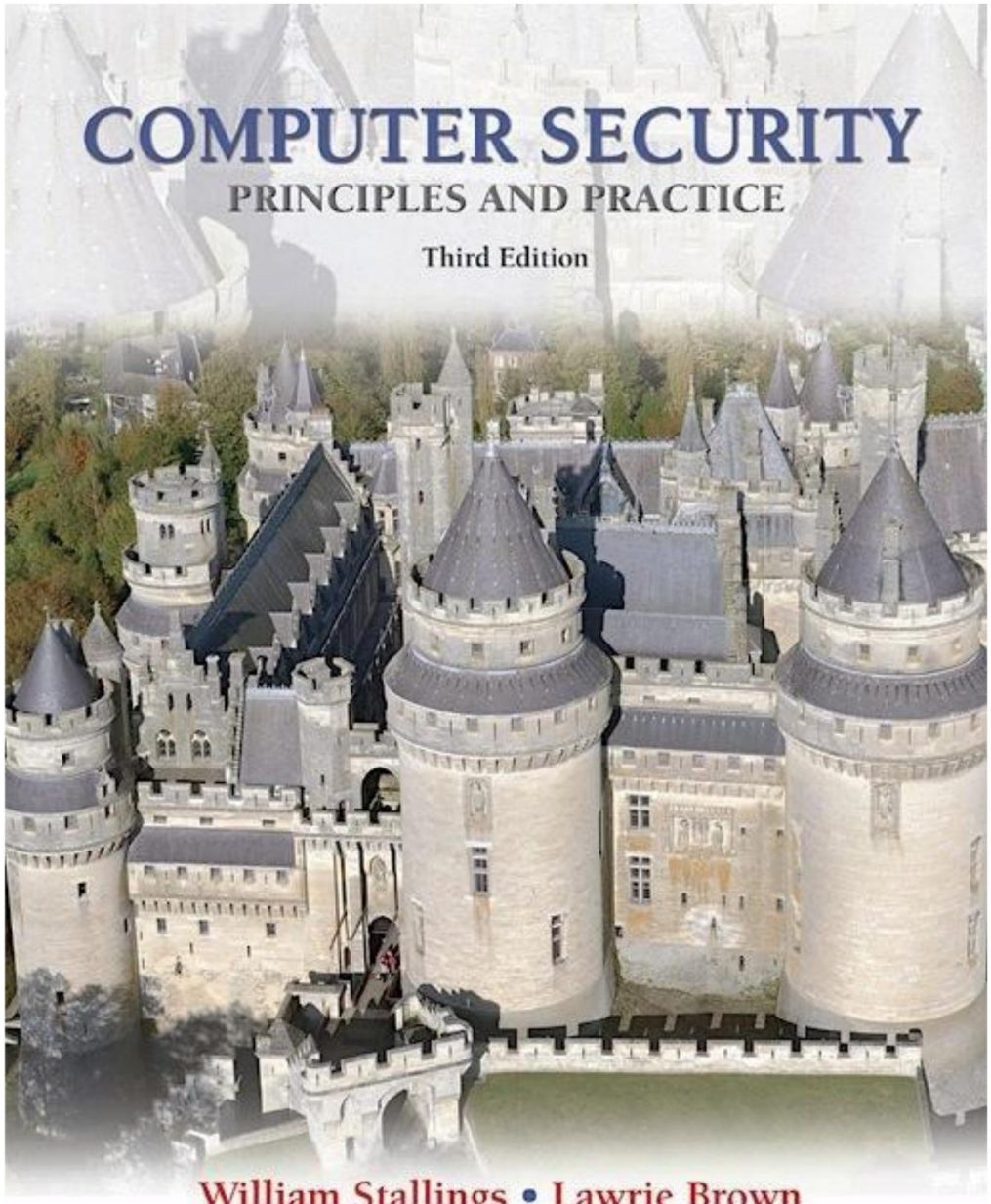


Capítulo 26

Seguridad de Windows

Contribuido por:
Michael Howard

Gerente Senior del Programa de Seguridad

Corporación Microsoft

Ventanas fundamentales

Arquitectura de seguridad

- Cualquiera que quiera comprender la seguridad de Windows debe tener conocimiento de los bloques de seguridad fundamentales básicos del sistema operativo.
- Algunos de los componentes de Windows que conforman la infraestructura de seguridad fundamental son:
  - o El Monitor de Referencia de Seguridad (SRM)
  - o La Autoridad de Seguridad Local (LSA)
  - o El Administrador de cuentas de seguridad (SAM)
  - o Directorio Activo (AD)
  - o Paquetes de autenticación
  - o WinLogon y NetLogon

Ventanas fundamentales

Arquitectura de seguridad

El Monitor de Referencia de Seguridad (SRM)

- Este componente en modo kernel realiza comprobaciones de acceso, genera entradas de registro de auditoría y manipula los derechos de usuario (también llamados privilegios).
- En última instancia, cada verificación de permisos la realiza el SRM.
- La mayoría de los sistemas operativos modernos incluyen una funcionalidad de tipo SRM que realiza comprobaciones de permisos privilegiados.
- Los SRM tienden a ser de tamaño pequeño, por lo que se puede verificar su exactitud.

