Assignment - 2

Computer Security - 1

**1) What is the purpose of the X.509 standard?**

Ans) X.509 is a digital certificate, which uses its public key infrastructure to verify the authenticity of the public keys. To mutually authenticate the users in a communication channel, one way to achieve this is using the x.509 certificates. x.509 is mostly used in the SSl/TSL connections to ensure that the client is trustworthy and secure. An x.509 certificate contains the user's public key and the user's identity along with encrypted hash code, which is also known as signature. Certificates are issued by the trusted source called Certificate Authority. Certificate Authority generates the signature for existing public keys. When a certificate is signed by a trusted authority. Someone holding that certificate can communicate by verifying its public key or by verifying its digital signature. Some of the benefits are, x.509 certificates are most secure and scalable. Using X.509 authentication gives more secure to the information than using the password method.

Some of the fields of the x.509 certificate are:

i) **Version** - Tells about the version of the certificate.

ii) **serial number** - Unique serial number given by the certificate authority after generating a

certificate for the user.

iii) **Algorithm information** - Tells about the algorithm used to generate the signature.

iv) **Issuer name** - Name of the CA issuing the certificate.

v) **Validity period** - period of validity of the certificate.

vi) **Subject name** - Name of the user to whom the certificate is issued.

vii) **Subject public key info** - Tells about the user's public key and its identity.

**2) How is an X.509 certificate revoked?**

Ans) Usually, if any certificate seems to be unsecure or not trusted then that certificate will be revoked by the Certificate Authority. In addition to this there are some more reasons to revoke

the certificate before it expires, Some of them are:

i) The user's secret key is assumed to be compromised.

ii) The user is no longer certified by this CA.

iii) The CA certificate is assumed to be compromised.

iv) Certificates are stolen from CA.

There are two methods available to revoke the certificates, They are

**Certificate Revocation List (CRL):**

A certificate revocation list is a list contains the certificates which are revoked by the certificate authority before its actual expiration period. The certificates which are in this list are no longer trustworthy and secure. CRL doesn't include the expired certificates. Everytime a client make a secure connection to site it'll go to contact the CA and download the CRL and search through along CRL, this causes a huge burden to the client.

**Online Certificate Status Protocol (OCSP):**

This protocol performs the real-time lookup of a certificate revocation status. This protocol defines the type of data that is exchanged between the requester of the revocation status and the server providing the revocation status information. Certificate revocation information is provided by the OCSP responder through OCSP response. OCSP responder uses the certificate serial number and responds good, revoked or unknown. Thus, OCSP overcomes the issue in the CRL.