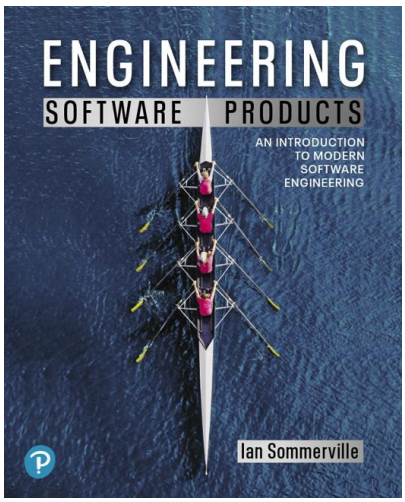
Ingeniería. Productos de Software

Primera Edición



Capítulo 7

Seguridad y Privacidad

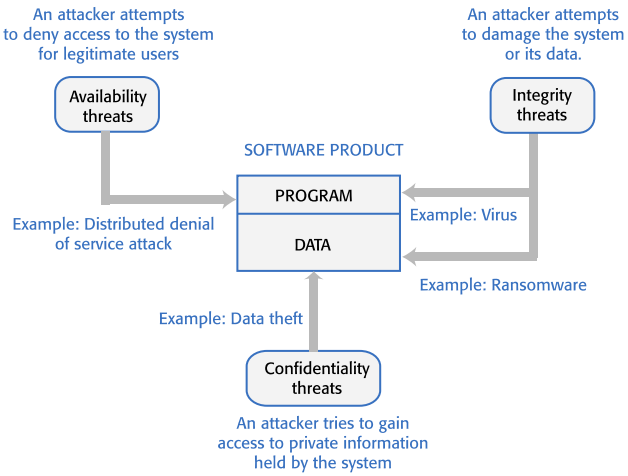
1

Seguridad del software

- La seguridad del software debería ser siempre un asunto de alta prioridad para los desarrolladores de productos y sus usuarios.
- Si no se prioriza la seguridad, los proveedores de productos de software y sus clientes inevitablemente sufrirán pérdidas como resultado de ataques maliciosos.
- En el peor caso, estos ataques podrían dejar a los proveedores de productos fuera del mercado.
  - Si los productos no están disponibles o si los datos de los clientes se comprometen, los clientes pueden cancelar sus suscripciones.
- Incluso, si se pueden recuperar de los ataques, ello tomará tiempo y esfuerzo que hubiese sido mejor utilizar trabajando en el software.

2

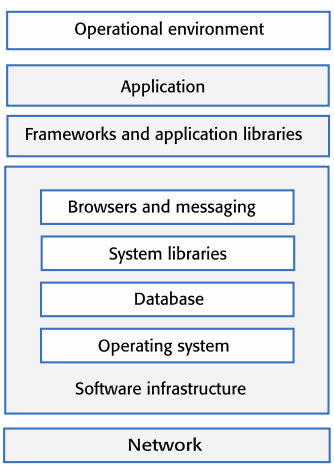
Figura 7.1



Tipos de amenazas de seguridad

3

Figure 7.2



Pila de infraestructura del sistema

4

Tabla 7.1 Gestión de seguridad

Procedimiento	Explicación
Autenticación y autorización	Se deben tener estándares y procedimientos de autenticación y autorización que garanticen que todos los usuarios tengan una autenticación sólida y que hayan configurado correctamente los permisos de acceso. Esto minimiza el riesgo de que usuarios no autorizados accedan a los recursos del sistema.
Gestión de infraestructura del sistema	El software de infraestructura se debe configurar correctamente y se deben aplicar las actualizaciones de seguridad, que corrigen las vulnerabilidades, tan pronto como estén disponibles.
Monitoreo de ataques	El sistema se debe revisar regularmente para detectar posibles accesos no autorizados. Si se detectan ataques, es posible implementar estrategias de resistencia que minimicen los efectos del ataque.
Respaldo	Se deben implementar políticas de respaldo para garantizar que se mantengan copias no dañadas de los archivos de programa y datos. Estos se pueden restaurar después de un ataque.

5

Seguridad operacional (1 de 2)

- La seguridad operacional se centra en ayudar a los usuarios a mantener la seguridad. Los ataques de usuario intentan engañar a los usuarios para que divulguen sus credenciales o accedan a un sitio web que incluye malware, tal como un sistema de registro de claves.

6

Seguridad operacional (2 de 2)

- Procedimientos y prácticas de seguridad operacional
  - Cierre de sesión automático, que soluciona el problema común de que los usuarios se olvidan de cerrar la sesión desde un equipo utilizado en un espacio compartido.
  - Registro de comandos de usuario, que permite descubrir las acciones realizadas por los usuarios que han dañado deliberadamente o accidentalmente algunos recursos del sistema.
  - Autenticación multifactor, que reduce las posibilidades de que un intruso obtenga acceso al sistema mediante credenciales robadas.

7

Ataques de inyección

- Los ataques de inyección son un tipo de ataque en el que un usuario malintencionado utiliza un campo de entrada válido para introducir comandos de código malintencionado o de base de datos.
- Estas instrucciones maliciosas se ejecutan, causando algunos daños en el sistema. Se puede inyectar código que filtra los datos del sistema a los atacantes.
- Los tipos comunes de ataque de inyección incluyen ataques de desbordamiento de búfer y ataques de envenenamiento SQL (o ataques de inyección SQL).

