Seguridad en Sistemas Operativos Modernos

Ciberseguridad – FPUNA

2024-05-23

Contenido

1. Introducción
2. Estados privilegiados y no privilegiados.
3. Procesos e hilos de aplicaciones.
4. Memoria
5. Sistemas de archivos
6. Virtualización. Hipervisores.
7. Creación y operación de tecnología de virtualización.
8. Principios fundamentales de diseño de seguridad aplicados a un sistema operativo.
9. Controles de Acceso.
10. Separación de dominios, aislamiento de procesos, encapsulación de recursos, disminuir privilegios.

Procesos e hilos

Procesos e hilos (Threads)

- Son unidades fundamentales de ejecución que permiten la gestión eficiente de recursos y la ejecución concurrente de múltiples tareas.

Procesos

- Un proceso es una instancia en ejecución de un programa. Cada proceso tiene su propio espacio de memoria, recursos asignados y estado de ejecución.
- Los procesos se crean, ejecutan y terminan por el sistema operativo, que gestiona su concurrencia y sincronización para garantizar un funcionamiento ordenado y eficiente.

Hilos (Threads)

- Un hilo es una unidad de ejecución dentro de un proceso. Múltiples hilos pueden coexistir dentro de un mismo proceso, compartiendo su espacio de memoria y recursos.
- Los hilos permiten una ejecución más eficiente de tareas dentro de un proceso, especialmente para operaciones que pueden ejecutarse de forma independiente.

Seguridad en Procesos e Hilos

- La seguridad de los procesos e hilos se aborda mediante una combinación de mecanismos del sistema operativo, prácticas de programación seguras y medidas de seguridad a nivel de aplicación.

Mecanismos del sistema operativo

- Aislamiento de procesos y memoria
- Protección de memoria
- Control de acceso
- Sincronización de hilos
- Aislamiento de hilos

Prácticas de programación seguras

- **Programación defensiva**: Escribir código que sea resistente a entradas y condiciones inesperadas para evitar errores y ataques.
- **Validación de entradas**: Validar cuidadosamente las entradas de usuario y datos externos para evitar inyecciones de código o datos maliciosos.
- **Gestión de memoria segura**: Utilizar técnicas de gestión de memoria seguras, como la asignación dinámica de memoria con liberación adecuada, para evitar fugas de memoria y ataques de desbordamiento de búfer.

Medidas de seguridad a nivel de aplicación

- **Control de acceso basado en roles**: Limitar el acceso a recursos y funcionalidades de la aplicación en función de los roles y privilegios de los usuarios.
- **Cifrado de datos**: Cifrar datos confidenciales en reposo y durante la transmisión para protegerlos de accesos no autorizados.
- **Análisis de vulnerabilidades**: Realizar análisis de vulnerabilidades regulares para identificar y corregir debilidades de seguridad en la aplicación.

Seguridad en Procesos

- **Aislamiento de procesos**: Cada proceso tiene su propio espacio de memoria, lo que evita que un proceso acceda o modifique los datos de otro proceso. Esto ayuda a contener el impacto de errores o ataques maliciosos.
- **Protección de memoria**: El sistema operativo utiliza mecanismos de protección de memoria para evitar que un proceso acceda a áreas de memoria no asignadas o privilegiadas. Esto ayuda a prevenir la ejecución de código malicioso o la corrupción de datos críticos.
- **Control de acceso**: El sistema operativo controla el acceso de los procesos a recursos del sistema, como archivos, dispositivos y servicios de red. Esto ayuda a prevenir que procesos no autorizados accedan a recursos sensibles.

Seguridad en Hilos

- **Sincronización de hilos**: Los hilos dentro de un proceso deben sincronizarse para acceder y modificar recursos compartidos de forma segura. El sistema operativo proporciona mecanismos de sincronización, como semáforos y mutex, para evitar conflictos y garantizar la integridad de los datos.
- **Aislamiento de hilos**: Aunque los hilos comparten el espacio de memoria del proceso, existen mecanismos para aislar su ejecución y evitar que un hilo malicioso afecte a otros hilos del mismo proceso.
- **Seguridad de las bibliotecas compartidas**: Los hilos pueden acceder a bibliotecas compartidas que contienen código de terceros. Es importante asegurarse de que estas bibliotecas sean confiables y no contengan vulnerabilidades que puedan ser explotadas por hilos maliciosos.

Memoria

Memoria

- La memoria es un componente crucial que almacena datos e instrucciones de forma temporal para que el sistema pueda funcionar. Es como un espacio de trabajo temporal donde se procesa la información en tiempo real.

