

Políticas y Modelos De Seguridad

PUA: Romero, Carlos Alberto

2011

Introducción

- Las instituciones se ven inmersas en ambientes agresivos.
- Importancia y sensibilidad de la información y servicios críticos.



La necesidad de las políticas

- Las políticas de alto nivel son pautas sobre la seguridad de la información.
- Sin políticas es imposible la creación de sistemas seguros.
- La institución de políticas de seguridad incluye las leyes, normas y prácticas que regulan cómo una institución gestiona y protege los recursos.



Las políticas de seguridad (I)

- ***Sistemas Abiertos / Cerrados:***
 - En un sistema cerrado, nada es accesible al menos que se autorice expresamente.
 - En un sistema abierto o institución todo es accesible a menos que esté explícitamente denegado.
- ***Menos privilegio (lo que necesita conocer):***
 - Deben ser autorizadas sólo para tener acceso a los recursos que necesitan.
- ***Maximizar el intercambio:***
 - Hacer a la información lo más accesible posible.
- ***Autorización:***
 - Las normas explícitas deben definir quién puede utilizar qué recursos y cómo.



Las políticas de seguridad (II)

- **Obligación:**
 - Estas políticas definen qué debe o no debe realizarse.
- **Separación de los derechos:**
 - Las funciones críticas deben ser asignadas a más de una persona o sistema.
- **Auditoria:**
 - Debe llevar un registro de lo que se hizo y en qué momento.
- **Control Centralizado / Descentralizado:**
 - En un sistema descentralizado sus divisiones tienen autoridad para definir sus propias políticas.
- **Propiedad y administración:**
 - Una política administrativa separa la administración de los datos de su uso.
 - La propiedad puede violar la separación de los derechos cuando el usuario de la información también es su administrador.



Las políticas de seguridad (III)

- ***Rendición de cuentas individuales:***

- Deben ser identificados y sus actuaciones grabadas y revisadas.

- ***Roles:***

- Un grupo de derechos que se le da a los usuarios de acuerdo a sus funciones.

- ***Nombre o número dependiendo de su control de acceso:***

- El acceso de control está designado por su número.

- ***Contenido- dependiendo del control de acceso-:***

- El acceso a los datos depende de los requerimientos de los archivos específicos.



Las políticas de seguridad (IV)

- ***Contexto-dependiendo del control de acceso-***
 - El acceso a los datos depende de que otra información también la requiere.
- ***Historia-dependiendo del control de acceso-***
 - Se considera todos o subgrupos de requerimientos para la decisión de acceso.



Aplicación - Políticas Específicas (I)

1. ***Políticas de confidencialidad.***

- *Clasificación de documentos:*

- Los documentos son clasificados en función de la sensibilidad de su información.

- *Categorías:*

- Definen particiones verticales de los niveles.

- *Originator controlled (ORCON):*

- Un documento sólo se libera a las personas o unidades que estén en una lista específica hecha por el inventor.

- *Acceso a lo total:*

- Los usuarios están autorizados a leer sólo los valores de los datos agregados.



Aplicación - Políticas Específicas (II)



2. ***Políticas de integridad.***

- *La integridad de los documentos:*

- Un documento no puede ser modificado o sólo se puede registrar las modificaciones.

- *Cambio limitado:*

- Los datos sólo se pueden modificar en la forma prescripta.

3. ***Grupo de políticas.***

- *Acciones autorizadas:*

- Sólo pueden realizar acciones para las que fueron autorizadas.

- *Rotación de los derechos:*

- Una tarea no debe ser realizada siempre por la misma persona.

- *Operación de la secuenciación:*

- Los pasos de algunas tareas deben llevarse a cabo en un orden específico.

Aplicación - Políticas Específicas (III)

4. *Políticas de conflicto de intereses.*

- *Política de Muralla:*
 - La información se agrupa en clases de “conflicto de intereses”.
- *Conflicto de roles:*
 - Un usuario no puede tener dos funciones que pueden implicar un conflicto de intereses.



Sistema de políticas (I)

- La mayoría de estas políticas pueden aplicarse también a bajo nivel.
- Otras políticas de sistema definen el uso específico de algún sistema.
 - Por ejemplo, una cuenta de usuario / contraseña.
- Se pueden definir políticas para el diseño y el uso de cualquier aspecto de un sistema informático.



Sistema de políticas (II)

- Moffett y Sloman clasifican las políticas de sistemas de seguridad en tres niveles:
 - 1. Políticas generales:**
 - Éstas se aplican a cualquier institución.
 - 2. Políticas específica:**
 - Estas se refieren a organizaciones específicas.
 - 3. Reglas de acceso:**
 - Define especificaciones para el acceso a recursos determinados.
- Un error común es definir las políticas de bajo nivel sin utilizar políticas de alto nivel como referencia.



Sistema de políticas (III)

- Algunas políticas se pueden aplicar a varios sistemas:
- ***Aislamiento o contención:***
 - Un sistema debe estar aislados de los sistemas externos.
- ***Compartir el control:***
 - Los recursos o la información deben ser compartidos por los procesos o sistemas de forma controlada.
- ***Sistemas sin memoria:***
 - Un programa no debe tener ningún vestigio de sus ejecuciones pasadas.
- En general, el aislamiento y la participación en el control se excluyen mutuamente cuando se aplica a un proceso específico.