La Autoridad de Seguridad Local (LSA)

- Reside en un proceso de modo de usuario llamado lsass.exe y es responsable de aplicar la política de seguridad local en Windows
- También emite tokens de seguridad a las cuentas para que inicien sesión en el sistema.
- La política de seguridad incluye:
  - Política de contraseñas (como reglas de complejidad y tiempos de expiración)
  - Política de auditoría (qué operaciones sobre qué objetos auditar)
  - Configuración de privilegios (qué cuentas pueden realizar operaciones privilegiadas)

Ventanas fundamentales

Arquitectura de seguridad

El administrador de cuentas de seguridad (SAM)

- Es una base de datos que almacena datos de cuentas e información de seguridad relevante sobre los directores locales y los grupos locales.
- Cuando un usuario inicia sesión en una computadora usando una cuenta local, el proceso SAM toma la información de inicio de sesión y realiza una búsqueda en la base de datos SAM.
- Si las credenciales coinciden el usuario puede iniciar sesión en el sistema
- El archivo SAM es binario en lugar de texto, y las contraseñas se almacenan utilizando el algoritmo hash MD4
- En Windows Vista y versiones posteriores, el SAM almacena información de contraseñas mediante una función de derivación de clave basada en contraseñas (PBKCS) que es sustancialmente más robusta contra ataques de adivinación de contraseñas que MD4.

Directorio Activo (AD)

- Directorio LDAP de Microsoft incluido con Windows Server 2000 y versiones posteriores
- Todas las versiones de cliente de Windows compatibles actualmente, incluido Windows XP y Windows 7, puede comunicarse con AD para realizar operaciones de seguridad, incluido el inicio de sesión de cuenta.
- Un cliente de Windows se autenticará mediante AD cuando el usuario inicie sesión en la computadora usando una cuenta de dominio en lugar de una cuenta local.

Ventanas fundamentales

Arquitectura de seguridad

Cuentas locales versus cuentas de dominio

- Una computadora Windows en red puede tener una de dos configuraciones: unida a un dominio o en un grupo de trabajo.
- Cuando una computadora está unida a un dominio, los usuarios pueden obtener acceso a esa computadora usando cuentas de dominio, que se administran de forma centralizada en AD.
- También pueden iniciar sesión usando cuentas locales, pero es posible que las cuentas locales no tengan acceso a los recursos del dominio, como impresoras en red, servidores web, servidores de correo electrónico, etc.
- Cuando una computadora está en un grupo de trabajo, solo se pueden usar cuentas locales, guardadas en el SAM.
- Un dominio tiene la gran ventaja de ser administrado de forma central y, como tal, es más seguro, las cuentas de los usuarios se pueden deshabilitar de forma centralizada en lugar de en todas las computadoras individuales, y las políticas de seguridad también se administran de forma centralizada cuando se usa AD.
- La única ventaja de usar cuentas locales es que una computadora no necesita la infraestructura necesaria para soportar un dominio que usa AD
- En un grupo de trabajo (conjunto de computadoras conectadas entre sí mediante una red), las máquinas usan solo cuentas locales.
- La diferencia entre un grupo de trabajo y un dominio es simplemente dónde se autentican las cuentas.

- Un grupo de trabajo no tiene controladores de dominio, la autenticación se realiza en cada computadora y un dominio autentica las cuentas en los controladores de dominio que ejecutan AD

Usando PowerShell para Administración de seguridad

Windows 7 y Windows Server 2008 y versiones posteriores incluyen un lenguaje de scripting increíblemente flexible llamado PowerShell

Aspectos fundamentales que debe conocer Potencia Shell:

- PowerShell se basa en .NET. Si puede hacerlo en C# o VB.NET, puede hacerlo en un entorno de PowerShell.
- Los comandos en PowerShell se denominan cmdlets y tienen una sintaxis verbo-sustantivo consistente
- Al igual que todos los entornos de scripts, PowerShell admite la canalización de la salida de un comando a otro. A diferencia de otros entornos de scripts, PowerShell canaliza objetos, no texto. Esto permite un procesamiento, filtrado y análisis de datos muy completos.

Conceptos básicos de seguridad de Windows –

Ejemplo de dominio de extremo a extremo

Antes de que un usuario pueda iniciar sesión en un Red de Windows: un administrador de dominio debe agregar la información de la cuenta del usuario al sistema (incluye el nombre del usuario, el nombre de la cuenta y la contraseña)

Después de que el administrador haya ingresado esta información Windows crea una cuenta para el usuario en el controlador de dominio que se ejecuta Directorio activo

Cada cuenta de usuario está representada de forma única por un Identificación de seguridad (SID)

Los SID son únicos dentro de un dominio y cada cuenta obtiene un SID diferente

Identificación de seguridad

(síguelo)

El SID de una cuenta de usuario tiene el siguiente formato:

S -1 -5 -21 – AAA – BBB – CCC – RRR

S simple significa que
SID 1 es el número de versión de SID

5 es la autoridad del identificador (en este ejemplo, 5 es SECURITY_NT_AUTHORITY) 21 significa

“no único”, lo que simplemente significa que no hay garantía de unicidad; sin embargo, un SID es único dentro de un dominio AAA-BBB-CCC es un

número único que representa el dominio RRR se denomina ID relativo

(RID): es un número que se incrementa en 1 a medida que se crea cada nueva cuenta. Los RID nunca se repiten, lo que hace que cada SID sea único

Nombre de usuario

En Windows, un nombre de usuario puede tener uno de dos formatos:

- El formato SAM ---- es compatible con todas las versiones de Windows y tiene el formato DOMINIO\Nombre de usuario
- Nombre principal de usuario (UPN) y se parece más a una dirección de correo electrónico

RFC822 (nombreusuario@dominio.empresa.com)

El nombre SAM debe considerarse un formato heredado

Si el usuario ingresa solo un nombre de usuario, entonces el dominio en el que reside la máquina se antepone al nombre de usuario.

nombre de usuario

Suponiendo que el usuario inicia sesión correctamente, el sistema operativo genera un token y lo asigna al usuario.

usuario

Un token contiene el SID del usuario,

información de membresía del grupo y privilegios.

