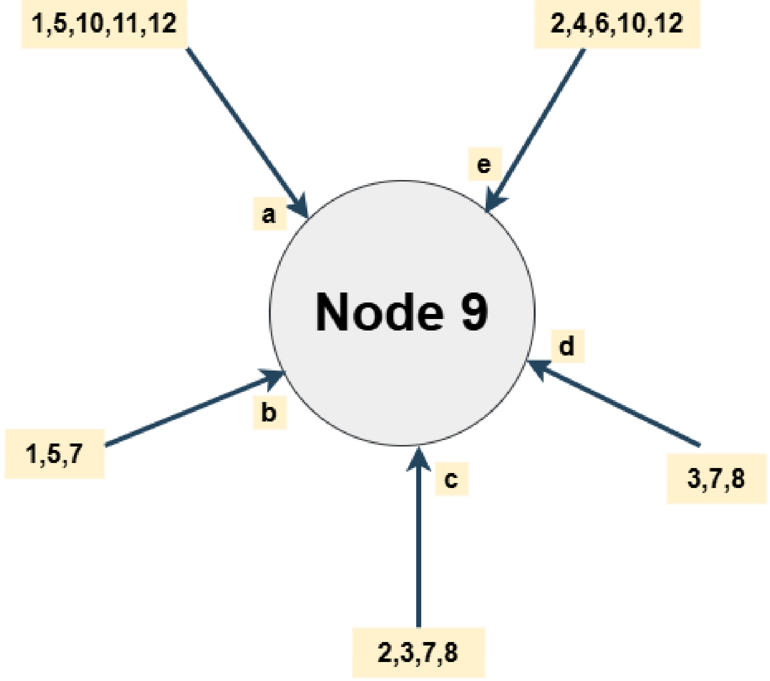
- Recall: most DDoS attack packets use spoofed source IP addresses
  - used to make it difficult for intrusion detection systems to pinpoint the true source of the attack and block it
- Egress router is the last router encountered by any packet generated inside the network before it exits that network and enters the Internet
- Let $\mathcal{A}$ be the set of all externally visible IP addresses within the network (behind the egress router)
- The egress router examines the source address of each packet leaving it
  - If the address does not match any address in $\mathcal{A}$, it drops the packet
- By thus detecting and filtering spoofed packets, it helps prevent DDoS attacks
  - Note: not all spoofed packets will be detected
- Shortcoming:
  - unlikely to be universally deployed
  - there is not always sufficient motivation for an ISP to implement egress filtering since it sees no incentive in forestalling a DDoS attack on someone else's server
- The idea of egress filtering has been extended to routers in the core of the Internet
  - called *Distributed Route Filtering (DRF)*

# Distributed Route Filtering

- Call a core router that performs filtering of spoofed packets a "filter"
- Filter uses a packet's source address to make a decision on whether or not to discard the packet
- To implement DRF, a filter maintains, for each of its interfaces:
  - ❑ the set of all source addresses from which packets arrive en route to some destination
- The filter uses Border Gateway Protocol (BGP) routing information to obtain the latest mapping between each of its interfaces and the subset of source addresses using that interface
- Filtering decision:
  - ❑ if a packet with source IP address $S$ arrives via an interface that it should not have, the packet is assumed to be spoofed and is hence discarded

# Example

- Fig. shows an example of a filter implementing DRF
- Each interface marked with the source addresses that use that interface en route to some destination
- Note that packets from the same source may enter the router through different interfaces
  - ❑ e.g., packets from source address 7 may arrive through interfaces b, c, or d
- Reason:
  - ❑ multiple shortest paths may exist between a given source-destination pair
- Router checks whether a packet has arrived on one of its acceptable interfaces based on the packet's source IP address
- E.g.:
  - ❑ a packet bearing source address 7 arriving on interface c would be forwarded
  - ❑ however, another packet with same source address but arriving on interface e would be discarded




1,2,3.....etc. represent source IP addresses.
a,b,c,d,e are network interfaces.

Interface d sees packets from nodes 3,7, and 8.
Interface e is the only interface that sees packets from node 4.
Interfaces c and d see packets from node 3.

# Shortcomings of Distributed Route Filtering

- Research studies have found that if about 18 % of the core routers in the Internet implement DRF, then excellent coverage against DDoS attacks is obtained
- However, since Internet is made up of thousands of core routers:
  - ❑ number of core routers that need to implement DRF is still a high number in an absolute sense
  - ❑ so it is expensive to implement DRF
- Also, the efficacy of DRF depends on how fast BGP route updates are disseminated:
  - ❑ routing information changes in response to failed nodes or congested links
  - ❑ this information, in turn, decides whether an incoming packet at a router should be filtered out or not
  - ❑ a wrong decision could discard legitimate packets in addition to spoofed ones