TEMA 14
SEGURIDAD DE LOS SISTEMAS OPERATIVOS

14.1 INTRODUCCION A LA SEGURIDAD DE LOS SISTEMAS OPERATIVOS: La evolución de la computación y de las comunicaciones hasta hoy, ha hecho más accesibles a los sistemas informáticos, y se incrementado los riesgos con respecto a la seguridad.
la importancia de la seguridad de los sistemas informáticos es cada vez mayor por la expansión de las redes de computación y la comunicación de datos.
Los datos administrados por el sistema informático cada vez son mas confidenciados y críticos (Ej. trasferencia de fondos). Los sistemas deben funcionar sin interrupciones y sus problemas.
El S.O. como administrador de los recursos del sistema es importante en el aspecto de la seguridad pero se debe complementar con métodos externos al S.O.
El nivel de seguridad a proporcionar depende del valor de los recursos que hay que asegurar.

14.2 REQUISITOS DE SEGURIDAD: los requisitos de la seguridad de un sistema define lo que significa la seguridad para el sistema. los requisitos son la base para determinar si el sistema implementado es seguro.

14.3 UN TRATAMIENTO TOTAL DE LA SEGURIDAD: incluye aspectos de la seguridad del computador distinto a los de la seguridad de los S.O.
La *seguridad externa* debe asegurar la instalación computacional contra intrusos y desastres como incendios e inundaciones. Luego del acceso físico al S.O. se debe identificar al usuario antes de que acceda a los recursos "*Seguridad de la interfaz del usuario*".
La *seguridad interna* trata de los controles incorporados al hardware y al s. O. Para asegurar que son confiables, operable y la integridad de los programas y datos.

14.4 SEGURIDAD EXTERNA Y SEGURIDAD OPERACIONAL:
Seguridad externa. Consiste en:
- *Seguridad física. Proteccion contra desastres e intrusos.*
- *Seguridad operacional.*

La seguridad física incluye: la protección contra desastres (costoso y no se analiza en detalle, depende de las consecuencia de la pérdida) y la protección contra intrusos (usando sistemas de identificación física, tarjeta, voz…)
En la seguridad física importan los mecanismos de detección de humo, Sensores de calor, detección de movimiento.
Seguridad operacional. Consiste en las diferentes políticas y procedimientos implementados por la administración de la instalación computacional.
La *autorización* determina que acceso se permite y a quien.
La *clasificación* divide el problema en sub problemas: Los datos del sistema y los usuarios se dividen en clases y a cada clase se conceden diferentes derechos de acceso.
Un aspecto crítico es la selección y asignación de personal: que sea confiable, pero lo principal es la división de responsabilidades.
Para diseñar medidas efectivas de seguridad se debe:
- Enumerar y comprender las amenazas potenciales.
- Definir que grado de seguridad se desea (y cuanto se esta dispuesto a gastar en seguridad).
- Analizar las contramedidas disponibles.

14.5 VIGILANCIA, VERIFICACION DE AMENAZAS Y AMPLIFICACION
Vigilancia. Tiene que ver con: La verificación y la auditoria del sistema; La autentificación de los usuarios.
Los sistemas sofisticados de autentificación de usuarios es difíciles de evitar por los intrusos. El problema es que se puede rechazar a usuarios legítimos (ej. en un sistema de reconocimiento de voz que se puede llegar a rechazar a un usuario resfriado).
Verificación de amenazas. Es una técnica por lo que los usuarios no pueden tener acceso directo a un recurso. Solo lo tiene rutinas del S.O. llamados "PROGRAMAS DE VIGILANCIA". El usuario solicita el proceso al S.O., el S.O. niega o permite el acceso. El acceso lo hace un programa de vigilancia que pasa los resultados al programa del usuario, y permite detectar los intentos de penetración, el momento que se producen y advertir.
Amplificación. Se producen cuando un programa de vigilancia necesita para cumplir su meta mayores derechos de acceso de los que disponen los usuarios.

14.6 PROTECCION POR CONTRASEÑA: Las clases de elementos para establecer la identidad de una persona son:
Algo sobre la persona: Ej.: huellas digitales, registro de la voz, fotografía, firma, etc.
Algo poseído por la persona: Ej.: insignias especiales, tarjetas de identificación, llaves, etc.
Algo conocido por la persona: Ej.: contraseñas, combinaciones de cerraduras, etc.
El esquema más común de autentificación es la *protección por contraseña:* donde el usuario elige una palabra clave, la amenaza, la teclea para que la admita el sistema (la clave no se ve en pantalla).
Desventajas: los usuarios tienden a elegir contraseñas fáciles de recordar (DNI, nombres) y esto puede ser conocida por quien intente violar la seguridad con actos repetidos debiendo limitar la cantidad de fallos de aciertos para el ingreso de la contraseña. La contraseña no debe ser muy corta para no facilitar la probabilidad de aciertos; pero tampoco muy larga para que se pueda recordar.