El token del usuario se asigna a cada proceso que ejecuta el usuario.

Privilegios en Windows

- Los privilegios son esencialmente permisos para todo el sistema. asignado a cuentas de usuario
- Algunos privilegios se consideran “peligrosos”, lo que significa que una cuenta maliciosa a la que se le otorga dicho privilegio puede causar daños.
- Algunos ejemplos de privilegios peligrosos incluyen:
  - o Actuar como parte del privilegio del sistema operativo
    - Este es el privilegio más peligroso en Windows y se concede solo a la cuenta del sistema local; ni siquiera a los administradores se les concede este privilegio.
  - o Privilegio de depuración de programas
    - Este privilegio básicamente significa que un usuario puede ejecutar cualquier código que desee en cualquier proceso en ejecución.
  - o Privilegio de copia de seguridad de archivos y directorios
    - Cualquier proceso que se ejecute con este privilegio omitirá todas las listas de control de acceso. cheques

acceso a la calle

(LCA)

Windows tiene dos formas de ACL:

- ACL discrecional (DACL)
  - Por lo general, lo que la mayoría de la gente quiere decir cuando dice LCA
  - Concede o deniega el acceso a recursos protegidos en Windows, como archivos, memoria compartida, canalizaciones con nombre, etc.
- Control de acceso al sistema (SACL)
  - Se utiliza para auditoría
  - En Windows Vista se utiliza para aplicar una política de integridad obligatoria

Dos cosas importantes a tener en cuenta sobre el control de acceso en Windows:

- No hay acceso implícito
- Cuando una aplicación de Windows accede a un objeto, debe solicitar el tipo de acceso que requiere la aplicación.

A los objetos que requieren protección se les asigna una DACL (y posiblemente una SACL) que incluye el SID del propietario del objeto (normalmente el creador del objeto), así como una lista de ACE

ACE

- Entradas de control de acceso
- Cada ACE en la DACL determina el acceso; y un ACE puede ser un ACE de permiso o un ACE de denegación
- Incluye un SID y una máscara de acceso (una máscara de acceso podría incluir la capacidad de leer, escribir, crear, eliminar, modificar)

Controles de acceso

- Cuando una cuenta de usuario intenta acceder a una objeto protegido el sistema operativo realiza una comprobación de acceso
- Compara la cuenta de usuario y el grupo. información en el token del usuario y las ACE en la ACL del objeto
- Si se conceden todas las operaciones solicitadas, se concede el acceso; de lo contrario, el usuario recibe un estado de error de acceso denegado.

Interpretación

- Windows es un sistema operativo multiproceso, lo que significa que un solo proceso puede tener más de un hilo de ejecución a la vez.
- Esto es muy común tanto para aplicaciones de servidor como de cliente.
- La suplantación significa configurar el token del usuario en el hilo actual.
- Cuando un hilo se hace pasar por un usuario, el token del usuario se asigna al hilo y la verificación de acceso para ese hilo se realiza contra el token del hilo, no contra el token del proceso.
- Cuando se realiza la conexión, el hilo "revierte" (el token se elimina del hilo).
- Con la suplantación es posible restringir quién puede hacer qué en el archivo db.tx

