9. seguridad

Con Jungwoo Ryoo y Phil Laplante

Su identidad personal no vale tanto como solía serlo, al menos para los ladrones dispuestos a robarla. Según los expertos que monitorean dichos mercados, el valor de los datos de tarjetas de crédito robadas puede variar desde $ 3 hasta tan solo 40 centavos. Eso es diez veces menos que hace una década, a pesar de que el costo para una persona a quien le roban una tarjeta de crédito puede elevarse a cientos de dólares.

—Forbes.com (Taylor Buley. "Hackonomics", Forbes.com, 27 de octubre de 2008, www.forbes.com/2008/10/25/credit-card-theft-tecurity-cz_tb1024theft.html)

La seguridad es una medida de la capacidad del sistema para proteger los datos y la información de accesos no autorizados a la vez que proporciona acceso a personas y sistemas autorizados. Una acción tomada contra un sistema informático con la intención de hacer daño se llama un ataque y puede tomar varias formas. Puede ser un intento no autorizado de acceder a datos o servicios o modificar datos, o puede estar destinado a negar servicios a usuarios legítimos.

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

1. *Confidencialidad* es la propiedad de que los datos o servicios están protegidos contra el acceso no autorizado. Por ejemplo, un pirata informático no puede acceder a sus declaraciones de impuestos sobre la renta en una computadora del gobierno.

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

3. La *disponibilidad* es la propiedad de que el sistema estará disponible para uso legítimo. Por ejemplo, un ataque de denegación de servicio no le impedirá pedir un libro de 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 en una transacción y verifica si son realmente quienes dicen ser. Por ejemplo,

cuando recibe un correo electrónico que pretende provenir de un banco, la autenticación garantiza que realmente proviene del banco.

5. El no *rechazo* garantiza que el remitente de un mensaje no puede negar más tarde haber enviado el mensaje y que el destinatario no puede negar haber recibido el mensaje. Por ejemplo, no puede denegar el pedido de algo desde Internet, o el comerciante no puede negarse a recibir su pedido.

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

Usaremos estas características en nuestros escenarios generales de seguridad. Los enfoques para lograr la seguridad se pueden caracterizar como aquellos que detectan ataques, aquellos que resisten los ataques, aquellos que reaccionan a los ataques y aquellos que se recuperan de ataques exitosos. Los objetos que están protegidos contra ataques son datos en reposo, datos en tránsito y procesos computacionales.

9.1. ESCENARIO DE SEGURIDAD GENERAL

Una técnica que se utiliza en el dominio de seguridad es el modelado de amenazas. Los ingenieros de seguridad utilizan un "árbol de ataque", similar a un árbol de fallas que se analiza en el Capítulo 5 , para determinar posibles amenazas. La raíz es un ataque exitoso y los nodos son posibles causas directas de ese ataque exitoso. Los nodos hijos descomponen las causas directas, y así sucesivamente. 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 a través del monitoreo de sus actividades. A partir de estas consideraciones, ahora podemos describir las partes individuales de un escenario general de seguridad. Estos se resumen en la Tabla 9.1 , y en la Figura 9.1 se presenta un ejemplo de escenario de seguridad .

Tabla 9.1. Escenario de Seguridad General

Portion of Scenario	Possible Values
Source	Human or another system which may have been previously identified (either correctly or incorrectly) or may be currently unknown. A human attacker may be from outside the organization or from inside the organization.
Stimulus	Unauthorized attempt is made to display data, change or delete data, access system services, change the system's behavior, or reduce availability.
Artifact	System services, data within the system, a component or resources of the system, data produced or consumed by the system
Environment	The system is either online or offline; either connected to or disconnected from a network; either behind a firewall or open to a network; fully operational, partially operational, or not operational.
Response	Transactions are carried out in a fashion such that ▪ Data or services are protected from unauthorized access. ▪ Data or services are not being manipulated without authorization. ▪ Parties to a transaction are identified with assurance. ▪ The parties to the transaction cannot repudiate their involvements. ▪ The data, resources, and system services will be available for legitimate use. The system tracks activities within it by ▪ Recording access or modification ▪ Recording attempts to access data, resources, or services ▪ Notifying appropriate entities (people or systems) when an apparent attack is occurring
Response Measure	One or more of the following: ▪ How much of a system is compromised when a particular component or data value is compromised ▪ How much time passed before an attack was detected ▪ How many attacks were resisted ▪ How long does it take to recover from a successful attack ▪ How much data is vulnerable to a particular attack

