DAR PERMISOS A LAS APPLETS

IMPORTANTE: Esta operación sólo deben realizarla USUARIOS EXPERTOS y no usuarios nóveles. **Un error durante el procedimiento de autorización,** en el cual se modifica el fichero java.security, podría dañarlo haciendo inoperativa la JVM o lo que podría ser peor dar la posibilidad de acceso a programas potencialmente peligrosos como virus, gusanos, etc.

1 Introducción

El control de acceso ha evolucionado para ser más fino que en versiones anteriores de la plataforma Java. Las applets necesitan que el usuario explícitamente les de permisos de seguridad para que el gestor de seguridad que vigila la ejecución de código Java les deje acceder al sistema local de ficheros

2 Modelo de Seguridad del JDK 1.0

El modelo original de seguridad proporcionado por la plataforma Java, conocido como el modelo "*sandbox*", existió para proporcionar un entorno muy restrictivo en el que ejecutar código no firmado obtenido desde una red abierta. En este modelo, mostrado en el siguiente diagrama, el código local tiene total acceso a los recursos vitales del sistema, como el sistema de ficheros, pero el código descargado remotamente (un applet) sólo puede tener acceso a recursos limitados proporcionados dentro del sandbox. Un controlador de seguridad es el responsable en cada plataforma de determinar qué accesos a recursos están permitidos.

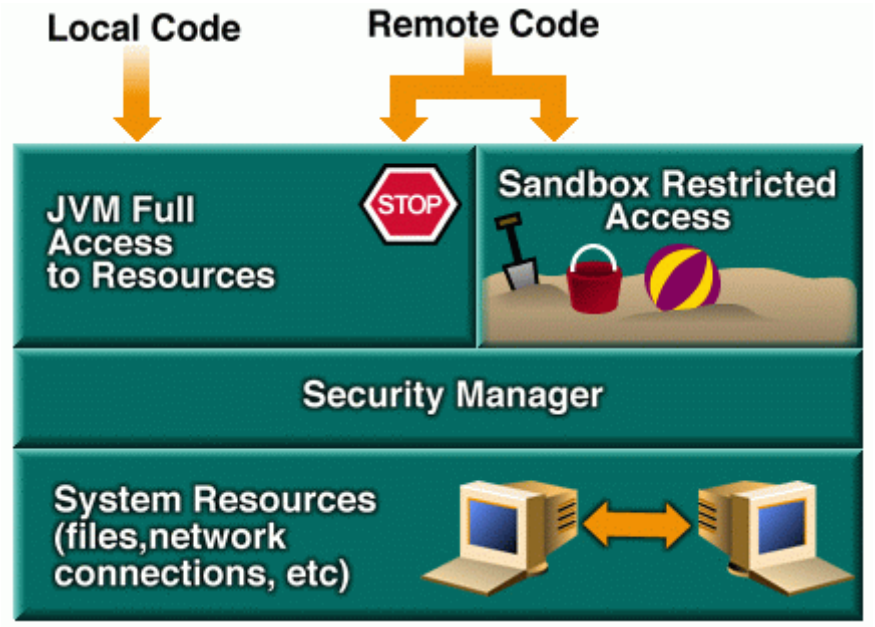
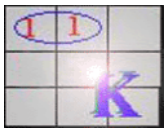


Figura 1 Modelo de seguridad JDK 1.0 (Documentación JDK de Sun)



3 Modelo de Seguridad del JDK 1.4

El JDK introduce un gran número de mejoras sobre el JDK 1.1. Primero, todo el código, sin importar si es local o remoto, puede ahora esta sujeto a una **política** de seguridad. Esta política define un conjunto de **permisos** disponibles para el código de varios firmantes o direcciones y puede ser configurado por el usuario o un administrador de sistemas. Cada permiso especifica un acceso permitido a un recurso particular, como accesos de lectura y escritura a un fichero o directorio específico o acceso de conexión a un *host* dado y a un puerto.

