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.

Seguridad Multilateral

Contenido

- Compartimentación
- Muro Chino
- Modelo BMA

Introducción

- La seguridad multilateral tiene como objetivo evitar la fuga de información 'a través' de departamentos (**horizontal**) en lugar de 'hacia abajo' (**vertical**) en una jerarquía. Esto es crucial en aplicaciones como la atención médica y la inteligencia nacional.
- Ejemplo: Los registros médicos en línea, como Microsoft HealthVault, plantean riesgos de acceso no autorizado por parte de aseguradoras y agencias gubernamentales.

Introducción

Figure 9.1: Multilevel security

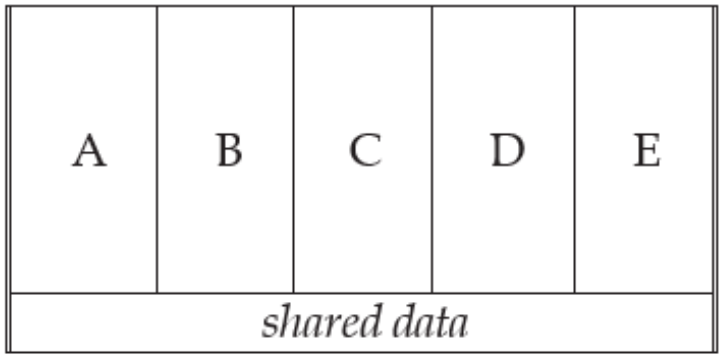

Figure 9.2: Multilateral security

Compartimentación, el Muro Chino y el Modelo de la BMA

- Se exploran tres modelos de seguridad multilateral: la compartimentación, el Muro Chino y el Modelo de la BMA, cada uno con aplicaciones específicas.

Compartimentación

La compartimentación es una práctica utilizada por los gobiernos para restringir el acceso a información sensible mediante el **uso de palabras clave**, además de clasificaciones tradicionales. Este método se ha empleado para proteger datos que, si se filtraran, podrían comprometer fuentes y métodos de inteligencia.

Funcionamiento

- **Creación de Compartimentos:** La información se divide en compartimentos, cada uno etiquetado con palabras clave y clasificaciones de seguridad.
- **Asignación de Accesos:** Los usuarios reciben autorizaciones específicas para acceder a ciertos compartimentos. Por ejemplo, solo el personal autorizado con la clave "Ultra" puede acceder a información etiquetada como "Ultra Secreto".
- **Control de Acceso:** Los usuarios solo pueden acceder a la información de los compartimentos para los cuales tienen autorización. Esto minimiza el riesgo de que información sensible caiga en manos no autorizadas.
- **Reglas de Manejo:** Se implementan reglas estrictas para el manejo y acceso a los compartimentos. Por ejemplo, ciertos documentos pueden requerir que solo personas específicas los manejen bajo condiciones específicas.

Ejemplo Histórico: Palabra Clave Ultra

Durante la **Segunda Guerra Mundial**, la palabra clave "**Ultra**" se utilizó para las descifraciones de mensajes alemanes codificados con la máquina Enigma. La protección de esta información era crítica, por lo que solo un pequeño grupo de personas, incluyendo criptanalistas y líderes aliados, tenía acceso. Se implementaron **estrictas reglas de manejo para evitar que el enemigo sospechara que su cifrado había sido roto**. Este alto nivel de seguridad se mantuvo mediante autorizaciones restringidas y políticas de manejo especiales.

Prácticas Modernas

Hoy en día, se toman medidas similares para proteger información que podría exponer fuentes o métodos de inteligencia. **La proliferación de palabras clave ha resultado en numerosos compartimentos de información, especialmente en niveles de clasificación altos, como "Ultra Secreto“**

Cada combinación de palabras clave forma un compartimento específico, lo que complica la gestión de accesos. Esto ha llevado a situaciones donde la acumulación de accesos puede **resultar en grandes vulnerabilidades, como el caso del oficial de la CIA Aldrich Ames**.

El Muro Chino

- Previene conflictos de interés dentro de firmas de servicios financieros mediante la separación estricta de departamentos que manejan información sensible.
- Ejemplo: Un abogado que trabaja para una compañía petrolera no puede trabajar para otra compañía del mismo sector.

Funcionamiento

- **Separación de Funciones:** Se separan físicamente y lógicamente las funciones dentro de una organización para evitar que el mismo grupo de personas acceda a información que podría generar un conflicto de interés.
- **Restricción de Acceso:** Los empleados en una unidad específica no pueden acceder a información de otra unidad que podría generar un conflicto de interés. Por ejemplo, en una firma financiera, los empleados del departamento de investigación no pueden acceder a información del departamento de ventas.
- **Monitoreo y Auditoría:** Se monitorean y auditan regularmente los accesos y flujos de información para asegurarse de que las políticas de separación se cumplan.
- **Reglas de Negocio:** Se implementan reglas estrictas para definir qué información puede ser accedida por qué departamentos y bajo qué condiciones.

El Modelo de la BMA

- Desarrollado para sistemas de información médica, asegura que los registros médicos estén accesibles solo para personal autorizado, siguiendo principios éticos y legales.
- Ejemplo: Un médico puede acceder a los registros de un paciente solo si está en la lista de control de acceso y ha obtenido el consentimiento del paciente.

