University of Colorado at Colorado Springs
Home Work Assignment 2
Due 11-20-02

This home work assignment involves researching Public Key Infrastructure (PKI), a topic for which we may not have have time in class.

Assume we have two participants: Alice and Bob. First and foremost, before Alice can use a public key, she needs to know who has the corresponding private key. When Alice verifies a signature, she is confirming (or denying) the Bob signed the message. If someone else has the corresponding private key, he or she sent the message, not Bob. When Alice encrypts her response to Bob, she needs to be sure that only Bob can read it. If Bob does not have the corresponding private key, he will not be able to decrypt the response.

Alice also needs to know what applications are appropriate to Bob’s key. Perhaps Bob’s key should only be used to sign or encrypt electronic mail, but not sign contracts. Finally, she needs to use a solution that will be scalable. That is, the solution must continue to work if Alice communicates with hundreds of people instead of just Bob.

There are two basic tools used in a PKI (Public Key Infrastructure) to determine who has a private key: the public key certificate and the certificate revocation list. The former will establish who, and the latter will ensure the information is up to date. The basic PKI tool that answers the question what the key can be used for is the certificate policy. The basic tool for scalability—the tool that lets Alice communicate with hundreds of people—is the certification path.

To do:

1. **Credit Card**: A credit card is a simple certificate. Write down in a list the pieces of information seen on a credit card. For each piece of information, specify what role each piece plays in the use of the credit card.

2. **Ideal Certificate**: List the characteristics you think an ideal certificate should have in the context of public key cryptography. Research on the Web or in the library.

3. **X.509 Certificates**: Write a page on X.509 certificates.

4. **Certificate Revocation List**: What does a certificate revocation list (CRL) do? What are some examples of information a CRL should contain? Present your answer in the form of a list.

5. **Scale**: For a certificate solution to scale, what do you think an entity like Alice have to do?

6. **Certificate-Based Authentication**: Several popular protocols provide authentication based on certificates. Examples are SSL (Secure Socket Layer), TLS (Transport Layer Security), IKE (Internet Key Exchange), PGP (Pretty Good Privacy) and OpenPGP. Explain briefly how certificate-based authentication works in general. Write the steps in a list. Draw a diagram to explain.
7. *Registration Authority (RA)*: An RA is designed to verify certificate contents for the CA. Certificate contents may reflect information presented by the entity requesting the certificate, such as a driver's license, or a recent pay stub. Do some research on the Web about an RA, and write one or more paragraphs on it.

8. *Certificate Repository and Archive*: Certificates and CRLs from one or more CAs are available to parties that need them to implement security services. Write a short note on certificate repositories and archives.