Criptografía y Seguridad *(72.44)*

GUÍA 6: MODELOS DE CONFIDENCIALIDAD E INTEGRIDAD - SOLUCIONES

Ejercicio 1:

a. Tamara puede leer legajos de personal y, si tiene permiso para leer archivos de correo, también puede hacerlo.
b. Simón no puede leer legajos porque no puede leer algo de mayor nivel de confidencialidad (Bell Lapadula protege la confidencialidad). Puede escribir legajos de personal sólo si está habilitado (discrecionalmente) para hacerlo.
c. Clara, por más que tenga el permiso de lectura para archivos de correo electrónico, no puede hacerlo porque ella tiene un nivel de seguridad inferior.
d. Vladimir puede leer la guía siempre que tenga el permiso discrecional para hacerlo.

Ejercicio 2:

a. (TS,{A,C}) **no** domina a(S, {B,C}) →No puede hacer nada
b. (C,{C}) **no** domina a (C,{B})→No puede hacer nada
c. (S,{C}) **domina** a (C,{C})→puede leer
d. (TS,{A,C}) **domina** a (C,{A})→puede leer
e. (U) **es dominado por** (C,{B})→puede escribir.

Ejercicio 3:

a. La secuencia de lecturas y escrituras que pueden usarse para transferir datos de A hacia B desclasificando ***(canal encubierto)*** es:
   - Antonio lee datos de A y los copia en F, archivo que él creó en alto nivel.
   - Antonio puede desclasificar F. Desclasifica F a bajo nivel.
   - Beto puede leer o_A y copiarlo en B.
b. En este caso la secuencia NO existe. Sólo Antonio puede leer en A y sólo puede escribir objetos de Alto Nivel. Si los eleva de clasificación, Beto no podrá leerlos (sólo puede leer archivos de menor o igual nivel)

Ejercicio 4:

a. Sí, está permitida. Bob escribe en nivel confidencial, entonces Alice puede leer (porque puede leer hacia un nivel menor)
b. No, no está permitida. Alice escribe a nivel secreto. Bob no puede leer nivel secreto.
c. Sí, está permitida. Bob escribió, entonces el documento es confidencial, entonces Alice puede leerlo. ¿Puede escribirlo en el nivel de Alice? Sí.
d. No, no está permitida. Alice escribe a nivel secreto o superior. Entonces Bob no puede leerlo. Alice no puede escribir a un nivel más bajo. Entonces no hay forma que lo envíe a Bob.
e. Sí, está permitido.
f. Sí, está permitido. Bob puede leer un nivel mas bajo y puede escribirlo al nivel de Alice.

Ejercicio 5:

Low Mark:

1. s1 baja a pri{admin.}
2. ok
3. s1 baja a public
4. no puede
5. ok
6. s2 baja a public
7. no puede
8. ok
9. ok
10. no puede

Low Mark sobre objetos:

1. ok
2. ok
3. ok
4. ok
5. ok
6. ok
7. ok
8. ok
9. o1 baja →o1 es public
10. ok (Ahora puede)

Estricta:

1. no
2. ok
3. no
4. ok
5. no
6. no
7. ok
8. ok
9. ok
10. no

Ejercicio 6:

a. Se tienen los sujetos s1 y s2 y los objetos o1 y o2. (nivel 1 es superior a nivel 2)

En Biba Low Mark:

S1 puede leer o2, pero entonces baja de nivel.
S2 lee o1.
S1, s2 escriben o2.

En Biba Estricta:

S1 no tiene permitido leer o2 porque es de menor nivel.

b. La secuencia dada para Biba Low Watermark no puede crear un camino de transferencia de información ya que ahora hay menos personas que pueden escribir objetos (si todos bajan de nivel, los niveles más altos no pueden ser escritos por nadie)

Ejercicio 7:

a. Un sujeto puede leer un objeto si tiene permiso de lectura sobre el objeto y el mismo nivel que el objeto.
b. Un sujeto puede escribir un objeto si tiene permiso de escritura sobre el objeto y el mismo nivel que el objeto.

Esto genera aislamiento, es decir, limita la posibilidad de compartir recursos.

Ejercicio 8:

La demostración es por inducción sobre n.

