Alumno: Rodrigo Vila

Experto Universitario en Seguridad de la Información

Modulo 6 Unidad 3: Diseño y arquitectura de seguridad

Ejercicio Número 1 Unidad 3

Explicar un modelo de seguridad a elección y mediante un pequeño resumen, explicarlo.

✓ Bell-LaPadula

✓ Biba

✓ Clark & Wilson

✓ “Brewer & Nash” - Chinese Wall (Muralla China)

✓ Lattice (Enrejado)

✓ State machine (Máquina de estados)

✓ Information flow (Flujo de información)

✓ Non-interference (No-interferencia)

✓ Access Matrix (Matriz de accesos)

Breve resumen de cada modelo mencionado:

1. Modelo Bell-LaPadula

- **Objetivo:** Asegura la confidencialidad de la información.
- **Características:**
  - Basado en controles de acceso obligatorios.
  - Principios clave:
    - **No lectura hacia arriba (No Read Up - Simple Security Property):** Un sujeto en un nivel de seguridad no puede leer datos de un nivel superior.
    - **No escritura hacia abajo (No Write Down - -Property):* Un sujeto en un nivel de seguridad no puede escribir datos a un nivel inferior.

- **Aplicación:** Común en entornos militares y gubernamentales donde la confidencialidad es crítica.

2. Modelo Biba

- **Objetivo:** Asegura la integridad de la información.
- **Características:**
    - Inverso al modelo Bell-LaPadula.
    - Principios clave:
        - **No lectura hacia abajo (No Read Down):** Un sujeto no puede leer datos de un nivel inferior.
        - **No escritura hacia arriba (No Write Up):** Un sujeto no puede escribir datos a un nivel superior.
- **Aplicación:** Utilizado en sistemas donde la integridad de los datos es más importante que la confidencialidad, como en sistemas financieros.

3. Modelo Clark & Wilson

- **Objetivo:** Mantener la integridad de la información a través de la separación de tareas y controles de acceso.
- **Características:**
    - Define transacciones bien formadas y la necesidad de separación de tareas.
    - Utiliza **Conjunto de reglas de integridad:** para garantizar que solo las transacciones autorizadas pueden realizar cambios en los datos.
    - **Transformación certificada y verificación certificada:** son claves en este modelo.
- **Aplicación:** Común en entornos comerciales y financieros.

4. Modelo Brewer & Nash (Muralla China)

- **Objetivo:** Evitar conflictos de interés en sistemas de información.
- **Características:**
    - Restringe el acceso basado en conflictos de interés.
    - Los usuarios solo pueden acceder a conjuntos de datos no relacionados con su trabajo actual para evitar un conflicto de interés.
- **Aplicación:** Utilizado en entornos donde la separación de datos por conflictos de interés es crítica, como en bufetes de abogados y firmas de consultoría.

5. Modelo Lattice (Enrejado)

- **Objetivo:** Establecer una estructura jerárquica de acceso a la información.

- **Características:**
    - Organiza los niveles de acceso en una estructura enrejada.
    - Proporciona un marco matemático para definir relaciones de seguridad entre diferentes niveles de acceso.
- **Aplicación:** Ideal para sistemas con múltiples niveles de clasificación de datos.

6. Modelo de Máquina de Estados (State Machine)

- **Objetivo:** Describir el comportamiento del sistema en diferentes estados.
- **Características:**
    - Basado en la idea de que el sistema de seguridad puede representarse mediante una máquina de estados.
    - Cada estado del sistema debe ser seguro, y las transiciones entre estados también deben ser seguras.
- **Aplicación:** Aplicable en sistemas donde la seguridad depende de mantener un estado consistente y seguro.

7. Modelo de Flujo de Información (Information Flow)

- **Objetivo:** Controlar cómo fluye la información entre diferentes niveles de seguridad.
- **Características:**
    - Asegura que la información no fluya desde un nivel de seguridad más alto a uno más bajo de manera no controlada.
    - Puede integrarse con otros modelos como Bell-LaPadula y Biba.
- **Aplicación:** Utilizado en sistemas donde es crucial controlar la dirección del flujo de información.

8. Modelo de No-interferencia (Non-interference)

- **Objetivo:** Garantizar que las acciones de los usuarios en un nivel no interfieran con los usuarios en otro nivel.
- **Características:**
    - Asegura que la actividad en un nivel no tenga ningún efecto observable en otro nivel.
    - Ideal para entornos multiseguro.
- **Aplicación:** Común en sistemas donde se necesita una estricta separación de niveles de seguridad.

9. Modelo de Matriz de Accesos (Access Matrix)

- **Objetivo:** Gestionar los permisos de acceso de usuarios a los recursos.

