Universidad Nacional de San Agustín de Arequipa
Facultad de Ingeniería, Producción y Servicios
Escuela Profesional de Ciencia de la Computación

Trabajo de Investigación Formativa 3

Modelo de Control a Discreción

Integrantes: - Castillo Caccire, Kemely Francis
- Chullunquía Rosas, Sharon Rossely
- Lipe Huamaní, Brayan Alexander

Docente: Mg. Lucy Delgado Barra

Fecha: 28 de septiembre de 2021

Arequipa, Perú

Índice de Contenidos

Índice de Figuras

1. Introducción

Uno de los primeros modelos más importantes de los Modelos Multinivel, es el modelo *Discretionary Access Control* (de sus siglas en inglés DAC), que traducido al español sería **Acceso de Control Discrecional o a Discreción**, el sitio oficial de Oracle [1] lo define de la siguiente forma,"es un mecanismo de software para controlar el acceso de usuarios a archivos y directorios. DAC deja que la configuración de protecciones para archivos y directorios las realice el propietario según su criterio". Por otro lado, el sitio [2] nos da a entender que es tipo de Control de Acceso, el cual "es un componente fundamental de seguridad de datos que dicta quién tiene permiso para acceder a y usar información y recursos de la empresa. Mediante la autenticación y autorización, las políticas de control de acceso se aseguran de que los usuarios sean quienes dicen ser y tengan acceso apropiado a los datos de empres".
Este tipo de control fue definido en base a los criterios de *Trusted Computer System Evaluation* (TCSEC). Los TCSEC tiene por objetivo aplicar la política de seguridad del Departamento de Defensa estadounidense. Esta política se preocupa fundamentalmente del mantenimiento de la confidencialidad de la información clasificada a nivel nacional. Este define siete conjuntos de criterios de evaluación denominados **clases** [3], que son; D, C1, C2, B1, B2, B3, A1. Entonces, el Control de Acceso Discrecional se define generalmente en oposición al control de acceso obligatorio (MAC) (algunas veces llamado control de acceso no-discrecional). A veces, un sistema en su conjunto dice tener control de acceso discrecional o puramente discrecional como una forma de indicar que carece de control obligatorio [4].

2. Conceptos relacionados

2.1. Control de Acceso

Anteriormente en la sección de 1, se encarga de limitar los acceso físico a los campus, edificios, habitaciones y centro de datos. Básicamente, el control de acceso identifica a los usuarios a base de verificar distintas credenciales de inicio de sesión, que pueden incluir nombres de usuarios y contraseña, PIN, escaneos biométricos y tokens de seguridad.

2.2. Lista de Controles de Acceso

Segúnd Wikipedia [5], es "una lista de control de acceso o ACL (del inglés, access control list) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido". Las ACL son un mecanismo básico para proporcionar seguridad a las redes de datos pudiéndose utilizar para restringir y controlar el acceso desde el punto de vista de la red como desde el punto de vista del sistema operativo para realizar esas mismas tareas sobre distintos recursos del sistema.

Las ACL tambien se aplican masivamente en servicios básicos de red como pueden ser los proxys, servidores DNS, servidores de correo electrónico, etc. Algunas ventajas del ACL en redes son [6]:

2.3. TCSEC

Como ya se ha mencionado anteriormente, esta serie de requerimientos esenciales para evaluar la eficacia de los controles de seguridad informática integrados en un sistema informático que fue evaluado para su uso por el Departamento de Defensa de los Estados Unidos (DoD). El TCSEC, frecuentemente conocido como el Libro Naranja, es la pieza central de las publicaciones de la Serie DoD Rainbow. Publicado inicialmente por el Centro Nacional de Seguridad Informática (NCSC), un brazo de la Agencia de Seguridad Nacional en 1983 y luego actualizado en 1985, TCSEC fue reemplazado con el desarrollo del estándar internacional Common Criteria publicado originalmente en 2005 [7].

