Seguridad

La seguridad es una medida de la capacidad del sistema para proteger los datos y la información de acceso no autorizado sin dejar de proporcionar acceso a personas y sistemas que están autorizadas. Una acción tomada contra un sistema informático con la intención de causar daño se denomina **ataque** y puede adoptar varias formas. Puede ser un intento no autorizado de acceder a datos o servicios o modificar datos, o puede tener la intención de negar servicios a usuarios legítimos.

El enfoque más simple para caracterizar la seguridad tiene tres características: confidencialidad, integridad y disponibilidad (CIA):

1. La **confidencialidad** es la propiedad de la que están protegidos los datos o servicios de accesos no autorizado. Por ejemplo, un pirata informático no puede acceder a su impuesto sobre la renta que devuelve una computadora del gobierno.

2. La **integridad** es la propiedad a la que los datos o servicios no están sujetos a manipulación. Por ejemplo, su calificación no ha cambiado desde su el instructor lo asignó.

3. La **disponibilidad** es la propiedad por la que el sistema estará disponible para fines legítimos de uso. Por ejemplo, un ataque de denegación de servicio no le impedirá pedir un libro en una librería en línea.

Otras características que se utilizan para apoyar a la CIA son estas:

4. La **autenticación** verifica las identidades de las partes de una transacción y comprueba si son realmente quienes dicen ser. Por ejemplo, cuando obtienes un correo electrónico que supuestamente proviene de un banco, la autenticación garantiza que en realidad proviene del banco.

5. El **no repudio** garantiza que el remitente de un mensaje no podrá negar posteriormente haber enviado el mensaje, y que el destinatario no puede negar haber recibido el mensaje. Por ejemplo, no puede negar haber pedido algo del Internet, o el comerciante no puede negarse a recibir su pedido.

6. La **autorización** otorga al usuario los privilegios para realizar una tarea. Por ejemplo, El sistema bancario en línea autoriza a un usuario legítimo a acceder a su cuenta.

Usaremos estas características en nuestros escenarios generales de seguridad. Enfoques para lograr la seguridad se pueden caracterizar como aquellas que detectan ataques, aquellas que resistin los ataques, los que reaccionan a los ataques y los que se recuperan de un éxito ataques. Los objetos que se protegen de los ataques son datos en reposo, datos en tránsito y procesos computacionales.

9.1 Escenario general de seguridad

Una técnica que se utiliza en el dominio de la seguridad es el modelado de amenazas. Un "ataque árbol", similar a un árbol de fallas discutido en el Capítulo 5, es utilizado por ingenieros de seguridad para determinar posibles amenazas. La raíz es un ataque exitoso y los nodos están posibles causas directas de ese ataque exitoso. Los nodos secundarios descomponen las causas directas, etc. Un ataque es un intento de romper la CIA, y las hojas de los árboles de ataque serían el estímulo en el escenario. La respuesta al ataque es preservar a la CIA o disuadir a los atacantes mediante el seguimiento de sus actividades. A partir de estas consideraciones, ahora podemos describir las partes individuales de una seguridad general.

■ **Fuente de estímulo**. La fuente del ataque puede ser un ser humano u otro sistema. Puede haber sido identificado previamente o puede ser desconocido. Un atacante humano puede ser de fuera de la organización o desde dentro de la organización.

■ **Estímulo**. El estímulo es un ataque. Caracterizamos esto como un intentar mostrar datos, cambiar o eliminar datos, acceder a los servicios del sistema, cambiar el comportamiento del sistema o reducir la disponibilidad.

■ **Artefacto**. El objetivo del ataque puede ser los servicios del sistema, los datos que contiene, o los datos producidos o consumidos por el sistema. Algunos ataques se realizan en componentes particulares del sistema que se sabe que son vulnerable.

■ **Medio ambiente**. El ataque puede ocurrir cuando el sistema está en línea o fuera de línea, ya sea conectado o desconectado de una red, ya sea detrás de un firewall o abierto a una red, completamente operativo, parcialmente operativo o no Operacional.

■ **Respuesta**. El sistema debe garantizar que las transacciones se lleven a cabo en uno de manera que los datos o servicios estén protegidos contra el acceso no autorizado; los datos o servicios no se manipulan sin autorización; las partes de la transacción no puede repudiar sus implicaciones; y los datos, recursos y sistema estarán disponibles para uso legítimo.

El sistema también debe rastrear las actividades dentro de él registrando el acceso o modificación; intenta acceder a datos, recursos o servicios; y notificando a las entidades apropiadas (personas o sistemas) cuando un ataque aparente es ocurriendo.

