Pawel Derkacz
151005994
Security Engineering
Assignment 3

Sequence is as follows,

- <Flaw>
  - <Potential Attack>
    - <Defense>

- TCP Packet Number Prediction → The sequence number for a given packet can be predicted if the issuer of the packet is not using a sophisticated enough manner to create the sequence number for said packet. This allows intruders to interject themselves into the stream.
  - For example, if an intruder can predict the packet sequence number being sent from a server, he can send a packet with a predicted sequence number in order to attempt to create a connection with that server via a spoofed IP address of a trusted machine (TCP sequence number attack).
    - Thus, to defend against such an attack, the sequence number should be encrypted using standard cryptographic algorithms (such as Rijndael, the Advanced Encryption Standard), causing the number to be not as predictable. A sufficient enough algorithm would be one that forces the intruder to spend an unreasonable amount of time trying to predict the next sequence number, when compared to the possible information the intruder could obtain by actually making a successful connection. As an additional defense, monitor any unusual traffic that would indicate an intruder attempting to find the round-trip time from himself to the server.
- Packet Routing → Say a server is set up in such a way that it uses the reverse of the source packet's route, in order to ensure a definite connection. An intruder could purposefully form a route that allows for easy infiltration (Source Routing attack). Tied with that, the Routing Information Protocol (RIP) can be used by an intruder in order to form a route that has the intruder's machine as a node (RIP attack).
  - For example, if an intruder spoofs himself as a trusted machine and sends a packet to the server along a certain chain. Likely, the chain is selected in such a way that the intruder could quickly read any information from outgoing packets, and send a response before the trusted machine can. In this way, the intruder can use the same facilities normally provided to the trusted machine. For the RIP case, the only difference is that traffic would go to the intruder directly, instead of the intruder having to sniff for packets (and thus allowing for passive data collection, instead of using the possible facilities at hand).
    - To defend against such attacks, analyze the source route and only accept the packet if trusted nodes were used. Specifically for RIP attacks, if there is no good reason to take a new route to the target, then do not do so. Nowadays, source routing is disabled by default on most machines, and RIP is deprecated.
- Abusing ICMP → If ICMP messages are not validated to a high degree, then there is a possibility that an intruder could spoof as a trusted machine and send these messages to a victim.

  - For example, the intruder (after spoofing) could send a “Redirect” message, in order to have any further packets go through a different, and likely compromised, gateway, instead of the primary one. Other ICMP messages could force the target to drop connections, and thus result in a denial of service (i.e. using “Destination Unreachable” or “Time to Live Exceeded”).
    - As a defense against forged ICMP messages, the host should first check if the message is actually correlated to an existing connection (and if the sequence number matches). Then, in the case of redirection messages, the route change should not be permanent (i.e. global routing table is untouched) and routing on the connection should be restricted, following the defensive measures outlined for “Packet Routing”. If possible, create firewall rules against ICMP messages, allowing only for certain ICMP to be sent, and of those, they could be one sided.
- “Authentication” Servers → Not all clients would have a host authenticating server, thus the packets from these clients could never be trusted. Additionally, if a client does have a host authenticating server, that server could be down (due to maintenance or the like), allowing intruders to act as the server, or intruders could put up a false authenticating server.
  - If an intruder puts up a false authenticating server, he can perform a DoS attack by telling the requesting servers that the connection is not part of its network (and thus not allowing the target to connect to servers). If an authenticating server is taken down, then an infiltrator could spoof as a machine that is part of that server’s network, and complete the TCP handshake between the target server and the authenticating server by use of TCP sequence prediction, and thus have access to the facilities the spoofed machine would normally have.
    - The defensive measure described by the paper is simply to not use TCP solely, and use a more secure means of validation, such as the Needham-Schroeder Protocol. The N-S Protocol uses public key cryptography, where a third party is needed (a server that holds public keys), in order to secure the connection via nonces and encryption.
- LAN Vulnerabilities → If physical access is allowed to the network, a new machine could be introduced. Additionally, if machines on the local network are trusted upon entry, then any new machine connected could communicate with other machines on the network.
  - If an intruder acquires physical access to the network, he can set up his own machine in order to connect to the network. Lacking that, if an intruder obtains access to a machine already connected to the network, he start communicating with other machines on the network, or potentially eavesdrop on them. Finally, the intruder could issue requests that send the network into chaos, if the right conditions exist (such as having all/most hosts act as gateways, and then sending a packet with an invalid destination – causing a broadcast storm).
    - To defend against such intrusions, restrict access to the physical network. Additionally, have the default protocol for new machines on the network to be untrusted, and thus unable to disrupt the network. Authentication servers can be used in addition to the last statement (should an intruder attempt to get access from outside the network). GFI Software group (www.gfi.com) advertise products that may help further secure the LAN, such as being able to find vulnerable machines on the network, traffic monitoring, and more.