8

Ataques de inyección SQL

- Los ataques de inyección SQL son ataques a productos de software que utilizan una base de datos SQL.
- Aprovechan una situación en la que se utiliza una entrada de usuario como parte de un comando SQL.
- Un usuario malintencionado utiliza un campo de entrada de un formulario para introducir un fragmento SQL que permite el acceso a la base de datos.
- El campo del formulario se agrega a la consulta SQL, que se ejecuta y devuelve la información al atacante.

9

Ataques cross-site scripting (1 de 2)

- Los ataques cross-site scripting son otra forma de ataque de inyección.
- Un atacante agrega código JavaScript malicioso a la página web que se devuelve desde un servidor a un cliente y este script se ejecuta cuando la página se muestra en el navegador del usuario.

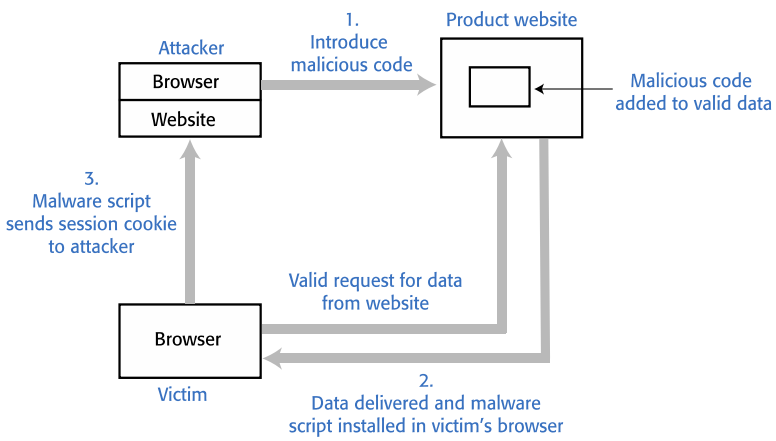
10

Ataques cross-site scripting (2 de 2)

- El script malicioso puede robar información de clientes o dirigirlos a otro sitio web.
  - El script puede tratar de capturar datos personales o mostrar anuncios (publicidad).
  - Las cookies pueden ser robadas, lo que hace posible un ataque de secuestro de sesión.
- Al igual que con otros tipos de ataque de inyección, los ataques cross-site scripting se pueden evitar mediante la validación de la entrada.

11

Figura 7.3



Ataque cross-site scripting

12

Ataques de secuestro de sesión (1 de 2)

- Cuando un usuario se autentica con una aplicación web, se crea una sesión.
  - Una sesión es un período de tiempo durante el cual la autenticación del usuario es válida. No tienen que volver a autenticarse para cada interacción con el sistema.
  - El proceso de autenticación implica colocar una cookie de sesión en el dispositivo del usuario.
- El secuestro de sesión es un tipo de ataque donde un atacante se apodera de una cookie de sesión y la utiliza para hacerse pasar por un usuario legítimo.

13

Ataques de secuestro de sesión (2 de 2)

- Hay varias maneras en que un atacante puede averiguar el valor de una cookie de sesión, incluidos los ataques de cross-site scripting y monitoreo de tráfico
  - En un ataque cross-site scripting, el malware instalado envía cookies de sesión a los atacantes.
  - El monitoreo de tráfico implica que los atacantes capturen el tráfico entre el cliente y el servidor. La cookie de sesión se puede identificar analizando los datos intercambiados.

14

Tabla 7.2 Acciones para reducir la probabilidad de hackeo

Acción	Explicación
Cifrado de tráfico	Cifrar siempre el tráfico de red entre los clientes y el servidor. Esto significa configurar sesiones mediante https en lugar de http. Si el tráfico está cifrado, es más difícil monitorear para hallar cookies de sesión.
autenticación multifactor	Utilizar siempre la autenticación multifactor y solicitar la confirmación de nuevas acciones que puedan ser perjudiciales. Por ejemplo, antes de que se acepte una nueva solicitud de beneficiario, se puede pedir al usuario que confirme su identidad introduciendo un código enviado a su teléfono. También se puede solicitar que se introduzcan caracteres de contraseña antes de cada acción potencialmente perjudicial, como la transferencia de fondos.
Tiempos de espera cortos	Utilizar tiempos de espera relativamente cortos en las sesiones. Si no ha habido ninguna actividad en una sesión durante unos minutos, la sesión se debe finalizar y las solicitudes futuras ser dirigidas a una página de autenticación. Esto reduce la probabilidad de que un atacante pueda acceder a una cuenta si un usuario legítimo se olvida de cerrar la sesión cuando ha terminado de trabajar.

15

Ataques de denegación de servicio (1 de 2)

- Los ataques de denegación de servicio (DoS) son ataques a un sistema de software que están destinados a hacer que ese sistema no esté disponible para su uso normal.
- Los ataques distribuidos de denegación de servicio (DDoS) son el tipo más común de ataques de denegación de servicio.
  - Estos implican equipos distribuidos, que por lo general han sido secuestrados como parte de una botnet, enviando cientos de miles de solicitudes de servicio a una aplicación web. Hay tantas solicitudes de servicio que se deniega el acceso a los usuarios legítimos.

16

Ataques de denegación de servicio (2 de 2)

- Otros tipos de ataques de denegación de servicio se dirigen a los usuarios de aplicaciones.
  - Los ataques de bloqueo de usuario aprovechan una directiva de autenticación común que bloquea a un usuario después de varios intentos de autenticación fallidos. Su objetivo es bloquear a los usuarios en lugar de obtener acceso y así denegar el servicio a estos usuarios.
  - Los usuarios a menudo utilizan su dirección de correo electrónico como su nombre de inicio de sesión por lo que si un atacante tiene acceso a una base de datos de direcciones de correo electrónico, él o ella puede intentar iniciar sesión con estas direcciones.
- Si no se bloquean las cuentas después de una validación fallida, los atacantes pueden usar ataques de fuerza bruta en contra del sistema. Si se bloquean, se puede denegar el acceso a usuarios legítimos.

