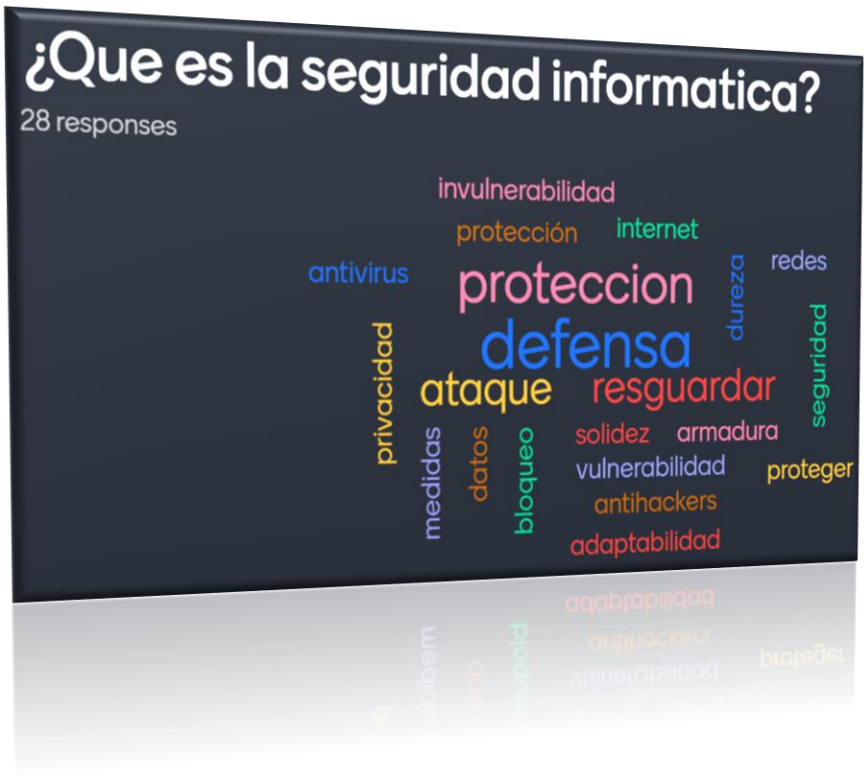
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

Principios de Diseño y Modelos en Seguridad Informática: Bell-LaPadula, BIBA, MAC y DAC

Introducción

Los principios de diseño y los modelos de seguridad informática son esenciales para la protección de datos y recursos en sistemas informáticos. Entre los modelos más importantes y utilizados se encuentran Bell-LaPadula, BIBA, MAC (Mandatory Access Control) y DAC (Discretionary Access Control). Este documento proporciona una visión extensa y detallada de cada uno de estos modelos, destacando sus principios, características, aplicaciones, limitaciones y ejemplos detallados.

1. Modelo Bell-LaPadula (BLP)

1.1 Introducción

El modelo Bell-LaPadula, desarrollado por David Bell y Leonard LaPadula en la década de 1970, se enfoca en mantener la confidencialidad de los datos en sistemas de seguridad. Es uno de los modelos más antiguos y ampliamente utilizados, especialmente en entornos militares y gubernamentales.

1.2 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, estrella 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.

1.3 Ejemplo Detallado

Contexto: Un sistema militar con varios niveles de clasificación:

- Top Secret.
- Secreto
- Confidencial
- No Clasificado

Escenario:

- El Coronel A tiene autorización para acceder a información de nivel Top Secret.
- El Capitán B tiene autorización para acceder a información de nivel Secreto.
- El Soldado C tiene autorización para acceder a información de nivel Confidencial.

Aplicación del Modelo:

- **No read up:** El Soldado C no puede leer documentos clasificados como Secreto o Top Secret.
- **No write down:** El Coronel A no puede escribir información en documentos clasificados como Secreto, Confidencial o No Clasificado.
- **Discreción:** El Coronel A puede decidir quién puede acceder a los documentos que él crea, siempre y cuando no viole las reglas de no write down y no read up.

Implicaciones:

- Se asegura que la información más sensible (Top Secret) no sea accesible para personal de menor nivel de seguridad, y que dicha información no se filtre a documentos de menor clasificación.

1.4 Implementación y Aplicaciones

El modelo Bell-LaPadula se implementa comúnmente en sistemas donde la confidencialidad es crítica. Ejemplos incluyen sistemas de defensa y entornos gubernamentales que manejan información clasificada. La implementación requiere una estructura jerárquica de niveles de seguridad y mecanismos estrictos para controlar el flujo de información entre estos niveles.

1.5 Limitaciones

El modelo Bell-LaPadula se centra únicamente en la confidencialidad y no aborda otros aspectos importantes de la seguridad como la integridad y la disponibilidad. Además, su aplicación puede ser compleja en sistemas con múltiples niveles de seguridad y en entornos dinámicos donde los niveles de seguridad pueden cambiar frecuentemente.

---

2. Modelo BIBA

2.1 Introducción

El modelo BIBA, propuesto por Kenneth J. Biba en 1977, se enfoca en mantener la integridad de los datos en sistemas de seguridad. Este modelo se desarrolló como una respuesta a la limitación del modelo Bell-LaPadula, que no aborda la integridad de los datos.

