Hacettepe University
Computer Science and Engineering Department
Name and Surname : Burak Karademir - Barkın Boz
Identity Number : 21527123 - 21327728
Course : BBM 465
Experiment : BBM465 Information Security Laboratory Experiment 1
Subject : Hash Function and Digital Signature
Due Date: 21/11/2018 - 23:59
Advisors : Assoc. Prof. Dr. Ahmet Burak Can, Dr. Ali Seydi Keçeli
Programming Language : Java

2. Software Using Documentation

2.1. Software Usage

For using our software firstly we must write command line arguments.Our software runs with this command:
integrity start -p P -r R -l L -h H -k PriKey PubKey -i #
-p specifies the path of the folder that will be monitored by the program. -r specifies the path of the registry file. -l specifies the path of the log file. -h specifies a hash function, which can be MD5 or SHA-512. -k specifies the path of the private and public key files. -i specifies interval time. When we run the code it calculates every file's hash value and writes them into a register file after that we calculate the register file's hash value and sign it with private key.Then our program runs again after a while(we enter that time in the command line arguments).Our code verify the signature and if it is successful then it checks the changes in the files.If the verify is failed then we write it to the log file.Also we write the file changes into the log file.

2.2 Error and Information Messages

Our program writes every information into the log file.Possible informations are:

1. time stamp (dd-MM-yyyy HH:mm:ss): path/to/file deleted
2. time stamp (dd-MM-yyyy HH:mm:ss): path/to/file altered
3. time stamp (dd-MM-yyyy HH:mm:ss): path/to/file created
4. time stamp (dd-MM-yyyy HH:mm:ss): verification failed

3.Software Design Notes

3.1. Description of the program

3.1.1. Problem

Our problem is we must detect the if register file changed after signed the register file and detecting the changes in the other files with register file.

3.2. System Chart

INPUT	PROGRAMS	OUTPUT
Taken from user with command line arguments	File integrity checking tool	Log file(writes the information into this file)

3.3. Algorithm

First we create a process class object in the main class and we call run method with this object.In the run method we read the first argument if it is start then we take the register file path and we create register file.Then we call register class's method createRegisterFile with registry object.In this method we create every files (in the given path) hash value and write all values and paths line by line into register file.The we call sign method with sign object which is belongs to sign class.In this method we hash the register file and sign the hash value with private key using RSA algorithm and write this into register file.After a certain time (which is given with arguments) our program runs again with this command:

```
integrity -p P -r R -l L -h H -k PubKey
```

When our program runs again we call again the process class's run method and this time we enter another else if statement since we don't have start in the command line arguments.We call verify class's verify method.In the verify method we call reader class's readregistry method in this method we read register file's all lines except last line and add lines into a list and returns that list.Then we back to verify method and add all elements of list into a string.Then we call hash class's gethash method and calculate string's hash value.Then we verify the signature in the verify method using public key and register file's hash value(calculated with all lines of register file (except last line)) and public key.Then we create log file in given path.After that if verification failed we write it to log file, if verification successful then we call findchanges method for checking changes in the files.This method check the altered and created files and writes the changes into log file. Then we call isdeleted method for checking deleted files and this method writes the deleted files into log file.