2.3.1. Divisiones

Cada división representa una diferencia significativa en la confianza que un individuo u organización puede depositar en el sistema evaluado. Además, las divisiones C, B y A se dividen en una serie de subdivisiones jerárquicas llamadas clases: C1, C2, B1, B2, B3 y A1. Cada división y clase amplía o modifica según se indica los requisitos de la división o clase inmediatamente anterior.

- **A (Protección verificada)**
- **B (Protección obligatoria)**
- **C (Protección Discrecional)**
- **D (Protección Mínima)**

3. Arquitectura

Básicamente, la estructura que maneja el control está compuesta de ciertos elementos y procedimientos, en la siguiente imagen 1 podemos una visión general de un control de acceso.

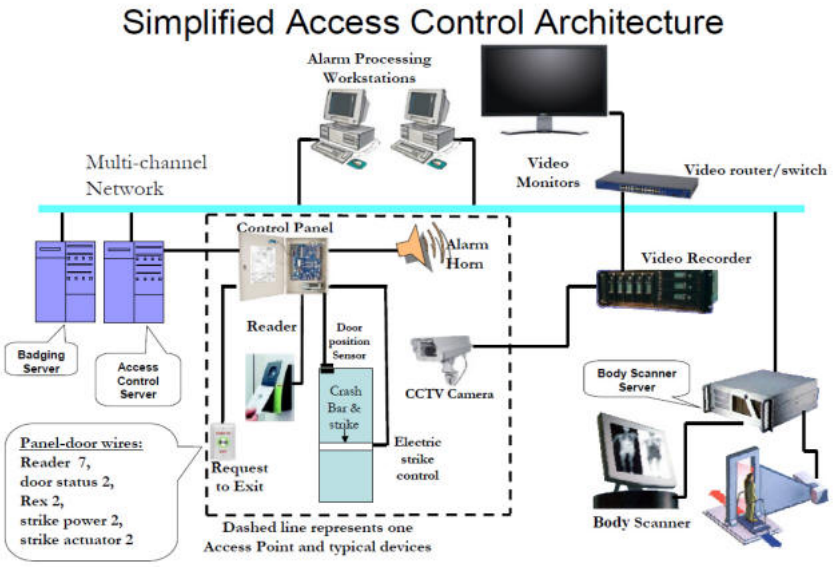

Figura 1: Arquitectura General de Sistema de Control de Acceso

Algunas razones del porqué se implementa este tipo de arquitectura son las siguientes [8]:

- Proporcionar .ªcceso controlado.ª la instalación.
- Permitir el acceso solo al personal autorizado.
- Implementar un "Protocolo y política de seguridad"para que los empleados, los visitantes y las instalaciones estén seguros.
- Implementar una jerarquía de niveles de seguridad y acceso basada en la función del personal.
- Automatizar y mejorar el proceso de identificación.
- Automatizar el seguimiento del personal.
- Minimizar el error humano.
- Rastrear contratistas y proveedores externos.
- Registrar y generar informes de acceso para cada área.

4. Atributos

Los atributos de DAC incluyen [9]:

- El usuario puede transferir la propiedad del objeto a otro(s) usuario(s).
- El usuario puede determinar el tipo de acceso de otros usuarios.
- Después de varios intentos, las fallas de autorización restringen el acceso de los usuarios.

- Los usuarios no autorizados son ciegos a las características del objeto, como el tamaño del archivo, el nombre del archivo y la ruta del directorio.
- El acceso al objeto se determina durante la autorización de la lista de control de acceso (ACL) y se basa en la identificación del usuario y / o la pertenencia a un grupo.

5. Implementaciones

El significado del término en la práctica no es tan claro como la definición dada en el estándar TCSEC, porque la definición TCSEC de DAC no impone ninguna implementación. Hay al menos dos implementaciones: con propietario (como ejemplo generalizado) y con capacidades[10].