El sistema de ejecución organiza el código en **dominios** individuales. Cada uno de ellos encierra un conjunto de clases cuyos ejemplares pueden acceder al mismo conjunto de permisos. Un dominio puede configurarse como un *sandbox*, por eso los applets aún se pueden ejecutar en entornos restrictivos si el usuario o el administrador lo eligen así. Por defecto, las aplicaciones se ejecutan sin restricciones, pero opcionalmente ahora pueden estar sujetas a una política de seguridad.

La nueva arquitectura de seguridad en el JDK 1.2 se ilustra en la siguiente figura. La flecha de la izquierda se refiere a un dominio cuyo código tiene total acceso a los recursos; la flecha de la derecha se refiere al extremo opuesto: un dominio restringido exactamente igual que en el sandbox original. Los dominios entremedias tienen más accesos permitidos que el sandbox pero menos que el acceso total.

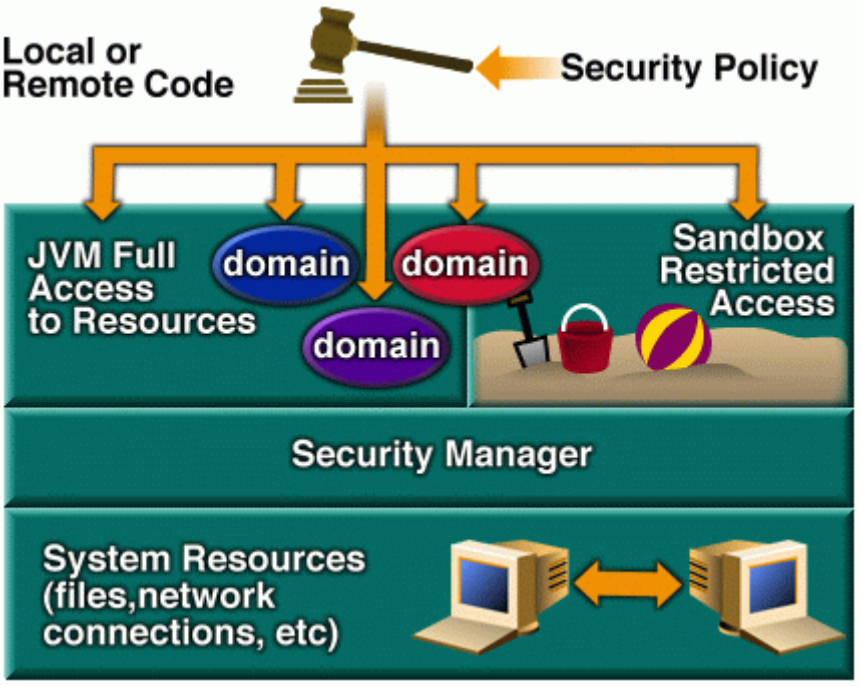
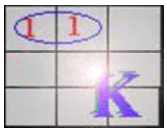


Figura 2 Modelo de seguridad JDK 1.4 (Documentación JDK de Sun)



4 Restricciones de las applets

Una forma en que la Plataforma Java proporciona protección contra ataques de un virus, por ejemplo, es a través del uso de un controlador de seguridad. Actualmente los códigos del sistema del JDK llaman a los métodos del controlador de seguridad para realizar chequeos del control de accesos a recursos.

La mayoría de los navegadores instalan un controlador de seguridad, por eso los applets se ejecutan para el escrutinio de un controlador de seguridad. Ningún applet tiene permitido el acceso a recursos a menos que explícitamente se lo concedamos, mediante un permiso en la política de seguridad. En las plataformas Java que son compatibles con el JDK 1.2, los permisos deben ser concedidos mediante una entrada en un fichero de política.

Los ficheros relacionados con la seguridad que se encuentran dentro del JDK 1.2 son.

- El fichero de Propiedades de Seguridad **java.security**.
- El fichero de política del Sistema **java.policy**.
- El Keystore de Certificados **cacerts**.

Estos ficheros internos residen en el directorio de propiedades de seguridad del JRE,

java.home/lib/security/ (Solaris)
java.home\lib/security\ (Windows)

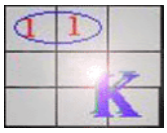
(Nota: java.home indica el directorio en el que se instaló el JRE.)