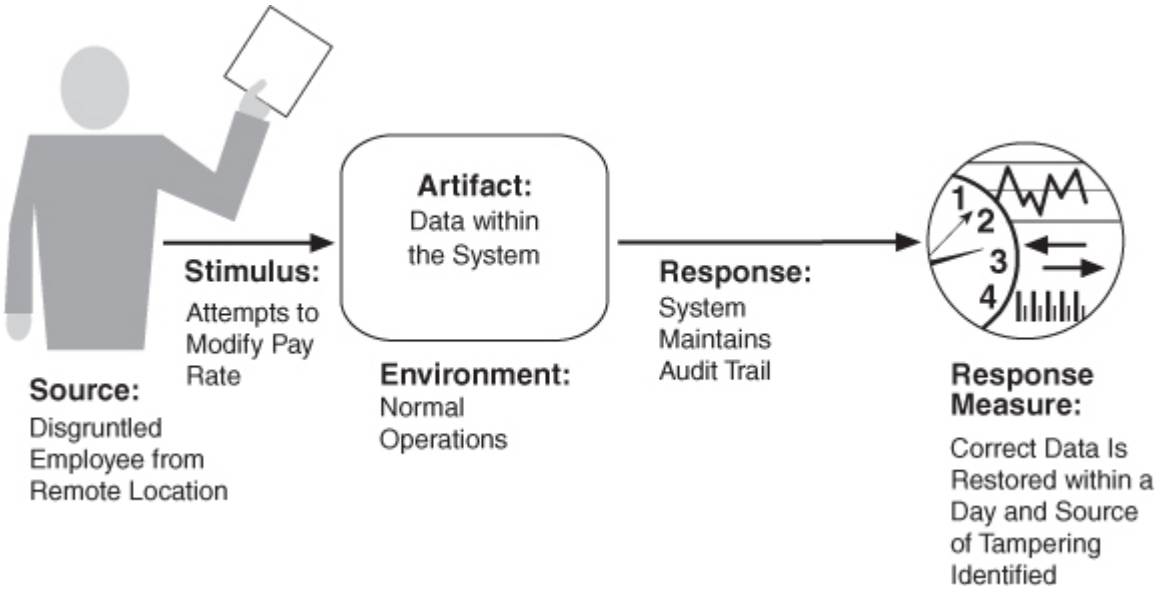

Figura 9.1. Ejemplo de escenario de seguridad concreto.

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

• *Estímulo*. El estímulo es un ataque. Caracterizamos esto como un intento no autorizado de mostrar datos, cambiar o eliminar datos, acceder a 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 son vulnerables.

• *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 operativo.

• *Respuesta*. El sistema debe garantizar que las transacciones se realicen de manera tal que los datos o servicios estén protegidos contra el acceso no autorizado; los datos o servicios no están siendo manipulados sin autorización; las partes en una transacción son identificadas con seguridad; las partes en la transacción no pueden

repudiar sus implicaciones; y los datos, recursos y servicios del sistema estarán disponibles para uso legítimo.

El sistema también debe realizar un seguimiento de las actividades dentro de él mediante el registro de acceso o modificación; intentos de acceso a datos, recursos o servicios; y notificar a las entidades apropiadas (personas o sistemas) cuando se está produciendo un ataque aparente.

• *Medida de respuesta* . Las medidas de la respuesta de un sistema incluyen cuánto se compromete un sistema cuando se compromete un componente o un valor de datos en particular, cuánto tiempo pasó antes de que se detectara un ataque, cuántos ataques se resistieron, cuánto tiempo tomó recuperarse de un ataque exitoso, y cuánta información fue vulnerable a un ataque en particular.

