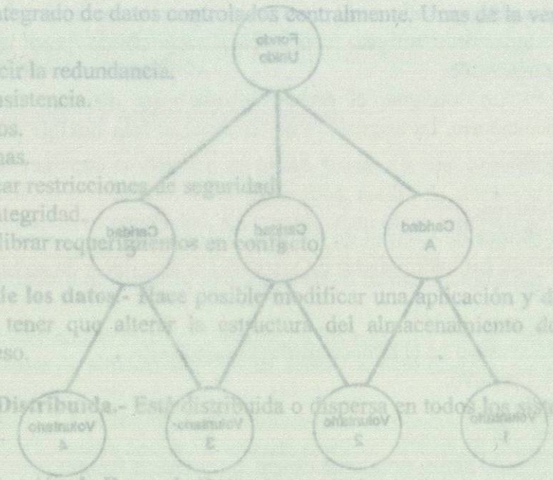

SEGURIDAD EN LOS SISTEMAS OPERATIVOS

La seguridad y el compartimiento son objetivos en conflicto.

Seguridad externa.- Se ocupa de proteger el sistema de computo de intrusos y desastres como incendios e inundaciones, etc.

Seguridad de interfaz con el usuario.- Se ocupa de establecer la identidad de un usuario antes de que se le conceda el acceso a un sistema.

Seguridad interna.- Se ocupa de garantizar el funcionamiento confiable y sin corrupción del sistema de computo y la integridad de los programas y datos.

Autorización.- Determina qué acceso se permite a qué entidades.

División de responsabilidades.- Asigna al personal subconjuntos distintos de deberes; ningún empleado se encarga de una porción grande de la operación de un sistema, por lo que un ataque a la seguridad tendría que implicar a varios empleados.

Vigilancia.- Se ocupa de supervisar el sistema y realizar auditorías así como de verificar la autenticidad de los usuarios.

Supervisión de amenazas.- El sistema operativo controla operaciones delicadas en lugar de ceder el control directamente a los usuarios. Los *programas de vigilancia* ejecutan las operaciones delicadas. Se habla de *amplificación* cuando éstos programas requieren un acceso más amplio para atender las solicitudes de los usuarios.

Protección por contraseña

Hay tres clases de elementos de la verificación de autenticidad con los cuales puede establecerse la identidad de una persona:

1. Algo característico de la persona (huellas digitales, patrones de voz, fotografías y firmas)
2. Algo que la persona posee (credenciales, tarjetas de identificación y claves).
3. Algo que sabe la persona (contraseñas, combinaciones de candados, el apellido de su maestra de tercer año de primaria).

El ciframiento de la lista maestra de contraseñas ayuda a mantener la seguridad de estas aun cuando haya penetración al sistema. Se recomienda cambiar con frecuencia las contraseñas.

Auditoría.- Se realiza por lo general en sistemas manuales *a posteriori.* Se convocan auditores periódicamente para examinar las transacciones recientes de una organización y determinar si se han realizado actividades fraudulentas. En los sistemas de computo puede implicar un procesamiento inmediato en el computador para revisar las transacciones que se acaban de realizar.

Bitácora de auditoría.- Es un registro permanente de eventos importantes que ocurren en el sistema de computo. Se produce automáticamente cada vez que sucede un evento así y se almacena en un área protegida del sistema; si el sistema se ve comprometido, la bitácora deberá permanecer intacta. Es un mecanismo de detección importante. Aunque logren penetrar las defensas de un sistema, las personas puden refrenar sus deseos de hacerlo si temen una detección posterior.

Controles de Acceso.- La clave para la seguridad interna es controlar el acceso a los datos almacenados. Los *derechos de acceso* definen qué acceso tienen varios sujetos a diversos objetos. Los objetos se protegen contra los sujetos.
Los accesos más comunes son el de lectura, escritura y ejecución.

Núcleos de seguridad.- Las medidas de seguridad más vitales se ponen en práctica en el núcleo, el cual se mantiene a propósito lo más pequeño posible. Esto hace más razonable la revisión cuidadosa del núcleo para detectar fallas y demostrar formalmente que este correcto.
La seguridad de un sistema operativo depende sobre todo de asegurar las funciones que se encargan del control de acceso, las entradas al sistema y la supervisión, y que administran el almacenamiento real, el almacenamiento virtual y el sistema de archivos.

Sistemas Tolerantes a Fallas.- Un sistema de cómputo tolerante a fallas continua funcionando aún después de haber fallado uno o más de sus componentes. La tolerancia a fallas se facilita mediante la incorporación de mecanismos a prueba de fallas, el empleo de multiprocesamiento transparente, el uso de múltiples subsistemas de E/S, la incorporación en hardware de gran parte del sistema operativo y la incorporación en hardware de mecanismos para la detección de fallas.

