

Autorización y control de acceso

Seguridad en Redes de Ordenadores

Enrique Soriano

LS, GSYC

23 de febrero de 2018



(cc) 2018 Grupo de Sistemas y Comunicaciones.

Algunos derechos reservados. Este trabajo se entrega bajo la licencia Creative Commons Reconocimiento - NoComercial - SinObraDerivada (by-nc-nd). Para obtener la licencia completa, véase <http://creativecommons.org/licenses> También puede solicitarse a Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

- ▶ IAAA: Identification, Authentication, Authorization and Auditing.
- ▶ Ya hemos visto las dos primeras.

Control de acceso

- ▶ Acceso: un sujeto activo que intenta interactuar con un objeto pasivo realizando una *operación de acceso*.
- ▶ El sistema permite/deniega en base a:
 - ▶ Lo que le está permitido hacer al sujeto.
 - ▶ Lo que está permitido hacerle al objeto.
- ▶ Errores en el diseño o la implementación pueden permitir realizar operaciones no autorizadas.
Ejemplo: *side-channel* de Dropbox.

Operaciones de acceso

Ejemplos:

- ▶ Añadir
- ▶ Leer
- ▶ Escribir
- ▶ Ejecutar
- ▶ Borrar
- ▶ Cambiar permisos
- ▶ Cambiar dueño
- ▶ Listar
- ▶ Buscar/atravesar

El control de acceso puede ser

- ▶ **Discrecional** (Discretionary Access Control o DAC): el usuario posee objetos y autoriza al resto del usuario para acceder.
- ▶ **Obligatorio** (Mandatory Access Control o MAC): los usuarios no gestionan el acceso a los objetos.

Mandatory Access Control

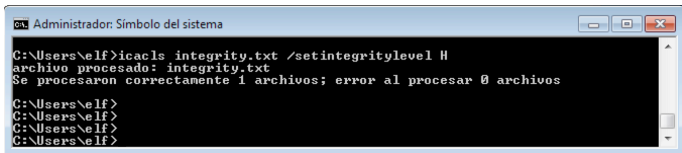
- ▶ Entornos muy restrictivos (p.ej., militares).
- ▶ Sistemas de Seguridad Multinivel (MLS):
 - ▶ Usuarios con rango.
 - ▶ Objetos con nivel de seguridad.
 - ▶ Compartimentos.
- ▶ Centrados en la confidencialidad (modelo Bell-LaPadula):
 - ▶ Puedes observar documentos de tu nivel o de más bajo nivel.
 - ▶ Puedes generar documentos de tu nivel o de más alto nivel.
 - ▶ Para generar documentos de un nivel más bajo al tuyo, tienes que degradarte.
- ▶ Centrados en la integridad (modelo BIBA):
 - ▶ Puedes modificar documentos de tu nivel o de más bajo nivel.

Mandatory Access Control

Ejemplo: Mandatory Integrity Control (MIC) en Windows 7 aplica MAC BIBA antes de aplicar el control de acceso discrecional:

Cuatro niveles:

- ▶ **Bajo** (no confiable). Los ejecutables pueden ser marcados como nivel bajo si son peligrosos (p.ej. bajados de Internet y no firmados). Sólo pueden modificar carpetas temporales, etc.
- ▶ **Medio** (usuario). Los usuarios normales y los objetos que no tienen etiqueta de integridad tienen este nivel.
- ▶ **Alto** (administrativo). Los administradores tienen este nivel, la carpeta de Archivos de Programa, etc.
- ▶ **Sistema** (control total). Los servicios del sistema tienen este nivel.



```
Administrador: Símbolo del sistema

C:\Users\elf>icacls integrity.txt /setintegritylevel H
archivo procesado: integrity.txt
Se procesaron correctamente 1 archivos; error al procesar 0 archivos

C:\Users\elf>
C:\Users\elf>
C:\Users\elf>
C:\Users\elf>
```


IBAC: Control de acceso basado en la identidad.

- ▶ Access Control Matrix: filas: usuarios, columnas: objetos.

	<i>list.c</i>	<i>a.doc</i>	<i>word.exe</i>
<i>esoriano</i>	r,w	r	-
<i>paurea</i>	r	r	w,x
<i>nemo</i>	r	r,w	-
<i>sdemingo</i>	-	-	r,w,x

- ▶ Access Control List: una columna de la matriz.