4.1 Fichero de propiedades de Seguridad java.security

En este fichero se configuran varias propiedades de seguridad para usarlas con las clases del paquete **java.security**.

Este fichero especifica

- nombres de paquetes provider, localizaciones y orden de precedencia.
- La clase a ejemplafizar como el objeto **Policy** cuyo permiso estará disponible para el código de varias fuentes.
- URLs para los ficheros de política a ser cargados y utilizados cuando se tomen decisiones de seguridad (si el objeto Policy ejemplarizado es uno que utiliza ficheros de política).
- si se debe permitir o no la expansión de propiedades en el fichero de política, por ejemplo expandir **${java.home}** al valor de la propiedad **"java.home"**.
- si se puede especificar o no un fichero de política adicional en la línea de comandos con **-Djava.security.policy=somefile**.
- el tipo de keystore por defecto (inicialmente llamado "jks", el tipo de keystore propietario de Sun Microsystems)



Para ver más detalles, el fichero se encuentra en.

java.home/lib/security/java.security (Solaris)
java.home\lib/security\java.security (Windows)

(java.home indica el directorio en el que se instaló el JRE.)

4.2 Fichero de Política del Sistema java.policy

Un fichero de política especifica qué permisos están disponibles para el código de varias fuentes.

A este fichero nos referimos como fichero de política del "sistema" porque se utiliza para conceder grandes permisos del sistema. El fichero **java.policy** instalado con el JDK concede todos los permisos a las extensiones estándards, permite a cualquiera escuchar en un puerto no-privilegiado, y permite a cualquier código leer ciertas propiedades "estándard" como las propiedades "os.name" y "file.separator".

Si es necesario, el fichero de política del sistema puede ser modificado, con un editor de texto, o con la herramienta **policytool**. Este último no requiere que conozcamos el formato del fichero de política, usándolo nos ahorramos teclear y evita errores.

El fichero **java.policy** por defecto está localizado en.

java.home/lib/security/java.policy (Solaris)
java.home\lib/security\java.policy (Windows)

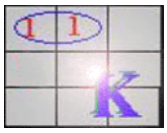
(java.home indica el directorio en el que instalamos el JRE.)

Las localizaciones de los ficheros de política realmente se especifican en el fichero de propiedades de seguridad como los valores cuyos nombres tienen la forma.

policy.url.n=URL

donde "n" es un número. El fichero de política del sistema está definido en el fichero de propiedades de seguridad como.

policy.url.1=file:${java.home}/lib/security/java.policy



5 Dar permisos a las applets

Para dar permisos de seguridad a las applets hay que modificar el fichero java.policy en el subdirectorio lib/security/ del directorio donde este instalado el JRE.

En Windows, para una instalación típica, la ruta hasta este fichero es:

c:/Archivos de Programa/Java/JRE/1.4.1/lib/security/java.policy

Los permisos de seguridad se dan a través de cláusulas que están en el fichero. A continuación se dan tres posibles cláusulas que permiten trabajar a las applets. Para incluir una de estas cláusulas en el fichero, basta con copiarla y luego pegarla en el fichero java.policy. Sólo es necesario incluir una de las tres.

5.1 Configurar un fichero de Política para Conceder los Permisos Requeridos

Para poder conceder los permisos necesarios se utiliza la herramienta Policy Tool que trae tanto el JRE como el JDK.

En el JRE este fichero se localiza:

JRE.home\bin

En el JDK se localiza

JDK.home\bin

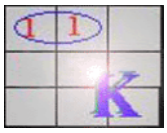
JDK.home y JRE.home se refieren a la carpeta donde se hallan instalados los mismos. Para ejecutar el fichero hay que hacer doble clic sobre el fichero **policytool.exe.**

Con este programa editaremos el fichero java.security para añadir una nueva entrada.

