Capítulo 3 - Arquitectura e ingeniería de seguridad

Table of Contents

Este capítulo cubre los siguientes tópicos:

- **Procesos de ingeniería que utilizan principios de diseño seguro : los** conceptos discutidos incluyen los estándares de ingeniería de sistemas ISO / IEC 15288: 2015 y NIST SP 800-160, objetos y temas, y sistemas cerrados versus abiertos.
- **Conceptos del modelo de seguridad : los** conceptos discutidos incluyen confidencialidad, integridad y disponibilidad, modos de seguridad, defensa en profundidad, tipos de modelos de seguridad, modelos de seguridad, pasos de la arquitectura del sistema, ISO / IEC 42010: 2011, plataformas informáticas, servicios de seguridad y componentes del sistema.
- **Modelos de evaluación de seguridad del sistema : los** conceptos discutidos incluyen TCSEC, ITSEC, Common Criteria, estándares de implementación de seguridad y controles y contramedidas.
- **Certificación y acreditación : los** conceptos discutidos incluyen certificación, acreditación y las fases de acreditación.
- **Selección de control** basada en los requisitos de seguridad de los sistemas **:** cubre la selección de controles para los sistemas según los requisitos de seguridad.
- **Capacidades de seguridad de los sistemas de información : los** conceptos discutidos incluyen protección de memoria, virtualización, módulo de plataforma confiable, interfaces, tolerancia a fallas, mecanismos de políticas y cifrado / descifrado.
- **Mantenimiento de la arquitectura de seguridad :** analiza el mantenimiento de la arquitectura de seguridad.
- **Vulnerabilidades de arquitecturas de seguridad, diseños y elementos de solución : los** conceptos discutidos incluyen sistemas basados en clientes, sistemas basados en servidores, sistemas de bases de datos, sistemas criptográficos, sistemas de control industrial, sistemas basados en la nube, sistemas de datos paralelos a gran escala, sistemas distribuidos y Internet de las Cosas.
- **Vulnerabilidades en sistemas basados en web : los** conceptos discutidos incluyen ganchos de mantenimiento, ataques de tiempo de verificación / tiempo de uso, ataques basados en web, XML, SAML y OWASP.
- **Vulnerabilidades en sistemas móviles :** cubre las vulnerabilidades encontradas al usar sistemas móviles, incluida la seguridad de los dispositivos, la seguridad de las aplicaciones y las preocupaciones sobre los dispositivos móviles.
- **Vulnerabilidades en dispositivos integrados :** explica los problemas que se están observando actualmente con la llegada de la comunicación de máquina a máquina y la Internet de las cosas.
- **Criptografía aplicada : los** temas tratados incluyen conceptos criptográficos, historia de la criptografía, características del criptosistema, matemáticas criptográficas y ciclo de vida criptográfico.
- **Tipos criptográficos : los** conceptos discutidos incluyen cifrados de ocultación y clave en ejecución, cifrados de sustitución, cifrados de transposición, algoritmos simétricos, algoritmos asimétricos y cifrados híbridos.
- **Algoritmos simétricos : Los** algoritmos discutidos incluyen Estándar de cifrado digital y Estándar de cifrado de datos triple, Estándar de cifrado avanzado, IDEA, Skipjack, Blowfish, Twofish, RC4 / RC5 / RC6 / RC7 y CAST.

- **Algoritmos asimétricos : los** algoritmos discutidos incluyen Diffie-Hellman, RSA, El Gamal, ECC, Knapsack y prueba de conocimiento cero.
- **Infraestructura de clave pública : los** conceptos discutidos incluyen CA y RA, certificados, ciclo de vida del certificado, CRL, OCSP, pasos de PKI y certificación cruzada.
- **Prácticas de administración de claves :** explica las prácticas de administración de claves que las organizaciones deben comprender, incluida la administración de claves simétricas y la administración de claves asimétricas.
- **Integridad del mensaje : los** conceptos discutidos incluyen hash, hash unidireccional, código de autenticación de mensajes y salazón.
- **Firmas digitales :** cubre el uso de firmas digitales, incluido DSS.
- **Criptografía aplicada :** cubre el cifrado de enlaces, el cifrado de un extremo a otro, la seguridad del correo electrónico y la seguridad de Internet.
- **Ataques criptoanalíticos : los** ataques discutidos incluyen ataque de solo texto cifrado, ataque de texto plano conocido, ataque de texto plano elegido, ataque de texto cifrado elegido, ingeniería social, fuerza bruta, criptoanálisis diferencial, criptoanálisis lineal, ataque algebraico, análisis de frecuencia, ataque de cumpleaños, ataque de diccionario, ataque de reproducción, ataque analítico, ataque estadístico, ataque de factorización, ingeniería inversa, ataque de encuentro en el medio, ataque de ransomware y ataque de canal lateral.
- **Gestión de** derechos digitales **:** explica la gestión de derechos digitales, incluidos documentos, música, películas, videojuegos y DRM de libros electrónicos.
- **Diseño de instalaciones y sitios : los** conceptos discutidos incluyen un modelo de defensa en capas, CPTED, plan de seguridad física y cuestiones de selección de instalaciones.
- **Controles de seguridad del sitio y de las instalaciones : Los** controles discutidos incluyen puertas, cerraduras, datos biométricos, entradas de vidrio, control de visitantes, armarios de cableado / instalaciones de distribución intermedia, áreas de trabajo, seguridad ambiental y seguridad del equipo.

El dominio de Arquitectura e Ingeniería de Seguridad aborda una amplia gama de temas que incluyen procesos de ingeniería de seguridad, modelos de seguridad, controles de seguridad, evaluación y mitigación de vulnerabilidades, criptografía y controles de seguridad de instalaciones y sitios. Del 100% del examen, este dominio tiene un peso promedio del 13%, que se relaciona con otros dos dominios para el tercer peso más alto.

La arquitectura y la ingeniería de seguridad se ocupan principalmente del diseño, implementación, monitoreo y protección de los activos de seguridad de la información. Estos activos incluyen computadoras, equipos, redes y aplicaciones. Dentro de esta área, un profesional de la seguridad debe comprender los modelos de seguridad, las vulnerabilidades del sistema, la criptografía y la seguridad física. Pero simplemente comprender la arquitectura y la ingeniería de seguridad no es suficiente. Un profesional de la seguridad también debe saber cómo implementar la ingeniería de la arquitectura de seguridad para garantizar que los activos estén protegidos. Las organizaciones deben comprender qué necesitan proteger, por qué necesitan protegerlo y cómo se protegerá.

Temas fundamentales

Procesos de ingeniería que utilizan principios de diseño seguro

La ingeniería de sistemas es un enfoque para el diseño, la realización, la gestión técnica, las operaciones y el retiro de un sistema. En general, un sistema es una colección de elementos que juntos producen resultados que los elementos no pueden obtener por sí solos. Específicamente en TI, un sistema puede involucrar una o varias computadoras o dispositivos que trabajen juntos para lograr un resultado particular. Por ejemplo, un sistema de pedidos en línea puede incluir un servidor web, un servidor de comercio electrónico y un servidor de base de datos. Sin embargo, estos sistemas por sí solos no pueden proporcionar la seguridad adecuada a las transacciones en línea. Una organización puede necesitar incluir enrutadores, firewalls y otros mecanismos de seguridad para garantizar que la seguridad esté integrada en las soluciones de diseño totales.

Las organizaciones deben implementar y administrar procesos de ingeniería de sistemas utilizando principios de diseño seguro. La ingeniería de sistemas generalmente se modela en base a un ciclo de vida. El Capítulo 1 , " Seguridad y gestión de riesgos ", analiza los grupos que establecennormas, incluida la Organización Internacional de Normalización (ISO) / Comisión Electrotécnica Internacional (IEC) y el Instituto Nacional de Normas y Tecnología (NIST). Ambos grupos han establecido estándares para la ingeniería de sistemas: ISO / IEC 15288: 2015 y NIST Special Publication (SP) 800-160, que reemplaza NIST SP 800-27.

ISO / IEC 15288: 2015 establece cuatro categorías de procesos:

- **Procesos de convenios:** esta categoría incluye adquisición y suministro.
- **Procesos organizativos de habilitación de proyectos:** esta categoría incluye la gestión del modelo de ciclo de vida, la gestión de la infraestructura, la gestión de la cartera, la gestión de los recursos humanos, la gestión de la calidad y la gestión del conocimiento.
- **Procesos de gestión técnica:** esta categoría incluye la planificación de proyectos, la evaluación y el control de proyectos, la gestión de decisiones, la gestión de riesgos, la gestión de la configuración, la gestión de la información, la medición y el aseguramiento de la calidad.
- **Procesos técnicos:** esta categoría incluye análisis de negocios o misión, definición de necesidades y requisitos de las partes interesadas, definición de requisitos del sistema, definición de arquitectura, definición de diseño, análisis del sistema, implementación, integración, verificación, transición, validación, operación, mantenimiento y eliminación.

Las etapas del ciclo de vida de los sistemas de este estándar incluyen concepto, desarrollo, producción, utilización, soporte y retiro. Si bien este estándar define los procesos del ciclo de vida del sistema, no aborda por sí mismo la seguridad durante la ingeniería de sistemas.

NIST SP 800-160 se basa en ISO / IEC 15288: 2015 y se analiza en el Capítulo 1 .

Para comprender la ingeniería utilizando principios de diseño seguro, las organizaciones deben comprender la diferencia entre objetos y sujetos y sistemas cerrados y abiertos.

Objetos y sujetos

Para comprender los principios del diseño seguro, los profesionales de la seguridad deben comprender la diferencia entre objetos y sujetos. Los objetos son recursos a los que un usuario o proceso desea acceder, mientras que los sujetos son los usuarios o procesos que solicitan acceso. Muchos recursos pueden ser tanto objetos como sujetos. Si el recurso solicita acceso, es un asunto. Si se accede a un recurso, es un objeto.

Veamos un ejemplo. Supongamos que Jim, un usuario, desea acceder a una aplicación. En este caso, Jim es un sujeto y la aplicación es un objeto. Supongamos entonces que una vez que Jimrecibe acceso a la aplicación, la aplicación necesita acceder a la información de una base de datos. Entonces, la aplicación se convierte en el sujeto y la base de datos se convierte en el objeto.

Sistemas cerrados versus abiertos

Otro principio de diseño seguro que los profesionales de la seguridad deben comprender es el de sistemas cerrados frente a abiertos. Un sistema cerrado es un sistema patentado que está diseñado para funcionar con una gama limitada de otros sistemas. Los sistemas abiertos cumplen con los estándares de la industria y pueden funcionar con sistemas que admiten el mismo estándar. Al integrar estos sistemas, los sistemas cerrados son más difíciles de integrar, mientras que los sistemas abiertos son mucho más fáciles de integrar.

Nota

No confunda sistema cerrado versus abierto con fuente cerrada versus abierta. Una solución de código abierto utiliza código fuente que es conocido por el público. Una solución de código cerrado utiliza código que solo el fabricante conoce. Tanto las soluciones de código abierto como las de código cerrado pueden ser sistemas abiertos o cerrados.

Conceptos del modelo de seguridad

Las medidas de seguridad deben tener un objetivo definido para asegurar que la medida sea exitosa. Todas las medidas están diseñadas para proporcionar una de las principales protecciones. En esta sección, se analizan los tres principios fundamentales de seguridad. Además, se cubre un enfoque para lograr estos objetivos. Además, esta sección cubre los modos de seguridad, defensa en profundidad, tipos de modelos de seguridad, modelos de seguridad y arquitectura del sistema. Finalmente, cubre ISO / IEC 42010: 2011, plataformas informáticas, servicios de seguridad y componentes del sistema.

Confidencialidad, integridad y disponibilidad

Los principios de seguridad esenciales de confidencialidad, integridad y disponibilidad se conocen como la tríada de la CIA. Se proporciona confidencialidad si los datos no se pueden leer mediante controles de acceso y cifrado de los datos tal como se encuentran en un disco duro o mediante cifrado cuando los datos están en tránsito. Con respecto a la seguridad de la información, la confidencialidad es lo opuesto a la divulgación.

Se proporciona integridad si puede estar seguro de que los datos no han cambiado de ninguna manera. Por lo general, se proporciona con un algoritmo hash o una suma de comprobación de algún tipo. Ambos métodos crean un número que se envía junto con los datos. Cuando los datos llegan al destino, este número se puede usar para determinar si incluso un solo bit ha cambiado en los datos calculando el valor hash a partir de los datos que se recibieron. Esto ayuda a proteger los datos contra daños no detectados.

Algunas metas de integridad adicionales son

- Evite que usuarios no autorizados realicen modificaciones
- Mantener la consistencia interna y externa
- Evitar que los usuarios autorizados realicen modificaciones indebidas

La disponibilidad describe el porcentaje de tiempo que el recurso o los datos están disponibles. Por lo general, esto se mide como un porcentaje de tiempo de actividad, y el 99,9% de tiempo de actividad representa más disponibilidad que el 99% de tiempo de actividad. Asegurarse de que los datos sean accesibles cuando y donde se necesiten es un objetivo primordial de la seguridad.

Confinamiento

El confinamiento es un término que se utiliza para describir los procesos de un sistema. Cuando un proceso está confinado, al proceso solo se le permite leer y escribir en ciertas ubicaciones de memoria y recursos. El confinamiento se realiza habitualmente mediante el sistema operativo, a través de un servicio de confinamiento o mediante un hipervisor.

Límites

En un sistema, los procesos se ejecutan a un nivel de autoridad asignado, que define lo que puede hacer el proceso. Dos niveles de autoridad comunes son el usuario y el kernel. Los límites de un proceso establecen límites en las direcciones de memoria y los recursos a los que puede acceder el proceso. Los límites segmentan lógicamente las áreas de memoria para que las utilice cada proceso. Los sistemas altamente seguros vincularán físicamente los procesos, lo que significa que los procesos se ejecutan en áreas de memoria que están físicamente separadas entre sí. La memoria delimitada lógicamente es más barata pero no tan segura como la memoria delimitada físicamente.

Aislamiento

Un proceso se ejecuta de forma aislada cuando está confinado mediante límites. El aislamiento del proceso garantiza que cualquier acción realizada por el proceso solo afectará la memoria y

los recursos utilizados por el proceso aislado. El aislamiento evita que otros procesos, aplicaciones o recursos accedan a la memoria o los recursos de otro.

Modos de seguridad

Un sistema de control de acceso obligatorio (MAC) opera en diferentes modos de seguridad en varios momentos, en función de variables como la sensibilidad de los datos, el nivel de autorización del usuario y las acciones que los usuarios están autorizados a realizar. Esta sección proporciona descripciones de estos modos.

Modo de seguridad dedicado

Un sistema está funcionando en modo de seguridad dedicado si emplea un solo nivel de clasificación. En este sistema, todos los usuarios pueden acceder a todos los datos, pero deben firmar un acuerdo de no divulgación (NDA, por sus siglas en inglés) y ser aprobados formalmente para el acceso según sea necesario.

Modo de alta seguridad del sistema

En un sistema que funciona en modo de alta seguridad del sistema, todos los usuarios tienen la misma autorización de seguridad (como en el modelo de seguridad dedicado), pero no todos poseen una autorización necesaria para conocer toda la información del sistema. En consecuencia, aunque un usuario puede tener autorización para acceder a un objeto, aún puede estar restringido si no tiene autorización necesaria para conocer el objeto.

Modo de seguridad compartimentado

En el sistema de modo de seguridad compartimentado, todos los usuarios deben poseer la autorización de seguridad más alta (tanto en seguridad dedicada como en el sistema de alta seguridad), pero también deben tener una autorización válida de necesidad de saber, un NDA firmado y una aprobación formal para toda la información a a los que tienen acceso. El objetivo es asegurar que el mínimo de personas posible tenga acceso a la información en cada nivel o compartimento.

Modo de seguridad multinivel

Cuando un sistema permite que se procesen dos o más niveles de clasificación de información al mismo tiempo, se dice que está operando en modo de seguridad multinivel. Los usuarios deben tener un NDA firmado para toda la información en el sistema y tendrán acceso a subconjuntos según su nivel de autorización, necesidad de conocer y aprobación de acceso formal. Estos sistemas implican el mayor riesgo porque la información se procesa en más de un nivel de seguridad, incluso cuando todos los usuarios del sistema no tienen las autorizaciones adecuadas o la necesidad de conocer toda la información procesada por el sistema. Esto también se denomina a veces modo de seguridad controlado. La Tabla 3-1 compara los cuatro modos de seguridad y sus requisitos.

Tabla 3-1 Resumen de modos de seguridad

	NDA firmado	Liquidación adecuada	Aprobación formal	Necesidad válida de saber
Dedicado	Toda la informacion	Toda la informacion	Toda la informacion	Toda la informacion
Sistema alto	Toda la informacion	Toda la informacion	Toda la informacion	Alguna información
Compartimentado	Toda la informacion	Toda la informacion	Alguna información	Alguna información
Multi nivel	Toda la informacion	Alguna información	Alguna información	Alguna información

Seguridad y confianza

Mientras que un nivel de confianza describe las protecciones que se pueden esperar de un sistema, la garantía se refiere al nivel de confianza de que las protecciones funcionarán según lo planeado. Por lo general, se logran niveles más altos de garantía al dedicar más escrutinio a la seguridad en el proceso de diseño. La sección “ Modelos de evaluación de la seguridad del sistema ” , más adelante en este capítulo, analiza varios métodos de clasificación de los sistemas para niveles de confianza y garantía.

Defensa en profundidad

La gestión y las técnicas de seguridad de las comunicaciones están diseñadas para prevenir, detectar y corregir errores de modo que se pueda mantener la CIA de las transacciones a través de las redes. La mayoría de los ataques informáticos resultan en una violación de una de las propiedades de seguridad: confidencialidad, integridad o disponibilidad. Un enfoque de defensa en profundidad se refiere a la implementación de capas de protección. Por ejemplo, incluso al implementar firewalls, las listas de control de acceso (ACL) deben aplicarse a los recursos para ayudar a prevenir el acceso a datos confidenciales en caso de que se infrinja el firewall.

Tipos de modelos de seguridad

Un modelo de seguridad describe la teoría de la seguridad que está diseñada en un sistema desde el principio. Se han desarrollado modelos formales para abordar el diseño de las operaciones de seguridad de un sistema. En el mundo real, el uso de modelos formales a menudo se omite porque retrasa un poco el proceso de diseño (aunque el costo podría ser un sistema menor). En esta sección se analizan algunos tipos de modelos básicos junto con algunos modelos formales derivados de los diversos enfoques disponibles.

Un modelo de seguridad mapea los deseos de los responsables de las políticas de seguridad con las reglas que debe seguir un sistema informático. Los diferentes tipos de modelos exhiben varios enfoques para lograr este objetivo. Los modelos específicos que se incluyen en la sección " Modelos de seguridad " incorporan varias combinaciones de estos tipos de modelos.

Modelos de máquina de estado

El estado de un sistema es su postura en cualquier momento específico. Las actividades que ocurren en el proceso de funcionamiento del sistema alteran el estado del sistema. Al examinar todos los estados posibles en los que podría estar el sistema y garantizar que el sistema mantenga la relación de seguridad adecuada entre los objetos y los sujetos en cada estado, se dice que el sistema es seguro. El modelo Bell-LaPadula que se analiza en la sección posterior " Modelos de seguridad " es un ejemplo de un modelo de máquina de estados.

Modelos de celosía multinivel

El modelo de control de acceso basado en celosía se desarrolló principalmente para abordar cuestiones de confidencialidad y se centra principalmente en el flujo de información. A cada sujeto de seguridad se le asigna una etiqueta de seguridad que define los límites superior e inferior del acceso del sujeto al sistema. Luego, los controles se aplican a todos los objetos organizándolos en niveles o celosías. Los objetos son contenedores de información en algún formato. A estos pares de elementos (objeto y sujeto) se les asigna un límite superior mínimo de valores y un límite inferior máximo de valores que definen lo que puede hacer ese sujeto con ese objeto.

La etiqueta de un sujeto (recuerde que un sujeto puede ser una persona pero también puede ser un proceso) define a qué nivel se puede acceder y qué acciones se pueden realizar en ese nivel. Con el modelo de control de acceso basado en celosía, una etiqueta de seguridad también se denomina clase de seguridad. Este modelo asocia cada recurso y cada usuario de un recurso con uno de un conjunto ordenado de clases. El modelo basado en celosía tiene como objetivo proteger contra el flujo de información ilegal entre las entidades.

Modelos basados en matrices

Un modelo basado en matrices organiza tablas de sujetos y objetos que indican qué acciones pueden realizar sujetos individuales sobre objetos individuales. Este concepto se encuentra en otros tipos de modelos, así como en el modelo de celosía discutido en la sección anterior. El control de acceso a los objetos se implementa a menudo como una matriz de control. Es un enfoque sencillo que define los derechos de acceso a los sujetos para los objetos. Las dos implementaciones más comunes de este concepto son las ACL y las capacidades. En su estructura de tabla, una fila indicaría el acceso que tiene un sujeto a una matriz de objetos. Por lo tanto, una fila podría verse como una lista de capacidades para un tema específico. Consta de las siguientes partes:

- Una lista de objetos
- Una lista de temas

- Una función que devuelve el tipo de un objeto.
- La matriz en sí, con los objetos formando las columnas y los sujetos formando las filas.

Modelos sin interferencia

En los modelos de seguridad multinivel, el concepto de no interferencia prescribe aquellas acciones que tienen lugar en un nivel de seguridad superior pero que no afectan ni influyen en las que se producen en un nivel de seguridad inferior. Debido a que este modelo se preocupa menos por laflujo de información y más preocupado por el conocimiento de un sujeto sobre el estado del sistema en un momento determinado, se concentra en evitar que las acciones que tienen lugar en un nivel alteren el estado presentado a otro nivel.

Uno de los tipos de ataques que este modelo conceptual pretende prevenir es la interferencia. Esto ocurre cuando alguien tiene acceso a información en un nivel que le permite inferir información sobre otro nivel.

Modelos de flujo de información

Cualquiera de los modelos discutidos en la siguiente sección que intenta prevenir el flujo de información de una entidad a otra que viola o niega la política de seguridad se denomina modelo de flujo de información. En el modelo de flujo de información, lo que relaciona dos versiones del mismo objeto se llama flujo. Un flujo es un tipo de dependencia que relaciona dos versiones del mismo objeto y, por lo tanto, la transformación de un estado de ese objeto en otro, en puntos sucesivos en el tiempo. En un sistema de seguridad multinivel (MLS), un dispositivo de flujo de información unidireccional llamado bomba evita el flujo de información desde un nivel inferior de clasificación de seguridad o sensibilidad a un nivel superior.

Por ejemplo, el modelo Bell-LaPadula (discutido en la sección “ Modelos de seguridad ”) se ocupa del flujo de información en los siguientes tres casos:

- Cuando un sujeto altera un objeto
- Cuando un sujeto accede a un objeto
- Cuando un sujeto observa un objeto

La prevención del flujo de información ilegal entre las entidades es el objetivo de un modelo de flujo de información.

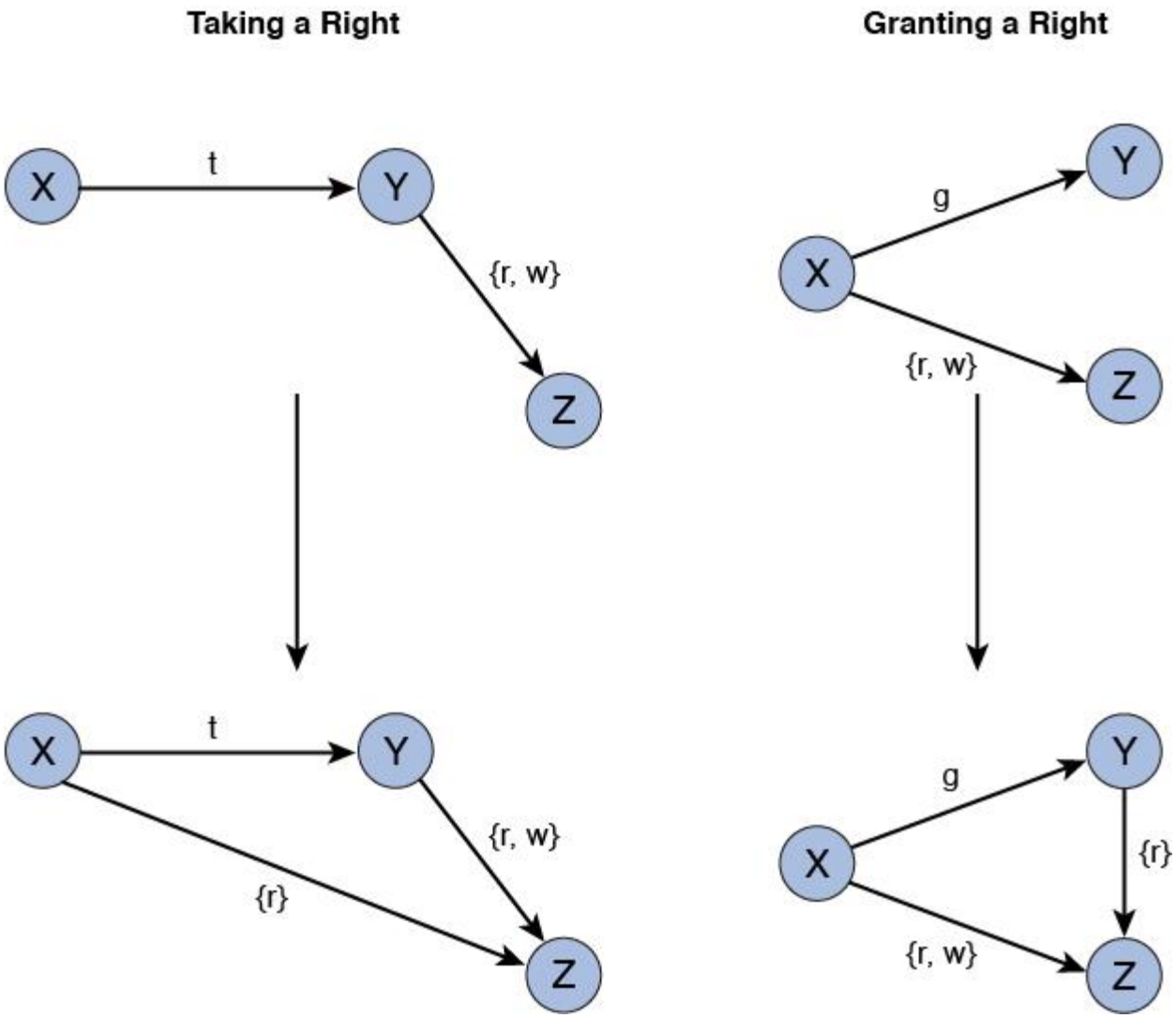
Modelo de concesión de subvenciones

Un sistema en el modelo Take-Grant se representa como un gráfico dirigido, llamado gráfico de protección. Los sujetos y objetos del sistema informático son los vértices y los derechos de acceso de los sujetos a los objetos están representados por arcos. Mientras que el modelo Take-Grant utiliza derechos de acceso estándar como lectura y escritura, el modelo Take-Grant incluye dos derechos de acceso adicionales:

- Take (t) es el derecho a tomar cualquier derecho de acceso del sujeto.

- Grant (g) es el derecho a ceder sus derechos de acceso a cualquier sujeto.

La Figura 3-1 muestra un gráfico de los derechos de acceso Take y Grant del modelo Take-Grant.



La figura de la izquierda representa "Tomando a la derecha". Una flecha hacia la derecha con la etiqueta t apunta de una X encerrada en un círculo a una Y en un círculo y una flecha hacia abajo desde la Y en un círculo fluye a una Z en un círculo. Esto se etiqueta como "{r, w}". En el siguiente paso, se accede conectando la X encerrada en un círculo con la Y encerrada en un círculo mediante la flecha hacia abajo etiquetada "{r}". La figura de la derecha representa "Concesión de un derecho". Una X en un círculo en el centro apunta a una Y (g) en un círculo y una Z en un círculo, "{r, w}" en la parte inferior. En el siguiente paso, se concede conectando la Y encerrada en un círculo con la Z encerrada en un círculo mediante una flecha hacia abajo. Esto está etiquetado como {r}.

Figura 3-1 Ejemplo de Take-Grant del modelo Take-Grant

Modelos de seguridad

Se han desarrollado y utilizado varios modelos formales que incorporan los conceptos discutidos en la sección anterior para guiar el diseño de seguridad de los sistemas. En esta sección se analizan algunos de los modelos de seguridad más importantes o más utilizados, incluidos los siguientes:

- Modelo Bell-LaPadula
- Modelo Biba
- Modelo de integridad de Clark-Wilson
- Modelo Lipner
- Modelo Brewer-Nash (muro chino)
- Modelo de Graham-Denning
- Modelo de Harrison-Ruzzo-Ullman
- Modelo Goguen-Meseguer
- Modelo Sutherland

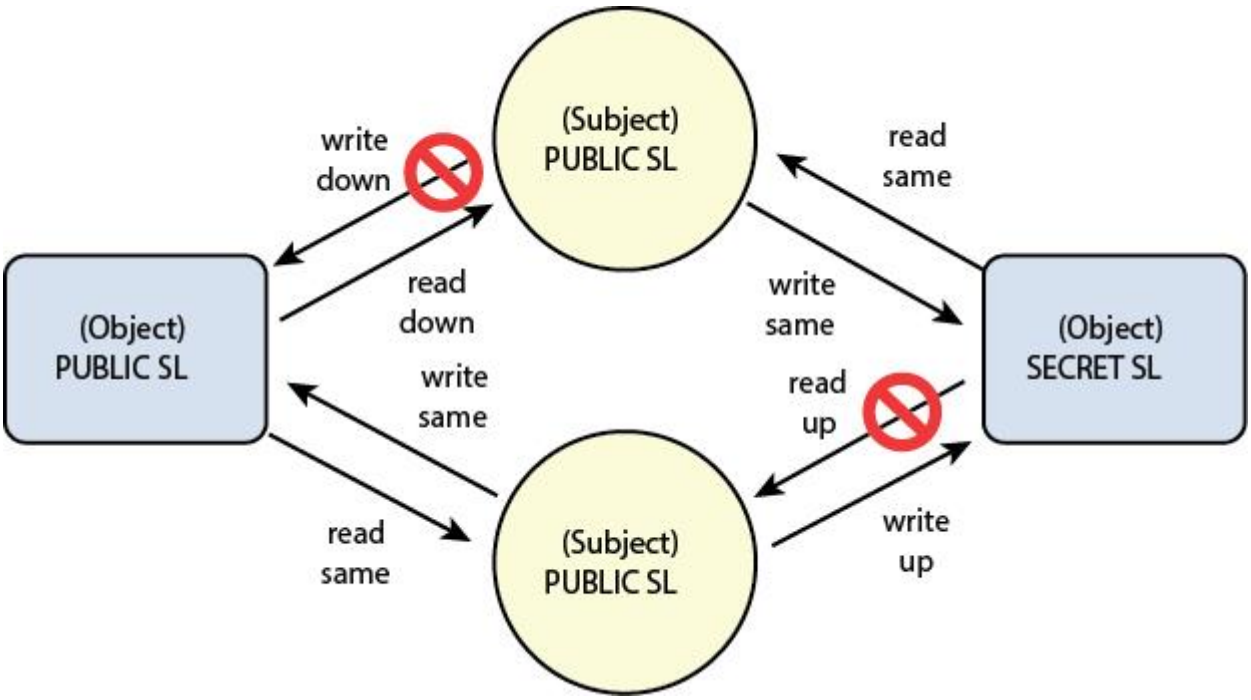
Modelo Bell-LaPadula

El modelo Bell-LaPadula fue el primer modelo matemático de un sistema multinivel que utilizó tanto los conceptos de máquina de estados como los de control del flujo de información. Formaliza la política de seguridad multinivel del Departamento de Defensa de EE. UU. Es un modelo de máquina de estado que captura los aspectos de confidencialidad del control de acceso. Cualquier movimiento de información de un nivel superior a un nivel inferior en el sistema debe ser realizado por un sujeto de confianza.

Bell-LaPadula incorpora tres reglas básicas con respecto al flujo de información en un sistema:

- **La regla de seguridad simple:** un sujeto no puede leer datos ubicados en un nivel de seguridad más alto que el que posee el sujeto (también llamado no lectura).
- **La estrella (*) - regla de propiedad:** Un sujeto no puede escribir a un nivel más bajo que el que posee el sujeto (también llamado no escribir o la regla de confinamiento).
- **La regla de la propiedad de la estrella fuerte:** un sujeto puede realizar funciones de lectura y escritura solo en el mismo nivel que posee el sujeto.

La regla * -property se muestra en la Figura 3-2 .



Subject Public SL y Object Secret SL permiten leer y escribir lo mismo entre sí. Subject Public SL no permite la lectura de Object Secret SL, pero esta última acepta la redacción de la primera. De manera similar, Subject Public SL y Object Public SL permiten entre sí leer lo mismo y escribir lo mismo. Sin embargo, Object Public SL no permite la anotación de Subject Public SL, pero esta última acepta la lectura de la primera.

Figura 3-2 La regla * -Property

La principal preocupación del modelo de seguridad de Bell-LaPadula y su uso de estas reglas es la confidencialidad. Aunque su modelo básico es un sistema MAC, otra regla de propiedad llamada propiedad de seguridad discrecional (ds-property) hace posible una combinación de controles obligatorios y discrecionales. Esta propiedad permite a un sujeto transferir permisos a su propia discreción. En la parte discrecional del modelo, los permisos de acceso se definen a través de una matriz de control de acceso utilizando un proceso llamadoLas políticas de autorización y seguridad evitan que la información fluya hacia abajo desde un nivel de seguridad alto a un nivel de seguridad bajo.

El modelo de seguridad de Bell-LaPadula tiene limitaciones. Entre ellos se encuentran

- No contiene ninguna disposición o política para cambiar el control de acceso a los datos. Por lo tanto, funciona bien solo con sistemas de acceso que son de naturaleza estática.
- No se dirige a los llamados canales encubiertos. Un sujeto de bajo nivel a veces puede detectar la existencia de un objeto de alto nivel cuando se le niega el acceso. A veces no basta con ocultar el contenido de un objeto; también podría ser necesario ocultar su existencia.
- Su principal aportación a expensas de otros conceptos es la confidencialidad.

Este modelo de política de seguridad fue la base del Libro Naranja, que se analiza en la sección posterior " TCSEC ".

Modelo Biba

El modelo Biba vino después del modelo Bell-LaPadula y comparte muchas características con ese modelo. Estos dos modelos son los más conocidos de los que se analizan en esta sección. También es un modelo de máquina de estado que utiliza una serie de celosías o niveles de seguridad, pero el modelo Biba se preocupa más por la integridad de la información que por la confidencialidad de esa información. Para ello, se basa en un sistema de clasificación de datos para evitar la modificación no autorizada de los datos. A los sujetos se les asignan clases de acuerdo con su confiabilidad; A los objetos se les asignan etiquetas de integridad de acuerdo con el daño que se produciría si los datos se modificaran incorrectamente.

Al igual que el modelo Bell-LaPadula, el modelo Biba aplica una serie de propiedades o axiomas para orientar la protección de la integridad. Su efecto es que los datos no deben fluir de un receptáculo de integridad dada a un receptáculo de integridad superior:

- **Axioma de integridad:** un sujeto no puede escribir con un nivel de integridad superior al que tiene acceso (no escribir).
- **Axioma de integridad simple:** un sujeto no puede leer a un nivel de integridad más bajo que aquel al que tiene acceso (no leer).
- **Propiedad de invocación:** un sujeto no puede invocar (solicitar servicio) de mayor integridad.

Modelo de integridad de Clark-Wilson

Desarrollado a partir del modelo Biba, este modelo también se ocupa de la integridad de los datos. El modelo describe una serie de elementos que se utilizan para controlar la integridad de los datos que se enumeran aquí:

- **Usuario:** un agente de **usuarios** activos
- **Procedimiento de transformación (TP):** una operación abstracta, como leer, escribir y modificar, implementada a través de la programación.
- **Elemento de datos restringidos (CDI):** un elemento que solo se puede manipular a través de un TP
- **Elemento de datos sin restricciones (UDI):** un elemento que puede ser manipulado por un usuario mediante operaciones de lectura y escritura.

- **Procedimiento de verificación de integridad (IVP):** una verificación de la coherencia de los datos con el mundo real

Este modelo refuerza estos elementos permitiendo solo que los datos sean alterados a través de programas y no directamente por los usuarios. En lugar de emplear una estructura de celosía, utiliza una relación de tres partes de sujeto / programa / objeto conocida como triple. También establece como objetivo los conceptos de separación de funciones y transacciones bien formadas:

- **Separación de funciones :** este concepto garantiza que determinadas operaciones requieran una verificación adicional.
- **Transacción bien formada:** este concepto garantiza que todos los valores se verifiquen antes y después de la transacción mediante la realización de operaciones particulares para completar el cambio de datos de un estado a otro.

Para garantizar que se logre y se preserve la integridad, el modelo de Clark-Wilson afirma que se necesitan reglas de monitoreo y preservación de la integridad. Las reglas de supervisión de la integridad se denominan reglas de certificación y las reglas de conservación de la integridad se denominan reglas de cumplimiento.

Modelo Lipner

El modelo Lipner es una implementación que combina elementos del modelo Bell-LaPadula y el modelo Biba. La primera forma de implementar la integridad con el modelo de Lipner utiliza Bell-LaPadula y asigna sujetos a uno de dos niveles de sensibilidad (administrador del sistema y cualquier otra persona) ya una de las cuatro categorías de trabajo. A los objetos se les asignan niveles y categorías específicos. Las categorías se convierten en el mecanismo de integridad (como el control de acceso) más importante. La segunda implementación utiliza tanto Bell-LaPadula como Biba. Este método evita que los usuarios no autorizados modifiquen los datos y evita que los usuarios autorizados realicen modificaciones incorrectas en los datos. Las implementaciones también comparten características con el modelo de Clark-Wilson en el sentido de que separa objetos en datos y programas.

Modelo Brewer-Nash (muro chino)

El modelo Brewer-Nash (muro chino) introdujo el concepto de permitir que los controles de acceso cambien dinámicamente en función de las acciones anteriores de un usuario. Uno de sus objetivos es hacer esto al mismo tiempo que se protege contra los conflictos de intereses. Este modelo también se basa en un modelo de flujo de información. La implementación implica agrupar conjuntos de datos en clases discretas, cada clase representa un conflicto de intereses diferente. Aislar conjuntos de datos dentro de una clase brinda la capacidad de mantener los datos de un departamento separados de otro en una base de datos integrada.

Modelo de Graham-Denning

El modelo de Graham-Denning aborda un problema ignorado por los modelos Bell-LaPadula (con la excepción de la propiedad ds) y Biba. Se trata del delegado y cesión de derechos. Se centra en cuestiones como

- Crear y eliminar objetos y sujetos de forma segura
- Proporcionar o transferir derechos de acceso de forma segura

Modelo de Harrison-Ruzzo-Ullman

Este modelo también se ocupa de los derechos de acceso. Restringe el conjunto de operaciones que se pueden realizar en un objeto a un conjunto finito para garantizar la integridad. Los ingenieros de software lo utilizan para evitar que las operaciones demasiado complejas introduzcan vulnerabilidades imprevistas.

Modelo Goguen-Meseguer

Aunque no es tan conocido como Biba y otros modelos de integridad, el modelo de Goguen-Meseguer es la base del modelo de no interferencia. Con este modelo, la lista de objetos a los que puede acceder un sujeto está predeterminada. Entonces, los sujetos solo pueden realizar estas acciones predeterminadas contra los objetos predeterminados. Los sujetos no pueden interferir con las actividades de los demás.

Modelo Sutherland

El modelo de Sutherland se centra en prevenir interferencias en apoyo de la integridad. Basado en la máquina de estados y los modelos de flujo de información, este modelo define un conjunto de estados del sistema, estados iniciales y transiciones de estado. Usando estos estados seguros predeterminados, el modelo de Sutherland mantiene la integridad y prohíbe la interferencia.

Pasos de la arquitectura del sistema

Varios modelos y marcos discutidos en este capítulo pueden diferir en los pasos exactos hacia el desarrollo de una arquitectura de sistema, pero siguen un patrón básico. Los pasos principales incluyen

1. **Fase de diseño:** en esta fase se recopilan los requisitos del sistema y se mapea la forma en que se cumplirán los requisitos utilizando técnicas de modelado que generalmente representan gráficamente los componentes que satisfacen cada requisito y las interrelaciones de estos componentes. En esta fase, muchos de los marcos y modelos de seguridad que se analizan más adelante en este capítulo se utilizan para ayudar a cumplir los objetivos arquitectónicos.
2. **Fase de desarrollo:** en esta fase, los componentes de hardware y software se asignan a equipos individuales para su desarrollo. En esta fase, el trabajo realizado en la primera fase puede ayudar a garantizar que estos equipos independientes estén trabajando hacia componentes que encajen para satisfacer los requisitos.

3. **Fase de mantenimiento:** en esta fase se evalúa el sistema y la arquitectura de seguridad para garantizar que el sistema funcione correctamente y que se mantenga la seguridad de los sistemas. El sistema y la seguridad deben revisarse y probarse periódicamente.
4. **Fase de retiro:** en esta fase, el sistema se retira del uso en el entorno en vivo. Los profesionales de seguridad deben asegurarse de que la organización siga los procedimientos de eliminación adecuados y asegurarse de que no se puedan obtener datos de los activos eliminados.

ISO / IEC 42010: 2011

ISO / IEC 42010: 2011 utiliza terminología específica cuando se habla de marcos arquitectónicos. La siguiente es una revisión de algunos de los términos más importantes:

- **Arquitectura :** describe la organización del sistema, incluyendo sus componentes y sus interrelaciones, junto con los principios que guían su diseño y evolución.
- **Descripción arquitectónica (AD):** Comprende el conjunto de documentos que transmiten la arquitectura de manera formal.
- **Partes interesadas:** individuos, equipos y departamentos, incluidos los grupos fuera de la organización con intereses o inquietudes a considerar.
- **Vista :** la representación del sistema desde la perspectiva de una parte interesada o un conjunto de partes interesadas
- **Punto de vista:** una plantilla que se utiliza para desarrollar vistas individuales que establecen la audiencia, las técnicas y las suposiciones hechas.

Plataformas informáticas

Una plataforma informática está compuesta por componentes de hardware y software que permiten que el software se ejecute. Esto generalmente incluye los componentes físicos, elsistemas operativos y los lenguajes de programación utilizados. Desde una perspectiva física y lógica, se están utilizando varios marcos o plataformas posibles. Esta sección analiza algunos de los más comunes.

Mainframe / Thin Clients

Cuando se utiliza una plataforma de mainframe / cliente ligero, existe una arquitectura cliente / servidor. El servidor retiene la aplicación y realiza todo el procesamiento. El software del cliente se ejecuta en las máquinas del usuario y simplemente envía solicitudes de operaciones y muestra los resultados. Cuando se utiliza un verdadero cliente ligero, existe muy poco en la máquina del usuario además del software que se conecta al servidor y genera el resultado.

Sistemas distribuidos

La plataforma distribuida también utiliza una arquitectura cliente / servidor, pero la división del trabajo entre la parte del servidor y la parte del cliente de la solución puede no ser tan unilateral como la que encontraría en un escenario de mainframe / cliente ligero. En muchos casos, múltiples ubicaciones o sistemas en la red pueden ser parte de la solución. Además, es más

probable que los datos confidenciales se encuentren en la máquina del usuario y, por lo tanto, los usuarios desempeñan un papel más importante en su protección con las mejores prácticas.

Otra característica de un entorno distribuido son las múltiples ubicaciones de procesamiento que pueden proporcionar alternativas para la computación en caso de que un sitio deje de estar disponible.

Los datos se almacenan en múltiples ubicaciones geográficamente separadas. Los usuarios pueden acceder a los datos almacenados en cualquier ubicación con la distancia de los usuarios de esos recursos transparente para el usuario.

Los sistemas distribuidos pueden introducir debilidades de seguridad en la red que deben tenerse en cuenta. Los siguientes son algunos ejemplos:

- Los sistemas de escritorio pueden contener información confidencial que podría estar en riesgo de quedar expuesta.
- Los usuarios generalmente pueden carecer de conciencia de seguridad.
- Los módems presentan una vulnerabilidad a los ataques de acceso telefónico.
- Es posible que exista una falta de respaldo adecuado.

Middleware

En un entorno distribuido, el middleware es un software que une el software del cliente y del servidor. No es parte del sistema operativo ni del software del servidor. Es el código que se encuentra entre el sistema operativo y las aplicaciones en cada lado de un sistema informático distribuido en una red. Puede ser lo suficientemente genérico para operar entre varios tipos de sistemas cliente / servidor de un tipo particular.

Sistemas embebidos

Un sistema integrado es una pieza de software integrada en una pieza de software más grande que se encarga de realizar alguna función específica en nombre del sistema más grande. La parte integrada de la solución puede abordar comunicaciones de hardware específicas y puede requerir que los controladores se comuniquen entre el sistema más grande y algún hardware específico.

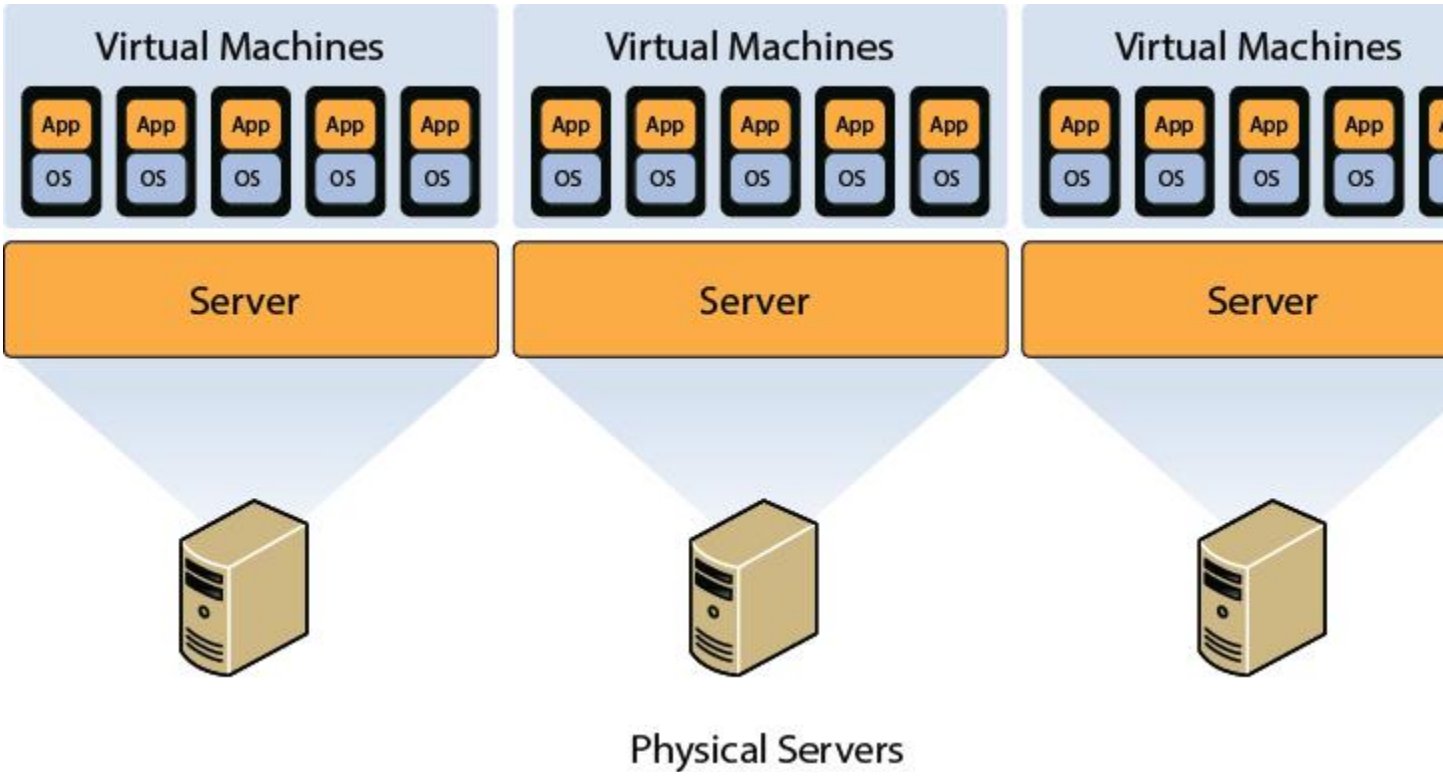
Informática móvil

El código móvil son instrucciones que se pasan a través de la red y se ejecutan en un sistema remoto. Un ejemplo de código móvil es el código Java y ActiveX descargado en un navegador web desde la World Wide Web. Cualquier introducción de código de un sistema a otro es un problema de seguridad, pero es necesario en algunas situaciones. Un módulo de contenido activo que intenta monopolizar y explotar los recursos del sistema se denomina subprograma hostil. El principal objetivo del modelo de seguridad de Java (JSM) es proteger al usuario del código móvil de red hostil. Lo hace colocando el código en una caja de arena, lo que restringe sus operaciones.

