16-124-836
Marcel Matti ZAUDER

5.4 Question 4

5.4.A List the available techniques for distributing public keys, ordering them by security level. (First = lowest)

- **Public Announcements of Keys**
  The public key is broadcasted to everyone. The huge problem with this method is forgery, such that anyone can create a key claiming to be someone else and broadcast it. Until forgery is discovered can masquerade as claimed user.
- **Publicly Available Directory**
  The public key is stored within a public directory, which are trusted by properties like Participant Registration for access or modifying the values. Directories can be accessed electronically but these are still vulnerable to forgery or tampering.
- **Public-Key Authority**
  A similar approach as the Directory one, but with improved security possible due to tightening control over the distribution of keys from the directory whereas the user is required to know the key for the directory/authority. Whenever the keys are needed, real-time access to the directory is made by the user to obtain any desired public key.
- **Public-Key Certificates**
  The authority provides a certificate (which binds an identity to the public key) to allow key exchange without real-time access to the public authority. The certificate is accompanied by some other information such as period of validity, rights of use, etc. All of the content is signed by the private key of the certificate authority and it can be verified by anyone possessing the authority's public key. In order to start the communication between two parties first the sender and the receiver both request the CA for a certificate which contains a public key and other information and then they can exchange these certificates.