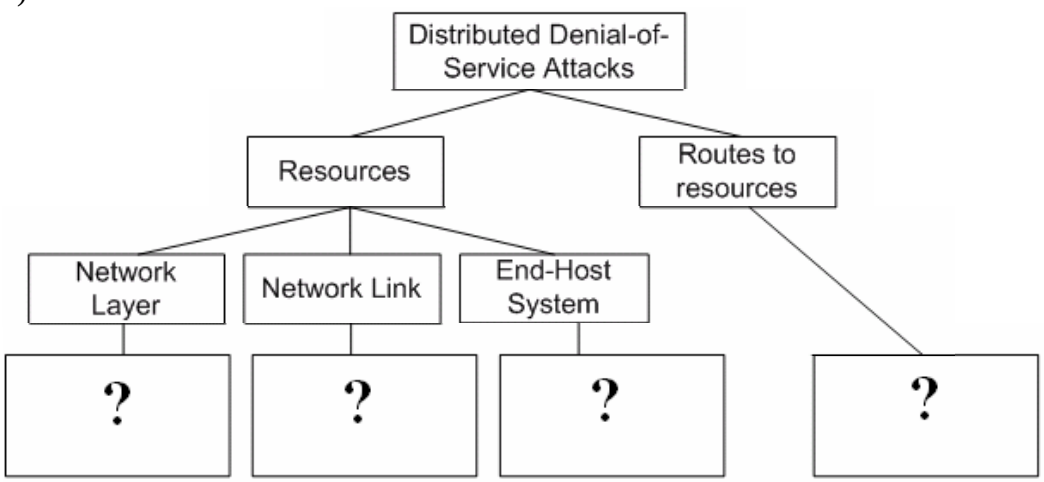
Distributed Systems

Tutorial 4

Lecturer: Vrizlynn Thing

1)



Briefly describe the following attacks. Which category do the following attacks belong to?

- TCP SYN flood
- Programming flaws
- UDP flood
- Worms
- BGP attack
- ICMP flood
- Email spamming
- DNS attack

2) What are the 3 main categories of mitigation techniques? Give an example for each category and briefly describe them.

3)

- R1 = 145.159.6.20, Hashed R1 = 168.23.5.67
- R2 = 136.179.4.50, Hashed R2 = 89.76.55.61
- R3 = 211.126.2.59, Hashed R3 = 136.41.5.89
- R6 = 176.12.33.84, Hashed R6 = 129.13.67.99

Assuming the hash function gives the above hashed values for the routers' IP addresses. Show:

a) the 64-bit "Bit-Interleave" values for all the routers,
b) the contents of the IP identification field for the first fragment of the "Bit-Interleave" marked by each router, and
c) how the partial IP addresses of the routers are computed at the victim's end.

Distributed Systems

Solutions (Tutorial 4)

Lecturer: Vrizlynn Thing

1) Network layer - TCP SYN flood
Network link - UDP flood, ICMP flood, Email spamming
End-host system - Programming flaws, Worms
Routes to resources - BGP attack, DNS attack

2) Prevention - guard and protect against attacks from having any effect on the target network and resources, e.g. egress filtering, ingress filtering, SYN cookies
Detection - provides monitoring and analysis to discover occurrence of on-going attacks and trigger alarm e.g. D-WARD, MULTOPS
Responses - take actions after detection of attacks to alleviate damaging effects caused and identify attackers to institute accountability, e.g. traceback, client puzzles

3)

- R1:
  - Odd – 10010001.10011111.00000110.00010100
  - Even – 10101000.00010111.00000101.01000011
  - Bit-interleave – 1100011001000010.1000001110111111.000000000111001.0001001000100101
- R2:
  - Odd – 10001000.10110011.00000100.00110010
  - Even – 01011001.01001100.00110111.00111101
  - Bit-interleave – 1001000111000001.1001101001011010.000001010 0110101.0000111101011001
- R3:
  - Odd – 11010011.01111110.00000010.00111011
  - Even – 10001000.00101001.00000101.01011001
  - Bit-interleave – 1110001001001010.0010111011101001.000000000011001.0001101111001011
- R6:
  - Odd – 10110000.00001100.00100001.01010100
  - Even – 10000001.00001101.01000011.01100011
  - Bit-interleave – 1100101000000001.0000000011110001.000110000 0000111.0011011000100101

- For first fragment, victim receives:
  - 000.00011.00101000 marked by R6
  - 000.00010.01110011 marked by R3
  - 000.00001.01010111 marked by R2
  - 000.00000.11000110 marked by R1
- Based on distance, R1 is the next hop router to victim
- Working upwards, first fragment bit-interleave address of R1 is 11000110, R2 is (01010111 xor 11000110) 10010001, R3 is (10010001 xor 01110011) 11100010, R6 is (11100010 xor 00101000) 11001010
- Extract the odd bits and perform hash and if they match the even bits, 4 bits of the address of the router is obtained. *(Similar steps for the rest of the fragments!)*