APPLET e SICUREZZA

Un'applet non può fare tutto quello che fa una applicazione. Poiché può essere scaricata dalla rete, *sarebbe troppo pericoloso* permettere a un'applet di fare qualunque cosa ed è *costretta* a rispettare un ben preciso *modello di sicurezza (**"sandbox"**)*

– è eseguita in una "scatola" da cui non può uscire

– non può contaminare (o spiare) i dati del computer dell'utente

Un'applet di norma *non può*:

- accedere al file system locale (neppure per leggere un file)
- eseguire un altro programma
- ottenere informazioni sull'utente
- connettersi via rete a un computer *diverso da quello da cui è stata scaricata*[1]
- caricare la libreria Java, chiamare System.exit()

In molte situazioni, questi vincoli sono *troppo rigidi* e rischierebbero di *rendere impossibile* la costruzioni di applet *utili.*

APPLET FIRMATE

Attraverso tecnologie di cifratura, un'applet può essere *firmata*, ossia a essa può essere allegato un *certificato* che ne garantisce l'origine. A tali applet firmate, cui si attribuisce maggiore fiducia, *l'utente può consentire di svolgere alcune o tutte le operazioni sottoposte a vincolo.*

Ogni browser può essere configurato per gestire le applet firmate.

POLITICHE DI SICUREZZA

A partire da Java 2, l'utente può decidere *caso per caso* quali politiche di sicurezza applicare, con una *granularità molto fine*

Esiste il concetto di *policy file*, che elenca le politiche locali e si può stabilire che *una certa applet*, proveniente da *un ben preciso sito*, ha diritti particolari. Un tale file può essere fornito da chi sviluppa l'applet, o modificato dall'utente con lo strumento *PolicyTool.*

[1] Per questo motivo si preferisce lavorare con applicazioni quando ci si connette a Internet e se ne usano le risorse.