Ataques de fuerza bruta (1 de 2)

- Los ataques de fuerza bruta son ataques a una aplicación web donde el atacante tiene cierta información, como un nombre de inicio de sesión válido, pero no tiene la contraseña del sitio.
- El atacante crea diferentes contraseñas e intenta iniciar sesión con cada una de ellas. Si el inicio de sesión falla, vuelve a intentarlo con una contraseña diferente.
  - Los atacantes pueden utilizar un generador de strings que genera todas las combinaciones posibles de letras y números y utilizarlos como contraseñas.
  - Para acelerar el proceso de detección de contraseñas, los atacantes aprovechan el hecho de que muchos usuarios eligen contraseñas fáciles de recordar. Comienzan probando contraseñas de las listas publicadas con las contraseñas más comunes.

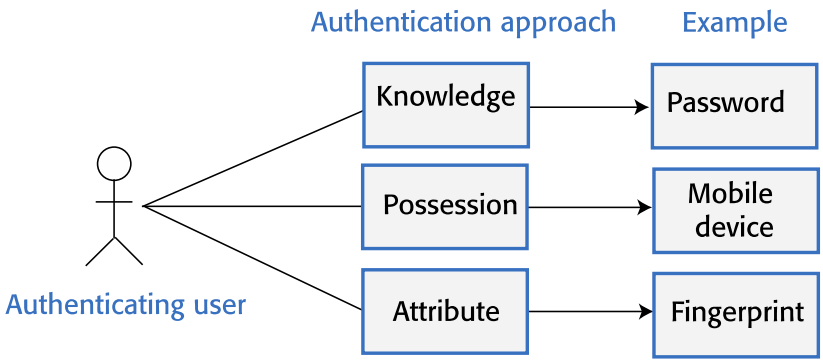
Ataques de fuerza bruta (2 de 2)

- Los ataques de fuerza bruta se realizan basándose en que los usuarios definen contraseñas débiles, por lo que es posible evitarlos insistiéndole a los usuarios que definan contraseñas largas (ocho o más caracteres), que no aparezcan en diccionarios o sean palabras de uso común.

Autenticación

- La autenticación es el proceso de asegurarse que un usuario de un sistema sea quien dice ser.
- Se necesita autenticación en todos los productos de software que mantienen información de usuario, para que solo los proveedores de esa información puedan acceder a ella y cambiarla.
- También se usa autenticación para obtener información sobre los usuarios que permita personalizar sus experiencias de uso del producto.

Figura 7.4



Enfoques de autenticación

Métodos de autenticación (1 de 2)

- Autenticación basada en conocimiento
  - El usuario proporciona información secreta y personal cuando se registra en el sistema. Cada vez que inicia sesión, el sistema le pide esta información.
- Autenticación basada en posesión
  - Esta se basa en que el usuario tiene un dispositivo físico (como un teléfono móvil) que puede generar o mostrar información que es conocida por el sistema de autenticación. El usuario introduce esta información para confirmar que posee el dispositivo de autenticación.

Métodos de autenticación (2 de 2)

- La autenticación basada en atributos se basa en un atributo biométrico único del usuario, como una huella digital, que se registra en el sistema.
- La autenticación multifactor combina estos enfoques y requiere que los usuarios utilicen más de un método de autenticación.

23

Tabla 7.3 Debilidades de la autenticación basada en contraseña

Debilidad	Explicación
Contraseñas inseguras	Los usuarios eligen contraseñas que son fáciles de recordar. Sin embargo, también es fácil para los atacantes adivinar o generar estas contraseñas, utilizando un diccionario o un ataque de fuerza bruta.
Ataques de phishing	Los usuarios hacen clic en un enlace de correo electrónico que apunta a un sitio falso que intenta recopilar sus datos de inicio de sesión y contraseña.
Reutilización de contraseñas	Los usuarios utilizan la misma contraseña para varios sitios. Si hay una brecha de seguridad en uno de estos sitios, los atacantes tienen contraseñas que pueden probar en otros sitios.
Contraseñas olvidadas	Los usuarios olvidan regularmente sus contraseñas, por lo que se debe configurar un mecanismo de recuperación de contraseña para permitir que se restablezcan. Esto puede ser una vulnerabilidad si las credenciales de los usuarios han sido robadas y los atacantes utilizan ese mecanismo para restablecer sus contraseñas.

24

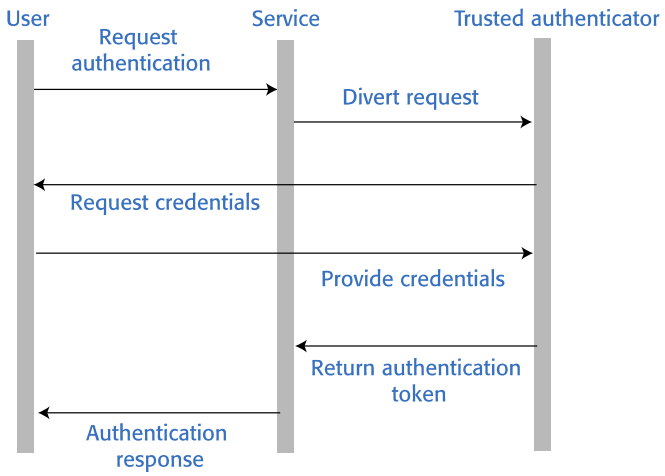
Identidad federada (1 de 2)

- La identidad federada es un enfoque de autenticación en el que se utiliza un servicio de autenticación externo.
- 'Iniciar sesión con Google’ e 'Iniciar sesión con Facebook' son ejemplos ampliamente utilizados de autenticación utilizando identidad federada.
- La ventaja de la identidad federada para un usuario es que tiene un único conjunto de credenciales almacenadas por un servicio de identidad de confianza.