Tipos de memoria

- **Memoria RAM (Random Access Memory)**: Es la memoria volátil, lo que significa que se borra cuando se apaga la computadora. Almacena datos e instrucciones que el procesador necesita para ejecutar programas y realizar tareas. La cantidad de RAM disponible determina la cantidad de programas que se pueden ejecutar simultáneamente y la velocidad general del sistema.
- **Memoria ROM (Read-Only Memory)**: Es la memoria no volátil, lo que significa que conserva los datos incluso cuando se apaga la computadora. Almacena información esencial del sistema, como el BIOS, que es el programa que inicia la computadora cuando se enciende.

La memoria en los Sistemas Operativos

- Los sistemas operativos gestionan la memoria de manera eficiente para garantizar que los programas tengan acceso a los recursos que necesitan

Gestión de la Memoria

- **Asignación de memoria**: El sistema operativo asigna espacio en la memoria RAM a cada programa que se ejecuta.
- **Paginación**: Cuando la memoria RAM se llena, el sistema operativo puede mover algunos datos a un almacenamiento temporal en el disco duro, liberando espacio en la RAM para otras tareas.
- **Intercambio**: Si la memoria RAM se agota por completo, el sistema operativo puede intercambiar programas completos entre la RAM y el disco duro.

Medidas de seguridad en la gestión de la Memoria

- **Prevención de ataques de desbordamiento de buffer**: Estos ataques intentan sobrescribir datos en la memoria con código malicioso. Los sistemas operativos modernos utilizan técnicas como ASLR (Address Space Layout Randomization) para dificultar estos ataques.
- **Protección de la memoria**: Los sistemas operativos pueden aislar la memoria de cada programa para evitar que un programa malicioso acceda a los datos de otro programa.
- **Encriptación de la memoria**: La memoria puede ser encriptada para proteger los datos confidenciales de ser accedidos si la computadora se pierde o es robada.

Prevención de ataques de desbordamiento de buffer

- **ASLR (Address Space Layout Randomization)**: Esta técnica aleatoriza la distribución de la memoria en el espacio de direcciones del programa, dificultando que los atacantes predigan la ubicación de los datos sensibles.
- **W^X (Write-eXecute)**: Esta característica marca ciertas áreas de memoria como no ejecutables, lo que impide que el código malicioso se ejecute directamente en la memoria.
- **DEP (Data Execution Prevention)**: Esta tecnología evita que los datos en la memoria se ejecuten como código, bloqueando la ejecución de código malicioso que se ha introducido en la memoria.

Protección de la memoria

- **Aislamiento de la memoria**: Los sistemas operativos pueden aislar la memoria de cada programa para evitar que un programa malicioso acceda a los datos de otro programa. Esto se logra mediante técnicas como MMU (Memory Management Unit) y sandboxing.
- **Control de acceso a la memoria**: Los sistemas operativos implementan mecanismos de control de acceso para regular el acceso a la memoria. Solo los programas autorizados pueden acceder a áreas específicas de la memoria.

Encriptación de la memoria

- **Encriptación de la memoria en reposo**: La memoria puede ser encriptada cuando la computadora está apagada o en reposo, protegiendo los datos confidenciales en caso de pérdida o robo del dispositivo.
- **Encriptación de la memoria en uso**: Algunas tecnologías permiten encriptar la memoria mientras la computadora está en uso, brindando un nivel de seguridad aún mayor.

Sistemas de archivos

Sistemas de archivos

Conjunto de estructuras de datos y algoritmos que permiten:

- Almacenar y organizar datos en un dispositivo de almacenamiento persistente.
- Acceder a los datos de forma eficiente y segura.
- Administrar el espacio de almacenamiento en el dispositivo.
- Proteger los datos contra accesos no autorizados y corrupción.

Sistemas de archivos en los Sistemas Operativos

Cada sistema operativo utiliza sus propios tipos de sistemas de archivos, ya que tienen diferentes necesidades y características. Por ejemplo:

- **Windows**: Utiliza principalmente NTFS (New Technology File System) y exFAT (Extended File Allocation Table).
- **macOS**: Utiliza HFS+ (Hierarchical File System Plus) y APFS (Apple File System).
- **Linux**: Utiliza ext4 (Fourth Extended File System), entre otros.

El sistema operativo reconoce y trabaja con el sistema de archivos del dispositivo de almacenamiento para poder leer, escribir y gestionar los datos.