■ **Medida de respuesta**. Las medidas de la respuesta de un sistema incluyen cuánto de un sistema se ve comprometido cuando un componente en particular o un valor de datos es comprometido, cuánto tiempo pasó antes de que se detectara un ataque, cómo se resistieron muchos ataques, cuánto tiempo se tardó en recuperarse de un éxito ataque y cuántos datos eran vulnerables a un ataque en particular.

La Tabla 9.1 enumera los elementos del escenario general, que caracterizan la seguridad, y la Figura 9.1 muestra un ejemplo de escenario concreto: Un descontento empleado desde una ubicación remota intenta modificar la tabla de tarifas de pago durante operaciones normales. El sistema mantiene una pista de auditoría y los datos correctos son restaurado en un día.

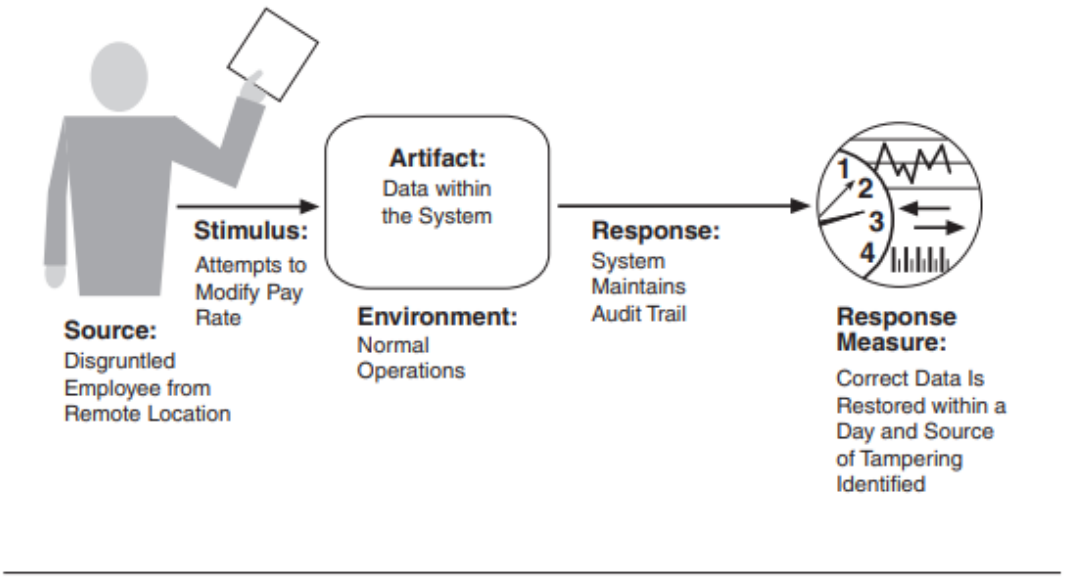

FIGURE 9.1 Sample concrete security scenario

Tabla 9.1 Escenario general de seguridad

Una porción del escenario	**Valores posibles**
FUENTE	Humano u otro sistema que pueda haber sido previamente identificado (ya sea correcta o incorrectamente) o puede estar actualmente desconocido. Un atacante humano puede ser de fuera de la organización o desde dentro de la organización.
ESTÍMULO	Se realiza un intento no autorizado de mostrar datos, cambiar o eliminar datos, acceder a los servicios del sistema, cambiar el comportamiento del sistema, o reducir la disponibilidad.
ARTEFACTOS	Servicios de sistemas, datos dentro del sistema, un componente o recursos del sistema, datos producidos o consumidos por el sistema
ENTORNO	El sistema está en línea o fuera de línea; ya sea conectado o desconectado de una red; ya sea detrás de un firewall o abierto a una la red; completamente operativo, parcialmente operativo o no operativo.
RESPUESTA	Las transacciones de respuesta se llevan a cabo de tal manera que ■ Los datos o servicios están protegidos contra el acceso no autorizado. ■ Los datos o servicios no se manipulan sin autorización. ■ Las partes de una transacción se identifican con seguridad. ■ Las partes de la transacción no pueden repudiar sus participaciones.

