Fundamentos de la Ciberseguridad

Ciberseguridad – FPUNA

Contenido

- Principios de Diseño
  - Modularidad
  - Simplicidad de Diseño (Economizar mecanismos)
  - Layering (Defensa en Profundidad)
- Principios de Autorización
  - Separación
  - Complete Mediation
  - Menor Privilegio
  - Seguro ante fallas (Fail Safe Defaults/Fail Secure)
- Principios de Minimización
  - Aislamiento (Isolation)
  - Encapsulamiento
- Usabilidad
- Diseño Abierto
- Least Astonishment
- Relaciones de Confianza
- Minimizar la superficie de confianza

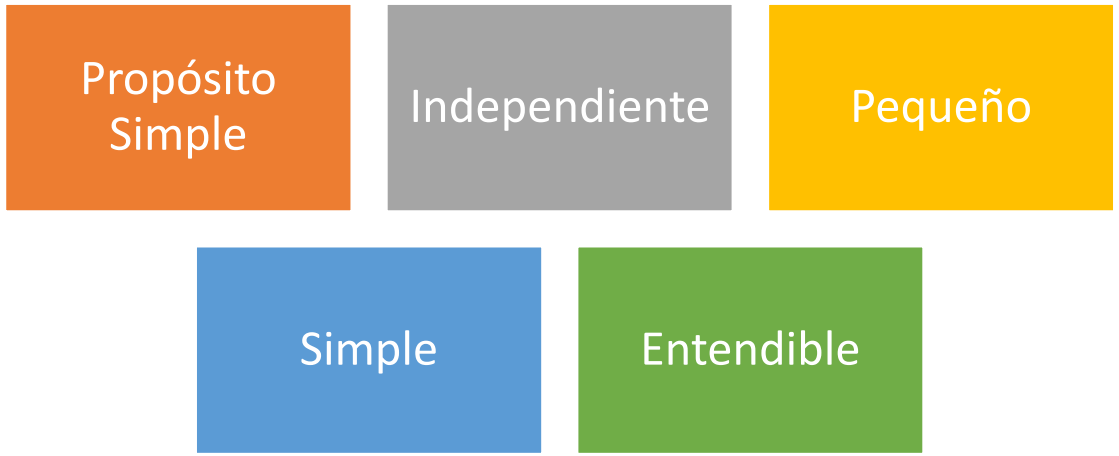
Introducción

- Carlos es un desarrollador de software. Su objetivo es crear un diseño que haga la tarea prevista, sea eficiente, efectivo y usable. Carlos utiliza principios de diseño de seguridad para ayudarlo a lograr los principios fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad del sistema, subsistema y datos del sistema.

Principios de Diseño

Modularidad

- Carlos subdividirá un sistema en partes o módulos más pequeños que pueden crearse de forma independiente y utilizarse después en varios sistemas. El desarrollo de funciones de seguridad como módulos separados y protegidos.



Simplicidad de Diseño (Economizar mecanismos)

- Cuando Carlos diseña una medida de seguridad, debe ser lo más sencilla y pequeña posible.

Layering (Defensa en Profundidad)

- Carlos utilizará enfoques de protección múltiples y superpuestos para abordar los aspectos humanos, tecnológicos y operativos de los sistemas de información. La defensa en profundidad protege con una serie de mecanismos de seguridad, de modo que si uno falla, los demás estarán en su sitio.

Principios de Autorización

Separación

- Carlos utiliza una práctica en la que se requieren múltiples atributos de privilegio para lograr el acceso a un recurso restringido.
- Los datos y/o sistemas se separan en dominios definidos lógicamente, y la comunicación entre dominios debe estar autorizada.

Complete Mediation

- Carlos debe comprobar cada acceso con la configuración de control de acceso para asegurarse de que el acceso está permitido.

Menor privilegio

- Carlos se asegurará de que cada proceso y cada usuario del sistema operen utilizando el menor conjunto de privilegios necesarios para realizar la tarea.

Seguro ante fallas (Fail Safe Defaults/Fail Secure)

- Carlos tomará decisiones de acceso basadas en el permiso y no en la exclusión. Si un hacker introduce información incorrecta, el sistema debe rechazar el intento con un mensaje que indique que el inicio de sesión ha fallado y no indicar que sólo la contraseña era incorrecta.

Principios de Minimización

Aislamiento (Isolation)

- Carlos sabe que los sistemas de acceso público deben estar aislados de los recursos críticos (datos, procesos, etc.) para evitar su divulgación o manipulación.
- Los sistemas operativos utilizan varias tecnologías de hardware y software para imponer el aislamiento de procesos. Por ejemplo, los procesos y archivos de usuarios individuales deben estar aislados unos de otros excepto cuando se desee explícitamente.

Encapsulamiento (Encapsulation)

- Carlos puede utilizar una forma específica de aislamiento basada en la funcionalidad orientada a objetos. La encapsulación oculta los valores o el estado de un objeto de datos estructurado dentro de una clase (un dominio propio), impidiendo cualquier acceso directo por parte de terceros no autorizados.

Usabilidad

Usabilidad (Usability)

- Carlos quiere asegurarse de que sus usuarios puedan utilizar fácilmente y aprender rápidamente una herramienta, dispositivo o software.

Diseño Abierto

Diseño Abierto (Open Design)

- Carlos sabe que el diseño de un mecanismo de seguridad debe ser abierto y no depender del secreto de los detalles de diseño o implementación.
- Por ejemplo, RSA es un algoritmo de cifrado asimétrico basado en el principio de que es fácil multiplicar números grandes, pero factorizar números grandes es difícil. La clave pública consta de dos números. Uno de ellos es el resultado de multiplicar dos números primos grandes. La clave privada se obtiene a partir de los mismos dos números primos. La dificultad de factorizar números grandes es lo que mantiene seguro el par de claves.

Menor Asombro

Menor Asombro/Sorpresa (Least Astonishment)

- Carlos es consciente de que un programa o una interfaz de usuario debe responder siempre de la forma que menos asombre al usuario. Cuando Microsoft eliminó el botón Inicio de su sistema operativo, lanzó una versión actualizada que volvía a añadirlo.

Relaciones de Confianza

Relaciones de Confianza (Trust Relationships)

- Carlos debe mantener un límite de confianza. Entre los problemas que plantea el establecimiento de la confianza figuran los siguientes
  - Autenticar el otro extremo para evitar la suplantación de identidad.
  - Garantizar la seguridad de la comunicación para mantener la confidencialidad de los datos.
  - Impedir la manipulación de los datos para mantener su integridad.

Minimizar la superficie de confianza

Minimizar la superficie de confianza (Minimize Trust Surface)

- La confianza debe crearse, no asumirse. Debe haber distinciones claras entre los niveles de privilegio cuando Carlos accede a los recursos. Si Carlos se conecta y se autentica, también debe tener autorización para acceder a un recurso.