Computación virtual

Los entornos virtuales se utilizan cada vez más como plataforma informática para soluciones. La mayoría de los mismos problemas de seguridad que deben mitigarse en el entorno físico también deben abordarse en la red virtual.

En un entorno virtual, las instancias de un sistema operativo se denominan máquinas virtuales (VM). Un sistema host puede contener muchas máquinas virtuales. El software llamado hipervisor gestiona la distribución de recursos (CPU, memoria y disco) a las VM. La Figura 3-3 muestra la relación entre la máquina host, sus recursos físicos, las VM residentes y los recursos virtuales que se les asignan.



Se muestran tres servidores físicos, cada uno de los cuales está asociado con varias máquinas virtuales. En cada bloque de máquinas virtuales, se muestran cinco pares de aplicaciones y sistemas operativos dentro de una pequeña caja rectangular.

Figura 3-3 Virtualización

Servicios de seguridad

El proceso de creación de la arquitectura del sistema también incluye el diseño de la seguridad que se proporcionará. Estos servicios se pueden clasificar en varias categorías según las protecciones para las que están diseñados. Esta sección examina y compara brevemente los tipos de servicios de seguridad.

Servicios de control de límites

Estos servicios son responsables de colocar varios componentes en zonas de seguridad y mantener el control de límites entre ellos. Generalmente, esto se logra indicando los componentes y servicios como confiables o no confiables. Por ejemplo, el espacio de memoria aislado de otros procesos en ejecución en un sistema de multiprocesamiento es parte de un límite de protección.

Servicios de control de acceso

En el Capítulo 5 , “ Administración de identidades y accesos (IAM) ”, aprenderá sobre varios métodos de control de acceso y cómo se pueden implementar. Se debe implementar un método apropiado para controlar el acceso a material sensible y brindar a los usuarios el acceso que necesitan para hacer su trabajo.

Servicios de integridad

Como recordará, la integridad implica que los datos no se han modificado. Cuando los servicios de integridad están presentes, garantizan que se pueda verificar que los datos que se mueven a través del sistema operativo o la aplicación no se hayan dañado o corrompido en la transferencia.

Servicios de criptografía

Si el sistema es capaz de codificar o codificar información en tránsito, se dice que proporciona servicios de criptografía. En algunos casos, este servicio no lo proporciona un sistema de forma nativa y, si se desea, debe proporcionarse de alguna otra manera, pero si la capacidad está presente, es valiosa, especialmente en los casos en que los sistemas están distribuidos y se comunican a través de la red.

Servicios de auditoría y seguimiento

Si el sistema tiene un método de seguimiento de las actividades de los usuarios y de las operaciones de los procesos del sistema, se dice que proporciona servicios de auditoría y seguimiento. Aunque nuestro enfoque aquí está en la seguridad, el valor de este servicio va más allá de la seguridad porque también permite monitorear lo que el sistema en sí mismo está haciendo.

Componentes del sistema

Cuando se habla de la forma en que se proporciona la seguridad en una arquitectura, resulta útil tener un conocimiento básico de los componentes de los equipos informáticos. Esta sección analiza esos componentes y algunas de las funciones que proporcionan.

UPC

La unidad central de procesamiento (CPU) es el hardware del sistema que ejecuta todas las instrucciones del código. Tiene su propio conjunto de instrucciones para su funcionamiento interno, y esas instrucciones definen su arquitectura. El software que se ejecuta en el sistema

debe ser compatible con esta arquitectura, lo que realmente significa que la CPU y el software pueden comunicarse.

Cuando hay más de un procesador presente y disponible, el sistema se vuelve capaz de multiprocesar. Esto permite que la computadora ejecute múltiples instrucciones en paralelo. Se puede hacer con procesadores físicos separados o con un solo procesador con múltiples núcleos. Cada núcleo funciona como una CPU independiente.

Las CPU tienen su propia memoria y la CPU puede acceder a esta memoria más rápido que cualquier otra ubicación de memoria. También suele tener una memoria caché donde se guardan las instrucciones ejecutadas más recientemente en caso de que se necesiten nuevamente. Cuando una CPU obtiene una instrucción de la memoria, el proceso se denomina recuperación.

Una unidad aritmética lógica (ALU) en la CPU realiza la ejecución real de las instrucciones. La unidad de control actúa como administrador del sistema mientras se ejecutan las instrucciones de las aplicaciones y los sistemas operativos. Los registros de la CPU contienen la información del conjunto de instrucciones y los datos que se ejecutarán e incluyen registros generales, registros especiales y un registro de contador de programa.

Las CPU pueden funcionar en modo de usuario o en modo privilegiado, que también se conoce como modo kernel o supervisor. Cuando las aplicaciones se comunican con la CPU, está en modo de usuario. Si una instrucción que se envía a la CPU está marcada para ejecutarse en modo privilegiado, debe ser un proceso de sistema operativo confiable y se le proporciona una funcionalidad que no está disponible en modo de usuario.

La CPU está conectada a un bus de direcciones. Los dispositivos de memoria y de E / S reconocen este bus de direcciones. Estos dispositivos pueden luego comunicarse con la CPU, leer los datos solicitados y enviarlos al bus de datos.

Cuando se desarrollaron por primera vez las microcomputadoras, el tiempo de obtención de instrucciones era mucho más largo que el tiempo de ejecución de las instrucciones debido a la velocidad relativamente lenta de acceso a la memoria. Esta situación llevó al diseño de la CPU CISC (Complex Instruction Set Computer). En esta disposición, el conjunto de instrucciones se redujo (aunque se hizo más complejo) para ayudar a mitigar el acceso relativamente lento a la memoria.

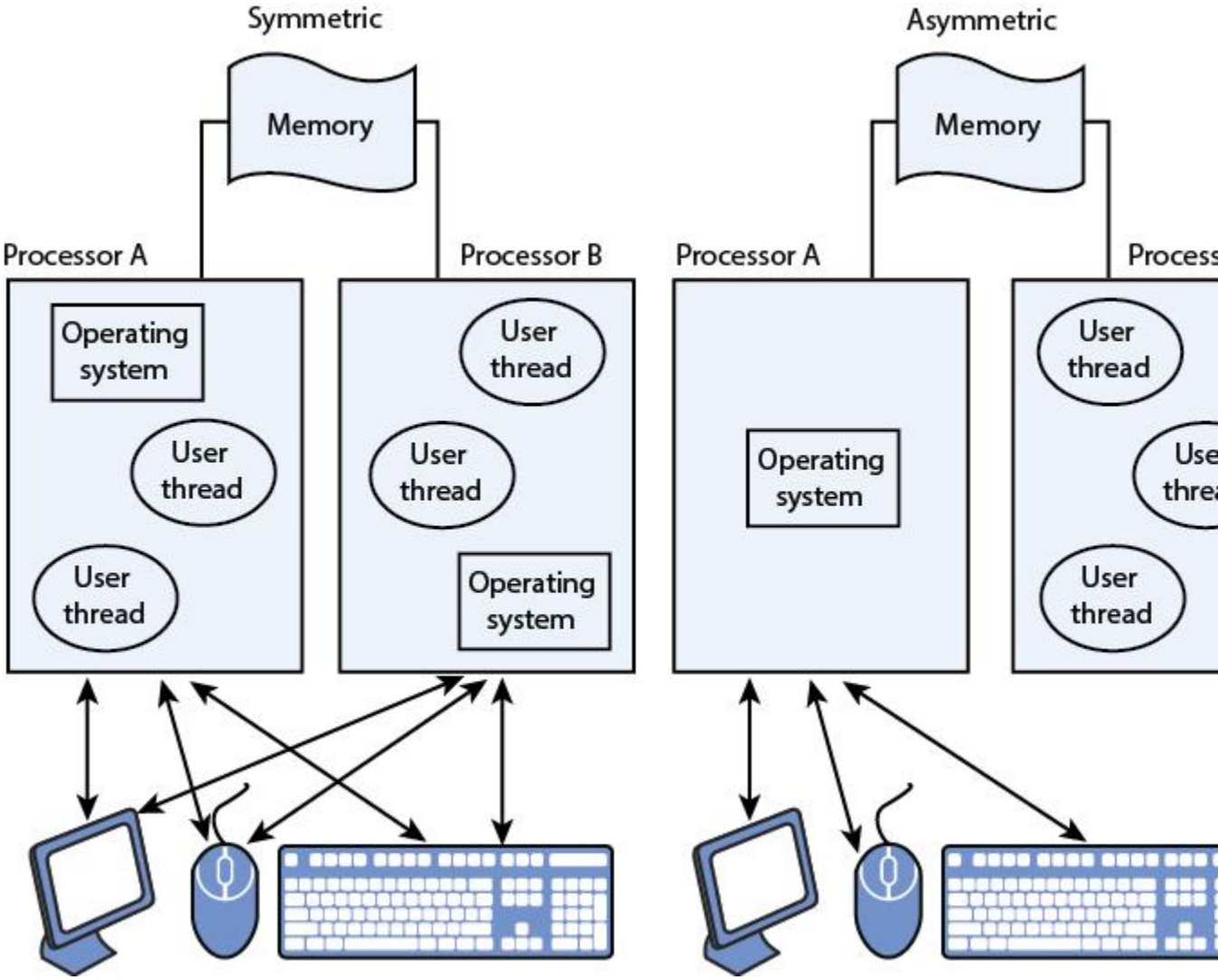
Después de que se mejoró el acceso a la memoria hasta el punto en que no existían muchas diferencias en los tiempos de acceso a la memoria y los tiempos de ejecución del procesador, se introdujo la arquitectura de Computadora con conjunto de instrucciones reducido (RISC). El objetivo de la arquitectura RISC era reducir el número de ciclos necesarios para ejecutar una instrucción, lo que se logró haciendo que las instrucciones fueran menos complejas.

Multitarea y multiprocesamiento

La multitarea es el proceso de realizar más de una tarea a la vez. La multitarea se puede realizar de dos formas diferentes. Cuando la computadora tiene un solo procesador con un núcleo, en

realidad no está realizando múltiples tareas a la vez. Está dividiendo sus ciclos de CPU entre tareas a una velocidad tan alta que parece estar haciendo múltiples tareas a la vez. Sin embargo, cuando una computadora tiene más de un procesador o tiene un procesador con múltiples núcleos, entonces es capaz de realizar dos tareas al mismo tiempo. Puede hacer esto de dos formas diferentes:

- **Modo simétrico :** en este modo, los procesadores o núcleos se entregan trabajo por turnos, hilo por hilo.
- **Modo asimétrico :** en este modo, un procesador está dedicado a un proceso o aplicación específicos; cuando el trabajo debe realizarse para ese proceso, siempre lo realiza el mismo procesador. La figura 3-4 muestra la relación entre estos dos modos.



En la multitarea simétrica, la memoria se pasa a los dos procesadores, Procesador A y Procesador B. El Procesador A (izquierda) y el Procesador B (derecha) constan de un sistema operativo y dos subprocesos de usuario. El procesador A y el procesador B están conectados al hardware externo como el mouse, el teclado y el monitor (representados

por una flecha de dos puntas). En la multitarea asimétrica, la memoria se pasa a los dos procesadores, el procesador A y el procesador B. El procesador A (izquierda) consta de un sistema operativo y el procesador B (derecha) consta de tres subprocesos de usuario. Los procesadores A y B están conectados al hardware externo como el mouse, el teclado y el monitor (representados por una flecha de dos puntas).

Figura 3-4 Tipos de multiprocesamiento

La multitarea preventiva significa que los cambios de tareas se pueden iniciar directamente desde los controladores de interrupciones. Con la multitarea cooperativa (no preventiva), un cambio de tarea solo se realiza cuando una tarea llama al kernel y le permite al kernel la oportunidad de realizar un cambio de tarea.

Subprocesos múltiples

El subproceso múltiple permite realizar múltiples tareas dentro de un solo proceso. Un subproceso es una secuencia de instrucciones autónoma que se puede ejecutar en paralelo con otros subprocesos que forman parte del mismo proceso. El subproceso múltiple se utiliza a menudo en aplicaciones para reducir los gastos generales y aumentar la eficiencia. Un ejemplo de multiproceso es cuando se abren varias hojas de cálculo de Microsoft Excel al mismo tiempo. En esta situación, el equipo no ejecuta varias instancias de Microsoft Excel. Cada hoja de cálculo se trata como un hilo único dentro del proceso único de Microsoft Excel y el software administra a qué hilo se accede.

Sistemas de un solo estado versus sistemas de varios estados

Los sistemas de un solo estado administran la información en diferentes niveles utilizando mecanismos de políticas aprobados por los administradores de seguridad. Estos sistemas manejan un nivel de seguridad a la vez. Los sistemas de varios estados gestionan varios niveles de seguridad al mismo tiempo mediante los mecanismos de protección que se describen en la siguiente sección. Los sistemas de varios estados son poco comunes porque son muy costosos de implementar.

Estados de proceso

Los estados del proceso son los diferentes modos en los que se puede ejecutar un proceso. Un proceso puede operar en uno de varios estados:

- **Listo:** el proceso está listo para comenzar a procesarse cuando sea necesario.
- **En espera:** el proceso está listo para su ejecución, pero está esperando el acceso a un objeto.
- **En ejecución:** el proceso se está ejecutando hasta que finaliza, el tiempo expira o el proceso se bloquea.
- **Supervisor:** el proceso está realizando una acción que requiere mayores privilegios.
- **Detenido:** el proceso ha finalizado o finalizado.

Nota

El estado del supervisor y el estado del problema también son procesos que se describen más adelante en este capítulo en la sección " Protección de la memoria ".

Memoria y almacenamiento

Un sistema informático necesita un lugar para almacenar información, tanto a largo como a corto plazo. Hay dos tipos de ubicaciones de almacenamiento: memoria, para necesidades de almacenamiento temporal y medios de almacenamiento a largo plazo. Se puede acceder a la información mucho más rápido desde la memoria que desde el almacenamiento a largo plazo, por lo que las instrucciones o la información utilizadas más recientemente se guardan normalmente en la memoria caché durante un tiempo.corto período de tiempo, lo que garantiza que el segundo acceso y los siguientes sean más rápidos que volver a la memoria a largo plazo.

Las computadoras pueden tener memoria de acceso aleatorio (RAM) y memoria de solo lectura (ROM). La RAM es volátil, lo que significa que la información debe actualizarse continuamente y se perderá si el sistema se apaga. La Tabla 3-2 contiene algunos tipos de RAM que se utilizan en computadoras portátiles y de escritorio.

Tabla 3-2 Tipos de memoria

Memoria de escritorio	Descripción
SDRAM: memoria dinámica síncrona de acceso aleatorio	Se sincroniza con el bus de la CPU.
DDR SDRAM: memoria de acceso aleatorio dinámica síncrona de doble velocidad de datos	Admite transferencias de datos en ambos bordes de cada ciclo de reloj (los bordes ascendente y descendente), duplicando efectivamente el rendimiento de datos del chip de memoria.
DDR2 SDRAM: doble velocidad de datos, dos (2) memorias dinámicas sincrónicas de acceso aleatorio	Transfiere 64 bits de datos dos veces por ciclo de reloj y no es compatible con las ranuras de memoria DDR SDRAM actuales.
DDR3-SDRAM: doble velocidad de datos, tres (3) memorias dinámicas síncronas de acceso aleatorio	Ofrece un consumo de energía reducido, un búfer de búsqueda previa duplicado y más ancho de banda debido a su mayor frecuencia de reloj. Permite módulos DIMM de hasta 16 GB de capacidad.
DDR4-SDRAM: memoria de acceso aleatorio dinámica síncrona con doble velocidad de datos y cuatro (4)	Incluye una mayor densidad de módulos y requisitos de voltaje más bajos. En teoría, permite DIMM de hasta 512 GB de capacidad, en comparación con el máximo de 128 GB de DDR4 por DIMM.

Memoria de escritorio	Descripción
Memoria del portátil	**Descripción**
SODIMM: DIMM de contorno pequeño	Se diferencia de la RAM de escritorio en tamaño físico y configuración de pines. Un DIMM de tamaño completo tiene 100, 168, 184, 240 o 288 pines y suele tener una longitud de 4,5 a 5 pulgadas. Por el contrario, un SODIMM tiene 72, 100, 144, 200, 204 o 260 pines y es más pequeño: de 2,5 a 3 pulgadas.

La ROM, por otro lado, no es volátil y tampoco se puede sobrescribir sin ejecutar una serie de operaciones que dependen del tipo de ROM. Por lo general, contiene instrucciones de bajo nivel de algún tipo que hacen que el dispositivo en el que está instalado sea operativo. Algunos ejemplos de ROM son

- **Memoria flash :** un tipo de ROM programable eléctricamente
- **Dispositivo lógico programable (PLD):** un circuito integrado con conexiones o puertas lógicas internas que se pueden cambiar mediante un proceso de programación.
- **Arreglo de puerta programable en campo (FPGA) :** un tipo de PLD que se programa soplando conexiones de fusibles en el chip o usando un antifusible que hace una conexión cuando se aplica un alto voltaje a la unión
- **Firmware :** un tipo de ROM donde se instala un programa o instrucciones de bajo nivel

La memoria directamente direccionable por la CPU, que es para el almacenamiento de instrucciones y datos que están asociados con el programa que se está ejecutando, se denomina memoria *primaria* . Independientemente del tipo de memoria en la que se encuentre la información, en la mayoría de los casos la CPU debe participar en la obtención de la información en nombre de otros componentes. Si un componente tiene la capacidad de acceder a la memoria directamente sin la ayuda de la CPU, se denomina *acceso directo a la memoria (DMA)* .

Algunos términos adicionales con los que debe estar familiarizado con respecto a la memoria incluyen los siguientes:

- **Memoria asociativa :** busca un valor de datos específico en la memoria en lugar de usar una dirección de memoria específica.
- **Direccionamiento implícito : se** refiere a los registros normalmente contenidos dentro de la CPU.
- **Direccionamiento absoluto : se** dirige a todo el espacio de la memoria primaria. La CPU utiliza las direcciones de memoria física que se denominan direcciones absolutas.
- **Caché :** Una cantidad relativamente pequeña (en comparación con la memoria primaria) de RAM de muy alta velocidad que contiene las instrucciones y los datos de la memoria primaria y que tiene una alta probabilidad de ser accedida durante la parte de ejecución de un programa.
- **Direccionamiento indirecto :** el tipo de direccionamiento de memoria donde la ubicación de la dirección que se especifica en la instrucción del programa contiene la dirección de la ubicación final deseada.

- **Dirección lógica:** la dirección en la que parece residir una celda de memoria o un elemento de almacenamiento desde la perspectiva de un programa de aplicación en ejecución.
- **Dirección relativa:** especifica su ubicación indicando su distancia de otra dirección.
- **Memoria virtual:** una ubicación en el disco duro que se usa temporalmente para almacenamiento cuando el espacio de memoria es bajo.
- **Pérdida de memoria:** ocurre cuando un programa de computadora administra incorrectamente las asignaciones de memoria, lo que puede agotar la memoria disponible del sistema mientras se ejecuta una aplicación.
- **Memoria secundaria :** medios magnéticos, ópticos o basados en flash u otros dispositivos de almacenamiento que contienen datos que el sistema operativo debe leer primero y almacenar en la memoria. Esta memoria es menos costosa que la memoria primaria.
- **Memoria volátil :** memoria que se vacía cuando el dispositivo se apaga.
- **Memoria no volátil :** almacenamiento persistente a largo plazo que permanece incluso cuando el dispositivo se apaga.

Acceso aleatorio versus secuencial

Los dispositivos de acceso aleatorio leen datos inmediatamente desde cualquier punto de la unidad. Los dispositivos de acceso secuencial leen los datos a medida que se almacenan en la unidad en el orden en que se almacenan. La RAM, los discos duros magnéticos y las unidades flash USB son dispositivos de acceso secuencial, mientras que las cintas magnéticas son dispositivos de acceso secuencial.

Dispositivos de entrada / salida

Los dispositivos de entrada / salida (E / S) se utilizan para enviar y recibir información al sistema. Algunos ejemplos son el teclado, el mouse, las pantallas y las impresoras. El sistema operativo controla la interacción entre los dispositivos de E / S y el sistema. En los casos en que el dispositivo de E / S requiere que la CPU realice alguna acción, envía una señal a la CPU con un mensaje llamado interrupción.

Estructuras de entrada / salida

Algunas actividades de la computadora son operaciones de E / S generales que requieren la configuración manual de los dispositivos. Las estructuras de E / S utilizadas por esas actividades utilizan E / S mapeadas en memoria, solicitudes de interrupción (IRQ) y acceso directo a memoria (DMA).

Con E / S mapeadas en memoria, la CPU administra el acceso a una serie de direcciones o ubicaciones de memoria mapeadas. Usando estas ubicaciones mapeadas en memoria, el usuario realmente obtiene información del dispositivo correspondiente. La entrada se copia en esas ubicaciones de memoria cuando el dispositivo indica que está listo. Cuando el usuario escribe en las ubicaciones asignadas en memoria, la salida al dispositivo se copia desde la ubicación de la memoria al dispositivo cuando la CPU indica que la salida está lista. Cuando se utiliza E / S con

asignación de memoria, un solo dispositivo debe asignarse a una dirección de memoria específica. Esa dirección no debe ser utilizada por nadie más. El sistema operativo administra el acceso a las ubicaciones de memoria asignadas.

Una IRQ asigna líneas de señal específicas a un dispositivo a través de un controlador de interrupciones. Cuando un dispositivo quiere comunicarse, envía una señal a la CPU a través de su IRQ asignada. Los dispositivos más antiguos deben tener uso exclusivo de una IRQ, mientras que los dispositivos plug-and-play (PnP) más nuevos pueden compartir una IRQ. Las computadoras más antiguas tenían IRQ de 0 a 15, mientras que las computadoras más nuevas tienen IRQ de 0 a 23. Si se produce un conflicto de IRQ, ninguno de los dispositivos que comparten la IRQ estará disponible. El sistema operativo gestiona el acceso a las IRQ.

El acceso DMA utiliza un canal con dos líneas de señal, una de las cuales es la línea de solicitud de DMA (DMQ) y la otra es la línea de reconocimiento de DMA (DACK). Este tipo de estructura de E / S permite que los dispositivos funcionen directamente con la memoria sin esperar a la CPU. La CPU simplemente autoriza el acceso y luego permite que el dispositivo se comunique con la memoria directamente. Se utiliza una señal DACK para devolver la ubicación de la memoria a la CPU. DMA es mucho más rápido que los otros dos métodos. El sistema operativo gestiona las asignaciones de DMA.

Firmware

El firmware es un software que se almacena en un chip EPROM o EEPROM dentro de un dispositivo. Si bien las actualizaciones del firmware pueden ser necesarias, son poco frecuentes. El firmware puede existir como el sistema básico de entrada / salida (BIOS) en una computadora o firmware de dispositivo.

BIOS / UEFI

El BIOS de una computadora contiene las instrucciones básicas que una computadora necesita para iniciar y cargar el sistema operativo desde una unidad. El proceso de actualización del BIOS con el software más reciente se conoce como actualización del BIOS. Los profesionales de seguridad deben asegurarse de que las actualizaciones de BIOS se obtengan del proveedor de BIOS y no se hayan manipulado de ninguna manera.

El BIOS tradicional ha sido reemplazado por la Interfaz de firmware extensible unificada (UEFI). UEFI mantiene la compatibilidad con dispositivos BIOS heredados, pero se considera una interfaz más avanzada que la BIOS tradicional. BIOS usa el registro de arranque maestro (MBR) para guardar información sobre los datos del disco duro, mientras que UEFI usa la tabla de particiones GUID (GPT). Las particiones de la BIOS tenían un máximo de 4 particiones, cada una con solo 2 terabytes (TB). UEFI permite hasta 128 particiones, con un límite de disco total de 9,4 zettabytes (ZB) o 9,4 mil millones de terabytes. UEFI también es más rápido y seguro que el BIOS tradicional. UEFI Secure Boot requiere que los cargadores de arranque tengan una firma digital.

UEFI es una capa de interfaz estándar abierta entre el firmware y el sistema operativo que requiere que las actualizaciones de firmware estén firmadas digitalmente. Los profesionales de la seguridad deben comprender los siguientes puntos relacionados con UEFI:

- Diseñado como reemplazo del BIOS de PC tradicional
- La funcionalidad adicional incluye soporte para arranque seguro, autenticación de red y controladores de gráficos universales
- Protege contra ataques de malware de BIOS, incluidos rootkits

El arranque seguro requiere que todos los componentes del cargador de arranque (p. Ej., Kernel del sistema operativo, controladores) den fe de su identidad (firma digital) y la atestación se compare con la lista de confianza.

- Cuando se fabrica una computadora, se incrusta en UEFI una lista de claves que identifican el hardware, el firmware y el código del cargador del sistema operativo confiables (y, en algunos casos, el malware conocido).
- Garantiza la integridad y seguridad del firmware.
- Evita que se carguen archivos maliciosos.
- Puede desactivarse para compatibilidad con versiones anteriores.

Firmware del dispositivo

Los dispositivos de hardware, como enrutadores e impresoras, requieren cierta potencia de procesamiento para completar sus tareas. Este firmware está contenido en los chips de firmware ubicados dentro de los dispositivos. Al igual que con las computadoras, este firmware a menudo se instala en EEPROM para permitir su actualización. Nuevamente, los profesionales de la seguridad deben asegurarse de que las actualizaciones solo se obtengan del proveedor del dispositivo y que las actualizaciones no se hayan modificado de ninguna manera.

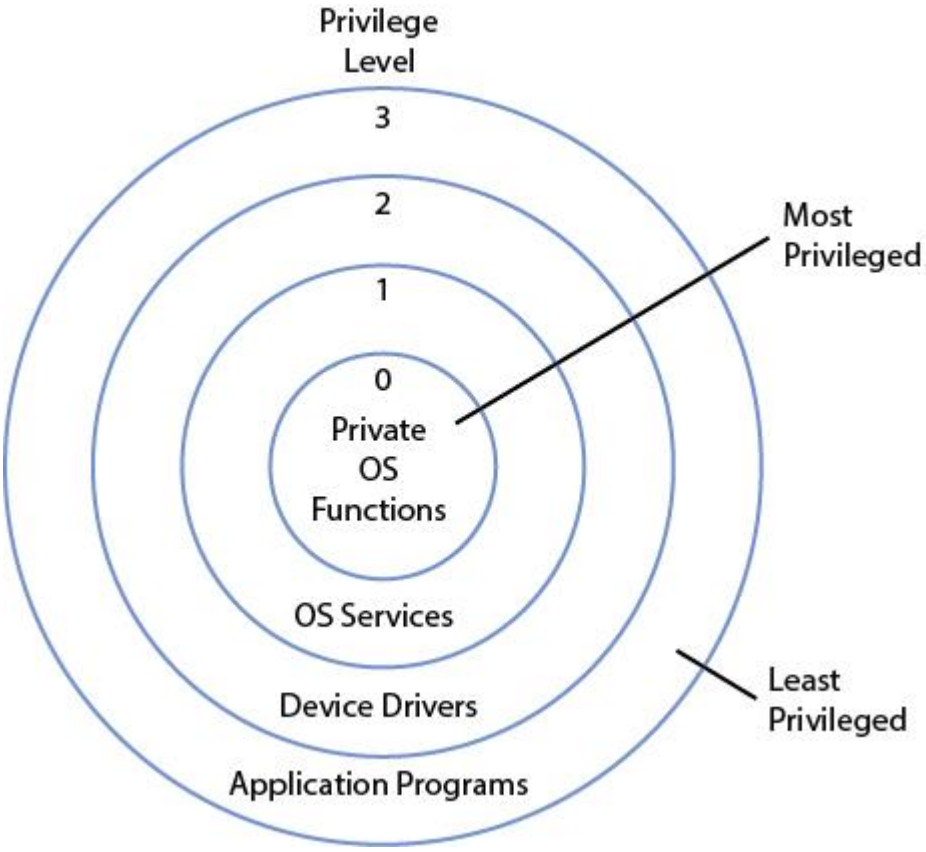
Sistemas operativos

El sistema operativo es el software que permite a un ser humano interactuar con el hardware que comprende la computadora. Sin el sistema operativo, la computadora sería inútil. Los sistemas operativos realizan una serie de funciones interesantes y dignas de mención como parte de la interfaz entre el ser humano y el hardware. En esta sección, analizamos algunas de estas actividades.

Un hilo es un trabajo individual realizado para un proceso específico. Un proceso es un conjunto de subprocesos que forman parte del mismo trabajo más grande realizado para una aplicación específica. Las instrucciones de una aplicación no se consideran procesos hasta que se cargan en la memoria, donde primero deben copiarse todas las instrucciones para ser procesadas por la CPU. Un proceso puede estar en estado de ejecución, listo o bloqueado. Cuando un proceso está bloqueado, simplemente está esperando que se le transmitan datos, generalmente a través de la entrada de datos del usuario. Un grupo de procesos que comparten el acceso a los mismos recursos se denomina dominio de protección.

Las CPU se pueden clasificar de acuerdo con la forma en que manejan los procesos. Una arquitectura de computadora superescalar se caracteriza por un procesador que permite la ejecución concurrente de múltiples instrucciones en la misma etapa de canalización. Un procesador en el que una sola instrucción especifica más de una operación simultánea se denomina procesador de palabra de instrucción muy larga (VLIW). Un procesador de canalización se superpone a los pasos de diferentes instrucciones, mientras que un procesador escalar ejecuta una instrucción a la vez, lo que aumenta la canalización.

Desde una perspectiva de seguridad, los procesos se colocan en una estructura de anillo de acuerdo con el concepto de privilegio mínimo, lo que significa que solo se les permite acceder a los recursos y componentes necesarios para realizar la tarea. En la Figura 3-5 se muestra una visualización común de esta estructura .



Se muestran cuatro estructuras de anillos concéntricos con sus niveles de privilegio. El anillo más interno marcado con 0 representa "Funciones privadas del sistema operativo". El segundo anillo más interno marcado con un 1 representa "Servicios de SO". El tercer anillo más interno marcado con 2 representa "Controladores de dispositivo". El anillo más externo marcado con 3 representa "Programas de aplicación". El anillo más interno está etiquetado como "Más privilegiado". y el anillo más externo está etiquetado como "Menos privilegiado".

Figura 3-5 Estructura de anillo

Cuando un sistema informático procesa instrucciones de E / S, está funcionando en modo supervisor. La terminación del procesamiento seleccionado, no crítico, cuando ocurre una falla de hardware o software y se detecta, se conoce como falla suave. Está en un estado a prueba de fallas si el sistema deja automáticamente los procesos y componentes del sistema en un estado seguro cuando ocurre una falla o se detecta en el sistema.

Gestión de la memoria

Debido a que toda la información va a la memoria antes de que pueda procesarse, la administración segura de la memoria es fundamental. El espacio de memoria aislado de otros procesos en ejecución en un sistema de multiprocesamiento es parte de un dominio de protección.

Modelos de evaluación de seguridad del sistema

En un intento por poner orden en el caos de seguridad que rodea a los productos de software tanto internos como comerciales (sistema operativo, aplicaciones, etc.), se han creado varios modelos de evaluación para evaluar y calificar la seguridad de estos productos. Un examen de nivel de garantía intenta examinar los componentes relacionados con la seguridad de un sistema y asignar un nivel de confianza de que el sistema puede proporcionar un nivel particular de seguridad. En las siguientes secciones, se discuten las organizaciones que han creado tales sistemas de evaluación.

TCSEC

El Trusted Computer System Evaluation Criteria (TCSEC) fue desarrollado por el National Computer Security Center (NCSC) para que el Departamento de Defensa de EE. UU. Evalúe los productos. NCSC ha publicado una serie de libros que se centran tanto en los sistemas informáticos como en las redes en las que operan. Abordan la confidencialidad, pero no la integridad. En 2005, TCSEC fue reemplazado por los Criterios Comunes, discutidos más adelante en el capítulo. Sin embargo, los profesionales de la seguridad aún necesitan comprender TCSEC debido a su efecto en las prácticas de seguridad en la actualidad y porque parte de su terminología todavía se utiliza.

Con TCSEC, la funcionalidad y la garantía se evalúan por separado y forman una base para evaluar la eficacia de los controles de seguridad integrados en los productos del sistema de procesamiento automático de datos. Por ejemplo, el concepto de privilegio mínimo se deriva de TCSEC. En esta sección, se analizan esos libros y las calificaciones que obtienen.

Serie arcoíris

La publicación original creada por TCSEC fue el Libro Naranja, pero con el paso del tiempo, también se crearon otros libros que se enfocaron en aspectos adicionales de la seguridad de los sistemas informáticos. En conjunto, este conjunto de más de 20 libros ahora se conoce como la Serie Arcoíris, en alusión al hecho de que cada libro es de un color diferente. Por ejemplo, el

Libro Verde se centra únicamente en la gestión de contraseñas. El resto de esta sección cubre los libros más importantes, el Libro Rojo, el Libro Naranja y el Libro Verde.

libro Rojo

La interpretación de la red confiable (TNI) extiende las clases de evaluación del TCSEC (DOD 5200.28-STD) a los componentes y sistemas de red confiables en el Libro Rojo. Entonces, donde el Libro naranja se centra en la seguridad de un solo sistema, el Libro rojo se ocupa de la seguridad de la red.

Libro naranja

El Libro Naranja es una colección de criterios basados en el modelo Bell-LaPadula que se utiliza para calificar o calificar la seguridad que ofrece un producto de sistema informático. El análisis de canal encubierto, la administración de instalaciones confiables y las recuperaciones confiables son conceptos que se tratan en este libro.

Los objetivos de este sistema se pueden dividir en dos categorías, requisitos de garantía operativa y requisitos de garantía del ciclo de vida, cuyos detalles se definen a continuación.

Los requisitos de garantía operativa especificados en el Libro naranja son los siguientes:

- Arquitectura del sistema
- Integridad del sistema
- Análisis de canal encubierto
- Gestión de instalaciones de confianza
- Recuperación confiable

Los requisitos de garantía del ciclo de vida especificados en el Libro naranja son los siguientes:

- Pruebas de seguridad
- Prueba y especificación de diseño
- Gestión de la configuración
- Distribución confiable

TCSEC utiliza un sistema de clasificación que asigna una letra y un número para describir la efectividad de la seguridad de los sistemas. La letra se refiere a un nivel o división de garantía de seguridad, de los cuales hay cuatro, y el número se refiere a gradientes dentro de ese nivel o clase de garantía de seguridad. Cada división y clase incorpora todos los elementos requeridos de las que están debajo.

En orden de menos seguro a más seguro, las cuatro clases y sus divisiones constituyentes y requisitos son los siguientes:

- **D — Protección mínima**

  Reservado para sistemas que han sido evaluados pero que no cumplen con los requisitos de una división superior.

- **C — Protección discrecional**
  - *C1 — Protección de seguridad discrecional*
    - Requiere identificación y autenticación.
    - Requiere separación de usuarios y datos.
    - Utiliza control de acceso discrecional (DAC) capaz de imponer limitaciones de acceso de forma individual o grupal.
    - Requiere documentación del sistema y manuales de usuario.
  - *C2 — Protección de acceso controlado*
    - Utiliza un DAC de grano más fino.
    - Proporciona responsabilidad individual a través de procedimientos de inicio de sesión.
    - Requiere pistas de auditoría protegidas.
    - Invoca la teoría de la reutilización de objetos.
    - Requiere aislamiento de recursos.
- **B — Protección obligatoria**
  - *B1 — Protección de seguridad etiquetada*
    - Utiliza una declaración informal de la política de seguridad.
    - Requiere etiquetas de clasificación o sensibilidad de datos.
    - Utiliza MAC sobre sujetos y objetos seleccionados.
    - Capaz de exportar etiquetas.
    - Requiere la eliminación o mitigación de fallas descubiertas.
    - Utiliza especificaciones de diseño y verificación.
  - *B2 — Protección estructurada*
    - Requiere una política de seguridad claramente definida y formalmente documentada.
    - Utiliza la aplicación de DAC y MAC extendida a todos los sujetos y objetos.
    - Analiza y previene los canales de almacenamiento encubiertos para la ocurrencia y el ancho de banda.
    - Estructura los elementos en categorías críticas para la protección y no críticas para la protección.
    - Permite pruebas y revisiones más completas a través del diseño y la implementación.
    - Fortalece los mecanismos de autenticación.
    - Proporciona una gestión de instalaciones confiable con segregación de administrador y operador.
    - Impone estrictos controles de gestión de la configuración.
  - *B3 — Dominios de seguridad*

        - Satisface los requisitos del monitor de referencia.
        - Excluye el código que no es esencial para la aplicación de la política de seguridad.
        - Minimiza la complejidad a través de una ingeniería de sistemas significativa.
        - Define el rol de administrador de seguridad.
        - Requiere una auditoría de eventos relevantes para la seguridad.
        - Detecta y responde automáticamente a la detección de intrusos inminentes, incluida la notificación al personal.
        - Requiere procedimientos de recuperación de sistema confiables.
        - Analiza y evita los canales de temporización encubiertos para la ocurrencia y el ancho de banda.
        - Un ejemplo de tal sistema es el XTS-300, un precursor del XTS-400.
- **A — Protección verificada**
    - *A1 — Diseño verificado*
        - Proporciona mayor seguridad que B3, pero es funcionalmente idéntico a B3.
        - Utiliza técnicas formales de diseño y verificación, incluida una especificación formal de nivel superior.
        - Requiere que se utilicen técnicas formales para demostrar la equivalencia entre las especificaciones de Trusted Computer Base (TCB) y el modelo de política de seguridad.
        - Proporciona procedimientos formales de administración y distribución.
        - Un ejemplo de un sistema de este tipo es el procesador de comunicaciones seguras (SCOMP) de Honeywell, un precursor del XTS-400.

Libro Verde

El Libro Verde brinda orientación sobre la creación y administración de contraseñas. Incluye responsabilidades de inicio de sesión único (SSO), responsabilidades de usuario, mecanismos de autenticación y protección con contraseña. En esta guía se recomiendan las siguientes características principales:

- Los usuarios deberían poder cambiar sus propias contraseñas.
- Las contraseñas deben ser generadas por máquina en lugar de creadas por el usuario.
- El sistema debe proporcionar ciertos informes de auditoría (por ejemplo, fecha y hora del último inicio de sesión) directamente al usuario.

ITSEC

TCSEC se ocupa únicamente de la confidencialidad y agrupa la funcionalidad y la garantía. A diferencia de TCSEC, los Criterios de evaluación de seguridad de la tecnología de la información (ITSEC) abordan la integridad y la disponibilidad, así como la confidencialidad. Otra diferencia es que la ITSEC era principalmente un conjunto de pautas utilizadas en Europa, mientras que la TCSEC se confiaba más en los Estados Unidos.

ITSEC tiene un sistema de clasificación en muchos aspectos similar al de TCSEC. ITSEC tiene 10 clases, F1 a F10, para evaluar los requisitos funcionales y 7 clases TCSEC, E0 a E6, para evaluar los requisitos de aseguramiento.

Los requisitos funcionales de seguridad incluyen lo siguiente:

- **F00:** Identificación y autenticación
- **F01:** Auditoría
- **F02:** Utilización de recursos
- **F03:** Rutas / canales confiables
- **F04:** Protección de datos del usuario
- **F05:** Gestión de seguridad
- **F06:** Acceso al producto
- **F07:** Comunicaciones
- **F08:** Privacidad
- **F09:** Protección de las funciones de seguridad del producto.
- **F10:** soporte criptográfico

Los requisitos de garantía de seguridad incluyen lo siguiente:

- **E00:** Documentos de orientación y manuales
- **E01:** Gestión de la configuración
- **E02:** Evaluación de vulnerabilidades
- **E03:** Entrega y operación
- **E04:** Soporte de ciclo de vida
- **E05:** Seguro de mantenimiento
- **E06:** Desarrollo
- **E07:** Prueba

Los sistemas TCSEC e ITSEC se pueden mapear entre sí, pero ITSEC proporciona una serie de calificaciones que no tienen un concepto correspondiente en las calificaciones TCSEC. La Tabla 3-3 muestra un mapeo de los dos sistemas.

Tabla 3-3 Mapeo de ITSEC y TCSEC

ITSEC	TCSEC
E0	D
F1 + E1	C1
F2 + E2	C2
F3 + E3	B1
F4 + E4	B2

ITSEC	TCSEC
F5 + E5	B3
F6 + E6	A1
F6	Sistemas que brindan alta integridad
F7	Sistemas que brindan alta disponibilidad
F8	Sistemas que brindan alta integridad de datos durante la comunicación
F9	Sistemas que brindan alta confidencialidad (usando criptografía)
F10	Redes con altas exigencias de confidencialidad e integridad

El ITSEC ha sido reemplazado en gran parte por Common Criteria, que se analiza en la siguiente sección.

Criterios comunes

En 1990, la ISO identificó la necesidad de un sistema de clasificación estandarizado que pudiera usarse a nivel mundial. Los Criterios Comunes (CC) para la Evaluación de la Seguridad de la Tecnología de la Información fue el resultado de un esfuerzo cooperativo para establecer este sistema. Este sistema utiliza los niveles de garantía de evaluación (EAL) para calificar los sistemas, y cada EAL representa un nivel sucesivamente más alto de pruebas de seguridad y diseño en un sistema. La calificación resultante representa el potencial que tiene el sistema para brindar seguridad. Se asume que el cliente configurará correctamente todas las soluciones de seguridad disponibles, por lo que se requiere que el proveedor siempre proporcione la documentación adecuada para permitir que el cliente logre completamente la calificación. ISO / IEC 15408-1: 2009 es la versión ISO del CC.

El CC representa los requisitos para la seguridad de TI de un producto o sistema en dos categorías: funcionalidad y garantía. Esto significa que la calificación debe describir lo que hace el sistema (funcionalidad) y el grado de certeza que tienen los evaluadores de que se puede proporcionar la funcionalidad (garantía).

El CC tiene siete niveles de garantía, que van desde EAL1 (el más bajo), donde se realizan las pruebas de funcionalidad, hasta EAL7 (el más alto), donde se realizan pruebas exhaustivas y se verifica el diseño del sistema.

Los designadores de aseguramiento utilizados en el CC son los siguientes:

- **EAL1:** probado funcionalmente
- **EAL2:** probado estructuralmente
- **EAL3:** probado y comprobado metódicamente
- **EAL4:** diseñado, probado y revisado metódicamente
- **EAL5:** diseñado y probado **semiformalmente**

- **EAL6: Diseño semiformalmente** verificado y probado
- **EAL7:** Diseño verificado formalmente y probado

El CC utiliza un concepto llamado perfil de protección durante el proceso de evaluación. El perfil de protección describe un conjunto de requisitos u objetivos de seguridad junto con supuestos funcionales sobre el entorno. Por lo tanto, si alguien identifica una necesidad de seguridad que ningún producto aborda actualmente, podría escribir un perfil de protección que describa la necesidad y la solución y todos los problemas que podrían salir mal durante el desarrollo del sistema. Esto se utilizaría para guiar el desarrollo de un nuevo producto. Un perfil de protección contiene los siguientes elementos:

- **Elementos descriptivos:** El nombre del perfil y una descripción del problema de seguridad a resolver.
- **Justificación:** Justificación del perfil y una descripción más detallada del problema del mundo real a resolver. El entorno, los supuestos de uso y las amenazas se proporcionan junto con la orientación de la política de seguridad que puede ser compatible con productos y sistemas que se ajustan a este perfil.
- **Requisitos funcionales:** establecimiento de un límite de protección, es decir, las amenazas o compromisos que se encuentran dentro de este límite deben ser contrarrestados. El producto o sistema debe hacer cumplir el límite.
- **Requisitos de aseguramiento del desarrollo:** Identificación de los requisitos específicos que el producto o sistema debe cumplir durante las fases de desarrollo, desde el diseño hasta la implementación.
- **Requisitos de garantía de la evaluación:** establecimiento del tipo e intensidad de la evaluación.

El resultado de seguir este proceso será un objetivo de seguridad. Esta es la explicación del proveedor de lo que el producto aporta a la mesa desde el punto de vista de la seguridad. Los grupos intermedios de requisitos de seguridad desarrollados a lo largo del camino hacia un objetivo de seguridad se denominan paquetes.

Si bien es importante comprender los niveles EAL del CC, el CC se ha rediseñado recientemente. Common Criteria Versión 3.1, Revisión 5, utiliza el término Objetivo de evaluación (TOE). Un TOE se define como un conjunto de software, firmware y / o hardware posiblemente acompañado de una guía. El TOE consta de una versión específica y una representación específica del TOE. Por ejemplo, el sistema operativo Windows 8.1 Pro esuna versión específica, y su configuración en una computadora basada en las políticas de seguridad de la organización es la representación específica.

El nuevo CC incluye dos tipos de evaluaciones: evaluación de objetivo de seguridad (ST) / evaluación de TOE y evaluación de perfil de protección (PP). En una evaluación ST, se determina la suficiencia del TOE y el entorno operativo. En una evaluación de TOE, se determina la corrección del TOE. La evaluación PP es un documento, normalmente creado por un usuario o una comunidad de usuarios, que identifica los requisitos de seguridad para una clase de dispositivos de seguridad relevantes para ese usuario para un propósito particular.

Los Criterios Comunes han categorizado los PP en 14 categorías:

- Dispositivos y sistemas de control de acceso
- Sistemas y dispositivos biométricos
- Dispositivos y sistemas de protección de límites
- Protección de Datos
- Bases de datos
- Circuitos integrados, tarjetas inteligentes y dispositivos y sistemas relacionados con tarjetas inteligentes
- Sistemas de gestión de claves
- Movilidad
- Dispositivos multifunción
- Dispositivos y sistemas de red y relacionados con la red
- Sistemas operativos
- Otros dispositivos y sistemas
- Productos para firmas digitales
- Computación confiable

A los perfiles de protección se les asigna un EAL después de que una organización miembro los analice en el Acuerdo de reconocimiento de criterios comunes (CCRA). Para obtener más información sobre la implementación más reciente de Common Criteria, visite https://www.commoncriteriaportal.org/ . Haga clic en la pestaña Perfiles de protección para ver los PP disponibles.

Estándares de implementación de seguridad

Es importante que un profesional de la seguridad comprenda los estándares de implementación de seguridad publicados por organismos internacionales. Además, los profesionales de la seguridad deben examinar los estándares de la industria que se aplican a sus organizaciones. Estos estándares incluyen ISO / IEC 27001 y 27002 y PCI DSS.

Nota

COBIT 5 también podría discutirse en esta sección. Sin embargo, se trata de manera adecuada en el Capítulo 1 . ISO / IEC 27001 y 27002 también se mencionan brevemente en ese capítulo, pero se tratan con más profundidad aquí.

ISO / IEC 27001

ISO / IEC 27001: 2013 es la última versión del estándar 27001 y es uno de los estándares más populares mediante los cuales las organizaciones obtienen la certificación de seguridad de la información. Proporciona orientación sobre cómo garantizar que el sistema de gestión de seguridad de la información (SGSI) de una organización se construya, administre, mantenga y progrese correctamente. Incluye los siguientes componentes:

- Alcance del SGSI

- Política de seguridad de la información
- Proceso de evaluación de riesgos y sus resultados
- Proceso de tratamiento de riesgos y sus decisiones
- Objetivos de seguridad de la información
- Competencia del personal de seguridad de la información
- Documentos relacionados con el SGSI que son necesarios
- Documentos de control y planificación operativa
- Evidencia de seguimiento y medición de la seguridad de la información
- Programa de auditoría interna del SGSI y sus resultados
- Evidencia de revisión del SGSI de la alta dirección
- Evidencia de no conformidades identificadas y acciones correctivas

Cuando una organización decide obtener la certificación ISO / IEC 27001, se debe seleccionar un director de proyecto para garantizar que todos los componentes se completen correctamente.