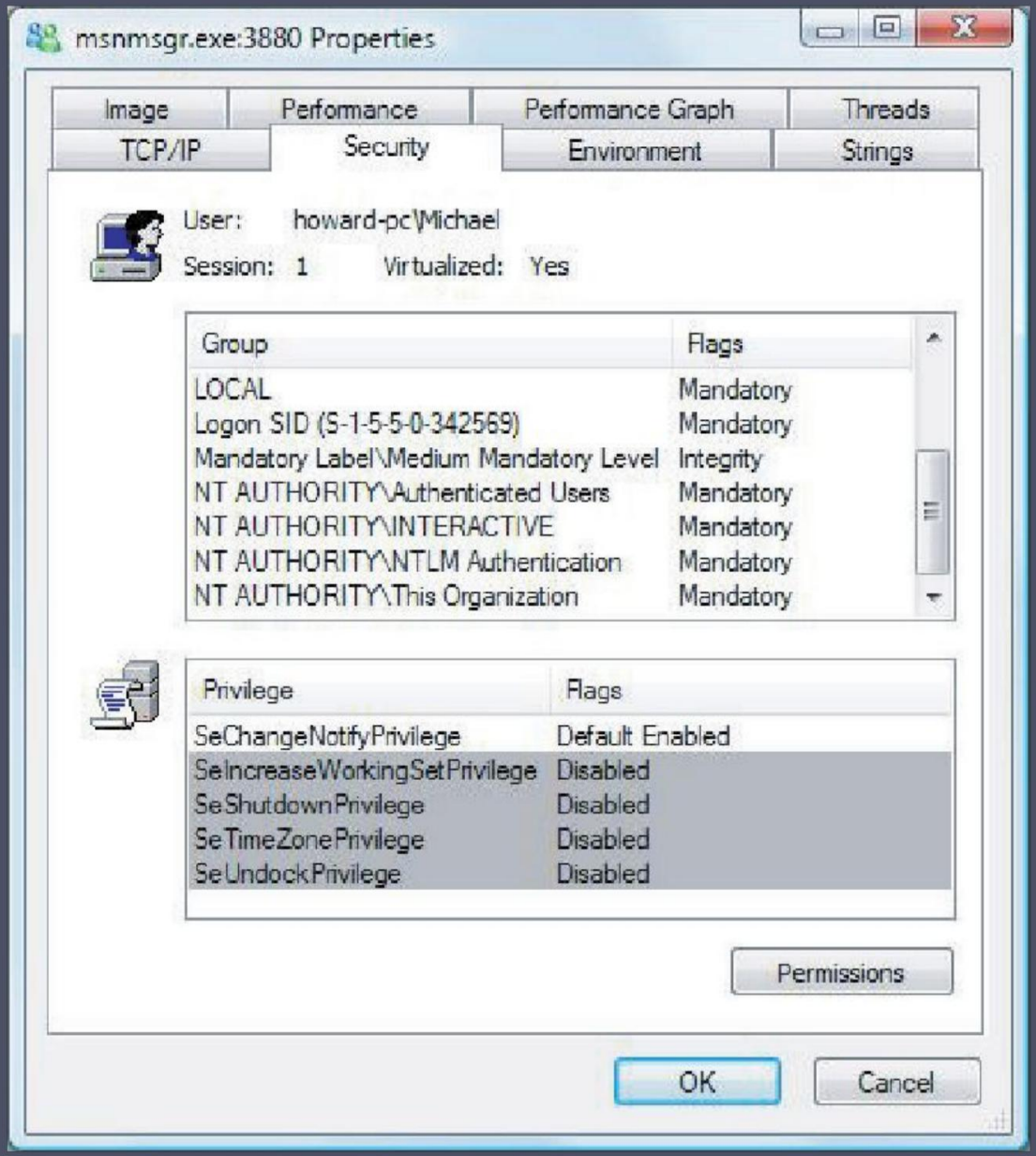


Figure 26.1 Screen Shot of User Account in Windows Vista

Vulnerabilidades de Windows

- Después de 2001, Microsoft decidió cambiar su proceso de desarrollo de software para adaptarse mejor a los requisitos de diseño, codificación, pruebas y mantenimiento seguros con el objetivo de reducir la cantidad de vulnerabilidades en todos los productos de Microsoft.
- Requisitos básicos del ciclo de vida del desarrollo de seguridad
  - o Educación obligatoria en seguridad
  - o Requisitos de diseño seguro
  - o Modelado de amenazas
  - o Análisis y reducción de la superficie de ataque
  - o Requisitos y herramientas de codificación segura
  - o Requisitos y herramientas de pruebas seguras
  - o Impulso de seguridad o Revisión final de seguridad
  - o Respuesta de seguridad

Seguridad de Windows Defensas

Las defensas con

Las ventanas se pueden agrupar en cuatro grandes categorías

- Defensas de cuenta
- Defensas de red
- Defensas contra la corrupción de la memoria
- Defensas del navegador

Sistema de Windows

Descripción general del endurecimiento

El proceso de endurecimiento es el proceso de reforzar las defensas, reducir la cantidad de funcionalidad expuesta a usuarios no confiables y deshabilitar las funciones menos utilizadas.

Este proceso se llama Ataque Superficie Reducción

Regla 80/20: si el 80 % de la población no utiliza la función, esta debe desactivarse de forma predeterminada.

Una de las formas más simples y efectivas de reducir la superficie de ataque es reemplazar los protocolos de red anónimos con protocolos de red autenticados.

Ventanas Server 2003 es un servidor y no una plataforma cliente. Navegador web Internet Se eliminó de manera predeterminada la compatibilidad con todo código móvil de Explorer

Defensas de la cuenta

El principio del mínimo privilegio dicta que los usuarios deben operar con el privilegio suficiente para realizar las tareas, y no más

Windows XP y Windows Server 2003 agregan una función llamada “Inicio de sesión secundario” que permite que una cuenta de usuario haga clic derecho en una aplicación, seleccione “Ejecutar como…” y luego ingrese otra cuenta de usuario y contraseña para ejecutar la aplicación.

Un token restringido es un token de hilo con privilegios eliminados y/o SID marcados como SID de solo denegación

Control de cuentas de usuario (UAC)

- Cuando un usuario desea realizar una operación privilegiada, se le solicita que ingrese el nombre de cuenta y la contraseña de un administrador.
- Si el usuario es administrador, se le solicita su consentimiento para la operación.
- A menudo denominado "inicio de sesión por encima del hombro"

Servicio de bajo privilegio Cuentas

- La cuenta de servicio local y la cuenta de servicio de red permiten que un servicio tenga acceso local o de red, pero los procesos que se ejecutan con estas cuentas operan con un nivel de privilegio mucho más bajo.
  - o Ninguna de estas cuentas es miembro del grupo del administrador local.
- RPCSS
  - o Se ejecutó como la cuenta del sistema (la cuenta más privilegiada en Windows) en versiones de Windows anteriores a Windows XP SP2
  - o En XP SP2, RPCSS se dividió en dos y se creó un nuevo servicio llamado DCOM.
    Se creó el iniciador de procesos del servidor ---- RPCSS se ejecuta como el de privilegios más bajos
    La cuenta de servicio de red y DCOM se ejecutan como SISTEMA
    - Apache, OpenSSH e Internet Information Services (IIS)6 y posteriores
      También utiliza este modelo
    - Una pequeña cantidad de código se ejecuta con identidad elevada y relacionada
      Los componentes se ejecutan con una identidad más baja

Despojándose de privilegios

Otra defensa útil es quitarle privilegios a una cuenta cuando se inicia la aplicación y debe realizarse muy temprano en el código de inicio de la aplicación.