Ejemplos de políticas

- Muchas políticas comunes se refieren a aspectos de autorización.
- Las autorizaciones definidas deben ajustarse a las necesidades de la aplicación.
- Lo siguiente es un posible conjunto de las políticas de un sistema universitario, asumiendo también la política de un sistema cerrado:
 - *Un instructor puede ver toda la información sobre el curso que está enseñando.*
 - *Un instructor puede cambiar las calificaciones de los estudiantes en el curso en que enseñanza.*
 - *Un estudiante puede ver sus calificaciones del curso que está realizando.*
 - *Un director de departamento puede añadir o suprimir cursos en su departamento.*
 - *Los miembros del profesorado puede acceder a información sobre sí mismos.*
 - *Un estudiante puede inscribirse en un curso.*
 - *Un director de departamento puede ver información sobre su departamento y pueden cambia la información sobre profesores y cursos.*
 - *Un decano puede ver la información de todos los departamentos en su universidad o facultad.*



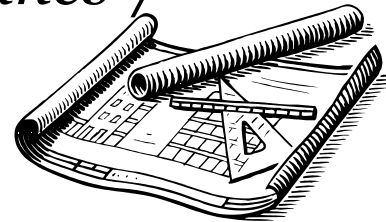
Uso de funciones en materia de políticas

- Es importante definir las funciones con respecto a la información producida.
- Algunas posibles funciones con respecto a los documentos son:
 - **Fuente:**
 - * La persona que emite un documento.
 - **Autorizador:**
 - * La persona que controla el acceso sobre el documento.
 - **Depositario:**
 - * La persona que guarda el documento de control y su uso.
 - **Usuario:**
 - * La persona que lee o modifica el documento.
 - **Auditor:**
 - * La persona que chequea las acciones, resultados, y los controla.
- También podemos definir las funciones apropiadas para las personas de acuerdo a sus funciones de trabajo.
 - *Por ejemplo, gerente, secretaria, estudiante, y el instructor.*



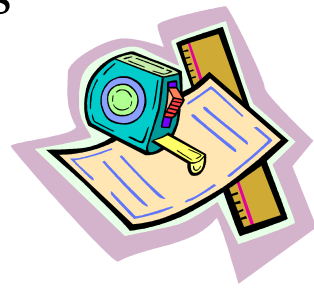
Políticas Estándares

- En los EE.UU. la primera institución gubernamental a cargo de las políticas de seguridad fue el Departamento de Defensa.
- Se publicó un documento que enumera una serie de requisitos para sistemas de seguridad (Libro Naranja) .
- Más tarde, el Instituto Nacional de Estándares y Tecnología (NIST) ha desarrollado un conjunto de documentos conocidos como los Criterios Comunes .
- Otras políticas se han definido por ECMA y la ISO.
- Las políticas para aplicaciones especializadas:
 - *La información médica: BMA en el Reino Unido y la HIPAA en los EE.UU..*
 - *La información financiera: La Ley Sarbanes-Oxley de los EE.UU..*



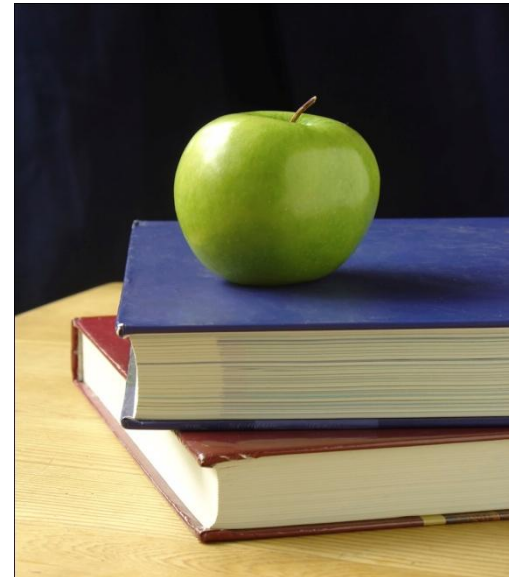
Normas para las políticas

- El Modelo de Política del Núcleo de Información (PCIM) es un modelo de política.
- Para ampliar el Modelo Común de información (CIM).
- La CIM define objetos genéricos.
- Incluye sistemas, elementos administradores del sistema, elementos físicos y lógicos, y los servicios.
- Se define una política de Estado y sus componentes, condiciones y acciones.
 - <condition set> hacer <action list>
- Las normas de política pueden ser simples o grupales (un patrón compuesto).
- Las condiciones y acciones pueden ser parte de normas específicas o ser almacenados en los repositorios de uso común por varias normas.



Políticas de lenguajes

- IBM ha desarrollado una Política de Lenguaje Fiduciario.
- Usa XML para definir los criterios de asignación.
- Las normas no pueden ser heredadas.



Políticas en conflictos

- Es posible que los objetos a que se refiere una política se superpongan con los de otra política.
- El conflicto puede resolverse mediante políticas tales como:
 - *“permisos tienen prioridad”*;
 - *“negaciones tienen prioridad”*;
 - o mediante la adición explícita a las prioridades de cada Estado.



Problemas con las políticas no apropiadas

- Un ejemplo de un caso real:
 - *Un ex-empleado de Global Crossing Holdings Ltd. Descontento con esta, colocó numerosos nombres, SSN, y fechas de nacimiento de empleados de la empresa en su sitio Web.*
- El primer problema fue la no aplicación de la necesidad de conocer la política.
- El segundo problema fue similar, el acceso a la información de facturación debería haberse limitado.