Identidad federada (2 de 2)

- En lugar de iniciar sesión directamente en un servicio, un usuario proporciona sus credenciales a un servicio conocido que confirma su identidad en el servicio de autenticación.
- No tienen que realizar un seguimiento de diferentes ids y contraseñas de usuario. Debido a que sus credenciales se almacenan en menos lugares, se reducen las posibilidades de una brecha de seguridad desde donde se puedan vulnerar.

Figura 7.5



Identidad federada

27

Autorización (1 de 2)

- La autenticación implica que un usuario pruebe su identidad en un sistema de software.
- La autorización es un proceso complementario en el que esa identidad se utiliza para controlar el acceso a los recursos del sistema de software.
  - Por ejemplo, si usted usa una carpeta compartida en Dropbox, el propietario de la carpeta puede autorizarlo a leer el contenido de esa carpeta, pero no a añadir nuevos archivos o sobrescribir archivos en la carpeta.

28

Autorización (2 de 2)

- Cuando una empresa desea definir el tipo de acceso que los usuarios obtienen a los recursos, esto se basa en una política de control de acceso.
- Esta política es un conjunto de reglas que definen qué información (datos y programas) se controla, quién tiene acceso a esa información y el tipo de acceso que se permite.

Políticas de control de acceso

- Las políticas explícitas de control de acceso son importantes tanto por razones legales como técnicas.
  - Las normas de protección de datos limitan el acceso a los datos personales y esto debe reflejarse en la política de control de acceso definida. Si esta política está incompleta o no se ajusta a las normas de protección de datos, puede haber acciones legales posteriores en caso de una violación de datos.
  - Técnicamente, una política de control de acceso puede ser un punto de partida para configurar el esquema de control de acceso para un sistema.
  - Por ejemplo, si la política de control de acceso define los derechos de acceso de los estudiantes, cuando se registran nuevos estudiantes, todos obtienen estos derechos de forma predeterminada.

Listas de control de acceso (1 de 2)

- Las listas de control de acceso (ACLs) se utilizan en la mayoría de los sistemas de archivos y bases de datos para implementar políticas de control de acceso.
- Las listas de control de acceso son tablas que vinculan a los usuarios con recursos y especifican lo que se permite hacer a esos usuarios.
  - Por ejemplo, para este libro me gustaría poder configurar una lista de control de acceso para un archivo del libro que permita a los revisores leer el archivo y anotar sus comentarios. Sin embargo, no se les permita editar el texto ni eliminar el archivo.

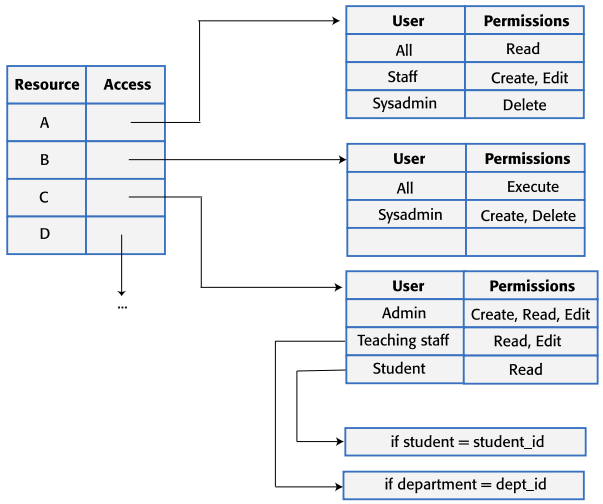
31

Listas de control de acceso (2 de 2)

- Si las listas de control de acceso se basan en permisos individuales, estos pueden llegar a ser muy grandes. Sin embargo, se puede reducir drásticamente su tamaño asignando usuarios a grupos y, a continuación, asignando permisos a los grupos.

32

Figura 7.8



Listas de control de acceso

33

Cifrado (1 de 2)

- El cifrado es el proceso de hacer que un documento sea ilegible mediante la aplicación de una transformación algorítmica.
- El algoritmo de cifrado utiliza una clave secreta como base de esta transformación. Puede decodificar el texto cifrado aplicando la transformación inversa.
- Las técnicas de cifrado modernas son tales que se puede cifrar los datos de modo que sea prácticamente irrompible utilizando la tecnología disponible actualmente.

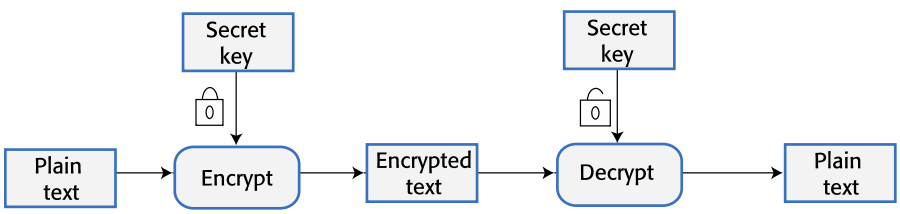
34

Cifrado (2 de 2)

- Sin embargo, la historia ha demostrado que el cifrado, aparentemente fuerte, se puede crackear cuando se dispone de nueva tecnología.
- Cuando se disponga comercialmente de sistemas quantum, se tendrá que usar un enfoque completamente diferente para el cifrado en Internet.