14.7 AUDITORIAS Y CONTROL DE ACCESO:
Auditoria. Suele realizarse e posteriori en sistemas manuales, se examinan las recientes transacciones de una organización para determinar si hubo hechos ilícitos.
La auditoria de un sistema informático implica un procesamiento inmediato: se verifican las transacciones que se acaban de hacer.
Un registro de auditoria es un registro permanente de acontecimientos importante que tiene un sistema. Se realiza automáticamente cuando ocurre un evento; se almacena en un área protegida del sistema. en un mecanismo importante de detección, debe ser revisado cuidadosamente y con frecuencia.
Controles de acceso. El control de accso a los datos almacenados es fundamental para la seguridad interna.
Los derechos de acceso son los tipos de acceso que tiene varios sujetos u objetos. Los sujetos acceden a los objetos. Los objetos son entidades que contienen información (discos, cintas, procesadores, almacenamiento, etc).
El objeto esta protegido contra los sujetos, las autorizaciones a un sistema se conceden a los sujetos. Los sujetos pueden ser varios tipos de entidades como usuarios, procesos, etc.
Los derechos de acceso mas comunes son acceso a lecturas, acceso a escrituras o acceso a ejecuciones. Una forma de implementar es mediante una MATRIZ de control de acceso que es protegida por el S.O. con filas para los sujetos, columnas para el objeto y celdas de las matriz para los derechos de acceso que un usuario tiene a un objeto.

14.8 NUCLEOS DE SEGURIDAD Y SEGURIDAD POR HARDWARE:
Núcleos de seguridad. es mas fácil hacer un sistema seguro si la seguridad se incorpora desde el principio al diseño del sistema. Las medidas de seguridad deben ser implementadas en todo el sistema. Un sistema de alta seguridad requiere que el núcleo del S.O. sea seguro. Las medidas de seguridad, mas decisivas están en el núcleo y se lo mantiene lo mas pequeña posible. La seguridad de un sistema depende de asegurar las funciones que realiza:

- El control de acceso.
- La entrada al sistema.
- La verificación.
- La administración del almacenamiento real, del almacenamiento virtual y del sistema de archivos.

Seguridad por hardware. Existe una tendencia a incorporar al hardware funciones del s. O. porque resultan mas seguras que cuando se acceden como instrucción de software que pueden ser modificadas y también porque pueden operar mas rápido que en el software. Mejora la performance, permite controlarlos con más frecuencia.

14.9 SISTEMAS SUPERVIVIENTES: El diseño de sistemas de alta seguridad debe asegurar: Su operación de manera continua y confiable y también su disponibilidad.
Un *sistema de computación superviviente* es aquel que continúa operando aun después de que uno o más de sus componentes falle. Generalmente continúan operando con una degradación suave en los niveles de prestaciones. Los componentes fallidos se deben poder reemplazar sin interrumpir el funcionamiento del sistema.
Una clave para la capacidad de supervivencia es la REBUNDANCIA, si un componente falla otro equivalente toma su puesto. Esto se puede implementar como un conjunto de recursos idénticos que funcionen en paralelo o un conjunto de accesos separados redundantes que se activan cuando se produce un fallo.
Características de supervivencia:

- La incorporación de mecanismos contra fallos en el hardware en vez de en el software.
- El uso de *multiprocesamiento transparente* para permitir mejorar el rendimiento sin modificar el software.
- El uso de subsistemas múltiples de e/s.
- La incorporación de mecanismos de detección de fallos en el hardware y en el software.

