05/11/2020 CS-767 Foundedations Network Security

Chakradhar Reddy Donuri

E949F496

Exam-3

1) a) B

b) C

c) A

2) (i) An exhaustive search of the Key space lengths ranging from 40 to 168 bits

(ii) It is prevented by use of nonces

(iii) It is prevented by the use of public Key certificates to authenticate the correspondents

(iv) IP spoofing : The spoofer must be in possession of secret Key as well as the bogus IP address

(v) SYN Flooding : TLS provides no protection against this attack

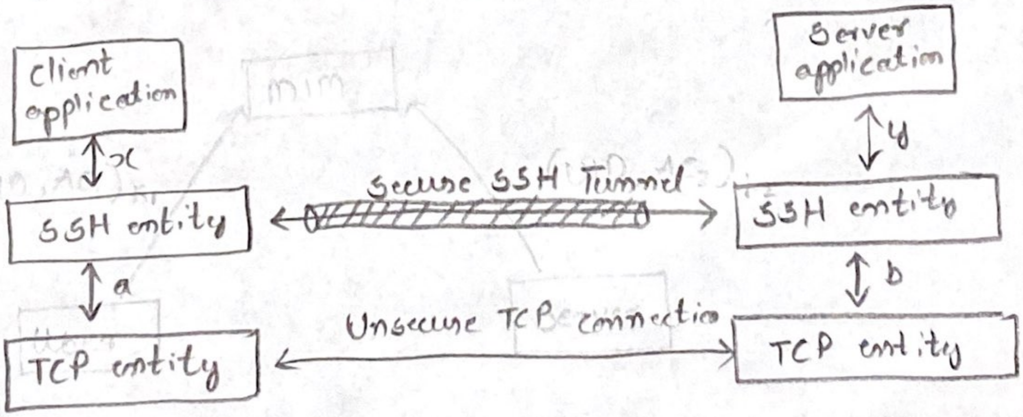
3) a) To protect MIM attacks, we need some kind of shared trust or shared secret between the client and server. The most commonly used methods are a) Some kind of proprietary certificate mechanism (eg open SSH) b) A public key on the client and private key on server (SSH) c) A share secret value (eg IPsec with pre shared Keys). Most SSH clients will trust the servers key during the 1st connectio and at any given time MIM attack are unlikely and it provides the best possible trade off b/w usability and security.

Use of HTTPS can prevent message eavesdropping in TLS protocol.

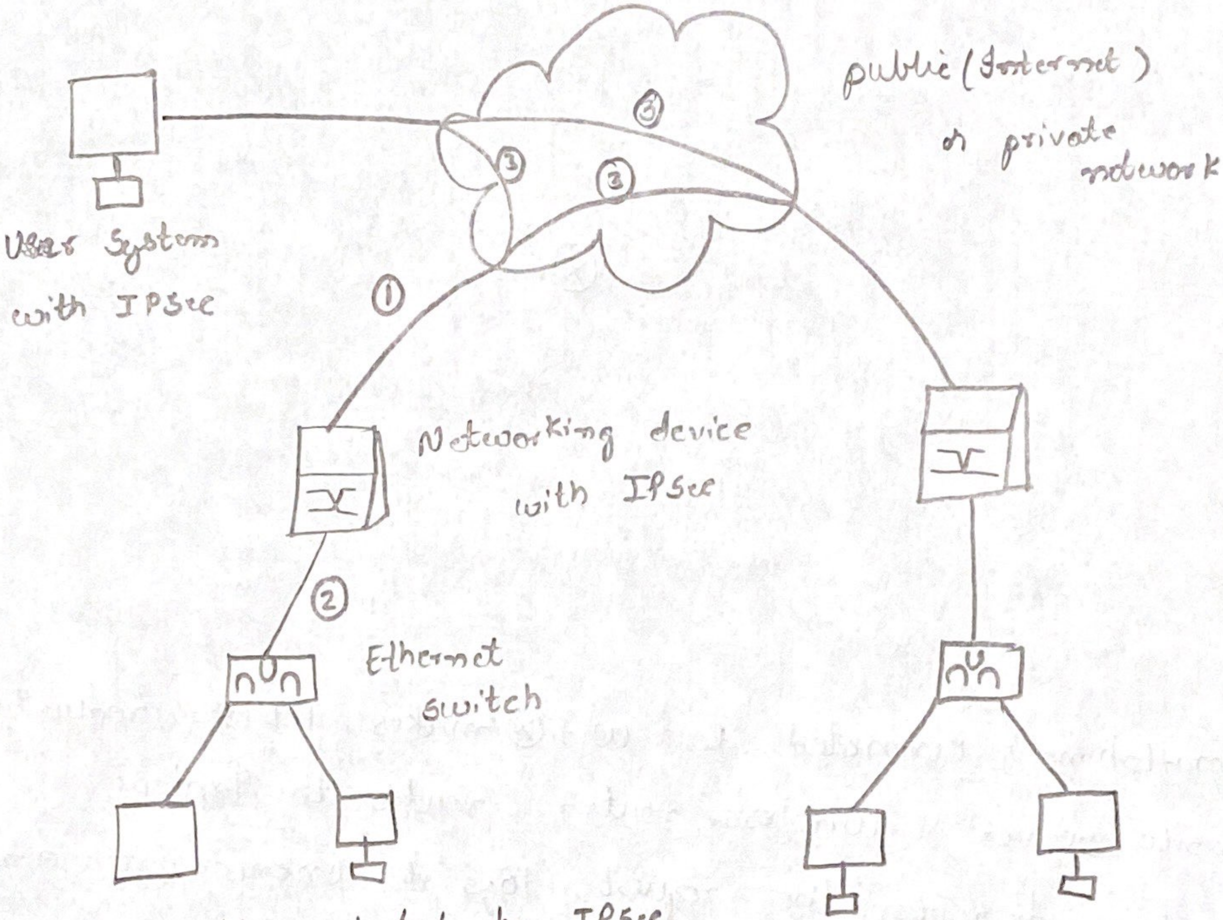
The certificate authority system is designed to stop the MIM attacks. In TLS, server uses the private key associated with their certificate to establish a valid connection. The server keeps the key secret, so MIM cant use the sites real certificate. The attacker has to either convince a CA to sign their certificate or just use it, as is.

~~Safeguard~~ against ~~MIM attacks on SSS TLS enabled~~ ~~application~~.

Connection via SSH Tunnel



3) b)



① - IP traffic protected by IPSec

② - Unprotected IP traffic

③ - Virtual tunnel : protected by IPSec.

WuIndustries maintains LAN's at different locations. Non-secure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN. IPSec protocols are used. These protocols operate in networking devices, such as a router or firewall, that connect each LAN to the outside world. The IPSec networking device will typically encrypt all traffic going into the WAN and decrypt traffic coming from the WAN. These operations are transparent to workstations and servers on the LAN. Secure transmission is also possible with individual users who dial into the WAN. Such users workstations must implement the IPsec protocals to provide security

3) c) No, the messages of the application are not at risk of an eavesdropping attack launched through wirelers network by the previous IT manager.