Importante: Si estas ejecutando tu propia copia del JDK, puedes fácilmente editar tu fichero de propiedades de seguridad. Si estás ejecutando una versión compartida con otros, sólo podrás modificarlo si tienes acceso de escritura, o si pides al administrador que modifique el fichero de la forma apropiada. Sin embargo, no es apropiado realizar modificaciones en un fichero de seguridad para todo el sistema sólo para probar este tutorial. Te sugiero que leas los pasos siguientes para ver cómo se hace o que te instales tu propia versión privada del JDK para usar con las lecciones del tutor.

El fichero de propiedades de seguridad está alojado en

Windows.
JRE.home\lib\security\java.security
UNIX.
JRE.home/lib/security/java.security



El ejecutar el fichero **policytool.exe** nos traerá la ventana de Policy Tool. Siempre que se arranca, Policy Tool intenta rellenar su ventana con información de algo que algunas veces es referido como "fichero de política de usuario", que, por defecto, es un fichero llamado **.java.policy** que está en el directorio home. Si Policy Tool no puede encontrar ese fichero, informa de la situación y muestra una ventana Policy Tool en blanco (es decir, una ventana con cabeceras y botones pero sin datos, como se muestra en la figura.

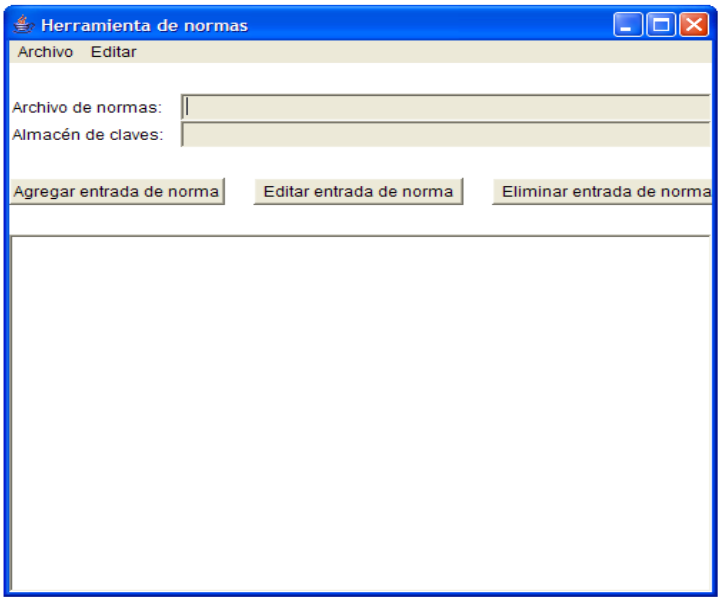


Figura 3 Programa Policy Tool

Asumiendo que estamos viendo una ventana de Policy Tool en blanco, Figura 2 (si no es así, seleccionamos **New** en el menú **File**), podemos proceder inmediatamente a abrir el fichero de políticas java.security.

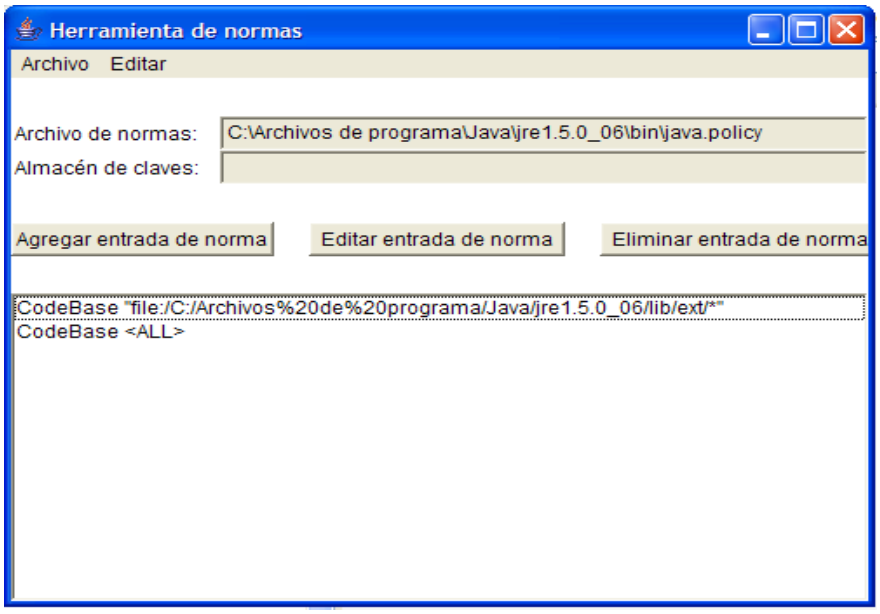
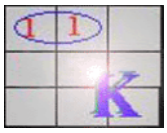