■ Los datos, recursos y servicios del sistema estarán disponibles para uso legítimo.
El sistema rastrea las actividades dentro de él por:
■ Registro de acceso o modificación
■ Registro de intentos de acceso a datos, recursos o servicios
■ Notificación a las entidades apropiadas (personas o sistemas) cuando un aparente ataque está ocurriendo

MEDIDA DE RESPUESTA Uno o más de los siguientes:

■ Qué parte de un sistema se ve comprometida cuando el valor del componente o de los datos está comprometido
■ Cuánto tiempo pasó antes de que se detectara un ataque
■ Cuántos ataques se resistieron
■ Cuánto tiempo se tarda en recuperarse de un ataque exitoso
■ Cuántos datos son vulnerables a un ataque en particular

9.2 Tácticas de seguridad

Un método para pensar en cómo lograr la seguridad en un sistema es pensar sobre seguridad física. Las instalaciones seguras tienen acceso limitado (p. Ej., Mediante el uso de puestos de control de seguridad), tener medios para detectar intrusos (por ejemplo, exigiendo que los visitantes legítimos usen insignias), tener mecanismos de disuasión tales como guardias, tienen mecanismos de reacción como el bloqueo automático de puertas, y tener mecanismos de recuperación, como copias de seguridad fuera del sitio. Estos conducen a nuestras cuatro categorías de tácticas: **detectar, resistir, reaccionar y recuperar.** La figura 9.2 muestra estas categorías como el objetivo de las tácticas de seguridad

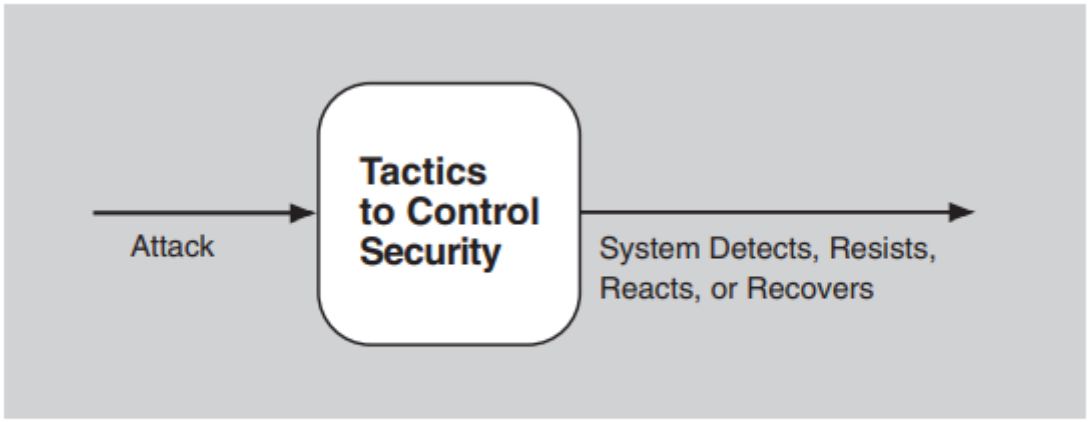

FIGURE 9.2 The goal of security tactics

Detectar ataques

La categoría de detección de ataques consta de cuatro tácticas: **detectar intrusión, detectar servicio denegación, verificar la integridad del mensaje y detectar el retraso del mensaje.**

■ **Detectar intrusiones** es la comparación del tráfico de red o la solicitud de servicio de patrones dentro de un sistema a un conjunto de firmas o patrones conocidos de comportamiento malicioso almacenado en una base de datos. Las firmas pueden basarse en protocolo, indicadores TCP, tamaños de carga útil, aplicaciones, origen o destino dirección o número de puerto.

■ **Detectar la denegación** del servicio es la comparación del patrón o la firma de tráfico de red que ingresa a un sistema a perfiles históricos de ataques conocidos de denegación de servicio.

■ **Verificar la integridad del mensaje**. Esta táctica emplea técnicas como sumas de control o valores hash para verificar la integridad de los mensajes, recursos archivos, archivos de implementación y archivos de configuración. Una suma de comprobación es un mecanismo de validación en el que el sistema mantiene información redundante para archivos de configuración y mensajes, y utiliza esta información redundante para verificar el archivo o mensaje de configuración cuando se utiliza. Un valor hash es una cadena única generada por una función hash cuya entrada podría ser archivos de configuración o mensajes. Incluso un ligero cambio en los archivos originales o mensajes da como resultado un cambio significativo en el valor hash.

■ **Detectar retraso en el mensaje** tiene como objetivo detectar posibles intermediarios ataques, donde una parte malintencionada está interceptando (y posiblemente modificando) mensajes. Al verificar el tiempo que se tarda en entregar un mensaje, es posible detectar un comportamiento de sincronización sospechoso, donde el tiempo que lleva entregar un mensaje es muy variable.