Capacidades y Sistemas Orientados a Objetos

Un derecho de acceso permite a algún sujeto obtener acceso a un objeto de una manera predeterminada. Los sujetos son usuarios de sistemas de computo o entidades que actúan a nombre de los usuarios o del sistema. Los objetos son recursos dentro del sistema. Los sujetos pueden ser cosas como tareas, procesos y procedimientos. Los objetos pueden ser archivos, programas, semáforos, directorios, terminales, canales, controladores, dispositivos, pistas de disco, bloques de almacenamiento primario, etc. Los sujetos también se consideran como objetos del sistema, de modo que un sujeto puede tener acceso a otro. Los sujetos son entidades activas; los objetos son pasivos.

Un *dominio de protección* define los derechos de acceso que tiene un sujeto a los diversos objetos del sistema. Es el conjunto de capacidades pertenecientes a un sujeto. Es importante que los dominios de protección sean pequeños para hacer cumplir el principio de menor privilegio.
Para que un objeto obtenga acceso a un objeto específico debe poseer una capacidad para ello.El problema del objeto perdido se refiere a lo que sucede cuando se elimina la capacidad para tener acceso a un objeto. La renovación de capacidades puede ser difícil, una capacidad podría haber sido copiadas muchas veces. Las capacidades por lo regular no se modifican, pero pueden reproducirse.

Criptografía

Criptografía.- Es el empleo de transformaciones de los datos a fin de hacerlos incomprensibles para todos con excepción de sus usuarios autorizados.

Problema de intimidad.- Se ocupa de evitar la extracción no autorizada de información de un canal de comunicación.

Problema de verificación de autenticidad.- Se ocupa de evitar que algún enemigo modifique una transmisión o inserte datos falsos en una transmisión.

Problemas de disputa.- Se ocupa de ofrecer al receptor de un mensaje una prueba legal de la identidad del remitente o sea el equivalente electrónico de una firma escrita. Como funciona: un remitente cifra texto simple para crear texto cifrado el cual se transmite a un receptor a través de un canal no seguro incluso vigilado por un espía. El receptor descifra el texto cifrado para reconstruir el texto simple original.

Criptoanálisis.- Es el proceso de intentar regenerar un texto simple a partir del texto cifrado pero sin conocer la clave de desciframiento.

Clave pública.- En los sistemas de clave pública las funciones de ciframeinto y desciframiento están separadas, cada una requiere una clave distinta, la clave se hace pública si la otra permanece en secreto. Cuando se cifra un mensaje con clave pública de un usuario sólo ese usuario puede descifrar el mensaje. Con los sistemas de clave pública es posible llevar a la práctica firmas digitales que garanticen la autenticidad de un mensaje.

Los esquemas DES y RSA

Dos de los esquemas criptográficos más importantes son la norma de ciframeinto de datos (DES) y el esquema Rivest, Shamir y Adleman (RSA).

DES es un esquema simétrico de ciframeinto en el cual se usa una sola clave para cifrar y descifrar y RSA es un esquema asimétrico en el cual se utilizan claves distintas para estos propósitos.

El uso más común en llos sistemas operativos actuales es para proteger la lista maestra de contraseñas de un sistema. El ciframiento también es usado para proteger datos almacenados en archivos y para proteger datos que se transmiten a través de una red. Las cintas y discos de respaldo cifrado no necesitan cuidarse con tanto celo como los no cifrados. El ciframiento de enlaces se ocupa de el ciframiento/desciframiento en cada nodo de una red de computadores.
Ejemplo: Si se usa ciframiento de extremo a extremo los mensajes se cifran sólo en su punto de origen y se descifran sólo en su punto destino.

Mediante un procedimiento de reto y respuesta, un sistema puede verificar la autenticidad de un usuario cuando trate de entrar, sin necesidad de transmitir una clave.

Penetración en el Sistema Operativo
Las defensas de un sistema operativo deben ser capaces de resistir un intento de penetración por parte de un usuario no privilegiado; hacer que un sistema operativo sea impenetrable es una tarea imposible, lo que podemos esperar es que sea altamente resistente a la penetración.

Defectos Funcionales Genéricos de los Sistemas
Se han encontrado varios defectos comunes a muchos sitemas de computo. Entre ellos están:

Verificación de autenticidad.- En muchos sistemas, los usuarios no pueden determinar si el equipo y los programas son lo que deberían de ser. Esto hace que un penetrador pueda reemplazar con facilidad un programa sin que se entere el usuario. Ejemplo.- Un usuario podría dar su contraseña a un programa falso de entrada al sistema.

El ciframiento.- La lista maestra de contraseñas debe almacenarse en forma cifrada. A veces no se hace.

Realización.- Un diseño bien pensado para un mecanismo de seguridad puede llevarse a la práctica en forma inadecuada.

Confianza implícita.- Una rutina supone que otra está funcionando correctamente, en vez de examinar con cuidado los parámetros suministrados por la otra.

Compartimiento implícito.- El sistema puede depositar sin darse cuenta información vital del sistema en el espacio de direcciones de un usuario.