14.10 CAPACIDADES Y SISTEMAS ORIENTADOS HACIA EL OBJETO: Un *derecho de acceso* permite a un *sujeto* acceder a un *objeto* de una manera preestablecida.
Los sujetos son los usuarios de los sistemas de computación o entidades que actúan por los usuarios o por el sistema como trabajo, procesos y procedimientos, etc. Los objetos son los recursos del sistema: Ej.: archivos, programas, directorios, terminales, pistas de discos, bloques de almacenamiento primario, etc. Pero los sujetos son objetos del sistema y acceden a otros sujetos. Los sujetos son entidades activas y los objetos son pasivos.
Una *capacidad* es una señal. La posesión de una capacidad por un sujeto le confiere derechos de acceso a un objeto. Las capacidades no suelen ser modificadas pero suelen ser reproducidas.
Un *dominio de protección* define los derechos de acceso que un sujeto tiene a los distintos objetos del sistema: Es el conjunto de capacidades que pertenecen al sujeto.
La creación de capacidades es una función de rutinas de los S.O. cuidadosamente guardadas. Se crea el objeto y luego una capacidad para ese objeto.

14.11 CRIPTOGRAFIA: el uso creciente de redes de computadoras y la importancia del tráfico cursado hace necesario proteger los datos. Se cifran los datos para la transmisión de información detectadas.
La criptografía es el uso de las transformaciones de datos para que sean incomprensibles a todos (excepto el usuario destinado).
Problemas:
- De Intimidad: como evitar la obtención no autorizada de información de un canal de comunicaciones.
- De la autentificación: evitar que modifiquen una transmisión.
- De la disputas: como proporcionar al receptor, de un mensaje, pruebas legales de la identidad del emisor.

Un sistema de intimidad criptográfica. El *remitente* transmite un mensaje que pasa por una unidad de codificación que lo transforma de texto simple o cifrado, o incomprensible para el espía y se transmite por un canal inseguro pero de forma segura.
El receptor legítimo pasa el texto cifrado por una unidad de descifrado para regenerar el texto simple.
Criptoanálisis. Es el proceso de intentar regenerar el texto simple a partir del texto cifrado, pero sin conocer la clave de ciframiento. Esta tarea lo hace el espía o CRIPTOANALISTA, si no lo logra el sistema es seguro.
Sistemas de clave publica. Las distribuciones de claves de un sistema criptográfico se debe hacer por canales muy seguros:
Los sistemas de clave pública ayudan ala distribución de claves porque se separan las funciones de cifrados y descifrados utilizando distintas claves. Una parte se hace pública (ciframiento) y la otra privada (desciframiento).
Firmas digitales. Para que una firma digital sea aceptado como sustituos de una forma escrita debe ser fácil de autentifica (reconocer) por cualquiera, pero producible solo por el autor.
En los criptosistemas de clave pública el procedimiento es:
  - El remitente usa la clave privada para crear un mensaje firmado.
  - El receptor: Usa la clave publica del remitente para descifrar el mensaje y queda el mensaje firmado para usarlo en caso de disputas.

Aplicaciones. La criptografía es útil en los sistemas multiusuario y en las redes de computadoras. Se la utiliza para proteger contraseñas, almacenándolas cifradas, o para proteger datos almacenados en sistemas de computación.
En el *cifrado de enlace* la red cifra y descifra en cada nodo.
En el *cifrado punto a punto* un mensaje se cifra en sus fuentes y se descifra solo una vez, en su destino. La dirección de destino no puede cifrarse.

14.12 PENETRACION AL SISTEMA OPERATIVO: La penetración cambia el estado de las máquinas, del estado problema al sistema supervisor.
Los estudios de penetración están diseñados para determinar si las defensas de un sistema contra ataques de usuarios no privilegiados son adecuadas.
El control de E/s es un área favorita para intentar penetrar a un sistema. los canales de E/S tienen acceso al almacenamiento primario y pueden modificar información importante.

Principales fallos genéricos funcionales de los sistemas.
- *Autentificación:* Los usuarios no pueden determinar si el hardware y el software con que funcionan son los que deben ser.
- *Cifrado:* No se almacena cifrada la lista maestra de contraseñas.
- *Implementación:* que no proviene de un buen diseño de seguridad
- *Confianza implícita:*