5.1. Con propietario

El término DAC se usa comúnmente en contextos que asumen que cada objeto tiene un propietario que controla los permisos para acceder al objeto, probablemente porque muchos sistemas implementan DAC usando el concepto de propietario. Pero la definición de TCSEC no dice nada sobre los propietarios, por lo que técnicamente un sistema de control de acceso no tiene que tener un concepto de propiedad para cumplir con la definición de TCSEC de DAC.
Los usuarios (propietarios) tienen bajo esta implementación de DAC la capacidad de tomar decisiones sobre políticas y / o asignar atributos de seguridad. Un ejemplo sencillo es el modo de archivo Unix que representa escritura, lectura y ejecución en cada uno de los 3 bits para cada uno de Usuario, Grupo y Otros. (Está precedido por otro bit que indica características adicionales).

5.2. Con capacidades

Como otro ejemplo, a veces se describe que los sistemas de capacidad proporcionan controles discrecionales porque permiten a los sujetos transferir su acceso a otros sujetos, aunque la seguridad basada en la capacidad fundamentalmente no se trata de restringir el acceso "basado en la identidad de los sujetos". En general, los sistemas de capacidad no permiten que se pasen permisos a ningún otro sujeto; el sujeto que desea aprobar sus permisos debe primero tener acceso al sujeto receptor, y los sujetos generalmente solo tienen acceso a un conjunto estrictamente limitado de sujetos de acuerdo con el principio de privilegio mínimo .

6. Ventajas y Desventajas

6.1. Ventajas

El control de acceso discrecional es un modelo bastante popular porque permite mucha libertad a los usuarios y no genera gastos administrativos[11].Algunos beneficios del control de acceso discrecional incluyen:

- **Fácil de usar**:La gestión de datos y permisos es más fácil con DAC. La interfaz de usuario es muy fácil de operar, por lo que no es necesario pasar por la molestia de planificarlo todo a la vez.
- **Flexible**: Mientras trabaja, a menudo surge la necesidad de compartir datos con compañeros de trabajo. El sistema DAC permite que cualquier usuario con acceso a cierta información otorgue acceso a otros también, lo que facilita el proceso de trabajo.
- **Menos dolor de cabeza para la administración**: DAC no requiere un mantenimiento regular, no requiere mucho tiempo. El intercambio de datos es mucho más fácil ya que la administración no necesita interferir cada vez que se necesita compartir un dato con un usuario.

6.2. Desventajas

Como sabemos solo los usuarios especificados por el propietario pueden tener alguna combinación de lectura,escribir, ejecutar y otros permisos para el archivo. La política del CAD tiende a ser muy flexible y es ampliamente utilizado en los sectores comercial y gubernamental. Sin embargo, se sabe que DAC inherentemente débil por dos razones [12].

- Primero, otorgar acceso de lectura es **transitivo**; por ejemplo, cuando Ann concede a Bob acceso de lectura a un archivo, nada impide que Bob copie el contenido del archivo de Ann a un objeto que Bob controla. Bob ahora puede otorgar acceso a cualquier otro usuario a la copia del archivo de Ann, sin el conocimiento de Ann.
- En segundo lugar, la política de DAC es **vulnerable** a los ataques de caballos de Troya. Porque programas heredan la identidad del usuario que invoca, Bob puede, por ejemplo, escribir un programa para Ann que, en la superficie, realiza alguna función útil, mientras que al mismo tiempo destruye el contenido de los archivos de Ann. Al investigar el problema, los archivos de auditoría indicarían que Ann destruyó sus propios archivos.

Por lo tanto, formalmente, los inconvenientes de DAC son los siguientes:

- La información se puede copiar de un objeto a otro; por lo tanto, no existe una garantía real sobre el flujo de información en un sistema.
- No se aplican restricciones al uso de la información cuando el usuario la ha recibido.
- Los privilegios para acceder a los objetos los decide el propietario del objeto, en lugar de a través de una política de todo el sistema que refleje los requisitos de seguridad de la organización.