(Ajustar privilegios de token)

Windows Vista y versiones posteriores también agregan una función para definir el conjunto de privilegios que necesita un servicio para ejecutarse correctamente.
(ChangeServiceConfig2)

Defensas de red – IPSec y IPv6

- La razón por la que ocurren los ataques de denegación de servicio distribuido (DDoS) es porque IPv4 es un protocolo no autenticado.
- El UDP es uno de los peores infractores porque es un protocolo sin conexión
- Incluso con TCP, el paquete SYN inicial no está autenticado y un conjunto de servidores de ataque podría incapacitar fácilmente a un servidor vulnerable en el Internet mediante el envío de millones de paquetes TCP SYN falsos
- Tanto IPSec como IPv6 admiten redes autenticadas. paquetes

Defensas de red – Cortafuegos

- Todas las versiones de Windows desde XP incluyen un firewall de software integrado
- La versión incluida con XP estaba limitada en que:
  - No estaba habilitado por defecto
  - Su configuración se limitó a bloquear únicamente las conexiones entrantes en direcciones específicas. puertos
- Cambios en XP SP2
  - Opción para abrir un puerto a Internet --- pero sólo en la subred local --- para que los usuarios con múltiples computadoras en el hogar puedan compartir archivos e imprimir documentos
  - El firewall está habilitado de forma predeterminada
- Cambios en Vista y versiones posteriores
  - El firewall es un componente totalmente integrado de la red TCP/IP reescrita. pila
  - El firewall admite opcionalmente el bloqueo de conexiones salientes

Corrupción de la memoria Defensas

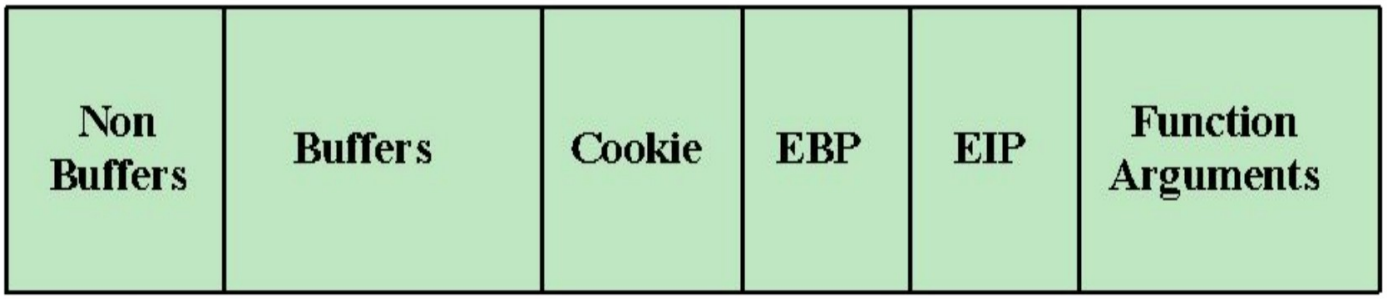
La mayoría de los sistemas operativos y software utilizados hoy en día están escritos en los lenguajes de programación C y C++.

C fue diseñado como un lenguaje ensamblador de alto nivel y debido a eso, le da al desarrollador acceso directo a la memoria a través de punteros y con esta funcionalidad viene el riesgo de tener la capacidad de corromper la memoria.

Convertir C y C++ a otro lenguaje sería una tarea monumental y no resuelve el problema real de que los desarrolladores de software confían demasiado en los datos que reciben.

Tiene vulnerabilidades de corrupción de memoria cuando la aplicación no restringe las operaciones de escritura a las ubicaciones de memoria correctas

(a) Without /GS option



(b) With /GS option

Figure 26.2 Stack Layout in Windows Vista

No ejecutar

Nombrado NX por Micro avanzado Dispositivos (AMD), Ejecución de datos Prevención (DEP) por Microsoft y la ejecución Desactivar (XD) por Intel, esta tecnología requiere soporte de CPU que ayuda a evitar que el código se ejecute en segmentos de datos

El más moderno Las CPU Intel admiten esta capacidad hoy en día y todas las actuales Las CPU AMD son compatibles con NX

Basado en ARM Las CPU también admiten NX

El soporte DEP se introdujo por primera vez en Windows XP SP2 y es una defensa de importancia crítica en Ventanas

El objetivo de NX es evitar la ejecución de datos.

De forma predeterminada, la mayoría de los componentes del sistema en Windows y las aplicaciones pueden usar NX vinculándose con el Opción del enlazador /NXCOMPAT

Aleatorización de pila

Esta defensa está disponible únicamente en Windows Vista y versiones posteriores

Cuando se inicia un hilo en Windows, el sistema operativo aleatorizará la dirección base de la pila en 0-31 páginas.

Una vez elegida la página, se elige un desplazamiento aleatorio dentro de la página y la pila comienza desde ese punto.

El propósito de la aleatorización es eliminar parte de la previsibilidad del atacante.

Buffer basado en montón Detección de desbordamiento

- Los desbordamientos de búfer basados en el montón son explotables y Puede conducir a la ejecución del código
- La primera defensa del montón, agregada a XP SP2, es agregar un valor aleatorio a cada bloque del montón y detectar que esta cookie no ha sido alterada.
  - o Si la cookie ha cambiado, el montón se ha dañado y el La aplicación podría verse obligada a bloquearse
  - o Nota: el bloqueo de la aplicación no se debe a la inestabilidad en la aplicación causada por la corrupción de datos, sino que el administrador del montón detecta la corrupción y hace que la aplicación falle.
  - o El proceso de cerrar una aplicación de esta manera a menudo se denomina "parada de emergencia"
- La segunda defensa es la comprobación de la integridad del montón.
  - o Cuando se liberan los bloques del montón, se verifica la validez de los metadatos en las estructuras de datos del montón y, si los datos se ven comprometidos, el bloque del montón se filtra o la aplicación se bloquea.