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

9.2. TÁCTICAS PARA LA SEGURIDAD

Un método para pensar cómo lograr la seguridad en un sistema es pensar en la seguridad física. Las instalaciones seguras tienen acceso limitado (p. Ej., Mediante el uso de puntos de control de seguridad), tienen medios para detectar intrusos (p. Ej., Al exigir que los visitantes legítimos usen distintivos), tienen mecanismos de disuasión como guardias armados, mecanismos de reacción como el bloqueo automático de las puertas, y Disponer de mecanismos de recuperación tales como copias de seguridad fuera del sitio. Estas conducen a nuestras cuatro categorías de tácticas: detectar, resistir, reaccionar y recuperarse. La figura 9.2 muestra estas categorías como el objetivo de las tácticas de seguridad.

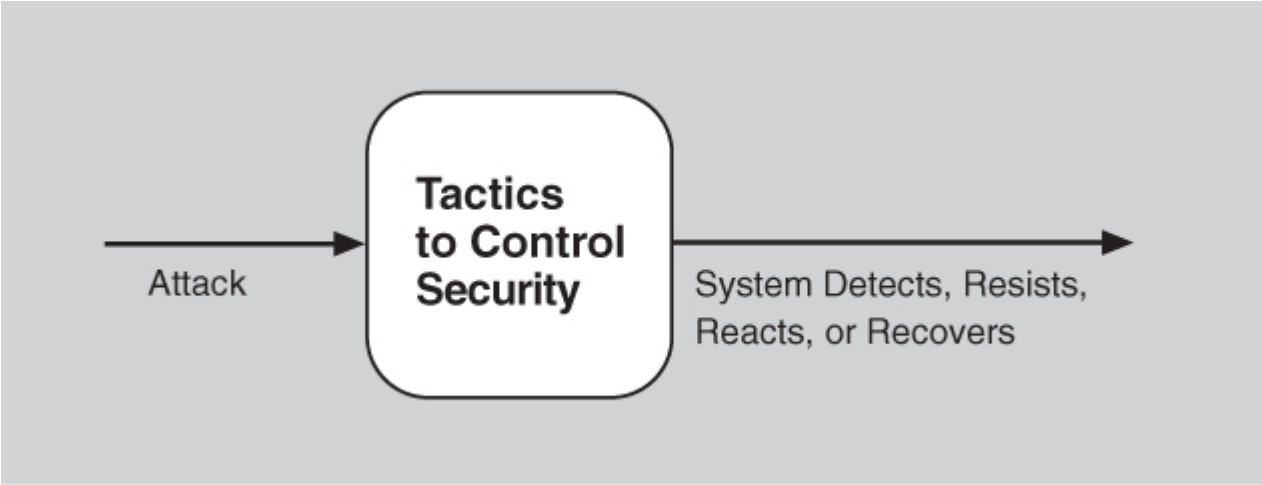

Figura 9.2. El objetivo de las tácticas de seguridad.

Detectar ataques

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

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

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

• *Verificar la integridad del mensaje*. Esta táctica emplea técnicas como sumas de comprobación o valores hash para verificar la integridad de los mensajes, archivos de recursos, 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 los archivos y mensajes de configuración, y utiliza esta información redundante para verificar el archivo o mensaje de configuración cuando se usa. Un valor de hash es una cadena única generada por una función de hashing cuya entrada podría ser archivos de configuración o mensajes. Incluso un ligero cambio en los archivos o mensajes originales produce un cambio significativo en el valor de hash.

• El *retraso en la detección de mensajes* está destinado a detectar posibles ataques de intermediarios, en los que una parte maliciosa está interceptando (y posiblemente modificando) los mensajes. Al verificar el tiempo que se tarda en entregar un mensaje, es posible detectar un comportamiento de tiempo sospechoso, donde el tiempo que se tarda en entregar un mensaje es muy variable.

Resistir los ataques

Existen varios medios 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 de ID de usuario. Otros sistemas pueden ser "identificados" a través de códigos de acceso, direcciones IP, protocolos, puertos, etc.