Medidas de seguridad en los Sistemas de Archivos

- **Control de acceso**: Limitar quién puede acceder a los datos y qué acciones pueden realizar.
- **Cifrado**: Codificar los datos para que solo puedan ser leídos por usuarios autorizados.
- **Permisos**: Asignar permisos específicos a cada usuario o grupo de usuarios, indicando qué operaciones pueden realizar sobre los archivos.
- **Copias de seguridad**: Crear copias de seguridad regulares de los datos para recuperarlos en caso de pérdida o corrupción.

Virtualización. Hipervisores

Virtualización

Tecnología que permite crear entornos informáticos virtuales, independientes y aislados dentro de un solo computador físico.

Hipervisor

- Es un software que actúa como el maestro de ceremonias, gestionando los recursos del computador físico y asignándolos a las diferentes máquinas virtuales (MV) que se ejecutan simultáneamente.
- El hipervisor crea una capa de abstracción que aísla cada MV, permitiendo que funcionen de forma independiente sin interferir entre sí.

Tipos de Hipervisores

- **Hipervisor de tipo 1 (bare metal)**: Se instala directamente en el hardware del host, proporcionando control completo sobre los recursos físicos. Es más eficiente y ofrece mayor seguridad, pero requiere conocimientos técnicos especializados para su administración. Ejemplos: VMware ESXi, Microsoft Hyper-V.
- **Hipervisor de tipo 2 (hospedado)**: Se ejecuta como un programa dentro de un sistema operativo host existente. Es más fácil de instalar y usar, pero consume más recursos y puede tener un impacto leve en el rendimiento del sistema operativo host. Ejemplos: VirtualBox, VMware Workstation Player.

Seguridad en los hipervisores

- **Aislamiento**: El aislamiento proporcionado por el hipervisor ayuda a prevenir ataques entre máquinas virtuales.
- **Control de acceso**: El hipervisor restringe el acceso a los recursos del sistema solo a usuarios y procesos autorizados.
- **Actualizaciones de seguridad**: Es importante aplicar actualizaciones de seguridad regularmente para corregir vulnerabilidades en el hipervisor.
- **Monitoreo y registro**: El monitoreo y registro de las actividades del hipervisor puede ayudar a detectar y prevenir intrusiones.

Seguridad en Sistemas Operativos hosts Hipervisores tipo 2

- **Firewall**: Un firewall puede bloquear el acceso no autorizado a la máquina virtual desde redes externas.
- **Software antivirus y anti-malware**: Es fundamental instalar y mantener software antivirus y anti-malware actualizado para proteger la máquina virtual contra malware.
- **Políticas de seguridad**: Implementar políticas de seguridad sólidas, como control de acceso de usuarios y contraseñas seguras, puede ayudar a prevenir intrusiones.
- **Actualizaciones del sistema operativo**: Aplicar actualizaciones del sistema operativo regularmente para corregir vulnerabilidades de seguridad.

Creación y operación de tecnología de virtualización

Tecnología de Virtualización

- La virtualización, si bien ofrece grandes beneficios, también introduce nuevos desafíos de seguridad que deben ser considerados y mitigados para proteger los entornos virtualizados.

Aspectos de seguridad en la creación de entornos virtualizados

- **Elección del hipervisor**: El hipervisor es el componente central de un entorno virtualizado, por lo que es crucial seleccionar uno que tenga un historial probado de seguridad y que reciba actualizaciones de seguridad regulares.
- **Configuración segura del hipervisor**: El hipervisor debe configurarse de forma segura para minimizar la superficie de ataque. Esto incluye medidas como habilitar la autenticación fuerte, deshabilitar servicios innecesarios y aplicar las últimas correcciones de seguridad.
- **Aislamiento de las máquinas virtuales**: Las máquinas virtuales (VM) deben aislarse entre sí y del servidor host para evitar que un ataque en una VM pueda afectar a las demás. Esto se puede lograr mediante el uso de redes virtuales, grupos de seguridad y otras técnicas de aislamiento.
- **Protección de datos**: Los datos almacenados en las VM deben protegerse mediante el cifrado, el control de acceso y otras medidas de seguridad.
- **Gestión de identidades y accesos**: Es importante implementar un sistema de gestión de identidades y accesos (IAM) para controlar el acceso a las VM y a los recursos del servidor host.

Aspectos de seguridad en la operación de entornos virtualizados

- **Monitoreo y registro**: Es importante monitorear los entornos virtualizados para detectar actividades sospechosas y registrar todos los eventos de seguridad.
- **Actualizaciones de software**: Es importante aplicar las últimas actualizaciones de seguridad al hipervisor, a las VM y al software que se ejecuta en las VM.
- **Pruebas de penetración**: Es recomendable realizar pruebas de penetración regulares para identificar y corregir las vulnerabilidades de seguridad.
- **Capacitación del personal**: Es importante capacitar al personal sobre los riesgos de seguridad de la virtualización y las mejores prácticas para mitigarlos.