Aleatorización de montón

Diseñado para quitarle algo de previsibilidad al atacante.

Cuando se crea un montón, el inicio del montón se desplaza entre 0 y 4 MB.

Esta característica es nueva para Windows Vista

Aleatorización de imágenes

Cuando se inicia el sistema operativo, se inicia en una de 256 configuraciones (en otras palabras, todo el sistema operativo se desplaza hacia arriba o hacia abajo en la memoria cuando se inicia).

Esto hace que el sistema operativo sea menos predecible para los atacantes y hace que sea menos probable que una explotación tenga éxito.

Política de reinicio del servicio

En Vista, Microsoft configuró algunos de los servicios críticos para que se reiniciaran solo dos veces, después de lo cual el servicio no se reiniciará a menos que el administrador lo reinicie manualmente.

Esto le da al atacante solo dos intentos para que el ataque funcione.

Defensas del navegador

- Una página web maliciosa podría aprovechar muchos vectores de ataque posibles
  - o El código y los datos crean un entorno de usuario final rico y productivo, pero es difícil protegerlos.
  - o Los navegadores web también pueden representar diversos objetos multimedia; muchos formatos de archivos son representados por objetos auxiliares llamados controladores MIME.

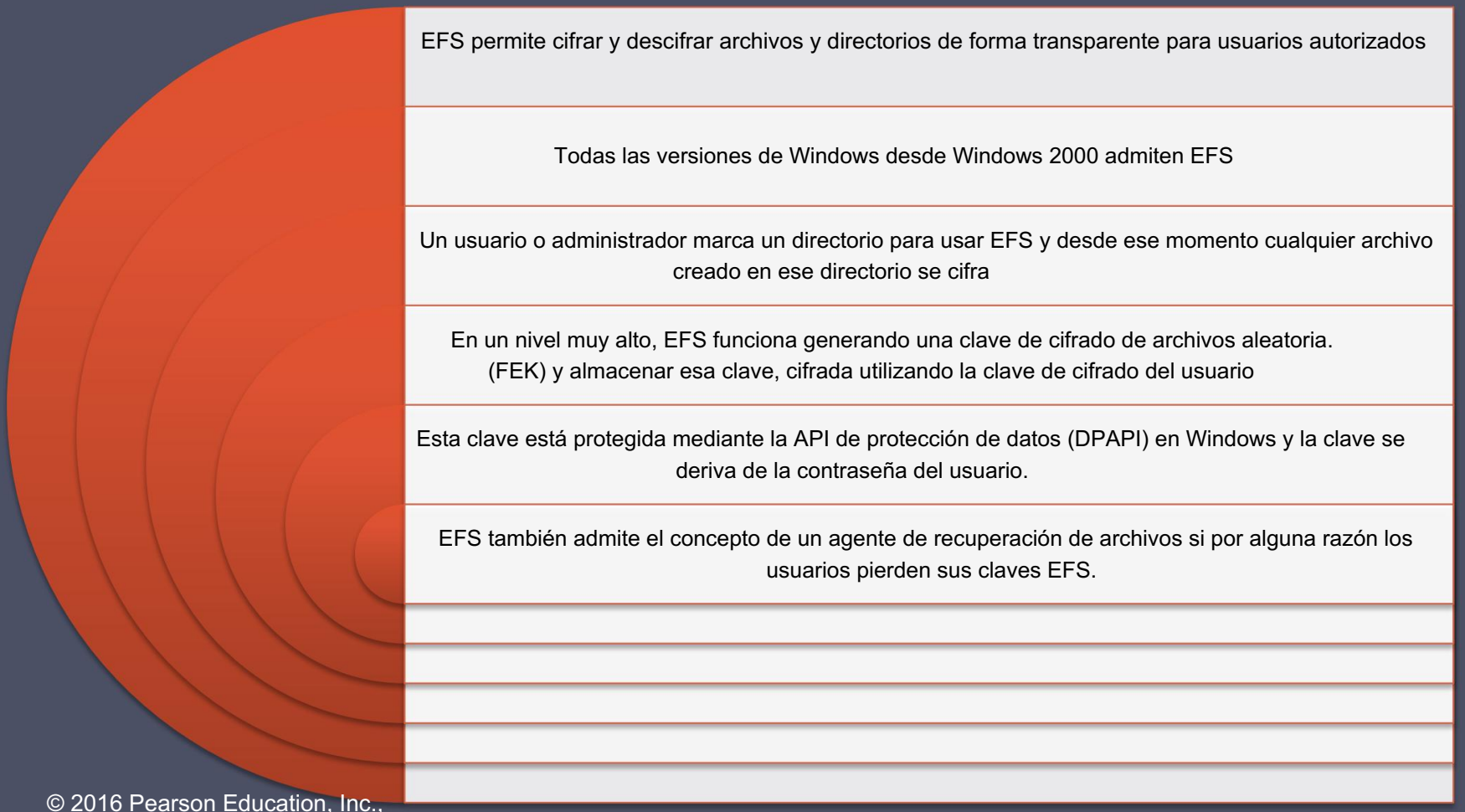
- Opción de inclusión activa de ActiveX
  - o Nueva característica agregada por Internet Explorer
  - o Básicamente, descarga los controles ActiveX de forma predeterminada y, cuando se utiliza un control por primera vez, se le solicita al usuario que permita que el control se ejecute.
- Modo protegido
  - o Cuando se utiliza esta configuración predeterminada, Internet Explorer se ejecuta a baja velocidad. nivel de integridad, lo que hace más difícil que el malware manipule el sistema operativo, que opera en un nivel de integridad medio o superior
- ASLR y DEP
  - o Las versiones actuales de Internet Explorer también las habilitan de forma predeterminada.