Base: Para n = 1, la tesis es que $i(o_1) \geq i(o_2)$

Demostración:

Si s_1 pudo leer o_1, entonces $i(o_1) \geq i(s_1)$

Si s_1 pudo escribir o_2, entonces $i(o_2) \leq i(s_1)$

$\therefore i(o_2) \leq i(o_1)$

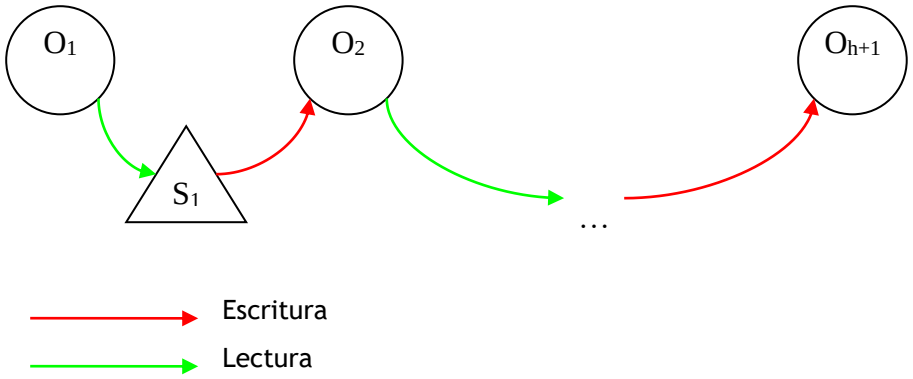
Paso Inductivo:

Hi) Es cierto que $i(o_{h+1}) \leq i(o_1)$

GUÍA 6: MODELOS DE CONFIDENCIALIDAD E INTEGRIDAD - SOLUCIONES

Ti) Es cierto que $i(o_{h+2}) \leq i(o_1)$

Demostración:



Para pasar información a o_{h+2}, s_{h+1} tiene que leer o_{h+1} y escribir en o_{h+2}.

O sea:

$i(o_{h+1}) \geq i(s_{h+1})$ para poder leer o_{h+1}

$i(s_{h+1}) \geq i(o_{h+2})$ para poder escribir o_{h+2}

$\therefore i(o_{h+1}) \geq i(o_{h+2})$

Como por Hipótesis Inductiva $i(o_{h+1}) \leq i(o_1)$, resulta, por transitividad que:

$i(o_{h+2}) \leq i(o_1)$

Como se demostró para el caso base y para el paso inductivo, la propiedad vale para todo n.

Ejercicio 9:

a. Para mostrar que un sistema que implementa el modelo de la Muralla China puede soportar el modelo de Bell – LaPadula, hay que mostrar que puede cumplir las propiedades * y ss.

Condición de Seguridad Simple (SS) en Bell Lapadula:

s puede leer o ⇔ s tiene permiso para leer o y L(s) dom L(o).

Condición * en Bell Lapadula:

s puede escribir o ⇔ s tiene permiso para escribir o y L(o) dom L(s)

Solución:[1]

Se pueden considerar dos niveles: clasificados (están en algún COI/CD) y desclasificados.
Con esos dos niveles, se cumple ss, ya que:

- si el objeto o es desclasificado, L(s) domina a desclasificado.
- Si el sujeto s lee objetos que son del mismo COI y el mismo CD, L(s) domina al L(o) porque L(s)=L(o)
- Si el sujeto s lee objetos que son de distinto COI, entonces L(s) = L(o) (lee objetos que están el el COI/CD asignado)

También se cumple la propiedad *, ya que: Sólo puede escribir si sólo puede leer objetos del mismo CD, entonces son objetos del mismo nivel, es decir L(s) = L(o), por lo tanto L(o)dom L(s)

b. El modelo de Bell Lapadula no es apropiado para modelar el de la Muralla China porque éste último asume un elemento temporal que en aquél no es tenido en cuenta. En el modelo de

[1] Ver el archivo brewer_nash_89.pdf, "The Chinese Wall Security Policy", de David Brewer y Michael Nash

Muralla China, si un sujeto S lee cualquier CD de un COI no puede volver a leer otra CD del mismo COI **nunca**.

Ejercicio 10:

Solución:

a. Habría un solo COI, debido a que Grupo Clarín tiene conflictos de interés con todas las empresas. Se puede hacer un grafo para analizar las relaciones de conflicto de interés: el grafo es conexo.
b. Por haber un solo COI y 6 empresas, no alcanza con tres personas. Hay que tomar personal nuevo: tres personas más.
c. Hace falta tomar una persona más para manejar lo de Malena, ya que los otros empleados trabajan o han trabajado en otros CD del mismo COI.
d. En este caso hay dos COI, con dos CD cada uno. Supongamos que se distribuye asi:
   Diego: Telecentro
   Malena: Frávega.
   Susana:Grupo Clarín y Garbarino.
   Acceder para lectura es posible con las tres personas. La regla de escritura en el modelo de Muralla China exige que si S puede leer otro objeto o', ese otro objeto debe pertenecer al mismo CD. (For all unsanitized objects O', S can read O' $\Rightarrow$ CD(O') = CD(O)) Como Susana está a cargo de un CD en un COI y de un CD en el otro COI, no puede escribir en ninguno, entonces habría que contratar a alguien más para esas acciones. Si Malena se va, Diego puede hacerse cargo de Frávega, pero sólo con acceso para lectura. Si hay que realizar modificaciones, deberá contratarse otra persona.
   Diego: Telecentro
   Malena: Frávega y Grupo Clarín.
   Susana: Garbarino.
   Acceder para lectura es posible con las tres personas. Como Malena está a cargo de un CD en un COI y de un CD en el otro COI, no puede escribir en ninguno, entonces habría que contratar a alguien más para ello. Si Malena se va, Diego podría tomar Frávega o Susana podría trabajar con Garbarino. Pero siempre estaría el problema de la escritura.

Ejercicio 11:

Solución:

Los niveles son tres: L= { TS, C, P}

Las categorías son tres, y el conjunto de partes es =

$$P(C) = \begin{Bmatrix} \{Asia, Europa, America\}, \{Asia, Europa\}, \{America, Europa\}, \{Asia, America\}, \\ \{Asia\}, \{America\}, \{Europa\}, \{\ \} \end{Bmatrix}$$

A los sujetos/objetos que tengan nivel TS, se les asigna alguno de los siguientes compartimentos:

$(TS, \{Asia\})$

$(TS, \{Europa\})$

$(TS, \{América\})$

A los sujetos de nivel confidencial, se les asigna alguno de los siguientes compartimentos:

$(C, \{Asia\})$

$(C, \{Europa\})$

$(C, \{América\})$

A los sujetos de nivel público se les asigna

$(P, \{\ \})$

No se usa ningún otro compartimento.

- Como es un modelo de Confidencialidad, la información no fluye hacia niveles más bajos.
- Como los que están en nivel de confidencialidad sólo son dominados por alguien que está en la misma área geográfica, no hay peligro de traspaso de información entre distintas áreas.

Ejercicio 12:

- **Solución 1:**

Esta primera propuesta asume un modelo Bell Lapadula.

Niveles:

CAR > DTO > MAT > DESCLASIF

En una primera aproximación se puede hacer:

Niveles de los sujetos:

Director de carrera →CAR

Director de departamento →DTO

Profesor de materia →MAT

Niveles de los objetos:

Planes → CAR

Programas → DTO

Evaluación de desempeño → MAT

Pero es incompleto, entonces se agregan como categorías a las materias.

Así, se arma entonces una jerarquía teniendo en cuenta nivel + categoría:

L(evaluación de desempeño de materia m) = (MAT,{m})

L(programa de materia m) = (MAT,{m})

L(plan de carrera) = (CARR, $\{m_1, m_2, \ldots . m_c\}$) Donde los m_i son todas las materias que se dictan en esa carrera.

L(profesor) = (MAT, $\{m_1, m_2, \ldots m_p\}$) Donde los m_i son todas las materias que se dicta ese profesor.

L(dir de depto) = (DTO,{ $m_1, m_2, \ldots m_d$}) Donde los m_i son todas las materias que se dicta en ese departamento.

L(dir de carrera) = (CAR,{ $m_1, m_2, \ldots m_c$}) Donde los m_i son todas las materias que se dictan en esa carrera.

Entonces, vemos si se cumplen los requisitos:

- Cada profesor participa de una o más materias. ✅
- Cada materia pertenece a un departamento. ✅
- Cada materia pertenece a una o más carreras. ✅
- L(plan de carrera)=L(director de carrera), entonces el director de carrera puede modificar el plan si se le otorga el permiso de escritura. ✅
- L(plan de carrera) domina a L(director de departamento), entonces el director de departamento puede modificar el plan de carrera si se le otorga el permiso de escritura. ✅
- L(programa de materia m) = (MAT,{m}). Entonces, L(profesor de m) domina a L(programa de materia m), L(director de departamento que tiene esa materia m) domina a L(programa de materia m), L(director de carrera que tiene esa materia m) domina a L(programa de materia m), por lo tanto todos pueden leer el programa si se les otorga el permiso de lectura. ✅ Los docentes pueden escribir si se les otorga el permiso de escritura **únicamente si un docente tuviera una sola materia**. Si un profesor tiene la materia m1 y m2, L(profesor que da materia m1 y m2) = (MAT,{m1,m2}) entonces domina a L(programa de m1) por lo que si tiene el permiso de lectura puede leer, pero aún teniendo permiso de escritura, por estar en un nivel más alto no podría escribir. Esto no respondería al requerimiento de que un profesor participa en una o más materias. ❌
- L(evaluación de desempeño de materia m)=(MAT,{m}) y por lo tanto L(profesor de materia m) domina L(evaluación de desempeño de materia m) y L(director de departamento de materia m) también, entonces si tienen permiso de lectura pueden leer las evaluaciones. ✅