• *Autenticar actores* . Autenticación significa asegurarse de que un actor (un usuario o una computadora remota) sea realmente quién o lo que pretende ser. Las contraseñas, las contraseñas de un solo uso, los certificados digitales y la identificación biométrica proporcionan un medio para la autenticación.

• *Autorizar a los actores* . La autorización significa garantizar que un actor autenticado tenga los derechos para acceder y modificar datos o servicios. Este mecanismo generalmente se habilita al proporcionar algunos mecanismos de control de acceso dentro de un sistema. El control de acceso puede ser por un actor o por una clase de actor. Las clases de actores pueden definirse por grupos de actores, por roles de actores o por listas de individuos.

• *Limitar el acceso* . Limitar el acceso a los recursos informáticos implica limitar el acceso a recursos como la memoria, las conexiones de red o los puntos de acceso. Esto se puede lograr utilizando la protección de memoria, bloqueando un host, cerrando un puerto o rechazando un protocolo. Por ejemplo, una zona desmilitarizada (DMZ) se usa cuando una organización quiere permitir que los usuarios externos accedan a ciertos servicios y no accedan a otros servicios. Se encuentra entre Internet y un firewall frente a la intranet interna. El firewall es un único punto de acceso a la intranet (límite de exposición). También restringe el acceso utilizando una variedad de técnicas para autorizar a los usuarios (autorizar a los actores).

• *Limite la exposición*. La táctica de exposición límite minimiza la superficie de ataque de un sistema. Esta táctica se enfoca en reducir la

probabilidad y minimizar los efectos del daño causado por una acción hostil. Es una defensa pasiva porque no impide proactivamente que los atacantes hagan daño. La exposición límite se realiza normalmente al tener el menor número posible de puntos de acceso para recursos, datos o servicios y al reducir el número de conectores que pueden proporcionar una exposición no anticipada.

• *Cifrar datos* . Los datos deben estar protegidos del acceso no autorizado. La confidencialidad se logra usualmente aplicando algún tipo de cifrado a los datos y a la comunicación. El cifrado proporciona protección adicional a los 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 controles de autorización. En tales casos, el cifrado es la única protección para pasar datos a través de enlaces de comunicación de acceso público. El enlace puede ser implementado por una red privada virtual (VPN) o por un Secure Sockets Layer (SSL) para un enlace basado en la web. El cifrado puede ser simétrico (ambas partes usan la misma clave) o asimétrico (claves públicas y privadas).

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

• *Cambiar la configuración predeterminada* . Muchos sistemas tienen configuraciones predeterminadas asignadas cuando se entrega el sistema. Forzar al usuario a cambiar esa configuración evitará que los atacantes obtengan acceso al sistema a través de configuraciones que, en general, están disponibles al público.

Reaccionar a los ataques

Varias tácticas están destinadas a responder a un ataque potencial:

• *Revocar el acceso*. Si el sistema o un administrador del sistema cree que un ataque está en curso, entonces el acceso puede estar muy limitado a recursos sensibles, incluso para usuarios y usos normalmente legítimos. Por ejemplo, si su escritorio se ha visto

afectado 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 posible ataque. Muchos sistemas limitan el acceso desde una computadora en particular si hay repetidos intentos fallidos 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 continuos pueden requerir la acción de los operadores, otro personal o sistemas de cooperación. Dicho personal o sistemas, el conjunto de actores relevantes, deben ser notificados cuando el sistema haya 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, los servidores adicionales o las conexiones de red pueden mantenerse en reserva para tal propósito. Dado que un ataque exitoso puede considerarse como un tipo de falla, el conjunto de tácticas de disponibilidad (del Capítulo 5) que se ocupa de recuperarse de una falla también se puede aplicar para este aspecto de la seguridad.

Además de las tácticas de disponibilidad que permiten la restauración de servicios, necesitamos mantener un registro de auditoría. Realizamos auditorías, 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 e identificarlo. Podemos analizar pistas de auditoría para intentar procesar a los atacantes o para crear mejores defensas en el futuro.