Defensas del navegador

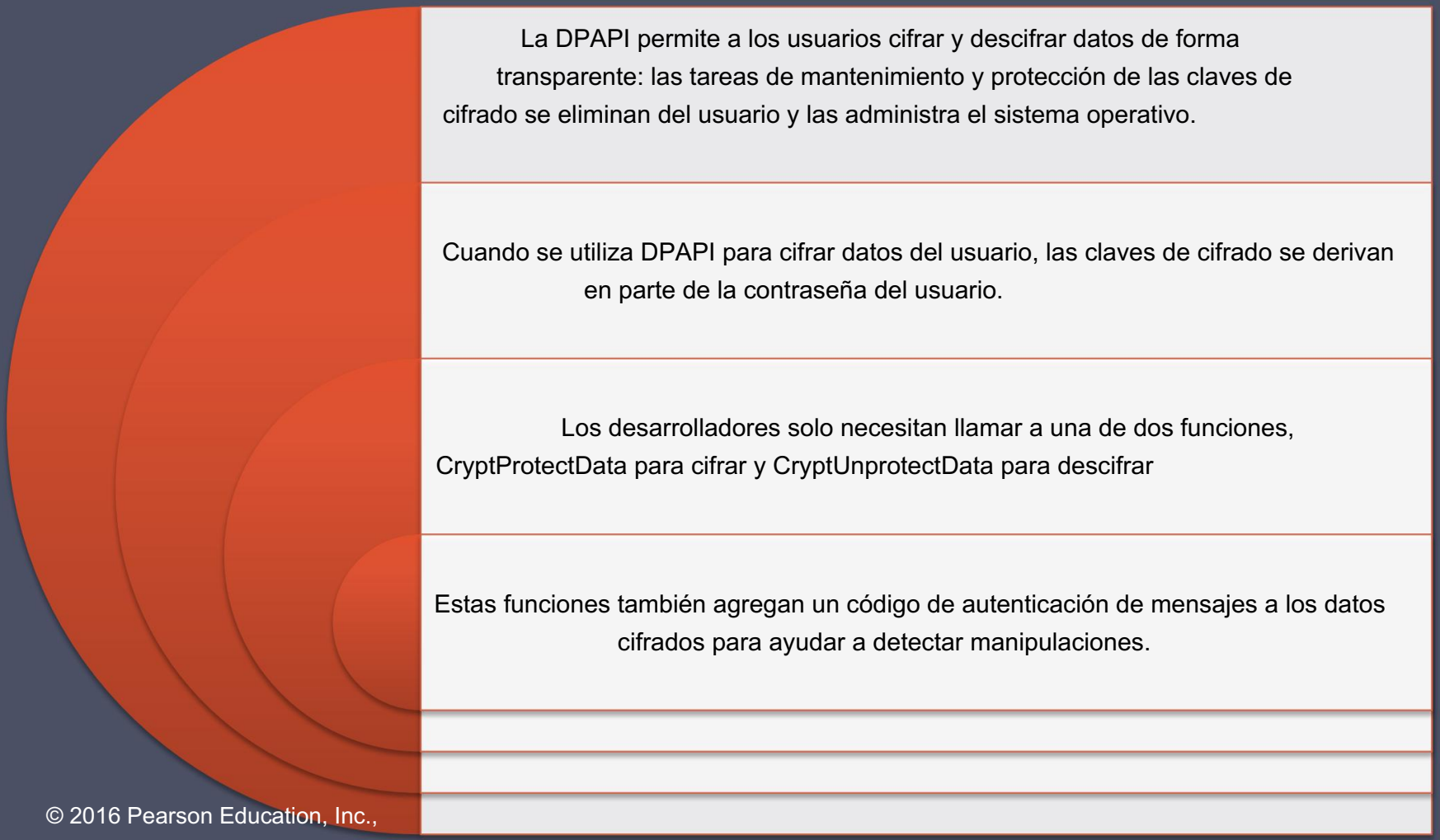
- Es importante señalar que el Modo Protegido, DEP y ASLR solo ayudan a mitigar las vulnerabilidades de corrupción de memoria, no ayudan a proteger contra ataques de phishing o vulnerabilidades comunes específicas de la web, como secuencias de comandos entre sitios (XSS).
- Microsoft agregó defensas a Internet Explorer para ayudar a resolver estos problemas
  - o En primer lugar, una lógica de detección de secuencias de comandos entre sitios para ayudar a detectar y prevenir algunas clases de XSS
  - o La segunda defensa es un filtro de phishing: cuando un usuario visita un sitio web, la URL del sitio se envía a un servicio que determina si el sitio es un sitio conocido de phishing o distribución de malware y se advierte al usuario si el sitio es sospechoso.
  - o Una defensa final para ayudar a evitar que los usuarios sean rastreados es un modo de mejora de la privacidad llamado modo InPrivate, que no conserva las cookies ni el historial del sitio.