7. Ejemplos

Bajo el modelo de control de acceso discrecional, cada objeto tiene un propietario que determina quién tiene acceso a ese archivo o recurso. Por lo general, el propietario es la persona que crea ese archivo o recurso, a menos que esa persona asigne un nuevo propietario. Comúnmente abreviado como DAC, los controles de acceso discrecional son el tipo más común de control de acceso, utilizado de forma predeterminada en ***Windows***, ***Macintosh*** y la mayoría de los sistemas operativos ***Linux***.[13]

Figura 2: Windows, Linux y Macintosh

Cada objeto tiene una lista de control de acceso compuesta por entradas, donde cada una de estas entradas enumera un usuario y los permisos que tiene. Para un archivo X en *Windows*, puede indicar que el usuario **Lena** tiene permisos completos, pero el usuario **Greg** solo tiene permisos para leer, por lo que Greg no puede modificar el archivo X. El propietario del objeto tiene la última palabra sobre quién tiene qué permisos.

8. DAC vs. MAC

Como se sabe, la seguridad de la información es importante para cualquier sistema automatizado. Por ende, estos sistemas requieren de mecanismos que garanticen la seguridad de la información. [14]

Generalmente, cuando un usuario desea ingresar a un sistema ,primero debe pasar por un proceso de autenticación. Al momento de proporcionar sus datos, el usuario se encuentra ya autorizado. Un ejemplo es cuando el usuario ingresa su correo y contraseña. Si estos datos son válidos, el usuario recién puede acceder al sistema.

Después de esta autenticación de usuario, se procede a la autorización, donde se determina los permisos otorgados al usuario autenticado. En este proceso de la autorización, el control de acceso es de ayuda.

El control de acceso es una de las prácticas de ciberseguridad más importantes y ayuda a proteger los datos confidenciales, reduciendo la posibilidad de un ataque. Existen 2 tipos de métodos de control de acceso, DAC (Discretionary Access Control) y MAC (mandatory

access control).[15]

A continuación se define las diferencias dentre DAC y MAC:

- **DAC**

  Pros:

  - **Fácil de usar:** Los usuarios pueden administrar sus datos y acceder rápidamente a los datos de otros usuarios.
  - **Flexible:** Los usuarios pueden configurar los parámetros de acceso a los datos sin administradores.
  - **Fácil de mantener:** El administrador no necesita mucho tiempo para agregar nuevos objetos y usuarios.
  - **Granular:** Los usuarios pueden configurar los parámetros de acceso para cada dato.

  Contras:

  - **Bajo nivel de protección de datos:** DAC no puede garantizar una seguridad confiable porque los usuarios pueden compartir sus datos como quieran.
  - **Oscuro:** No hay una administración de acceso centralizada, por lo que para conocer los parámetros de acceso, debe verificar cada lista de control de acceso.

- **MAC**

  Pros:

  - **Alto nivel de protección de datos:** Un administrador define el acceso a los objetos y los usuarios no pueden editar ese acceso.
  - **Granular:** Un administrador establece los derechos de acceso de los usuarios y los parámetros de acceso a los objetos manualmente.
  - **Inmune a los ataques del caballo de Troya:** Los usuarios no pueden desclasificar datos ni compartir el acceso a datos clasificados.

  Contras:

  - **Capacidad de mantenimiento:** la configuración manual de los niveles de seguridad y las autorizaciones requiere una atención constante por parte de los administradores.
  - **Escalabilidad:** MAC no escala automáticamente.
  - **No es fácil de usar:** Los usuarios deben solicitar acceso a cada nuevo dato; no pueden configurar los parámetros de acceso para sus propios datos.

Después de ver los pros y contras de cada modelo, se tiene el siguiente resumen en cuadro comparativo:

Característica	MAC	DAC
Control de acceso impuesto por	Administradores y sistema operativo	Administradores y usuarios
Flexibilidad	–	✓
Escalabilidad	–	✓
Sencillez	–	✓
Mantenimiento	Duro	Fácil
Costo de implementación	Elevado	Bajo
Granularidad	Alto (los administradores ajustan las autorizaciones para cada usuario y objeto manualmente)	Alto (los usuarios pueden asignar derechos de acceso a cualquier otro usuario o grupo)
Fácil de usar	–	✓
Nivel de seguridad	Elevado	Bajo
Útil para	Gobierno, ejército, aplicación de la ley	Pequeñas y medianas empresas

Figura 3: DAC vs. MAC [15]

DAC y MAC son dos modelos opuestos de control de acceso. MAC está controlado por administradores y requiere mucho tiempo y esfuerzo de mantenimiento, pero proporciona un alto nivel de seguridad. DAC es mucho más fácil de implementar y mantener, ya que los usuarios pueden administrar el acceso a los datos que poseen. Sin embargo, DAC no es lo suficientemente bueno para proteger datos confidenciales.