35

Figura 7.9



Cifrado y descifrado

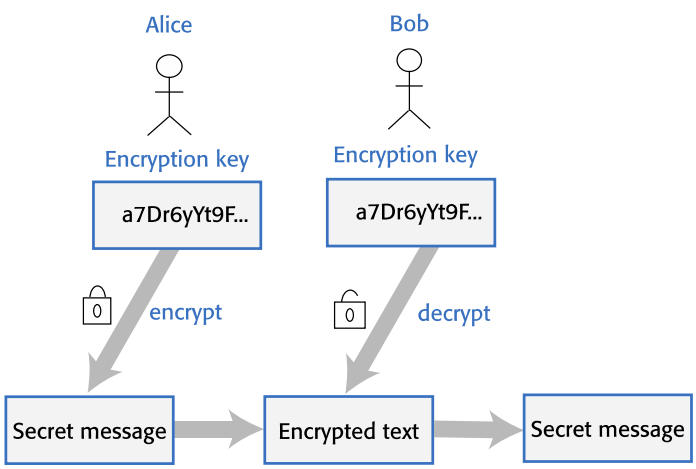
36

Cifrado simétrico

- En un esquema de cifrado simétrico, la misma clave de cifrado se utiliza para codificar y decodificar la información que se debe mantener en secreto.
- Si Alice y Bob desean intercambiar un mensaje secreto, ambos deben tener una copia de la clave de cifrado. Alice cifra el mensaje con esta clave. Cuando Bob recibe el mensaje, lo decodifica usando la misma clave para leer su contenido.
- El problema fundamental con un esquema de cifrado simétrico es compartir de forma segura la clave de cifrado.
- Si Alice simplemente envía la clave a Bob, un atacante puede interceptar el mensaje y obtener acceso a la clave. El atacante puede decodificar todas las comunicaciones secretas futuras.

37

Figura 7.10



Cifrado simétrico

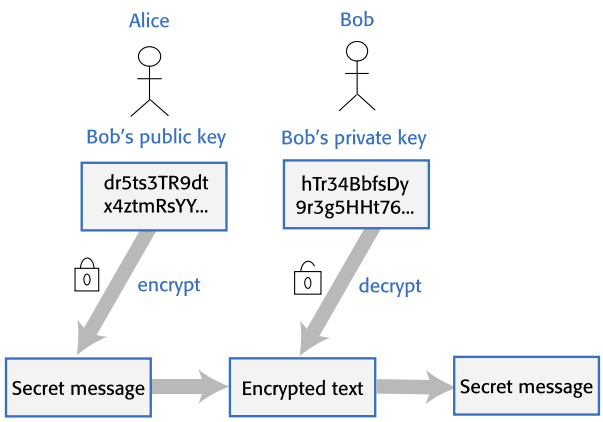
38

Cifrado asimétrico

- El cifrado asimétrico no requiere que se compartan claves secretas.
- Un esquema de cifrado asimétrico utiliza diferentes claves para cifrar y descifrar mensajes.
- Cada usuario tiene una clave pública y una clave privada. Los mensajes se pueden cifrar con cualquiera de las claves, pero solo se pueden descifrar con la otra clave.
- Las claves públicas pueden ser publicadas y compartidas por el propietario de la clave. Cualquier persona puede acceder y utilizar una clave pública publicada.
- Sin embargo, los mensajes solo pueden ser descifrados mediante la clave privada del usuario, por lo que solo es legible por el destinatario previsto.

39

Figura 7.11



Cifrado asimétrico

40

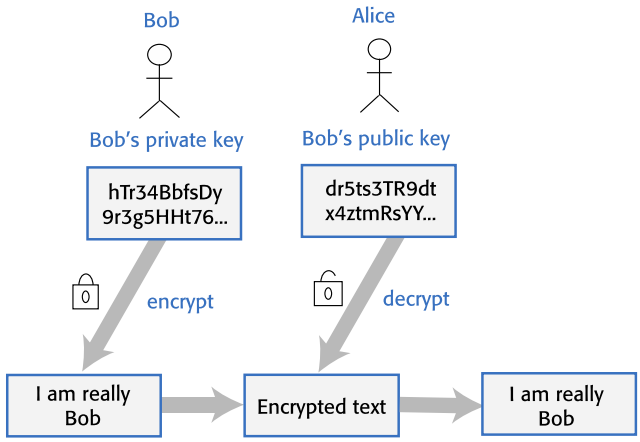
Cifrado y autenticación (1 de 2)

- El cifrado asimétrico también se puede utilizar para autenticar al remitente de un mensaje cifrándolo con una clave privada y descifrándolo con la clave pública correspondiente.
- Supongamos que Alice quiere enviar un mensaje a Bob y ella tiene una copia de la clave pública de Bob.

Cifrado y autenticación (2 de 2)

- Sin embargo, ella no está segura de si la clave pública que tiene de Bob es correcta y le preocupa que el mensaje pueda ser enviado a la persona equivocada.
- El cifrado de clave pública/privada se puede utilizar para verificar la identidad de Bob.
  - Bob usa su clave privada para cifrar un mensaje y envía esto a Alice. Si Alice puede descifrar el mensaje recibido usando la clave pública de Bob, entonces Alice tiene la clave correcta.