Resistir ataques

Hay una serie de métodos bien conocidos para resistir un ataque:

■ **Identificar actores**. La identificación de "actores" se trata realmente de identificar la fuente de cualquier entrada externa al sistema. Los usuarios se identifican normalmente a través del usuario.ID. Otros sistemas pueden "identificarse" mediante códigos de acceso, direcciones IP, protocolos, puertos, etc.

■ **Autenticar actores.** Autenticación significa asegurarse de que un actor (un usuario o una computadora remota) es en realidad quién o qué pretende ser.

■ **Autorizar a los actores.** Autorización significa asegurarse de que un actor autenticado tiene los derechos de acceso y modificación de datos o servicios. Este mecanismo generalmente se habilita al proporcionar algunos mecanismos de control de acceso dentro un sistema. El control de acceso puede ser por un actor o por una clase de actor. Clases de actores se puede definir por grupos de actores, por roles de actores o por listas de individuos.

■ **Limite el acceso.** Limitar el acceso implica controlar qué y quién puede acceder y qué partes de un sistema. Esto puede incluir limitar el acceso a recursos como procesadores, memoria y conexiones de red, que se pueden lograr mediante el uso de la gestión de procesos, la protección de la memoria, el bloqueo de un host, el cierre un puerto, o rechazar un protocolo. Por ejemplo, un cortafuegos es un único punto de acceso a la intranet de una organización. Una zona desmilitarizada (DMZ) es una subred entre Internet y una intranet, protegido por dos cortafuegos: uno frente Internet y el otro la intranet. Una DMZ se utiliza cuando una organización quiere permitir que los usuarios externos accedan a servicios que deberían estar disponibles públicamente fuera de la intranet. De esta forma, la cantidad de puertos abiertos en el firewall interno puede minimizarse. Esta táctica también limita el acceso de los actores (al identificar, autenticarlos y autorizarlos).

■ **Limite la exposición**. Limitar la exposición se refiere en última instancia e indirectamente a reducir la probabilidad de un ataque exitoso, o restringir la cantidad de daño potencial. Esto se puede lograr ocultando hechos sobre un sistema. para ser protegido ("seguridad por oscuridad") o dividiendo y distribuyendo recursos críticos para que la explotación de una sola debilidad no pueda comprometer cualquier recurso ("no pongas todos tus huevos en una canasta"). Para Por ejemplo, una decisión de diseño para ocultar cuántos puntos de entrada tiene un sistema es una forma de limitar la exposición. Una decisión de distribuir servidores entre varios Los centros de datos geográficamente dispersos también son una forma de limitar la exposición.

■**Cifre los datos**. Los datos deben protegerse del acceso no autorizado. La confidencialidad generalmente se logra mediante la aplicación de algún tipo de cifrado a los datos y a la comunicación. El cifrado proporciona protección adicional a datos mantenidos de forma persistente más allá de los disponibles a partir de la autorización.

Los enlaces de comunicación, por otro lado, pueden no tener autorización. En tales casos, el cifrado es la única protección para transmitir datos a través de enlaces de comunicación de acceso público. El enlace se puede implementar por una red privada virtual (VPN) o por un Secure Sockets Layer (SSL) para un enlace basado en web. El cifrado puede ser simétrico (ambas partes usan el mismo key) o asimétrica (claves públicas y privadas).

■ **Entidades separadas.** La separación de diferentes entidades dentro del sistema puede ser hecho a través de la separación física en diferentes servidores que están conectados a diferentes redes; el uso de máquinas virtuales (consulte el Capítulo 26 para una discusión sobre máquinas virtuales); o un "espacio de aire", es decir, al no tener conexión entre diferentes partes de un sistema. Finalmente, sensible Los datos se separan con frecuencia de los datos no sensibles para reducir el ataque. posibilidades de quienes tienen acceso a datos no sensibles.

■ **Cambiar la configuración predeterminada.** Muchos sistemas tienen asignadas configuraciones predeterminadas cuando se entrega el sistema. Obligar al usuario a cambiar esa configuración evitar que los atacantes obtengan acceso al sistema a través de configuraciones que están, por lo general, disponibles públicamente.

Reaccionar a los ataques

Varias tácticas están destinadas a responder a un posible ataque:

■ **Revocar el acceso**. Si el sistema o un administrador del sistema cree que un ataque está en marcha, entonces el acceso puede estar severamente limitado a recursos sensibles, incluso para usuarios y usos normalmente legítimos. Por ejemplo, si tu escritorio ha sido comprometido por un virus, su acceso a ciertos recursos puede estar limitado hasta que el virus se elimine de su sistema.