Para implementar ISO / IEC 27001: 2013, un gerente de proyecto debe completar los siguientes pasos:

1. Obtenga apoyo administrativo.
2. Determine si utilizar consultores o completar la implementación internamente y, en este último caso, comprar el estándar 27001, redactar el plan del proyecto, definir las partes interesadas y organizar el inicio del proyecto.
3. Identifica los requisitos.
4. Definir el alcance del SGSI, la política de seguridad de la información y los objetivos de seguridad de la información.
5. Desarrollar procedimientos de control de documentos, auditoría interna y acciones correctivas.
6. Realizar evaluación de riesgos y tratamiento de riesgos.
7. Desarrolle una declaración de aplicabilidad y plan de tratamiento de riesgos y acepte todos los riesgos residuales.
8. Implementar controles definidos en el plan de tratamiento de riesgos y mantener registros de implementación.
9. Desarrollar e implementar programas de concientización y capacitación en seguridad.
10. Implementar el SGSI, mantener políticas y procedimientos y realizar acciones correctivas.
11. Mantener y monitorear el SGSI.
12. Realice una auditoría interna y redacte un informe de auditoría.
13. Realizar la revisión de la dirección y mantener registros de la revisión de la dirección
14. Seleccione un organismo de certificación y complete la certificación.
15. Mantener registros de visitas de vigilancia.

ISO / IEC 27002

ISO / IEC 27002: 2013 es la última versión del estándar 27002 y proporciona un código de prácticas para la gestión de la seguridad de la información.

Incluye las siguientes 14 áreas de contenido:

- Política de seguridad de la información
- Organización de la seguridad de la información
- Seguridad de los recursos humanos
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y ambiental
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Relaciones con proveedores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información de la continuidad del negocio
- Cumplimiento

Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)

PCI DSS Versión 3.2 es para comerciantes y otras entidades involucradas en el procesamiento de tarjetas de pago. El cumplimiento de PCI DSS ayuda a aliviar las vulnerabilidades y proteger los datos de los titulares de tarjetas. Hay tres pasos continuos para adherirse a PCI DSS:

- **Evaluar:** Identifique todas las ubicaciones de datos de titulares de tarjetas, realice un inventario de sus activos de TI y procesos comerciales para el procesamiento de tarjetas de pago y analícelos en busca de vulnerabilidades que podrían exponer los datos de titulares de tarjetas.
- **Reparación:** solucione las vulnerabilidades identificadas, elimine de forma segura cualquier almacenamiento innecesario de datos del titular de la tarjeta e implemente procesos comerciales seguros.
- **Informe:** documente los detalles de la evaluación y corrección, y envíe informes de cumplimiento al banco adquirente y a las marcas de tarjetas u otra entidad solicitante.

PCI DSS se aplica a todas las entidades que almacenan, procesan y / o transmiten datos de titulares de tarjetas. Cubre los componentes técnicos y operativos del sistema incluidos o conectados a los datos del titular de la tarjeta. Si una organización acepta o procesa tarjetas de pago, PCI DSS se aplica a esa organización.

Para obtener más información sobre PCI-DSS, puede descargar la Guía de inicio rápido de PCI-DSS en https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf .

Controles y contramedidas

Después de que una organización implementa un modelo de evaluación de la seguridad del sistema y un estándar de implementación de la seguridad, la organización debe asegurarse de que se implementen los controles y contramedidas adecuados, en función de las evaluaciones de vulnerabilidad y riesgo más recientes realizadas por profesionales de la seguridad. Comprender las diferentes categorías y tipos de controles de acceso es vital para garantizar que una organización implemente un programa de seguridad integral. La seguridad de la información siempre debe ser algo que la organización evalúe y persiga.

Nota

Las categorías y tipos de control de acceso se analizan en profundidad en el Capítulo 1 .

Certificación y acreditación

Aunque los términos se utilizan como sinónimos en conversaciones casuales, la acreditación y la certificación son dos conceptos diferentes en el contexto de los niveles de garantía y las calificaciones, aunque están estrechamente relacionados. La certificación evalúa los componentes técnicos del sistema, mientras que la acreditación se produce cuando la dirección acepta la idoneidad de la seguridad general de un sistema.

El Proceso Nacional de Certificación y Acreditación de Aseguramiento de la Información (NIACAP) proporciona un conjunto estándar de actividades, tareas generales y una estructura de gestión para certificar y acreditar sistemas que mantendrán la seguridad de la información y la postura de seguridad de un sistema o sitio.

El proceso de acreditación desarrollado por NIACAP tiene cuatro fases:

- Fase 1: Definición
- Fase 2: Verificación
- Fase 3: Validación
- Fase 4: Post Acreditación

NIACAP define los siguientes tres tipos de acreditación:

- La acreditación de tipo evalúa una aplicación o sistema que se distribuye a varias ubicaciones diferentes.
- La acreditación del sistema evalúa una aplicación o un sistema de apoyo.
- La acreditación del sitio evalúa la aplicación o el sistema en una ubicación autónoma específica.

Selección de control basada en los requisitos de seguridad de los sistemas

Si bien los controles deben seleccionarse en función de los modelos de evaluación de la seguridad de los sistemas, también deben seleccionarse en función de los requisitos de seguridad de los sistemas. Los controles de seguridad incluyen las contramedidas administrativas, operativas y técnicas utilizadas dentro de un sistema de información organizacional para proteger a la CIA del sistema y su información.

Seleccionar e implementar los controles de seguridad apropiados para un sistema de información son tareas importantes que pueden tener implicaciones importantes en las operaciones y activos de una organización. De acuerdo con el Marco de Gestión de Riesgos del NIST, las organizaciones deben mitigar adecuadamente el riesgo que surge del uso de información y sistemas de información en la ejecución de misiones y funciones comerciales. Un desafío importante para las organizaciones es determinar el conjunto apropiado de controles de seguridad que, si se implementan y se determina que son efectivos, mitigarían el riesgo de manera más rentable mientras se cumplen los requisitos de seguridad definidos por las leyes, directivas, políticas, estándares o estándares federales aplicables. regulaciones.

El proceso de selección del control de seguridad incluye, según corresponda:

- Elegir un conjunto de controles de seguridad básicos
- Adaptación de los controles de seguridad de línea base mediante la aplicación de orientación de control de alcance, parametrización y compensación
- Complementar los controles de seguridad de línea de base personalizados, si es necesario, con controles adicionales o mejoras de control para abordar las necesidades organizacionales únicas basadas en una evaluación de riesgos y condiciones locales, incluido el entorno de operación, los requisitos de seguridad específicos de la organización, información de amenazas específicas, análisis de costo-beneficio o circunstancias especiales
- Especificación de requisitos mínimos de garantía

El propietario del sistema de información y el arquitecto de seguridad de la información son responsables de seleccionar los controles de seguridad para el sistema de información y de documentar los controles en el plan de seguridad.

Nota

El Marco de Gestión de Riesgos del NIST se trata con más detalle en el Capítulo 1 .

Capacidades de seguridad de los sistemas de información

Las organizaciones deben comprender las capacidades de seguridad de cualquier sistema de información que implementen. Esta sección trata sobre la protección de la memoria, la virtualización, el módulo de plataforma segura, las interfaces y la tolerancia a fallas.

Protección de la memoria

En un sistema de información, la memoria y el almacenamiento son los recursos más importantes. Los datos dañados o corruptos en la memoria pueden hacer que el sistema deje de funcionar. Los datos almacenados en la memoria pueden divulgarse y, por lo tanto, deben protegerse. La memoria no aísla los procesos y subprocesos en ejecución de los datos. Los profesionales de la seguridad deben utilizar estados de procesador, capas, aislamiento de procesos, abstracción, segmentación de hardware y ocultación de datos para ayudar a mantener los datos aislados.

La mayoría de los procesadores admiten dos estados de procesador: estado de supervisor (o modo de kernel) y estado de problema (o modo de usuario). En el estado de supervisor, se utiliza el nivel de privilegio más alto del sistema para que el procesador pueda acceder a todo el hardware y los datos del sistema. En estado de problema, el procesador limita el acceso al hardware y los datos del sistema. Los procesos que se ejecutan en el estado de supervisor están aislados de los procesos que no se ejecutan en ese estado; Los procesos del estado del supervisor deben limitarse únicamente a las funciones básicas del sistema operativo.

Un profesional de la seguridad puede utilizar capas para organizar la programación en funciones independientes que interactúan de forma jerárquica. En la mayoría de los casos, cada capa solo tiene acceso a las capas directamente encima y debajo de ella. La protección de anillo es la implementación más común de las capas, siendo el anillo interior (anillo 0) el anillo más privilegiado y el anillo exterior (anillo 3) el privilegiado más bajo. El kernel del sistema operativo generalmente se ejecuta en el anillo 0 y las aplicaciones de usuario generalmente se ejecutan en el anillo 3.

Un profesional de seguridad puede aislar procesos proporcionando espacios de direcciones de memoria para cada proceso. Otros procesos no pueden acceder al espacio de direcciones asignado a otro proceso. Las distinciones de nombres y el mapeo virtual se utilizan como parte del aislamiento de procesos.

La abstracción se utiliza en la programación orientada a objetos. Esta doctrina establece que los usuarios deben conocer la sintaxis adecuada para usar un objeto y el tipo de datos que se devolverán. Los usuarios no necesitan conocer los detalles de cómo funciona el objeto. El acceso a los servicios o datos está mediado. Los grupos de objetos, llamados clases, permiten a los administradores controlar el acceso y los derechos de operación de las clases de objetos, en lugar de los objetos individuales. Esto alivia la carga administrativa.

La segmentación de hardware funciona como el aislamiento de procesos. Impide el acceso a información que pertenece a un nivel de seguridad superior. Sin embargo, la segmentación de hardware aplica las políticas mediante controles de hardware físico en lugar del aislamiento de procesos lógicos del sistema operativo. La segmentación de hardware es poco común y generalmente se reestructura para uso gubernamental, aunque algunas organizaciones pueden optar por utilizar este método para proteger datos privados o confidenciales.

La ocultación de datos evita que los procesos que operan en otros niveles de seguridad vean los datos de un nivel de seguridad.

Virtualización

Hoy en día, los servidores físicos se están consolidando cada vez más como servidores virtuales en la misma caja física. Incluso existen redes virtuales que utilizan conmutadores virtuales en los dispositivos físicos que albergan estos servidores virtuales. Estos sistemas de redes virtuales y su tráfico se pueden segregar de todas las mismas formas que en una red física utilizando subredes, VLAN y, por supuesto, firewalls virtuales. Los firewalls virtuales son software que se ha escrito específicamente para operar en el entorno virtual. Cada vez más, los proveedores de virtualización como VMware están poniendo parte de su código a disposición de los proveedores de seguridad para crear firewalls (y productos antivirus) que se integran estrechamente con el producto.

Tenga en cuenta que en cualquier entorno virtual cada servidor virtual alojado en el servidor físico debe configurarse con sus propios mecanismos de seguridad. Estos mecanismos incluyen software antivirus y antimalware y los últimos paquetes de servicios y actualizaciones de seguridad para TODO el software alojado en la máquina virtual. Además, recuerde que todos los servidores virtuales comparten los recursos del dispositivo físico.

Modulo de plataforma confiable

Trusted Platform Module (TPM) es un chip de seguridad instalado en las placas base de las computadoras que se encarga de administrar claves simétricas y asimétricas, hashes y certificados digitales. Este chip proporciona un servicio para proteger contraseñas, cifrar unidades y administrar derechos digitales, lo que dificulta mucho más a los atacantes el acceso a las computadoras que tienen un chip TPM habilitado.

Dos usos particularmente populares de TPM son la unión y el sellado. La vinculación en realidad "vincula" el disco duro mediante encriptación a una computadora en particular. Debido a que la clave de descifrado se almacena en el chip TPM, el contenido del disco duro está disponiblesólo cuando está conectado a la computadora original. Pero tenga en cuenta que todos los contenidos están en riesgo si el chip TPM falla y no existe una copia de seguridad de la clave.

El sellado, por otro lado, "sella" el estado del sistema a una configuración particular de hardware y software. Esto evita que los ataques realicen cambios en el sistema. Sin embargo, también puede dificultar mucho la instalación de una nueva pieza de hardware o un nuevo sistema operativo. El sistema solo puede arrancar después de que el TPM verifique la integridad del sistema comparando el valor hash calculado original de la configuración del sistema con el valor hash de su configuración en el momento del arranque.

El TPM consta de memoria estática y memoria dinámica que se utiliza para retener la información importante cuando la computadora está apagada.

La memoria utilizada en un chip TPM es la siguiente:

- **Clave de aprobación (EK):** memoria persistente instalada por el fabricante que contiene un par de claves pública / privada
- **Storage Root Key (SRK):** memoria persistente que protege las claves almacenadas en el TPM
- **Clave de identidad de atestación (AIK):** memoria dinámica que garantiza la integridad del EK
- **Hash del registro de configuración de la plataforma (PCR):** memoria dinámica que almacena datos hash para la función de sellado
- **Claves de almacenamiento:** memoria dinámica que contiene las claves utilizadas para cifrar el almacenamiento de la computadora, incluidos discos duros, unidades flash USB, etc.

Interfaces

Una interfaz es un mecanismo que emplea un usuario para acceder a un sistema, una aplicación, un dispositivo u otra entidad. La mayoría de los usuarios asumen que las interfaces que utilizan son seguras. Las organizaciones son responsables de garantizar que se implementen interfaces seguras en toda la red. Si una entidad tiene múltiples interfaces de usuario, como una interfaz gráfica de usuario, una interfaz de línea de comandos y una interfaz de acceso remoto, todas estas interfaces deben requerir autenticación segura. Es el trabajo de un profesional de la seguridad comprender la diferencia entre interfaces seguras e inseguras y asegurarse de que las interfaces inseguras sean reemplazadas por interfaces seguras.

Tolerancia a fallos

La tolerancia a fallas permite que un sistema continúe funcionando correctamente en caso de que fallen los componentes dentro del sistema. Por ejemplo, proporcionar tolerancia a fallas para un sistema de disco duro implica el uso de unidades tolerantes a fallas y adaptadores de unidades tolerantes a fallas.Sin embargo, el costo de cualquier tolerancia a fallas debe compararse con el costo del dispositivo o hardware redundante. Si las capacidades de seguridad de los sistemas de información no son tolerantes a fallas, los atacantes pueden acceder a los sistemas si fallan los mecanismos de seguridad. Las organizaciones deben sopesar el costo de implementar un sistema tolerante a fallas con el costo de cualquier ataque contra el sistema que se está protegiendo. Puede que no sea vital proporcionar un mecanismo de seguridad tolerante a fallas para proteger los datos públicos, pero es muy importante proporcionar un mecanismo de seguridad tolerante a fallas para proteger los datos confidenciales.

Mecanismos de política

Las organizaciones pueden implementar diferentes mecanismos de políticas para aumentar la seguridad de los sistemas de información. Los mecanismos de política incluyen el principio de privilegio mínimo, separación de privilegios y responsabilidad.

Principio de privilegio mínimo

El principio de privilegio mínimo es importante en el diseño de sistemas. Al diseñar los procesos del sistema operativo, los profesionales de la seguridad deben asegurarse de que los procesos del sistema se ejecuten en modo de usuario cuando sea posible. Cuando un proceso se ejecuta en modo privilegiado, el potencial de vulnerabilidades aumenta enormemente. Si un proceso necesita acceso a servicios privilegiados, es mejor utilizar una interfaz de programación de aplicaciones (API) para solicitar servicios en modo supervisor.

Relacionado con el principio de privilegio mínimo, el principio de funcionalidad mínima es que los sistemas y dispositivos deben configurarse para proporcionar solo las capacidades esenciales y prohibir o restringir específicamente el uso de funciones, puertos, protocolos y servicios.

Nota

El principio de privilegio mínimo también se analiza en el Capítulo 5 , “ Administración de acceso e identidad (IAM) ” y el Capítulo 7 , “ Operaciones de seguridad ”.

Separación de privilegios

El principio de separación de privilegios está ligado al principio de privilegio mínimo. La separación de privilegios requiere que los profesionales de la seguridad implementen diferentes permisos para cada tipo de operación privilegiada. Este principio asegura que el principio de privilegio mínimo se aplique a los usuarios de nivel administrativo. Muy pocos usuarios de nivel administrativo necesitan acceso completo a nivel administrativo a todos los sistemas. La separación de privilegios garantiza que el acceso de nivel administrativo solo se otorgue a los usuarios a solo aquellos recursos o privilegios que el usuario necesita para realizar.

Nota

No confunda la separación de privilegios con la separación de deberes, que se discutió en el Capítulo 1 .

Responsabilidad

La rendición de cuentas garantiza que los usuarios sean responsables de las acciones que realizan. Sin embargo, la responsabilidad depende en gran medida de la capacidad del sistema para monitorear la actividad. La rendición de cuentas generalmente se proporciona mediante funciones de auditoría del sistema. Cuando la auditoría está habilitada, también es importante asegurarse de que los registros de auditoría no se puedan editar. Por último, tenga en cuenta que la contabilidad también depende en gran medida de los sistemas de autorización y autenticación.

Las organizaciones no pueden rastrear las actividades de los usuarios si los usuarios no están autenticados y autorizados individualmente.

Cifrado / descifrado

Los sistemas de información utilizan cifrado y descifrado para brindar confidencialidad a los datos. El cifrado es el proceso de traducir datos de texto sin formato (texto sin formato) en datos ilegibles (texto cifrado), y el descifrado es el proceso de traducir texto cifrado de nuevo en texto sin formato. El cifrado y el descifrado se tratan más adelante en este capítulo en la sección " Criptografía ".

Mantenimiento de la arquitectura de seguridad

Desafortunadamente, después de que un producto ha sido evaluado, certificado y acreditado, la historia no termina. El producto generalmente evoluciona con el tiempo a medida que se desarrollan actualizaciones y parches para abordar nuevos problemas de seguridad que surgen o para agregar funcionalidad o corregir errores. Cuando ocurren estos cambios, como mantenimiento continuo, se debe mantener la arquitectura de seguridad.

Idealmente, las soluciones deben someterse a evaluaciones, certificaciones y acreditaciones adicionales a medida que ocurren estos cambios, pero en muchos casos las presiones del mundo real impiden este paso que requiere mucho tiempo. Esto es desafortunado porque a medida que los desarrolladores corrigen y parchean cosas, a menudo se desvían más y más del diseño de seguridad original mientras intentan apagar los incendios urgentes.

Aquí es donde el modelo de madurez se vuelve importante. La mayoría de los modelos de madurez se basan en el CMMI del Software Engineer Institute, que se analiza en el Capítulo 1 . Tiene cinco niveles: inicial, administrado, definido, administrado cuantitativamente y optimizado.

El modelo de madurez de capacidad (CMM) del Instituto de Ingeniería de Software (SEI) del Departamento de Defensa de EE. UU. (DoD) clasifica a las organizaciones según las mejores prácticas de la industria y las pautas internacionales. Incluye seis niveles de calificación, numerados de cero a cinco: inexistente, inicial, repetible, definido, administrado y optimizado. El nivel inexistente no corresponde a ningún nivel CMMI, pero todos los demás niveles sí.

Vulnerabilidades de arquitecturas de seguridad, diseños y elementos de solución

Las organizaciones deben evaluar y mitigar las vulnerabilidades de las arquitecturas, los diseños y los elementos de la solución de seguridad. Los sistemas inseguros están expuestos a muchas vulnerabilidades y amenazas comunes. Esta sección analiza las vulnerabilidades de los sistemas basados en clientes, sistemas basados en servidores, sistemas de bases de datos, sistemas criptográficos, sistemas de control industrial, sistemas basados en la nube, sistemas de datos paralelos a gran escala, sistemas distribuidos e Internet de las cosas.

Sistemas basados en el cliente

En la mayoría de las redes, los sistemas cliente son los más utilizados porque son los sistemas en los que más confían los usuarios para acceder a los recursos. Los sistemas cliente van desde sistemas de escritorio hasta computadoras portátiles y dispositivos móviles de todo tipo. Esta sección se centra principalmente en las vulnerabilidades de las computadoras de escritorio y portátiles.

Nota

Las vulnerabilidades de seguridad de los dispositivos móviles se tratan más adelante en este capítulo.

Debido a que los sistemas cliente son tan prolíficos, todos los días parecen surgir nuevos ataques contra estos sistemas. Los profesionales de la seguridad deben asegurarse de saber qué sistemas cliente se conectan a la red para poder asegurarse de que se implementen los controles adecuados para protegerlos.

Las vulnerabilidades tradicionales del lado del cliente suelen tener como objetivo los navegadores web, los complementos del navegador y los clientes de correo electrónico. Pero también se pueden realizar a través de las aplicaciones y sistemas operativos que se despliegan. Los sistemas cliente también tienden a tener implementados servicios expuestos que no son necesarios. A menudo, los sistemas cliente están expuestos a servidores hostiles. A estos problemas se suma el hecho de que la mayoría de los usuarios normales no son expertos en seguridad y, a menudo, sin darse cuenta, causan problemas de seguridad en los sistemas cliente.

La arquitectura de seguridad para los sistemas cliente debe incluir políticas y controles que cubran las siguientes áreas:

- Implementar solo sistemas operativos compatibles con licencia. Estos sistemas operativos deben actualizarse con todos los parches de proveedores, actualizaciones de seguridad y paquetes de servicios.
- Implementación de software antivirus y antimalware en cada sistema cliente. Las actualizaciones de este software deben ser automáticas para garantizar que se cubran las vulnerabilidades más recientes.
- Implementar un firewall y un sistema de detección de intrusiones basado en host en los sistemas cliente.
- Uso de cifrado de unidades para proteger los datos de los discos duros.
- Emitir cuentas de usuario con los permisos mínimos que los usuarios necesitan para realizar su trabajo. Los usuarios que necesitan acceso administrativo deben tener una cuenta administrativa y una cuenta regular y deben usar la cuenta administrativa solo cuando realicen tareas administrativas.
- Probar todas las actualizaciones y parches, incluidos los de los sistemas operativos y las aplicaciones, antes de la implementación a nivel de cliente.

Un subprograma es una pequeña aplicación que realiza una tarea específica. Se ejecuta dentro de un motor de widgets dedicado o un programa más grande, a menudo como un complemento. Los subprogramas de Java y los subprogramas de ActiveX son ejemplos. Los atacantes suelen

desplegar subprogramas maliciosos y parecen provenir de fuentes legítimas. Estos subprogramas se pueden utilizar para comprometer un sistema cliente. Un profesional de la seguridad debe asegurarse de que los clientes solo descarguen subprogramas de proveedores válidos. Además, un profesional de la seguridad debe asegurarse de que cualquier aplicación que incluya subprogramas se mantenga actualizada con los últimos parches.

Un sistema cliente contiene varios tipos de cachés locales. La caché de DNS contiene los resultados de las consultas de DNS en Internet y es la caché que se ataca con más frecuencia. Los atacantes pueden intentar envenenar la caché de DNS con direcciones IP falsas para dominios válidos. Lo hacen enviando una respuesta DNS maliciosa a un sistema afectado. Como ocurre con muchos otros problemas, debe asegurarse de que el sistema operativo y todas las aplicaciones se mantengan actualizados. Además, se debe capacitar a los usuarios para que nunca hagan clic en enlaces no verificados. No siempre apuntan al sitio que se muestra en el enlace visible.

Sistemas basados en servidor

En muchos casos, un ataque se centra en las operaciones del propio sistema operativo del servidor en lugar de en las aplicaciones web que se ejecutan sobre él. Más adelante en esta sección, veremos la forma en que se implementan estos ataques centrándonos principalmente en el tema de la manipulación del flujo de datos.

Control de flujo de datos

Los ataques de software a menudo subvierten el flujo de datos previsto de un programa vulnerable. Por ejemplo, los atacantes aprovechan los desbordamientos de búfer y formatean las vulnerabilidades de las cadenas para escribir datos en ubicaciones no deseadas. El objetivo final es leer datos de ubicaciones prohibidas o escribir datos en ubicaciones de memoria con el fin de ejecutar comandos, bloquear el sistema o realizar cambios maliciosos en el sistema. La mitigación adecuada para este tipo de ataques es la validación de entrada adecuada y los controles de flujo de datos integrados en el sistema.

Con respecto a las bases de datos en particular, una arquitectura de flujo de datos es aquella que entrega los tokens de instrucción a las unidades de ejecución y devuelve los tokens de datos a las memoria direccionable por contenido (CAM). (CAM es memoria de hardware, no lo mismo que RAM). A diferencia de la arquitectura convencional, los tokens de datos no se almacenan permanentemente en la memoria; más bien, son mensajes transitorios que solo existen cuando están en tránsito hacia el almacenamiento de instrucciones. Esto los hace menos propensos a verse comprometidos.

Sistemas de bases de datos

En muchos sentidos, una base de datos es el Santo Grial para el atacante. Por lo general, es donde reside la información confidencial. Al considerar la seguridad de la base de datos, debe comprender los siguientes términos: inferencia, agregación, contaminación y almacén de minería de datos.

Inferencia

La inferencia ocurre cuando alguien tiene acceso a información en un nivel que le permite inferir información sobre otro nivel. La principal técnica de mitigación para la inferencia es la poliinstanciación, que es el desarrollo de una versión detallada de un objeto a partir de otro objeto utilizando diferentes valores en el nuevo objeto. Evita que los usuarios de bases de datos de bajo nivel infieran la existencia de datos de nivel superior.

Agregación

La agregación se define como reunir o compilar unidades de información en un nivel de sensibilidad y tener la totalidad de datos resultante de un nivel de sensibilidad más alto que los componentes individuales. Por lo tanto, podría pensar en la agregación como una forma diferente de lograr el mismo objetivo que la inferencia, que es aprender información sobre los datos en un nivel al que no se tiene acceso.

Contaminación

La contaminación es la mezcla o mezcla de datos de un nivel de sensibilidad o necesidad de conocer con el de otro. La implementación adecuada de los niveles de seguridad es la mejor defensa contra estos problemas.

Almacén de minería de datos

Un almacén de datos es un depósito de información de bases de datos heterogéneas. Permite que múltiples fuentes de datos no solo se almacenen en un lugar, sino que se organicen de tal manera que se reduzca la redundancia de datos (lo que se denomina normalización de datos), y se utilizan herramientas de minería de datos más sofisticadas para manipular los datos para descubrir relaciones. que puede no haber sido evidente antes. Junto con los beneficios que brindan, también ofrecen más desafíos de seguridad.

Los siguientes son pasos de control que deben realizarse en aplicaciones de almacenamiento de datos:

- Supervise las tablas de resumen para su uso habitual.
- Supervise el plan de depuración de datos.
- Concilie los datos transferidos entre el entorno de operaciones y el almacén de datos.

Sistemas criptográficos

Por diseño, los sistemas criptográficos son responsables de cifrar los datos para evitar su divulgación. Los profesionales de la seguridad deben asegurarse de que su organización esté utilizando la última versión de un algoritmo criptográfico, si es posible. Una vez que se conoce el compromiso de un algoritmo criptográfico, ese algoritmo ya no debe utilizarse.

Nota

La criptografía se analiza con mayor detalle más adelante en este capítulo.

Sistemas de control industrial

Los sistemas de control industrial (ICS) es un término general que abarca varios tipos de sistemas de control utilizados en la producción industrial. El más extendido es el control de supervisión y la adquisición de datos (SCADA). SCADA es un sistema que opera con señales codificadas sobre canales de comunicación para proporcionar control de equipos remotos.

ICS incluye los siguientes componentes:

- **Sensores: los** sensores suelen tener E / S digitales o analógicas y no están en una forma que pueda comunicarse fácilmente a largas distancias.
- **Unidades terminales remotas (RTU): las** RTU se conectan a los sensores y convierten los datos del sensor en datos digitales, incluido el hardware de telemetría.
- **Controladores lógicos programables (PLC): los** PLC se conectan a los sensores y convierten los datos del sensor en datos digitales; no incluyen hardware de telemetría.
- **Sistema de telemetría:** este sistema conecta RTU y PLC a los centros de control y la empresa.
- **Interfaz humana:** una interfaz de este tipo presenta datos al operador.

Los ICS deben estar separados de forma segura de otras redes como capa de seguridad. El virus Stuxnet golpeó el SCADA utilizado para el control y seguimiento de procesos industriales. Los componentes SCADA se consideran objetivos privilegiados para los ciberataques. Mediante el uso de cybertooles, es posible destruir un proceso industrial. Esta fue la idea utilizada en el ataque a la planta nuclear de Natanz para interferir con el programa nuclear iraní.

Teniendo en cuenta la criticidad de los sistemas, el acceso físico a los sistemas basados en SCADA debe estar estrictamente controlado. Se deben implementar sistemas que integren la seguridad de TI con controles de acceso físico, como sistemas de identificación y vigilancia por video. Además, la solución debe integrarse con las herramientas de seguridad de la información existentes, como la gestión de registros e IPS / IDS. Una publicación útil de NIST, SP 800-82, ofrece recomendaciones sobre seguridad ICS. Los problemas con estos sistemas emergentes incluyen

- Los cambios necesarios en el sistema pueden anular la garantía.
- Los productos pueden lanzarse al mercado rápidamente con seguridad como una ocurrencia tardía.
- El retorno de la inversión puede llevar décadas.
- No hay regulación suficiente con respecto a estos sistemas.

NIST SP 800-82, Rev. 2 proporciona una guía de seguridad ICS.

Según esta publicación, los principales objetivos de seguridad para una implementación de ICS deben incluir lo siguiente:

- Restringir el acceso lógico a la red ICS y la actividad de la red
- Restringir el acceso físico a la red y los dispositivos de ICS
- Protección de los componentes individuales de ICS de la explotación
- Restringir la modificación no autorizada de datos
- Detectar incidentes y eventos de seguridad
- Mantener la funcionalidad durante condiciones adversas
- Restaurar el sistema después de un incidente

En un ICS típico, esto significa una estrategia de defensa en profundidad que incluye lo siguiente:

- Desarrollar políticas, procedimientos, capacitación y material educativo de seguridad que se aplique específicamente al ICS.
- Abordar la seguridad durante todo el ciclo de vida del ICS.
- Implemente una topología de red para el ICS que tenga múltiples capas, con las comunicaciones más críticas ocurriendo en la capa más segura y confiable.
- Proporcione una separación lógica entre las redes corporativas e ICS.
- Emplee una arquitectura de red DMZ.
- Asegúrese de que los componentes críticos sean redundantes y estén en redes redundantes.
- Diseñe sistemas críticos para una degradación elegante (tolerante a fallas) para evitar eventos catastróficos en cascada.
- Deshabilite los puertos y servicios no utilizados en los dispositivos ICS después de la prueba para asegurarse de que esto no afectará el funcionamiento del ICS.
- Restrinja el acceso físico a la red y los dispositivos de ICS.
- Restrinja los privilegios de usuario de ICS solo a aquellos que sean necesarios para realizar el trabajo de cada persona.
- Utilice mecanismos de autenticación y credenciales independientes para los usuarios de la red ICS y la red corporativa.
- Utilice tecnología moderna, como tarjetas inteligentes, para la verificación de identidad personal (PIV).
- Implementar controles de seguridad, como software de detección de intrusiones, software antivirus y software de verificación de integridad de archivos, cuando sea técnicamente posible, para prevenir, disuadir, detectar y mitigar la introducción, exposición y propagación de software malicioso hacia, dentro y desde el ICS.
- Aplicar técnicas de seguridad como cifrado y / o hashes criptográficos al almacenamiento de datos y comunicaciones de ICS cuando se considere apropiado.
- Implemente rápidamente los parches de seguridad después de probar todos los parches en condiciones de campo en un sistema de prueba, si es posible, antes de la instalación en el ICS.

- Seguimiento y seguimiento de pistas de auditoría en áreas críticas del ICS.
- Emplee protocolos y servicios de red confiables y seguros cuando sea posible.

Al diseñar soluciones de seguridad para dispositivos ICS, los profesionales de seguridad deben incluir las siguientes consideraciones: requisitos de puntualidad y rendimiento, requisitos de disponibilidad, requisitos de gestión de riesgos, efectos físicos, operación del sistema, limitaciones de recursos, comunicaciones, gestión de cambios, soporte gestionado, vida útil de los componentes y componentes. localización.

Las implementaciones de ICS utilizan una variedad de protocolos y servicios, que incluyen

- **Modbus :** un protocolo maestro / esclavo que usa el puerto 50
- **BACnet2 :** un protocolo maestro / esclavo que usa el puerto 47808
- **LonWorks / LonTalk3 :** un protocolo de igual a igual que utiliza el puerto 1679
- **DNP3 :** un protocolo maestro / esclavo que usa el puerto 19999 cuando se usa Transport Layer Security (TLS) y el puerto 20000 cuando no se usa TLS

También pueden utilizar IEEE 802.1X, Zigbee y Bluetooth para comunicarse.

El proceso básico para desarrollar un programa de seguridad ICS incluye lo siguiente:

1. Desarrolle un caso comercial para la seguridad.
2. Construya y entrene un equipo multifuncional.
3. Definir estatuto y alcance.
4. Definir políticas y procedimientos específicos de ICS.
5. Implementar un marco de gestión de riesgos de seguridad de ICS.
    1. Definir e inventariar los activos de ICS.
    2. Desarrollar un plan de seguridad para los sistemas ICS.
    3. Realice una evaluación de riesgos.
    4. Definir los controles de mitigación.
6. Brindar capacitación y sensibilizar sobre la seguridad al personal de ICS.

La arquitectura de seguridad del ICS debe incluir segregación y segregación de red, protección de límites, firewalls, una red de control separada lógicamente y tarjetas de interfaz de red dual (NIC) y debe centrarse principalmente en un aislamiento adecuado entre las redes de control y las redes corporativas.

Los profesionales de la seguridad también deben comprender que muchos sistemas ISC / SCADA utilizan una autenticación débil y sistemas operativos obsoletos. La incapacidad de parchear estos sistemas (e incluso la falta de parches disponibles) significa que el proveedor generalmente no está abordando proactivamente ningún problema de seguridad identificado.

Finalmente, muchos de estos sistemas permiten el acceso remoto no autorizado, lo que facilita que un atacante pueda violar el sistema con poco esfuerzo.

Sistemas basados en la nube

La computación en la nube es la centralización de datos en un entorno web al que se puede acceder desde cualquier lugar en cualquier momento. Una organización puede crear un entorno de nube (nube privada) o puede pagarle a un proveedor para que brinde este servicio (nube pública). Si bien este arreglo ofrece muchos beneficios, el uso de una nube pública presenta todo tipo de problemas de seguridad. ¿Cómo sabe que sus datos se mantienen separados de otros clientes? ¿Cómo sabe que sus datos están seguros? A muchas organizaciones les incomoda subcontratar la seguridad de sus datos.

La computación en la nube está de moda en estos días y se presenta en muchas formas. La idea básica de la computación en la nube es hacer que los recursos estén disponibles en un centro de datos basado en la web para que se pueda acceder a los recursos desde cualquier lugar. Cuando una empresa paga a otraempresa para alojar y gestionar este entorno, lo llamamos una solución de nube pública. Cuando las empresas alojan este entorno por sí mismas, lo llamamos una solución de nube privada.

Existe una compensación cuando se debe tomar una decisión entre las dos arquitecturas. La solución privada proporciona el mayor control sobre la seguridad de sus datos, pero también requiere el personal y el conocimiento para implementar, administrar y asegurar la solución. Una nube pública pone la seguridad de sus datos en manos de un tercero, pero esa parte suele ser más capaz y conocedora de la protección de los datos en este entorno y la gestión del entorno de la nube.

El almacenamiento en la nube ubica los datos en un servidor central, pero la diferencia clave es que se puede acceder a los datos desde cualquier lugar y, en muchos casos, desde una variedad de tipos de dispositivos.

Además, las soluciones en la nube suelen ofrecer tolerancia a fallos.

NIST SP 800-145 brinda definiciones para implementaciones en la nube que los profesionales de TI deben comprender. Los profesionales de la seguridad deben estar familiarizados con cuatro implementaciones en la nube:

- **Nube privada :** esta es una solución que pertenece y es administrada por una empresa exclusivamente para el uso de esa empresa. Esto proporciona el mayor control y seguridad, pero también requiere la mayor inversión tanto en hardware como en experiencia.

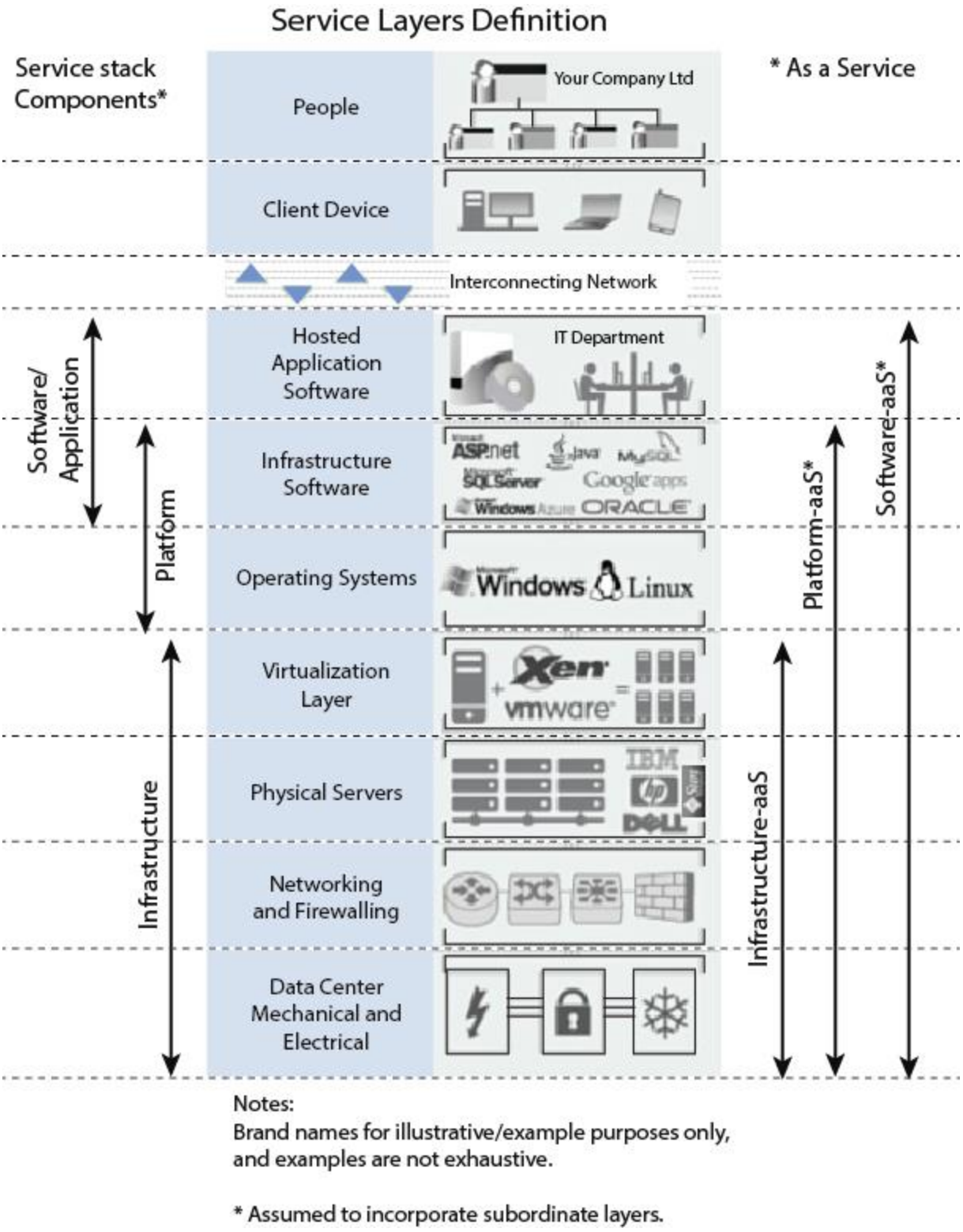
- **Nube pública :** esta es una solución proporcionada por un tercero. Descarga los detalles a ese tercero, pero cede cierto control y puede presentar problemas de seguridad. Por lo general, usted es un inquilino que comparte espacio con otros y, en muchos casos, no sabe dónde se guardan físicamente sus datos.
- **Nube híbrida : se** trata de una combinación de público y privado. Por ejemplo, quizás solo use las instalaciones del proveedor pero aún así administre los datos usted mismo.
- **Nube comunitaria :** esta es una solución que pertenece y es administrada por un grupo de organizaciones que crean la nube con un propósito común, tal vez para abordar una preocupación común, como el cumplimiento de la regularidad.

Cuando se selecciona una solución pública, se pueden adquirir varios niveles de servicio.

Algunos de estos niveles incluyen

- **Infraestructura como servicio (IaaS) :** involucra al proveedor que proporciona la plataforma de hardware o el centro de datos y a la empresa que instala y administra sus propios sistemas operativos y sistemas de aplicaciones. El proveedor simplemente proporciona acceso al centro de datos y mantiene ese acceso.
- **Plataforma como servicio (PaaS) :** involucra al proveedor que proporciona la plataforma de hardware o el centro de datos y el software que se ejecuta en la plataforma. Estoincluye los sistemas operativos y el software de infraestructura. La empresa todavía está involucrada en la gestión del sistema.
- **Software como servicio (SaaS) :** involucra al proveedor que proporciona la solución completa. Esto incluye el sistema operativo, el software de infraestructura y la aplicación. Podría proporcionarle un sistema de correo electrónico, por ejemplo, mediante el cual el proveedor aloja y gestiona todo por usted.

La figura 3-6 muestra las relaciones de estos servicios entre sí.



La relación entre varios servicios cae en los componentes de la pila de servicios y como un servicio de abajo hacia arriba. Los centros de datos mecánicos y eléctricos, redes y cortafuegos, servidores físicos y la capa de virtualización constituyen la infraestructura en los componentes de

la pila de servicios y la infraestructura, a a S en la categoría "como servicio". Los sistemas operativos y el software de infraestructura constituyen la plataforma en los componentes de la pila de servicios. La sección "como servicio", los sistemas operativos y el software de infraestructura se agregan a la infraestructura -a a S para hacer una plataforma-a a S. A esto se agrega el componente de software de aplicación alojada para hacer software-a a S en la categoría como servicio . Por otro lado, el software de infraestructura y el software de aplicaciones alojadas constituyen en conjunto software o aplicación en la categoría de componentes de la pila de servicios. La red de interconexión conecta esta parte al dispositivo del cliente y finalmente a las personas, la capa superior en las capas de servicio. Notas: Los nombres de marca solo tienen fines ilustrativos / de ejemplo, y los ejemplos no son exhaustivos. Se supone que incorpora capas subordinadas.

Figura 3-6 Computación en la nube

NIST SP 800-144 brinda pautas sobre seguridad y privacidad en la computación en nube pública. Esta publicación define dos tipos de contratos de servicios de computación en la nube: acuerdos predefinidos no negociables y acuerdos negociados. Los acuerdos no negociables son, en muchos sentidos, la base de las economías de escala de las que disfruta la computación en la nube pública. Los términos de servicio los prescribe completamente el proveedor de la nube. Por lo general, no se redactan prestando atención a los requisitos federales de privacidad y seguridad. Además, con algunas ofertas, el proveedor puede realizar modificaciones a los términos de servicio unilateralmente (por ejemplo, publicando una versión actualizada en línea) sin dar ninguna notificación directa al consumidor de la nube.

Los acuerdos de servicios negociados se parecen más a los contratos tradicionales de subcontratación de servicios de tecnología de la información. A menudo se utilizan para abordar las preocupaciones de una organización sobre la política de seguridad y privacidad, los procedimientos y los controles técnicos, como la investigación de antecedentes de los empleados, la propiedad de los datos y los derechos de salida, la notificación de violaciones, el aislamiento de las aplicaciones de inquilinos, el cifrado y la segregación de datos, el seguimiento y la generación de informes la eficacia del servicio, el cumplimiento de las leyes y normativas y el uso de productos validados que cumplan con los estándares nacionales o internacionales.

Los datos y aplicaciones críticos pueden requerir que una agencia lleve a cabo un acuerdo de servicio negociado. Debido a que los puntos de negociación pueden afectar negativamente el acuerdo de servicio, un acuerdo de servicio negociado normalmente es menos rentable. El resultado de una negociación también depende del tamaño de la organización y la influencia que puede ejercer. Independientemente del tipo de contrato de servicio, se recomienda obtener el asesoramiento legal y técnico adecuado para garantizar que los términos del servicio satisfagan adecuadamente las necesidades de la organización.

Las áreas potenciales de mejora en las que las organizaciones pueden obtener beneficios de seguridad y privacidad de la transición a un entorno de computación en la nube pública incluyen las siguientes:

- Especialización del personal

- Fuerza de la plataforma
- Disponibilidad de recursos
- Copia de seguridad y recuperación
- Puntos finales móviles
- Concentración de datos

Algunas de las preocupaciones más fundamentales al realizar la transición a una nube pública son las siguientes:

- Complejidad del sistema
- Entorno compartido de múltiples inquilinos
- Orientado a Internet
- Pérdida de control

La Tabla 3-4 proporciona una lista de problemas de seguridad y privacidad y recomendaciones para implementaciones de nube pública desde NIST SP 800-144.

Tabla 3-4 NIST SP 800-144 Problemas y recomendaciones de seguridad y privacidad en la nube

Áreas	Recomendaciones
Gobernancia	Ampliar las prácticas organizativas relacionadas con las políticas, los procedimientos y los estándares utilizados para el desarrollo de aplicaciones y el suministro de servicios en la nube, así como el diseño, la implementación, las pruebas, el uso y la supervisión de los servicios implementados o comprometidos. Poner en marcha mecanismos y herramientas de auditoría para garantizar que se sigan las prácticas organizativas durante todo el ciclo de vida del sistema.
Cumplimiento	Comprender los diversos tipos de leyes y regulaciones que imponen obligaciones de seguridad y privacidad en la organización y que potencialmente impactan las iniciativas de computación en la nube, particularmente aquellas que involucran ubicación de datos, controles de privacidad y seguridad, administración de registros y requisitos de descubrimiento electrónico. Revise y evalúe las ofertas del proveedor de la nube con respecto a los requisitos organizativos que deben cumplirse y asegúrese de que los términos del contrato cumplan adecuadamente con los requisitos. Asegúrese de que las capacidades y los procesos de descubrimiento electrónico del proveedor de la nube no comprometan la privacidad o la seguridad de los datos y las aplicaciones.

Áreas	Recomendaciones
Confianza	Asegúrese de que los acuerdos de servicio tengan los medios suficientes para permitir la visibilidad de los controles y procesos de seguridad y privacidad empleados por el proveedor de la nube, y su desempeño a lo largo del tiempo. Establezca derechos de propiedad claros y exclusivos sobre los datos. Instituya un programa de gestión de riesgos que sea lo suficientemente flexible para adaptarse al panorama de riesgos en constante evolución y cambio para el ciclo de vida del sistema. Supervise continuamente el estado de seguridad del sistema de información para respaldar las decisiones de gestión de riesgos en curso.
Arquitectura	Comprender las tecnologías subyacentes que utiliza el proveedor de la nube para brindar servicios, incluidas las implicaciones que los controles técnicos involucrados tienen en la seguridad y privacidad del sistema, durante todo el ciclo de vida del sistema y en todos los componentes del sistema.
Gestión de identidades y accesos	Asegúrese de que se hayan implementado las salvaguardas adecuadas para asegurar la autenticación, autorización y otras funciones de administración de identidad y acceso, y que sean adecuadas para la organización.
Aislamiento de software	Comprenda la virtualización y otras técnicas de aislamiento lógico que el proveedor de la nube emplea en su arquitectura de software de múltiples inquilinos y evalúe los riesgos involucrados para la organización.
Protección de Datos	Evaluar la idoneidad de las soluciones de gestión de datos del proveedor de la nube para los datos de la organización en cuestión y la capacidad de controlar el acceso a los datos, proteger los datos mientras están en reposo, en tránsito y en uso, y desinfectar los datos. Tenga en cuenta el riesgo de cotejar los datos de la organización con los de otras organizaciones cuyos perfiles de amenazas son altos o cuyos datos representan colectivamente un valor concentrado significativo. Comprender y sopesar completamente los riesgos involucrados en la gestión de claves criptográficas con las instalaciones disponibles en el entorno de la nube y los procesos establecidos por el proveedor de la nube.
Disponibilidad	Comprenda las disposiciones y los procedimientos del contrato para la disponibilidad, la copia de seguridad y la recuperación de datos y la recuperación ante desastres, y asegúrese de que cumplan con los requisitos de planificación de contingencia y continuidad de la organización. Asegúrese de que durante una interrupción intermedia o prolongada o un desastre grave, las operaciones críticas puedan reanudarse de inmediato y que todas las operaciones puedan eventualmente reiniciarse de manera oportuna y organizada.

