Information Security Course

Practical Project

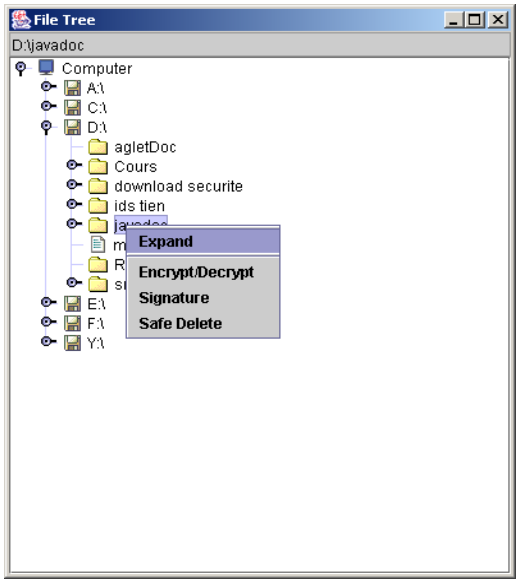
This document will give you a description of the practical project which you are asked to implement, in order to give you an occasion to put the knowledge acquired during the course into practice.
The software you will be asked to develop should allow a user to apply a certain number of security services on the files of the file system. For instance, a user should be able to :

- encrypt the content of a file
- decrypt an encrypted file
- sign a file
- verify the signature on a file,
- associate a file with its digest,
- verify the integrity of a file,
- completely remove a file from the system
- …

You are free to implement additional functionalities that you feel may be important for such an application.

For this work, you will be provided with the GUI of the application. The GUI is in fact a set of Java classes that allow the exploration of the file hierarchy with a tree like structure.
You will also be provided with a Cryptographic Service Provider that provides the traditional asymmetric and symmetric ciphers.
All these files can be found on the labs ftp server :

Spyware.tgz : the application's GUI
JCSI-Provider_2.3.tgz : the CSP
exemple.tgz : various examples illustrating the main concepts.



Authentication

The system should provide an authentication mechanism which only allows pre-registered users to use the system.
You should think of a way of checking the identity of users and verifying that they are registered before they can run the system.

Confidentiality

The system should provide a way for users to encrypt/decrypt files in the file system. It should be possible for a user to recursively encrypt the entire content of a directory. When encryption is applied to a file or a directory, both the content and the name of the file/directory should be made unreadable. Particular attention will be placed on the characters that appear in encrypted file names so that they may still be displayable by usual operating systems.

Signatures

Applying signatures

A user should have the possibility to sign files and directories. A signature will consist of a file containing all the information needed for the signature.A signed file or directory will not necessarily have to be encrypted.

Verifying signatures

The system should provide a way to verify the signature applied to a filename or a drectory.

Safe deletion

When a file is deleted from the filesystem, what usually happens is that it is simply removed from the File Allocation Table and its content is not physically removed from the disk. The system should provide a means to physically remove a file or directory from the disk. This result may be obtained by rewritting data over the content of the file before deleting it.