UNIVERSIDAD PARAGUAYO ALEMANA

Ingeniería en Tecnologías de la Información Empresarial TIE

Seguridad en TICs

Prof.: Chrystian Ruiz Diaz

DISCLAIMER

Todo el contenido de esta presentación se proporciona **exclusivamente con fines didácticos y educativos en el ámbito académico**.

El uso inapropiado de las técnicas y/o conocimientos expuestos en esta presentación puede violar leyes nacionales e internacionales.

El autor y la institución educativa no se hacen responsables del uso indebido de la información contenida en esta presentación.

Se enfatiza que la información debe ser empleada únicamente para propósitos éticos, legales y con la debida autorización de las autoridades competentes.

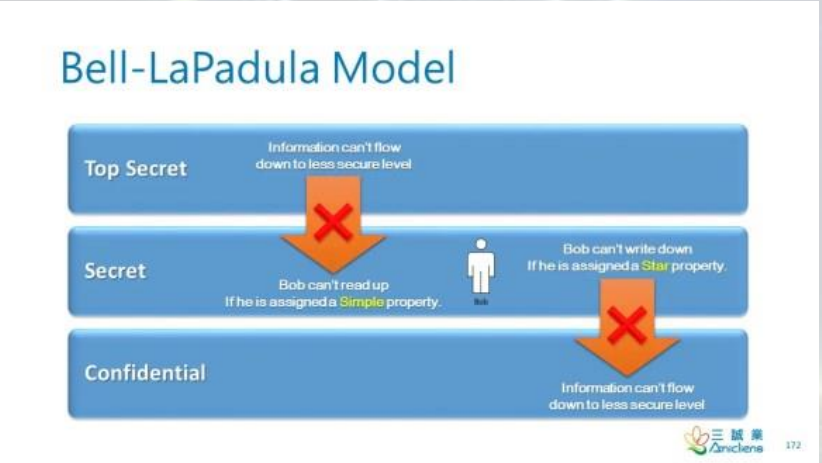
Contenido

Principios de Diseño y Modelos en Seguridad Informática

- ✓ **Bell-LaPadula (BLP)**: David Bell y Leonard LaPadula. 1970
- ✓ **BIBA**: Kenneth J. Biba. 1977
- ✓ **MAC**: Mandatory Access Control
- ✓ **DAC**: Discretionary Access Control

Modelo Bell-LaPadula (BLP)

- Desarrollado en la década de 1970 por David Bell y Leonard LaPadula.
- Enfoque en la **confidencialidad** de los datos.



Principios Clave:

- **No read up** (simple security property): Un sujeto en un nivel de seguridad no puede leer datos de un nivel más alto. Esto asegura que los usuarios no accedan a información clasificada superior a su nivel de autorización
- **No write down** (*-property): Un sujeto en un nivel de seguridad no puede escribir datos en un nivel más bajo. Esto previene la divulgación de información clasificada a niveles de menor seguridad.
- **Discreción** (discretionary security property): Control de acceso basado en matrices de acceso y listas de control de acceso (ACL), permitiendo a los propietarios de los objetos controlar el acceso a sus datos.

Matriz de Acceso

Sujeto/Objeto	Archivo1	Archivo2	Impresora1
Usuario1	Leer	Escribir	Usar
Usuario2	Leer	-	-
Usuario3	-	Leer	Usar

Listas de Control de Acceso (ACL)

- Cada objeto tiene una lista asociada que indica qué sujetos tienen qué derechos sobre él.
- Ejemplo:
  - **Archivo1**: {(Usuario1, Leer), (Usuario2, Leer)}
  - **Archivo2**: {(Usuario1, Escribir), (Usuario3, Leer)}
  - **Impresora1**: {(Usuario1, Usar), (Usuario3, Usar)}

Ejemplo del Modelo Bell-LaPadula

Contexto: Sistema militar con niveles de clasificación

Escenario:

- Coronel A: acceso a Top Secret
- Capitán B: acceso a Secreto
- Soldado C: acceso a Confidencial

- ***Top Secret.***
- ***Secreto***
- ***Confidencial***
- ***No Clasificado***

Aplicación del Modelo:

- **No read up**: El Soldado C no puede leer documentos Secreto o Top Secret
- **No write down**: El Coronel A no puede escribir información en documentos Confidencial o No Clasificado
- **Discreción**: El Coronel A puede decidir quién accede a sus documentos

Implementación y Aplicaciones de Bell-LaPadula

- Sistemas de defensa y entornos gubernamentales.

- Estructura jerárquica de niveles de seguridad.

- **Ventajas**:
- - Protección estricta de la confidencialidad
- - Uso en sistemas militares y gubernamentales

- **Desventajas**:
- - No aborda la integridad ni la disponibilidad
- - Complejidad en sistemas con múltiples niveles de seguridad

Limitaciones de Bell-LaPadula

- No aborda la integridad y la disponibilidad.
- Complejidad en sistemas con múltiples niveles de seguridad.