Áreas	Recomendaciones
	Comprender las disposiciones y los procedimientos del contrato para la respuesta a incidentes y asegurarse de que cumplan con los requisitos de la organización.
Respuesta al incidente	Asegúrese de que el proveedor de la nube cuente con un proceso de respuesta transparente y mecanismos suficientes para compartir información durante y después de un incidente.
	Asegúrese de que la organización pueda responder a los incidentes de manera coordinada con el proveedor de la nube de acuerdo con sus respectivos roles y responsabilidades para el entorno informático.

Otra publicación del NIST, NIST SP 800-146, ofrece una sinopsis y recomendaciones de computación en la nube.

NIST SP 800-146 enumera los siguientes beneficios de las implementaciones de SaaS:

- Huella de herramienta de software muy modesta
- Uso eficiente de licencias de software
- Gestión y datos centralizados
- Responsabilidades de la plataforma gestionadas por proveedores
- Ahorro en costos iniciales

NIST SP 800-146 enumera los siguientes problemas y preocupaciones de las implementaciones de SaaS:

- Riesgos basados en el navegador y corrección de riesgos
- Dependencia de la red
- Falta de portabilidad entre nubes SaaS
- Aislamiento frente a eficiencia (compensaciones entre seguridad y costo)

NIST SP 800-146 ofrece un único beneficio de las implementaciones de PaaS:

- Desarrollo e implementación de aplicaciones escalables facilitado

Los problemas y preocupaciones de las implementaciones de PaaS son los siguientes:

- Falta de portabilidad entre nubes PaaS
- Programación del procesador basada en eventos
- Ingeniería de seguridad de aplicaciones PaaS

NIST SP 800-146 enumera los siguientes beneficios de las implementaciones de IaaS:

- Control total de los recursos informáticos a través del acceso administrativo a las máquinas virtuales.
- Alquiler flexible y eficiente de hardware informático
- Portabilidad, interoperabilidad con aplicaciones heredadas

Los problemas y preocupaciones de las implementaciones de IaaS son los siguientes:

- Compatibilidad con vulnerabilidades de seguridad heredadas
- Expansión de la máquina virtual
- Verificación de la autenticidad de un sitio web de proveedor de nube IaaS
- Robustez del aislamiento a nivel de VM
- Funciones para la configuración de red dinámica para proporcionar aislamiento
- Prácticas de borrado de datos

Sistemas de datos paralelos a gran escala

La mayoría de los sistemas de datos paralelos a gran escala se han diseñado para manejar problemas científicos e industriales, como el control del tráfico aéreo, la defensa contra misiles balísticos, el análisis de imágenes obtenidas por satélite, la guía de misiles y la predicción meteorológica. Requieren una enorme potencia de procesamiento. Debido a que los datos de estos sistemas se analizan con tanta rapidez, a menudo es difícil detectar y prevenir un intento de intrusión. EstasLos tipos de sistemas deben encontrar una manera de dividir las consultas en varios nodos paralelos para que las consultas se puedan procesar en paralelo.

Debido a que estos sistemas de datos paralelos a menudo abarcan varias organizaciones, los profesionales de la seguridad deben considerar las áreas de confianza, privacidad y seguridad general cada vez que sus organizaciones operan dentro de sistemas de datos paralelos a gran escala. Los problemas relacionados con la confianza, como los siguientes, deben tenerse en cuenta en las redes de confianza:

- Verificación de claves
- Mitigación de ataques de denegación de servicio (DoS) basada en la confianza
- Detección de fugas de datos

Los problemas relacionados con la privacidad que deben tenerse en cuenta incluyen los siguientes:

- Autenticación remota
- Control de acceso descentralizado
- Enmascaramiento de tráfico
- Criptografía de conjuntos de datos a gran escala

Otros problemas generales de seguridad que deben tenerse en cuenta incluyen credenciales de usuario inconsistentes y problemas de autorización e intercambio de datos relacionados con el uso de la criptografía.

Sistemas distribuidos

Los sistemas distribuidos se analizan anteriormente en la sección " Plataformas informáticas ".

Computación en cuadrícula

La computación en cuadrícula es el proceso de aprovechar la potencia de la CPU de varias máquinas físicas para realizar un trabajo. En algunos casos, es posible que se permita a los sistemas individuales salir y volver a unirse a la red. Aunque la ventaja de la potencia de procesamiento adicional es grande, debe preocuparse por la seguridad de los datos que podrían estar presentes en las máquinas que entran y salen de la red. Por lo tanto, la computación en red no es una implementación segura cuando el secreto de los datos es un tema clave.

Computación entre pares

Cualquier solución cliente / servidor en la que cualquier plataforma pueda actuar como cliente o servidor, o ambos, se denomina informática de igual a igual. Un ejemplo ampliamente utilizado de esto es la mensajería instantánea (IM). Estas implementaciones presentan problemas de seguridad que no se presentan en una disposición estándar de cliente / servidor. En muchos casos, estos sistemas operan fuera del control normal de los administradores de red.

Esto puede presentar problemas como los siguientes:

- Los virus, gusanos y caballos de Troya se pueden enviar a través de este punto de entrada a la red.
- En muchos casos, la falta de autenticación sólida permite la suplantación de cuentas.
- Los ataques de desbordamiento de búfer y los ataques que utilizan paquetes con formato incorrecto a veces pueden tener éxito.

Si estos sistemas deben tolerarse en el medio ambiente, se deben seguir las siguientes pautas:

- Las políticas de seguridad deben abordar el uso adecuado de estas aplicaciones.
- Todos los sistemas deben tener instalados un firewall y productos antivirus.
- Configure cortafuegos para bloquear el tráfico de mensajería instantánea no deseado.
- Si es posible, permita solo productos que proporcionen cifrado.

Internet de las Cosas

El Internet de las cosas (IoT) se refiere a un sistema de dispositivos informáticos, máquinas mecánicas y digitales y objetos interrelacionados que cuentan con identificadores únicos y la capacidad de transferir datos a través de una red sin requerir de persona a persona o de persona a persona. interacción con la computadora. El IoT ha presentado a los atacantes un nuevo medio a través del cual llevar a cabo un ataque. A menudo, los desarrolladores de los dispositivos de IoT agregan la funcionalidad de IoT sin considerar a fondo las implicaciones de seguridad de dicha funcionalidad o sin incorporar ningún control de seguridad para proteger los dispositivos de IoT.

Nota

IoT es un término para todos los objetos físicos, o "cosas", que ahora están integrados con electrónica, software y conectividad de red. Gracias a IoT, estos objetos, incluidos automóviles, electrodomésticos de cocina y controladores de calefacción y aire acondicionado, pueden recopilar e intercambiar datos. Desafortunadamente, los ingenieros otorgan a la mayoría de estos objetos esta capacidad solo por conveniencia y sin ninguna consideración real de los impactos de seguridad. Cuando estos objetos se implementan, los consumidores tampoco piensan en la seguridad. El resultado es comodidad para el consumidor, pero también riesgo. A medida que IoT evoluciona, los profesionales de la seguridad deben participar cada vez más en la evolución de IoT para ayudar a garantizar que los controles de seguridad estén diseñados para proteger estos objetos y los datos que recopilan y transmiten.

Ejemplos de IoT

Las implementaciones de IoT incluyen una amplia variedad de dispositivos, pero se clasifican en cinco grupos:

- **Hogar inteligente:** incluye productos que se utilizan en el hogar. Van desde dispositivos de asistencia personal, como Alexa de Amazon, hasta componentes de HVAC, como el termostato Nest. Los objetivos de estos dispositivos son la automatización y la gestión del hogar.

- **Wearables:** incluye productos que usan los usuarios. Van desde relojes, como el Apple Watch, hasta dispositivos de fitness personales, como el Fitbit.
- **Ciudades inteligentes:** incluye dispositivos que ayudan a resolver los problemas de congestión del tráfico y a reducir el ruido, la delincuencia y la contaminación. Incluyen energía inteligente, transporte inteligente, datos inteligentes, infraestructura inteligente y movilidad inteligente.
- **Automóviles conectados:** incluye vehículos que incluyen acceso a Internet y capacidades para compartir datos. Incluyen dispositivos GPS, OnStar y automóviles conectados a AT&T.
- **Automatización empresarial:** incluye dispositivos que automatizan la climatización, la iluminación, el control de acceso y la detección de incendios para las organizaciones.

Métodos para proteger los dispositivos de IoT

Los profesionales de la seguridad deben comprender los diferentes métodos para proteger los dispositivos de IoT. Las siguientes son algunas recomendaciones:

- Asegure y centralice los registros de acceso de los dispositivos de IoT.
- Utilice protocolos encriptados para asegurar la comunicación.
- Cree políticas de contraseñas seguras.
- Implemente políticas de comunicaciones de red restrictivas y configure LAN virtuales.
- Actualice periódicamente el firmware del dispositivo según las recomendaciones de los proveedores.

Al seleccionar dispositivos de IoT, particularmente aquellos que se implementan a nivel organizacional, los profesionales de seguridad deben considerar lo siguiente:

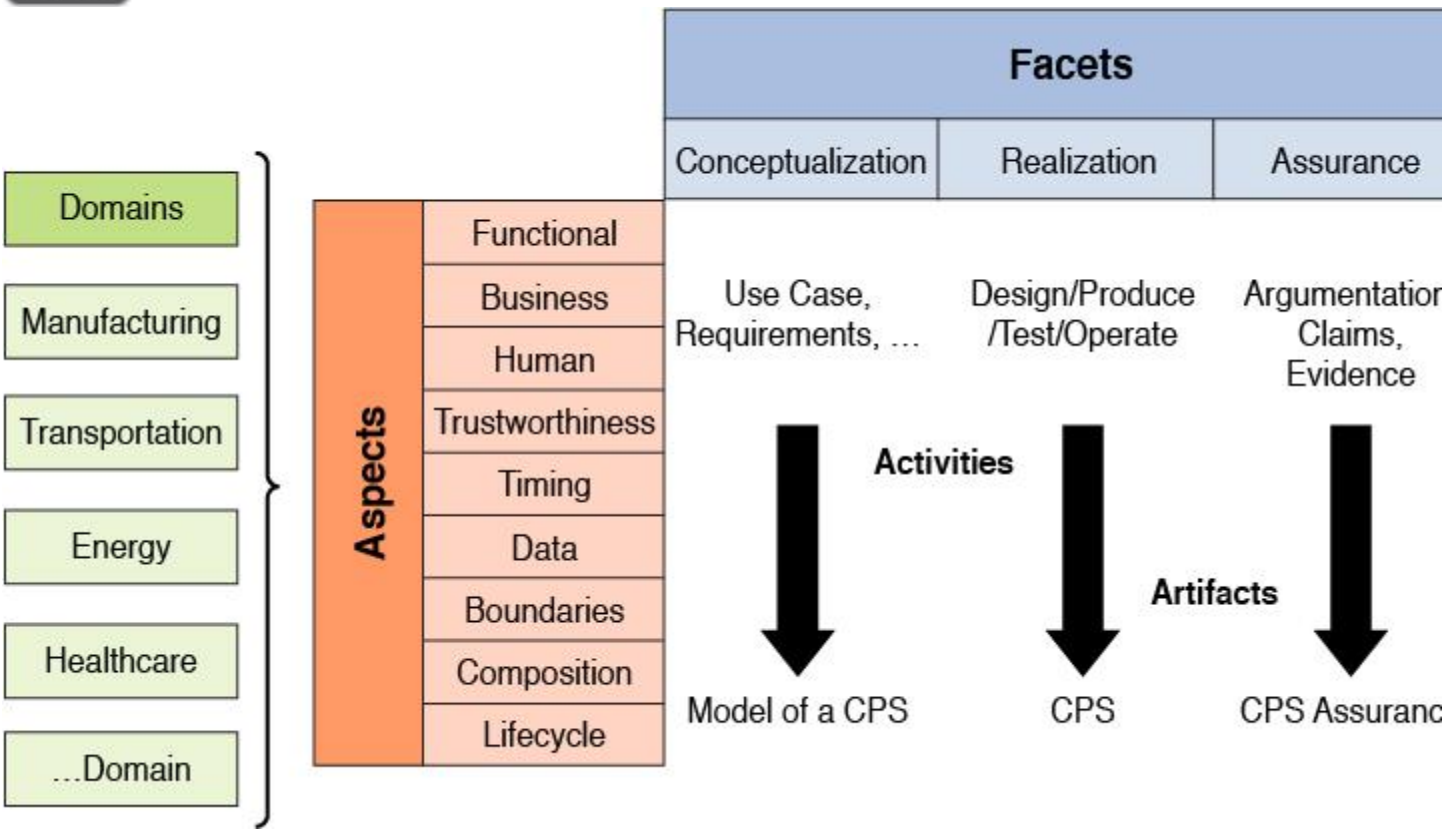
- ¿El proveedor diseña explícitamente para la privacidad y la seguridad?
- ¿Tiene el proveedor un programa de recompensas por errores y un sistema de informes de vulnerabilidades?
- ¿El dispositivo tiene anulaciones manuales o funciones especiales para operaciones desconectadas?

Marco NIST para sistemas ciberfísicos

Los sistemas ciberfísicos (CPS) son sistemas inteligentes que incluyen redes interactivas diseñadas de componentes físicos y computacionales. Estos sistemas altamente interconectados e integrados proporcionan nuevas funcionalidades para mejorar la calidad de vida y permitir avances tecnológicos en áreas críticas, como atención médica personalizada, respuesta a emergencias, gestión del flujo de tráfico, fabricación inteligente, defensa y seguridad nacional, y suministro y uso de energía. Además de CPS, hay muchas palabras y frases (Internet industrial, IoT, máquina a máquina [M2M], ciudades inteligentes y otras) que describen sistemas y conceptos similares o relacionados. Existe una superposición significativa entre estos conceptos, en particular CPS e IoT, de modo que CPS e IoT a veces se usan indistintamente; por lo tanto,

El marco de CPS incluye dominios, aspectos y facetas, como se muestra en la Figura 3-7 .

Key Topic



El marco CPS consta principalmente de dominios, aspectos y facetas. El dominio incluye Manufactura, Transporte, Energía, Salud y otros dominios que colectivamente apuntan a aspectos. Los aspectos que se muestran a la derecha incluyen Funcional, Comercial, Humano, Confiabilidad, Tiempo, Datos, Límites, Composición y Ciclo de vida. Las facetas que se muestran en la parte superior incluyen la conceptualización, la realización y la seguridad. Entre los aspectos y las facetas, una flecha hacia abajo del caso de uso, los requisitos apunta al modelo de un CP S. La flecha hacia abajo del diseño / producir / probar / operar apunta a CPS. La flecha hacia abajo de la argumentación, afirmaciones, evidencia apunta a CPS Assurance. Las actividades y los artefactos están etiquetados entre las tres flechas hacia abajo.

Figura 3-7 Marco NIST CPS (Imagen cortesía de NIST)

Los dominios representan las diferentes áreas de aplicación de CPS e incluyen todas las enumeradas en la Tabla 3-5 . Se espera que esta lista se amplíe a medida que se lancen nuevos dispositivos CPS e IoT.

Tabla 3-5 Dominios de CPS

Dominios	
Publicidad	Entretenimiento / deportes

Dominios	
Aeroespacial	Monitoreo ambiental
Agricultura	Servicios financieros
Edificios	Cuidado de la salud
Ciudades	Infraestructura (comunicaciones, energía, agua)
Comunidades	Ocio
Consumidor	Fabricación
Defensa	Ciencias
Resiliencia ante desastres	Redes sociales
Educación	Cadena de suministro / minorista
Respuesta de emergencia	Transporte
Energía	Tiempo

La Tabla 3-6 describe las tres facetas de CPS.

Tabla 3-6 Facetas de CPS

Faceta	Descripción
Conceptualización	Qué deben ser y qué se supone que deben hacer las cosas: el conjunto de actividades que producen un modelo de CPS (incluye descomposición funcional, requisitos y modelos lógicos).
Realización	Cómo se deben hacer y operar las cosas: el conjunto de actividades que producen, implementan y operan un CPS (incluye compensaciones de ingeniería y diseños detallados en la ruta crítica para la creación de una instancia de CPS).
Garantía	Cómo lograr el nivel deseado de confianza en que las cosas funcionarán como deberían: el conjunto de actividades que brindan la confianza de que un CPS se desempeña según lo especificado (incluye afirmaciones, evidencia y argumentación).

La tabla 3-7 enumera los diferentes aspectos del marco de CPS.

Tabla 3-7 Aspectos del marco de la CPS

Aspecto	Descripción
Funcional	Preocupaciones sobre la función, incluida la detección, la actuación, el control, las comunicaciones, la fisicalidad, etc.
Negocio	Preocupaciones sobre la empresa, el tiempo de comercialización, el medio ambiente, la regulación, el costo, etc.
Humano	Preocupaciones sobre la interacción humana con y como parte de un CPS.
Integridad	Preocupaciones sobre la confiabilidad de CPS, incluida la seguridad, la privacidad, la seguridad, la confiabilidad y la resistencia.

Aspecto	Descripción
Momento	Preocupaciones sobre el tiempo y la frecuencia en CPS, incluida la generación y transporte de señales de tiempo y frecuencia, sellado de tiempo, gestión de latencia, componibilidad de tiempos, etc.
Datos	Preocupaciones sobre la interoperabilidad de los datos, incluida la fusión, los metadatos, el tipo, la identidad, etc.
Límites	Preocupaciones relacionadas con las demarcaciones de interacciones topológicas, funcionales, organizativas u otras formas de interacción.
Composición	Inquietudes relacionadas con la capacidad de calcular propiedades seleccionadas de un ensamblaje de componentes a partir de las propiedades de sus componentes. La composicionalidad requiere componentes que sean componibles: no cambian sus propiedades en un ensamblaje. La componibilidad de tiempos es particularmente difícil.
Ciclo vital	Preocupaciones sobre el ciclo de vida de CPS, incluidos sus componentes.

Para obtener más información sobre el marco CPS y otras iniciativas de IoT del NIST, vaya a https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot .

Vulnerabilidades en sistemas basados en web

A pesar de todos los esfuerzos para diseñar una arquitectura web segura, los ataques a un sistema basado en la web aún ocurren y aún tienen éxito. En esta sección, examinamos algunos de los tipos más comunes de ataques, incluidos los ganchos de mantenimiento, los ataques de tiempo de verificación / tiempo de uso y los ataques basados en la web. También exploraremos las vulnerabilidades de XML y SAML y OWASP, un recurso dedicado a la defensa contra ataques basados en la web.

Ganchos de mantenimiento

Desde la perspectiva del desarrollo de software, un gancho de mantenimiento es un conjunto de instrucciones integradas en el código que le permite a alguien que conoce la llamada puerta trasera usar las instrucciones para conectarse para ver y editar el código sin usar los controles de acceso normales. En muchos casos, los ganchos de mantenimiento se colocan allí para facilitar que el proveedor brinde soporte al cliente. En otros casos, se colocan allí para ayudar a probar y rastrear las actividades del producto y nunca se eliminan más tarde.

Nota

Una cuenta de mantenimiento a menudo se confunde con un gancho de mantenimiento. Una cuenta de mantenimiento es una cuenta de puerta trasera creada por programadores para otorgar permisos completos a alguien en una aplicación o sistema operativo en particular. Una cuenta de mantenimientoPor lo general, se puede eliminar o deshabilitar fácilmente, pero un verdadero gancho de mantenimiento suele ser una parte oculta de la programación y mucho más difícil de deshabilitar. Ambos pueden causar problemas de seguridad porque muchos atacantes prueban primero los enlaces de mantenimiento documentados y las cuentas de mantenimiento. Le

sorprendería la cantidad de equipos atacados a diario porque estos dos problemas de seguridad no se tratan.

Independientemente de cómo los ganchos de mantenimiento ingresaron al código, pueden presentar un problema de seguridad importante si los piratas informáticos los conocen y pueden usarlos para acceder al sistema. Las contramedidas por parte del cliente para mitigar el peligro son

- Utilice un IDS basado en host para registrar cualquier intento de acceder al sistema mediante uno de estos ganchos.
- Cifre toda la información confidencial contenida en el sistema.
- Implementar auditorías para complementar el IDS.

La mejor solución es que el proveedor elimine todos los ganchos de mantenimiento antes de que el producto entre en producción. Se deben realizar revisiones codificadas para identificar y eliminar estos ganchos.

Ataques de tiempo de verificación / tiempo de uso

Los ataques de tiempo de verificación / tiempo de uso intentan aprovechar la secuencia de eventos que ocurren cuando el sistema completa tareas comunes. Se basa en el conocimiento de las dependencias presentes cuando ocurre una serie específica de eventos en sistemas de multiprocesamiento. Al intentar insertarse entre los eventos e introducir cambios, el pirata informático puede obtener el control del resultado.

Un término que se usa a menudo como sinónimo de un ataque de tiempo de verificación / tiempo de uso es *condición de carrera* , que en realidad es un ataque diferente. En este ataque, el hacker se inserta entre instrucciones, introduce cambios y altera el orden de ejecución de las instrucciones, alterando así el resultado.

Las contramedidas a estos ataques son hacer que los conjuntos críticos de instrucciones sean atómicos. Esto significa que se ejecutan en orden y en su totalidad o que los cambios que realizan se revierten o se evitan. También es mejor que el sistema bloquee el acceso a ciertos elementos que usará o tocará al llevar a cabo este conjunto de instrucciones.

Ataques basados en web

Los ataques a las infraestructuras de seguridad de la información han seguido evolucionando de manera constante a lo largo del tiempo, y los últimos ataques utilizan ataques basados en aplicaciones web mucho más sofisticados. Estos ataques han demostrado ser más difíciles de defender con los tradicionales.enfoques que utilizan cortafuegos perimetrales. Todos los ataques a aplicaciones web operan mediante la realización de al menos una solicitud normal o una solicitud modificada para aprovechar la validación de entrada inadecuada y los parámetros o la suplantación de instrucciones.

XML

El lenguaje de marcado extensible (XML) es el lenguaje web más utilizado en la actualidad y ha sido objeto de algunas críticas. El método que se utiliza actualmente para firmar datos para verificar su autenticidad ha sido descrito como inadecuado por algunos, y las otras críticas se han dirigido a la arquitectura de seguridad XML en general. En la siguiente sección, se analiza una extensión de este lenguaje que intenta abordar algunas de estas preocupaciones.

SAML

Security Assertion Markup Language (SAML) es un formato de datos estándar abierto basado en XML para intercambiar datos de autenticación y autorización entre partes, en particular, entre un proveedor de identidad y un proveedor de servicios. SAML permite al usuario tener una identidad portátil para la autenticación y autorización en Internet. El problema principal en el que se centra se denomina problema de inicio de sesión único (SSO) del navegador web.

SSO es la capacidad de autenticarse una vez para acceder a múltiples conjuntos de datos. El SSO a nivel de Internet generalmente se logra con cookies, pero extender el concepto más allá de Internet ha dado como resultado muchos enfoques de propiedad que no son interoperables. El objetivo de SAML es crear un estándar para este proceso.

OWASP

El Proyecto de seguridad de aplicaciones web abiertas (OWASP) es un proyecto de seguridad de aplicaciones de código abierto. Este grupo crea pautas, procedimientos de prueba y herramientas para ayudar con la seguridad web. También son conocidos por mantener una lista de los diez principales riesgos de seguridad de las aplicaciones web. Se puede obtener información sobre OWASP en https://www.owasp.org .

Vulnerabilidades en sistemas móviles

Hoy casi todo el mundo tiene un dispositivo móvil. A medida que los dispositivos móviles se han vuelto más populares, los problemas de seguridad relacionados con esos dispositivos han aumentado. Los profesionales de la seguridad enfrentan desafíos únicos debido al uso cada vez mayor de dispositivos móviles combinado con el hecho de que muchos de estos dispositivos se conectan mediante redes públicas con poca o ninguna seguridad.

Educar a los usuarios sobre los riesgos relacionados con los dispositivos móviles y asegurarse de que implementen las medidas de seguridad adecuadas puede ayudar a proteger contra las amenazas relacionadas con estos dispositivos. Algunas de las pautas que deben proporcionarse a los usuarios de dispositivos móviles incluyen la implementación de un PIN de bloqueo del dispositivo, el uso de cifrado del dispositivo, la implementación de servicios de ubicación GPS y la implementación de borrado remoto. Además, se debe advertir a los usuarios sobre la descarga de aplicaciones sin asegurarse de que provienen de una fuente confiable. En los últimos años, los sistemas de administración de dispositivos móviles (MDM) y de administración de aplicaciones móviles (MAM) se han vuelto populares en las empresas. Estos sistemas se implementan para garantizar que una organización pueda controlar la configuración de los dispositivos móviles, las aplicaciones y otros parámetros cuando esos dispositivos están conectados a la empresa.

Las amenazas que presenta la introducción de dispositivos móviles personales (teléfonos inteligentes y tabletas) a la red de una organización incluyen

- Navegación web insegura
- Conectividad Wi-Fi insegura
- Dispositivos perdidos o robados que contienen datos de la empresa
- Descargas e instalaciones de aplicaciones dañadas
- Faltan parches de seguridad
- Actualización constante de dispositivos personales
- Uso de servicios de ubicación

Si bien los tipos más comunes de información corporativa almacenada en dispositivos personales son los correos electrónicos corporativos y la información de contacto de la empresa, es alarmante observar que casi la mitad de estos dispositivos también contienen datos de clientes, credenciales de inicio de sesión de red y datos corporativos a los que se accede a través de aplicaciones comerciales.

Los principales problemas relacionados con los sistemas móviles son la seguridad de los dispositivos, la seguridad de las aplicaciones y las preocupaciones de los dispositivos móviles. Además, cubriremos NIST SP 800-164, que proporciona pautas para dispositivos móviles.

Seguridad del dispositivo

La seguridad del dispositivo implica la seguridad física del dispositivo móvil. En el caso de que un dispositivo se pierda o sea robado, los usuarios también necesitan la capacidad de rastrear y bloquear el dispositivo de forma remota. Algunas de las recomendaciones para la seguridad del dispositivo incluyen

- Bloquear su teléfono con una contraseña o detección de huellas dactilares
- Cifrar sus datos
- Configurar el borrado remoto
- Hacer una copia de seguridad de los datos del teléfono
- Evitar hacer jailbreak a tu iPhone o rootear tu Android
- Actualizar el sistema operativo con frecuencia
- Estar al tanto de las estafas de ingeniería social
- Usar Wi-Fi público con cuidado

Seguridad de la aplicación

Si bien la seguridad de los dispositivos es importante para los dispositivos móviles, la seguridad de las aplicaciones es igualmente importante. Los usuarios solo deben descargar aplicaciones aprobadas de las tiendas de aplicaciones de los proveedores. Algunas de las recomendaciones para la seguridad de las aplicaciones incluyen

- Evitar aplicaciones de terceros
- Estar al tanto de las estafas de ingeniería social

- Descargando anti-malware para su dispositivo móvil

Inquietudes sobre dispositivos móviles

Para abordar estos problemas y satisfacer la creciente demanda de traer y usar dispositivos personales, muchas organizaciones están creando políticas de traer su propio dispositivo (BYOD). Al respaldar una iniciativa BYOD, un profesional de seguridad debe considerar que los usuarios descuidados son una amenaza mayor que los piratas informáticos. Los usuarios no solo son menos diligentes en el mantenimiento de actualizaciones de seguridad y parches en los dispositivos, sino que compran nuevos dispositivos tan a menudo como se cambian de ropa. Estos factores dificultan el control de la seguridad de las redes en las que estos dispositivos pueden operar.

Otras iniciativas en la actualidad incluyen implementaciones de propiedad de la empresa, solo para empresas (COBO), propiedad de la empresa, habilitadas personalmente (COPE) y elija su propio dispositivo (CYOD). Independientemente de la implementación que utilice una organización, los profesionales de seguridad deben asegurarse de que se comprendan los riesgos de cada modelo y de que se implementen las políticas adecuadas para proteger los datos y los activos de la empresa. Los profesionales de seguridad son responsables de garantizar que la administración comprenda estos riesgos e implemente las herramientas adecuadas para controlar el acceso a la empresa.

Las herramientas de administración de dispositivos móviles centralizadas son una solución de rápido crecimiento. Algunas de estas herramientas aprovechan las capacidades de administración del servidor de mensajería y otras son herramientas de terceros que pueden administrar múltiples marcas de dispositivos. Systems Manager de Cisco es un ejemplo que se integra con los servicios en la nube de Cisco Meraki. Otro ejemplo de dispositivos iOS es el Configurador de Apple. Uno de los desafíos con la implementación de un sistema de este tipo es que no todos los dispositivos personales pueden admitir el cifrado nativo y / o el proceso de administración.

Por lo general, las herramientas de administración de dispositivos móviles centralizadas manejan los dispositivos móviles personales y los emitidos por la empresa de manera diferente. Para los dispositivos emitidos por la organización, una aplicación cliente generalmente administra la configuración y la seguridad de todo el dispositivo. Si el dispositivo es un dispositivo personal permitido a través de una iniciativa BYOD, la aplicación generalmente administra la configuración y la seguridad de sí misma y solo de sus datos. La aplicación y sus datos se guardan en un espacio aislado de las otras aplicaciones y datos. El resultado es que los datos de la organización y los datos del usuario están protegidos en caso de robo del dispositivo.

Independientemente de si se utiliza una herramienta de administración de dispositivos móviles centralizada, una política BYOD debe incluir lo siguiente en la política de seguridad de la organización:

- Identificar los usos permitidos de dispositivos personales en la red corporativa.

- Cree una lista de aplicaciones permitidas en los dispositivos y diseñe un método para evitar la instalación de aplicaciones que no están en la lista (por ejemplo, políticas de restricción de software).
- Asegúrese de que los altos niveles de gestión estén a bordo y brinden apoyo.
- Capacite a los usuarios en las nuevas políticas.

En el proceso de implementación y soporte de una solución móvil, siga estas pautas:

- Asegúrese de que la solución seleccionada admita la aplicación de controles de seguridad de forma remota.
- Asegúrese de que el proveedor seleccionado tenga un buen historial de publicidad y corrección de fallas de seguridad.
- Haga de la implementación de una herramienta MDM una prioridad absoluta.
- En ausencia de un sistema MDM, diseñe un proceso para garantizar que todos los dispositivos se mantengan actualizados con los parches de seguridad.
- Actualice la política a medida que cambien la tecnología y los comportamientos.
- Exija a todos los empleados que acepten permitir la limpieza remota de cualquier dispositivo robado o perdido.
- Prohibir estrictamente que los dispositivos rooteados (Android) o con jailbreak (iOS) accedan a la red.
- Si es posible, elija un producto que admita:
    - Cifrar la unidad de estado sólido (SSD) y la RAM no volátil
    - Requerir un PIN para acceder al dispositivo
    - Bloquear el dispositivo cuando se intenta una cantidad específica de PIN incorrectos

Como ocurre con muchos de los otros problemas de seguridad que se tratan en este libro, la educación del usuario es clave. Un profesional de la seguridad debe asegurarse de que los usuarios comprendan la importancia de la seguridad de los dispositivos móviles.

Si una organización no implementa una solución MDM o MAM, la política de seguridad del dispositivo móvil debe incluir, como mínimo, las siguientes políticas:

- Implemente software anti-malware / antivirus en todos los dispositivos móviles.
- Utilice solo comunicaciones seguras.
- Utilice una autenticación sólida.
- Solicite un PIN o algún otro mecanismo de inicio de sesión con cada uso del dispositivo después de un cierto período de inactividad (no más de 10 minutos de inactividad).
- Limite el software de terceros.
- Implementar GPS y otros servicios de ubicación.
- Habilite las funciones de bloqueo remoto y borrado remoto.
- Nunca deje el dispositivo desatendido.
- Informe de inmediato cualquier dispositivo perdido o robado.
- Desactive todas las opciones, aplicaciones y servicios innecesarios, incluido Bluetooth.
- Realice copias de seguridad de los datos con regularidad.
- Instale todas las actualizaciones del fabricante del dispositivo.

NIST SP 800-164

NIST SP 800-164 es un borrador de publicación especial que brinda pautas sobre la seguridad con raíz de hardware en dispositivos móviles. Define tres componentes de seguridad necesarios para los dispositivos móviles: Roots of Trust (RoTs), una interfaz de programación de aplicaciones (API) para exponer los RoTs a la plataforma y un Policy Enforcement Engine (PEnE).

Las raíces de la confianza son la base de la garantía de la confiabilidad de un dispositivo móvil. Los RoT siempre deben comportarse de la manera esperada porque no se puede detectar su mal comportamiento. Los RoT de hardware se prefieren sobre los RoT de software debido a su inmutabilidad, superficies de ataque más pequeñas y comportamiento más confiable. Pueden proporcionar un mayor grado de seguridad de que se puede confiar en ellos para realizar su función o funciones de confianza. Los RoT de software podrían proporcionar el beneficio de una implementación rápida en diferentes plataformas. Para respaldar la integridad, el aislamiento y el almacenamiento protegido del dispositivo, los dispositivos deben implementar los siguientes RoT:

- Raíz de confianza para el almacenamiento (RTS)
- Raíz de confianza para la verificación (RTV)
- Raíz de confianza para la integridad (RTI)
- Raíz de confianza para la presentación de informes (RTR)
- Raíz de confianza para la medición (RTM)

Los RoT deben ser expuestos por el sistema operativo a las aplicaciones a través de una API abierta. Esto proporcionará a los desarrolladores de aplicaciones un conjunto de servicios y capacidades de seguridad que pueden utilizar para asegurar sus aplicaciones y proteger los datos que procesan. Al proporcionar una capa abstracta de servicios y capacidades de seguridad, estas API pueden reducir la carga de los desarrolladores de aplicaciones para implementar características de seguridad de bajo nivel y, en su lugar, permitirles reutilizar componentes confiables proporcionados en los RoT y el sistema operativo. Las API deben estandarizarse dentro de una plataforma móvil determinada y, en la medida de lo posible, entre plataformas. Las aplicaciones pueden utilizar las API y los RoT asociados para solicitar informes de integridad del dispositivo, proteger los datos a través de los servicios de cifrado proporcionados por el RTS y almacenar y recuperar credenciales de autenticación y otros datos confidenciales.

El PEnE aplica políticas en el dispositivo con la ayuda de otros componentes del dispositivo y permite el procesamiento, mantenimiento y administración de políticas tanto en el dispositivo como en los entornos de los propietarios de la información. El PEnE proporciona a los propietarios de la información la capacidad de expresar el control que necesitan sobre su información. Es necesario confiar en el PEnE para implementar correctamente los requisitos del propietario de la información y para evitar que los requisitos de un propietario de la información afecten negativamente a los de otro. Para realizar funciones clave, el PEnE debe poder consultar la configuración y el estado del dispositivo.

Los dispositivos móviles deben implementar las siguientes tres capacidades de seguridad móvil para abordar los desafíos con la seguridad de los dispositivos móviles:

- **Integridad del dispositivo: la integridad del** dispositivo es la ausencia de corrupción en el hardware, firmware y software de un dispositivo. Un dispositivo móvil puede proporcionar evidencia de que ha mantenido la integridad del dispositivo si se puede demostrar que sus configuraciones de software, firmware y hardware se encuentran en un estado en el que confía una parte que confía.
- **Aislamiento: el** aislamiento evita la interacción no deseada entre aplicaciones y contextos de información en el mismo dispositivo.
- **Almacenamiento protegido: el almacenamiento** protegido preserva la confidencialidad e integridad de los datos en el dispositivo mientras está en reposo, mientras está en uso (en el caso de que una aplicación no autorizada intente acceder a un elemento en el almacenamiento protegido) y tras la revocación del acceso.

Vulnerabilidades en dispositivos integrados

Un sistema integrado es un sistema informático con una función dedicada dentro de un sistema más grande, a menudo con limitaciones de computación en tiempo real. Está integrado como parte del dispositivo, y a menudo incluye hardware y piezas mecánicas. Los sistemas integrados controlan muchos dispositivos de uso común en la actualidad e incluyen sistemas integrados en automóviles, sistemas HVAC, alarmas de seguridad e incluso sistemas de iluminación. La comunicación de máquina a máquina (M2M), el Internet de las cosas (IoT) y los sistemas industriales controlados de forma remota han aumentado la cantidad de dispositivos conectados y, al mismo tiempo, han convertido estos dispositivos en objetivos.

Debido a que los sistemas integrados generalmente se colocan dentro de otro dispositivo sin la intervención de un profesional de seguridad, la seguridad ni siquiera está integrada en el dispositivo. Entonces, si bien permitir que el dispositivo se comunique a través de Internet con un sistema de diagnóstico brinda un gran servicio al consumidor, a menudo el fabricante no ha considerado que un pirata informático pueda revertir la comunicación y hacerse cargo del dispositivo con el sistema integrado. Al momento de escribir este artículo, han surgido informes de personas que pueden tomar el control de los vehículos utilizando sus sistemas integrados. Los fabricantes han lanzado parches que abordan estos problemas, pero no todos los propietarios de vehículos los han aplicado o incluso conocen los parches.

A medida que M2M e IoT aumentan en popularidad, los profesionales de la seguridad pueden esperar ver un aumento en incidentes como este. Se espera que un profesional de seguridad comprenda las vulnerabilidades que presentan estos sistemas y cómo implementar controles para reducir el riesgo de una organización.

Criptografía

Si bien la arquitectura y la ingeniería de seguridad implican proteger todos los dispositivos que implementa una organización, no basta con proteger los dispositivos. Las organizaciones también deben proteger los datos, ya que residen en los dispositivos y se transmiten a través de la

red. La criptografía implica el uso de algoritmos para proteger los datos. Esta sección analiza los conceptos de criptografía, la historia de la criptografía, las características del criptosistema, las matemáticas criptográficas y el ciclo de vida criptográfico.

Conceptos de criptografía

Un profesional de la seguridad debe comprender muchos términos y conceptos relacionados con la criptografía.

Estos términos se utilizan a menudo cuando se habla de criptografía:

- **Cifrado :** el proceso de convertir datos de texto sin formato a texto cifrado. También conocido como cifrado.
- **Descifrado :** el proceso de convertir datos de texto cifrado a texto sin formato. También conocido como descifrar.
- **Clave :** parámetro que controla la transformación de texto plano en texto cifrado o viceversa. Es imposible determinar los datos originales en texto plano sin la clave. Las claves pueden ser tanto públicas como privadas. También se denomina criptovariable.
- **Sincrónico:** cuando el cifrado o descifrado se produce de forma inmediata.
- **Asincrónico:** cuando las solicitudes de cifrado o descifrado se procesan desde una cola. Este método utiliza hardware y varios procesadores en el proceso.
- **Simétrico:** método de cifrado mediante el cual una única clave privada cifra y descifra los datos. También se conoce como cifrado de clave privada o secreta.
- **Asimétrico:** método de cifrado mediante el cual un par de claves, una clave privada y una pública, realiza el cifrado y el descifrado. Una clave realiza el cifrado, mientras que la otra clave realiza el descifrado. También conocido como cifrado de clave pública.
- **Firma digital :** método para proporcionar autenticación de remitente e integridad de mensajes. El mensaje actúa como una entrada para una función hash y la clave privada del remitente cifra el valor hash. El receptor puede realizar un cálculo hash sobre el mensaje recibido para determinar la validez del mensaje.
- **Hash :** función unidireccional que reduce un mensaje a un valor hash. Una comparación del valor hash del remitente con el valor hash del receptor determina la integridad del mensaje. Si los valores hash resultantes son diferentes, entonces el mensaje se ha alterado de alguna manera, siempre que tanto el remitente como el receptor usen la misma función hash.
- **Certificado digital :** documento electrónico que identifica al titular del certificado.
- **Texto sin formato :** un mensaje en su formato original. También conocido como texto sin cifrar.
- **Texto cifrado :** una forma alterada de un mensaje que es ilegible sin conocer la clave y el sistema de cifrado utilizado. También conocido como criptograma.
- **Criptosistema :** todo el proceso criptográfico, incluidas las funciones de algoritmo, clave y administración de claves. La seguridad de un criptosistema se mide por el tamaño del espacio de claves y la potencia computacional disponible.

- **Criptoanálisis :** la ciencia de descifrar texto cifrado sin conocimiento previo de la clave o el criptosistema utilizado. El propósito del criptoanálisis es falsificar señales o mensajes codificados que serán aceptados como señales o mensajes auténticos.
- **Agrupación de claves :** ocurre cuando diferentes claves de cifrado generan el mismo texto cifrado a partir del mismo mensaje de texto sin formato.
- **Espacio de claves :** todos los valores clave posibles cuando se utiliza un algoritmo particular u otra medida de seguridad. Una clave de 40 bits tendría 240 valores posibles, mientras que una clave de 128 bits tendría 2128 valores posibles.
- **Colisión :** evento que ocurre cuando una función hash produce el mismo valor hash en diferentes mensajes.
- **Algoritmo :** función matemática que cifra y descifra datos. También conocido como cifrado.
- **Criptología :** la ciencia que estudia la comunicación y los datos cifrados.
- **Codificación :** El proceso de cambiar datos a otra forma usando código.
- **Decodificación :** El proceso de cambiar un mensaje codificado a su formato original.
- **Transposición :** el proceso de mezclar o reordenar el texto sin formato para ocultar el mensaje original. También conocido como permutación. Por ejemplo, AEEGMSS es una versión transpuesta de MESSAGE.
- **Sustitución :** proceso de intercambio de un byte en un mensaje por otro. Por ejemplo, ABCCDEB es una versión sustituida de MESSAGE.
- **Confusión :** el proceso de cambiar el valor de una clave durante cada ronda de cifrado. La confusión a menudo se lleva a cabo por sustitución. La confusión oculta una conexión estadística entre el texto plano y el texto cifrado. Claude Shannon primero habló sobre la confusión.
- **Difusión :** El proceso de cambiar la ubicación del texto sin formato dentro del texto cifrado. La difusión se lleva a cabo a menudo mediante transposición. Claude Shannon introdujo por primera vez la difusión.
- **Efecto de avalancha :** la condición en la que cualquier cambio en la clave o el texto sin formato, sin importar cuán pequeño sea, cambiará significativamente el texto cifrado. Horst Feistel introdujo por primera vez el efecto de avalancha.
- **Factor de trabajo o función de trabajo :** la cantidad de tiempo y recursos que se necesitarían para romper el cifrado.
- **Trampilla :** Mecanismo secreto que permite la implementación de la función inversa en una función unidireccional.
- **Función unidireccional : función** matemática que se puede realizar más fácilmente en una dirección que en la otra.

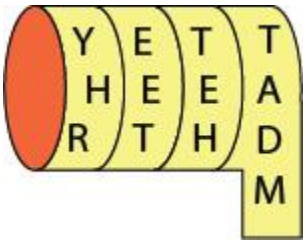
Historia de la criptografía

La criptografía tiene sus raíces en civilizaciones antiguas. Aunque las primeras soluciones de criptografía eran de naturaleza simplista, podían proporcionar a los líderes un medio para ocultar mensajes a los enemigos.

En sus formas más tempranas, la mayoría de los métodos criptográficos implementaron algún tipo de cifrado de sustitución, donde cada carácter del alfabeto fue reemplazado por otro. Un cifrado de sustitución mono-alfabético utiliza solo un alfabeto, y un cifrado de sustitución

polialfabético utiliza varios alfabetos. Al igual que con todos los demás métodos de criptografía, los primeros cifrados de sustitución tuvieron que ser reemplazados por métodos más complejos.

Los espartanos crearon el cifrado scytale, que usaba una hoja de papiro envuelta alrededor de una varilla de madera. El mensaje encriptado tuvo que ser envuelto alrededor de una barra del tamaño correcto para ser descifrado, como se muestra en la Figura 3-8 .



Una varilla de madera cilíndrica se envuelve con un papel que crea tres anillos con algunos alfabetos escritos sobre ellos. Los alfabetos que están escritos en el primer anillo (izquierda) dicen: (de arriba a abajo) Y, H y R; en el segundo anillo: E, E y T; en el tercer anillo: T, E y H. El último anillo dice: T, A, D y M.

Figura 3-8 Cifrado Scytale

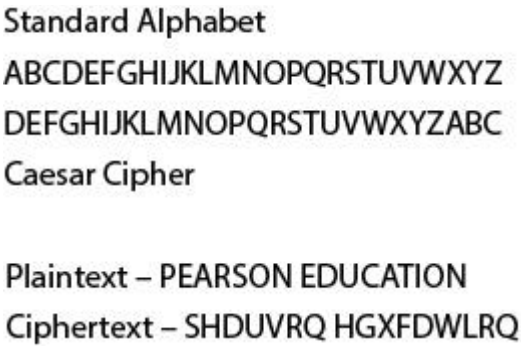
Otros avances notables en la historia de la criptografía incluyen los siguientes:

- Cifrado césar
- Cifrado de Vigenere
- Principio de Kerckhoff
- Enigma de la Segunda Guerra Mundial
- Lucifer por IBM

Julio César y el cifrado César

Julio César desarrolló un cifrado mono-alfabético que cambia las letras del alfabeto en tres lugares. Aunque esta técnica es muy simplista, las variaciones de la misma fueron muy fáciles de desarrollar porque la clave (el número de ubicaciones en las que se desplazó el alfabeto) se puede cambiar. Debido a que era tan simple, es fácil realizar ingeniería inversa y condujo al desarrollo de cifrados polialfabéticos.

En la Figura 3-9 se muestra un ejemplo de un mensaje cifrado con cifrado Caesar . En este ejemplo, las letras del alfabeto se aplican a un cambio de sustitución de tres letras, lo que significa que las letras se desplazaron en tres letras. Como puede ver, el alfabeto inglés estándar aparece en primer lugar. Debajo, se enumeran las letras de sustitución.



Los alfabetos estándar dicen: ABCDEFGHIJKLMNOPQRSTUVWXYZ y sus correspondientes alfabetos de cifrado Caesar dicen: DEFGHIJKLMNOPQRSTUVWXYZABC. Para el texto sin formato: PEARSON EDUCATION, el texto cifrado se proporciona como SHDUVRQ HGXFDWLRQ.

Figura 3-9 Cifrado César

Cifrado de Vigenere

En el siglo XVI, Blaise de Vigenere de Francia desarrolló uno de los primeros cifrados de sustitución polialfabéticos, hoy conocido como cifrado de Vigenere. Aunque se basa en el cifrado de César, el cifrado de Vigenere es considerablemente más complicado porque utiliza 27 alfabetos desplazados (consulte la tabla de Vigenere en la Figura 3-10). Para cifrar un mensaje, debe conocer la clave de seguridad y utilizarla junto con el mensaje de texto sin formato para determinar el texto cifrado.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	S	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Al salir de la primera celda, las columnas están etiquetadas de la A a la Z, cada alfabeto en la celda superior de una columna. De manera similar, dejando la primera fila que ahora está llena de alfabetos, la primera columna vertical se llena con los alfabetos de la A a la Z, y cada alfabeto ocupa la celda del extremo izquierdo de una fila. Los alfabetos se llenan en la tabla de la siguiente manera: la columna que comienza con A tiene los alfabetos de la A a la Z; la columna que comienza con B tiene los alfabetos B a Z y A; la columna que comienza con C tiene los alfabetos de C a Z seguidos de A y B; y así.