➢ **Solución 2: Propuesta por Axel Preiti – Cuatrimestre 1 2024.**

Esta segunda propuesta asume un modelo Biba Ring Policy (modelo de integridad).
Sean los sujetos:

- Alumnos
- Profesores
- Directores de Departamento
- Directores de Carrera

Sean los objetos:

- Planes de carrera
- Programas de materia
- Evaluaciones de desempeño

Se propone un modelo de integridad Biba Ring-Policy, extendido con categorías. Inicialmente, cualquier sujeto podrá leer cualquier objeto pero esto se restringirá a partir de los permisos discrecionales, mientras que los niveles de integridad y las categorías, junto a otros permisos discrecionales, limitarán la escritura de objetos.

GUÍA 6: MODELOS DE CONFIDENCIALIDAD E INTEGRIDAD - SOLUCIONES

Sean los niveles de integridad L = {D, P, A}, que se los puede pensar como los niveles para **D**irectores, **P**rofesores y **A**lumnos
Por su parte, el conjunto de categorías C estará conformado por los elementos:

C = {m / m es una materia} U {c / c es una carrera}

Los objetos tendrán los siguientes compartimentos:

- Para todo plan de carrera: **(D, {c})**, donde c es la carrera del plan
- Para todo programa de materia: **(P, {m})**, donde m es la materia del programa
- Para toda evaluación de desempeño: **(A, {m})**, donde m es la materia que está siendo evaluada

Los sujetos tendrán los siguientes compartimentos y permisos discrecionales:

- Para todo alumno **a**:
  - **Compartimento**: **(A, {m / el alumno a cursa m} U {c / el alumno a está en la carrera c})**
  - **Permisos**
    - Plan de carrera: Permiso de lectura solo para la carrera en la que está **a**
    - Programa de materia: Permiso de lectura para las materias que curse **a**
    - Evaluación de desempeño: Permiso de escritura para las materia que curse **a**

- Para todo profesor **p**:
  - **Compartimento**: **(P, {m / el profesor p dicta la materia m})**
  - **Permisos**
    - Plan de carrera: Permiso de lectura para las materias que dicte **p**
    - Programa de materia: Permiso de lectura y escritura para las materias que dicte **p**
    - Evaluación de desempeño: Permiso de lectura para las materia que dicte **p**

- Para todo director de departamento **dd**:
  - **Compartimento**: **(D, {m / la materia m está en el departamento que dirige dd} U {c / alguna materia del departamento que dirige dd está en la carrera c})**
  - **Permisos**
    - Plan de carrera: Permiso de lectura para las carreras que tengan una materia del departamento que dirige **dd**
    - Programa de materia: Permiso de lectura y escritura para las materias que pertenezcan al departamento que dirige **dd**
    - Evaluación de desempeño: Permiso de lectura para las materia que pertenezcan al departamento que dirige **dd**

- Para todo director de carrera **dc**:
  - **Compartimento**: **(D, {m / la materia m está en la carrera que dirige dc} U {c / dc dirige la carrera c})**
  - **Permisos**

- Plan de carrera: Permiso de lectura y escritura solo para la carrera que dirige **dc**
- Programa de materia: Permiso de lectura para las materias que pertenezcan a la carrera que dirige **dc**
- Evaluación de desempeño: -

De esta forma:

- Solo los alumnos podrán escribir evaluaciones de desempeño y sólo de las materias que cursan (pues solo dominan los objetos que tengan alguna de sus materias y por el permiso discrecional)
- Los alumnos no podrán escribir los planes de carrera ni los programas de materia porque no dominan dichos objetos
- Los profesores no podrán escribir las evaluaciones de desempeño porque, si bien dominan el objeto, no cuentan con el permiso discrecional
- Los profesores no podrán escribir los planes de carrera porque no dominan dichos objetos
- Los profesores podrán leer los planes de carrera ya que Ring-Policy y cuenta con los permisos discrecionales
- Los directores de departamento no podrán escribir los planes de carrera porque, si bien dominan el objeto, no tienen el permiso discrecional
- Etc.

Axel Preiti Tasat