ECE: Advanced Information and Network Security
Computer Project 1, Due Date: November 6, 2007
Fall 2007

Project Description

In this project, your team (consisting of at most two students) will build a simple "fake" application that provides security-enhancement for email.

The motivation: Email is an unauthenticated and cleartext form of correspondence. You are to write a program that will encrypt a file (e.g. an MS Word document that contains an email correspondence), allows for authentication of this email, and that prepends (attaches before the main document) a custom-designed public key certificate that provides the key to be used for decryption.

Specifically, you are to do the following

1. Choose a symmetric encryption algorithm (such as DES, AES, SERPENT, Twofish, Blowfish, etc.) that will be used to encrypt the bulk of the file.

2. Use RSA-signatures with hashing to perform a digital signature of the document. In choosing the hash function, you should try for either SHA-1 or MD5.

3. It is up to you to figure out how to best perform encryption and digital signing simultaneously.

4. Lastly, you need to distribute the keys needed for decryption and verification. You may assume the existence of a trusted third party TTP for which everyone knows its public key. Further, you may assume the TTP has a secure method of distributing certificates (note: you will have to design your own certificate framework for this small problem). Certificates should be included at the front of the file.

5. You are to encrypt an MS Word (or text file if you are a Linux user) file using your design, and attach it to an email, send it to yourself (or another team mate), and then verify that your verification and decryption procedure works on the attached file.

Your team will turn in a short report (roughly 6 pages) that describes the approach you used and the explains your observations. Make certain to describe which language and libraries you used (if they are public), and attach a copy of your code. Your grade will be based upon the clarity and thoroughness of your report (note: if you say you got the project to work, then back it up with observations that can convince a relatively astute and suspicious professor!). Be sure to include the name of all team members on the report.