

RESTRICCIONES EN EL MODELO DE SEGURIDAD FLASH

Ámbito del problema

Los contenidos que se ejecutan en Flash Player lo hacen dentro de un sandbox de seguridad que limita sus operaciones. Dependiendo de dónde se ejecute el contenido (ejecución remota o local), del tipo de compilación de los contenidos y de la configuración global de Flash Player en el ordenador en el que se ejecuten esos contenidos, las restricciones pueden variar.

En concreto, en el escenario más restrictivo, cuando la ejecución es en local, el modelo de seguridad elegido es local-with-filesystem, y la configuración global de Flash es la de por defecto, el sandbox de seguridad de Flash impedirá cualquier comunicación de los contenidos con la red, incluyendo la invocación de cualquier función (JavaScript, ejecutables nativos o internas de Flash) mediante el método `fscommand` o la clase `ExternalInterface`. En este caso, cuando la aplicación intenta invocar una función Flash Player mostrará una alerta de seguridad, ofreciendo la posibilidad de cambiar la configuración global de Flash Player. Si el usuario no cambia la configuración, la función no podrá ser invocada.



Fig. 1: Alerta de seguridad Flash Player



Fig. 2: Configuración global de Flash

Problema

El problema viene dado por varias razones:

Por definición en los requisitos, no es posible cambiar la configuración global de Flash. Se asume que el usuario final no podrá o no querrá cambiarla.

En ciertos casos es necesaria la comunicación con el entorno LMS, que se realiza a través de funciones JavaScript.

El entorno de ejecución podrá ser local, y no remoto.

Debido a ello, habrá ocasiones en las que la invocación de funciones externas lanzará la alerta de seguridad.

Solución

Como solución, y ya que no es necesaria la trazabilidad fuera de un LMS, hay que evitar acceder a cualquier función JavaScript desde AS.

Se recomienda usar un patrón de estrategia, para variar el comportamiento dependiendo de si la ejecución es local o en un LMS.

Se puede usar la variable `System.security.sandboxType` para ver el modo de ejecución. Esta variable es de sólo lectura, y permite saber en tiempo de ejecución qué modelo de seguridad se está ejecutando la película swf. De esta manera podemos saber si el OA se está ejecutando dentro de un LMS (valor `remote`) o en un PC en local (valor `localWithFile`).

Una vez obtenido el valor de la variable es cuando podremos aplicar el patrón de estrategia, estableciendo comunicación con el LMS en el caso de que el OA se esté ejecutando dentro del mismo, o evitando esa comunicación en el caso de que la ejecución sea local. De esta manera evitaremos los errores que se muestran al usuario.