Computer Networks – Fall 2020

Momina Atif Dar || P18-0030 || Section: B

Report on ICMP Protocol and Mobile IP

ICMP:

Internet Control Message Protocol (ICMP) is a transport layer protocol which is used in support of IP to generate error messages when there's a network issue and IP packets are not getting through. If gives information for transmission failure for both TCP and UDP. It can work with IPv4 as well as IPv6. An ICMP packet is generated when the incoming data packet's IP header has some issues in it. ICMP's header has three things; the category of error, a sub-code field – which has description of error – and checksum. Some of ICMP message codes are 0 (echo reply), 3 (destination unreachable), 4 (source quench), 5 (redirect), 8 (echo request), 9 (router advertisement reply), 10 (router solicitation) and 11 (time exceeded). PING command uses ICMP. When PING sends a data packet, packet contains ICMP code of *echo request* and when it's receiving the packet contains ICMP code *echo reply.*

ICMP is vulnerable to many attacks like Smurf Attack, Ping flood Attack, Ping of death Attack, Twinge Attack. In Smurf attacks, attacker provokes other systems to send messages to target system. It sends a ping request on broadcast IP of network used by target user. All the systems connected to that network receive *echo request* and in response they send back *echo reply* – causes flooding. In Ping Flood Attack, the option of 'flood' in ping is exploited although this option is not available to everybody so this minimizes the risk of it. In Ping of Death Attack, the attacker sends a very lengthy ping request packet which is then broken down into fragments and fragments are sent to the target. The target will assemble the packets but if the length is greater than the available memory then the target computer will be jammed. In Twinge Attack, it's the same as Ping Flood Attack with 'flood' option implemented. It overwhelms the target system. There are some ways which can protect target systems from ICMP attacks; turn off ICMP, install a web application firewall or install an intrusion detection system, limiting the allowed size of ping requests.

Mobile IP:

Mobile IP is a protocol that is used for allowing mobile devices to move from one network to another while maintaining their IP address. It is to ensure that user's connections and sessions will not drop with the change of IP address. Mobile IP has some functional entities; Mobile Node (host/router that changes its point of attachment from one network to another), Home Agent (router that intercepts datagrams which are for mobile node – maintains current location information for mobile node), Foreign Agent (router that provides routing services to mobile node while MN is registered), Correspondent Node (device on internet that communicates with MN) and Care of Address (temporary address that is assigned to MN while it is moving away from home network).

Mobile node receives data packets from correspondent node and those packets have information regarding source (correspondent node's address) and destination (home address) but since mobile node is roaming so foreign agent sends care-of-address to home agent. Now home agent sends all the incoming data packets to foreign agent which in turn sends these data packets to mobile node. This establishes a tunnel between home agent and foreign agent. Tunneling provides a virtual tunnel between foreign and home agents for communication. The main function of tunneling is encapsulation and decapsulation. Home agent now encapsulates data packets which has information about source (home address) and destination (care-of-address) and sends it via tunnel. Foreign agent decapsulates the data packets and sends them to mobile node. Mobile node after receiving data packet sends an acknowledgement to foreign agent who in turn sends it to correspondent node.