Figura 7.12



Cifrado para la autenticación

TLS y certificados digitales (1 de 2)

- El protocolo https es un protocolo estándar para el intercambio seguro de textos en la web. Es el protocolo http estándar más una capa de cifrado llamada TLS (Transport Layer Security). Esta capa de cifrado se utiliza para 2 cosas:
  - para verificar la identidad del servidor web;
  - para cifrar las comunicaciones de modo que no puedan ser leídas por un atacante que intercepta los mensajes entre el cliente y el servidor.

TLS y certificados digitales (2 de 2)

- El cifrado TLS depende de un certificado digital que se envía desde el servidor web al cliente.
  - Los certificados digitales son emitidos por una entidad de certificación (CA), que es un servicio de verificación de identidad de confianza.
  - La CA cifra la información del certificado utilizando su clave privada para crear una firma única. Esta firma se incluye en el certificado junto con la clave pública de la CA. Para comprobar que el certificado es válido, se puede descifrar la firma mediante la clave pública de la CA.

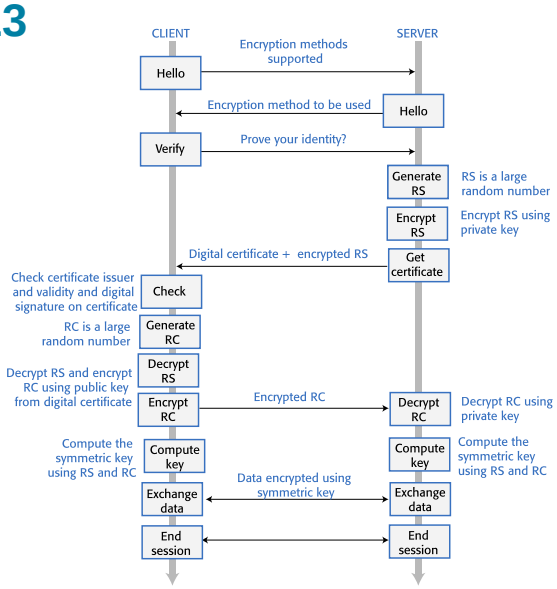
45

Tabla 7.5 Certificados digitales

Elemento del certificado	Explicación
Información del sujeto	Información sobre la empresa o persona cuyo sitio web está siendo visitado. Los solicitantes solicitan un certificado digital de una entidad de certificación que comprueba que el solicitante es una organización válida.
Información de la entidad de certificación	Información sobre la entidad de certificación (CA) que ha emitido el certificado.
Información del certificado	Información sobre el propio certificado, incluido un número de serie único y un período de validez, definido por fechas de inicio y finalización.
Firma digital	La combinación de todos los datos anteriores identifica de forma única el certificado digital. Los datos de firma se cifran con la clave privada de la CA para confirmar que los datos son correctos. También se especifica el algoritmo utilizado para generar la firma digital.
Información clave pública	La clave pública de la CA se incluye junto con el tamaño de la clave y el algoritmo de cifrado utilizado. La clave pública se puede utilizar para descifrar la firma digital.

46

Figura 7.13



Uso de cifrado simétrico y asimétrico en TLS

TLS explicado (1 de 2)

- El certificado digital que el servidor envía al cliente incluye la clave pública del servidor. El servidor también genera un número aleatorio extenso, lo cifra usando su clave privada y lo envía al cliente.
- El cliente puede, entonces, descifrar esto utilizando la clave pública del servidor y, a su vez, genera su propio número aleatorio extenso. Cifra este número mediante la clave pública del servidor y lo envía al servidor, que descifra el mensaje mediante su clave privada. Luego, tanto el cliente como el servidor tienen dos números aleatorios extensos.

TLS explicado (2 de 2)

- El método de cifrado acordado incluye una forma de generar una clave de cifrado a partir de estos números. El cliente y el servidor determinan de forma independiente la clave que se usará para cifrar los mensajes posteriores mediante un enfoque simétrico.
- Todo el tráfico cliente-servidor se cifra y descifra con esa clave determinada. No hay necesidad de intercambiar la clave en sí.

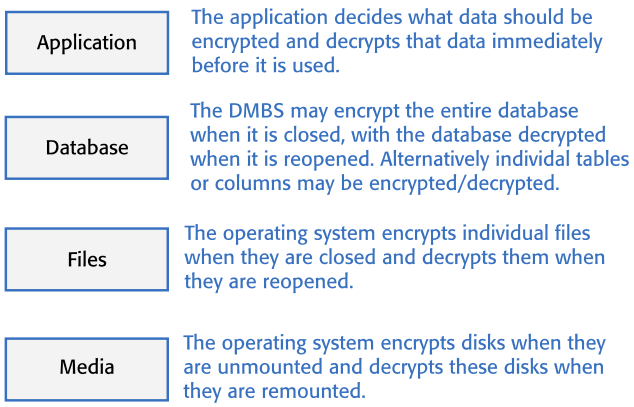
49

Cifrado de datos

- El proveedor de un producto, inevitablemente debe almacenar información sobre sus usuarios y, para productos basados en la nube, datos de usuario.
- El cifrado se puede utilizar para reducir el daño que puede producirse por el robo de datos. Si la información está encriptada, es imposible, o muy difícil, que los ladrones accedan y usen los datos no cifrados.
  - Datos en tránsito.
    Al transferir datos a través de Internet, siempre se debe utilizar el protocolo https en lugar del protocolo http para garantizar el cifrado.
  - Datos en reposo.
    Cuando los datos no estén siendo usados, entonces los archivos que los almacenan se deberían cifrar, de modo que si se roban dichos archivos, ello no provocará que se revelen datos confidenciales.
  - Datos en uso.
    Los datos se están procesando activamente. El cifrado y descifrado de los datos ralentiza el tiempo de respuesta del sistema. La implementación de un mecanismo de búsqueda general con datos cifrados es imposible.

