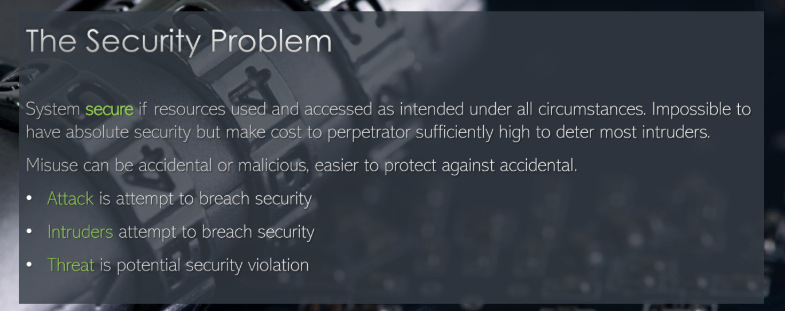
Operating System Concepts book

•

•

•

### **El problema de la seguridad**



### **Categorías de violación de seguridad**

Violación de la confidencialidad Lectura no autorizada de datos

Infracción de integridad Modificación no autorizada de datos

Infracción de disponibilidad Destrucción no autorizada de datos

Robo de servicio Uso no autorizado de recursos

Denegación de servicio (DOS) Prevención del uso legítimo

### **Métodos de violación de seguridad**

Enmascarando pretendiendo ser un usuario autorizado

(incumplimiento de autenticación)

Repetir ataque Repetir la transmisión de datos, a.s es o con

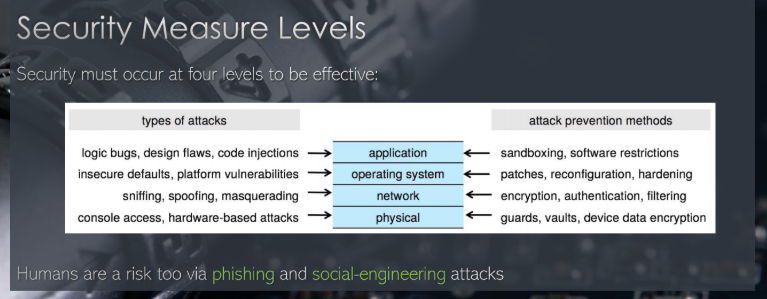
modificación del mensaje

Ataque de hombre en el medio Intruso se sienta en el flujo de datos, disfrazado de remitente

al receptor y viceversa

Secuestro de sesión Intercepte una sesión ya establecida para evitar la autenticación Escalada de privilegios Tipo de ataque común, otorga a los atacantes más privilegios de los que se supone que tienen.

### **Niveles de medidas de seguridad**



### 

### **Amenazas del programa**

Malware: software diseñado para explotar, deshabilitar o dañar

computadora.

Caballo de Troya, spyware

Secuestro de datos

Puerta trampa, bomba lógica

Inyección de código: se produce cuando el código del sistema no es malicioso pero tiene

errores que permiten agregar código ejecutable o

modificado.

Desbordamiento de búfer

Fragmento de código de virus incrustado en un programa legítimo.

gusano

### 

### **Principio de menor privilegio**

Todos los programas y todos los usuarios privilegiados del sistema deben operar con la menor cantidad de privilegios necesarios para completar el trabajo. El propósito de este principio es reducir la cantidad de interacciones potenciales entre programas privilegiados al mínimo necesario para operar correctamente, de modo que uno pueda desarrollar la confianza de que no ocurren usos de privilegios involuntarios, no deseados o inapropiados. ”- Jerome H. Saltzer , que describe un principio de diseño del sistema operativo Multics en 1974.