9. Conclusiones

En conclusión, DAC es un modelo de control de acceso que es fácil de implementar y mantener, ya que los usuarios pueden administrar el acceso a los datos que poseen. DAC funciona bien para organizaciones que requieren flexibilidad y flujos de trabajo fáciles de usar. En cambio, DAC no es lo suficientemente bueno para proteger datos confidenciales. Mientras que MAC es más eficiente para organizaciones que trabajan con datos altamente sensibles. [15]

Debido a esta limitación, DAC no puede ser utilizado por organizaciones que trabajan con datos extremadamente sensibles (Ej. médicos, financieros, militares, etc.). Sin embargo, DAC es una buena opción para las pequeñas empresas con personal de TI (Tecnología de la información) y presupuestos de ciberseguridad limitados. Permite compartir información y asegura el buen funcionamiento del negocio.

Referencias

[1] Oracle, "Control de acceso discrecional." https://docs.oracle.com/cd/E56339_01/html/E53985/ugintro-8.html, 2014. Accessed: 2021-09-27.

[2] Citrix, "Acceso seguro." https://www.citrix.com/es-mx/solutions/secure-access/what-is-access-control.html, 2021. Accessed: 2021-09-27.

[3] UPM, "Tcsec - trusted computer system evaluation criteria." http://www.dit.upm.es/~pepe/401/index.html#!7249, 2021. Accessed: 2021-09-27.

[4] Wikipedia, "Control de acceso discrecional." https://es.wikipedia.org/wiki/Control_de_acceso_discrecional, 02 2021. Accessed: 2021-09-27.

[5] Wikipedia, "Lista de control de acceso." https://es.wikipedia.org/wiki/Lista_de_control_de_acceso, 2021. Accessed: 2021-09-27.

[6] Alberto Linares - Google Sites, "Listas de control de acceso." https://sites.google.com/site/albertolinares2smr/3-seguridad-logica/3-2-acceso-a-sistemas-operativos-y-aplicaciones/3-2-2-listas-de-control-de-acceso, 2021. Accessed: 2021-09-27.

[7] Wikipedia, "Trusted computer system evaluation criteria." https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria, 2021. Accessed: 2021-09-27.

[8] Systems I/O Inc., "Access control system overview." http://www.systems-io.com/AccessControl.html, 2021. Accessed: 2021-09-27.

[9] Techopedia.Com, "What is discretionary access control (dac)?." https://www.techopedia.com/definition/229/discretionary-access-control-dac. Accessed: 2021-09-28.

[10] Wikipedia, "Discretionary access control." https://en.wikipedia.org/wiki/Discretionary_access_control. Accessed: 2021-09-28.

[11] Bernhard Mehl, "Discretionary access control explained." https://www.getkisi.com/blog/discretionary-access-control-explained. Accessed: 2021-09-28.

[12] V. C. Hu, D. Ferraiolo, D. R. Kuhn, *et al.*, *Assessment of access control systems*. Citeseer, 2006.

[13] M. X. Heiligenstein, "8 access control models – strengths, weaknesses, and more." https://firewalltimes.com/access-control-models/, Jun 2021.

[14] Sawakinome, "Diferencia entre dac y mac." https://es.sawakinome.com/articles/technology/difference-between-dac-and-mac.html.

[15] Ekran, "Mandatory access control vs discretionary access control: Which to choose?." https://www.ekransystem.com/en/blog/mac-vs-dac, Mar 2020.