Propiedades e interacciones de las políticas

- Algunas políticas pueden ser representadas formalmente con el uso de modelos .
- Mientras que otros en su mayoría se describen con palabras.
- Un buen conjunto de políticas pueden ser reutilizables.
- Las políticas aplicadas en un sistema interactúan unas con otras.
- Idealmente, deberían colaborar o convergen.
- Pueden superponerse.
- La peor situación es cuando las políticas entran en conflicto entre sí.
- Los sistemas distribuidos requieren la coexistencia de muchas políticas.



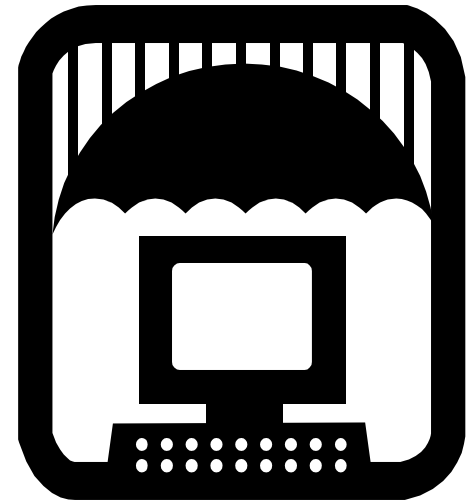
Políticas y diseño de sistemas de seguridad

- Cuáles de estas amenazas son importantes y cómo podemos evitarlas.
- Las políticas que guiarán la selección de los mecanismos específicos.
- Las políticas son también importantes para la evaluación de un sistema seguro.
- Los mecanismos de más bajo nivel deben aplicar las políticas definidas por los de alto nivel.
- La mayoría de los sistemas comerciales no lo aplican.
- También es importante definir las políticas de seguridad en un contexto.
- Jerarquías de las políticas que pueden tener conflictos.
- En este momento podemos considerar los casos de uso del sistema para definir los derechos.
- Un modelo nos permite analizar las propiedades de seguridad y es la base para el diseño del sistema.



Modelos de seguridad

- Los modelos de seguridad son más precisos y detallados que la expresión de las políticas.
- Pueden describirse de manera formal o semi-formal.
- Pueden ser obligatorios o discrecionales.
- Una clasificación divide a los modelos:
 - La matriz de acceso.
 - Acceso basado en funciones de Control.
 - Los modelos multinivel.



La matriz de acceso (I)

- Es un modelo de seguridad que se pueden aplicar a cualquier sistema.
- El modelo define:
 - Un conjunto de sujetos S.
 - Un conjunto de objetos protegidos O.
 - Un conjunto de tipos de acceso T.
- Una combinación (sujeto, objeto protegido, tipo de acceso) o (s, o, t) es una norma de autorización.
- Un amplio modelo de acceso: la autorización de la regla tiene la forma (a, s, o, t, p, c, f) .
- Los sistemas de bases de datos generalmente utilizan un subconjunto (s, o, t, p)



La matriz de acceso (II)