Figura 3-10 Tabla Vigenere

Como ejemplo de un mensaje en el que se aplica el cifrado de Vigenere, usemos la clave de seguridad PEARSON y el mensaje de texto sin formato de MEETING IN CONFERENCE ROOM. La primera letra del mensaje de texto sin formato es M, y la primera letra de la clave es P. Debemos ubicar la letra M en los encabezados de las columnas. Seguimos esa columna hacia abajo hasta que se cruza con la fila que comienza con la letra P, lo que da como resultado la letra B. La segunda letra del mensaje de texto sin formato es E, y la segunda letra de la clave es E. Usando el mismo método, usamos obtenemos la letra I. Continuamos de esta misma manera

hasta que nos quedemos sin letras clave, luego comenzamos de nuevo con la clave, lo que resultaría en la segunda letra I en el mensaje de texto plano trabajando con la letra P de la clave.

Entonces, al aplicar esta técnica a todo el mensaje, el mensaje de texto sin formato MEETING IN CONFERENCE ROOM se convierte en un mensaje de texto cifrado BIEKABT XR CFFTRGINTW FBDQ.

Principio de Kerckhoff

En el siglo XIX, Auguste Kerckhoff desarrolló seis principios de diseño para el uso militar de cifrados. Los seis principios son los siguientes:

- El sistema debe ser prácticamente, si no matemáticamente, indescifrable.
- No debe exigirse que sea secreto y debe poder caer en manos del enemigo sin inconvenientes.
- Su clave debe ser comunicable y retenible sin la ayuda de notas escritas, y debe ser cambiable o modificable a voluntad de los corresponsales.
- Debe ser aplicable a la correspondencia telegráfica.
- Debe ser portátil y su uso y función no deben requerir el concurso de varias personas.
- Finalmente, dadas las circunstancias que condicionan su aplicación, el sistema debe ser fácil de usar, no requiriendo esfuerzo mental ni el conocimiento de una larga serie de reglas para observar.

En el principio de Kerckhoff, recuerde que la clave es secreta y el algoritmo es conocido.

Enigma de la Segunda Guerra Mundial

Durante la Segunda Guerra Mundial, la mayoría de las principales potencias militares desarrollaron máquinas de cifrado. La más famosa de las máquinas utilizadas durante la guerra fue la máquina Enigma, desarrollada por Alemania. La máquina Enigma constaba de rotores y una placa de conexión.

Para convertir un mensaje de texto plano en texto cifrado, el operador de la máquina primero configuraría sus ajustes iniciales. Luego, el operador escribiría cada letra del mensaje de texto sin formato original en la máquina, una a la vez. La máquina mostraría una letra diferente para cada letra ingresada. Después de que el operador anotó la letra de texto cifrado, el operador haría avanzar los rotores a la nueva configuración. Entonces, con cada letra ingresada, el operador tenía que cambiar la configuración de la máquina. La clave de este proceso fue la configuración inicial de la máquina y la serie de incrementos utilizados para hacer avanzar el rotor, ambos debían ser conocidos por el receptor para convertir correctamente el texto cifrado de nuevo en texto plano.

Tan complicado como era el sistema, un grupo de criptógrafos polacos pudo descifrar el código, por lo que se le atribuye el acortamiento de la Segunda Guerra Mundial en dos años.

Lucifer por IBM

El proyecto Lucifer, desarrollado por IBM, desarrolló ecuaciones matemáticas complejas. Estas ecuaciones fueron utilizadas más tarde por la Agencia de Seguridad Nacional de EE. UU. En el desarrollo del Estándar de cifrado digital (DES) de EE. UU., Que todavía se usa en la actualidad de alguna forma. Lucifer usó un cifrado de Feistel, un cifrado de bloque iterado que cifra el texto plano dividiendo el bloque en dos mitades. Luego, el cifrado aplica una ronda de transformación a una de las mitades mediante una subclave. La salida de esta transformación se XORed con la otra mitad del bloque. Finalmente, las dos mitades se intercambian para completar la ronda.

Características del criptosistema

Un criptosistema consta de software, protocolos, algoritmos y claves. La fuerza de cualquier criptosistema proviene del algoritmo y la longitud y el secreto de la clave. Por ejemplo, un método para hacer que una clave criptográfica sea más resistente a ataques exhaustivos es aumentar la longitud de la clave. Si el criptosistema utiliza una clave débil, facilita los ataques contra el algoritmo.

Mientras que un criptosistema es compatible con los tres principios básicos de la tríada CIA, los criptosistemas proporcionan directamente autenticación, confidencialidad, integridad, autorización y no repudio. El principio de disponibilidad de la tríada CIA está respaldado por criptosistemas, lo que significa que la implementación de la criptografía ayudará a garantizar que los datos de una organización permanezcan disponibles. Sin embargo, la criptografía no garantiza directamente la disponibilidad de los datos, aunque puede usarse para proteger los datos.

Autenticación

Los criptosistemas proporcionan autenticación al poder determinar la identidad y validez del remitente. Las firmas digitales verifican la identidad del remitente. La protección de la clave garantiza que solo los usuarios válidos puedan cifrar y descifrar correctamente el mensaje.

Confidencialidad

Los criptosistemas brindan confidencialidad al alterar los datos originales de tal manera que se asegure que los datos no puedan ser leídos excepto por el destinatario válido. Sin la clave adecuada, los usuarios no autorizados no pueden leer el mensaje.

Integridad

Los criptosistemas brindan integridad al permitir que los destinatarios válidos verifiquen que los datos no han sido alterados. Las funciones hash no evitan la alteración de datos, pero proporcionan un medio para determinar si se ha producido una alteración de datos.

Autorización

Los criptosistemas proporcionan autorización al proporcionar la clave a un usuario válido después de que ese usuario demuestre su identidad a través de la autenticación. La clave dada al usuario le permitirá acceder a un recurso.

No repudio

El no repudio en los criptosistemas proporciona una prueba del origen de los datos, lo que evita que el remitente niegue que envió el mensaje y respalda la integridad de los datos. La criptografía de clave pública y las firmas digitales proporcionan no repudio.

NIST SP 800-175A y B

NIST SP 800-175A y B son dos publicaciones especiales que proporcionan pautas para el uso de estándares criptográficos en el gobierno federal. SP 800-175A enumera todas las directivas, mandatos y políticas que afectan la selección de estándares criptográficos para el gobierno federal, mientras que SP 800-175B analiza los estándares criptográficos que están disponibles y cómo deben usarse.

NIST SP 800-175A enumera las siguientes leyes que afectan a los estándares criptográficos:

- Ley Federal de Gestión de la Seguridad de la Información (FISMA)
- Ley de tecnología de la información sanitaria para la salud económica y clínica (HITECH)
- Ley Federal de Modernización de los Sistemas de Información de 2014
- Ley de mejora de la ciberseguridad de 2014

Las acciones ejecutivas y las circulares y memorandos de la Oficina de Administración y Presupuesto (OMB) que afectan los estándares de criptografía de los sistemas del gobierno de EE. UU. También se enumeran en NIST SP 800-175A. También proporciona las definiciones de las siguientes políticas:

- **Política de gestión de la información:** especifica qué información se recopilará o creará y cómo se gestionará.
- **Política de seguridad de la información:** respalda y hace cumplir partes de la política de gestión de la información de la organización al especificar con más detalle qué información se protegerá de las amenazas anticipadas y cómo se obtendrá esa protección.
- **Política de gestión de claves:** incluye descripciones de los objetivos y restricciones de autorización y protección que se aplican a la generación, distribución, contabilidad, almacenamiento, uso, recuperación y destrucción de material de codificación criptográfica y los servicios criptográficos que se proporcionarán.

Finalmente, NIST SP 800-175A enumera los pasos del Marco de gestión de riesgos de NIST SP 800-37 que afectan la selección de criptografía: categorización de información y sistemas de información y selección de controles de seguridad.

Nota

Las leyes y NIST SP 800-37 se tratan en el Capítulo 1 .

NIST SP 800-175B cubre los siguientes algoritmos criptográficos:

- Funciones hash criptográficas
- Algoritmos de clave simétrica
- Algoritmos de clave asimétrica

También analiza la fuerza de seguridad del algoritmo, la vida útil del algoritmo y la administración de claves.

Los profesionales de la seguridad que necesiten ayuda para seleccionar los algoritmos criptográficos adecuados deben consultar estos SP.

Matemáticas criptográficas

Todos los algoritmos criptográficos implican el uso de matemáticas. Los conceptos matemáticos fundamentales para la criptografía se analizan en las siguientes secciones.

Booleano

Las reglas utilizadas para los bits y bytes que forman una computadora están establecidas por matemáticas booleanas. En un sistema booleano, los valores de cada circuito son verdaderos y falsos, generalmente se indican con 1 y 0, respectivamente.

Operaciones lógicas (And, Or, Not, Exclusive Or)

Cuando se trata de matemáticas booleanas, se utilizan cuatro operadores lógicos básicos: Y, O, NO y O EXCLUSIVO. Los operadores AND, OR y EXCLUSIVE OR toman dos valores y generan un valor. El operador NOT toma un valor y genera un valor.

Una operación AND, también denominada conjunción, comprueba si dos valores son verdaderos. La Tabla 3-8 muestra el resultado de una operación AND.

Tabla 3-8 Resultados de la operación AND

Valor X	Valor Y	Y Resultado de la operación
0	0	0
0	1	0
1	0	0
1	1	1

Una operación OR, también conocida como disyunción, comprueba si al menos uno de los valores es verdadero. La Tabla 3-9 muestra el resultado de una operación OR.

Tabla 3-9 Resultados de la operación de quirófano

Valor X	Valor Y	O Resultado de la operación
0	0	0
0	1	1
1	0	1
1	1	1

Una operación NOT, también conocida como negación, invierte el valor de una variable. La Tabla 3-10 muestra el resultado de una operación NOT.

Tabla 3-10 Resultados de la operación NO

Valor X	NO Resultado de la operación
0	1
1	0

Una operación O EXCLUSIVA, también conocida como XOR, devuelve un valor verdadero cuando solo uno de los valores de entrada es verdadero. Si ambos valores son verdaderos o ambos valores son falsos, la salida siempre es falsa. La Tabla 3-11 muestra el resultado de una operación XOR.

Tabla 3-11 Resultados de la operación XOR

Valor X	Valor Y	Resultado de la operación XOR
0	0	0
0	1	1
1	0	1
1	1	0

Función de módulo

Utilizada en criptografía, una función de módulo es el valor que queda después de que se realiza una operación de división. Por ejemplo, 32 dividido por 8 tendría un valor sobrante de 0 porque 8 entra en 32 un número par de veces (4); 10 dividido por 3 tendría un valor sobrante de 1 porque 10 dividido por 3 es igual a 3 con un resto de 1.

Función unidireccional

Una función unidireccional produce valores de salida para cada combinación posible de entradas. Esto hace que sea imposible recuperar los valores de entrada de una función unidireccional. Los algoritmos de clave pública se basan en funciones unidireccionales. Las entradas utilizadas son números primos. Por ejemplo, suponga que una entrada contiene solo números primos con tres

dígitos. La salida o el resultado de esos tres números primos se puede determinar con una buena calculadora. Sin embargo, si alguien obtiene el resultado de 19,786,001, sería difícil determinar qué tres números primos de tres dígitos se usaron. (Por cierto, 101, 227 y 863 son los tres números primos utilizados).

Mientras tanto

Un nonce es un número aleatorio que se usa solo una vez y actúa como una variable de marcador de posición en funciones. Cuando la función se ejecuta realmente, el nonce se reemplaza con un número aleatorio generado en el momento del procesamiento. Un ejemplo común de nonce es un vector de inicialización (IV). Los IV son valores que se utilizan para crear un texto cifrado único cada vez que se cifra el mismo mensaje con la misma clave.

Conocimiento dividido

El conocimiento dividido es el término que se utiliza cuando la información o los privilegios se dividen entre varios usuarios o entidades, de modo que ningún usuario tiene suficientes privilegios para comprometer la seguridad. Un ejemplo de conocimiento dividido en criptografía es el depósito de claves. Concustodia de la clave, la clave está en manos de un tercero para garantizar que la clave pueda recuperarse si la parte emisora deja de existir o tiene un evento catastrófico.

Ciclo de vida criptográfico

Al considerar la implementación de técnicas de cifrado o criptografía en una organización, los profesionales de seguridad deben analizar completamente las necesidades de la organización. Cada técnica tiene fortalezas y debilidades. Además, cada uno tiene propósitos específicos. Analizar las necesidades de la organización asegurará que identifique el mejor algoritmo para implementar.

Las organizaciones profesionales administran algoritmos para garantizar que brinden la protección necesaria. Es esencial que los profesionales de seguridad investiguen los algoritmos que implementan y comprendan cualquier anuncio de la organización gobernante con respecto a actualizaciones, retiros o reemplazos de los algoritmos implementados. El ciclo de vida de cualquier algoritmo criptográfico implica implementación, mantenimiento y retiro o reemplazo. Cualquier profesional de seguridad que no obtenga información actualizada sobre los algoritmos implementados puede encontrar la reputación de la organización y su propia reputación personal dañada como resultado de su negligencia.

Gestión de claves

La gestión de claves en criptografía es esencial para garantizar que la criptografía proporcione confidencialidad, integridad y autenticación. Si una clave se ve comprometida, puede tener graves consecuencias en toda la organización.

La gestión de claves implica todo el proceso de garantizar que las claves estén protegidas durante la creación, distribución, transmisión y almacenamiento. Como parte de este proceso, las claves también deben destruirse correctamente. Cuando se considera la gran cantidad de redes a través de las cuales se transmite la clave y los diferentes tipos de sistemas en los que se almacena una clave, la enormidad de este problema realmente sale a la luz.

Como el aspecto más exigente y crítico de la criptografía, es importante que los profesionales de la seguridad comprendan los principios de administración de claves.

Las claves siempre deben almacenarse en texto cifrado cuando se almacenan en un dispositivo no criptográfico. La distribución, el almacenamiento y el mantenimiento de claves deben ser automáticos integrando los procesos en la aplicación.

Debido a que las claves se pueden perder, se deben realizar copias de seguridad y almacenarlas en un lugar seguro. Una persona designada debe tener el control de las copias de seguridad con otras personas designadas que sirven como copias de seguridad de emergencia. El proceso de recuperación de claves también debería requerir más de un operador para garantizar que solo se completen las solicitudes de recuperación de claves válidas. En algunos casos, las claves incluso se dividen en partes y se depositan en agentes de confianza, que proporcionan su parte de la clave a una autoridad central cuandoautorizado para hacerlo. Aunque se utilizan otros métodos de distribución de partes de una clave, todas las soluciones implican el uso de agentes fiduciarios a quienes se confía parte de la clave y una autoridad central encargada de ensamblar la clave a partir de sus partes. Además, el personal de recuperación de claves debe abarcar toda la organización y no solo ser miembros del departamento de TI.

Las organizaciones también deben limitar la cantidad de claves que se utilizan. Cuantas más claves tenga, más claves debe preocuparse y asegurarse de que estén protegidas. Aunque nunca se debe ignorar una razón válida para emitir una clave, limitar el número de claves emitidas y utilizadas reduce el daño potencial.

Al diseñar el proceso de administración de claves, debe considerar cómo hacer lo siguiente:

- Almacene y transmita las claves de forma segura.
- Utilice claves aleatorias.
- Emita claves de longitud suficiente para garantizar la protección.
- Destruya adecuadamente las llaves cuando ya no las necesite.
- Realice una copia de seguridad de las claves para asegurarse de que se puedan recuperar.

Selección de algoritmo

Al seleccionar un algoritmo, las organizaciones deben comprender los datos que deben protegerse y el entorno organizacional, incluidas las regulaciones y estándares que deben

cumplir. Las organizaciones deben responder las siguientes preguntas al seleccionar el algoritmo a utilizar:

- **¿Cuál es el plazo de la encriptación?** Utilice un cifrado que pueda sobrevivir a un ataque de fuerza bruta al menos el tiempo suficiente para que los datos ya no sean importantes para mantener en secreto.
- **¿Qué tipos de datos deben cifrarse?** Los datos en reposo, los datos en uso y los datos en movimiento necesitarán diferentes tipos de cifrado para su protección.
- **¿Qué restricciones del sistema existen?** Las consideraciones incluyen presupuesto, restricciones del sistema operativo, restricciones de infraestructura, etc.
- **¿Quién intercambiará los datos cifrados?** Los sistemas heredados pueden causar restricciones en el cifrado que se puede utilizar cuando se intercambian datos.

Tipos criptográficos

Los algoritmos que se utilizan en los sistemas informáticos implementan fórmulas matemáticas complejas al convertir texto plano en texto cifrado. Los dos componentes principales de cualquierEl sistema de cifrado son la clave y el algoritmo. En algunos sistemas de cifrado, las dos partes que se comunican utilizan la misma clave. En otros sistemas de cifrado, las dos partes que se comunican utilizan claves diferentes en el proceso, pero las claves están relacionadas.

En esta sección, discutimos lo siguiente:

- Ejecución de cifrados de clave y ocultación
- Cifrados de sustitución
- Cifrados de transposición
- Algoritmos simétricos
- Algoritmos asimétricos
- Cifrados híbridos

Ejecución de cifrados de clave y ocultación

La ejecución de cifrados de clave y cifrados de ocultación se considera métodos clásicos de producción de texto cifrado. El cifrado de clave en ejecución utiliza un componente físico, generalmente un libro, para proporcionar los caracteres polialfabéticos. Se debe incluir un bloque indicador en algún lugar del texto para que el receptor sepa en qué parte del libro comenzó el autor. Por lo tanto, las dos partes deben acordar qué libro usar y dónde se incluirá el bloque indicador en el mensaje cifrado. Los cifrados de clave en ejecución también se denominan cifrados de clave y cifrados en ejecución.

Un cifrado de ocultación, también conocido como cifrado nulo, se produce cuando se intercala texto sin formato en algún lugar dentro de otro material escrito. Las dos partes deben ponerse de acuerdo sobre el valor clave, que define qué letras forman parte del mensaje real. Por ejemplo, cada tercera letra o la primera letra de cada palabra es parte del mensaje real. Un cifrado de ocultación pertenece al ámbito de la esteganografía.

Nota

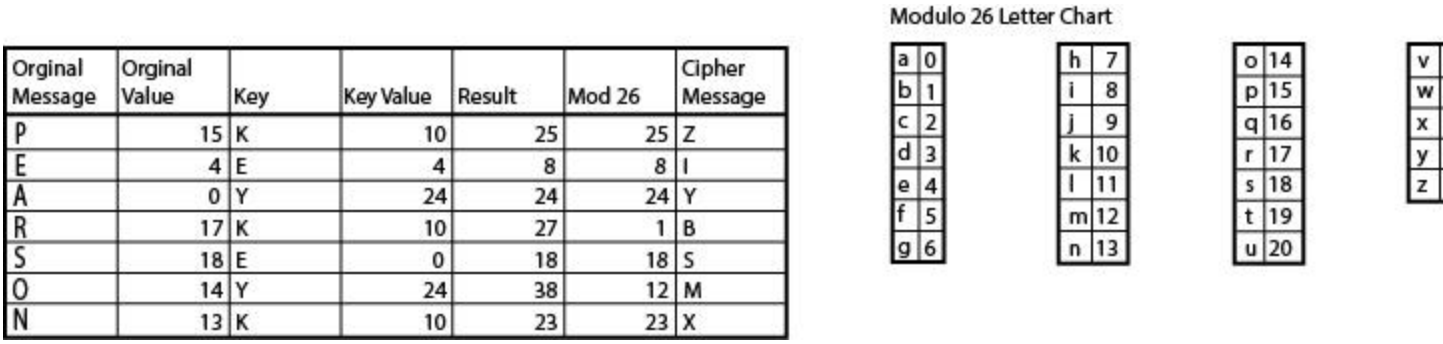
La esteganografía se analiza en la siguiente sección.

Cifrados de sustitución

Un cifrado de sustitución utiliza una clave para sustituir caracteres o bloques de caracteres con diferentes caracteres o bloques de caracteres. El cifrado César y el cifrado Vigenere son dos de las primeras formas de cifrado de sustitución.

Otro ejemplo de un cifrado de sustitución es un cifrado de sustitución módulo 26. Con este cifrado, las 26 letras del alfabeto se numeran en orden comenzando en cero. El remitente toma el mensaje original y determina el número de cada letra enel mensaje original. Luego, los valores de las letras para las claves se agregan a los valores de las letras originales. A continuación, el resultado del valor se vuelve a convertir en texto.

La Figura 3-11 muestra un ejemplo de un cifrado de cifrado de sustitución módulo 26. Con este ejemplo, el mensaje original es PEARSON y la clave es CLAVE. El mensaje de texto cifrado es ZIYBSMX.



Orginal Message	Orginal Value	Key	Key Value	Result	Mod 26	Cipher Message
P	15	K	10	25	25	Z
E	4	E	4	8	8	I
A	0	Y	24	24	24	Y
R	17	K	10	27	1	B
S	18	E	0	18	18	S
O	14	Y	24	38	12	M
N	13	K	10	23	23	X

La tabla de la izquierda se muestra con siete encabezados de columna que incluyen Mensaje original, Valor original, Clave, Valor clave, Resultado, Mod 26 y Mensaje cifrado. La primera fila dice: P, 15, K, 10, 25, 25 y Z. La segunda fila dice: E, 4, E, 4, 8, 8 e I. La tercera fila dice: A, 0, Y, 24 , 24, 24 e Y. La cuarta fila dice: R, 17, K, 10, 27, 24 y B. La quinta fila dice: S, 18, E, 0, 18, 18 y S. La sexta fila dice: O, 14, Y, 24, 38, 12 y M. La séptima fila dice: N, 13, K, 10, 23, 23 y X. El cuadro de letras del módulo 26 se muestra a la derecha con cuatro tablas. La primera tabla consta de dos columnas y siete filas como a = 0, b = 1, c = 2, d = 3, e = 4, f = 5 y g = 6. La segunda tabla consta de dos columnas y siete filas como h = 7, i = 8, j = 9, k = 10, l = 11, m = 12 y n = 13. La tercera tabla consta de dos columnas y siete filas como o = 14, p = 15, q = 16, r = 17, s = 18,

Figura 3-11 Ejemplo de cifrado de sustitución del módulo 26

Los cifrados de sustitución que se explican en esta sección incluyen lo siguiente:

- Almohadillas de un solo uso

- Esteganografía

Almohadillas de un solo uso

Un bloc de notas de un solo uso, inventado por Gilbert Vernam, es el esquema de cifrado más seguro que se puede utilizar. Si se usa correctamente, un atacante no puede romper una almohadilla de un solo uso. Un pad de una sola vez funciona como un cifrado en ejecución en el sentido de que el valor de la clave se agrega al valor de las letras. Sin embargo, un pad de una sola vez usa una clave que tiene la misma longitud que el mensaje de texto sin formato, mientras que el cifrado en ejecución usa una clave más pequeña que se aplica repetidamente al mensaje de texto sin formato.

La Figura 3-12 muestra un ejemplo de un cifrado de almohadilla de una sola vez. Con este ejemplo, el mensaje original es PEARSON y la clave es JOHNSON. El mensaje de texto cifrado es YSHEKCA.

Orginal Message	Orginal Value	Key	Key Value	Result	Mod 26	Cipher Message
P	15	J	9	24	24	Y
E	4	O	14	18	18	S
A	0	H	7	7	7	H
R	17	N	13	30	4	E
S	18	S	18	36	10	K
O	14	O	14	28	2	C
N	13	N	13	26	0	A

Modulo 26 Letter Chart

a	0
b	1
c	2
d	3
e	4
f	5
g	6

h	7
i	8
j	9
k	10
l	11
m	12
n	13

o	14
p	15
q	16
r	17
s	18
t	19
u	20

v
w
x
y
z

La tabla de la izquierda se muestra con siete encabezados de columna que incluyen Mensaje original, Valor original, Clave, Valor clave, Resultado, Mod 26 y Mensaje cifrado. La primera fila dice: P, 15, J, 9, 24, 24 e Y. La segunda fila dice: E, 4, O, 14, 18, 18 y S. La tercera fila dice: A, 0, H, 7 , 7, 7 y H. La cuarta fila dice: R, 17, N, 13, 30, 4 y E. La quinta fila dice: S, 18, S, 18, 36, 10 y K. La sexta fila dice: O , 14, O, 14, 28, 2 y C. La séptima fila dice: N, 13, N, 13, 26, 0 y A. El cuadro de letras del módulo 26 se muestra a la derecha con cuatro tablas. La primera tabla consta de dos columnas y siete filas como a = 0, b = 1, c = 2, d = 3, e = 4, f = 5 y g = 6. La segunda tabla consta de dos columnas y siete filas como h = 7, i = 8, j = 9, k = 10, l = 11, m = 12 y n = 13. La tercera tabla consta de dos columnas y siete filas como o = 14, p = 15, q = 16, r = 17, s = 18, t = 19,

Figura 3-12 Ejemplo de almohadilla de un solo uso

Para garantizar que la almohadilla de un solo uso sea segura, deben darse las siguientes condiciones:

- Debe usarse solo una vez
- Debe ser tan largo (o más largo que) el mensaje
- Debe constar de valores aleatorios
- Debe distribuirse de forma segura

- Debe estar protegido en su origen y destino.

Aunque el ejemplo anterior usa un pad de una sola vez en un esquema de módulo 26, los pads de una sola vez también se pueden usar a nivel de bit. Cuando se utiliza el nivel de bits, el mensaje se convierte en binario y se produce una operación XOR de dos bits a la vez. Los bits del mensaje original se combinan con los valores clave para obtener el mensaje cifrado. Cuando combina los valores, el resultado es 0 si ambos valores son iguales y 1 si ambos valores son diferentes. Un ejemplo de una operación XOR es el siguiente:

Mensaje original	0 1 1 0 1 1 0 0
Clave	1 1 0 1 1 1 0 0
Mensaje cifrado	1 0 1 1 0 0 0 0

Esteganografía

La esteganografía ocurre cuando un mensaje se oculta dentro de otro objeto, como una imagen o un documento. En la esteganografía, es crucial que solo aquellos que esperan el mensaje sepan que el mensaje existe.

Un cifrado de ocultación, discutido anteriormente, es un método de esteganografía. Otro método de esteganografía es la marca de agua digital. La marca de agua digital es un logotipo o marca comercial que está incrustado en documentos, imágenes u otros objetos. Las marcas de agua disuaden a las personas de utilizar los materiales de forma no autorizada.

Cifrados de transposición

Un cifrado de transposición codifica las letras del mensaje original en un orden diferente. La clave determina las posiciones a las que se mueven las letras.

La figura 3-13 muestra un ejemplo de un cifrado de transposición simple. Con este ejemplo, el mensaje original es PEARSON EDUCATION y la clave es 4231 2314. El mensaje de texto cifrado es REAP ONSE AUCD IOTN. Entonces, toma las primeras cuatro letras del mensaje de texto sin formato (PEAR) y usa los primeros cuatro números (4231) como clave para la transposición. En el nuevo texto cifrado, las letras serían REAP. Luego, toma las siguientes cuatro letras del mensaje de texto sin formato (SONE) y usa los siguientes cuatro números (2314) como clave para la transposición. En el nuevo texto cifrado, las letrassea ONSE. Luego, toma las siguientes cuatro letras del mensaje original y aplica los primeros cuatro números de la clave porque no tiene más números en la clave. Continúe con este patrón hasta completarlo.

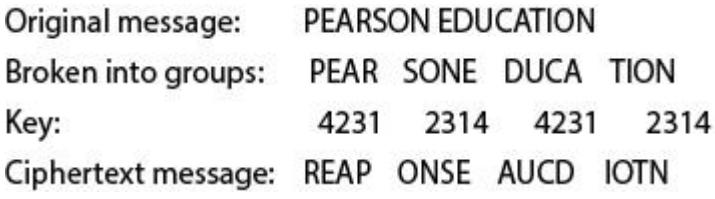


Figura 3-13 Ejemplo de transposición

Algoritmos simétricos

Los algoritmos simétricos utilizan una clave privada o secreta que debe permanecer secreta entre las dos partes. Cada pareja requiere una clave privada separada. Por lo tanto, un solo usuario necesitaría una clave secreta única para cada usuario con el que se comunica.

Considere un ejemplo donde hay 10 usuarios únicos. Cada usuario necesita una clave privada independiente para comunicarse con los demás usuarios. Para calcular la cantidad de claves que se necesitarían en este ejemplo, usaría la siguiente fórmula:

de usuarios × (# de usuarios - 1) / 2

Usando nuestro ejemplo, calcularía 10 × (10 - 1) / 2, o 45 claves necesarias.

Con algoritmos simétricos, la clave de cifrado debe permanecer segura. Para obtener la clave secreta, los usuarios deben encontrar un método seguro fuera de banda para comunicar la clave secreta, incluido el servicio de mensajería o el contacto físico directo entre los usuarios.

Un tipo especial de clave simétrica llamada clave de sesión cifra los mensajes entre dos usuarios durante una sesión de comunicación.

Los algoritmos simétricos pueden denominarse criptografía de clave única, clave secreta, clave privada o clave compartida.

Los sistemas simétricos brindan confidencialidad pero no autenticación o no repudio. Si ambos usuarios usan la misma clave, es imposible determinar dónde se originó el mensaje.

Los algoritmos simétricos incluyen DES, AES, IDEA, Skipjack, Blowfish, Twofish, RC4 / RC5 / RC6 / RC7 y CAST. Todos estos algoritmos se discutirán más adelante en este capítulo.

La tabla 3-12 enumera las fortalezas y debilidades de los algoritmos simétricos.

Tabla 3-12 Fortalezas y debilidades del algoritmo simétrico

Fortalezas	Debilidades
1.000 a 10.000 veces más rápido que los algoritmos asimétricos	La cantidad de claves únicas necesarias puede causar problemas de administración de claves
Dificil de romper	La distribución segura de claves es fundamental
Más barato de implementar que asimétrico	El compromiso clave ocurre si una de las partes está comprometida, lo que permite la suplantación

Los dos tipos generales de algoritmos simétricos son cifrados basados en flujo y cifrados en bloque. Los vectores de inicialización (IV) son una parte importante de los cifrados en bloque. Estos tres componentes se discutirán en las próximas secciones.

Cifrados basados en flujo

Los cifrados basados en flujo realizan el cifrado bit a bit y utilizan generadores de flujo de claves. Los generadores de flujo de claves crean un flujo de bits que se XORed con los bits de texto sin formato. El resultado de esta operación XOR es el texto cifrado.

Un cifrado de flujo síncrono depende solo de la clave, y un cifrado de flujo asíncrono depende de la clave y el texto sin formato. La clave garantiza que el flujo de bits que se aplica XOR al texto sin formato sea aleatorio.

Un ejemplo de cifrado basado en flujo es RC4, que se analiza más adelante en este capítulo.

Las ventajas de los cifrados basados en flujo incluyen las siguientes:

- Generalmente tienen una menor propagación de errores porque el cifrado se produce en cada bit.
- Generalmente se usa más en la implementación de hardware
- Utilice la misma clave para el cifrado y el descifrado
- Generalmente más barato de implementar que los cifrados en bloque
- Emplea solo confusión

Nota

La confusión se define en la sección " Conceptos de criptografía ", anteriormente en este capítulo. Recuerde consultar esa lista cada vez que encuentre términos en este capítulo con los que no esté familiarizado.

Cifrados de bloque

Los cifrados en bloque realizan el cifrado dividiendo el mensaje en unidades de longitud fija. Un mensaje de 1.024 bits se puede dividir en 16 bloques de 64 bits cada uno. Cada uno deesos 16 bloques son procesados por las fórmulas del algoritmo, lo que da como resultado un solo bloque de texto cifrado.

Los ejemplos de cifrados de bloque incluyen IDEA, Blowfish, RC5 y RC6, que se describen más adelante en este capítulo.

Las ventajas de los cifrados en bloque incluyen las siguientes:

- La implementación es más fácil que la implementación de cifrado basado en flujo.
- Generalmente menos susceptible a problemas de seguridad.
- Generalmente se usa más en implementaciones de software.

Los cifrados en bloque emplean tanto confusión como difusión. Los cifrados de bloque a menudo usan diferentes modos: ECB, CBC, CFB y CTR. Estos modos se describen en detalle más adelante en este capítulo.

Vectores de inicialización (IV)

Los modos mencionados anteriormente utilizan IV para garantizar que no se produzcan patrones durante el cifrado. Estos IV proporcionan este servicio mediante el uso de valores aleatorios con los algoritmos. Sin usar IV, una frase repetida dentro de un mensaje de texto sin formato podría resultar en el mismo texto cifrado. Los atacantes posiblemente pueden usar estos patrones para romper el cifrado.

Algoritmos asimétricos

Los algoritmos asimétricos utilizan tanto una clave pública como una clave privada o secreta. La clave pública es conocida por todas las partes y la clave privada solo la conoce su propietario. Una de estas claves cifra el mensaje y la otra descifra el mensaje.

En la criptografía asimétrica, determinar la clave privada de un usuario es prácticamente imposible incluso si se conoce la clave pública, aunque ambas claves están relacionadas matemáticamente. Sin embargo, si se descubre la clave privada de un usuario, el sistema puede verse comprometido.

Los algoritmos asimétricos pueden denominarse criptografía de clave doble o clave pública.

Los sistemas asimétricos brindan confidencialidad, integridad, autenticación y no repudio. Debido a que ambos usuarios tienen una clave única que es parte del proceso, es posible determinar dónde se originó el mensaje.

Si la confidencialidad es la principal preocupación de una organización, un mensaje debe cifrarse con la clave pública del receptor, que se conoce como formato de mensaje seguro. Si la autenticación es la principal preocupación de una organización, un mensaje debe cifrarse con la clave privada del remitente, que se conoce como formato de mensaje abierto. Cuando se usa el formato de mensaje abierto, cualquiera que tenga la clave pública puede descifrar el mensaje.

Los algoritmos asimétricos incluyen Diffie-Hellman, RSA, El Gamal, ECC, Knapsack, DSA y prueba de conocimiento cero. Todos estos algoritmos se discutirán más adelante en este capítulo.

La tabla 3-13 enumera las fortalezas y debilidades de los algoritmos asimétricos.

Tabla 3-13 Fortalezas y debilidades del algoritmo asimétrico

Fortalezas	Debilidades
La distribución de claves es más fácil y manejable que con algoritmos simétricos.	Más caro de implementar que los algoritmos simétricos.
La administración de claves es más fácil porque todas las partes utilizan la misma clave pública.	1.000 a 10.000 veces más lento que los algoritmos simétricos.

Cifrados híbridos

Debido a que los algoritmos simétricos y asimétricos tienen debilidades, se han desarrollado soluciones que utilizan ambos tipos de algoritmos en un cifrado híbrido. Al utilizar ambos tipos de algoritmos, el cifrado proporciona confidencialidad, autenticación y no repudio.

El proceso para el cifrado híbrido es el siguiente:

1. El algoritmo simétrico proporciona las claves utilizadas para el cifrado.
2. Las claves simétricas se pasan luego al algoritmo asimétrico, que cifra las claves simétricas y las distribuye automáticamente.
3. Luego, el mensaje se cifra con la clave simétrica.
4. Tanto el mensaje como la clave se envían al receptor.
5. El receptor descifra la clave simétrica y usa la clave simétrica para descifrar el mensaje.

Una organización debe utilizar el cifrado híbrido si las partes no tienen una clave secreta compartida y deben transmitirse grandes cantidades de datos confidenciales.

Algoritmos simétricos

Los algoritmos simétricos se explicaron anteriormente en este capítulo. En esta sección, discutimos algunos de los algoritmos simétricos más populares. Es posible que algunos de estos ya no se utilicen comúnmente porque existen alternativas más seguras.

Los profesionales de la seguridad deben estar familiarizados con los siguientes algoritmos simétricos:

- DES / 3DES
- AES

- OCURRENCIA
- Barrilete
- Pez globo
- Dos peces
- RC4 / RC5 / RC6 / RC7
- EMITIR

DES y 3DES

El Estándar de cifrado digital (DES) es un sistema de cifrado simétrico creado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) pero basado en el algoritmo Lucifer de 128 bits de IBM. Originalmente, el algoritmo se denominó Algoritmo de cifrado de datos (DEA) y se utilizó el acrónimo DES para referirse al estándar. Pero en el mundo actual, DES es el término más común para ambos.

DES utiliza una clave de 64 bits, de los cuales 8 bits se utilizan para la paridad. Por lo tanto, la longitud de clave efectiva para DES es de 56 bits. DES divide el mensaje en bloques de 64 bits. Se realizan dieciséis rondas de transposición y sustitución en cada bloque, lo que da como resultado un bloque de texto cifrado de 64 bits.

DES ha sido reemplazado principalmente por 3DES y AES (que se analiza en la siguiente sección).

DES-X es una variante de DES que utiliza varias claves de 64 bits además de la clave DES de 56 bits. La primera clave de 64 bits se aplica mediante XOR al texto sin formato, que luego se cifra con DES. La segunda clave de 64 bits se aplica mediante XOR al cifrado resultante.

Double-DES, una versión DES que usaba una longitud de clave de 112 bits, ya no se usa. Después de su lanzamiento, se produjo un ataque de seguridad que redujo la seguridad de Double-DES al mismo nivel que DES.

Modos DES

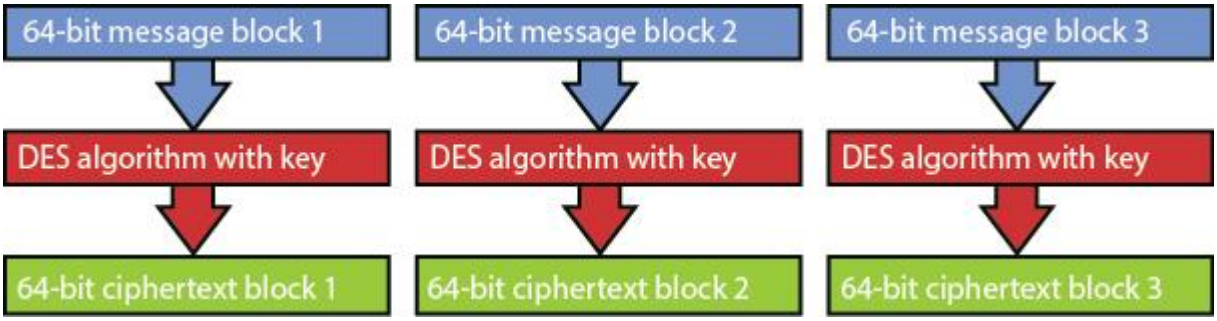
DES viene en los siguientes cinco modos:

- Libro de códigos electrónico (ECB)
- Encadenamiento de bloques de cifrado (CBC)
- Comentarios de cifrado (CFB)
- Realimentación de salida (OFB)
- Modo contador (CTR)

En ECB, el algoritmo procesa bloques de datos de 64 bits utilizando la clave. El texto cifrado producido se puede rellenar para garantizar que el resultado sea un bloque de 64 bits. Si se produce un error de cifrado, solo se verá afectado un bloque del mensaje. Las operaciones del BCE se ejecutan en paralelo, lo que lo convierte en un método rápido.

Aunque ECB es el modo más fácil y rápido de usar, tiene problemas de seguridad porque cada bloque de 64 bits está encriptado con la misma clave. Si un atacante descubre la clave, se pueden leer todos los bloques de datos. Si un atacante descubre ambas versiones del bloque de 64 bits (texto sin formato y texto cifrado), se puede determinar la clave. Por estas razones, el modo no debe usarse al cifrar una gran cantidad de datos porque podrían surgir patrones.

ECB es una buena opción si una organización necesita cifrado para sus bases de datos porque ECB funciona bien con el cifrado de mensajes cortos. La figura 3-14 muestra el proceso de cifrado ECB.

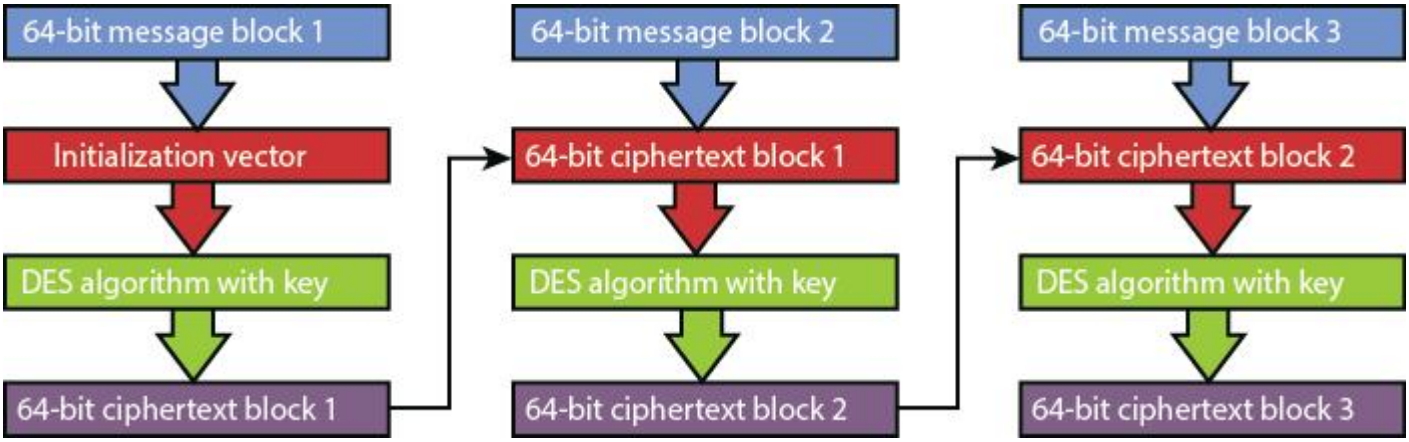


Tres bloques de mensajes de 64 bits separados: 1, 2 y 3 se cifran por separado. El siguiente paso en el proceso en cada uno de los tres bloques de mensajes es el algoritmo DES con la clave que convierte los tres mensajes de bloque en el bloque 1 de texto cifrado de 64 bits, el bloque 2 de texto cifrado de 64 bits y el bloque 3 de texto cifrado de 64 bits, respectivamente.

Figura 3-14 Modo ECB de DES

En CBC, cada bloque de 64 bits está encadenado porque cada bloque de texto cifrado de 64 bits resultante se aplica al siguiente bloque. Por lo tanto, el algoritmo procesa el bloque de mensajes de texto sin formato 1 mediante un IV (discutido anteriormente en este capítulo). El bloque de mensaje de texto cifrado resultante 1 se XOR con el bloque de mensaje de texto plano 2, lo que da como resultado el mensaje de texto cifrado 2. Este proceso continúa hasta que se completa el mensaje.

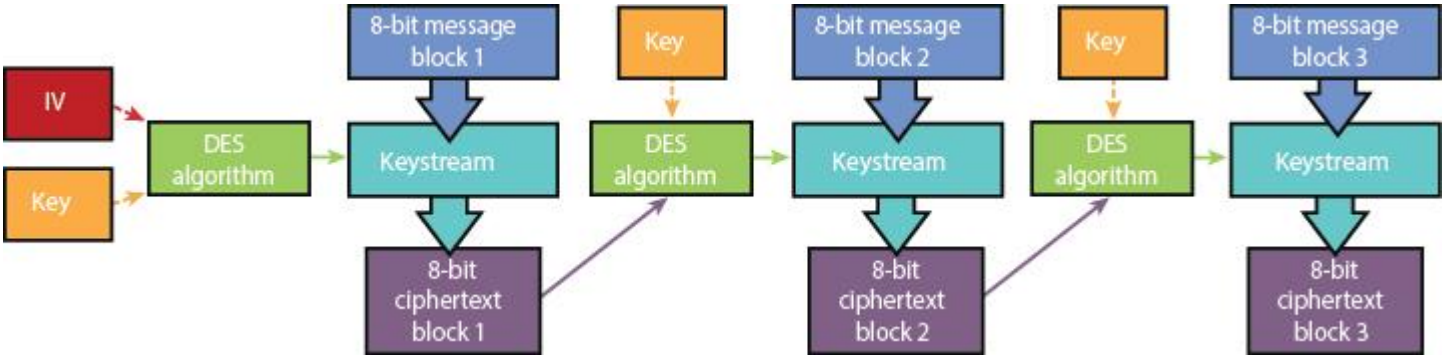
A diferencia de ECB, CBC cifra archivos grandes sin tener ningún patrón dentro del texto cifrado resultante. Si se usa un IV único con cada cifrado de mensaje, el texto cifrado resultante será diferente cada vez, incluso en los casos en que se use el mismo mensaje de texto sin formato. La Figura 3-15 muestra el proceso de encriptación CBC.



Se muestran tres conjuntos de cuatro bloques que están conectados por una flecha hacia abajo. El primer conjunto consta del bloque 1 de mensajes de 64 bits, el vector de inicialización, el algoritmo DES con clave y el bloque 1 de texto cifrado de 64 bits. El segundo conjunto consta del bloque 2 de mensajes de 64 bits, el bloque 1 de mensajes de 64 bits, el algoritmo DES con clave y bloque 2 de texto cifrado de 64 bits. El tercer conjunto consta del bloque 3 de mensajes de 64 bits, el bloque 2 de mensajes de 64 bits, el algoritmo DES con clave y el bloque 3 de texto cifrado de 64 bits. el primer conjunto se genera en el bloque 1 de texto cifrado de 64 bits del segundo conjunto. El bloque 2 de texto cifrado de 64 bits del segundo conjunto se genera en el bloque 2 de texto cifrado de 64 bits del tercer conjunto representado por flechas hacia arriba.

Figura 3-15 Modo CBC de DES

Mientras que CBC y ECB requieren bloques de 64 bits, CFB funciona con bloques de 8 bits (o más pequeños) y utiliza una combinación de cifrado de flujo y cifrado de bloques. Al igual que CBC, el algoritmo aplica XOR al primer bloque de 8 bits del mensaje de texto sin formato mediante un flujo de claves, que es el resultado de un IV y la clave. El mensaje de texto cifrado resultante se aplica al siguiente bloque de mensaje de texto sin formato. La Figura 3-16 muestra el proceso de cifrado CFB.



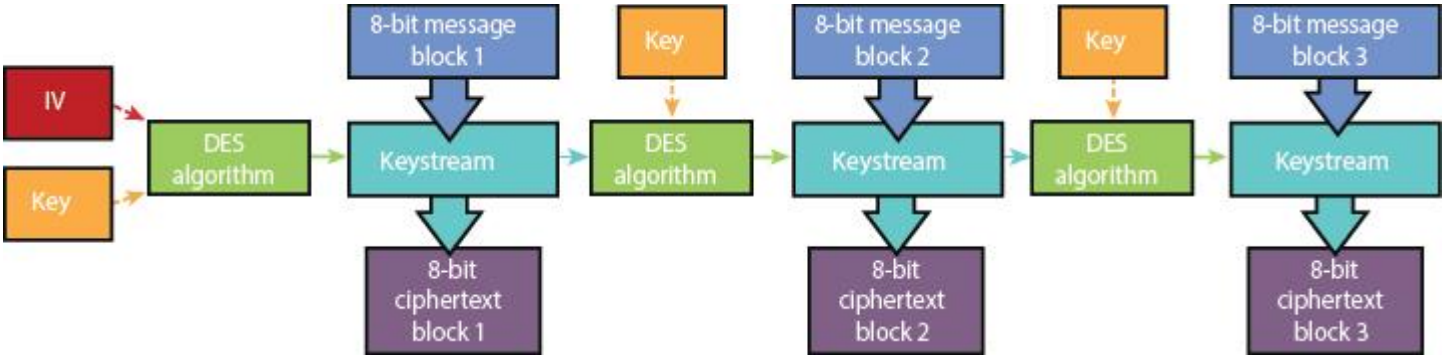
El primer mensaje de bloque de 8 bits se procesa con keystream utilizando un algoritmo DES, que es el resultado de un IV y la clave. El mensaje de texto cifrado resultante se aplica al bloque 2 de mensaje de 8 bits. Este se procesa de nuevo con el flujo de claves utilizando un algoritmo DES que da como resultado el bloque 2 de texto cifrado. El bloque 2 de mensaje de texto cifrado

resultante se aplica al bloque 3 de mensaje de 8 bits. Esto se procesa nuevamente con keystream utilizando un algoritmo DES que da como resultado el bloque 3 de texto cifrado de 8 bits.

Figura 3-16 Modo CFB de DES

El tamaño del bloque de texto cifrado debe ser del mismo tamaño que el bloque de texto sin formato. El método que usa CFB puede tener problemas si algún resultado de texto cifrado tiene errores porque esos errores afectarán cualquier cifrado de bloque futuro. Por esta razón, CFB no debe usarse para encriptar datos que puedan verse afectados por este problema, particularmente señales de video o voz. Este problema llevó a la necesidad del modo DES OFB.

