

Java security model

4 Nov 2007

By default, applets you run from the network can neither read nor write local files; this protects you from skeezy programmers who will vandalise your data or send it off to somewhere else. Locally-run applets can read local files, but only those in the same directory as the applet, and they can't write files at all. I suppose that's to protect you from yourself, or perhaps from pranksters who try to get you to run their applet or something.

Anyway, Java also provides various ways to override these default permissions. For network applets, it's a good idea to require that they be digitally signed, and even so to carefully restrict what they have access to. For what we're doing, we'll essentially just say that any applet that you're running from somewhere inside your home directory will be able to read and write any file that is also inside your home directory.

To do so, create a file in your home directory named `.java.policy` and type the following into it:

```
grant codeBase "file:/home/student/loginname/-" {
    permission java.io.FilePermission "/home/student/loginname/-", "read";
    permission java.io.FilePermission "/home/student/loginname/-", "write";
    permission java.io.FilePermission "/home/student/loginname/-", "delete";
};
```

except replacing `loginname` with your actual login name.

If you've made a typo, the next time you run an applet you'll get a complaint about an "error parsing file" and the nature of the error (e.g. missing semicolon, bad keyword, etc). This file is read afresh every time you run an applet, so you can just fix the typo and run the applet again. If you're not sure if the file is being read, you can remove a semicolon to force the error message to appear....

Note, by the way, that this mechanism doesn't override the basic system permissions; if you don't have permission to read or modify a file, you can't get it this way. Essentially this is bringing the applet permissions in line with the permissions you'd have if you were writing a regular command-line program or a full-on GUI app.