    - Una rutina supone que otra esta funcionando correctamente cuando, de hecho, deberia examinar los parametros suministrados por la otra rutina.
- *Compartimiento implicito:*
    - El s. O. Deposita inadvertidamente informacion importante del sistema en un espacio de direcciones del usuario.
- *Comunicacion entre procesos:*
    - Usos inadecuados de los mecanismos de send / receive que pueden ser aprovechados por los intrusos.
- *Verificacion de la legalidad:*
    - Validacion insuficiente de los parametros del usuario.
- *Desconexion de linea:*
    - Ante una desconexion de linea el s. O. Deberia:
        - Dar de baja al usuario (o los usuarios) de la linea.
        - Colocarlos en un estado tal que requiera la re - autorizacion para obtener nuevamente el control.
- *Descuido del operador:*
    - Un intruso podria engañar a un operador y hacer que le habilite determinados recursos.
- *Paso de parametros por referencia en funcion de su valor:*
    - Es mas seguro pasar los parametros directamente en registros que tener los registros apuntando a las areas que contienen los parametros.
    - El paso por referencia puede permitir que los parametros, estando aun en el area del usuario, puedan ser modificados antes de ser usados por el sistema.
- *Contraseñas:*
    - No deben ser facilmente deducibles u obtenibles mediante ensayos repetidos.
- *Entrampamiento al intruso:*
    - Los s. O. Deben tener mecanismos de entrampamiento para atraer al intruso inexperto.
- *Privilegio:*
    - Cuando hay demasiados programas con demasiados privilegios se viola el *principio del menor privilegio*.
- *Confinamiento del programa:*
    - Un programa “prestado” de otro usuario puede actuar como un “caballo de troya”:
- *Prohibiciones:*
    - Se advierte a los usuarios que no utilicen ciertas opciones porque los resultados podrian ser “indeterminados”, pero no se bloquea su uso.
        - Puede robar o alterar datos.
- *Residuos:*
    - Un intruso podria encontrar una lista de contraseñas con solo buscar en lugares tales como una “papelera”:
        - Del sistema o fisica.
        - La informacion delicada debe ser sobrescrita o destruida antes de liberar o descartar el medio que ocupa.
- *Blindaje:*
    - Los intrusos pueden conectarse a una linea de transmision sin hacer contacto fisico:
        - Utilizan el campo inducido por la circulacion de corriente en un cable.
        - Se previene con un adecuado blindaje electrico.
- *Valores de umbral:*
    - Si no se dispone de valores umbral, no habra:
        - Limites al n° de intentos fallidos de ingreso.
        - Bloqueos a nuevos intentos.
        - Comunicaciones al supervisor o administrador del sistema.

Ataques genericos a sistemas operativos.

- *Asincronismo:*
    - Se tienen procesos multiples que progresan asincronicamente.
    - Un proceso podria modificar los parametros ya validados por otro proceso pero aun no utilizados.

    - Un proceso podria pasar valores malos a otro aun cuando el segundo realice una verificacion extensa.
- *Rastreo:*
    - Un usuario revisa el sistema intentando localizar informacion privilegiada.
- *Entre lineas:*
    - Se utiliza una linea de comunicaciones mantenida por un usuario habilitado que esta inactivo.
- *Codigo clandestino:*
    - Se modifica el s. O. Bajo una presunta depuracion pero se incorpora codigo que permite ingresos no autorizados.
- *Prohibicion de acceso:*
    - Un usuario escribe un programa que bloquea el acceso o servicio a los usuarios legitimos mediante:
        - Caidas del sistema, ciclos infinitos, monopolio de recursos, etc.
- *Procesos sincronizados interactivos:*
    - Se utilizan las primitivas de sincronizacion del sistema para compartir y pasarse informacion entre si.
- *Desconexion de linea:*
    - El intruso intenta acceder al trabajo de un usuario desconectado:
        - Luego de una desconexion de linea.
        - Antes de que el sistema reconozca la desconexion.
- *Disfraz:*
    - El intruso asume la identidad de un usuario legitimo luego de haber obtenido la identificacion apropiada por medios clandestinos.
- *Ataque "nak":*
    - Si el s. O. Permite a un usuario:
        - Interrumpir un proceso en ejecucion mediante una "tecla" de "reconocimiento negativo".
        - Realizar otra operacion.
        - Reanudar el proceso interrumpido.
    - Un intruso podria "encontrar" al sistema en un estado no protegido y hacerse con el control.
- *Engaño al operador:*
    - Con un engaño se hace realizar al operador una accion que comprometa la seguridad del sistema.
- *Parasito:*
    - Mediante equipamiento especial el intruso:
        - Intercepta los mensajes entre un usuario habilitado y el procesador.
        - Los modifica o reemplaza totalmente.
- *Caballo de troya:*
    - El intruso coloca un codigo dentro del sistema que luego le permita accesos no autorizados.
    - Puede permanecer en el sistema.
    - Puede borrar todo rastro de si mismo luego de la penetracion.
- *Parametros inesperados:*
    - El intruso suministra valores inesperados a una llamada al nucleo.
    - Intenta aprovechar una debilidad de los mecanismos de verificacion de la legalidad del s. O.