Al igual que CFB, OFB funciona con bloques de 8 bits (o más pequeños) y utiliza una combinación de cifrado de flujo y cifrado de bloques. Sin embargo, OFB usa el flujo de claves anterior con la clave para crear el siguiente flujo de claves. La Figura 3-17 muestra el proceso de cifrado OFB.

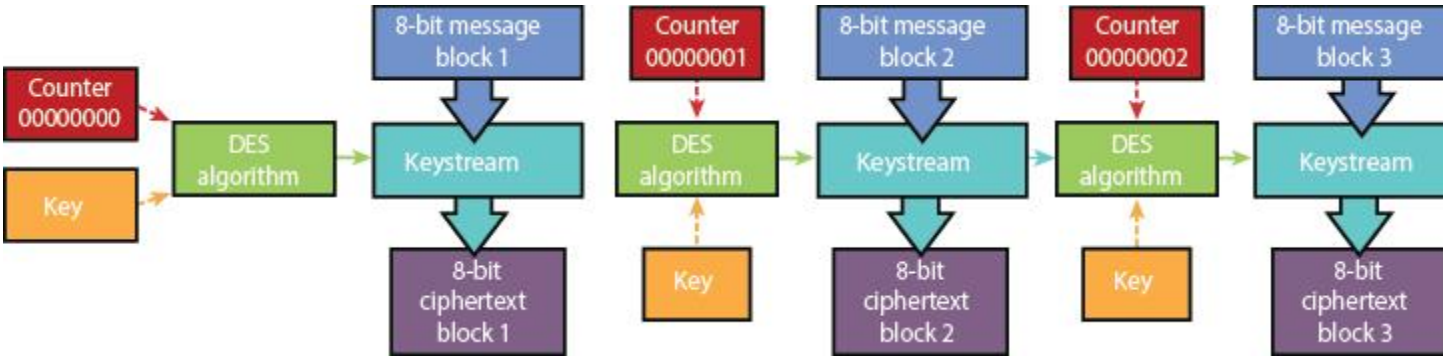


El primer bloque de mensajes de 8 bits 1 se procesa con keystream utilizando un algoritmo DES, que es el resultado de un IV y la clave resulta en el bloque 1 de texto cifrado de 8 bits. El keystream se combina con el algoritmo DES con la clave se aplica al 8- el bloque de mensajes de bits 2 resulta en el bloque de texto cifrado 2. El flujo de claves resultante se procesa posteriormente con el algoritmo DES y la clave se aplica al bloque de mensajes de 8 bits 3 que da como resultado el bloque de texto cifrado 3 de 8 bits.

Figura 3-17 Modo OFB de DES

Con OFB, el tamaño del valor del flujo de claves debe ser del mismo tamaño que el bloque de texto sin formato. Debido a la forma en que se implementa OFB, OFB es menos susceptible al tipo de error que tiene CFB.

El modo CTR es similar al modo OFB. La principal diferencia es que el modo CTR usa un contador IV creciente para garantizar que cada bloque esté encriptado con un flujo de claves único. Además, el texto cifrado no se encadena en el proceso de cifrado. Debido a que este encadenamiento no ocurre, el rendimiento de CTR es mucho mejor que los otros modos. La Figura 3-18 muestra el proceso de cifrado CTR.



El primer mensaje de bloque de 8 bits se procesa con keystream utilizando un algoritmo DES, que es el resultado del Contador 00000000 y la clave resulta en el bloque 1 de texto cifrado de 8 bits. El keystream se combina con el algoritmo DES con la clave y el Contador 00000001. El algoritmo DES se aplica al flujo de claves del bloque 2 de mensajes de 8 bits, lo que da como resultado el bloque 2 de texto cifrado de 8 bits. El flujo de claves resultante se combina con el algoritmo DES con la clave y el contador 00000002, lo que da como resultado el bloque 3 de texto cifrado de 8 bits.

Figura 3-18 Modo CTR de DES

3DES y modos

Debido a la necesidad de reemplazar rápidamente DES, se desarrolló Triple DES (3DES), una versión de DES que aumenta la seguridad mediante el uso de tres claves de 56 bits. Aunque 3DES es resistente a los ataques, es hasta tres veces más lento que DES. 3DES sirvió como un reemplazo temporal de DES. Sin embargo, NIST ha designado el Estándar de cifrado avanzado (AES) como el reemplazo de DES, a pesar de que 3DES todavía está en uso hoy.

3DES viene en los siguientes cuatro modos:

- **3DES-EEE3:** Cada bloque de datos se cifra tres veces, cada vez con una clave diferente.
- **3DES-EDE3:** Cada bloque de datos se cifra con la primera clave, se descifra con la segunda clave y se cifra con la tercera clave.
- **3DES-EEE2:** Cada bloque de datos se cifra con la primera clave, se cifra con la segunda clave y finalmente se vuelve a cifrar con la primera clave.
- **3DES-EDE2:** Cada bloque de datos se cifra con la primera clave, se descifra con la segunda clave y finalmente se vuelve a cifrar con la primera clave.

AES

El estándar de cifrado avanzado (AES) es el algoritmo de sustitución de DES. Cuando el NIST decidió que se necesitaba un nuevo estándar porque el DES se había resquebrajado, se le presentaron cinco opciones de la industria al NIST:

- MARS de IBM
- RC6 de RSA Laboratories
- Anderson, Biham y la serpiente de Knudsen
- Twofish de Counterpane Systems
- Daemen y Rijndael de Rijmen

De estas opciones, NIST seleccionó a Rijndael. Entonces, aunque AES se considera el estándar, el algoritmo que se utiliza en el estándar AES es el algoritmo de Rijndael. Los términos AES y Rijndael a menudo se usan indistintamente.

Los tres tamaños de bloque que se utilizan en el algoritmo de Rijndael son 128, 192 y 256 bits. Una clave de 128 bits con un tamaño de bloque de 128 bits se somete a 10 rondas de transformación. Una clave de 192 bits con un tamaño de bloque de 192 bits se somete a 12 rondas de transformación. Finalmente, una clave de 256 bits con un tamaño de bloque de 256 bits se somete a 14 rondas de transformación.

Rijndael emplea transformaciones compuestas por tres capas: la capa no lineal, la capa de adición de claves y la capa de máximo lineal. El diseño de Rijndael es muy simple y su código es compacto, lo que permite su uso en una variedad de plataformas. Es el algoritmo necesario para datos gubernamentales de EE. UU. Confidenciales pero no clasificados.

OCURRENCIA

El algoritmo de cifrado de datos internacional (IDEA) es un cifrado de bloques que utiliza bloques de 64 bits. Cada bloque de 64 bits se divide en 16 bloques más pequeños. IDEA usa una clave de 128 bits y realiza ocho rondas de transformaciones en cada uno de los 16 bloques más pequeños.

IDEA es más rápido y más difícil de romper que DES. Sin embargo, IDEA no se usa tan ampliamente como DES o AES porque fue patentado, y las tarifas de licencia tuvieron que pagarse al propietario de IDEA, una empresa suiza llamada Ascom. Sin embargo, la patente expiró en 2012. IDEA se usa en PGP, que se analiza más adelante en este capítulo.

Barrilete

Skipjack es un algoritmo simétrico de cifrado en bloques desarrollado por la NSA de EE. UU. Utiliza una clave de 80 bits para cifrar bloques de 64 bits. Este es el algoritmo que se utiliza en el chip Clipper. Los detalles del algoritmo están clasificados.

Pez globo

Blowfish es un cifrado de bloques que utiliza bloques de datos de 64 bits con claves de cifrado de 32 a 448 bits. Blowfish realiza 16 rondas de transformación. Desarrollado inicialmente con la intención de servir como reemplazo de DES, Blowfish es uno de los pocos algoritmos que no están patentados.

Dos peces

Twofish es una versión de Blowfish que utiliza bloques de datos de 128 bits con claves de 128, 192 y 256 bits. Utiliza 16 rondas de transformación. Al igual que Blowfish, Twofish no está patentado.

RC4 / RC5 / RC6 / RC7

Ron Rivest ha desarrollado un total de siete algoritmos RC. RC1 nunca se publicó, RC2 era un cifrado en bloque de 64 bits y RC3 se rompió antes del lanzamiento. Entonces, las principales implementaciones de RC que un profesional de seguridad debe comprender son RC4, RC5, RC6 y RC7.

RC4, también llamado ARC4, es uno de los cifrados de flujo más populares. Se utiliza en SSL y WEP (los cuales se describen con más detalle en el Capítulo 4 , " Comunicación y seguridad de la red "). RC4 utiliza un tamaño de clave variable de 40 a 2048 bits y hasta 256 rondas de transformación.

RC5 es un cifrado de bloque que utiliza un tamaño de clave de hasta 2048 bits y hasta 255 rondas de transformación. Los tamaños de bloque admitidos son 32, 64 o 128 bits. Debido a todas las variables posibles en RC5, la industria a menudo usa una designación RC5 = *w* / *r* / *b* , donde *w* es el tamaño del bloque, *r* es el número de rondas y *b* es el número de bytes de 8 bits en la clave. . Por ejemplo, RC5-64 / 16/16 denota una palabra de 64 bits (o bloques de datos de 128 bits), 16 rondas de transformación y una clave de 16 bytes (128 bits).

RC6 es un cifrado de bloque basado en RC5 y utiliza el mismo tamaño de clave, rondas y tamaño de bloque. RC6 se desarrolló originalmente como una solución AES, pero perdió el concurso ante Rijndael. RC6 es más rápido que RC5.

RC7 es un cifrado de bloques basado en RC6. Si bien utiliza el mismo tamaño de clave y rondas, tiene un tamaño de bloque de 256 bits. Además, utiliza seis registros de trabajo en lugar de cuatro. Como resultado, es mucho más rápido que RC6.

EMITIR

CAST, inventado por Carlisle Adams y Stafford Tavares, tiene dos versiones: CAST-128 y CAST-256. CAST-128 es un cifrado de bloque que utiliza una clave de 40 a 128 bits que realizará 12 o 16 rondas de transformación en bloques de 64 bits. CAST-256 es uncifrado de bloque que utiliza una clave de 128, 160, 192, 224 o 256 bits que realizará 48 rondas de transformación en bloques de 128 bits.

La tabla 3-14 enumera los datos clave sobre cada algoritmo simétrico.

Tabla 3-14 Datos clave de los algoritmos simétricos

Nombre del algoritmo	¿Bloquear o transmitir cifrado?	Tamaño de clave	Numero de rondas	Tamaño de bloque
DESDE	Cuadra	64 bits (longitud efectiva 56 bits)	dieciséis	64 bits
3DES	Cuadra	56, 112 o 168 bits	48	64 bits
AES	Cuadra	128, 192 o 256 bits	10, 12 o 14 (según el tamaño del bloque / clave)	128, 192 o 256 bits
OCURRENCIA	Cuadra	128 bits	8	64 bits
Barrilete	Cuadra	80 bits	32	64 bits
Pez globo	Cuadra	32 a 448 bits	dieciséis	64 bits
Dos peces	Cuadra	128, 192 o 256 bits	dieciséis	128 bits
RC4	Arroyo	40–2,048 bits	Hasta 256	N / A
RC5	Cuadra	Hasta 2048	Hasta 255	32, 64 o 128 bits
RC6	Cuadra	Hasta 2048	Hasta 255	32, 64 o 128 bits
RC7	Cuadra	Hasta 2048	Hasta 255	256 bits

Algoritmos asimétricos

Los algoritmos asimétricos se explicaron anteriormente en este capítulo. En esta sección, discutimos algunos de los algoritmos asimétricos más populares. Es posible que algunos de estos ya no se utilicen comúnmente porque existen alternativas más seguras.

Los profesionales de la seguridad deben estar familiarizados con los siguientes algoritmos simétricos:

- Diffie-Hellman
- RSA
- El Gamal
- ETC
- Mochila
- Prueba de conocimiento cero

Diffie-Hellman

Diffie-Hellman es un algoritmo de acuerdo de clave asimétrico creado por Whitfield Diffie y Martin Hellman. Diffie-Hellman es responsable del proceso de acuerdos clave. El proceso de acuerdo clave incluye los siguientes pasos:

1. John y Sally necesitan comunicarse a través de un canal cifrado y deciden utilizar Diffie-Hellman.
2. John genera una clave pública y privada, y Sally genera una clave pública y privada.
3. John y Sally comparten sus claves públicas entre sí.
4. Una aplicación en la computadora de John toma la clave privada de John y la clave pública de Sally y aplica el algoritmo Diffie-Hellman, y una aplicación en la computadora de Sally toma la clave privada de Sally y la clave pública de John y aplica el algoritmo Diffie-Hellman.
5. A través de esta aplicación, se crea el mismo valor compartido para John y Sally, que a su vez crea la misma clave simétrica en cada sistema utilizando el algoritmo de acuerdo de clave asimétrica.

A través de este proceso, Diffie-Hellman proporciona una distribución segura de claves, pero no confidencialidad, autenticación o no repudio. La clave de este algoritmo es lidiar con logaritmos discretos. Diffie-Hellman es susceptible a ataques man-in-the-middle a menos que una organización implemente firmas digitales o certificados digitales para la autenticación al comienzo del proceso Diffie-Hellman.

Nota

Los ataques de encuentro en el medio se analizan más adelante en este capítulo.

RSA

RSA es el algoritmo asimétrico más popular y fue inventado por Ron Rivest, Adi Shamir y Leonard Adleman. RSA puede proporcionar intercambio de claves, cifrado y firmas digitales. La fuerza del algoritmo RSA es la dificultad de encontrar los factores primos de números muy grandes. RSA usa una clave de 1.024 a 4.096 bits y realiza una ronda de transformación.

Se han factorizado RSA-768 y RSA-704. Si se produce la factorización de los números primos utilizados por una implementación de RSA, entonces la implementación se considera rompible y no debe usarse. RSA-2048 es el número RSA más grande. RSA-4096 también está disponible y tampoco se ha roto.

Como protocolo de intercambio de claves, RSA cifra una clave simétrica DES o AES para una distribución segura. RSA utiliza una función unidireccional para proporcionar cifrado / descifrado y verificación / generación de firmas digitales. La clave pública funciona con la función unidireccional para realizar el cifrado y la verificación de la firma digital. La clave privada funciona con la función unidireccional para realizar el descifrado y la generación de firmas.

En RSA, la función unidireccional es una trampilla. La clave privada conoce la función unidireccional. La clave privada es capaz de determinar los números primos originales. Finalmente, la clave privada sabe cómo utilizar la función unidireccional para descifrar el mensaje cifrado.

Los atacantes pueden usar Number Field Sieve (NFS), un algoritmo de factorización, para atacar RSA.

El Gamal

El Gamal es un algoritmo de clave asimétrica basado en el algoritmo Diffie-Hellman. Al igual que Diffie-Hellman, El Gamal trata con logaritmos discretos. Sin embargo, mientras que Diffie-Hellman solo se puede utilizar para acuerdos de claves, El Gamal puede proporcionar intercambio de claves, cifrado y firmas digitales.

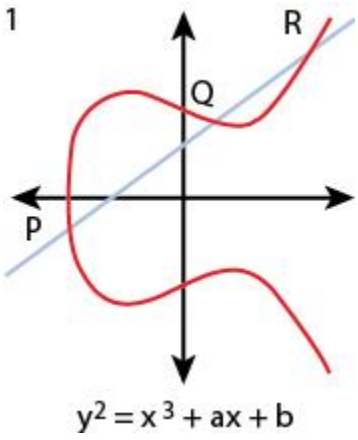
Con El Gamal, se puede utilizar cualquier tamaño de clave. Sin embargo, un tamaño de clave más grande afecta negativamente al rendimiento. Debido a que El Gamal es el algoritmo asimétrico más lento, sería prudente usar un tamaño de clave de 1.024 bits o menos.

ETC

El criptosistema de curva elíptica (ECC) proporciona una distribución segura de claves, cifrado y firmas digitales. El tamaño de la curva elíptica define la dificultad del problema.

Aunque ECC puede usar una clave de cualquier tamaño, puede usar una clave mucho más pequeña que RSA o cualquier otro algoritmo asimétrico y aún proporcionar una seguridad comparable. Por lo tanto, el beneficio principal prometido por ECC es un tamaño de clave más pequeño, lo que reduce los requisitos de almacenamiento y transmisión. ECC es más eficiente y proporciona mejor seguridad que las claves RSA del mismo tamaño.

La figura 3-19 muestra un ejemplo de curva elíptica con la ecuación de la curva elíptica.



Un plano de coordenadas muestra una curva elíptica sin cúspides y autointersección que pasa por los cuatro cuadrantes y una línea recta interseca la curva en tres puntos P en el eje x negativo, Q

en el eje y positivo y R en el primer cuadrante . La ecuación debajo del gráfico dice: y al cuadrado es igual a x al cubo más ax más b.

Figura 3-19 Ejemplo de curva elíptica con ecuación

Mochila

Mochila es una serie de algoritmos asimétricos que proporcionan cifrado y firmas digitales. Esta familia de algoritmos ya no se utiliza debido a problemas de seguridad.

Prueba de conocimiento cero

Una prueba de conocimiento cero es una técnica que se utiliza para garantizar que solo se divulgue la información mínima necesaria sin dar todos los detalles. Un ejemplo de esta técnica ocurre cuando un usuario cifra datos con su clave privada y el receptor los descifra con la clave pública del originador. El autor no ha entregado su clave privada al receptor. Pero el autor está demostrando que tiene su clave privada simplemente porque el receptor puede leer el mensaje.

Infraestructura de Clave Pública

Una infraestructura de clave pública (PKI) incluye sistemas, software y protocolos de comunicación que distribuyen, administran y controlan la criptografía de clave pública. Una PKI publica certificados digitales. Debido a que una PKI establece confianza dentro de un entorno, una PKI puede certificar que una clave pública está vinculada a una entidad y verificar que una clave pública sea válida. Las claves públicas se publican mediante certificados digitales.

El estándar X.509 es un marco que permite la autenticación entre redes y a través de Internet. Una PKI incluye marcas de tiempo y revocación de certificados para garantizar que los certificados se gestionen correctamente. Una PKI proporciona confidencialidad, integridad de mensajes, autenticación y no repudio.

La estructura de una PKI incluye autoridades de certificación, certificados, autoridades de registro, listas de revocación de certificados, certificación cruzada y el Protocolo de estado de certificados en línea (OCSP). En esta sección, analizamos estos componentes de PKI, así como algunos otros conceptos de PKI.

Autoridad de certificación y autoridad de registro

Cualquier participante que solicite un certificado debe pasar primero por la autoridad de registro (RA), que verifica la identidad del solicitante y registra al solicitante. Una vez que se verifica la identidad, la RA pasa la solicitud a la autoridad de certificación (CA).

Una CA es la entidad que crea y firma certificados digitales, mantiene los certificados y los revoca cuando es necesario. Toda entidad que quiera participar en la PKI debe contactar a la CA y solicitar un certificado digital. La CA es la máxima autoridad para la autenticidad de cada

participante en la PKI y firma cada certificado digital. El certificado vincula la identidad del participante a la clave pública.

Existen diferentes tipos de CA. Existen organizaciones que brindan una PKI como un servicio pagadero a las empresas que las necesitan. Un ejemplo es Symantec. Algunas organizaciones implementan sus propias CA privadas para que la organización pueda controlar todos los aspectos del proceso PKI. Si una organización es lo suficientemente grande, es posible que deba proporcionar una estructura de CA, siendo la CA raíz la más alta en la jerarquía.

Debido a que a menudo más de una entidad está involucrada en el proceso de certificación de PKI, la validación de la ruta de certificación permite a los participantes verificar la legitimidad de los certificados en la ruta de certificación.

Certificados

Un certificado digital proporciona a una entidad, generalmente un usuario, las credenciales para probar su identidad y asocia esa identidad con una clave pública. Como mínimo, un certificado digital debe proporcionar el número de serie, el emisor, el sujeto (propietario) y la clave pública.

Un certificado X.509 cumple con el estándar X.509. Un certificado X.509 contiene los siguientes campos:

- Versión
- Número de serie
- ID de algoritmo
- Editor
- Validez
- Sujeto
- Información de clave pública del sujeto
- Algoritmo de clave pública
- Clave pública del sujeto
- Identificador único del emisor (opcional)
- Identificador único del sujeto (opcional)
- Extensiones (opcional)

Symantec introdujo por primera vez las siguientes clases de certificados digitales:

- **Clase 1:** para particulares; utilizado para proteger el correo electrónico. Estos certificados se guardan mediante navegadores web.
- **Clase 2:** Para organizaciones que deben proporcionar prueba de identidad.
- **Clase 3:** Para servidores y firma de software en los que la CA emisora realiza una verificación independiente y una verificación de identidad y autoridad.

Ciclo de vida del certificado

Los profesionales de la seguridad deben comprender el ciclo de vida del certificado. Según Microsoft, el ciclo de vida del certificado incluye los siguientes eventos:

- Se instalan las CA y se emiten los certificados de CA.
- Los certificados son emitidos por las CA a las entidades.
- Los certificados se revocan (según sea necesario), se renuevan o se les permite caducar.
- Los certificados de las CA se renuevan antes de que caduquen, se revoquen o se retiren.

El Informe interinstitucional del NIST (NISTIR) 7924, titulado "Política de certificado de referencia", identifica un conjunto básico de controles y prácticas de seguridad para respaldar la emisión segura de certificados. Este informe está en su segundo borrador y se puede encontrar en https://csrc.nist.gov/CSRC/media/Publications/nistir/7924/draft/documents/nistir_7924_2nd_draft.pdf .

Según NISTIR 7924, el proceso de solicitud de certificado debe proporcionar información suficiente para

- Establecer la autorización del solicitante (por parte de la organización que lo emplea o patrocinadora) para obtener un certificado.
- Establecer y registrar la identidad del solicitante.
- Obtenga la clave pública del solicitante y verifique que el solicitante posea la clave privada para cada certificado requerido.
- Verifique cualquier rol o información de autorización solicitada para su inclusión en el certificado.

En este documento, los pasos del proceso del certificado son los siguientes:

1. Solicitud de certificado
2. Procesamiento de solicitud de certificado
3. Emisión de certificados
4. Aceptación del certificado
5. Par de claves y uso de certificados
6. Renovación de certificado
7. Cambio de clave de certificado
8. Modificación de certificado
9. Revocación y suspensión de certificados
10. Fin de la suscripción
11. Depósito y recuperación de claves

Estos pasos se pueden realizar en cualquier orden que sea conveniente para la CA y los solicitantes que no comprometa la seguridad, pero todos deben completarse antes de la emisión del certificado.

Para el examen CISSP, debe conocer los cuatro pasos principales que involucran un certificado emitido a una entidad: inscripción, verificación, revocación y renovación y modificación.

Inscripción

La inscripción es el proceso de solicitar un certificado a la CA. De acuerdo con NISTIR 7924, el suscriptor, el representante organizacional autorizado (AOR) o un RA en nombre del suscriptor enviarán una solicitud de certificado a la CA. Se pueden enviar varias solicitudes de certificado de un RA o AOR como un lote.

Al inscribir a un suscriptor, todas las comunicaciones entre las autoridades de PKI que respaldan la solicitud del certificado y el proceso de emisión deberán estar autenticadas y protegidas contra modificaciones; Se protegerá cualquier transmisión electrónica de secretos compartidos e información de identificación personal. Las comunicaciones pueden ser electrónicas o fuera de banda. Cuando se utilicen comunicaciones electrónicas, se utilizarán mecanismos criptográficos acordes con la fuerza del par de claves pública / privada. Las comunicaciones fuera de banda protegerán la confidencialidad e integridad de los datos.

Verificación

La verificación es el proceso mediante el cual una aplicación verifica que un certificado es válido. Las aplicaciones utilizan dos tipos de métodos de verificación para comprobar la validez de un certificado digital: listas de revocación de certificados (CRL) y Protocolo de estado de certificados en línea (OCSP), los cuales se describen en las secciones siguientes.

Para emitir un certificado, la CA debe verificar que se haya verificado la identidad y autorización del solicitante. Si esta información no se puede verificar, al recibir la solicitud, las CA / RA deberán

- Verifique la identidad del solicitante.
- Verifique la autoridad del solicitante y la integridad de la información en la solicitud de certificado.
- Cree y firme un certificado si se han cumplido todos los requisitos del certificado (en el caso de una RA, haga que la CA firme el certificado).
- Ponga el certificado a disposición del suscriptor después de confirmar que el suscriptor ha reconocido formalmente sus obligaciones.

La solicitud de certificado ya puede contener un certificado a firmar creado por el RA o el suscriptor. Este certificado no se firmará hasta que todas las verificaciones y modificaciones, si las hubiera, se hayan completado a satisfacción de la CA. Toda la información de autorización y demás atributos recibida de un posible suscriptor deberá verificarse antes de su inclusión en un certificado. La falta de objeción al certificado o su contenido constituirá la aceptación del certificado.

Revocación

La revocación es el proceso mediante el cual se revoca un certificado. Las CA que operan bajo NISTIR 7924 deben hacer pública una descripción de cómo obtener información de revocación para los certificados que publican, y una explicación de las consecuencias del uso de información

de revocación fechada. Esta información se proporcionará a los suscriptores durante la solicitud o emisión del certificado, y estará disponible para cualquier posible parte de confianza. Las solicitudes de revocación deben estar autenticadas.

Un certificado se revocará cuando la vinculación entre el sujeto y la clave pública del sujeto definida en el certificado ya no se considere válida. Cuando esto ocurra, el certificado asociado se revocará y se colocará en la CRL y / o se agregará al respondedor OCSP. Los certificados revocados se incluirán en todas las publicaciones nuevas de la información sobre el estado del certificado hasta que caduquen.

Las CA deben revocar los certificados tan pronto como sea posible al recibir una solicitud de revocación adecuada y después del tiempo de revocación solicitado.

Renovación y Modificación

Cualquier certificado puede renovarse si la clave pública no ha llegado al final de su período de validez, la clave privada asociada no ha sido revocada o comprometida y el nombre y los atributos del suscriptor no se modifican. Además, el período de validez del certificado no debe exceder la vida útil restante de la clave privada.

Los certificados de CA y los certificados de respuesta OCSP se pueden renovar siempre que la vida útil agregada de la clave pública no exceda la vida útil del certificado. La CA puede renovar los certificados emitidos previamente durante la recuperación del compromiso de la clave de la CA sin la solicitud o aprobación del sujeto, siempre que la CA esté segura de la precisión de la información que se incluirá en los certificados.

Una CA puede realizar la modificación del certificado para un suscriptor cuyas características han cambiado (por ejemplo, cambio de nombre debido al matrimonio). Si el nombre del suscriptor ha cambiado, el suscriptor se someterá al proceso de registro inicial.

Lista de revocación de certificados

Una lista de revocación de certificados (CRL) es una lista de certificados digitales que una CA ha revocado. Para saber si se ha revocado un certificado digital, el navegadordebe comprobar la CRL o recibir los valores de CRL extraídos de la CA. Esto puede resultar bastante abrumador si se tiene en cuenta que la CRL contiene todos los certificados que se han revocado.

Un concepto a tener en cuenta es el período de gracia de la solicitud de revocación. Este período es la cantidad máxima de tiempo entre el momento en que la CA recibe la solicitud de revocación y el momento en que la revocación ocurre realmente. Un período de revocación más corto proporciona una mayor seguridad, pero a menudo resulta en un mayor costo de implementación.

OCSP

Online Certificate Status Protocol (OCSP) es un protocolo de Internet que obtiene el estado de revocación de un certificado digital X.509. OCSP es una alternativa a la CRL estándar que utilizan muchas PKI. OCSP valida automáticamente los certificados e informa el estado del certificado digital accediendo a la CRL en la CA.

Pasos de PKI

Los pasos necesarios para solicitar un certificado digital son los siguientes:

1. Un usuario solicita un certificado digital y la RA recibe la solicitud.
2. La RA solicita información de identificación del solicitante.
3. Una vez recibida la información requerida, la RA envía la solicitud de certificado a la CA.
4. La CA crea un certificado digital para el solicitante. La clave pública y la información de identidad del solicitante se incluyen como parte del certificado.
5. El usuario recibe el certificado.

Una vez que el usuario tiene un certificado, está listo para comunicarse con otras entidades de confianza. El proceso de comunicación entre entidades es el siguiente:

1. El usuario 1 solicita la clave pública del usuario 2 del repositorio de certificados.
2. El repositorio envía el certificado digital del Usuario 2 al Usuario 1.
3. El usuario 1 verifica el certificado y extrae la clave pública del usuario 2.
4. El usuario 1 cifra la clave de sesión con la clave pública del usuario 2 y envía la clave de sesión cifrada y el certificado del usuario 1 al usuario 2.
5. El usuario 2 recibe el certificado del usuario 1 y verifica el certificado con una CA de confianza.

Una vez que se produce este proceso de verificación e intercambio de certificados, las dos entidades pueden comunicarse mediante cifrado.

Certificación cruzada

La certificación cruzada establece relaciones de confianza entre las CA para que las CA participantes puedan confiar en los certificados digitales y las claves públicas de los demás participantes. Permite a los usuarios validar los certificados de los demás cuando en realidad están certificados bajo diferentes jerarquías de certificación. Una CA de una organización puede validar certificados digitales de la CA de otra organización cuando existe una relación de confianza de certificación cruzada.

Prácticas de gestión clave

Una discusión sobre criptografía estaría incompleta sin una cobertura de las prácticas de gestión de claves. NIST SP 800-57 contiene recomendaciones para la gestión de claves en tres partes:

- **Parte 1:** esta publicación cubre recomendaciones generales para la gestión de claves.
- **Parte 2:** esta publicación cubre las mejores prácticas para una organización de gestión de claves.
- **Parte 3:** esta publicación cubre la guía de administración de claves específica de la aplicación.

Los profesionales de la seguridad deben comprender al menos los principios de administración de claves en la Parte 1 de SP 800-57 Revisión 1. Si los profesionales de seguridad están involucrados en organizaciones que brindan servicios de administración de claves a otras organizaciones, comprender la Parte 2 es una necesidad. La parte 3 es necesaria cuando una organización implementa aplicaciones que utilizan claves. En esta sección, cubrimos las recomendaciones en la Parte 1.

La parte 1 define los siguientes tipos diferentes de claves. Las claves se identifican según su clasificación como claves públicas, privadas o simétricas, así como según su uso. Para las claves de acuerdo de claves públicas y privadas, también se especifica el estado como claves estáticas o efímeras.

- **Clave de firma privada:** esta es la clave privada de pares de claves asimétricas (públicas) que utilizan los algoritmos de clave pública para generar firmas digitales con posibles implicaciones a largo plazo. Cuando se manejan correctamente, las claves de firma privadas se pueden utilizar para proporcionar autenticación de origen, proporcionar autenticación de integridad y respaldar el no repudio de mensajes, documentos o datos almacenados.
- **Clave de verificación de firma pública:** esta es la clave pública de un par de claves asimétricas (públicas) que utiliza un algoritmo de clave pública para verificar firmas digitales que están destinadas a proporcionar autenticación de origen, proporcionar autenticación de integridad y respaldar el no repudio. de mensajes, documentos o datos almacenados.
- **Clave de autenticación simétrica:** esta clave se utiliza con algoritmos de clave simétrica para proporcionar autenticación de origen y garantía de la integridad de las sesiones de comunicación, mensajes, documentos o datos almacenados (es decir, autenticación de integridad).
- **Clave de autenticación privada:** esta es la clave privada de un par de claves asimétricas (públicas) que se utiliza con un algoritmo de clave pública para garantizar la identidad de una entidad de origen (es decir, la fuente) al establecer una sesión de comunicación autenticada.
- **Clave de autenticación pública:** esta es la clave pública de un par de claves asimétricas (públicas) que se utiliza con un algoritmo de clave pública para garantizar la identidad de una entidad de origen (es decir, la fuente) al establecer una sesión de comunicación autenticada.
- **Clave de cifrado de datos simétrica:** esta clave se utiliza con algoritmos de clave simétrica para aplicar protección de confidencialidad a la información (es decir, para

cifrar la información). La misma clave también se utiliza para eliminar la protección de confidencialidad (es decir, para descifrar la información).

- **Clave de envoltura de clave simétrica (también llamada clave de cifrado de clave):** esta clave se utiliza para cifrar otras claves mediante algoritmos de clave simétrica. La clave de envoltura de claves utilizada para cifrar una clave también se utiliza para revertir la operación de cifrado (es decir, para descifrar la clave cifrada). Dependiendo del algoritmo con el que se use la clave, la clave también se puede usar para brindar protección de integridad.
- **Clave de generación de números aleatorios simétricos:** esta clave se utiliza para generar números aleatorios o bits aleatorios.
- **Clave maestra simétrica:** esta clave se utiliza para derivar otras claves simétricas (por ejemplo, claves de cifrado de datos, claves de envoltura de claves o claves de autenticación de origen) utilizando métodos criptográficos simétricos. La clave maestra también se conoce como clave de derivación de clave.
- **Clave de transporte de clave** privada **:** esta es la clave privada de pares de claves asimétricas (públicas) que se utiliza para descifrar claves que se han cifrado con la clave pública correspondiente mediante un algoritmo de clave pública. Las claves de transporte de claves se utilizan generalmente para establecer claves (por ejemplo, claves de envoltura de claves, claves de cifrado de datos o claves MAC) y, opcionalmente, otro material de claves (por ejemplo, vectores de inicialización).
- **Clave de transporte de clave** pública **:** esta es la clave pública de pares de claves asimétricas (públicas) que se utiliza para cifrar claves mediante un algoritmo de clave pública. Estas claves se utilizan para establecer claves (por ejemplo, claves de envoltura de claves, claves de cifrado de datos o claves MAC) y, opcionalmente, otro material de claves (por ejemplo, vectores de inicialización). La forma cifrada de la clave establecida puede almacenarse para su posterior descifrado utilizando la clave de transporte de clave privada.
- **Clave de acuerdo de clave simétrica:** esta clave se utiliza para establecer claves (p. Ej., Claves de envoltura de claves, claves de cifrado de datos o claves MAC) y, opcionalmente, otro material de claves (p. Ej., Vectores de inicialización), utilizando un acuerdo de clave simétrico algoritmo.
- **Clave de acuerdo de clave estática privada:** esta es la clave privada a largo plazo de pares de claves asimétricas (públicas) que se utiliza para establecer claves (p. Ej., Claves de envoltura de claves, claves de cifrado de datos o claves MAC) y, opcionalmente, otras material de codificación (por ejemplo, vectores de inicialización).
- **Clave de acuerdo de clave estática pública:** esta es la clave pública a largo plazo de pares de claves asimétricas (públicas) que se utiliza para establecer claves (p. Ej., Claves de envoltura de claves, claves de cifrado de datos o claves MAC) y, opcionalmente, otras material de codificación (por ejemplo, vectores de inicialización).
- **Clave de acuerdo de clave efímera privada:** esta es la clave privada a corto plazo de pares de claves asimétricas (públicas) que se usa solo una vez para establecer una o más claves (p. Ej., Claves de envoltura de claves, claves de cifrado de datos o claves MAC) y, opcionalmente, otro material de codificación (por ejemplo, vectores de inicialización).
- **Clave de acuerdo de clave pública efímera:** esta es la clave pública a corto plazo de pares de claves asimétricas que se utiliza en una transacción de establecimiento de clave única para establecer una o más claves (p. Ej., Claves de envoltura de claves, claves de

cifrado de datos o MAC claves) y, opcionalmente, otro material de codificación (por ejemplo, vectores de inicialización).
- **Clave de autorización simétrica:** este tipo de clave se utiliza para proporcionar privilegios a una entidad mediante un método criptográfico simétrico. La clave de autorización es conocida por la entidad responsable de monitorear y otorgar privilegios de acceso a las entidades autorizadas y por la entidad que busca el acceso a los recursos.
- **Clave de autorización privada:** esta es la clave privada de un par de claves asimétricas (públicas) que se utiliza para proporcionar privilegios a una entidad.
- **Clave de autorización pública:** esta es la clave pública de un par de claves asimétricas (públicas) que se utiliza para verificar los privilegios de una entidad que conoce la clave de autorización privada asociada.

En general, una sola clave se usa para un solo propósito (por ejemplo, encriptación, integridad, autenticación, envoltura de claves, generación de bits aleatorios o firmas digitales). Un *criptoperiodo* es el lapso de tiempo durante el cual una clave específica está autorizada para ser utilizada por entidades legítimas, o el tiempo que las claves para un sistema dado permanecerán en vigor. Entre los factores que afectan la duración de un criptoperíodo se encuentran

- La fuerza criptográfica (por ejemplo, el algoritmo, la longitud de la clave, el tamaño del bloque y el modo de operación)
- La realización de los mecanismos (por ejemplo, una implementación de FIPS 140 Nivel 4 o una implementación de software en una computadora personal)
- El entorno operativo (por ejemplo, una instalación segura de acceso limitado, un entorno de oficina abierta o una terminal de acceso público)
- El volumen de flujo de información o el número de transacciones.
- La vida de seguridad de los datos
- La función de seguridad (p. Ej., Cifrado de datos, firma digital, derivación de claves o protección de claves)
- El método de reintroducción (p. Ej., Entrada de teclado, reintroducción mediante un dispositivo de carga de claves donde los humanos no tienen acceso directo a la información clave o reintroducción remota dentro de una PKI)
- El proceso de actualización o derivación de claves
- La cantidad de nodos en una red que comparten una clave común.
- El número de copias de una clave y la distribución de esas copias.
- Rotación de personal (por ejemplo, personal del sistema de CA)
- La amenaza a la información de los adversarios (por ejemplo, de quién está protegida la información y sus capacidades técnicas y recursos financieros percibidos para montar un ataque)
- La amenaza a la información de tecnologías nuevas y disruptivas (por ejemplo, computadoras cuánticas)

Los requisitos de protección para claves criptográficas se muestran en la Tabla 3-15 . La columna Servicio de seguridad enumera el servicio de seguridad proporcionado por la clave. La columna Protección de seguridad enumera el tipo de protección requerida para la clave.

Tabla 3-15 Requisitos de protección para claves criptográficas

Tipo de clave	Servicio de seguridad	Protección de seguridad	Período de protección
Clave de firma privada	Autenticación de origen	Integridad	Desde la generación hasta el final del criptoperiodo
	Autenticación de integridad	Confidencialidad	
	Apoyar el no repudio		
Clave de verificación de firma pública	Autenticación de origen	Integridad	Desde la generación hasta que no es necesario verificar los datos protegidos
	Autenticación de integridad		
	Apoyar el no repudio		
Clave de autenticación simétrica	Autenticación de origen	Integridad	Desde la generación hasta que no es necesario verificar los datos protegidos
	Autenticación de integridad	Confidencialidad	
Clave de autenticación privada	Autenticación de origen	Integridad	Desde la generación hasta el final del criptoperiodo
	Autenticación de integridad	Confidencialidad	
Clave de autenticación pública	Autenticación de origen	Integridad	Desde la generación hasta que no es necesario autenticar datos protegidos
	Autenticación de integridad		
Clave de cifrado / descifrado de datos simétrico	Confidencialidad	Integridad	Desde la generación hasta el final de la vida útil de los datos o el final del criptoperíodo, lo que ocurra más tarde
		Confidencialidad	
Llave de envoltura de clave simétrica	Apoyo	Integridad	Desde la generación hasta el final del criptoperíodo o hasta que ninguna clave envuelta requiera protección, lo que ocurra más tarde
		Confidencialidad	
Llave simétrica RBG	Apoyo	Integridad	Desde la generación hasta la sustitución
		Confidencialidad	

Tipo de clave	Servicio de seguridad	Protección de seguridad	Período de protección
Llave maestra simétrica	Apoyo	Integridad Confidencialidad	Desde la generación hasta el final del criptoperíodo o el final de la vida útil de las claves derivadas, lo que ocurra más tarde
Clave de transporte de clave privada	Apoyo	Integridad Confidencialidad	Desde la generación hasta el final del período de protección para todas las claves transportadas
Clave de transporte de clave pública	Apoyo	Integridad	Desde la generación hasta el final del criptoperiodo
Clave simétrica de acuerdo de clave	Apoyo	Integridad Confidencialidad	Desde la generación hasta el final del criptoperiodo o hasta que ya no sea necesario para determinar una clave, lo que ocurra más tarde
Clave de acuerdo de clave estática privada	Apoyo	Integridad Confidencialidad	Desde la generación hasta el final del criptoperiodo o hasta que ya no sea necesario para determinar una clave, lo que ocurra más tarde
Clave de acuerdo de clave estática pública	Apoyo	Integridad	Desde la generación hasta el final del criptoperiodo o hasta que ya no sea necesario para determinar una clave, lo que ocurra más tarde
Clave de acuerdo de clave efímera privada	Apoyo	Integridad Confidencialidad	Desde la generación hasta el final del proceso de acuerdo de claves; una vez finalizado el proceso, la clave se destruye
Clave de acuerdo de clave efímera pública	Apoyo	Integridad	Desde la generación hasta que se completa el proceso de acuerdo de claves
Clave de autorización simétrica	Autorización	Integridad Confidencialidad	Desde la generación hasta el final del criptoperiodo de la clave
Clave de autorización privada	Autorización	Integridad Confidencialidad	Desde la generación hasta el final del criptoperiodo de la clave
Clave de autorización pública	Autorización	Integridad	Desde la generación hasta el final del criptoperiodo de la clave

Una clave se usa de manera diferente, dependiendo de su estado en el ciclo de vida de la clave. Los estados clave se definen desde el punto de vista del sistema, a diferencia del punto de vista de un solo módulo criptográfico. Los estados que puede asumir una clave operativa o con copia de seguridad son los siguientes:

- **Estado de preactivación:** la clave se ha generado pero no se ha autorizado su uso. En este estado, la clave solo se puede utilizar para realizar una prueba de posesión o una confirmación de la clave.
- **Estado activo:** la clave puede usarse para proteger criptográficamente información (por ejemplo, cifrar texto plano o generar una firma digital), para procesar criptográficamente información previamente protegida (por ejemplo, descifrar texto cifrado o verificar una firma digital), o ambos. Cuando una clave está activa, se puede designar solo para protección, solo procesamiento, o para protección y procesamiento, según su tipo.
- **Estado suspendido:** el uso de una clave o un par de claves puede suspenderse por varias razones posibles; en el caso de pares de claves asimétricas, tanto la clave pública como la privada se suspenden al mismo tiempo. Una razón para una suspensión podría ser un posible compromiso clave, y la suspensión se emitió para dar tiempo a investigar la situación. Otra razón podría ser que la entidad que posee un par de claves de firma digital no está disponible (por ejemplo, está en una licencia prolongada); las firmas supuestamente firmadas durante el tiempo de suspensión no serían válidas. Una clave suspendida o un par de claves puede restaurarse a un estado activo en un momento posterior o puede desactivarse o destruirse, o puede pasar al estado comprometido.
- **Estado desactivado: las** claves en el estado desactivado no se utilizan para aplicar protección criptográfica, pero en algunos casos, pueden utilizarse para procesar información protegida criptográficamente. Si una clave ha sido revocada (por razones distintas a un compromiso), entonces la clave puede seguir utilizándose para el procesamiento. Tenga en cuenta que se puede considerar que las claves recuperadas de un archivo están en estado desactivado a menos que estén comprometidas.
- **Estado comprometido:** generalmente, las claves se ven comprometidas cuando se entregan a una entidad no autorizada o lo determina una entidad no autorizada. No se utilizará una clave comprometida para aplicar protección criptográfica a la información. Sin embargo, en algunos casos, se puede utilizar una clave comprometida o una clave pública que corresponda a una clave privada comprometida de un par de claves para procesar información protegida criptográficamente. Por ejemplo, una firma puede verificarse para determinar la integridad de los datos firmados si su firma ha estado protegida físicamente desde un tiempo antes de que ocurriera el compromiso. Este procesamiento se realizará únicamente en condiciones muy controladas, donde los usuarios de la información sean plenamente conscientes de las posibles consecuencias.
- **Estado destruido:** la llave ha sido destruida como se especifica en la fase destruida, que se comenta en breve. Aunque la clave ya no existe cuando se encuentra en este estado, se pueden retener ciertos metadatos de clave (por ejemplo, historial de transición de estado de clave, nombre de clave, tipo, criptoperíodo).

El ciclo de vida de la gestión de claves criptográficas se puede dividir en las siguientes cuatro fases:

1. **Fase preoperativa:** el material de codificación aún no está disponible para operaciones criptográficas normales. Es posible que las claves aún no se hayan generado o estén en estado de preactivación. Los atributos del sistema o de la empresa también se establecen durante esta fase. Durante esta fase, ocurren las siguientes funciones:
    1. Registro de usuario

    2. Inicialización del sistema
    3. Inicialización del usuario
    4. Instalación de material de codificación
    5. Establecimiento clave
    6. Registro de claves
2. **Fase operativa:** El material de codificación está disponible y en uso normal. Las claves están en estado activo o suspendido. Las claves en el estado activo se pueden designar como proteger solamente, procesar solamente o proteger y procesar; las claves en el estado suspendido se pueden usar solo para procesamiento. Durante esta fase, ocurren las siguientes funciones:
    1. Almacenamiento operativo normal
    2. Continuidad de operaciones
    3. Cambio de clave
    4. Derivación de claves
3. **Fase** posoperativa **:** el material de codificación ya no se utiliza normalmente, pero es posible acceder al material de codificación y el material de codificación se puede utilizar para el procesamiento solo en determinadas circunstancias. Las claves están en estado desactivado o comprometido. Las claves en la fase posoperatoria pueden estar en un archivo cuando no se procesan datos. Durante esta fase ocurren las siguientes funciones:
    1. Almacenamiento de archivos y recuperación de claves
    2. Baja de la entidad
    3. Dar de baja clave
    4. Destrucción de llaves
    5. Revocación de claves
4. **Fase destruida: las** llaves ya no están disponibles. Los registros de su existencia pueden haber sido borrados o no. Las llaves están en los estados destruidos. Aunque las claves en sí mismas se destruyen, los metadatos de la clave (por ejemplo, nombre de clave, tipo, criptoperíodo, período de uso) pueden conservarse.

Los sistemas que procesan información valiosa requieren controles para proteger la información de la divulgación y modificación no autorizadas. Los sistemas criptográficos que contienen claves y otra información criptográfica son especialmente críticos. Los profesionales de la seguridad deben trabajar para garantizar que la protección del material de claves proporcione responsabilidad, auditoría y supervivencia.

La rendición de cuentas implica la identificación de entidades que tienen acceso o control de claves criptográficas a lo largo de sus ciclos de vida. La rendición de cuentas puede ser una herramienta eficaz para ayudar a prevenir compromisos clave y reducir el impacto de los compromisos cuando se detectan. Aunque se prefiere que ningún ser humano pueda ver las claves, como mínimo, el sistema de administración de claves debe tener en cuenta a todas las personas que pueden ver claves criptográficas en texto plano. Además, los sistemas de gestión de claves más sofisticados pueden dar cuenta de todas las personas autorizadas para acceder o controlar cualquier clave criptográfica, ya sea en forma de texto plano o cifrado.

Se deben realizar dos tipos de auditorías en los sistemas de gestión de claves:

- **Seguridad:** El plan de seguridad y los procedimientos que se desarrollan para respaldar el plan deben auditarse periódicamente para garantizar que continúen respaldando la política de administración de claves.
- **Protección:** Los mecanismos de protección empleados deben reevaluarse periódicamente con respecto al nivel de seguridad que brindan actualmente y se espera que brinden en el futuro. También deben evaluarse para determinar si los mecanismos apoyan correcta y eficazmente las políticas adecuadas. Los nuevos desarrollos y ataques tecnológicos deben considerarse parte de una auditoría de protección.

La supervivencia de la gestión de claves implica realizar copias de seguridad o archivar copias de todas las claves utilizadas. Deben establecerse procedimientos de copia de seguridad y recuperación de claves para garantizar que las claves no se pierdan. La redundancia del sistema y la planificación de contingencias también deben evaluarse adecuadamente para garantizar que todos los sistemas involucrados en la administración de claves sean tolerantes a fallas.

Integridad del mensaje

La integridad es uno de los tres principios básicos de la seguridad. La integridad del mensaje garantiza que un mensaje no se haya alterado mediante el uso de bits de paridad, comprobaciones de redundancia cíclica (CRC) o sumas de comprobación.

