Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Escuela de Ciencias Exactas y Naturales
Departamento de Ciencias de la Computación
Seguridad Informática
2024 Maximiliano Cristia Alejandro Hernandez

Práctica 1
Unidades 1 (Conceptos básicos) y 2 (Confidencialidad)

Entrega. Se deberán entregar resueltos 4 o 5 ejercicios a determinar por el docente de práctica. Tener en cuenta que la presentación de los mismos será evaluada.

1. Discuta la diferencia entre datos e información. Encuentre ejemplos en donde controlar el acceso a los datos no necesariamente controla el acceso a la información.

2. Las empresas usualmente restringen a sus empleados el uso de e-mail para fines laborales, pero permiten un mínimo uso para razones personales.

1. Piense cómo podría una empresa detectar un uso excesivo de e-mails personales, sin tener que leerlos.
2. Intuitivamente, parece razonable evitar TODO uso personal de e-mail. Explique por qué la mayoría de las empresas no hacen esto.

3. Discuta cómo las políticas de seguridad y los modelos para hacerlas cumplir pueden imponer barreras comerciales.

4. Los ataques pueden venir tanto de afuera como de adentro de una organización. ¿Hay alguna diferencia entre estas amenazas internas de las amenazas externas? ¿Cuál es la importancia relativa de las amenazas internas? ¿Piensa que fue adaptada a medida que la tecnología fue progresando?

5.
a) Para cada una de las cualidad de software mencionadas, brinde algún ejemplo de posible incorporación de seguridad en un sistema, el cual perjudica la cualidad mencionada.

- Performance
- Usabilidad
- Mantenibilidad
- Reusabilidad

b) Qué otras cualidades de software pueden ser perjudicadas por intentar proveer de mayor seguridad a un sistema?

6. Clasifique cada una de las siguientes situaciones como una violación de confidencialidad, de integridad, de disponibilidad, o una combinación de ellas:

1. Juan se copia de la tarea de María
2. Pablo le rompe el sistema a Jimena
3. Carolina cambia el monto del cheque de Diego de $100 a $1000
4. Mirta falsifica la firma de Rodrigo en una escritura
5. Esteban registra el nombre de dominio “AddisonWesley.com” y se rehusa permitir a la editorial comprar o usar ese nombre de dominio
6. Manuel obtiene el número de tarjeta de crédito de Pedro y logra que la Empresa cancele la tarjeta y la reemplace por otra tarjeta con un número diferente

7. Dé un ejemplo de una situación en la cual un compromiso de confidencialidad conduce a un compromiso de integridad.

8. Dé un ejemplo en donde un problema de *security* es también un problema de *safety*; uno donde un problema de *security* NO es problema de *safety*; y uno donde un problema de *safety* NO es problema de *security*.

9. El aforismo "seguridad a través de oscuridad" sugiere que el ocultamiento de informació provee algún grado de seguridad. Dé un ejemplo de alguna situación en que el ocultamiento de información no agrega apreciable seguridad a un sistema. Luego dé un ejemplo en que sí.

10. En un sistema de información médica que controla el acceso a los registros de los pacientes y las recetas:

- Los doctores pueden leer y escribir registros de pacientes y recetas.
- Las enfermeras pueden leer y escribir recetas pero no pueden saber nada sobre los registros.

¿Cómo puede capturar esta política en un modelo de látices que prevenga flujo de información de los registros a las recetas?

11.
a) Busque y discuta sobre la definición de: disclosure (revelación), disruption (alteración), deception (engaño), usurpation (usurpación).
b) Muestre que los tres servicios de seguridad: confidencialidad, integridad y disponibilidad; son suficientes para lidiar con esas cuatro amenazas.

12. Investigue sobre las características de AppArmor en Ubuntu para proveer seguridad del tipo MAC.

13.
a) Lea sobre el modelo de Biba para integridad.
b) ¿Es posible usar los modelos de Bell-LaPadula y de Biba para modelar confidencialidad e integridad simultáneamente? ¿Se pueden usar las mismas categorÍas de seguridad para ambas políticas?