50

Figura 7.14



Niveles de cifrado

Gestión de claves (1 de 2)

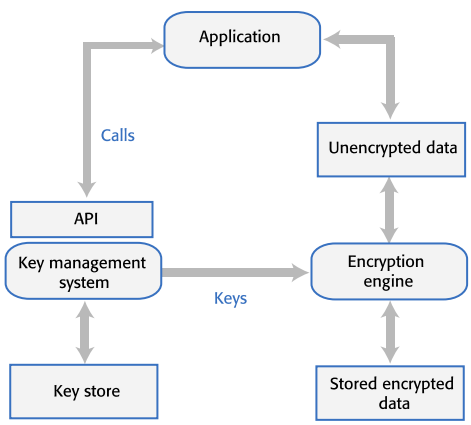
- La gestión de claves es el proceso de garantizar que los usuarios autorizados generen, almacenen y accedan de forma segura a las claves de cifrado.
- Las empresas pueden tener que administrar decenas de miles de claves de cifrado por lo que no es práctico hacer la gestión de claves manualmente y es necesario utilizar algún tipo de sistema automatizado de gestión de claves (KMS).

Gestión de claves (2 de 2)

- La gestión de claves es importante porque, en caso de cometer algún error, usuarios no autorizados pueden acceder a las claves y con ello descifrar datos supuestamente privados. Aún peor, si se pierden claves de cifrado, entonces los datos cifrados podrían ser permanentemente inaccesibles.
- Un sistema de gestión de claves (KMS) es una base de datos especializada que está diseñada para almacenar y administrar de forma segura claves de cifrado, certificados digitales y otra información confidencial.

53

Figura 7.15



Uso de un KMS para la gestión del cifrado

54

Almacenamiento de claves a largo plazo (1 de 2)

- Las empresas pueden estar obligadas a mantener copias de todos sus datos durante varios años debido a la contabilidad y otras regulaciones
  - Por ejemplo, en el Reino Unido, los datos fiscales y de las empresas deben mantenerse durante al menos seis años, con un período de retención más extenso para algunos tipos de datos. Las regulaciones de protección de datos pueden requerir que estos datos se almacenen de forma segura, por lo que los datos deben cifrarse.

55

Almacenamiento de claves a largo plazo (1 de 2)

- Para reducir los riesgos de una brecha de seguridad, las claves de cifrado deben cambiarse regularmente. Esto significa que los datos almacenados (datos históricos) pueden estar cifrados con una clave diferente a la usada para los datos actuales del sistema.
- Por lo tanto, los sistemas de gestión de claves deben mantener varias versiones de claves, con marca de tiempo, para que las copias de seguridad y los archivos (históricos) del sistema se puedan descifrar si es necesario.

56

Privacidad (1 de 2)

- La privacidad es un concepto social que se relaciona con la recopilación, difusión y uso adecuado de la información personal en poder de un tercero, como una empresa o un hospital.
- La importancia de la privacidad ha cambiado con el tiempo y las personas tienen sus propios puntos de vista sobre qué grado de privacidad es importante.

57

Privacidad (2 de 2)

- La cultura y la edad también afectan las opiniones de las personas sobre lo que significa la privacidad.
  - Los más jóvenes fueron los primeros en adoptar las primeras redes sociales y muchos de ellos parecen estar menos inhibidos por compartir información personal en estas plataformas que las personas mayores.
  - En algunos países, el nivel de ingresos obtenido por un individuo se considera un asunto privado; en otros, todas las declaraciones de impuestos (donde aparecen los ingresos obtenidos) se publican abiertamente.

58

Razones comerciales para la privacidad (1 de 2)

- Si se ofrece un producto directamente a los consumidores y no se cumple con las normas de privacidad, entonces se pueden enfrentar acciones legales por parte de los compradores del producto o de un regulador de datos. Si el cumplimiento es parcial y no es posible otorgar la protección ofrecida por las regulaciones de protección de datos en algunos países, no se podrá vender el producto en estos países.

Razones comerciales para la privacidad (2 de 2)

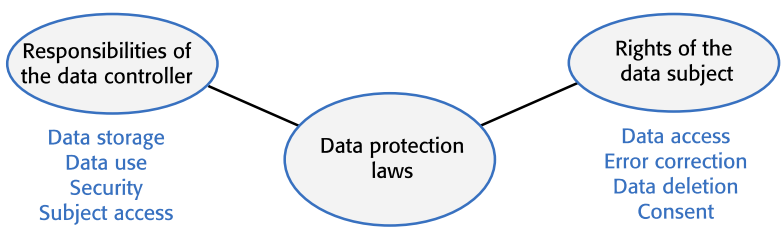
- Si el producto es un producto comercial de una empresa, los clientes de esa empresa requieren garantías de privacidad para que no corran el riesgo de sufrir violaciones de privacidad y acciones legales por parte de los usuarios.
- Si la información personal se filtra o se utiliza incorrectamente, incluso si esto no se ve como una violación de las normas de privacidad, esto puede conducir a graves daños a la reputación. Los clientes pueden dejar de usar el producto debido a esto.