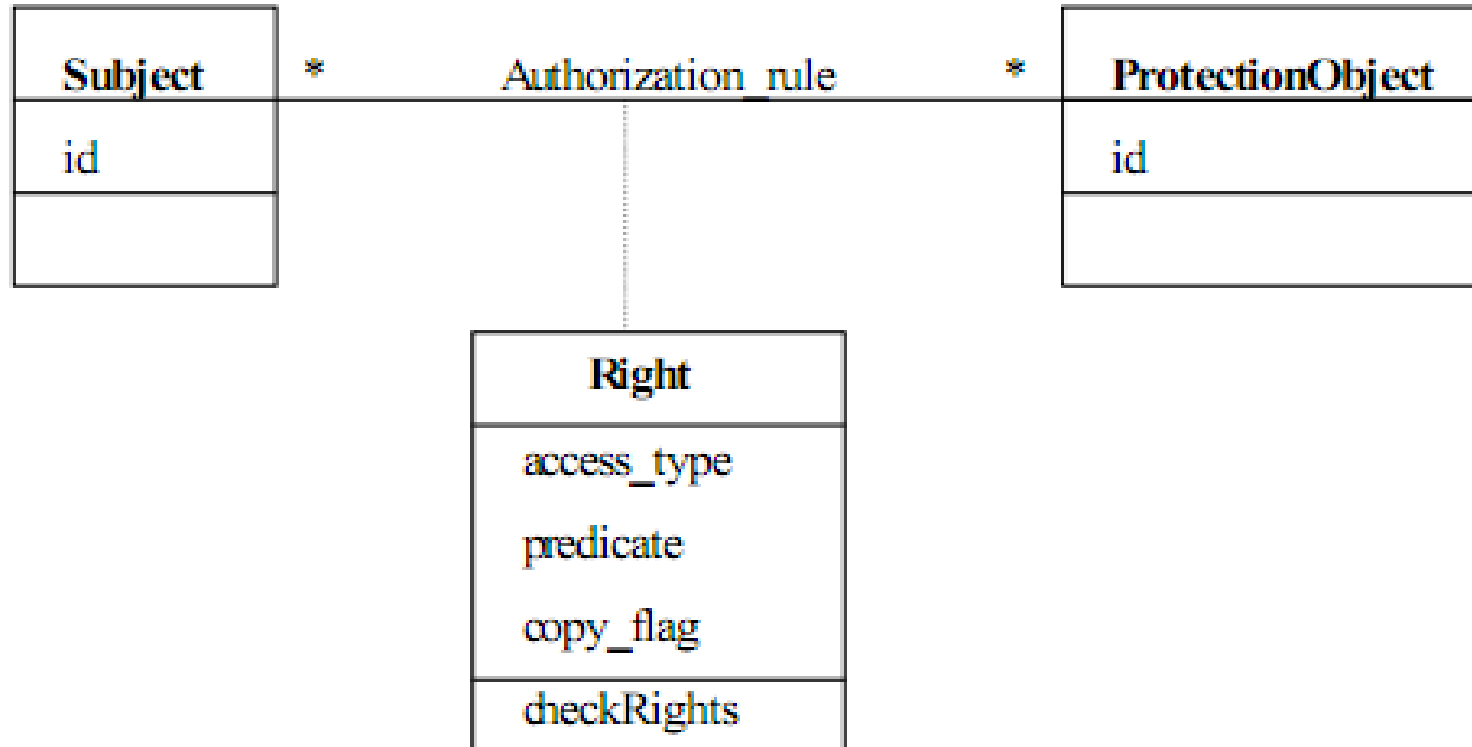


Figura 1.1: The authorization pattern.

La matriz de acceso (III)

- La matriz original de Lampson, tenía el concepto de propietario.
- La matriz de Lampson y su extensión, incluyen las operaciones de modificar la matriz y permiten la propagación de los derechos.
- Harrison, Ruzzo y Uhlman ampliaron y formalizaron este modelo.
- La principal diferencia es la forma en que la matriz es cambiada.
- Añaden un conjunto de comandos:

Command $c(x_1, x_2, \dots, x_k)$ //the x 's stand for s or o

if t_1 in $M(s_1, o_1)$ and

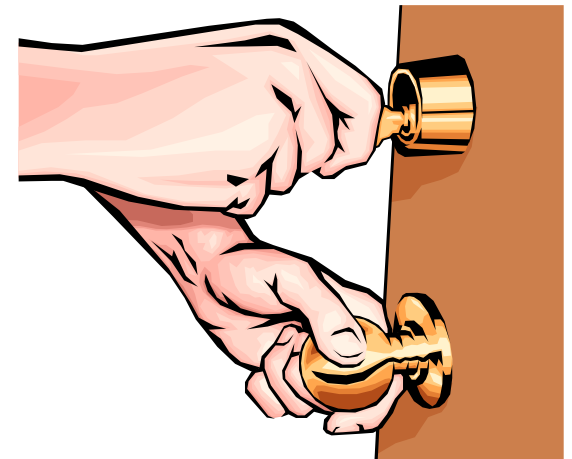
if t_2 in $M(s_2, o_2)$ and

..

if t_m in $M(s_m, o_m)$

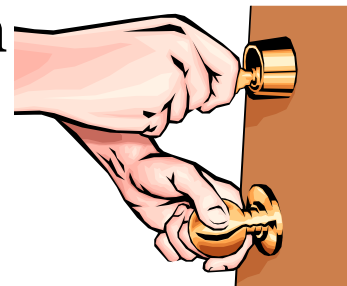
then op_1, op_2, \dots, op_n

end



La matriz de acceso (IV)

- En particular, se demostró que el problema de seguridad para el acceso a la matriz no está resuelto.
- Una aplicación de la matriz de acceso debe tener una manera de almacenar adecuadamente la autorización de las normas.
- Utilizar una versión obligatoria de la matriz de acceso, tales como RBAC.
- Para luego comparar la solicitud de acceso a la matriz para decidir si otorgarlo o no.
- Las políticas especiales son necesarias cuando un sujeto o un objeto puede implicar otros.



Control de Acceso basado en funciones- RBAC (Role-Based Access Control) (I)

- Puede considerarse como una variación de la matriz de acceso, donde los sujetos sólo pueden ser funciones.
- Los derechos se asignan a las funciones, no a los individuos.
- RBAC convenientemente puede aplicar las políticas de mínimos privilegios, y la separación de funciones.
- También utiliza el concepto de período de sesiones.
- Una manera de hacer cumplir la política de mínimos privilegios es asignar derechos a las funciones de casos de uso .
- Los casos de uso se utilizan para definir un sistema con todos los accesos necesarios para sus funciones.



Control de Acceso basado en funciones- RBAC (Role-Based Access Control) (II)