Ejemplo de Limitación:

- En un sistema financiero, mantener la confidencialidad es importante, pero también lo es asegurar que los datos no sean modificados indebidamente (integridad).

Solución:

- Complementar Bell-LaPadula con otros modelos como BIBA.

Modelo BIBA

- Propuesto por Kenneth J. Biba en 1977.
- Enfoque en la integridad de los datos.

Principios Clave:

- - No write up
- - No read down
- - Integridad de objetos (objec integrity axiom)

Ejemplo del Modelo BIBA

Escenario:

El Analista de Finanzas X tiene un nivel de integridad Alto.

El Supervisor de Finanzas Y tiene un nivel de integridad Medio.

El Asistente de Finanzas Z tiene un nivel de integridad Bajo.

Aplicación del Modelo:

No write up: El Asistente de Finanzas Z no puede modificar registros financieros de nivel Medio o Alto.

No read down: El Analista de Finanzas X no puede leer registros financieros de nivel Medio o Bajo.

Integridad de objetos: Solo el Analista de Finanzas X puede aprobar cambios finales en los registros financieros críticos.

Implementación y Aplicaciones de BIBA

- Sistemas financieros, control de calidad.

- Definición de niveles de integridad.

Ventajas:
- Asegura la integridad de los datos
- Previene la modificación indebida de información crítica

Desventajas:
- No aborda la confidencialidad
- Puede ser complejo en sistemas dinámicos con múltiples fuentes de datos

Limitaciones de BIBA

- No aborda la confidencialidad.
- Complejidad en sistemas dinámicos.

Ejemplo de Limitación:

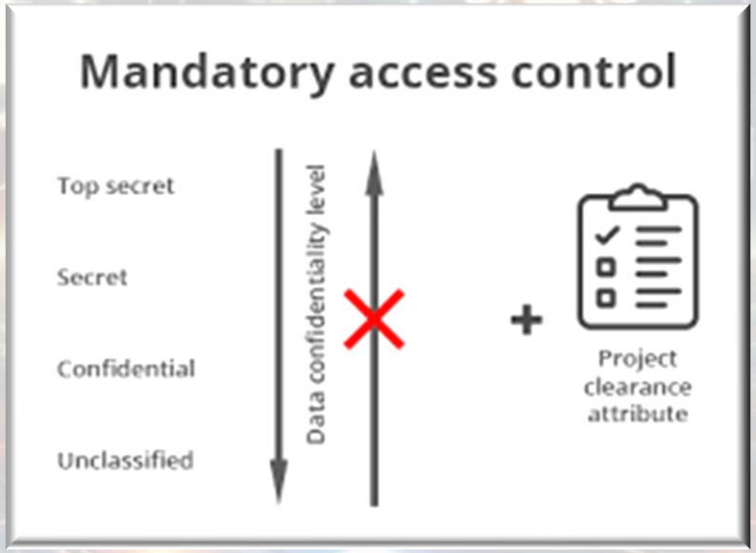
- En un entorno militar, es crucial mantener la confidencialidad además de la integridad. BIBA por sí solo no puede asegurar ambos aspectos.

Solución:

- Uso combinado con modelos de confidencialidad como Bell-LaPadula.

Control de Acceso Obligatorio (MAC)

- Políticas de acceso definidas por el administrador del sistema.
- Uso en entornos de alta seguridad.



Principios Clave:

- Etiquetas de seguridad
- Políticas estrictas

Ejemplo:

- Documentos y usuarios tienen etiquetas de seguridad (Pública, Confidencial, Secreta, Top Secret).
- Un documento marcado como Top Secret solo puede ser accedido por usuarios con etiqueta Top Secret.

Principios Clave de MAC

- Etiquetas de seguridad.
- Políticas estrictas.

Ventajas:
- Control centralizado y uniforme
- Ideal para entornos de alta seguridad

Desventajas:
- Menos flexible en comparación con DAC
- Menor usabilidad en sistemas dinámicos

Ejemplo del Modelo MAC

Contexto:

Un sistema de gestión de documentos clasificados en una agencia gubernamental

Escenario

- Documentos y usuarios tienen etiquetas de seguridad como: Pública, Confidencial, Secreta y Top Secret.
- Un documento marcado como Top Secret solo puede ser accedido por usuarios con etiqueta Top Secret.
- El acceso es controlado centralmente por el administrador del sistema.

Ejemplo del Modelo MAC

Aplicación del Modelo:

- **Etiquetas de seguridad:** Todos los documentos y usuarios tienen una etiqueta que indica su nivel de acceso.
- **Políticas estrictas:** Un usuario con etiqueta Confidencial no puede acceder a documentos marcados como Secreto o Top Secret, sin importar las preferencias del propietario del documento.

Implicaciones del Modelo MAC

Se asegura un control riguroso y centralizado sobre el acceso a la información, evitando accesos no autorizados a documentos clasificados.

Implementación y Aplicaciones de MAC

- Sistemas militares, gubernamentales.
- Sistema de etiquetado de seguridad.

