Tarea: Seguridad en Sistemas Informáticos Parte 2

Jorge Chávez Saab

July 7, 2020

Problema 1.4

Para cada uno de los siguientes sistemas, asigne una calificación de bajo, moderado o alto al nivel de impacto de la pérdida de confidencialidad, disponibilidad e integridad, respectivamente. Justifique sus respuestas.

a) Una organización que maneje información pública en su servidor web.

b) Una organización jurisdiccional que maneja información extremadamente sensible para una investigación.

c) Una organización financiera que maneja información administrativa de rutina (no privada).

d) Un sistema informático usado para adquisiciones en una organización contratista que contiene tanto información sensible para la fase de presolicitación de proyectos como información administrativa de rutina. Evaluar separadamente para ambos conjuntos de información y para la organización completa.

e) Un sistema que controla la distribución de poder eléctrico para un complejo militar, que contiene información en tiempo real de sensores e información administrativa. Evaluar separadamente para ambos conjuntos de datos y para la organización completa.

Respuesta

a) Confidencialidad - **baja**. Ya que la información que se maneja es pública, por suposición no hay necesidad de ocultarla de nadie.

Disponibilidad - **alta**. Ya que se trata de información pública, se asume que un gran número de personas puede necesitar hacer uso de ella. Por ejemplo, un servidor que provee el pronóstico del clima, cuya falta de disponibilidad podría tener afectaciones mayores.

Integridad - **alta**. De nuevo ya que mucha gente puede depender de ella, es importante que la información se mantenga íntegra. Podría tratarse de una página que publique anuncios importantes por parte de un gobierno. Por ejemplo, si alguien modificara la página de información sobre el programa "hoy no circula" para que anuncie las placas que no circulan erróneamente, esto podría llevar a mucho caos y confusión.

b) Confidencialidad - **media**. En un juicio eventualmente se tiene que hacer pública toda la evidencia que funcione en contra del acusado, por lo que no es tan crucial mantener esto confidencial. Sin embargo, durante el proceso de investigación antes del juicio, puede ser importante para el investigador mantener su mano escondida.

Disponibilidad - **alta**. Es extremadamente importante mantener la evidencia disponible, de lo contrario alguien podría prevenirnos el acceso a ella para que no se pueda usar en su contra.

Integridad - **alta**. Por la misma razón que el punto anterior. Si alguien pudiera modificar o incluso eliminar evidencia de una base de datos, la investigación se volvería completamente inútil.

c) Confidencialidad - **baja**. Por suposición la información que maneja la organización no es privada, por lo que la confidencialidad puede ser importante pero no de la más alta prioridad.

Disponibilidad - **alta**. Se asume que la organización necesita acceso a los datos que ha recolectado para tomar decisiones sobre cómo actuar, por lo que no tener acceso a ella podría generar retrazos y pérdidas de dinero.

Integridad - **alta**. La organización puede contar con un sistema que toma decisiones sobre como invertir el dinero de forma automatizada por algún algoritmo. Si los datos que este algoritmo analiza fueran

modificados maliciosamente podrían provocar que se invierta el dinero incorrectamente y generar pérdidas catastróficas.

d) Confidencialidad - **alta** para la información de proyectos ya que el robo de esta información podría ayudar a otras organizaciones que compitan directamente con ella, **baja** para la información administrativa ya que el conocimiento de cómo opera la organización no pone en riesgo directamente sus operaciones. Para la organización entera, la prioridad es **media**.

   Disponibilidad - **baja** en todos los casos ya que son raros los casos en que la organización deberá accesar información y actuar en forma inmediata.

   Integridad - **media** para la información de proyectos porque podría causar retrazos en un proyecto si se descubre que la información no es íntegra, **alta** en la información administrativa ya que podría causar que la organización no maneje un proyecto adecuadamente, deje pasar una fecha límite, etc. En general, es de prioridad **alta**.

e) Confidencialidad - **alta** en todos los casos ya que el conocimiento tanto de la información de los sensores (por ejemplo, cuándo están operando ciertos equipos) como la información administrativa proveen conocimiento sobre cómo opera el complejo lo cual podría comprometer su seguridad ante un ataque físico.

   Disponibilidad - **alta** en el caso de los sensores ya que si no se recibe esta información el sistema podría seguir entregando poder cuando no se requiere hasta llegar a una sobrecarga. **Baja** para la información administrativa ya que no necesariamente se necesita tener acceso a esta en todo momento y de manera urgente. En general, la prioridad es **media**.