Leyes de protección de datos

- En muchos países, el derecho a la privacidad individual está protegido por las leyes de protección de datos.
- Estas leyes limitan la recopilación, difusión y uso de datos personales a los fines para los que fueron recopilados.
  - Por ejemplo, una empresa de seguros de viaje puede recopilar información médica de sus usuarios para poder evaluar el nivel de riesgo de estos. Ello es legal y permisible.
  - Sin embargo, no sería legal que esas empresas utilizaran esta información para orientar la publicidad en línea de productos de salud, a menos que sus usuarios hubieran dado permiso específico para esto.

61

Figura 7.16



Leyes de protección de datos

62

Tabla 7.6 Principios de protección de datos (1 de 2)

Principio de protección de datos	Explicación
Conciencia y control	Los usuarios de un producto deben ser conscientes de qué datos se recopilan cuando utilizan ese producto, y deben tener control sobre la información personal que se recopila de ellos.
Propósito	Se debe indicar a los usuarios por qué se recopilan datos y estos no se deben utilizar para otros fines.
Consentimiento	Siempre se debe tener el consentimiento de un usuario antes de revelar sus datos a otras personas.
Duración de los datos	No se deben conservar los datos durante más tiempo del necesario. Si un usuario elimina una cuenta, se deben eliminar los datos personales asociados a esa cuenta.

63

Tabla 7.6 Principios de protección de datos (2 de 2)

Principio de protección de datos	Explicación
Almacenamiento seguro	Se deben mantener los datos de forma segura para que no puedan ser manipulados o divulgados a personas no autorizadas.
Descubrimiento y corrección de errores	Se debe permitir que los usuarios descubran qué datos personales se almacenan. Se debe proporcionar una manera para que los usuarios corrijan errores en sus datos personales.
Ubicación	No se deben almacenar datos en países donde se apliquen leyes de protección de datos más débiles a menos que haya un acuerdo explícito de que se mantendrán las normas de protección de datos más estrictas.

64

Política de privacidad (1 de 2)

- Se debe establecer una política de privacidad que defina cómo se recopila, almacena y administra la información personal y confidencial sobre los usuarios.
- Los productos de software utilizan los datos de diferentes maneras, por lo que la política de privacidad tiene que definir los datos personales que se recopilarán y cómo se utilizará esos datos.
- Los usuarios de productos deben poder revisar la política de privacidad y cambiar sus preferencias con respecto a la información que se almacena.

65

Política de privacidad (2 de 2)

- Una política de privacidad es un documento legal y debe ser auditable para comprobar que es coherente con las leyes de protección de datos en los países donde se vende el software asociado.
- Las políticas de privacidad no deben expresarse a los usuarios en un documento de "términos y condiciones" extenso que, en la práctica, nadie lee.
- El RGPD (Reglamento General de Protección de Datos) ahora requiere que las empresas de software incluyan un resumen de la política de privacidad, escrito en un lenguaje sencillo en lugar de usar jerga legal, en el sitio web de la empresa de software.

66

Puntos clave 1 (1 de 2)

- La seguridad es un concepto técnico que se relaciona con la capacidad de un sistema de software para protegerse de ataques maliciosos que pueden amenazar su disponibilidad, la integridad del sistema y/o sus datos, y el robo de información confidencial.
- Los tipos comunes de ataques a productos de software incluyen ataques de inyección, ataques de cross-site scripting, ataques de secuestro de sesión, ataques de denegación de servicio y ataques de fuerza bruta.
- La autenticación puede basarse en algo que un usuario sabe, algo que un usuario tiene o algún atributo físico del usuario.

67

Puntos clave 1 (2 de 2)

- La autenticación federada implica delegar la responsabilidad de la autenticación a un tercero como Facebook o Google, o al servicio de autenticación de una empresa.
- La autorización implica controlar el acceso a los recursos del sistema en función de la identidad autenticada del usuario. Las listas de control de acceso son el mecanismo más utilizado para implementar la autorización.
- El cifrado simétrico implica cifrar y descifrar la información con la misma clave secreta. El cifrado asimétrico utiliza un par de claves: una clave privada y una clave pública. La información cifrada con la clave pública solo se puede descifrar con la clave privada.

68

Puntos clave 2 (1 de 2)

- Un problema importante en el cifrado simétrico es el intercambio de la clave. El protocolo TLS, que se utiliza para proteger el tráfico web, evita este problema mediante el cifrado asimétrico para transferir información utilizada para generar una clave compartida.
- Si el producto almacena datos confidenciales del usuario, estos se deben cifrar cuando no estén en uso.
- Un sistema de gestión de claves (KMS) almacena claves de cifrado. El uso de un KMS es esencial porque una empresa puede tener que administrar miles o incluso millones de claves y puede tener que descifrar los datos históricos que se cifraron con una clave de cifrado obsoleta.

69

Puntos clave 2 (2 de 2)

- La privacidad es un concepto social que se relaciona con cómo se sienten las personas acerca de la divulgación de su información personal a los demás. Diferentes países y culturas tienen ideas diferentes sobre qué información debe y no debe ser privada.
- En muchos países se han establecido leyes de protección de datos para proteger la privacidad individual. Requieren que las empresas que gestionan los datos de los usuarios los almacenen de forma segura, para asegurarse de que no se utilizan o venden sin el permiso de los usuarios, y para permitir a los usuarios ver y corregir los datos personales en poder del sistema.

70

Copyright