Funcionamiento

- **Asignación de Clasificaciones:** Los sujetos (usuarios) y objetos (datos) se asignan a diferentes niveles de clasificación de seguridad. Ejemplos de clasificaciones incluyen "Confidencial", "Secreto" y "Ultra Secreto".
- **Reglas de Acceso:**
  - **Condición Simple de Seguridad:** Un sujeto puede leer un objeto si el nivel de clasificación del objeto es menor o igual al nivel de autorización del sujeto y si el acceso discrecional lo permite.
  - **Regla de Estrella (*):** Un sujeto solo puede escribir en un objeto si el nivel de clasificación del objeto es mayor o igual al nivel de autorización del sujeto.
- **Estructura de Lattice:** Utiliza una estructura matemática de lattice para definir y gestionar las relaciones de dominancia entre diferentes niveles de clasificación. Esta estructura asegura que no haya flujo de información no autorizado entre niveles incompatibles.
- **Control de Acceso Combinado:** Combina controles obligatorios (basados en clasificaciones de seguridad) con controles discrecionales (basados en permisos específicos).

Cuestiones Actuales de Privacidad

- Discuten problemas contemporáneos en la privacidad de los datos médicos, especialmente con la centralización y acceso por terceros.
- **Ejemplo**: Los registros electrónicos de pacientes en el Reino Unido que permiten acceso amplio para investigación y gestión del servicio de salud.

Problemas Básicos del Control de Inferencias

- El control de **inferencias** busca evitar que las consultas estadísticas revelen información sensible sobre individuos.
- **Ejemplo**: Una consulta sobre mujeres de 36 años con hijas de 14 y 16 años con psoriasis puede identificar a un individuo específico.

Otras Aplicaciones del Control de Inferencias

- El control de inferencias se aplica también en datos censales y comerciales, donde la privacidad es crucial.
- **Ejemplo**: Los datos del censo deben protegerse para evitar que se identifiquen individuos basándose en atributos como edad, ingresos y educación.

La Teoría del Control de Inferencias

- Se presenta la teoría que guía el control de inferencias, incluyendo técnicas como la supresión de celdas y la aleatorización.
- **Ejemplo**: En bases de datos de salud, se suprimen datos de enfermedades raras en estadísticas locales para evitar la identificación de pacientes.

Limitaciones de los Enfoques Genéricos

- Discuten las limitaciones inherentes a los enfoques genéricos de control de inferencias y su efectividad variable según el contexto.
- Ejemplo: La desidentificación de datos puede ser ineficaz si los registros detallados permiten la reidentificación de individuos.

Desidentificación vs Anonimizacion

El Problema Residual

- Aborda la dificultad de gestionar la privacidad en sistemas complejos y la necesidad de políticas adecuadas.
- Ejemplo: La retención de copias de registros médicos por aseguradoras y empleadores presenta un riesgo continuo para la privacidad de los pacientes.

Relación

Aspecto	Compartimentación	Muro Chino	Modelo de la BMA (Bell-LaPadula Modelo de Lattice)
Definición	Restricción del acceso a información mediante palabras clave y clasificaciones adicionales.	Separación de funciones y flujos de información dentro de una organización para evitar conflictos de interés.	Modelo de seguridad que combina controles de acceso obligatorios y discrecionales basado en clasificaciones de confidencialidad.
Objetivo	Proteger información sensible limitando el acceso a personal autorizado.	Evitar el uso indebido de información confidencial dentro de una organización.	Prevenir el flujo no autorizado de información entre diferentes niveles de seguridad.
Aplicación	Utilizado en sectores gubernamentales y militares.	Común en el sector financiero y corporativo.	Utilizado en sistemas militares y gubernamentales para la protección de datos sensibles.
Método de Control	Uso de palabras clave y clasificaciones para crear compartimentos de información.	Separación física y lógica de unidades dentro de una organización.	Uso de niveles de clasificación y etiquetas para definir permisos de acceso.
Ejemplo Histórico	Uso de la palabra clave "Ultra" durante la Segunda Guerra Mundial para proteger descifraciones de Enigma.	Separación de departamentos de investigación y ventas en una empresa financiera.	Prohibición de lectura y escritura entre niveles diferentes de seguridad.

Relación

Aspecto	Compartimentación	Muro Chino	Modelo de la BMA (Bell-LaPadula Modelo de Lattice)
Ventajas	Alta seguridad y protección de información crítica.	Minimiza el riesgo de conflictos de interés y mal uso de información interna.	Claridad y estructura en la gestión de accesos, reduciendo el riesgo de fuga de información.
Desventajas	Complejidad en la gestión de numerosos compartimentos y accesos.	Puede generar ineficiencias y falta de comunicación dentro de la organización.	Puede ser rígido y difícil de implementar en entornos con alta interdependencia de datos.
Modelo Matemático	No especificado.	No especificado.	Basado en estructuras de lattice (rejilla) para gestionar permisos de acceso.
Control de Acceso	Basado en la combinación de autorizaciones y palabras clave.	Basado en la separación de roles y funciones.	Basado en el control de acceso obligatorio y discrecional.
Nivel de Flexibilidad	Moderado; necesita gestión rigurosa.	Moderado; depende de la estructura organizacional.	Estricto; basado en reglas predefinidas de acceso.

UPA
UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN

¿PREGUNTAS?

Actividad de Proceso

Referencias

ESCRIVA, G. R. (2013). *Seguridad informática*. España: Macmillan Iberia SA.

UPA
UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN

Muchas Gracias..!!