Herramientas de seguridad para entornos virtualizados

Existen diversas herramientas de seguridad disponibles para ayudar a proteger los entornos virtualizados. Estas herramientas pueden proporcionar funciones como:

- **Análisis de vulnerabilidades**: Identifica las vulnerabilidades en el hipervisor, las VM y el software que se ejecuta en las VM.
- **Detección de intrusiones**: Detecta actividades sospechosas en los entornos virtualizados.
- **Prevención de intrusiones**: Evita que los ataques se ejecuten en los entornos virtualizados.
- **Protección de datos**: Cifra y protege los datos almacenados en las VM.

Principios fundamentales de diseño de seguridad aplicados a un sistema operativo

Principios fundamentales de diseño de seguridad

- Conjunto de directrices que ayudan a crear sistemas operativos más seguros y confiables. Con estos principios, los desarrolladores pueden crear sistemas que sean más resistentes a ataques y que protejan mejor los datos de los usuarios.

Principios fundamentales de diseño de seguridad

- 1. Principio de mínima confianza
- 2. Defensa en profundidad
- 3. Falla segura
- 4. Separación de privilegios
- 5. Menor superficie de ataque
- 6. Protección contra errores de software
- 7. Cifrado
- 8. Gestión de identidades y accesos
- 9. Monitoreo y registro
- 10. Actualizaciones y parches

1. Principio de mínima confianza

Establece que ningún componente del sistema debe tener más privilegios de los que necesita para realizar su función. Esto ayuda a limitar el daño que puede causar un componente si se ve comprometido.

2. Defensa en profundidad

Se deben implementar múltiples capas de seguridad para proteger el sistema. Esto hace que sea más difícil para los atacantes penetrar en el sistema y, si lo logran, les dificulta escalar sus privilegios y acceder a datos confidenciales.

3. Falla segura

El sistema debe diseñarse de manera que, en caso de fallo, se encuentre en un estado seguro. Esto ayuda a prevenir que los errores o fallos del sistema sean explotados por los atacantes.

4. Separación de privilegios

Las tareas críticas del sistema deben realizarse por diferentes componentes con diferentes privilegios. Esto ayuda a prevenir que un atacante que comprometa un componente pueda realizar tareas críticas.

5. Menor superficie de ataque

Se debe minimizar la cantidad de código y interfaces expuestas a los usuarios y atacantes. Esto ayuda a reducir el número de posibles puntos de entrada para ataques.

6. Protección contra errores de software

El sistema debe diseñarse de manera que sea resistente a errores de software. Esto incluye la validación de entrada, la gestión de errores y las pruebas exhaustivas

7. Cifrado

Los datos confidenciales deben cifrarse tanto en reposo como en tránsito. Esto ayuda a proteger los datos contra el acceso no autorizado, incluso si el sistema se ve comprometido.

8. Gestión de identidades y accesos

El sistema debe implementar mecanismos sólidos para la gestión de identidades y accesos. Esto ayuda a garantizar que solo los usuarios autorizados puedan acceder a los recursos del sistema.

9. Monitoreo y registro

El sistema debe registrar los eventos de seguridad y que estos registros deben ser monitoreados para detectar actividades sospechosas. Esto ayuda a identificar y responder a los ataques de manera oportuna.

10. Actualizaciones y parches

El sistema debe mantenerse actualizado con los últimos parches de seguridad. Esto ayuda a proteger el sistema contra las vulnerabilidades conocidas.

Consideraciones de seguridad adicionales

Además de los principios fundamentales de diseño de seguridad, existen otras consideraciones importantes al diseñar un sistema operativo seguro. Estas consideraciones incluyen:

- **Amenazas**: Es importante identificar las amenazas potenciales a las que está expuesto el sistema operativo. Esto ayudará a determinar qué tipos de medidas de seguridad son necesarias.
- **Requisitos de seguridad**: El sistema operativo debe cumplir con todos los requisitos de seguridad relevantes, como los establecidos por las leyes y regulaciones.
- **Facilidad de uso**: Las medidas de seguridad no deben dificultar el uso del sistema operativo para los usuarios legítimos.

Al considerar todos estos factores, es posible crear un sistema operativo que sea seguro, confiable y fácil de usar.