14.
a) Codifique en Z el modelo de Bell-LaPadula, definiendo operaciones de lectura y escritura con condiciones de disparo de acuerdo a niveles de seguridad.
b) Pruebe usando Z/EVES que las operaciones preservan las propiedades definidas del modelo (security condition y *-property).

15.
a) Implemente en Haskell una función:

```
grant :: User -> File -> Access -> Bool
grant user file bool =
```

Que, dado un usuario (sujeto), un archivo (objeto) y un tipo de acceso (lectura, escritura), devuelva un booleano indicando si se puede llevar adelante el acceso, siguiendo la política del modelo Bell-LaPadula.
Obs: Puede agregar parámetro(s) adicional(es) con la información necesaria para poder devolver lo que corresponda.
b) Si no lo hizo en el inciso anterior, modifique la función de manera que mantenga el estado de archivos accedidos (abiertos), para tener en cuenta también la propiedad *.

16.
a) Investigue el sistema de permisos clásico de Linux.
b) Instale y configure alguna ACL. Discuta sus descubrimientos.

17. Explicar qué hace el bit `t` en los permisos de la carpeta `/tmp`.

18. Cuando no hay ACLs disponibles, una alternativa para dar determinado acceso a un grupo de usuarios es crear un grupo ad hoc para ese archivo, y cambiar con `chgrp` al grupo creado, dándole los permisos buscados al grupo. Explicar qué inconvenientes trae esto, y dar un caso donde, aunque se usen grupos ad hoc, no alcance el sistema de permisos de Linux para especificar todos los permisos que se desean dar.

19. En un directorio montado en una partición con ACL:

```
$ getfacl bar
# file: bar
# owner: jose
# group: jose
user::---
user:jose:rwx
user:exp:r--
group::---
mask::rwx
other::---
```

El usuario `joe`, ¿puede leer el fichero `bar`? ¿Y `exp`? ¿Y `jose`? ¿Y `root`? ¿Cuál es la función de `mask`? ¿Qué pasa si `mask` fuese `---`?

20. El comando `ping` necesita permisos especiales de red, por lo que es necesario que tenga más permisos que los básicos de ejecución del usuario que lo ejecuta. Esto es logrado en la actualidad gracias a los atributos dados por `capabilities`. En el pasado, esto se lograba con setuid (bit s en lugar de x), que otorgaba al comando ping permisos de `root`. ¿Qué ventajas trae el enfoque actual?

21. Determinar si hay flujo indebido de información en cada uno de estos programas:

```
-- Prog 1
magic = readL();
if (magic == 0xdeadbeef)
  writeH("hey");
else
  writeH("ho");

-- Prog 2
x = readH();
writeL("Loading...");
writeH(x);

-- Prog 3
x = readH();
writeL("Loading");
while (x-- > 100)
  writeL(".");
writeH(x);
```

```
-- Prog 4
user = readL();
pass = readL();
if (user == "root" && pass == "1234")
  msg = "Bienvenido";
else
  msg = "Usuario/password incorrecto";
writeL(msg);

-- Prog 5
db_pass = readPassFromDBH();
db_user = readUserFromDBH();
user = readL();
pass = readL();
if (user == db_user && pass == db_pass)
  msg = "Bienvenido";
else
  msg = "Usuario/password incorrecto";
writeL(msg);
```

22. Para los programas del ejercicio anterior, explique cómo funcionaría la ejecución bajo el sistema de seguridad por multi-ejecución.

23. Resuelva los desafíos propuestos en el siguiente link: `http://ifc-challenge.appspot.com/`
Para los que pueda resolver, explique las conclusiones a las que arribe, por ejemlo:

- Qué tipo de ataque logró llevar adelante?
- Qué limitación tiene el sistema de reglas?
- Qué cambio habría que hacerle para impedir el ataque?