Figura 4 Abriendo fichero java.security



Elegimos el botón **Agregar entrada de norma** en la ventana principal de Policy Tool. Esto nos trae la caja de diálogo Policy Entry. Desde alli añadimos la dirección de la carpeta a la que deseamos añadir los permisos.

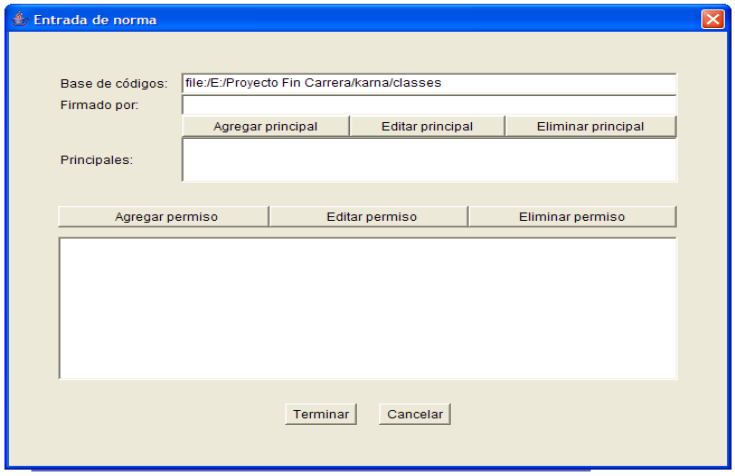


Figura 5 Entrada de norma

Seleccionamos AllPermissión para conceder todos los permisos, escritura, lectura, etc a **todo** el código que se ejecute desde la carpeta especificada.

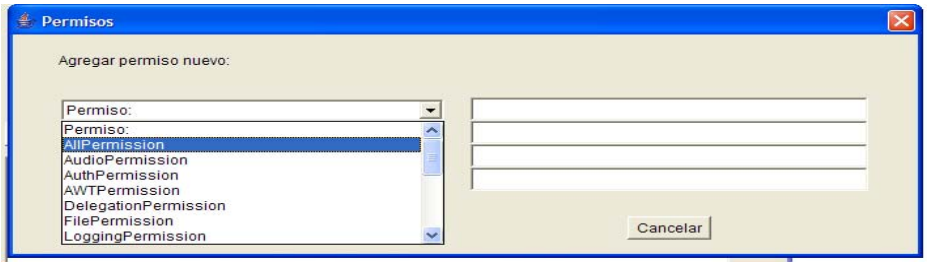


Figura 6 Añadiendo permisos

Una vez añadidos los permisos, se acepta en el botón terminar.

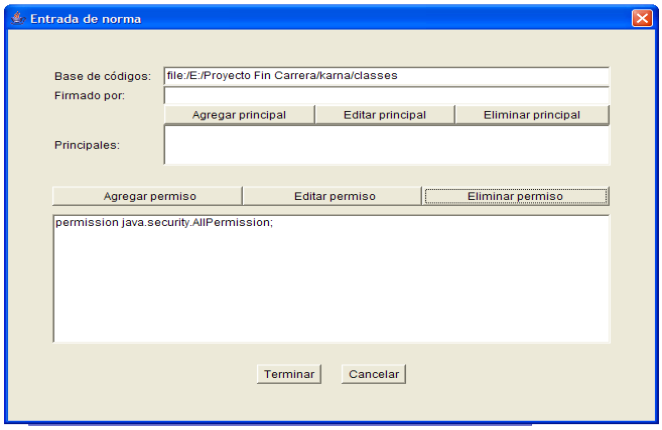
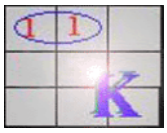


Figura 7 Entrada norma



Si lo que deseamos es dar los permisos necesarios para que un applet de una página determinada tenga acceso a nuestro ordenador se deberá añadir la dirección de Internet en la base de códigos.

