

Lab 8

Java file signature verification

Objective: To gain an understanding of the security organization in the Java platform

Task: Check the signature of the java file

Work order:

1. Explore the material
2. Verify the signature of the jar file from the previous laboratory

Work progress:

You can verify signed JAR files yourself using the JDK 1.2 Jarsigner utility. You may want to do this, for example, to verify a signed JAR file that you have prepared. The Jarsigner utility can verify files that have been signed by either Jarsigner itself or the JDK 1.1 Javakey utility.

The basic command for verifying a signed JAR file is:

```
jarsigner -verify jar-file
```

This command will check the signature of the JAR file and make sure that the files in the archive have not changed since they were signed. If verification is successful, you will see the following message:

```
jar verified.
```

If you are trying to verify an unsigned JAR file, you will receive the following message:

```
jar is unsigned. (signatures missing or not parsable)
```

If verification fails, a corresponding message will be displayed. For example, if the contents of a JAR file were modified after the JAR file was signed, an attempt to validate such a file will display a message similar to the following:

```
jarsigner: java.lang.SecurityException: invalid SHA1  
signature file digest for test/classes/Manifest.class
```