- **Características:**
    - Define una matriz donde las filas representan sujetos (usuarios) y las columnas representan objetos (recursos).
    - Cada celda de la matriz indica los tipos de acceso permitidos.
- **Aplicación:** Base para sistemas de control de acceso discrecional (DAC).

La elección del modelo depende de los requisitos específicos del sistema, como la prioridad en confidencialidad, integridad o separación de tareas.

Poniendo como prioridad la confidencialidad de la información, el modelo Bell-LaPadula parece ser el más adecuado.

Explicación:

El Modelo Bell-LaPadula es uno de los modelos de seguridad más antiguos y ampliamente utilizados en sistemas de información, especialmente en contextos donde la confidencialidad es de suma importancia, como en entornos militares y gubernamentales.

Historia y Contexto

El modelo fue desarrollado en la década de 1970 por David Elliott Bell y Leonard J. LaPadula, quienes trabajaban en el Departamento de Defensa de los Estados Unidos. Fue diseñado en respuesta a la necesidad de formalizar un marco de seguridad que garantizara que la información clasificada no fuera accedida o divulgada por personas no autorizadas.

Fundamentos del Modelo Bell-LaPadula

El Modelo Bell-LaPadula es un modelo de control de acceso basado en la teoría de sistemas formales, que se centra exclusivamente en la confidencialidad de la información. Se basa en la idea de niveles de seguridad que categorizan tanto a los usuarios (sujetos) como a la información (objetos). Los niveles de seguridad pueden ser, por ejemplo, "No clasificado", "Confidencial", "Secreto", y "Altamente Secreto".

Principios Clave

El modelo establece dos principios fundamentales para garantizar la confidencialidad:

1. No lectura hacia arriba (Simple Security Property o "No Read Up"):
    - Un sujeto (usuario) en un nivel de seguridad específico no puede leer información de un nivel superior.
    - Ejemplo: Un usuario con nivel "Confidencial" no puede acceder a un documento etiquetado como "Secreto". Esto asegura que la información

más sensible no se exponga a usuarios que no tienen la autorización adecuada.

2. No escritura hacia abajo (Star Property o *-Property, también conocida como "No Write Down"):
    - Un sujeto no puede escribir información en un nivel de seguridad inferior al que posee.
    - Ejemplo: Un usuario con acceso a información "Secreta" no puede escribir o copiar esa información en un documento que esté clasificado como "Confidencial". Esto previene que la información sensible se degrade a un nivel de seguridad inferior, donde podría estar menos protegida y ser accesible por personas con menor autorización.

Propiedad Discrecional de Seguridad (Discretionary Security Property)

Además de las dos propiedades principales, el Modelo Bell-LaPadula también contempla la Propiedad Discrecional de Seguridad, que permite a un sujeto con un permiso discrecional controlar el acceso a los objetos que posee. Esto se refiere a los controles de acceso discrecionales (DAC), donde el propietario del recurso puede decidir quién más puede acceder a él.

Formalización y Aplicación

El modelo se formaliza a través de una Máquina de Estados Finita, en la cual cada estado del sistema representa un conjunto de condiciones de seguridad. Las transiciones entre estados deben cumplir con las propiedades del modelo para garantizar que el sistema se mantenga en un estado seguro.

Aplicaciones Típicas

- Sistemas de Defensa y Gobierno: Donde la información clasificada es crítica, y cualquier fuga de información puede tener consecuencias graves.
- Entornos Corporativos de Alta Seguridad: Donde se manejan datos sensibles que requieren estrictos controles de acceso.

Ventajas y Limitaciones

Ventajas:

- Proporciona un marco claro y riguroso para proteger la confidencialidad de la información.
- Es sencillo de entender y aplicar en entornos donde la clasificación de la información es jerárquica y clara.

Limitaciones:

- Enfoque Unidimensional: Se enfoca exclusivamente en la confidencialidad, sin considerar otros aspectos críticos como la integridad o la disponibilidad.

- Rigidez: Su rigidez puede ser un inconveniente en entornos dinámicos donde los niveles de acceso pueden necesitar ajustes más flexibles.
- No aplica bien en situaciones donde la integridad es prioritaria, como en el caso de sistemas financieros o médicos, donde asegurar la exactitud y la consistencia de los datos es tan importante como proteger su confidencialidad.

Conclusión

El Modelo Bell-LaPadula sigue siendo un pilar en la teoría de la seguridad de la información, proporcionando un marco robusto para la protección de la confidencialidad. Sin embargo, debe ser complementado con otros modelos y controles para cubrir los diferentes aspectos de la seguridad, como la integridad y la disponibilidad, que son igualmente importantes en muchos entornos de TI.

Rodrigo Vila.-