<code>list.c</code>	
<i>esoriano</i>	r,w
<i>paurea</i>	r
<i>nemo</i>	r
<i>sdemingo</i>	-

Permisos POSIX:

- ▶ Permisos `rx` para dueño, grupo, y resto.
- ▶ Los grupos se especifican en `/etc/groups`.
- ▶ `chmod` cambia los permisos.
- ▶ `chown` cambia el dueño de un fichero. Sólo puede hacerlo root.

Permisos POSIX:

- ▶ `chgrp` cambia el grupo de un fichero. Lo puede hacer el dueño del fichero (tiene que pertenecer al grupo al que se cambia).
- ▶ sticky bit (+t) en directorios: restringe la eliminación de entradas de directorio aunque el directorio tenga permisos de escritura para todo el mundo: sólo puede borrar/renombrar el dueño y root. P. ej. `/tmp`

OJO: en sistemas modernos (Linux, OSX) los permisos Unix conviven con ACLs. En cada sistema se evalúan las reglas de una forma (leer manual).

Caso: ACLs en Windows

Windows 7 tiene dos tipos de ACLs:

- ▶ DACL (Discretionary ACL): lista de ACEs que permiten o deniegan un tipo de acceso para una cuenta o grupo.

Evaluación:

1. Si el objeto no tiene ACL (p. ej. FAT), se garantiza el acceso.
 2. Si alguna entrada deniega el acceso, se deniega.
 3. Si alguna entrada permite el acceso, se permite.
 4. Si no se especifica el acceso, se deniega.
- ▶ SACL (System ACL): usada para **auditar**, es una lista de ACEs que indican el tipo de acción que provocará una entrada en el Security Event Log.

RBAC: Control de acceso basado en roles.

- ▶ **Rol: colección de permisos con nombre.** Un grupo es un conjunto de usuarios, un rol es un conjunto de permisos.
- ▶ Se asignan roles a los sujetos/grupos del sistema. Un usuario puede tener más de un rol. Los roles pueden ser dinámicos.
- ▶ Puede haber una jerarquía de roles.
- ▶ Es útil para implementar la *separación de deberes*.
- ▶ Escalabilidad: los usuarios del mismo tipo suelen tener los mismos privilegios.
- ▶ Cómodo: en general, los usuarios cambian más frecuentemente que los privilegios que tienen las distintas clases de usuarios.

Control de acceso basado en *capabilities*:

- ▶ El sujeto presenta un *capability* junto con su petición para realizar una operación de acceso.
- ▶ La *capability* puede ser un certificado firmado, un ticket, una secuencia pseudo-aleatoria, etc.
- ▶ Facilita la delegación de privilegios y la escalabilidad.
- ▶ Dificulta la revocación de privilegios y la auditoría (quién puede hacer qué en un momento dado).

Autorización en el WWW: OAuth

OAuth :

- ▶ Propósito: **autorización** para usar APIs de terceros sin dar las credenciales.
- ▶ El usuario permite a un tercero acceder a ciertas operaciones del API de un servicio web, sin darle tu contraseña.
- ▶ Usa timestamps, nonces y firmas digitales.
- ▶ Ejemplos: Twitter, YouTube.

Autorización en el WWW: OAuth

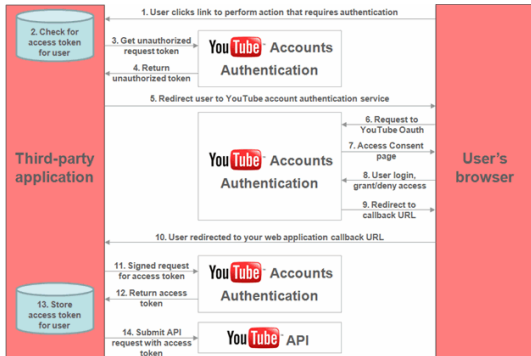


Imagen © Google

Otros tipos de control de acceso

- ▶ ABAC: Control de acceso basado en atributos.
 - ▶ Ciertos atributos (edad, nacionalidad, etc.) del usuario le autorizan para realizar ciertas operaciones.
 - ▶ Esos atributos pueden ser concedidos por otras entidades.
 - ▶ P. ej.: Si el usuario tiene asociado un timeline de una red social, puede realizar tal operación.
- ▶ CBAC: Control de acceso basado en el contexto.
- ▶ ...