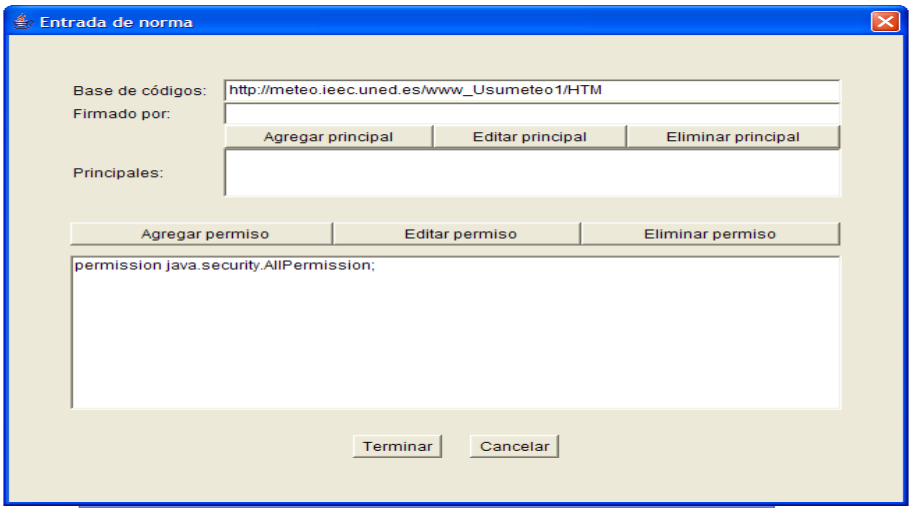


Figura 8 Entrada norma para una dirección de Internet

Se añade de nuevo permisos pulsando en el botón *Agregar permiso*, se selecciona *AllPermission* para conceder todos los permisos y se finaliza pulsando *Terminar*.

Una vez añadidas las autorizaciones deseadas se guarda por el fichero java.security. Desde ese momento las applets ejecutadas dentro de la carpeta especificada o desde la dirección de Internet indicada tendrán acceso al ordenador del usuario.

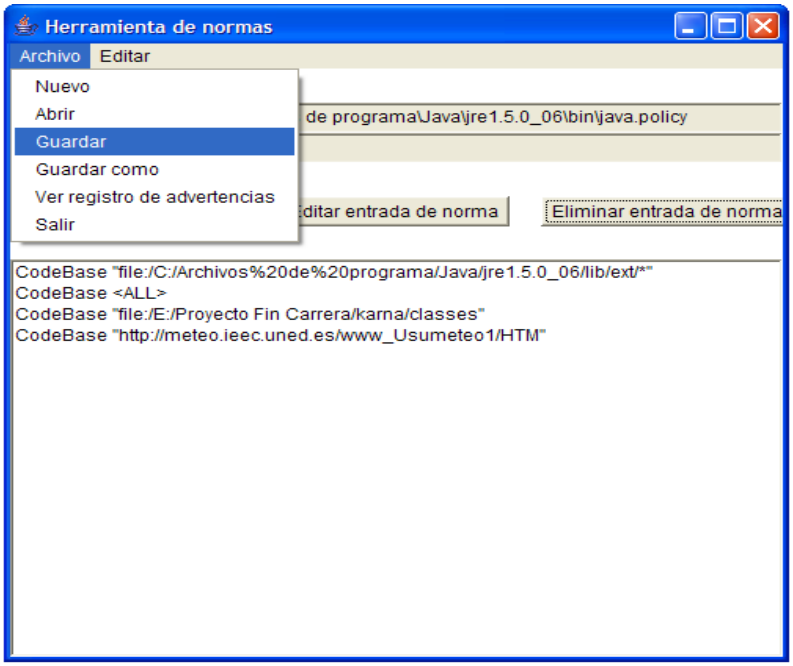


Figura 9 Guardando el fichero java.policy