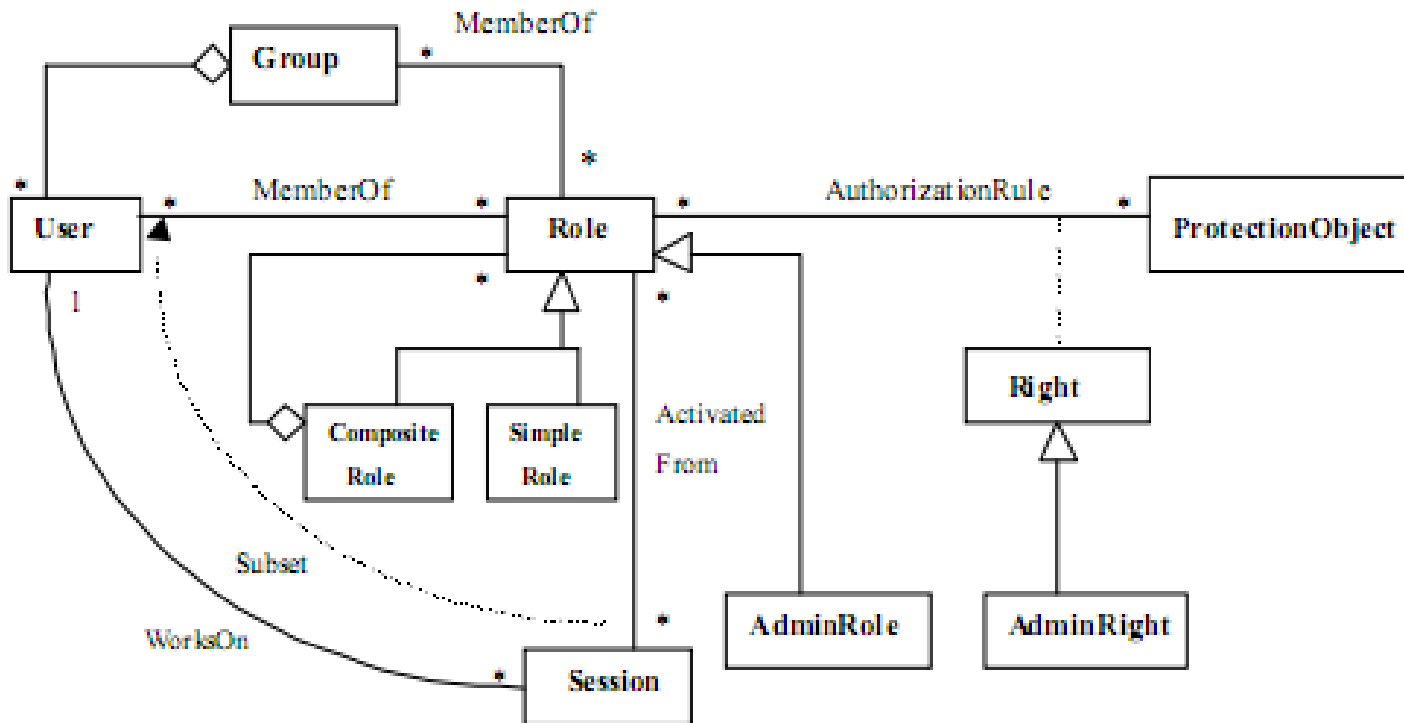


Figura 1.2: The RBAC pattern.

Los modelos multinivel

- Los datos se clasifican en niveles de sensibilidad y los usuarios tienen acceso de acuerdo con sus autorizaciones.
- Estos modelos se han formalizado en tres formas diferentes:
 1. **El modelo de La Bell-Padula:** *destinado a controlar las fugas de información entre los niveles.*
 2. **El modelo de Biba:** *que controla la integridad de los datos.*
 3. **El modelo de celosía:** *generaliza los niveles parcialmente ordenados de los modelos anteriores utilizando el concepto de matemática de celosías.*



Modelo de confidencialidad La Bell-Padula (I)

- Clasifica los temas y datos en niveles de sensibilidad.
- La clasificación, C , de los objetos de datos define su sensibilidad.
- En cada nivel superior de acceso de la matriz se va refinando el control de acceso.
- Un nivel de seguridad se define como un par (nivel de clasificación, conjunto de categorías).
- Un nivel de seguridad domina otro si y sólo si su nivel es mayor o igual que las otras categorías y su nivel incluye las otras categorías.



Modelo de confidencialidad La Bell-Padula (II)

- Dos propiedades, conocidas como "no leer" y "no escribir", definen un flujo seguro de información:
 1. **Propiedad de seguridad simple (ss)**: *Un sujeto S puede leer un objeto O sólo si su clasificación domina la clasificación del objeto, es decir, $C(s) \Rightarrow C(o)$.*
 2. ***- Propiedad**: *Un sujeto S que puede leer un objeto o se le permite escribir sobre un objeto p sólo si la clasificación de p domina la clasificación de la o, por ejemplo, el $C(p) \Rightarrow C(o)$.*
- Este modelo también incluye sujetos de confianza.
- Son necesarios para el desempeño de las funciones administrativas.
- Este modelo se complementa con el modelo de integridad Biba.



El modelo de integridad Biba

- Clasifica los datos en los niveles de integridad.
- Incluye las propiedades:
 1. **Propiedad de seguridad simple:** *Un sujeto S puede modificar un objeto o sólo si $I(s) \geq I(o)$.*
 2. **Integridad *- propiedad:** *Si un sujeto s tiene acceso para leer un objetos o con el nivel de integridad $I(o)$, s puede escribir en el objeto sólo si $I(o) \geq I(p)$.*



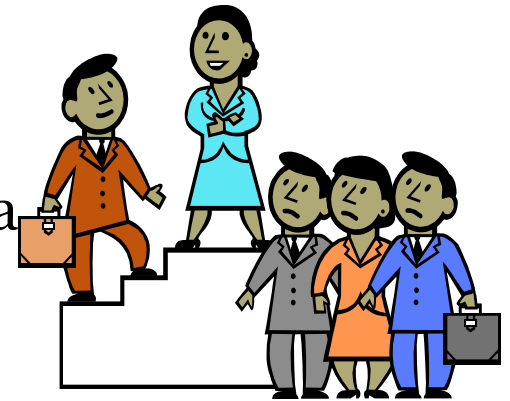
El modelo de celosía

- Una celosía es una estructura matemática que consta de elementos parcialmente ordenados.
- Cada par de elementos tiene un límite superior mínimo y un máximo límite inferior.
- Las celosías no son estrictamente de orden jerárquico.
- Son más difíciles de aplicar que las jerarquías simples.
- Por todo ello, se utilizan con poca frecuencia en la práctica.