El método del bit de paridad agrega un bit extra a los datos. Este bit de paridad simplemente indica si el número de 1 bits es par o impar. El bit de paridad es 1 si el número de 1 bits es impar y el bit de paridad es 0 si el número de 1 bits es par. El bit de paridad se establece antes de que se transmitan los datos. Cuando llegan los datos, el bit de paridad se compara con los demás datos. Si el bit de paridad no coincide con los datos enviados, se envía un error al originador.

El método CRC utiliza la división polinomial para determinar el valor CRC de un archivo. El valor CRC suele tener una longitud de 16 o 32 bits. Debido a que CRC es muy preciso, el valor de CRC no coincidirá si un solo bit es incorrecto.

El método de suma de comprobación suma los bytes de datos que se envían y luego transmite ese número para verificarlo más tarde utilizando el mismo método. La fuente suma los valores de los bytes y envía los datos y su suma de comprobación. El extremo receptor recibe la información, suma los bytes de la misma manera que lo hizo la fuente y obtiene la suma de comprobación. El receptor luego compara su suma de verificación con la suma de verificación de la fuente. Si los valores coinciden, la integridad del mensaje está intacta. Si los valores no coinciden, los datos deben reenviarse o reemplazarse. Las sumas de comprobación también se denominan sumas hash porque normalmente utilizan funciones hash para el cálculo.

La integridad del mensaje es proporcionada por las funciones hash y el código de autenticación del mensaje.

Hashing

Las funciones hash se explicaron anteriormente en este capítulo. En esta sección, discutimos algunas de las funciones hash más populares. Es posible que algunos de estos ya no se utilicen comúnmente porque hay disponibles alternativas más seguras.

Los profesionales de la seguridad deben estar familiarizados con las siguientes funciones hash:

- Hash unidireccional
- MD2 / MD4 / MD5 / MD6
- SHA / SHA-2 / SHA-3
- HAVAL
- RIPEMD-160
- Tigre

Hash unidireccional

Una función hash toma un mensaje de longitud variable y produce un valor hash de longitud fija. Los valores hash, también denominados resúmenes de mensajes, se calculan utilizando el mensaje original. Si el receptor calcula un valor hash que es el mismo, entonces el mensaje original está intacto. Si el receptor calcula un valor hash que es diferente, entonces el mensaje original ha sido alterado.

Usando una función H dada, la siguiente ecuación debe ser verdadera para asegurar que el mensaje original, M1, no haya sido alterado o reemplazado por un mensaje nuevo, M2:

H (M1) <> H (M2)

Para que un hash unidireccional sea efectivo, la creación de dos mensajes diferentes con el mismo valor hash debe ser matemáticamente imposible. Dado un valor hash, descubrir el mensaje original del que se obtuvo el valor hash debe ser matemáticamenteimposible. Un algoritmo hash unidireccional está libre de colisiones si proporciona protección contra la creación del mismo valor hash a partir de diferentes mensajes.

A diferencia de los algoritmos simétricos y asimétricos, el algoritmo hash es de dominio público. Las funciones hash siempre se realizan en una dirección. Usarlo a la inversa es innecesario.

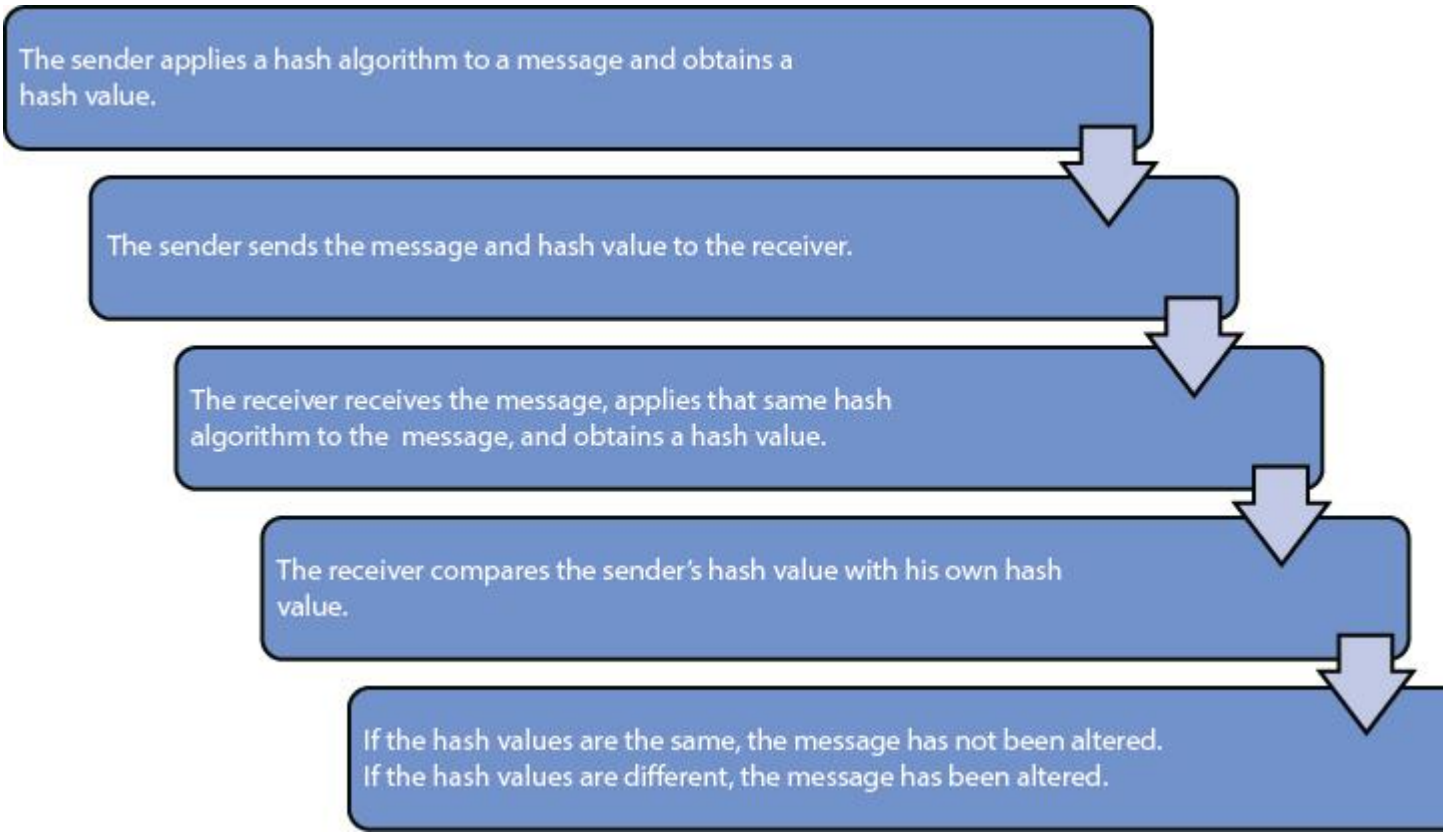
Sin embargo, las funciones hash unidireccionales tienen limitaciones. Si un atacante intercepta un mensaje que contiene un valor hash, el atacante puede alterar el mensaje original para crear un segundo mensaje no válido con un nuevo valor hash. Si el atacante envía el segundo mensaje no válido al destinatario previsto, el destinatario previsto no tendrá forma de saber que recibió un mensaje incorrecto. Cuando el receptor realiza un cálculo del valor de hash, el mensaje no válido parecerá válido porque el mensaje no válido se agregó con el nuevo valor de hash del atacante, no con el valor de hash del mensaje original. Para evitar que esto suceda, el remitente debe utilizar el código de autenticación de mensajes (MAC).

El cifrado de la función hash con un algoritmo de clave simétrica genera una MAC con clave. La clave simétrica no cifra el mensaje original. Se usa solo para proteger el valor hash.

Nota

Los tipos básicos de MAC se describen más adelante en este capítulo.

La figura 3-20 ilustra los pasos básicos de una función hash.



El primer paso en un proceso de función hash es donde el remitente aplica un algoritmo hash a un mensaje y obtiene un valor hash. A continuación, el remitente envía el mensaje y el valor hash al receptor. El tercer paso es que el receptor recibe el mensaje, aplica ese mismo algoritmo hash al mensaje y obtiene un valor hash. El cuarto paso es que el receptor compara el valor hash del remitente con su propio valor hash. El paso final en el proceso de la función hash es si los valores hash son los mismos, el mensaje no ha sido alterado. Si los valores hash son diferentes, el mensaje se ha modificado.

Figura 3-20 Proceso de la función hash

MD2 / MD4 / MD5 / MD6

El algoritmo de resumen de mensajes MD2 produce un valor hash de 128 bits. Realiza 18 rondas de cálculos. Aunque MD2 todavía se usa hoy en día, es mucho más lento que MD4, MD5 y MD6.

El algoritmo MD4 también produce un valor hash de 128 bits. Sin embargo, solo realiza tres rondas de cálculos. Aunque MD4 es más rápido que MD2, su uso ha disminuido significativamente debido a que los ataques contra él han tenido tanto éxito.

Como los otros algoritmos MD, el algoritmo MD5 produce un valor hash de 128 bits. Realiza cuatro rondas de cálculos. Se creó originalmente debido a problemas con MD4 y es más complejo que MD4. Sin embargo, MD5 no está libre de colisiones. Por este motivo, no debe utilizarse para certificados SSL o firmas digitales. El gobierno de EE. UU. Requiere el uso de SHA-2 en lugar de MD5. Sin embargo, en el uso comercial, muchos proveedores de software publican el valor hash MD5 cuando lanzan parches de software para que los clientes puedan verificar la integridad del software después de la descarga.

El algoritmo MD6 produce un valor hash variable, realizando un número variable de cálculos. Aunque originalmente se presentó como candidato para SHA-3, se retiró debido a los primeros problemas que tenía el algoritmo con los ataques diferenciales. Desde entonces, MD6 ha sido relanzado con este problema solucionado. Sin embargo, ese lanzamiento fue demasiado tarde para ser aceptado como el estándar NIST SHA-3.

SHA / SHA-2 / SHA-3

El algoritmo de hash seguro (SHA) es una familia de cuatro algoritmos publicados por el NIST de EE. UU. SHA-0, originalmente denominado simplemente SHA porque no había otros "miembros de la familia", produce un valor hash de 160 bits después de realizar 80 rondas de cálculos en bloques de 512 bits. SHA-0 nunca fue muy popular porque se descubrieron colisiones.

Al igual que SHA-0, SHA-1 produce un valor hash de 160 bits después de realizar 80 rondas de cálculos en bloques de 512 bits. SHA-1 corrigió la falla en SHA-0 que lo hacía susceptible a ataques.

SHA-2 es en realidad una familia de funciones hash, cada una de las cuales proporciona diferentes límites funcionales. La familia SHA-2 es la siguiente:

- **SHA-224:** produce un valor hash de 224 bits después de realizar 64 rondas de cálculos en bloques de 512 bits.
- **SHA-256:** produce un valor hash de 256 bits después de realizar 64 rondas de cálculos en bloques de 512 bits.
- **SHA-384:** produce un valor hash de 384 bits después de realizar 80 rondas de cálculos en bloques de 1.024 bits.
- **SHA-512:** produce un valor hash de 512 bits después de realizar 80 rondas de cálculos en bloques de 1.024 bits.
- **SHA-512/224:** produce un valor hash de 224 bits después de realizar 80 rondas de cálculos en bloques de 1.024 bits. La designación 512 aquí indica el tamaño del estado interno.

- **SHA-512/256:** produce un valor hash de 256 bits después de realizar 80 rondas de cálculos en bloques de 1.024 bits. Una vez más, la designación 512 indica el tamaño del estado interno.

SHA-3, como SHA-2, es una familia de funciones hash. SHA-2 aún no se ha roto. Los tamaños de los valores hash para SHA-3 varían de 224 a 512 bits. Los tamaños de bloque van de 576 a 1152 bits. SHA-3 realiza 120 rondas de cálculos, de forma predeterminada.

Tenga en cuenta que SHA-1 y SHA-2 todavía se utilizan ampliamente en la actualidad. SHA-3 no se desarrolló debido a alguna falla de seguridad con los dos estándares anteriores, sino que se propuso como una función hash alternativa a los demás.

HAVAL

HAVAL es una función unidireccional que produce valores hash de longitud variable, incluidos 128 bits, 160 bits, 192 bits, 224 bits y 256 bits, y utiliza bloques de 1.024 bits. El número de rondas de cálculos puede ser tres, cuatro o cinco. Se han descubierto problemas de colisión si se produce un valor hash de 128 bits con tres rondas de cálculos. Todas las demás variaciones no tienen problemas descubiertos a partir de esta impresión.

RIPEMD-160

Aunque existen varias variaciones de la función hash de RIPEMD, los profesionales de seguridad solo deben preocuparse por RIPEMD-160 para fines de examen. RIPEMD-160 produce un valor hash de 160 bits después de realizar 160 rondas de cálculos en bloques de 512 bits.

Tigre

Tiger es una función hash que produce valores hash de 128, 160 o 192 bits después de realizar 24 rondas de cálculos en bloques de 512 bits, siendo la versión más popular la que produce valores hash de 192 bits. A diferencia de MD5, RIPEMD, SHA-0 y SHA-1, Tiger no se basa en la arquitectura MD4.

Código de autenticación de mensajes

MAC se explicó anteriormente en este capítulo. En esta sección, analizamos los tres tipos de MAC con los que los profesionales de la seguridad deben estar familiarizados:

- HMAC
- CBC-MAC
- CMAC

HMAC

Un MAC hash (HMAC) es un MAC hash con clave que implica una función hash con clave simétrica. HMAC proporciona integridad y autenticación de datos. Cualquiera de las funciones hash enumeradas anteriormente se puede utilizar con HMAC, con el nombre de HMAC adjunto al nombre de la función hash, como en HMAC-SHA-1. La fuerza de HMAC depende de la fuerza de la función hash, incluido el tamaño del valor hash y el tamaño de la clave.

El tamaño de salida del valor hash de HMAC será el mismo que el de la función hash subyacente. HMAC puede ayudar a reducir la tasa de colisión de la función hash.

Los pasos básicos de un proceso HMAC son los siguientes:

1. El remitente y el receptor acuerdan qué clave simétrica utilizar.
2. El remitente une la clave simétrica al mensaje.
3. El remitente aplica un algoritmo hash al mensaje y obtiene un valor hash.
4. El remitente agrega un valor hash al mensaje original y el remitente envía el nuevo mensaje al receptor.
5. El receptor recibe el mensaje y une la clave simétrica al mensaje.
6. El receptor aplica el algoritmo hash al mensaje y obtiene un valor hash.
7. Si los valores hash son los mismos, el mensaje no se ha modificado. Si los valores hash son diferentes, el mensaje se ha modificado.

CBC-MAC

El MAC de encadenamiento de bloques de cifrado (CBC-MAC) es un MAC de cifrado de bloques que funciona en modo CBC. CBC-MAC proporciona integridad y autenticación de datos.

Los pasos básicos de un proceso CBC-MAC son los siguientes:

1. El remitente y el receptor acuerdan qué cifrado de bloque simétrico utilizar.
2. El remitente cifra el mensaje con el cifrado de bloque simétrico en modo CBC. El último bloque es el MAC.
3. El remitente agrega el MAC al mensaje original y el remitente envía el nuevo mensaje al receptor.
4. El receptor recibe el mensaje y lo cifra con el cifrado de bloque simétrico en modo CBC.
5. El receptor obtiene el MAC y lo compara con el MAC del remitente.
6. Si los valores son los mismos, el mensaje no se ha modificado. Si los valores son diferentes, el mensaje se ha modificado.

CMAC

MAC basado en cifrado (CMAC) funciona de la misma manera que CBC-MAC pero con funciones matemáticas mucho mejores. CMAC resuelve algunos problemas de seguridad con CBC-MAC y está aprobado para trabajar con AES y 3DES.

Salazón

Las tablas de búsqueda y las tablas de arco iris funcionan porque cada contraseña se codifica exactamente de la misma manera. Si dos usuarios tienen la misma contraseña, su contraseña es la misma. Para evitar ataques, los profesionales de la seguridad deben asegurarse de que cada hash sea aleatorio. Entonces, cuando la misma contraseña se hash dos veces, los hash no son los mismos.

Salar significa agregar datos aleatoriamente a una función unidireccional que "aplica un hash" a una contraseña o frase de contraseña. La función principal de la salazón es defenderse de los ataques de diccionario frente a una lista de hashes de contraseñas y de los ataques de tablas de arco iris precalculados.

Un profesional de seguridad debe aleatorizar los hash añadiendo o anteponiendo una cadena aleatoria, llamada salt, a la contraseña antes de aplicar el hash. Para comprobar si una contraseña es correcta, el atacante necesita la sal. La sal generalmente se almacena en la base de datos de la cuenta de usuario, junto con el hash, o como parte de la propia cadena de hash.

Un atacante no sabe de antemano cuál será la sal, por lo que no puede calcular previamente una tabla de búsqueda o una tabla de arco iris. Si la contraseña de cada usuario tiene un hash diferente, un ataque de tabla de búsqueda inversa tampoco funciona.

Si se utilizan sales, los profesionales de la seguridad deben asegurarse de que no se reutilicen y no sean demasiado cortas. Se debe generar una nueva sal aleatoria cada vez que un administrador crea una cuenta de usuario o un usuario cambia su contraseña. Una buena regla general es usar una sal del mismo tamaño que la salida de la función hash. Por ejemplo, la salida de SHA-256 es de 256 bits (32 bytes), por lo que la sal debe tener al menos 32 bytes aleatorios.

Las sales deben generarse utilizando un generador de números pseudoaleatorios criptográficamente seguro (CSPRNG). Como sugiere el nombre, un CSPRNG está diseñado para proporcionar un alto nivel de aleatoriedad y es completamente impredecible.

Firmas digitales

Una firma digital es un valor hash cifrado con la clave privada del remitente. Una firma digital proporciona autenticación, no repudio e integridad. Una firma ciega es una forma de firma digital en la que el contenido del mensaje se enmascara antes de firmarlo.

La criptografía de clave pública, que se analiza en la siguiente sección, se utiliza para crear firmas digitales. Los usuarios registran sus claves públicas con una CA, que distribuye un

certificado que contiene la clave pública del usuario y la firma digital de la CA. Lo digitalla firma se calcula mediante la clave pública del usuario y el período de validez se combina con el emisor del certificado y el identificador del algoritmo de firma digital.

Al considerar la criptografía, tenga en cuenta los siguientes hechos:

- El cifrado proporciona confidencialidad.
- El hash proporciona integridad.
- Las firmas digitales proporcionan autenticación, no repudio e integridad.

DSS

El Estándar de firma digital (DSS) es un estándar de seguridad digital federal que gobierna el Algoritmo de seguridad digital (DSA). DSA genera un resumen de mensaje de 160 bits. El gobierno federal de los EE. UU. Requiere el uso de DSA, RSA (discutido anteriormente en este capítulo) o DSA de curva elíptica (ECDSA) y SHA para firmas digitales. DSA es más lento que RSA y solo proporciona firmas digitales. RSA proporciona firmas digitales, cifrado y distribución segura de claves simétricas.

Criptografía aplicada

El cifrado puede proporcionar una protección diferente según el nivel de comunicación que se esté utilizando. Los dos tipos de niveles de comunicación de cifrado son el cifrado de enlace y el cifrado de extremo a extremo. Además, la criptografía se utiliza para la seguridad del correo electrónico e Internet. Estos se tratan en detalle en la sección " Criptografía de comunicaciones " en el Capítulo 4 .

Cifrado de enlaces versus cifrado de un extremo a otro

El cifrado de enlace cifra todos los datos que se transmiten a través de un enlace. El cifrado de extremo a extremo cifra menos información del paquete que el cifrado de enlace.

Seguridad del correo electrónico

Los métodos de seguridad del correo electrónico incluyen los estándares de correo electrónico PGP, MIME y S / MIME que son populares en el mundo actual.

seguridad de Internet

La seguridad de Internet incluye acceso remoto; SSL / TLS; HTTP, HTTPS y S-HTTP; COLOCAR; galletas; SSH; e IPsec e ISAKMP.

Ataques criptoanalíticos

Los ataques de criptografía se clasifican en ataques pasivos o activos. Un ataque pasivo generalmente se implementa solo para descubrir información y es mucho más difícil de detectar

porque generalmente se lleva a cabo mediante escuchas ilegales o rastreo de paquetes. Los ataques activos involucran a un atacante que realmente lleva a cabo pasos, como la alteración de mensajes o la modificación de archivos. La criptografía generalmente se ataca a través de la clave, el algoritmo, la ejecución, los datos o las personas. Pero la mayoría de estos ataques intentan descubrir la clave utilizada.

Los ataques de criptografía que se analizan incluyen los siguientes:

- Ataque de solo texto cifrado
- Ataque de texto sin formato conocido
- Ataque de texto plano elegido
- Ataque de texto cifrado elegido
- Ingeniería social
- Fuerza bruta
- Criptoanálisis diferencial
- Criptoanálisis lineal
- Ataque algebraico
- Análisis de frecuencia
- Ataque de cumpleaños
- Ataque de diccionario
- Repetir ataque
- Ataque analítico
- Ataque estadístico
- Ataque de factoring
- Ingeniería inversa
- Ataque de encuentro en el medio
- Ataque de ransomware
- Ataque de canal lateral

Ataque de solo texto cifrado

En un ataque de solo texto cifrado, un atacante utiliza varios mensajes cifrados (texto cifrado) para averiguar la clave utilizada en el proceso de cifrado. Aunque es un tipo de ataque muy común, generalmente no tiene éxito porque se sabe muy poco sobre el cifrado utilizado.

Ataque de texto plano conocido

En un ataque de texto plano conocido, un atacante utiliza las versiones de texto plano y cifrado de un mensaje para descubrir la clave utilizada. Este tipo de ataque implementa ingeniería inversa, análisis de frecuencia o fuerza bruta para determinar la clave de modo que se puedan descifrar todos los mensajes.

Ataque de texto plano elegido

En un ataque de texto sin formato elegido, un atacante elige el texto sin formato a cifrar para obtener el texto cifrado. El atacante envía un mensaje con la esperanza de que el usuario reenvíe

ese mensaje como texto cifrado a otro usuario. El atacante captura la versión de texto cifrado del mensaje e intenta determinar la clave comparando la versión de texto sin formato que originó con la versión de texto cifrado capturada. Una vez más, el descubrimiento de claves es el objetivo de este ataque.

Ataque de texto cifrado elegido

Un ataque de texto cifrado elegido es lo opuesto a un ataque de texto plano elegido. En un ataque de texto cifrado elegido, un atacante elige el texto cifrado que se descifrará para obtener el texto sin formato. Este ataque es más difícil porque se necesita el control del sistema que implementa el algoritmo.

Ingeniería social

Los ataques de ingeniería social contra algoritmos criptográficos no difieren mucho de los ataques de ingeniería social contra cualquier otra área de seguridad. Los atacantes intentan engañar a los usuarios para que le den al atacante la clave criptográfica utilizada. Los métodos comunes de ingeniería social incluyen la intimidación, la tentación o el estímulo.

Fuerza bruta

Al igual que con un ataque de fuerza bruta contra contraseñas, un ataque de fuerza bruta ejecutado contra un algoritmo criptográfico utiliza todas las claves posibles hasta que se descubre una clave que descifra con éxito el texto cifrado. Este ataque requiere un tiempo y una potencia de procesamiento considerables y es muy difícil de completar.

Criptoanálisis diferencial

El criptoanálisis diferencial mide los tiempos de ejecución y la potencia requerida por el dispositivo criptográfico. Las medidas ayudan a detectar la clave y el algoritmo utilizados.

Criptoanálisis lineal

El criptoanálisis lineal es un ataque de texto plano conocido que utiliza aproximación lineal, que describe el comportamiento del cifrado en bloque. Un atacante tiene más éxito con este tipo de ataque cuando se obtienen más mensajes de texto sin formato y de texto cifrado coincidente.

Ataque algebraico

Los ataques algebraicos se basan en el álgebra que utilizan los algoritmos criptográficos. Si un atacante explota vulnerabilidades conocidas del álgebra utilizada, buscar esas vulnerabilidades puede ayudar al atacante a determinar la clave y el algoritmo utilizados.

Análisis de frecuencia

El análisis de frecuencia es un ataque que se basa en el hecho de que los cifrados de sustitución y transposición darán como resultado patrones repetidos en el texto cifrado. Reconocer los patrones de 8 bits y contarlos puede permitir que un atacante utilice la sustitución inversa para obtener el mensaje de texto sin formato.

El análisis de frecuencia generalmente implica la creación de un cuadro que enumera todas las letras del alfabeto junto con el número de veces que aparece esa letra. Entonces, si la letra Q en las listas de frecuencias tiene el valor más alto, existe una buena posibilidad de que esta letra sea en realidad E en el mensaje de texto sin formato porque E es la letra más utilizada en el idioma inglés. La letra de texto cifrado se reemplaza en el texto cifrado con la letra de texto sin formato.

Los algoritmos actuales se consideran demasiado complejos para ser susceptibles a este tipo de ataque.

Ataque de cumpleaños

Un ataque de cumpleaños utiliza la premisa de que encontrar dos mensajes que den como resultado el mismo valor hash es más fácil que hacer coincidir un mensaje y su valor hash. La mayoría de los algoritmos hash pueden resistir simples ataques de cumpleaños.

Ataque de diccionario

Similar a un ataque de fuerza bruta, un ataque de diccionario utiliza todas las palabras en un diccionario hasta que se descubre una clave que descifra con éxito el texto cifrado. Este ataquerequiere un tiempo y una potencia de procesamiento considerables y es muy difícil de completar. También requiere un diccionario completo de palabras.

Repetir ataque

En un ataque de repetición, un atacante envía los mismos datos repetidamente en un intento de engañar al dispositivo receptor. Estos datos suelen ser información de autenticación. Las mejores contramedidas contra este tipo de ataque son las marcas de tiempo y los números de secuencia.

Ataque analítico

En los ataques analíticos, los atacantes utilizan debilidades o fallas estructurales conocidas para determinar el algoritmo utilizado. Si se puede aprovechar una debilidad o falla en particular, es más probable que se utilice un algoritmo en particular.

Ataque estadístico

Mientras que los ataques analíticos buscan debilidades o fallas estructurales, los ataques estadísticos utilizan debilidades estadísticas conocidas de un algoritmo para ayudar en el ataque.

Ataque de factorización

Se lleva a cabo un ataque de factorización contra el algoritmo RSA utilizando las soluciones de factorización de números grandes.

Ingeniería inversa

Uno de los ataques criptográficos más populares, la ingeniería inversa, ocurre cuando un atacante compra un producto criptográfico en particular para intentar aplicar ingeniería inversa al producto para descubrir información confidencial sobre el algoritmo criptográfico utilizado.

Ataque de encuentro en el medio

En un ataque de encuentro en el medio, un atacante intenta romper el algoritmo cifrando desde un extremo y descifrando desde el otro para determinar el problema matemático utilizado.

Ataque de ransomware

En un ataque de ransomware, un usuario instala accidentalmente un programa que permite a un atacante cifrar archivos o carpetas en la computadora del usuario. Para obtener acceso a los archivos y carpetas que están encriptados, el usuario debe pagar una multa para obtener acceso a sudatos. Dos de las variantes más recientes de este tipo de ataque son el CryptoLocker, que se dirigió a las computadoras con Windows y los archivos adjuntos de correo electrónico infectados mediante un troyano, y WannaCry, que también se dirigió a las computadoras con Windows y exigió el pago en Bitcoin.

Ataque de canal lateral

En un ataque de canal lateral, se obtiene información de la implementación de un sistema informático, en lugar de explotar una debilidad en el algoritmo en sí. Las áreas que se explotan incluyen la memoria caché, la sincronización, la acústica y la remanencia de datos de la computadora. Por lo general, implica monitorear la comunicación dentro de los diferentes componentes de la computadora para determinar la clave secreta.

Gestión de derechos digitales

La gestión de derechos digitales (DRM) se trata en el Capítulo 1 . Para la arquitectura y la ingeniería de seguridad, los profesionales de seguridad deben asegurarse de que las organizaciones empleen políticas y procedimientos de DRM para proteger la propiedad intelectual, incluidos documentos, música, películas, videojuegos y libros electrónicos.

Las implementaciones de DRM de hoy incluyen lo siguiente:

- Directorios:
    - Protocolo ligero de acceso a directorios (LDAP)
    - Directorio activo (AD)
    - Personalizado
- Permisos:

    - Abierto
    - Impresión
    - Modificar
    - Portapapeles
- Controles adicionales:
    - Caducidad (revocación absoluta, relativa, inmediata)
    - Control de versiones
    - Cambiar la política de los documentos existentes
    - Marca de agua
    - Conectado desconectado
    - Revisión de cuentas
- Procesos estructurados y ad hoc:
    - Usuario iniciado en el escritorio
    - Mapeado al sistema
    - Integrado en el proceso de flujo de trabajo

DRM de documento

Las organizaciones implementan DRM para proteger documentos y datos confidenciales o sensibles. Los productos DRM comerciales permiten a las organizaciones proteger documentos e incluyen la capacidad de restringir y auditar el acceso a los documentos. Algunos de los permisos que se pueden restringir con los productos DRM incluyen leer y modificar un archivo, eliminar y agregar marcas de agua, descargar y guardar un archivo, imprimir un archivo o incluso tomar capturas de pantalla. Si se implementa un producto DRM, la organización debe asegurarse de que el administrador esté debidamente capacitado y de que existan políticas para garantizar que los derechos se otorguen y revoquen de manera adecuada.

Música DRM

DRM se ha utilizado en la industria de la música desde hace algún tiempo. Los servicios de música basados en suscripción, como Napster, utilizan DRM para revocar el acceso de un usuario a la música descargada una vez que expira su suscripción. Si bien las empresas de tecnología han solicitado a la industria de la música que les permita vender música sin DRM, la industria se ha mostrado reacia a hacerlo.

DRM de película

Si bien la industria del cine ha utilizado una variedad de esquemas de DRM a lo largo de los años, se utilizan dos tecnologías principales para la distribución masiva de medios:

- **Content Scrambling System (CSS):** utiliza cifrado para hacer cumplir las restricciones de reproducción y región en los DVD. Este sistema se puede romper con la herramienta DeCSS de Linux.
- **Sistema de contenido de acceso avanzado (AACS):** protege el contenido de Blu-ray y HD DVD. Los piratas informáticos han podido obtener las claves de cifrado de este sistema.

Esta industria continúa avanzando para evitar que los piratas informáticos creen copias no cifradas de material protegido por derechos de autor.

DRM de videojuegos

La mayoría de las implementaciones de DRM de videojuegos se basan en consolas propietarias que utilizan conexiones a Internet para verificar las licencias de los videojuegos. La mayoría de las consolas actuales verificanlicencia en el momento de la instalación y permite el uso sin restricciones desde ese punto. Sin embargo, para obtener actualizaciones, se volverá a verificar la licencia antes de descargar e instalar la actualización.

DRM de libros electrónicos

La DRM de libros electrónicos se considera la implementación de DRM más exitosa. Tanto el Kindle de Amazon como los dispositivos Nook de Barnes and Nobles implementan DRM para proteger los formatos electrónicos de los libros. Ambas empresas han lanzado aplicaciones móviles que funcionan como dispositivos físicos de libros electrónicos.

La implementación de hoy utiliza una clave de descifrado que está instalada en el dispositivo. Esto significa que los libros electrónicos no se pueden copiar fácilmente entre dispositivos o aplicaciones de libros electrónicos. Adobe creó la tecnología de protección de la experiencia digital de Adobe (ADEPT) que utilizan la mayoría de los lectores de libros electrónicos, excepto el Kindle de Amazon. Con ADEPT, AES se utiliza para cifrar el contenido multimedia y RSA cifra la clave AES.

Diseño de instalaciones y emplazamientos

Para muchas organizaciones con visión de futuro, las consideraciones de seguridad física comienzan durante la selección y el diseño del sitio. Estas empresas han aprendido que incorporar seguridad es más fácil que parchear la seguridad a posteriori. En esta sección, se tratan las prácticas de selección y construcción de sitios que pueden conducir a una mayor seguridad física.

Modelo de defensa en capas

Toda la seguridad física debe basarse en un modelo de defensa en capas. En tal modelo, la confianza no debe basarse en un solo concepto de seguridad física, sino en el uso de múltiples enfoques que se apoyan entre sí. La teoría es que si falla un nivel de defensa (digamos, por ejemplo, seguridad perimetral), otra capa servirá como respaldo (como cerraduras en la puerta de la sala de servidores). La superposición de los conceptos discutidos en este capítulo puede fortalecer la seguridad física general.

CPTED

La prevención del delito a través del diseño ambiental (CPTED) se refiere al diseño de una instalación desde cero para respaldar la seguridad. En realidad, es un concepto amplio que se

puede aplicar a cualquier proyecto (urbanizaciones, edificios de oficinas y establecimientos comerciales). Aborda la entrada del edificio, el paisajismo y el diseño de interiores. Tiene como objetivo crear efectos conductuales que reduzcan la delincuencia. Las tres estrategias principales que guían a CPTED se tratan en esta sección.

Control de acceso natural

El concepto de control de acceso natural se aplica a las entradas de la instalación. Abarca la colocación de puertas, luces, vallas e incluso paisajismo. Su objetivo es satisfacer los objetivos de seguridad de la manera menos molesta y estéticamente atractiva. En muchos casos, se puede diseñar un solo objeto para cumplir con múltiples objetivos de seguridad.

Por ejemplo, muchos edificios tienen bolardos o postes grandes en el frente del edificio con luces encendidas. Estos objetos sirven para varios propósitos. Protegen la entrada del edificio de los coches que entran en ella. Las luces también iluminan la entrada y desalientan el crimen, y finalmente pueden guiar a las personas hacia la entrada.

El control de acceso natural también fomenta la idea de crear zonas de seguridad en el edificio. Estas áreas se pueden etiquetar y luego se pueden usar sistemas de tarjetas para evitar el acceso a áreas más sensibles. Este concepto también fomenta la minimización de los puntos de entrada y un control estricto sobre esos puntos de entrada. También fomenta una entrada separada en la parte posterior para los proveedores que no está disponible o no es muy visible para el público.

Vigilancia natural

La vigilancia natural es el uso de características ambientales físicas para promover la visibilidad de todas las áreas y así desalentar el crimen en esas áreas. La idea es fomentar el flujo de personas de manera que el mayor porcentaje posible del edificio esté siempre poblado, porque la gente de una zona desalienta la delincuencia. También intenta maximizar la visibilidad de todas las áreas.

Natural Territoriales Reinforcement

El objetivo del refuerzo de los territorios naturales es crear un sentimiento de comunidad en la zona. Intenta extender el sentido de propiedad a los empleados. También intenta hacer que los posibles infractores sientan que sus actividades corren el riesgo de ser descubiertas. Esto a menudo se implementa en forma de paredes, cercas, paisajismo y diseño de luces.

Plan de seguridad física

Otro aspecto importante del diseño del sitio y de las instalaciones es la convergencia adecuada entre el diseño físico y el plan de seguridad físico. No siempre es posible lograr todos los objetivos de CPTED y, en los casos en que existan brechas, el plan de seguridad física debe incluir políticas y / o procedimientos diseñados para cerrar las brechas. El plan debe abordar los siguientes problemas.

Disuadir la actividad delictiva

Tanto el diseño como las políticas de apoyo deben disuadir la actividad delictiva. Por ejemplo, la mayor cantidad de áreas posibles deben estar abiertas y verse fácilmente. Debería haber unmínimo de áreas aisladas y oscurecidas. La señalización que indica cámaras o monitoreo en el sitio y la presencia de guardias también pueden servir como elementos disuasorios.

Retrasar intrusos

Otra característica beneficiosa del plan de seguridad física es agregar impedimentos a la entrada, como cerraduras, vallas y barreras. Cualquier procedimiento que ralentice y controle la entrada de personas a las instalaciones también puede ayudar. Cuanto más se demore el intruso, es menos probable que elija la instalación y más probabilidades hay de que lo atrapen.

Detectar intrusos

Deben existir sistemas y procedimientos que permitan detectar la actividad delictiva. Los sensores de movimiento, las cámaras y similares son todas formas de detección de intrusos. Registrar a todos los visitantes también podría ser una forma de disuasión.

Evaluar la situación

El plan debe identificar al personal específico y las acciones que se tomarán cuando ocurra un evento. Puede resultar beneficioso compilar una lista de tipos de incidentes que indiquen una respuesta, un tiempo de respuesta y nombres de contacto aceptables. Los planes escritos desarrollados con anticipación brindan una respuesta mucho más efectiva y consistente.

Responder a intrusiones e interrupciones

El plan también debe intentar anticipar y desarrollar respuestas apropiadas a los intrusos y a las interrupciones comunes (cortes de energía, problemas de servicios públicos, etc.). Aunque anticipar cada evento potencial es imposible, debería ser factible crear una lista que cubra posibles intrusiones e interrupciones. Luego, se pueden desarrollar respuestas escritas para asegurar una respuesta consistente y predecible a estos eventos por parte de todo el personal.

Problemas de selección de instalaciones

Cuando una organización se muda a una nueva instalación o amplía una existente, es una gran oportunidad para incluir problemas de seguridad física en el proceso de selección del sitio o en el plan de expansión. En esta sección, analizamos algunos elementos críticos para considerar si se presenta esta oportunidad.

Visibilidad

La cantidad de visibilidad deseada depende de la organización y los procesos que se llevan a cabo en la instalación. En algunos casos, es beneficioso tener una alta visibilidad de la ubicación

para ayudar a promover la marca o para la conveniencia de los clientes. En otros casos, se desea un perfil más bajo cuando se llevan a cabo operaciones sensibles. CuándoEste es el caso, se debe considerar la probabilidad de escuchas desde fuera de la instalación a través de las ventanas. También es importante tener en cuenta las áreas comunes. Si es posible, estas áreas no deben aislarse ni oscurecerse. Colóquelos en áreas visibles con iluminación para desalentar el crimen. Esto incluye pasillos, estacionamientos y otras áreas compartidas.

Nota

Los controles de seguridad perimetral, incluida la iluminación, las cercas y la detección de intrusiones perimetrales, se tratan con más profundidad en el Capítulo 7 .

Entidades circundantes y externas

También es importante tener en cuenta el entorno en el que se encuentra la instalación. ¿Qué tipo de barrio es? ¿Es un área que tiene una alta tasa de criminalidad o está aislada? El aislamiento puede ser bueno, pero también invita a la delincuencia que puede pasar desapercibida durante un período de tiempo más largo. También considere la distancia a las estaciones de policía, instalaciones médicas y estaciones de bomberos. Finalmente, considere la naturaleza de las operaciones de las empresas circundantes. ¿Representan algún tipo de amenaza para sus operaciones?

Accesibilidad

Se debe tener en cuenta la facilidad con la que los empleados y funcionarios pueden acceder a las instalaciones. ¿Cuáles son las condiciones de tráfico que encontrarán los empleados? Si se trata de una instalación nueva que reemplaza a una antigua, ¿es inconveniente para la mayoría de los empleados? ¿Corre el riesgo de perder empleados durante el viaje? ¿Es esta ubicación conveniente para las opciones de transporte, como estaciones de tren y aeropuertos? Si sus empleados requieren muchos viajes, la accesibilidad podría ser importante. Si a menudo recibe a empleados de otras ubicaciones de forma temporal o recibe a socios comerciales, ¿hay alojamientos seguros cerca?

Construcción

Los materiales utilizados para construir una instalación son otro tema crítico. Pero las cuestiones a considerar aquí no se limitan simplemente a la composición de las paredes y los techos, aunque eso es crucial. Los sistemas de soporte integrados en el edificio también son importantes e incluyen lo siguiente:

- Paredes
- Puertas
- Techos
- Ventanas
- Piso
- HVAC

- Fuente de alimentación
- Utilidades
- Detección y extinción de incendios

Algunas consideraciones especiales incluyen las siguientes:

- Según (ISC) [2] , todas las paredes deben tener una clasificación mínima de resistencia al fuego de dos horas.
- Las puertas deben resistir la entrada a la fuerza.
- Se debe conocer la ubicación y el tipo de los sistemas de extinción de incendios.
- El piso de las salas de servidores y los armarios de cableado deben elevarse para ayudar a mitigar los daños por inundaciones.
- Deben existir fuentes de energía alternativas y de respaldo.
- Se deben dedicar unidades de aire acondicionado separadas y se debe controlar la calidad / humedad del aire para los centros de datos y las salas de computadoras.

Compartimentos internos

En muchas áreas de una instalación, las particiones se utilizan para separar áreas de trabajo. Estas particiones, aunque parecen ser paredes, no son paredes completas en el sentido de que no se extienden hasta el techo. Cuando este enfoque de construcción se combina con un falso techo, también común en muchos edificios, existe una oportunidad para que alguien acceda a una habitación contigua a través del falso techo. Todas las habitaciones que deben asegurarse, como las salas de servidores y los armarios de cableado, no deben tener este tipo de paredes.

Salas de Computadoras y Equipos

Si bien estamos en el tema de las salas que contienen equipos al que se debe controlar el acceso físico, como las que contienen servidores sensibles y equipos de red cruciales, las salas de computadoras y equipos deben estar cerradas con llave en todo momento y aseguradas y equipadas con las siguientes medidas de seguridad:

- Ubique las salas de computadoras y equipos en el centro del edificio, cuando sea posible.
- Las salas de computadoras y equipos deben tener una puerta de acceso única o un punto de entrada.
- Evite los pisos superiores de los edificios para salas de computadoras y equipos.
- Instale y pruebe con frecuencia sistemas de detección y extinción de incendios.
- Instale piso elevado.
- Instale fuentes de alimentación separadas para las salas de computadoras y equipos cuando sea posible.
- Utilice solo puertas sólidas.

Controles de seguridad del sitio y de las instalaciones

Aunque la seguridad del perímetro es importante, la seguridad dentro del edificio también es importante según lo prescrito en el modelo de círculo concéntrico. Esta sección cubre temas que afectan el interior de la instalación.

Puertas

Se pueden utilizar una variedad de tipos de puertas y materiales de puertas en los edificios. Pueden ser huecos, que se utilizan dentro del edificio, o sólidos, normalmente utilizados en el borde del edificio y en lugares donde se requiere seguridad adicional. Algunos tipos de puertas con los que un profesional de seguridad debería estar familiarizado y preparado para seleccionar para protección son

- **Puertas de bóveda:** conducen a cajas fuertes o salas de seguridad
- **Puertas de personal:** utilizadas por humanos para ingresar a la instalación
- **Puertas industriales: Puertas** grandes que permiten el acceso a vehículos más grandes.
- **Puertas de acceso de vehículos:** Puertas a edificios o lotes de estacionamiento
- Puertas a prueba de **balas:** puertas diseñadas para resistir armas de fuego

Tipos de cerradura de puerta

Las cerraduras de las puertas pueden ser mecánicas o electrónicas. Las cerraduras eléctricas o las cerraduras cifradas utilizan un teclado que requiere el código correcto para abrir la cerradura. Estos son programables y las organizaciones que los utilizan deben cambiar la contraseña con frecuencia. Otro tipo de sistema de seguridad de la puerta es un dispositivo de autenticación de proximidad, con el que se utiliza una tarjeta programable para entregar un código de acceso al dispositivo, ya sea deslizando la tarjeta o, en algunos casos, simplemente estando cerca del lector. Estos dispositivos suelen contener los siguientes componentes de control de acceso electrónico (EAC):

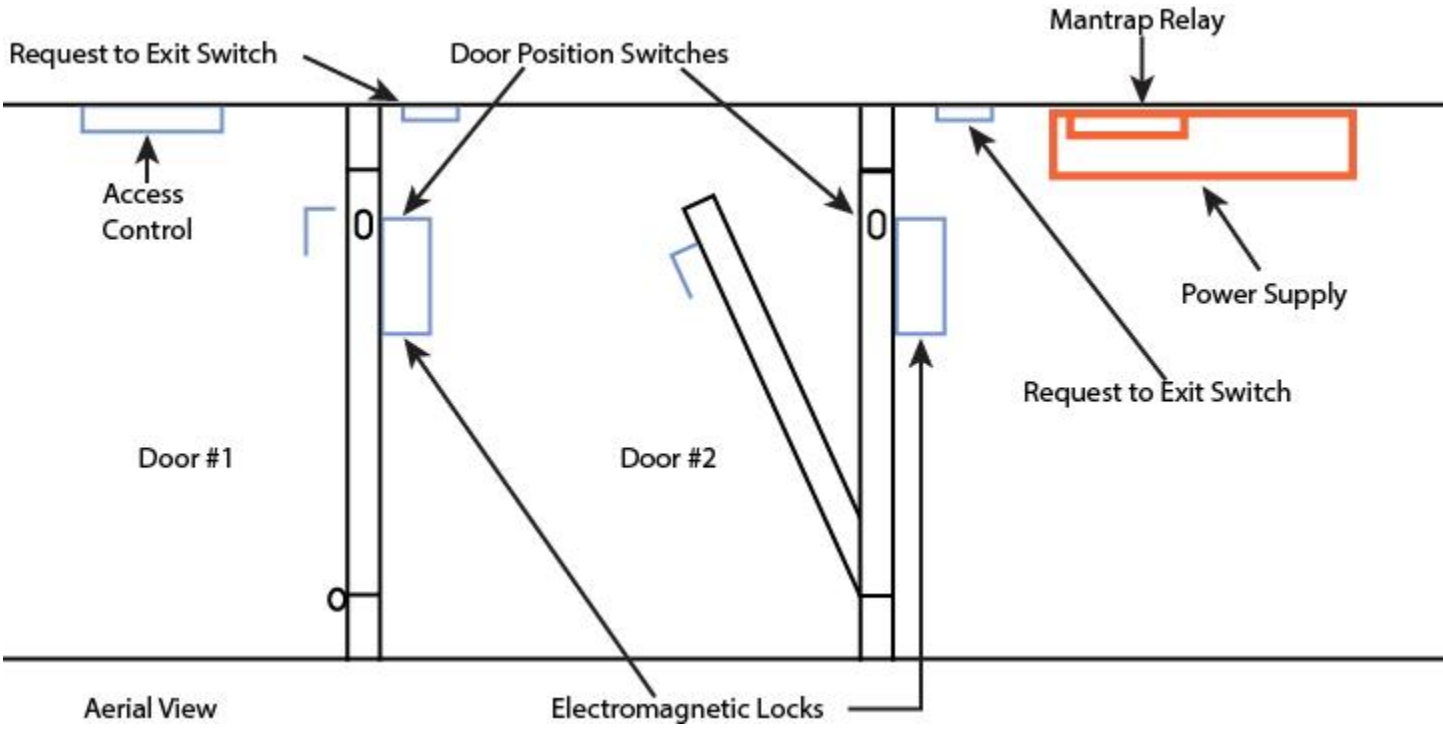
- Una cerradura electromagnética
- Un lector de credenciales
- Un sensor de puerta cerrada

Torniquetes y Mantraps

Dos tipos especiales de dispositivos de control de acceso físico, mantraps y torniquetes, también requieren mención. Aunque es posible que esté familiarizado con un torniquete, que se puede abrir escaneando o deslizando una tarjeta de acceso, un mantrap es un sistema inusual con el que quizás no esté familiarizado.

Un mantrap es una serie de dos puertas con una pequeña habitación entre ellas. El usuario se autentica en la primera puerta y luego se le permite ingresar a la habitación. En ese punto, se produce una verificación adicional (como un guardia que identifica visualmente a la persona) y luego se le permite pasar por la segunda puerta. Estas puertas se utilizan normalmente solo en situaciones de muy alta seguridad. Los Mantraps también suelen requerir que la primera puerta

esté cerrada antes de permitir que se abra la segunda puerta. La figura 3-21 muestra un diseño de mantra.



Hay dos puertas, puerta número 1 y puerta número 2. Ambas puertas están equipadas con cerraduras electromagnéticas e interruptores de posición de puerta. Junto a la puerta 1, hay un interruptor de control de acceso. Después de cada puerta, hay una solicitud para salir del interruptor. Más allá de la segunda puerta, hay una fuente de alimentación y un relé mantrap.