Servicios criptográficos –

Sistema de cifrado de archivos (EFS)



Servicios criptográficos – API de protección de datos (DPAPI)



Servicios criptográficos – BitLocker

Windows agrega una defensa muy necesaria al sistema operativo, Cifrado de unidad BitLocker

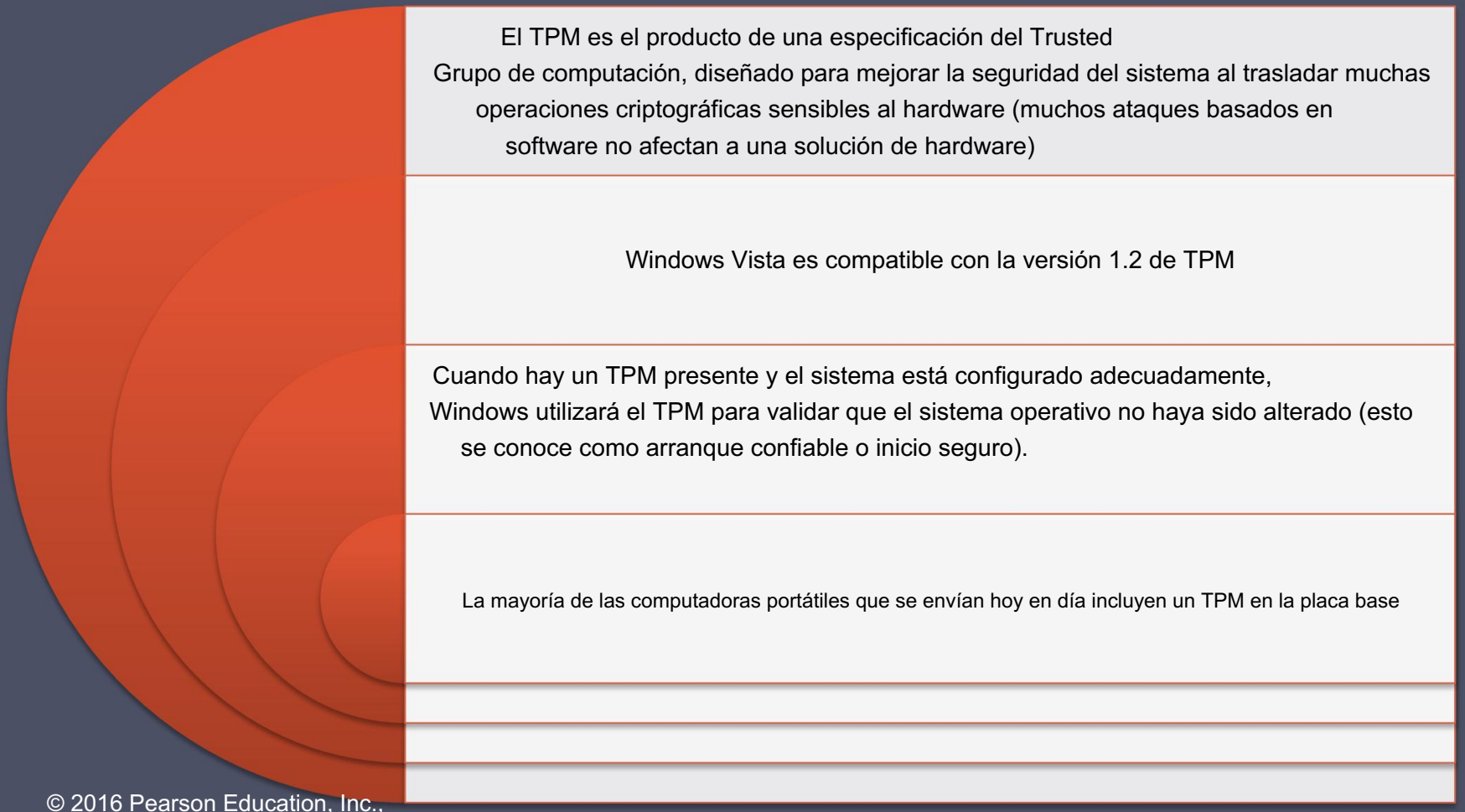
La principal amenaza que esta tecnología ayuda a mitigar es la divulgación de datos en computadoras portátiles robadas.

BitLocker cifra todo el volumen mediante AES y la clave de cifrado se almacena en una unidad USB o dentro de un módulo de plataforma confiable. Chip (TPM) en la placa base del ordenador

Al iniciar un sistema que requiere el dispositivo USB, el dispositivo debe estar presente para que la computadora pueda leer las claves, después de lo cual BitLocker descifra el disco duro (la desventaja es si se pierde el dispositivo)

Quizás el aspecto más importante de BitLocker es que la política de BitLocker se puede configurar como una política para una sola computadora y esa política se puede "enviar" a las computadoras que usan Active Directory.

Servicios criptográficos – Módulo de plataforma confiable (TPM)



Criterios comunes

Las versiones de Windows posteriores a Windows 2000 obtuvieron Common Criteria EAL4 + Flaw Remediation (ALC_FLR.3) o están en proceso de obtener la acreditación.

Lo que es de importancia crítica sobre el trabajo que Microsoft ha realizado para obtener la acreditación de sus sistemas operativos es que la pila de software (el objetivo de seguridad) que se evalúa es utilizable.

Resumen

- Fundamental

  Arquitectura de seguridad de Windows

- Vulnerabilidades de Windows
- Defensas de seguridad de Windows

- Defensas del navegador
- Servicios criptográficos
- Criterios comunes