5 10784.36
2.719372
9 ÷ 1

Aplicación de los modelos multiniveles

- Los modelos multiniveles son teóricamente los más seguros de los tres modelos básicos de seguridad.
- Sin embargo, son difíciles de aplicar.
- También son complejos de utilizar, se necesita al menos dos modelos.
- Tienen valor para la aplicación de sistemas que necesitan capas.



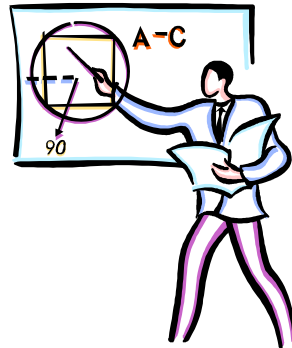
El modelo de Clark-Wilson

- Se basa en la jerarquización de aplicaciones para el manejo de información de parte de los usuarios.
- La integridad de la aplicación era un aspecto mucho más importante que la confidencialidad.
- Se hace hincapié en las transacciones bien realizadas y en la separación de servicio.



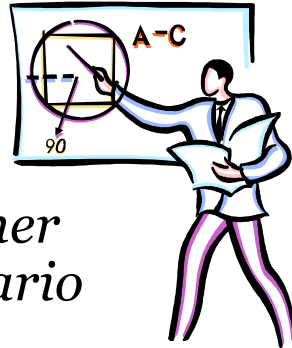
Modelos y diseño de sistemas de seguro (I)

- Una visión de estados de un sistema seguro.
- Si se parte de un estado inicial seguro y todas las transiciones de estado son seguros vamos a estar siempre en un estado seguro.
- Esta definición no tiene en cuenta si el estado inicial o las transiciones son significativas o si contradicen las políticas de las instituciones.
- Hay ejemplos de tres de las posibles combinaciones de los modelos:
 1. Los modelos basados en la matriz de acceso discrecional se han utilizado en la mayoría de sistemas operativos.
 2. RBAC es el modelo más común de los sistemas modernos.
 3. Los modelos multiniveles se han utilizado sólo en sistemas militares



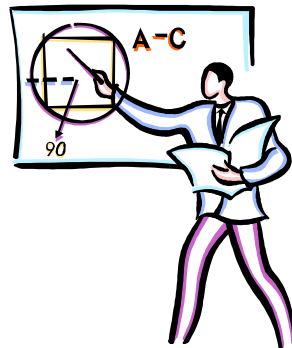
Modelos y diseño de sistemas de seguro (II)

- Para elegir un modelo primero debemos decidir qué políticas queremos para un sistema dado.
- El siguiente paso es convertirlas en modelos.
- Por ejemplo:
 - *Si tenemos un sistema en el que los usuarios deben tener determinados tipos de accesos a los documentos, será necesario algún tipo de matriz de acceso.*
- Podemos definir los sujetos de esta matriz de acuerdo con las funciones de usuario y si los usuarios no deben conceder o recibir derechos de otros usuarios.
- Está claro que necesitamos RBAC.
- Este modelo cubrirá sólo una parte de los requisitos de la política.
- El siguiente paso consiste en reflejar el modelo seleccionado en los niveles inferiores.



El modelo Monitor de Referencia (I)

- Presentamos ahora la plantilla que vamos a utilizar para describir los patrones:
- **Intento**
 - Hacer cumplir las autorizaciones cuando un sujeto solicita un objeto protegido.
- **Contexto**
 - Un entorno multiprocesamiento en el que los sujetos solicitan objetos protegidos para llevar a cabo sus funciones.
- **Problema**
 - Si no se define las autorizaciones correctamente es lo mismo que no tenerlas.
 - Los sujetos pueden realizar todo tipo de acciones ilegales.
 - Cualquier usuario puede leer cualquier archivo.



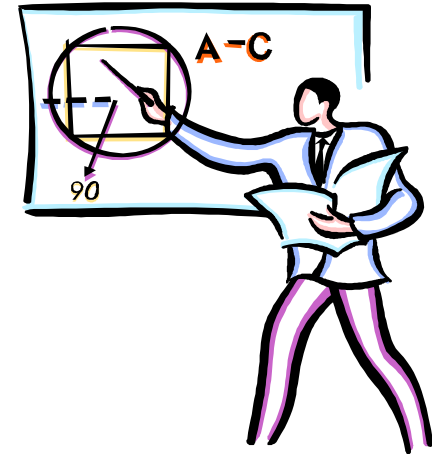
El modelo Monitor de Referencia (II)

- **Fuerzas**

- Definir las normas de autorización no es suficiente.
 - Debe aplicarse siempre que un sujeto formule una solicitud a un objeto protegido.
- Existen muchas posibles aplicaciones.
 - Necesitamos un modelo abstracto de ejecución.

- **Solución**

- Definir un proceso abstracto que intercepta todas las peticiones de recursos y controles para el cumplimiento de las autorizaciones.