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

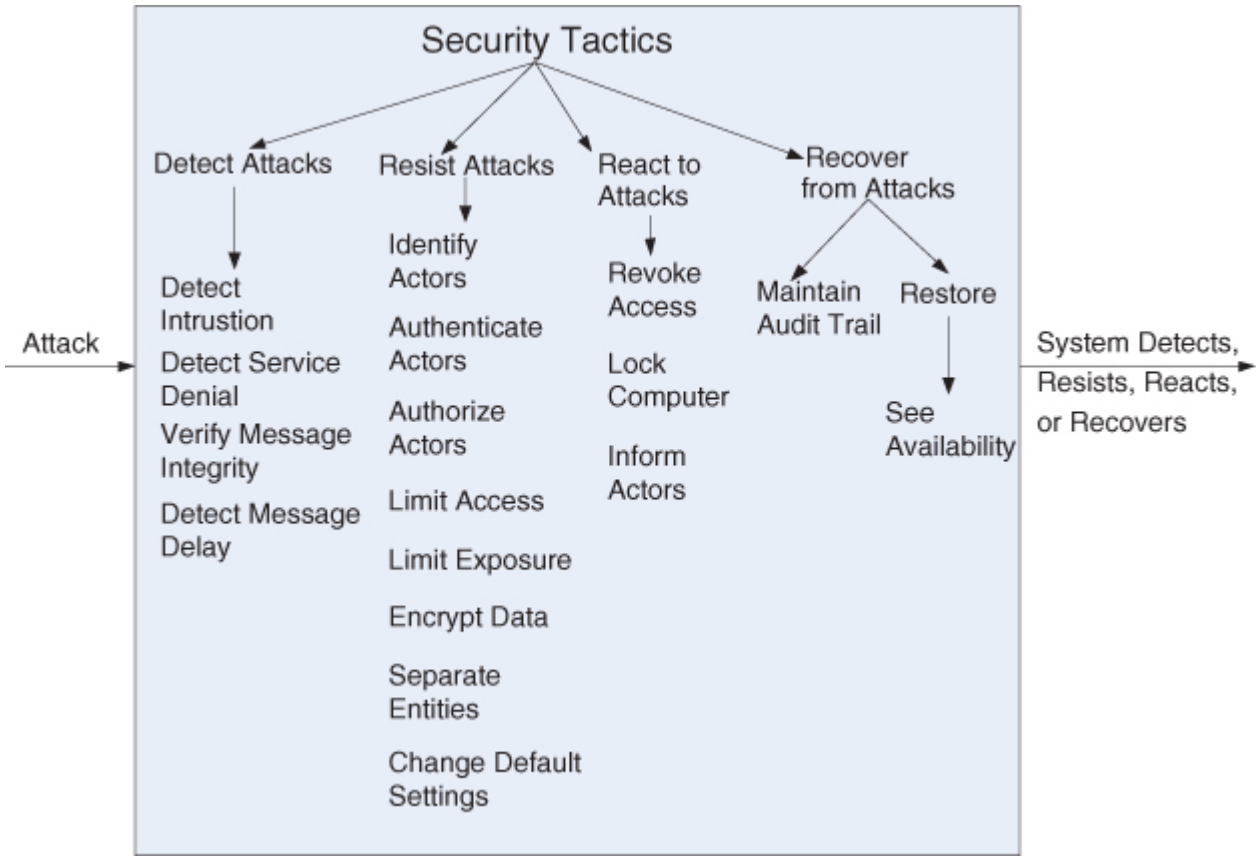

Figura 9.3. Tácticas de seguridad

9.3. UNA LISTA DE VERIFICACIÓN DE DISEÑO PARA LA SEGURIDAD

La Tabla 9.2 es una lista de verificación para respaldar el proceso de diseño y análisis para la seguridad.