2.2 Principios Clave

- **No write up:** Un sujeto en un nivel de integridad no puede escribir datos en un nivel más alto. Esto asegura que los datos no sean contaminados por usuarios de menor integridad.
- **No read down:** Un sujeto en un nivel de integridad no puede leer datos de un nivel más bajo. Esto previene que los datos de alta integridad sean influenciados por información de menor integridad.
- **Integridad de objetos (object integrity axiom):** La integridad de los objetos se mantiene mediante restricciones en las operaciones permitidas, asegurando que solo los usuarios autorizados puedan modificar los datos.

2.3 Ejemplo Detallado

Contexto: Un sistema financiero con niveles de integridad: Alta, Media y Baja.

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.

Implicaciones:

- Se asegura que los datos financieros críticos solo puedan ser modificados por personal con el nivel adecuado de integridad, previniendo alteraciones indebidas y manteniendo la confianza en los registros.

2.4 Implementación y Aplicaciones

El modelo BIBA se utiliza en sistemas donde la integridad de los datos es primordial. Ejemplos incluyen sistemas financieros, sistemas de control de calidad y entornos donde es crucial asegurar que los datos no sean alterados de manera indebida. La implementación requiere definir niveles de integridad y aplicar políticas estrictas para controlar las operaciones de lectura y escritura entre estos niveles.

2.5 Limitaciones

El modelo BIBA no aborda la confidencialidad de los datos, centrándose exclusivamente en la integridad. Esto lo hace menos adecuado para sistemas donde la

confidencialidad y la integridad son igualmente importantes. Además, puede ser complejo de implementar en sistemas dinámicos con múltiples fuentes de datos.

---

3. Control de Acceso Obligatorio (MAC)

3.1 Introducción

El Control de Acceso Obligatorio (Mandatory Access Control, MAC) es un enfoque en el que las políticas de acceso son definidas por un administrador del sistema y no pueden ser modificadas por los usuarios finales. MAC se utiliza en entornos donde la seguridad es crítica y se requiere un control estricto sobre el acceso a los recursos.

3.2 Principios Clave

- **Etiquetas de seguridad:** Cada objeto y sujeto en el sistema tiene una etiqueta de seguridad que determina su nivel de acceso.
- **Políticas estrictas:** Las reglas de acceso son definidas por el sistema y no pueden ser cambiadas por los usuarios. Esto asegura un control centralizado y uniforme sobre el acceso a los recursos.

3.3 Ejemplo Detallado

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.

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:

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

3.4 Implementación y Aplicaciones

MAC se implementa comúnmente en sistemas militares, gubernamentales y entornos de alta seguridad donde es crucial prevenir accesos no autorizados. La implementación requiere un sistema de etiquetado de seguridad y mecanismos para aplicar políticas de acceso basadas en estas etiquetas.

3.5 Limitaciones

MAC puede ser rígido y menos flexible en comparación con otros modelos de control de acceso como DAC. Esto puede llevar a una menor usabilidad y a desafíos en la administración de usuarios y recursos en sistemas dinámicos y heterogéneos.

---

4. Control de Acceso Discrecional (DAC)

4.1 Introducción

El Control de Acceso Discrecional (Discretionary Access Control, DAC) permite a los usuarios finales controlar el acceso a sus propios recursos. Es el modelo de control de acceso más flexible y comúnmente usado en sistemas operativos y bases de datos.

4.2 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.

4.3 Ejemplo Detallado

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:** El Usuario A, como propietario del archivo, puede decidir y modificar quién puede leer o escribir en su archivo.
- **Listas de control de acceso (ACL):** La ACL del archivo especifica que el Usuario B tiene permisos de lectura y el Usuario C tiene permisos de escritura.

Implicaciones:

- Proporciona una gran flexibilidad y control a los propietarios de los recursos, permitiéndoles gestionar quién tiene acceso a su información.

4.4 Implementación y Aplicaciones

DAC se utiliza ampliamente en sistemas operativos como UNIX y Windows, así como en bases de datos y aplicaciones empresariales. La implementación implica el uso de listas de control de acceso y permisos definidos por los propietarios de los recursos.

4.5 Limitaciones

DAC puede ser vulnerable a ataques internos, ya que los usuarios tienen la capacidad de modificar los permisos de acceso. Esto puede llevar a una menor seguridad en comparación con modelos como MAC. Además, la administración de permisos en grandes sistemas puede ser compleja y propensa a errores.

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	- Los sujetos no	- Controlado por	- Controlado por

Modelo/ Principio	Bell-LaPadula (BLP)	BIBA	MAC (Mandatory Access Control)	DAC (Discretionary Access Control)
	leer información en niveles superiores	pueden leer información en niveles inferiores	el administrador del sistema	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

Referencias

1. Bishop, Matt. *Computer Security: Art and Science*. Addison-Wesley Professional, 2018.
2. Pfleeger, Charles P., y Shari Lawrence Pfleeger. *Security in Computing*. Prentice Hall, 2018.

3. Stamp, Mark. *Information Security: Principles and Practice*. Wiley, 2011.
4. Sandhu, Ravi S., y Pierangela Samarati. "Access Control: Principles and Practice." *IEEE Communications Magazine,* vol. 32, no. 9, 1994, pp. 40-48.
5. Biba, Kenneth J. "Integrity Considerations for Secure Computer Systems." *MITRE Corporation*, 1977.
6. Bell, David Elliott, y Leonard J. LaPadula. "Secure Computer System: Unified Exposition and Multics Interpretation." *MITRE Corporation*, 1976.