   Integridad - **alta** para los sensores ya que alguien que modifique esta información podría ocasionar sobrecargas o apagones que dejen sin funcionar a equipos esenciales. **Media** para la información administrativa ya que esto también podría llevar a un manejo inadecuado que cause mal funcionamiento, aunque con un efecto menos inmediato. En general, la prioridad es **alta**.

Problema 3.6

Asuma que las contraseñas están limitadas al uso de los 96 caracteres ASCII y que todas tienen longitud de 10 caracteres. Si un quebrador de contraseñas puede hacer 6.4 millones de encripciones por segundo, cuánto tardaría en probar exhaustivamente todas las contraseñas de un sistema UNIX?

Respuesta

Si tenemos 10 caracteres y cada uno puede ser uno de 96, en total tenemos 96^{10} contraseñas que debe de probar el quebrador, lo cual le tomará

$$\frac{96^{10} \text{ encripciones}}{6.4 \times 10^6 \text{ encripciones/segundo}} \approx 1.039 \times 10^{13} \text{ segundos} \approx 329,402 \text{ años.}$$

Problema 4.5

UNIX trata a los directorios de la misma forma que a los archivos: es decir, ambos se definen con la misma estructura de datos llamada inodo. Al igual que los archivos, los directorios contienen una cadena de protección de 9 bits, lo cual puede crear problemas de acceso si no se tiene cuidado. Por ejemplo, considere un archivo con modo de protección 8x644 contenido en un directorio con modo de protección 8x730. ¿Cómo podría estar comprometido el archivo en este caso?

Respuesta

El modo 644 significa que el dueño tiene permiso de escribir y leer del archivo, pero no ejecutarlo, mientras que el resto de los usuarios sólamente tienen permiso de leer de él. Por otra parte, el modo 730 significa que el dueño tiene todos los permisos sobre el directorio, mientras que los otros usuarios del grupo tienen permiso de ejectutar y escribir en él, y otros usarios no tienen ningún permiso.

El problema es que un usuario del grupo, gracias a que tiene permisos de ejecución y escritura sobre el directorio, puede operar dentro de él. El hecho de que no tenga permiso de escribir sobre el archivo pareciera indicar que no tiene forma de modificarlo, pero si conoce el nombre de éste puede

simplemente removerlo del índice del directorio (al que sí puede escribir) lo cual para fines prácticos es lo mismo que haber borrado el archivo. Peor aun, el intruso después de borrar el archivo podría crear otro con el mismo nombre pero que contenga los datos que él quiera y esté bajo control de él, y esto es probablemente algo que el dueño no esperaba que fuera posible al haber denagado permisos de escritura.

Problema 19.12

Comparar la copia del Código de Ética del IEEE de 1979 con la del 2006.

a) ¿Hay algún elemento del código de 1979 que no se encuentre en el de 2006? Proponga una razón para esta exclusión.

b) ¿Hay algún elemento del código del 2006 que no se encuentre en el de 1979? Proponga una razón para esta adición.

Respuesta

a) El artículo IV.b, *contribuir consejo profesional a organizaciones civicas, caritativas y sin fines de lucro* junto con el II.b, *reportar, publicar y diseminar informacion libremente a otros*, han sido removidos del código. Esto puede reflejar la emergencia de la competencia y el capitalismo donde tristemente, muchos trabajadores desarrollan tecnología solo para el beneficio propio y no se puede esperar que compartan su conocimiento o realizen actos caritativos.

b) El artículo 9, *evitar herir a la persona, propiedad, reputación o empleo de otros por medio de acciones falsas o maliciosas*, no está presente en la versión de 1979. Esta inclusión refleja la necesidad de proteger contra la difamación, la cual posiblemente se haya vuelto un problema conforme el crecimiento de las empresas nos llevo a un mundo más competitivo.

   En el artículo 5, *mejorar el entendimiento de la tocnología, sus aplicaciones, y sus potenciales consecuencias*, la ultima parte (sobre las consecuencias) no se encontraba en la versión de 1979. Esto podría

deberse a que en ese entonces no se tenía tanta conciencia de la velocidad a la que la tecnología avanzaría y las muchas consecuencias que se darían sin que nadie las prediga, lo cual es más evidente hoy en dia.