Tabla 9.2. Lista de verificación para apoyar el proceso de diseño y análisis para la seguridad

Category	Checklist
Allocation of Responsibilities	Determine which system responsibilities need to be secure. For each of these responsibilities, ensure that additional responsibilities have been allocated to do the following: ▪ Identify the actor ▪ Authenticate the actor ▪ Authorize actors ▪ Grant or deny access to data or services ▪ Record attempts to access or modify data or services ▪ Encrypt data ▪ Recognize reduced availability for resources or services and inform appropriate personnel and restrict access ▪ Recover from an attack ▪ Verify checksums and hash values
Coordination Model	Determine mechanisms required to communicate and coordinate with other systems or individuals. For these communications, ensure that mechanisms for authenticating and authorizing the actor or system, and encrypting data for transmission across the connection, are in place. Ensure also that mechanisms exist for monitoring and recognizing unexpectedly high demands for resources or services as well as mechanisms for restricting or terminating the connection.
Data Model	Determine the sensitivity of different data fields. For each data abstraction: ▪ Ensure that data of different sensitivity is separated. ▪ Ensure that data of different sensitivity has different access rights and that access rights are checked prior to access. ▪ Ensure that access to sensitive data is logged and that the log file is suitably protected. ▪ Ensure that data is suitably encrypted and that keys are separated from the encrypted data. ▪ Ensure that data can be restored if it is inappropriately modified.

Mapping among Architectural Elements	Determine how alternative mappings of architectural elements that are under consideration may change how an individual or system may read, write, or modify data; access system services or resources; or reduce availability to system services or resources. Determine how alternative mappings may affect the recording of access to data, services or resources and the recognition of unexpectedly high demands for resources. For each such mapping, ensure that there are responsibilities to do the following: ▪ Identify an actor ▪ Authenticate an actor ▪ Authorize actors ▪ Grant or deny access to data or services ▪ Record attempts to access or modify data or services ▪ Encrypt data ▪ Recognize reduced availability for resources or services, inform appropriate personnel, and restrict access ▪ Recover from an attack
Resource Management	Determine the system resources required to identify and monitor a system or an individual who is internal or external, authorized or not authorized, with access to specific resources or all resources. Determine the resources required to authenticate the actor, grant or deny access to data or resources, notify appropriate entities (people or systems), record attempts to access data or resources, encrypt data, recognize inexplicably high demand for resources, inform users or systems, and restrict access.

	For these resources consider whether an external entity can access a critical resource or exhaust a critical resource; how to monitor the resource; how to manage resource utilization; how to log resource utilization; and ensure that there are sufficient resources to perform the necessary security operations. Ensure that a contaminated element can be prevented from contaminating other elements. Ensure that shared resources are not used for passing sensitive data from an actor with access rights to that data to an actor without access rights to that data.
Binding Time	Determine cases where an instance of a late-bound component may be untrusted. For such cases ensure that late-bound components can be qualified; that is, if ownership certificates for late-bound components are required, there are appropriate mechanisms to manage and validate them; that access to late-bound data and services can be managed; that access by late-bound components to data and services can be blocked; that mechanisms to record the access, modification, and attempts to access data or services by late-bound components are in place; and that system data is encrypted where the keys are intentionally withheld for late-bound components
Choice of Technology	Determine what technologies are available to help user authentication, data access rights, resource protection, and data encryption. Ensure that your chosen technologies support the tactics relevant for your security needs.

9.4. RESUMEN

Los ataques contra un sistema pueden caracterizarse como ataques contra la confidencialidad, integridad o disponibilidad de un sistema o sus datos. La confidencialidad significa mantener los datos lejos de aquellos que no deberían tener acceso y otorgar acceso a los que deberían. La integridad significa que no hay modificaciones no autorizadas o eliminación de datos, y la disponibilidad significa que el sistema es accesible para aquellos que tienen derecho a usarlo.

El énfasis de distinguir varias clases de actores en la caracterización lleva a muchas de las tácticas utilizadas para lograr la seguridad. Identificar, autenticar y autorizar a los actores son tácticas destinadas a determinar qué usuarios o sistemas tienen derecho a qué tipo de acceso a un sistema.

Se asume que ninguna táctica de seguridad es infalible y que los sistemas se verán comprometidos. Por lo tanto, existen tácticas para

detectar un ataque, limitar la propagación de cualquier ataque y para reaccionar y recuperarse de un ataque.

Recuperarse de un ataque implica muchas de las mismas tácticas que la disponibilidad y, en general, implica devolver el sistema a un estado coherente antes de cualquier ataque.