Ventajas:

- Control centralizado y uniforme
- Ideal para entornos de alta seguridad

Desventajas:

- Menos flexible en comparación con DAC - *Discretionary Access Control*
- Menor usabilidad en sistemas dinámicos

Limitaciones de MAC

- Menor flexibilidad en comparación con DAC.
- Desafíos en sistemas dinámicos.

Ejemplo de Limitación:

- En sistemas empresariales, puede ser necesario un control de acceso más flexible para adaptarse a cambios rápidos.

Solución:

- Uso combinado con modelos más flexibles como DAC.

Control de Acceso Discrecional (DAC)

- Control de acceso definido por los usuarios finales.
- Uso en sistemas operativos y bases de datos.

Principios Clave:

- **Propiedad y control**: Los propietarios de los recursos pueden decidir quién tiene acceso a sus recursos y qué tipo de acceso se permite.

- **Listas de control de acceso (ACL):** Se utilizan para definir los permisos que los usuarios tienen sobre objetos específicos. Las ACL especifican qué usuarios o grupos de usuarios pueden acceder a un recurso y qué operaciones pueden realizar.

Control de Acceso Discrecional (DAC)

Contexto

Un sistema de archivos en una empresa.

Escenario

- Un archivo creado por el Usuario A tiene permisos que permiten al Usuario B leerlo y al Usuario C modificarlo.
- El Usuario A puede cambiar estos permisos en cualquier momento.

Principios Clave de DAC

- Propiedad y control.
- Listas de control de acceso (ACL).

Ventajas:
- Gran flexibilidad
- Permite a los propietarios controlar el acceso a sus recursos

Desventajas:
- Vulnerabilidad a ataques internos
- Complejidad en la administración de permisos en grandes sistemas

Ejemplo del Modelo DAC

Contexto

Un sistema de archivos en una empresa.

Escenario

Un archivo creado por el Usuario A tiene permisos que permiten al Usuario B leerlo y al Usuario C modificarlo.

El Usuario A puede cambiar estos permisos en cualquier momento

Aplicación del Modelo

Propiedad y control, Listas de control de acceso (ACL).

Implementación y Aplicaciones de DAC

- Sistemas operativos como UNIX y Windows.
- Bases de datos y aplicaciones empresariales.

Ventajas:

- - Gran flexibilidad
- - Permite a los propietarios controlar el acceso a sus recursos

Desventajas:

- - Vulnerabilidad a ataques internos
- - Complejidad en la administración de permisos en grandes sistemas

Limitaciones de DAC

- Vulnerabilidad a ataques internos.
- Complejidad en la administración de permisos en grandes sistemas.

Ejemplo de Limitación:

- En sistemas con muchos usuarios y recursos, administrar permisos puede volverse complicado y propenso a errores.

Solución:

- Uso de herramientas automatizadas para la gestión de permisos.

Comparación de los Modelos

Modelo/Principio	Bell-LaPadula (BLP)	BIBA	MAC (Mandatory Access Control)	DAC (Discretionary Access Control)
Enfoque Principal	Confidencialidad	Integridad	Control de acceso obligatorio	Control de acceso discrecional
Principios Clave	- No read up (simple security property)	- No write up	- Etiquetas de seguridad	- Propiedad y control
	- No write down (*-property, estrella property)	- No read down	- Políticas estrictas	- Listas de control de acceso (ACL)
	- Discreción (discretionary security property)	- Integridad de objetos (object integrity axiom)		
Acceso a Información	- Los sujetos no pueden leer información en niveles superiores	- Los sujetos no pueden leer información en niveles inferiores	- Controlado por el administrador del sistema	- Controlado por los propietarios de los recursos
	- Los sujetos no pueden escribir información en niveles inferiores	- Los sujetos no pueden escribir información en niveles superiores	- Basado en etiquetas de seguridad	- Basado en permisos definidos por los propietarios
Uso Común	Sistemas militares y gubernamentales	Sistemas que requieren alta integridad de datos	Entornos con alta seguridad	Sistemas operativos, bases de datos
Flexibilidad	Media	Media	Baja	Alta
Complejidad de Implementación	Alta	Alta	Alta	Media
Ejemplos de Aplicación	- Sistemas de defensa	- Sistemas financieros	- Sistemas militares	- Sistemas operativos como UNIX y Windows
	- Entornos gubernamentales	- Sistemas de control de calidad	- Entornos gubernamentales	- Bases de datos

¿PREGUNTAS?

Referencias

- - Bishop, Matt. Computer Security: Art and Science.
- - Pfleeger, Charles P., y Shari Lawrence Pfleeger. Security in Computing.
- - Stamp, Mark. Information Security: Principles and Practice.
- - Sandhu, Ravi S., y Pierangela Samarati. Access Control: Principles and Practice.
- - Biba, Kenneth J. Integrity Considerations for Secure Computer Systems.
- - Bell, David Elliott, y Leonard J. LaPadula. Secure Computer System: Unified Exposition and Multics Interpretation.

Actividad de Proceso

Muchas Gracias..!!