El modelo Monitor de Referencia (III)

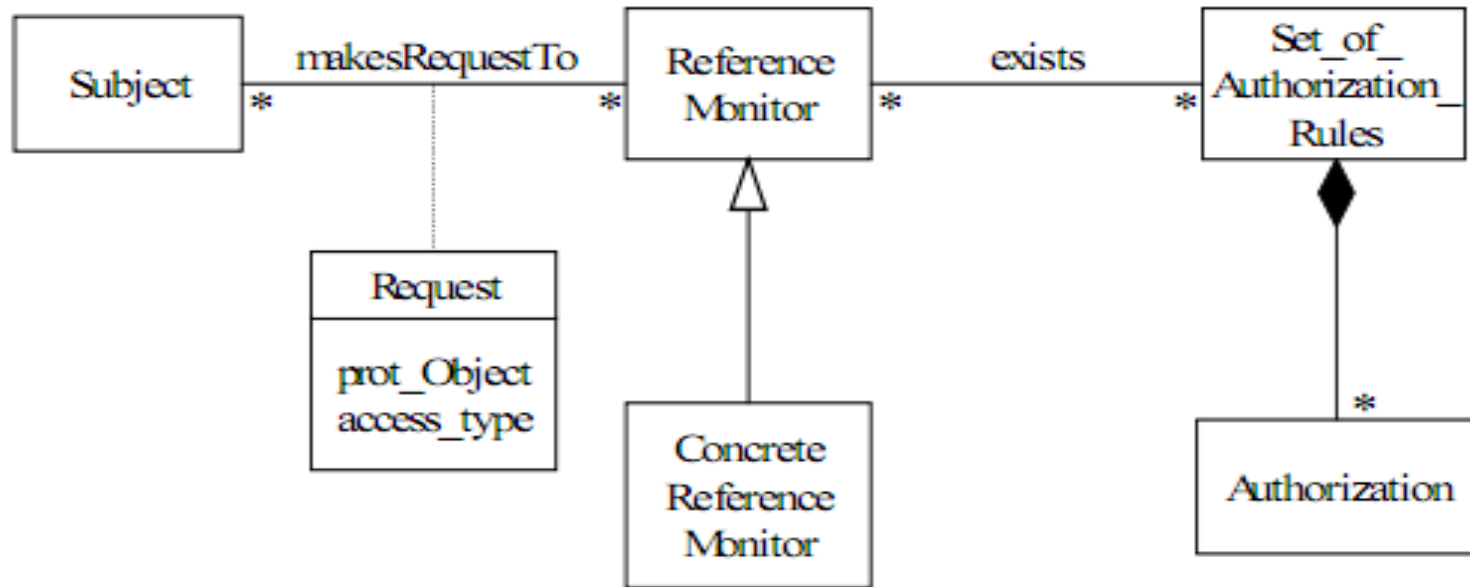


Figura 1.4: Class diagram for the reference mon

- Set_of_Authorization_Rules denota un conjunto de normas de autorización organizado de una manera conveniente.

El modelo Monitor de Referencia (IV)

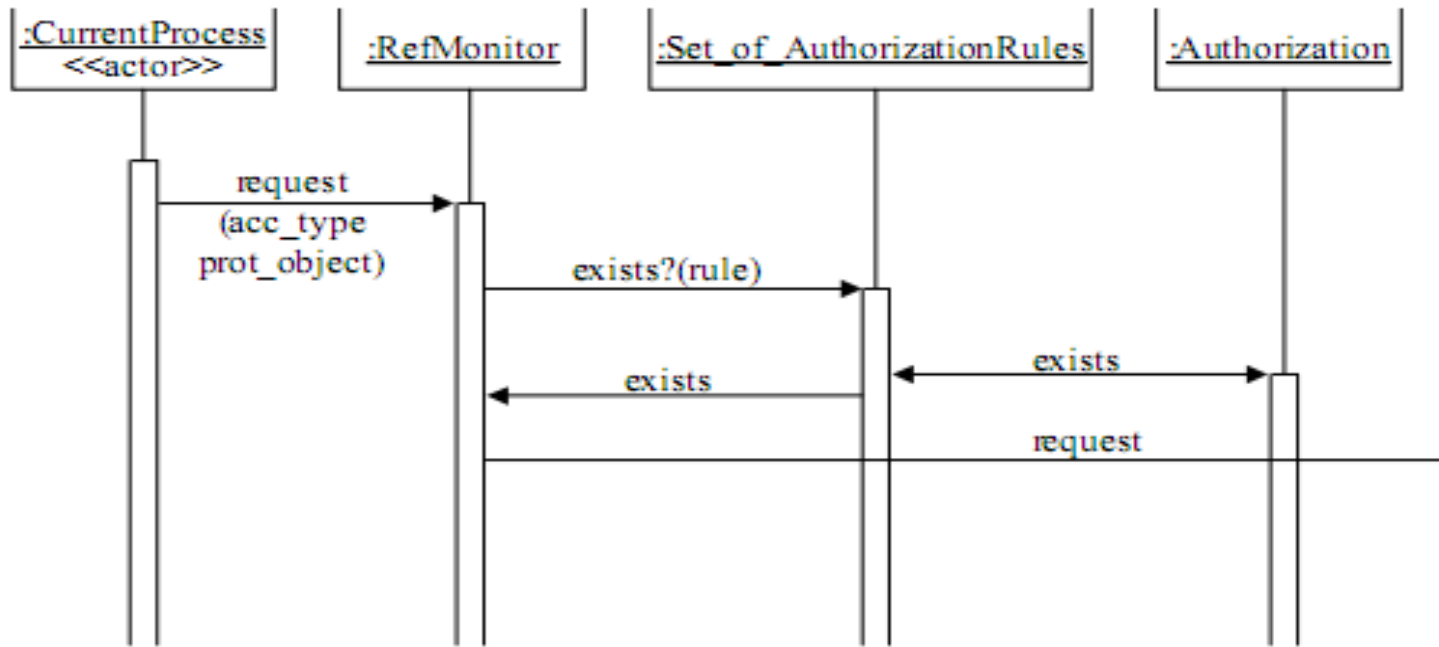
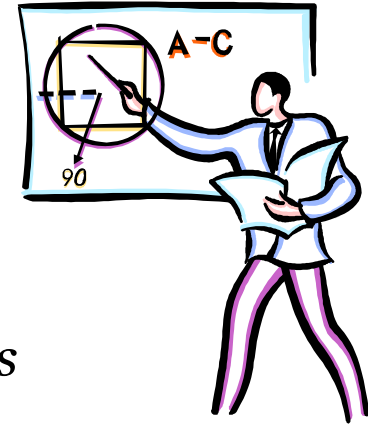


Figura 1.5: Sequence diagram for enforcing security of requests.

