Homework 3

1. Assume root server has Xbank's certificate. Bob would like to securely communicate to Xbank's server. Assume Bob has no trust established beforehand. (20 points)

1) What certificate/certificates does Bob need?

Bob can obtain Root CA public keys to validate Xbank digital certifcate -3

2) Show the names of issuer and owner (to whom this certificate is issued to) of each certificate/certificates

Issuer: Root Server -5

Owner: Xbank

2. Why PGP certificates allows more than one signatures enclosed in one certificate? (10 points)

Assuming that we trust the initial party it's easier to add additional signatures to the certificate in order to impart trust to another party.

-2

3. What is the different of DOS attack and Distributed DOS (DDOS) attack? (10 points)

A DoS attack is a denial-of-service attack where a computer is used to flood a server with TCP and UDP packets. It's easy to defend against DoS by using a firewall to block the computer.

A DDoS attack is where multiple systems such as many botnets and many computers maybe involved to conduct a DoS attack on a system or a network. The targeted network is then bombarded with packets from multiple locations. It's hard to defend against DDoS attacks because its hard to trace the location of the attack. Apart from that
Both aims to deny the network service to the legitimate users.

4. What security property could be achieved after establishing TLS/SSL connection? (10 points)

TLS will provide confidentiality via encryption.
The MAC value protects a message's data integrity, as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

5. If you as the client are using VPN to connect to a host V in a private network (e.g., the BSU campus network). The packet structure generated by client-side VPN is like this (only the IP address parts are shown): (20 points)

Src: 201.188.1.23 | Dst: 231.34.221.231 | Src: 192.168.0.31 | Dst: 10.31.331.59

1) For an intermediate router that transfers this packet in the middle of tunneling route, which source IP address and destination IP address are exposed?
Src: 201.188.1.23 and Dst: 231.34.221.231 are exposed.

2) For the host V inside the private network, what is the source IP address of the received packet?

Src: 192.168.0.31