COMP90043: Cryptography and security

Week 10: Workshop-10 Public Key Distribution

Q1. Discuss four methods which are used to distribute public keys?

Public announcement.

Publicly available directory.

Public-key authority.

Public-key certificates

Q2. What are the essential ingredients of a public-key directory?

1. The authority maintains a directory with a {name, public key} entry for each participant.

2. Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication.

3. A participant may replace the existing key with a new one at any time, either because of the desire to replace a public key that has already been used for a large amount of data, or because the corresponding private key has been compromised in some way.

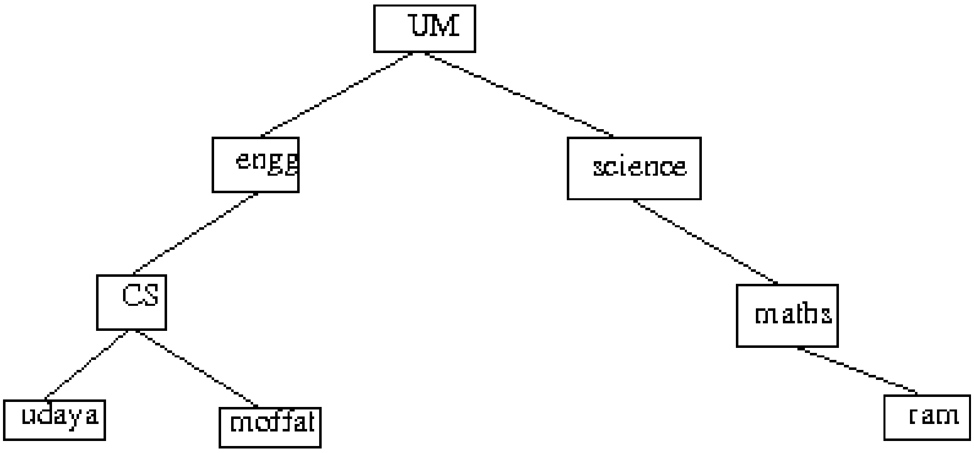
4. Periodically, the authority publishes the entire directory or updates to the directory. For example, a hard-copy version much like a telephone book could be published, or updates could be listed in a widely circulated newspaper.

5. Participants could also access the directory electronically. For this purpose, secure, authenticated communication from the authority to the participant is mandatory.

Q3. What is a chain of certificates? What are forward and reverse certificates?

A chain of certificates consists of a sequence of certificates created by different certification authorities (CAs) in which each successive certificate is a certificate by one CA that certifies the public key of the next CA in the chain.

Q4. For the following hierarchy, what is the chain of certificates that user “moffat” needs to obtain in order to establish a certificate path to “ram”? You can use X.509 conventions for the certificate chain discussed in the book, for example the certificate for “moffat” by CA “CS” is represented as CS<<moffat>>.



Forward Certificates: Certificates of X generated by other CAs.

Reverse Certificates: Certificates generated by X that are the certificates of other CAs.

CS<<engg>> engg <<UM>>UM<<Science>>Science<<maths>> maths<<ram>>

Maths<<Science>>Science<<UM>> UM<<engg>>engg<<cs>>cs<<moffat>

Q5. How a X.509 certificate is revoked?

The signer of a public-key can issue a certificate revocation list that revokes one or more certificates. Each CA maintains a list that contains all revoked but not expired certificates issued by that CA, including those issued to users and other CAs.

Each Certificate Revocation List (CRL) posted to the directory is signed by the issuer and includes issuer's name, the date the list was created, the date the next CRL is scheduled to be issued, and an entry for each revoked certificate.

When a user receives a certificate in a message, the user must determine whether the certificate has been revoked. The user could check the directory each time a certificate is received.

Q6. Explain how certificates can be used to protect Diffie-Hellman key exchange against MITM attacks.

Suppose Alice has a certificate $\mathbf{C_A = E(PR_{auth}, [ID_A, PU_A, T])}$ and Bob has a certificate $\mathbf{C_B = E(PR_{auth}, [ID_B, PU_B, T])}$, both certified by KDC with its private key $\mathbf{PR_{auth}}$. KDC's public key $\mathbf{Pu_{auth}}$ is known to public.

When Alice tries to initiate a conversation with Bob, she chooses a private key **A** and sends a message $\mathbf{E(PR_A, g^A)||C_A}$. Bob then decrypts the encrypted part with Alice's public key to retrieve $\mathbf{g^A}$. He chooses his private key **B** and sends to Alice $\mathbf{E(PR_B, g^B)||C_B}$. Alice decrypts the first part with Bob’s public key to retrieve $\mathbf{g^B}$. Finally, Alice computes $\mathbf{(g^B)^A}$ while Bob computes $\mathbf{(g^A)^B}$. They now share a common secret key.

Q7. Find at least one intermediate certification authority’s certificate and one trusted root certification authority’s certificate on your computer (e.g. in the browser). Print screenshots of both the general and details tab for each certificate.

Homework Questions:

1. What are the core components of a PKI? Briefly describe each component.
2. Explain the problems with key management and how it affects symmetric cryptography.