LECTURE 9

PUBLIC KEY INFRASTRUCTURE

1. What is Public Key Cryptography?

* Asymmetric algorithms allow you to generate a key pair.
* To communicate securely with someone, you only need their public key.
* Once content has been encrypted with a public key, only the private key can decrypt it.
* Once content has been encrypted with a private key, only the public key can decrypt it

If we have both private keys, we can find their public key.

If we have both public keys, we cannot find their private key.

If we have private key and public key, we cannot know the private and public key of the other side.

1. What is Digital certificate used for?

* Are used to assure authenticity of the sender.
* Companies apply by sending CA their public key and I identifying info.
* CA verifies this info and creates a certificate containing public key and identifying and info encrypt this using its private key.
* Usually have an expiration date

1. What is X.509?

* A standard for formatting digital certificates.

Types of certificates:

* Self-signed (certificate owned by same entity that signs it)
* Root (certificates all other certificate below it / CA)
* Use / Computer (Certificate for authentication rather than passwords)
* Email (encrypt and authenticate an email message)
* Code signing

1. What is CA (Certification Authority)?

* Is a trusted organization that issues digital certificates. These certificates help verify the identity of websites , organizations or individuals online.

1. What are CA Functions?

* Authentication
* Managing certificates
* Building trust

They verify the identity of entities before issuing certificates.

Handle the lifecycle of the certificate including issuing and renewing them when necessary.

Help users trust that the website they visit is secure.

1. What is the process from http to https?

* Obtain an SSL/TSL certificate
* Install the certificate
* Update the links Change all the website links from HTTP to HTTPS.
* Redirects HTTP traffic to the HTTPS version of the site.
* Check SSL errors and ensure everything works correctly