- Un diagrama de secuencia que muestra cómo se realiza la comprobación.

El modelo Monitor de Referencia (V)



- **Consecuencias**

- **Las ventajas incluyen:**

1. *Si se interceptan todas las peticiones, podemos asegurarnos de que cumplen las normas.*
2. *La aplicación no se ha limitado al uso de procesos abstractos.*

- **Las desventajas son:**

1. *Las implementaciones específicas son necesarios para cada tipo de recurso.*
2. *Comprobar cada solicitud puede resultar una pérdida de rendimiento intolerable.*

Muchas
Gracias

Bibliografía (I)

- Common Criteria home page. <http://csrc.nist.gov/cc>.
- Policy 200X: Workshop on Policies for Distributed Systems and Networks. <http://www-dse.doc.ic.ac.uk/events>.
- M. Andress. An overview of security policies. <http://searchsecurity.techtarget.com>, December 2002.
- S. Barman. Writing information security policies. New Riders Publ.,2002.
- D. Blacharski. Emerging Technology: Create order with a strong security policy. <http://www.networkmagazine.com/article/NMG20000710S0015>, Network Magazine, July 2000.
- D.E. Denning. Cryptography and data security. Addison-Wesley, 1982.
- E.B.Fernandez and J.C.Hawkins. Determining role rights from use cases. Procs. 2nd ACM Workshop on Role-Based Access Control, 121-125.<http://www.cse.fau.edu/ed/RBAC.pdf>, 1997.



Bibliografía (II)

- C.Wood; E.B.Fernandez; and R.C. Summers. Data base security: require-ments, policies, and models. IBM Systems Journal, vol. 19, No 2,229-252,1980.
- R. Sandhu et al. Role-Based Access Control models. Computer , vol. 29, No2,38-47, February 1996.
- E.B. Fernandez and R. Pan. A pattern language for security models. Procs. of PLoP 2001, <http://jerry.cs.uiuc.edu/plop/plop2001>, 2001.
- GMU Laboratory for Information Security Technology.
<http://www.list.gmu.edu>.
- J.B.D.Joshi; W.G.Aref; A. Ghafoor and E. H. Spafford. Security models for web-based applications. Comm. of the ACM, vol. 44, No. 2,38-44, February 2001.
- G.S. Graham and P. Denning. Protection: Principles and practice. AFIPS Conf. Procs., 40,SJCC, 417-429, 1972.
- H. Hosmer. Multiple security policies for business. Notes for a tutorial at the IFIP/SEC'95 Conference, 1995.



Bibliografía (III)

- Cano; Heimy J. Pautas y Recomendaciones para Elaborar Políticas de Seguridad Informática (PSI). Universidad de los Andes, Colombia, 1998.
- J.D.Moffett and M. Sloman. The source of authority for commercial access control. Computer, IEEE, 59-69, February 1988.
- W.E. Kuenhauser. A paradigm for user-defined security policies. Procs. of the 14th IEEE Symp. On Reliable Distributed Systems, 1995.
- W.E. Kuenhauser and M. von Kopp Ostrowski. A framework to support multiple security policies. Procs. of the 7th Annual Canadian Comp. Security Symp, 1995.
- B.W. Lampson. Protection. Procs. 5th Annual Conf. on Info. Sciences and Sys., 437-443. Reprinted in ACM Operating Sys. Review, 8, 1 (January 1974), 18-24, 1971, 1974.
- E. Lupu and M.Sloman. Conflict analysis for management policies. May 1997.
- E.B. Fernandez; R.C.Summers and T.Lang. Definition and evaluation of access rules in data management systems. Procs. First Int. Conf. On Very Large Databases, 268-285, Boston, MA, 1975.



Bibliografía (IV)

- E.B.Fernandez; R.C.Summers and C. Wood. Database security and integrity. Addison-Wesley, 1981.
- M. Schaefer. Reflections on current issues in trusted DBMS.ARCA Systems, August 1990.
- M. Sloman and E. Lupu. Security and management policy specification.IEEE Network,10-19, March/April 2002.
- L. Snyder. Formal models of capability-based protection systems.IEEETrans. on Computers, Vol. C-30, No 3,172-181, March 1981.
- J. Vijayan. Employee data exposed on web.
<http://www.computerworld.com>, Computerworld, Feb. 11, 2002.
- M.A. Harrison; W.L.Ruzzo; and J.D. Ullman. Protection in operating systems. Comm. of the ACM, 19, 461-471, 8 (August 1976).
- C.C. Wood. Information security policies made easy, Version 7.
<http://www.pentasafer.com/products/vsapolicybook.htm>, 2000.
- E. B. Fernandez; J. Wu and M. H. Fernandez. User group structures in object-oriented databases. Proc. 8th Annual IFIP W.G.11.3 Working Conference on Database Security, Bad Salzdetfurth, Germany, August 199