Figura 3-21 Mantrap

Cerraduras

Las cerraduras también se utilizan en lugares distintos de las puertas, como armarios de protección y dispositivos de seguridad. Los tipos de cerraduras mecánicas con las que debería estar familiarizado son

- **Cerraduras protegidas:** tienen un cerrojo con resorte con una muesca. La cerradura tiene pabellones o saliente metálico dentro de la cerradura con el que la llave coincidirá y permitirá abrir la cerradura. En la Figura 3-22 se muestra un diseño de candado protegido .

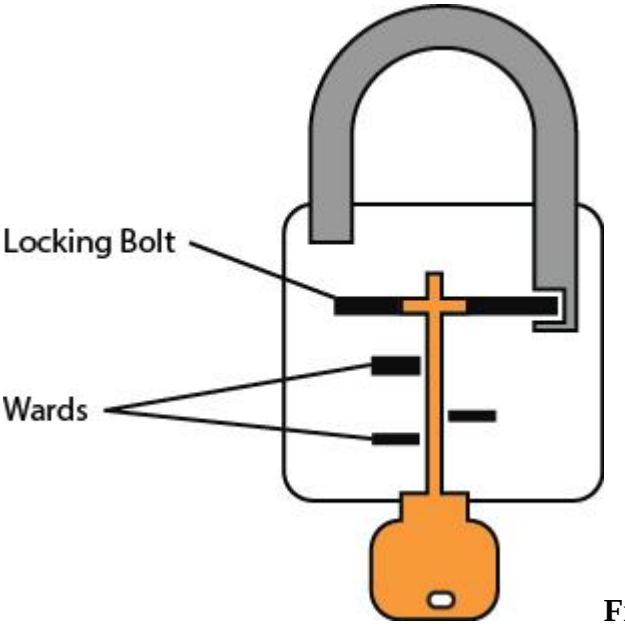


Figura 3-22 Cerradura protegida

- **Cerraduras de tambor:** tienen más partes móviles que la cerradura protegida, y la llave eleva la pieza de metal de la cerradura a la altura correcta. En la Figura 3-23 se muestra un diseño de cerradura de tambor .

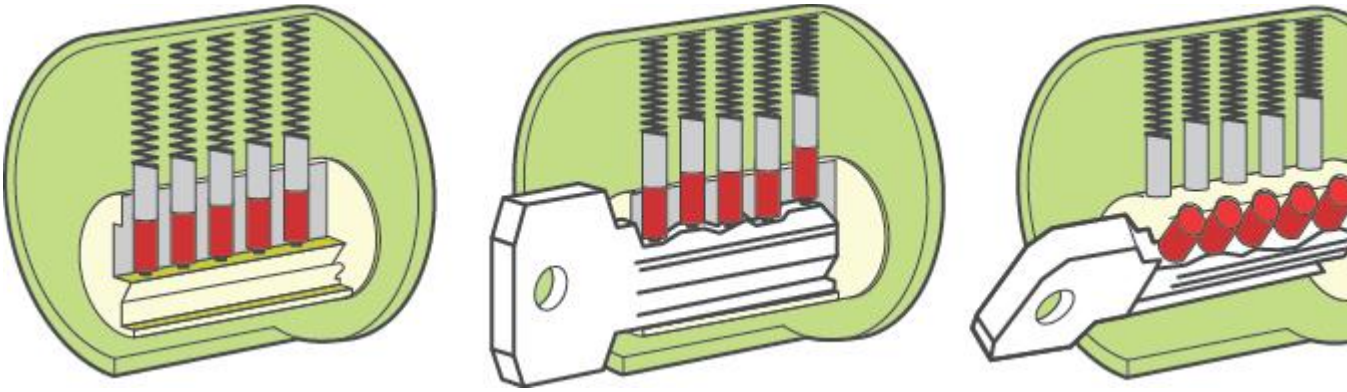
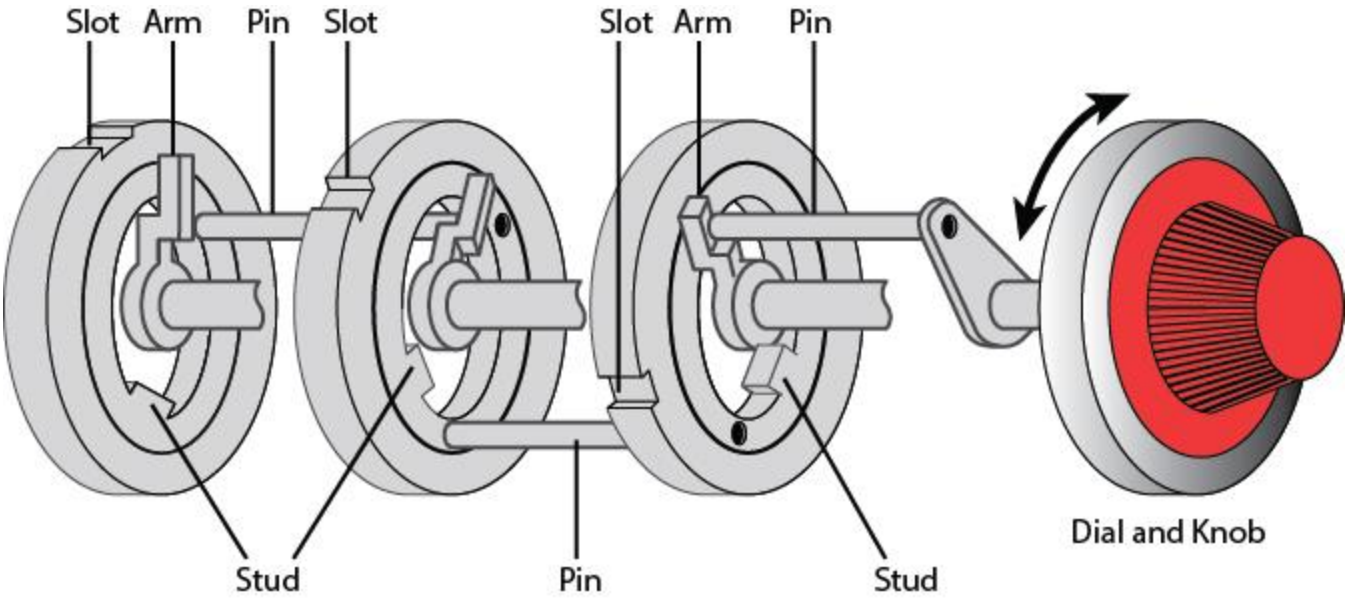


Figura 3-23 Bloqueo de vaso

- **Cerraduras de combinación:** requieren girar la cerradura en un patrón que, si es correcto, alinee las secadoras y abra la cerradura. En la Figura 3-24 se muestra un diseño de candado con combinación .



Cada unidad de una cerradura de combinación tiene una ranura, un brazo y un perno. Las unidades están conectadas entre sí mediante un pin. Al final, hay un dial y una perilla que pueden girar en ambas direcciones. Las unidades requieren girar la cerradura en un patrón para que, cuando la combinación sea correcta, alinee las secadoras, abriendo la cerradura.

Figura 3-24 Candado de combinación

En el caso de los bloqueos de dispositivos, las computadoras portátiles son el elemento principal que debe protegerse porque son muy fáciles de robar. Las computadoras portátiles nunca deben dejarse al aire libre sin estar aseguradas a algo sólido con un candado de cable. Estos son cables de acero recubiertos de vinilo que se conectan a la computadora portátil y luego se bloquean alrededor de un objeto.

Biometria

El nivel más alto de control de acceso físico y el más caro de implementar es un dispositivo biométrico. Los dispositivos biométricos se tratan ampliamente en el Capítulo 5 .

Entradas de vidrio

Las entradas de vidrio, que se han vuelto comunes en muchas instalaciones, incluyen ventanas, puertas de vidrio y paredes de vidrio. Se debe seleccionar el vidrio adecuado para la situación. Un profesional de seguridad debe estar familiarizado con los siguientes tipos de vidrio:

- **Estándar: se** usa en áreas residenciales y se rompe fácilmente
- **Templado:** creado calentando el vidrio, lo que le da una resistencia adicional.
- **Acrílico:** Hecho de policarbonato acrílico; es mucho más fuerte que el vidrio normal pero produce humos tóxicos cuando se quema

- **Laminado:** Dos hojas de vidrio con una película de plástico entre ellas, lo que dificulta su rotura.

En áreas donde se debe usar vidrio normal pero la seguridad es una preocupación, se puede usar vidrio incrustado con alambre para reducir la probabilidad de rotura y entrada. Una opción aún más fuerte es complementar las ventanas con barras de acero.

Control de visitantes

Debe existir algún sistema para identificar a los visitantes y controlar su acceso a las instalaciones. El mejor sistema es tener una persona presente para requerir que todos los visitantes se registren antes de ingresar. Si eso no es factible, otra opción es proporcionar un punto de entrada en el que se presente a los visitantes una puerta cerrada con llave y un teléfono que se pueda usar para llamar y solicitar acceso. Cualquiera de estos métodos ayuda a evitar que personas no autorizadas simplemente entren al edificio y vayan a donde quieran.

Otra buena práctica con respecto a los visitantes es acompañar siempre a un contratista o visitante a su destino para asegurarse de que no vayan a donde no deberían. En situaciones de baja seguridad, esta práctica puede no ser necesaria, pero se recomienda en áreas de alta seguridad. Finalmente, registre todas las visitas.

Armarios de cableado / instalaciones de distribución intermedia

Cierre todas las áreas donde se almacene el equipo y controle el acceso a ellas. También es importante tener un inventario estricto de todo el equipo para que se pueda descubrir el robo. Para los centros de datos y las salas de servidores, el listón se eleva aún más. Habrá más sobre este tema más adelante en esta sección.

Areas de trabajo

Debe haber algún sistema para separar áreas por seguridad. En esta sección se analizan algunos lugares específicos donde se pueden requerir medidas de seguridad adicionales. La mayoría de estas medidas se aplican tanto a los visitantes como a los empleados. Prohibir a algunos empleados en determinadas áreas puede resultar beneficioso.

Centro de datos seguro

Los centros de datos deben estar físicamente asegurados con sistemas de bloqueo y no deben tener falsos techos. Las siguientes son algunas consideraciones adicionales para las salas que contienen muchos equipos costosos:

- No deben ubicarse en los pisos superiores ni en los sótanos.
- Debe haber un interruptor de apagado cerca de la puerta para facilitar el acceso.
- Se recomienda HVAC independiente para estas habitaciones.
- Se debe implementar un monitoreo ambiental para alertar sobre problemas de temperatura o humedad.

- Los pisos deben elevarse para ayudar a prevenir daños por agua.
- Todos los sistemas deben tener un UPS con toda la habitación conectada a un generador.

Área de trabajo restringida

La instalación puede tener áreas que deben estar restringidas solo a los trabajadores involucrados, incluso a otros empleados. En estos casos, los sistemas de acceso físico deben implementarse utilizando tarjetas inteligentes, lectores de proximidad, teclados o cualquiera de los otros mecanismos de acceso físico descritos en este libro.

Cuarto de servicio

Algunas empresas más pequeñas implementan una sala de servidores en lugar de un centro de datos seguro. Los controles de seguridad física necesarios para una sala de servidores son similares a los que se implementan en un centro de datos seguro o en un área de trabajo restringida.

Instalaciones de almacenamiento de medios

Una instalación de almacenamiento de medios es un edificio o un área segura dentro de un edificio donde se almacenan los medios. Debido a que los medios pueden venir en una variedad de formas, las organizaciones deben determinar qué medios de almacenamiento utilizarán antes de seleccionar una instalación de almacenamiento de medios. Si solo se almacenan cintas o medios ópticos, podría ser suficiente instalar una caja fuerte a prueba de fuego en el centro de datos existente de una organización y almacenar una copia de respaldo en una ubicación remota. Sin embargo, en algunos casos, es necesaria una solución mucho mayor debido a la cantidad de datos que se están protegiendo. Si se necesita una instalación de almacenamiento de medios separada, la organización debe asegurarse de que la instalación proporcione la seguridad física adecuada para proteger los medios almacenados allí.

Almacenamiento de pruebas

Si una organización ha recopilado evidencia que es crucial para una investigación, la organización debe asegurarse de que la evidencia esté protegida contra el acceso de usuarios no autorizados. Solo el personal involucrado en la investigación debe tener acceso a las pruebas almacenadas. La evidencia debe almacenarse en una habitación cerrada con llave y el acceso a la evidencia debe registrarse. Las pruebas deben entregarse a las fuerzas del orden en el momento adecuado. Si se retienen copias de seguridad de la evidencia digital durante la investigación, las copias de seguridad también deben estar en un área de almacenamiento segura con acceso limitado para el personal.

Seguridad ambiental

Aunque la mayoría de las consideraciones relativas a la seguridad giran en torno a la prevención de daños, la prevención de daños a los datos y al equipo a causa de las condiciones ambientales

también es responsabilidad del equipo de seguridad porque aborda la parte de disponibilidad de la tríada CIA. En esta sección, se tratan algunas de las consideraciones más importantes.

Protección contra incendios

La protección contra incendios tiene una historia más larga que muchos de los temas discutidos en este libro, y aunque las consideraciones tradicionales sobre la prevención de incendios y daños por incendios siguen siendo válidas, la presencia de equipos informáticos sensibles requiere diferentes enfoques de detección y prevención, que es el tema de esta sección.

Detección de fuego

Hay varias opciones disponibles para la detección de incendios.

Debe estar familiarizado con los siguientes tipos básicos de sistemas de detección de incendios:

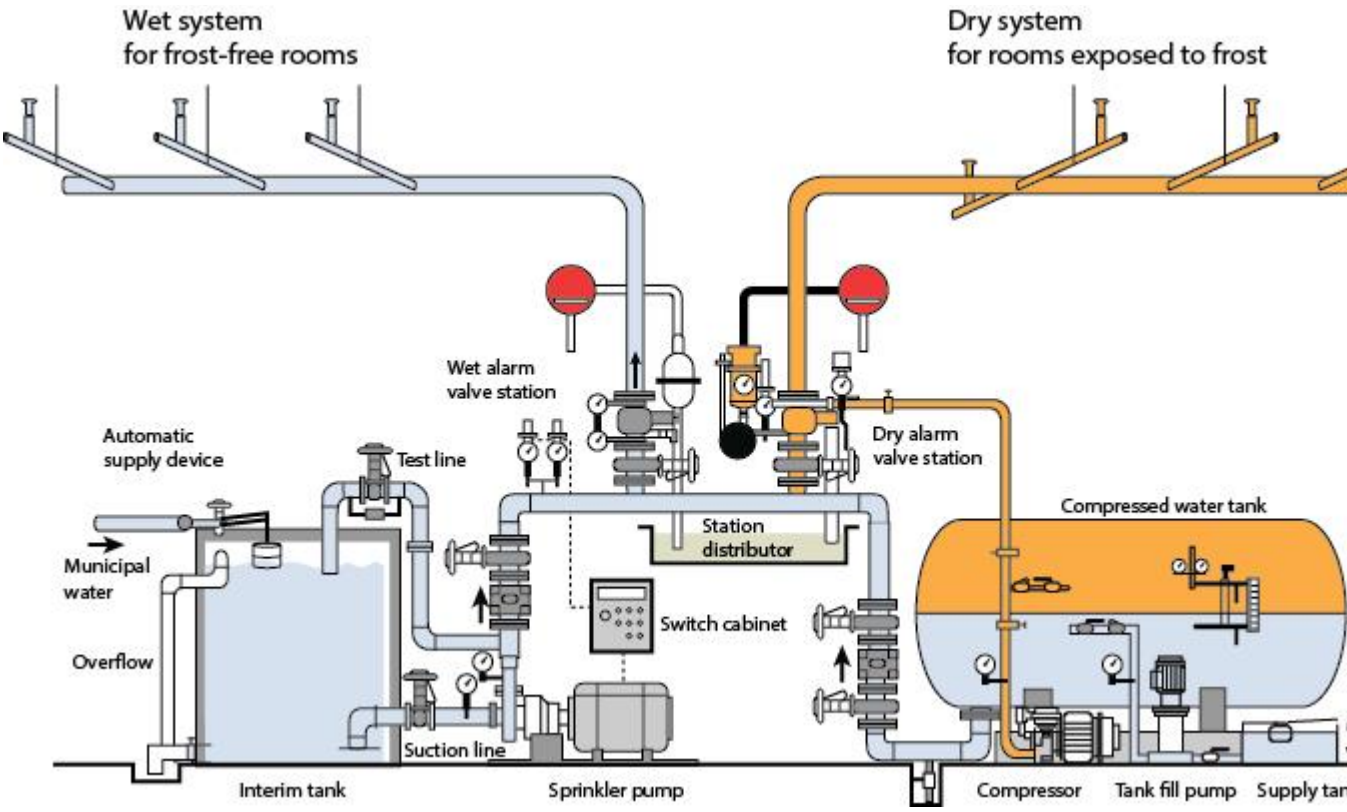
- **Activado por humo : funciona** mediante un dispositivo fotoeléctrico para detectar variaciones de luz provocadas por partículas de humo.
- **Activado por calor (también llamado sensor de calor) : funciona** detectando cambios de temperatura. Estos sistemas pueden alertar cuando se alcanza una temperatura predefinida o alertar cuando la tasa de aumento es de cierto valor.
- **Actuado por llama :** dispositivos ópticos que "miran" el área protegida. Por lo general, reaccionan más rápido a un incendio que los dispositivos no ópticos.

Supresión de incendios

Aunque los extintores de incendios (cubiertos en el Capítulo 1) son una forma manual de extinción de incendios, también existen otros sistemas más automatizados.

Debe estar familiarizado con los siguientes tipos de sistemas de rociadores:

- **Tubería húmeda :** Utilice agua contenida en tuberías para extinguir el fuego. En algunas áreas, el agua puede congelarse y reventar las tuberías, causando daños. Tampoco se recomiendan para habitaciones donde el agua dañará el equipo.
- **Tubería seca :** en este sistema, el agua no se retiene en las tuberías sino en un tanque de retención. Las tuberías contienen aire presurizado, que se reduce cuando se detecta un incendio, lo que permite que el agua ingrese a la tubería y los rociadores. Esto minimiza la posibilidad de una descarga accidental. La figura 3-25 muestra una comparación de sistemas secos y húmedos.



Se utiliza un sistema húmedo para habitaciones libres de heladas, mientras que el sistema seco se utiliza para habitaciones expuestas a heladas. En el sistema de tubería húmeda, el agua se almacena en el tanque intermedio que está equipado con un dispositivo de suministro automático y un sistema de detección de desbordamiento. Desde este tanque, el agua va a la bomba de rociadores que se activa cuando la estación de la válvula de alarma húmeda activa la alarma y el agua fluye por la tubería hacia los rociadores. En este sistema, el agua se mantiene en la tubería. Por el contrario, en el sistema seco el agua no se retiene en las tuberías sino en un tanque de retención. Las tuberías contienen aire presurizado, lo que activa el sistema de válvula de alarma seca cuando se detecta el fuego, lo que permite que el agua ingrese a la tubería y a los rociadores.

Figura 3-25 Sistemas de tuberías secas y húmedas

- **Preacción : funciona** como un sistema de tubería seca, excepto que el cabezal del rociador sostiene un enlace termofusible que debe fundirse antes de que se libere el agua. Este es actualmente el sistema recomendado para una sala de informática.
- **Diluvio :** permite que se liberen grandes cantidades de agua en la habitación, lo que obviamente hace que esta no sea una buena opción donde se ubicarán los equipos informáticos.

En un momento, los sistemas de extinción de incendios usaban gas halón, que funciona bien al suprimir la combustión a través de una reacción química. Sin embargo, estos sistemas ya no se utilizan porque se ha descubierto que dañan la capa de ozono.

Los reemplazos aprobados por la EPA para Halon incluyen

- Agua
- Argón
- NAF-S-III

Otro sistema de extinción de incendios que se puede utilizar en salas de informática que no daña las computadoras y que es seguro para los humanos es el FM-200.

Fuente de alimentación

La fuente de alimentación es el elemento vital de la empresa y de todos sus equipos. En esta sección, analizamos los problemas comunes de energía y algunos de los mecanismos de prevención y técnicas de mitigación que permitirán que la empresa continúe operando cuando surjan problemas de energía.

Tipos de interrupciones

Al hablar de problemas de energía, debe estar familiarizado con los siguientes términos:

- **Surge :** un alto voltaje prolongado
- **Caída de voltaje :** una caída prolongada de energía que está por debajo del voltaje normal
- **Fallo :** un corte de energía momentáneo
- **Apagón :** un apagón prolongado
- **Sag:** una reducción momentánea en el nivel de potencia

Sin embargo, los posibles problemas de energía van más allá de la pérdida total o parcial de energía. Las líneas eléctricas pueden introducir ruido e interferir con las comunicaciones en la red. En cualquier caso donde haya motores eléctricos grandes o fuentes de ciertos tipos de luz, como iluminación fluorescente, se debe utilizar cableado blindado para ayudar a prevenir la interferencia de radiofrecuencia (RFI) y la interferencia electromagnética (EMI).

Medidas preventivas

Deben observarse los procedimientos para evitar que la electricidad estática dañe los componentes. Algunas precauciones a tomar son

- Utilice aerosoles antiestáticos.
- Mantenga los niveles de humedad adecuados.
- Utilice alfombrillas y muñequeras antiestáticas.

Para protegerse contra la energía sucia (caídas y sobretensiones) y cortes de energía tanto parciales como totales, se pueden implementar los siguientes dispositivos:

- **Acondicionadores de energía :** vaya entre el tomacorriente de pared y el dispositivo y suavice las fluctuaciones de la energía entregada al dispositivo, protegiéndolo contra caídas y subidas de tensión.
- **Fuentes de alimentación ininterrumpida (UPS) :** vaya entre el tomacorriente de la pared y el dispositivo y use una batería para proporcionar energía si se pierde la fuente de la pared. También existen UPS que pueden proporcionar energía a una sala de servidores.

HVAC

Los sistemas de calefacción, ventilación y aire acondicionado no solo están instalados para la comodidad de los empleados. Las enormes cantidades de equipos informáticos desplegados por la mayoría de las empresas dependen aún más de estos sistemas que los humanos. Sin las condiciones ambientales adecuadas, los equipos informáticos no se quejarán; simplemente dejará de funcionar. Los equipos informáticos y los dispositivos de infraestructura, como enrutadores y conmutadores, no se ven afectados por las siguientes condiciones:

- **Calor: el** calor excesivo provoca reinicios y bloqueos.
- **Humedad: la** humedad provoca problemas de corrosión en las conexiones.
- **Baja humedad: las** condiciones secas fomentan la electricidad estática, que puede dañar el equipo.

Con respecto a la temperatura, algunos hechos importantes que debe conocer son

- A los 100 grados, comienzan a producirse daños en los medios magnéticos.
- A 175 grados, comienzan a producirse daños en las computadoras y los periféricos.
- A 350 grados, comienzan a producirse daños en los productos de papel.

En resumen, las condiciones deben ser perfectas para estos dispositivos. Es por esta razón que las unidades de aire acondicionado deben estar dedicadas a las instalaciones de procesamiento de información y en una fuente de energía separada de los otros sistemas HVAC.

Fugas de agua e inundaciones

Por mucho que a los sistemas informáticos les disguste el calor, les disgusta aún más el agua. También puede causar grandes daños a los pisos, las paredes y los cimientos de las instalaciones. AguaLos detectores deben colocarse debajo de pisos elevados y sobre techos falsos para que las fugas en el techo y el agua debajo de los pisos se detecten antes de que causen un problema.

Hablando de pisos elevados, en áreas como armarios de cableado, centros de datos y salas de servidores, todos los pisos deben elevarse para proporcionar un margen de error adicional en el caso de aumento de agua.

Alarmas ambientales

Un error que hace que un sistema sea vulnerable debido al entorno en el que está instalado se denomina error ambiental. Teniendo en cuenta los diversos desafíos que presentan las demandas ambientales impuestas a la instalación por el equipo de cómputo y los costos de no atender estas necesidades, corresponde a la empresa tener algún sistema que avise cuando las condiciones ambientales son menos deseables. Un sistema de alerta, como un higrómetro, que monitorea la humedad, debe estar instalado en las áreas donde reside el equipo sensible. El sistema también debe monitorear la temperatura. Estos tipos de controles se consideran controles físicos.

Seguridad del equipo

La seguridad física del equipo se enfatiza a lo largo de este libro. Esta sección analiza los procedimientos corporativos relacionados con equipos y medios y el uso de cajas fuertes y bóvedas para proteger otros activos físicos valiosos.

Procedimientos corporativos

La seguridad física de los equipos y los medios debe integrarse en las políticas y procedimientos de seguridad de la empresa. Estos procedimientos deben abordar los problemas cubiertos en las secciones siguientes.

Protección contra manipulación

No debería ser posible que personas no autorizadas accedan y cambien la configuración de ningún dispositivo. Esto significa que se deben seguir medidas adicionales, como las que se encuentran en el resto de esta sección, para evitar esto. La manipulación incluye desfigurar, dañar o cambiar la configuración de un dispositivo. Las aplicaciones deben utilizar programas de verificación de integridad para buscar evidencia de manipulación de datos, errores y omisiones.

Cifrado

Cifrar los datos confidenciales almacenados en los dispositivos puede ayudar a prevenir la exposición de los datos en caso de robo o en caso de acceso inadecuado al dispositivo. Los conceptos de criptografía y encriptación se tratan ampliamente al principio de este capítulo.

Inventario

Reconocer cuándo se roban los artículos es imposible si no existe un sistema de inventario o recuento de artículos. Se debe hacer un inventario de todo el equipo y se debe mantener y actualizar toda la información relevante sobre cada dispositivo. Mantenga esta información tanto en formato electrónico como en papel.

Protección física de dispositivos de seguridad

Los dispositivos de seguridad, como los cortafuegos, los dispositivos NAT y los sistemas de detección y prevención de intrusiones, deben recibir la mayor atención porque se relacionan con la seguridad física y lógica.

Más allá de esto, los dispositivos que se pueden robar fácilmente, como computadoras portátiles, tabletas y teléfonos inteligentes, deben guardarse bajo llave. Si eso no es práctico, bloquee este tipo de dispositivos en un objeto estacionario. Un buen ejemplo de esto son los candados de cable que se utilizan con las computadoras portátiles.

Dispositivos de seguimiento

Cuando la tecnología está disponible, el seguimiento de dispositivos pequeños se puede utilizar para ayudar a mitigar la pérdida de ambos dispositivos y sus datos, como se mencionó anteriormente. La mayoría de los teléfonos inteligentes ahora incluyen un software de rastreo que le permite ubicar el dispositivo después de que haya sido robado o perdido mediante el rastreo de la torre celular o el GPS. Implemente esta tecnología cuando esté disponible.

Otra función útil disponible en estos mismos tipos de dispositivos es una función de borrado remoto. Esto permite enviar una señal a un dispositivo robado indicándole que borre los datos contenidos en el dispositivo. Por último, estos dispositivos también suelen tener la capacidad de bloquear de forma remota el dispositivo cuando se extravían.

Procedimientos de medios portátiles

Como se mencionó anteriormente, el control estricto del uso de dispositivos de medios portátiles puede ayudar a evitar que la información confidencial salga de la red. Esto incluye CD, DVD, unidades flash, unidades de memoria USB y discos duros externos. Aunque las reglas escritas deben estar vigentes sobre el uso de estos dispositivos, también es posible usar políticas de seguridad para evitar la copia de datos en estos tipos de medios. También es posible permitir la copia de datos en estos tipos de unidades siempre que los datos estén cifrados. Si estas funciones las proporciona el sistema operativo de red, debe implementarlas.

Cajas fuertes, bóvedas y cerraduras

Con respecto a la protección de activos físicos como computadoras portátiles, teléfonos inteligentes, tabletas, etc., nada mejor que bloquear físicamente los dispositivos. En los casos en que sea posible hacerlo, los armarios con cerradura son una buena solución para almacenar estos dispositivos. Además de seleccionar la cerradura adecuada (las cerraduras se discutieron anteriormente en este capítulo), todosSe debe inventariar el equipo y diseñar un sistema para mantener estos conteos a medida que los dispositivos van y vienen.

Algunos elementos requieren incluso más protección que un armario cerrado con llave. Guarde los documentos legales importantes y cualquier otro artículo de valor extremo en una caja fuerte o en una bóveda para la protección adicional que estos artículos requieren. Las cajas fuertes y bóvedas ignífugas pueden proteger el contenido incluso durante un incendio.

Tareas de preparación de exámenes

Como se menciona en la sección " Acerca de la *Guía de certificación CISSP* , tercera edición " en la Introducción, tiene un par de opciones para la preparación del examen: los ejercicios aquí,

Capítulo 9 , " Preparación final " y las preguntas de simulación del examen en el Examen de Pearson. Software de preparación en línea.

Revisar todos los temas clave

Revise los temas más importantes de este capítulo, señalados con el icono de Temas clave en el margen exterior de la página. La Tabla 3-16 enumera una referencia de estos temas clave y los números de página en los que se encuentra cada uno.

Tabla 3-16 Temas clave para el Capítulo 3

Elemento de tema clave	Descripción	Número de página
Lista	Categorías de procesos ISO / IEC 15288: 2015	181
Tabla 3-1	Resumen de modos de seguridad	184
Lista	Reglas de Bell-LaPadula	189
Lista	Axiomas de Biba	190
Lista	Elementos de Clark-Wilson	191
Lista	Sistema de clasificación TCSEC	207
Tabla 3-3	Mapeo de ITSEC y TCSEC	210
Lista	Niveles de garantía de los Criterios Comunes	211
Lista	ISO / IEC 27001: Pasos de 2013	214
Lista	Fases de NIACAP	217
Lista	Proceso de selección de control de seguridad	218
Lista	Memoria de chip TPM	221
Lista	Componentes de sistemas de control industrial	227
Lista	NIST SP 800-82, Rev.2 Objetivos de seguridad de ICS	228
Lista	Pasos del programa de seguridad de ICS	230
Lista	Implementaciones en la nube NIST SP 800-145	231
Lista	Niveles de nubes	231
Tabla 3-4	NIST SP 800-144 Problemas y recomendaciones de seguridad y privacidad en la nube	234
Lista	NIST SP 800-146 beneficios de SaaS	235
Lista	NIST SP 800-146 problemas y preocupaciones de SaaS	236
Lista	NIST SP 800-146 beneficio de PaaS	236
Lista	NIST SP 800-146 problemas y preocupaciones de PaaS	236
Lista	NIST SP 800-146 beneficios de IaaS	236

Elemento de tema clave	Descripción	Número de página
Lista	NIST SP 800-146 problemas y preocupaciones de IaaS	236
Figura 3-7	Marco NIST CPS	240
Lista	Conceptos de criptografía	250
Lista	Elementos clave del proceso de gestión	262
Tabla 3-12	Fortalezas y debilidades del algoritmo simétrico	267
Lista	Ventajas de los cifrados basados en flujo	267
Lista	Ventajas de los cifrados en bloque	268
Tabla 3-13	Fortalezas y debilidades del algoritmo asimétrico	269
Lista	Modos	270
Lista	Modos 3DES	273
Tabla 3-14	Datos clave de los algoritmos simétricos	276
Lista	Pasos de PKI	284
Lista	Pasos básicos de un proceso HMAC	298
Lista	Pasos básicos de un proceso CBC-MAC	298
Lista	Tipos básicos de sistemas de detección de incendios	317
Lista	Tipos de sistemas de rociadores	318
Lista	Términos de emisión de energía	319

Complete las tablas y listas de memoria

Imprima una copia del Apéndice A , “ Tablas de memoria ” , o al menos la sección de este capítulo, y complete las tablas y listas de la memoria. El Apéndice B , “ Clave de respuestas de las tablas de memoria ” , incluye tablas y listas completadas para verificar su trabajo.

Definir términos clave

Defina los siguientes términos clave de este capítulo y verifique sus respuestas en el glosario:

direccionamiento absoluto

acreditación

vidrio acrílico

agregación

algoritmo

arquitectura

memoria asociativa

cifrado asimétrico

modo asimétrico

cifrado asincrónico

autenticación

autorización

disponibilidad

efecto de avalancha

BACnet2

Modelo Bell-LaPadula

Modelo Biba

apagón

cifrado de bloque

Pez globo

bolardos

Modelo Brewer-Nash (muro chino)

apagón

bloqueo de cable

cache

CAST-128

CAST-256

lista de revocación de certificados (CRL)

Certificación

autoridad de certificación (CA)

ataque de texto cifrado elegido

ataque de texto plano elegido

cifrar

Encadenamiento de bloques de cifrado (CBC)

MAC de encadenamiento de bloques de cifrado (CBC-MAC)

Comentarios de cifrado (CFB)

cerraduras de cifrado

texto cifrado

ataque de solo texto cifrado

Modelo de integridad de Clark-Wilson

Borrar texto

sistema cerrado

computación en la nube

colisión

cerradura de combinación

Criterios comunes (CC)

nube comunitaria

cifrado de ocultación

circulo concentrico

confidencialidad

confinamiento

Confusión

contaminación

Modo contador (CTR)

Prevención del delito a través del diseño ambiental (CPTED)

criptoanálisis

criptograma

criptografía

criptologia

criptosistema

criptovariable

almacén de datos

descodificación

descifrado

defensa en profundidad

extintor de diluvio

DES-X

difusión

certificado digital

Estándar de cifrado digital (DES)

firma digital

Estándar de firma digital (DSS)

DNP3

Doble-DES

extintor de tubo seco

Libro de códigos electrónico (ECB)

sistema Integrado

codificacion

cifrado

inscripción

error ambiental

Lenguaje de marcado extensible (XML)

estado a prueba de fallas

fallar estado suave

culpa

atractivo

matriz de puerta programable en campo (FPGA)

firmware

sensor accionado por llama

memoria flash

Modelo de Graham-Denning

computación en cuadrícula

Modelo de Harrison-Ruzzo-Ullman

picadillo

hash MAC (HMAC)

HAVAL

sensor activado por calor

nube híbrida

higrómetro

direccionamiento implícito

direccionamiento indirecto

inferencia

modelo de flujo de información

Criterios de evaluación de la seguridad de la tecnología de la información (ITSEC)

Infraestructura como servicio (IaaS)

integridad

Algoritmo de cifrado de datos internacional (IDEA)

Internet de las cosas (IoT)

interrumpir

clave

agrupación de claves

espacio de teclas

ataque de texto plano conocido

Vidrio laminado

modelo de defensa en capas

Modelo Lipner

LonWorks / LonTalk3

gancho de mantenimiento

amenazas causadas por humanos

cepo

modelo basado en matriz

MD2

MD4

MD5

MD6

código móvil

Modbus

cifrado de subestación mono-alfabético

modelo de celosía multinivel

multitarea

multihilo

control de acceso natural

vigilancia natural

natural territoriales Reinforcement

mientras tanto

modelo de no interferencia

no repudio

memoria no volátil

cifrado nulo

objeto

cojín de una sola vez

función unidireccional

Protocolo de estado de certificado en línea (OCSP)

sistemas abiertos

Proyecto de seguridad de aplicaciones web abiertas (OWASP)

Libro naranja

Realimentación de salida (OFB)

Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)

informática de igual a igual

permutación

procesador canalizado

Texto sin formato

Plataforma como servicio (PaaS)

cifrado de subestación polialfabética

poliinstanciación

acondicionador de energía

extintor de preacción

nube privada

cifrado de clave privada

proceso

dispositivo de autenticación de proximidad

nube publica

cifrado de clave pública

RC4

RC5

RC6

RC7

libro Rojo

monitor de referencia

autoridad de registro (RA)

revocación

Algoritmo de Rijndael

RIPEMD-160

cifrado de clave en ejecución

salazón

memoria secundaria

cifrado de clave secreta

Lenguaje de marcado de aserción de seguridad (SAML)

kernel de seguridad

Barrilete

sensor activado por humo

Software como servicio (SaaS)

vidrio estándar

modelos de máquinas de estado

esteganografía

cifrado basado en flujo

sujeto

sustitución

cifrado de sustitución

superescalar

modo supervisor

aumento

cifrado simétrico

modo simétrico

cifrado sincrónico

vidrio templado

hilo

Tigre

ataque de tiempo de verificación / tiempo de uso

transposición

cifrado de transposición

trampilla (cifrado)

Triple DES (3DES)

Base de computadora confiable (TCB)

Criterios de evaluación de sistemas informáticos de confianza (TCSEC)

Módulo de plataforma confiable (TPM)

cerradura de vaso

Dos peces

fuente de alimentación ininterrumpida (UPS)

verificación

memoria volatil

cerradura protegida

extintor de tubería húmeda

factor de trabajo (cifrado)

Responder preguntas de revisión

1 . ¿Cuál de las siguientes opciones se proporciona si no se pueden leer los datos?

1. Integridad
2. Confidencialidad
3. Disponibilidad
4. Defensa en profundidad

2 . En un entorno distribuido, ¿cuál de los siguientes es un software que une el software del servidor y el cliente?

1. Sistema Integrado
2. Código móvil
3. Computación virtual
4. Middleware

3 . ¿Cuál de los siguientes está compuesto por los componentes (hardware, firmware y / o software) en los que se confía para hacer cumplir la política de seguridad del sistema?

1. Perímetro de seguridad
2. Monitor de referencia
3. Base de computadora confiable (TCB)
4. Kernel de seguridad

4 . ¿Qué proceso convierte texto plano en texto cifrado?

1. Hashing
2. Descifrado
3. Cifrado
4. Firma digital

5 . ¿Qué tipo de cifrado es el cifrado César?

1. Sustitución polialfabética
2. Sustitución mono-alfabética
3. Transposición polialfabética
4. Transposición mono-alfabética

6 . ¿Cuál es el esquema de cifrado más seguro?

1. Cifrado de ocultación
2. Algoritmo simétrico
3. Cojín de una sola vez

4. Algoritmo asimétrico

7 . ¿Qué implementación de 3DES cifra cada bloque de datos tres veces, cada vez con una clave diferente?

1. 3DES-EDE3
2. 3DES-EEE3
3. 3DES-EDE2
4. 3DES-EEE2

8 . ¿Cuál de las siguientes opciones NO es una función hash?

1. ETC
2. MD6
3. SHA-2
4. RIPEMD-160

9 . ¿Cuál de los siguientes es un ejemplo de cómo prevenir una amenaza interna?

1. Un sistema de cerradura de puerta en una sala de servidores.
2. Una cerca eléctrica que rodea una instalación.
3. Guardias armados fuera de una instalación
4. Cámaras de estacionamiento

10 . ¿Cuál de las siguientes NO es una de las tres estrategias principales que guían a CPTED?

1. Control de acceso natural
2. Refuerzo de vigilancia natural
3. Natural territoriales Reinforcement
4. Vigilancia natural

11 . ¿Qué ocurre cuando diferentes claves de cifrado generan el mismo texto cifrado a partir del mismo mensaje de texto sin formato?

1. Agrupación de claves
2. Criptoanálisis
3. Espacio de claves
4. Confusión

12 . ¿Qué sistema de cifrado utiliza una clave privada o secreta que debe permanecer secreta entre las dos partes?

1. Cifrado de clave en ejecución
2. Cifrado de ocultación
3. Algoritmo asimétrico
4. Algoritmo simétrico

13 . ¿Cuál de los siguientes es un algoritmo asimétrico?

1. OCURRENCIA
2. Dos peces
3. RC6
4. RSA

14 . ¿Qué componente de PKI contiene una lista de todos los certificados que se han revocado?

1. QUE
2. FUERA
3. CRL
4. OCSP

15 . ¿Qué ataque ejecutado contra un algoritmo criptográfico utiliza todas las claves posibles hasta que se descubre una clave que descifra con éxito el texto cifrado?

1. Análisis de frecuencia
2. Ingeniería inversa
3. Ataque de solo texto cifrado
4. Fuerza bruta

16 . En ISO / IEC 15288: 2015, ¿qué categoría de proceso incluye adquisición y suministro?

1. Procesos de gestión técnica
2. Procesos tecnicos
3. Procesos de acuerdos
4. Procesos organizativos de habilitación de proyectos

17 . ¿Qué afirmación es verdadera sobre el modo de seguridad dedicado?

1. Emplea un solo nivel de clasificación.
2. Todos los usuarios tienen la misma autorización de seguridad, pero no todos poseen la autorización necesaria para conocer toda la información del sistema.
3. Todos los usuarios deben poseer la autorización de seguridad más alta, pero también deben tener una autorización válida de necesidad de conocer, un NDA firmado y una aprobación formal para toda la información a la que tienen acceso.
4. Los sistemas permiten procesar dos o más niveles de clasificación de información al mismo tiempo.

18 . ¿Cuál es el primer paso en ISO / IEC 27001: 2013?

1. Identifica los requisitos.
2. Realizar evaluación de riesgos y tratamiento de riesgos.
3. Mantener y monitorear el SGSI.
4. Obtenga apoyo administrativo.

19 . ¿Qué dos estados de procesador son compatibles con la mayoría de los procesadores?

1. Estado del supervisor y estado del problema
2. Estado del supervisor y estado del kernel
3. Estado del problema y estado del usuario
4. Estado de supervisor y estado elevado

20 . Al apoyar una iniciativa BYOD, ¿de qué grupo probablemente tiene más que temer?

1. Hacktivistas
2. Usuarios descuidados
3. Proveedores de software
4. Proveedores de dispositivos móviles

21 . ¿Qué término se aplica a los dispositivos integrados que traen consigo problemas de seguridad porque los ingenieros que diseñan estos dispositivos no siempre se preocupan por la seguridad?

1. BYOD
2. NDA
3. IoT
4. ITSEC

22 . ¿Qué opción describe mejor la preocupación principal de NIST SP 800-57?

1. Cifrado asimétrico
2. Cifrado simétrico
3. Integridad del mensaje
4. Gestión de claves

23 . ¿Cuál de los siguientes tipos de claves solo requiere protección de seguridad de integridad?

1. Clave de verificación de firma pública
2. Clave de firma privada
3. Clave de autenticación simétrica
4. Clave de autenticación privada

24 . ¿Cuál es la fase final del ciclo de vida de la gestión de claves criptográficas, según NIST SP 800-57?

1. Fase operativa
2. Fase destruida
3. Fase preoperativa
4. Fase posoperatoria

Respuestas y explicaciones

1 **. B.** Se proporciona confidencialidad si los datos no se pueden leer. Esto se puede proporcionar mediante controles de acceso y cifrado de los datos tal como están en un disco duro o mediante cifrado cuando los datos están en tránsito.

2 **. D.** En un entorno distribuido, el middleware es un software que une el software del cliente y del servidor. No es parte del sistema operativo ni del software del servidor. Es el código que se encuentra entre el sistema operativo y las aplicaciones en cada lado de un sistema informático distribuido en una red.

3 **. C.** Trusted Computer Base (TCB) está compuesta por los componentes (hardware, firmware y / o software) que son confiables para hacer cumplir la política de seguridad del sistema y que, si se ven comprometidos, ponen en peligro las propiedades de seguridad de todo el sistema.

4 **. C.** El cifrado convierte el texto sin formato en texto cifrado. El hash reduce un mensaje a un valor hash. El descifrado convierte el texto cifrado en texto sin formato. Una firma digital es un objeto que proporciona autenticación del remitente e integridad del mensaje al incluir una firma digital con el mensaje original.

5 **. B.** El cifrado Caesar es un cifrado de sustitución mono-alfabético. La sustitución de Vigenere es una sustitución polialfabética.

6 **. C.** Un pad de un solo uso es el esquema de cifrado más seguro porque se usa solo una vez.

7 **. B.** La implementación 3DES-EEE3 cifra cada bloque de datos tres veces, cada vez con una clave diferente. La implementación 3DES-EDE3 cifra cada bloque de datos con la primera clave, descifra cada bloque con la segunda clave y cifra cada bloque con la tercera clave. La implementación 3DES-EDE2 cifra cada bloque de datos con la primera clave, descifra cada bloque con la segunda clave y luego cifra cada bloque con la primera clave. La implementación de 3DES-EEE2 cifra cada bloque de datos con la primera clave, cifra cada bloque con la segunda clave y luego cifra cada bloque con la tercera clave.

8 **. una.** El criptosistema de curva elíptica (ECC) NO es una función hash. Es un algoritmo asimétrico. Todas las demás opciones son funciones hash.

9 **. una.** Una cerca eléctrica que rodea una instalación está diseñada para evitar el acceso al edificio por parte de aquellos que no deberían tener acceso (una amenaza externa), mientras que un sistema de cerradura de puerta en la sala de servidores que requiere deslizar la tarjeta de empleado está diseñado para evitar el acceso. por aquellos que ya están en el edificio (una amenaza interna).

10 **. B.** Las tres estrategias son control de acceso natural, refuerzo de territorios naturales y vigilancia natural.

11 **. una.** La agrupación de claves se produce cuando diferentes claves de cifrado generan el mismo texto cifrado a partir del mismo mensaje de texto sin formato. El criptoanálisis es la ciencia de descifrar el texto cifrado sin conocimiento previo de la clave o el criptosistema

utilizado. Un espacio de claves son todos los valores clave posibles cuando se utiliza un algoritmo particular u otra medida de seguridad. La confusión es el proceso de cambiar el valor de una clave durante cada ronda de cifrado.

12 . D. Un algoritmo simétrico utiliza una clave privada o secreta que debe permanecer secreta entre las dos partes. Un cifrado de clave en ejecución utiliza un componente físico, generalmente un libro, para proporcionar los caracteres polialfabéticos. Un cifrado de ocultación ocurre cuando el texto sin formato se intercala en algún lugar dentro de otro material escrito. Un algoritmo asimétrico utiliza tanto una clave pública como una clave privada o secreta.

13 . D. RSA es un algoritmo asimétrico. Todos los demás algoritmos son algoritmos simétricos.

14 . C. Una lista de revocación de certificados (CRL) contiene una lista de todos los certificados que se han revocado. Una autoridad de certificación (CA) es la entidad que crea y firma certificados digitales, mantiene los certificados y los revoca cuando es necesario. Una autoridad de registro (RA) verifica la identidad del solicitante, registra al solicitante y pasa la solicitud a la CA. Online Certificate Status Protocol (OCSP) es un protocolo de Internet que obtiene el estado de revocación de un certificado digital X.509.

15 . D. Un ataque de fuerza bruta ejecutado contra un algoritmo criptográfico utiliza todas las claves posibles hasta que se descubre una clave que descifra con éxito el texto cifrado. Un ataque de análisis de frecuencia se basa en el hecho de que los cifrados de sustitución y transposición darán como resultado patrones repetidos en el texto cifrado. Un ataque de ingeniería inversa ocurre cuando un atacante compra un producto criptográfico en particular para intentar aplicar ingeniería inversa al producto para descubrir información confidencial sobre el algoritmo criptográfico utilizado. Un ataque de solo texto cifrado utiliza varios mensajes cifrados (texto cifrado) para averiguar la clave utilizada en el proceso de cifrado.

16 . C. ISO / IEC 15288: 2015 establece cuatro categorías de procesos:

- Procesos de acuerdos, incluida la adquisición y el suministro
- Procesos organizativos de habilitación de proyectos, incluida la gestión de la infraestructura, la gestión de la calidad y la gestión del conocimiento.
- Procesos de gestión técnica, incluida la planificación de proyectos, la gestión de riesgos, la gestión de la configuración y el aseguramiento de la calidad.
- Procesos técnicos, incluida la definición de los requisitos del sistema, el análisis del sistema, la implementación, la integración, la operación, el mantenimiento y la eliminación.

17 . una. El modo de seguridad dedicado emplea un solo nivel de clasificación.

18 . D. El primer paso en ISO / IEC 27001: 2013 es obtener apoyo administrativo.

19 . una. La mayoría de los procesadores admiten dos estados de procesador: estado de supervisor (o modo de núcleo) y estado de problema (o modo de usuario).

20 **. B.** Como profesional de la seguridad, al respaldar una iniciativa BYOD, debe tener en cuenta que probablemente tenga más que temer del descuido de los usuarios que de los piratas informáticos.

21 **. C.** Internet de las cosas (IoT) es el término utilizado para los dispositivos integrados y sus preocupaciones de seguridad porque los ingenieros que diseñan estos dispositivos no siempre se preocupan por la seguridad.

22 **. D.** La gestión de claves es la principal preocupación de NIST SP 800-57.

23 **. una.** Las claves de verificación de firmas públicas solo requieren protección de seguridad de integridad.

24 **. B.** La fase destruida es la fase final del ciclo de vida de la gestión de claves criptográficas, según NIST SP 800-57.