■ **Bloquear la computadora**. Los intentos repetidos de inicio de sesión fallidos pueden indicar un potencial ataque. Muchos sistemas limitan el acceso desde una computadora en particular si hay son intentos fallidos repetidos de acceder a una cuenta desde esa computadora. Los usuarios legítimos pueden cometer errores al intentar iniciar sesión. Por lo tanto, el acceso limitado puede ser solo por un período de tiempo determinado.

■ **Informar a los actores**. Los ataques en curso pueden requerir la acción de los operadores, otros personal o sistemas cooperantes. Dicho personal o sistemas, el conjunto de actores relevantes: deben ser notificados cuando el sistema ha detectado un ataque.

Recuperarse de los ataques

Una vez que un sistema ha detectado e intentado resistir un ataque, necesita recuperarse.

Parte de la recuperación es la restauración de los servicios. Por ejemplo, se pueden reservar servidores o conexiones de red adicionales para tal fin. Desde un exitoso el ataque puede considerarse una especie de falla, el conjunto de tácticas de disponibilidad que tratan sobre la recuperación de una falla se pueden aplicar para este aspecto de seguridad también.

Además de las tácticas de disponibilidad que permiten la **restauración de los servicios**, **necesidad de mantener una pista de auditoría.** Auditamos, es decir, mantenemos un registro de las acciones del usuario y del sistema y sus efectos, para ayudar a rastrear las acciones de un atacante y para identificarlo. Podemos analizar pistas de auditoría para intentar enjuiciar a los atacantes o crear mejores defensas en el futuro.

El conjunto de tácticas de seguridad se muestra en la Figura 9.3.

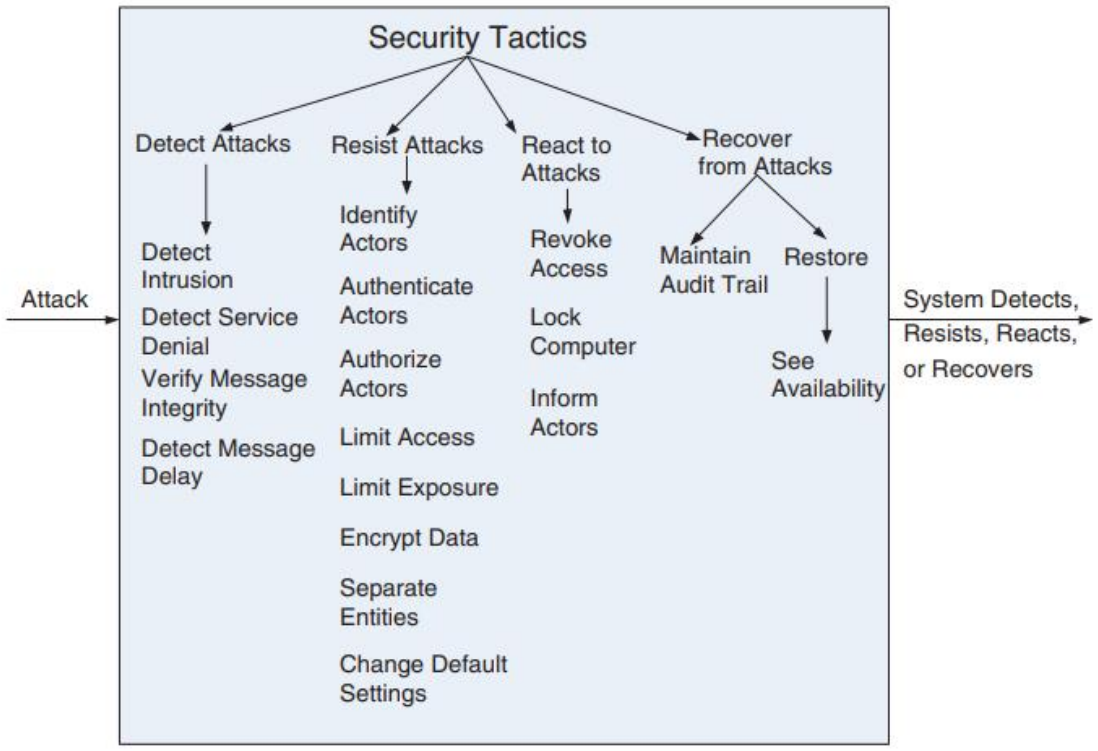

FIGURE 9.3 Security tactics