Comunicación entre procesos.- El penetrador puede usar un mecanismo de transmisión/recepción para probar diversas posibilidades. Ejemplo.- El penetrador puede solicitar un recurso del sistema y suministrar una contraseña; la información de vuelta puede indicar "contraseña correcta", comfirmando la contraseña adivinada por el penetrador.

Comprobación de legalidad.- El sistema quizá no verifique lo suficiente la validez de los parámetros del usuario.

Desconexión de línea.- En sistemas de tiempo compartido y redes, cuando se pierde la línea el sistema operativo deberá clausurar de inmediato la sesión del usuario o poner a éste en un estado tal que sea necesaria una nueva autorización para otorgarle el control. Un penetrador podría obtener control del proceso y utilizar los recursos a los cuales puede tener acceso este último.

Descuido del operador.- Un penetrador puede engañar a un operador para que monte un disco de sistema operativo falso.

Paso de parámetros por referéncia en vez de por valor.- Es más pasar parámetros directamente en registros y no hacer que los registros apunten a localidades donde estan los parámetros. El paso por referencia puede conducir a una situación en la cual los parámetros siguen en el espacio de direcciones del usuario después de haberse realizado la verificación de legalidad; así, el usuario podría sumisnistrar parámetros legítimos, hacer que sean verificados y después modificarlos justo antes de que los utilice el sistema.

Contraseñas.- A menudo las contraseñas son fáciles de adivinar o de obtener por intentos repetidos.

Trampas para el penetrador.- Los sistemas deben incluir mecanismos de trampa para atraer al intruso inexperto, pues constituyen una buena primera línea de detección. La mayor parte de los sistemas tienen mecanismos de trampa inadecuados.

Privilegios.- En algunos sistemas, son demasiados los programas que tienen demasiados privilegios. Esto va contra el principio del menor privilegio.

Confinamiento de programas.- Un programa prestado por otro usuario puede actuar como Caballo de Troya; podría robar o alterar los archivos de quien lo pidió prestado.

Prohibición.- Muchas veces se indica a los usuarios que se abstengan de usar ciertas funciones porque los resultados pueden ser "indeterminados". No obstante, estas funciones siguen siendo accesibles para los usuarios.

Residuo.- El penetrador puede encontrar una lista de contraseñas examinando el cesto de la basura. En ocasiones se deja residuo en el almacenamiento después de ejecutarse una rutina del sistema. Toda información confidencial deberáreemplazarse o destruise antes de liberar o desechar el medio que ocupa.

Blindaje.- Una corriente en un alambre genera un campo magnético alrededor de este; los penetradores pueden intervenir de hecho una línea de transmisión o un sistema de computo sin hacer contacto físico. El blindaje eléctrico puede servir para evitar estas "intrusiones invisibles".

Valores de Umbral.- El propósito de estos es refrenar intentos repetidos de entrar en el sistema. Ejemplo: Después de un cierto número de intentos de entrada no válidos, ese usuario deberá bloquearse, notificando al administrador del sistema. Muchos sistemas no cuentan con esta característica.

Ataques Genéricos a los Sistemas Operativos.- Metodologías de penetración:

Asincronía.- Cuando varios procesos avanzan en forma asíncrona, es posible que un proceso modifique parámetros cuya validez ha sido verificada por otro, aunque este último todavía no los haya usado; así un proceso que tiene valores malos a otro aunque el segundo realice una verificación exhaustiva.

Hojeo.- Un usuario revisa el sistema de computo intentando localizar información privilegiada.

Entre Líneas.- Se usa una terminal especial para intervenir una línea de comunicaciones empleada por un usuario inactivo que haya entrado en el sistema.

Código clandestino.- Se instala un parche con la pretensión de corregir un error en el sistema operativo; el código contiene escotillones, a través de los cuales se puede entrar después en el sistema sin autorización.

Rechazo de acceso.- Un usuario escribe un programa para hacer que se caiga el sistema, para ponerlo en un ciclo infinito o para monopolizar sus recursos. La intención en este caso es impedir que usuarios legítimos obtengan acceso o servicio.

Interacción de procesos sincronizados.- Los procesos usan las primitivas de sincronización del sistema para compartir o pasara información entre ellos.

Desconexión de línea.- El penetrador intenta obtener acceso al trabajo de un usuario después de una desconexión de línea, pero antes de que el sistema reconozca la desconexión.

Disfraz.- El penetrador asume la identidad de un usuario legítimo después de haber obtenido la identificación correcta por medios clandestinos.

Ataque NAK.- Muchos sistemas permiten a un usuario interrumpir un proceso en ejecución(utilizando la tecla "negative acknowledge"), realizar otra operación y después continuar el proceso interrumpido. El penetrador puede "atrapar" al sistema en un estado no protegido y adueñarse del control con facilidad.

Engaño del operador.- Un penetrador astuto a menudo puede engañar al operador del computador para que realice una acción que ponga en peligro la seguridad del sistema.

Parásito.- El penetrador utiliza una terminal especial para intervenir una línea de comunicación. El penetrador intercepta mensajes entre el usuario y el procesador y los modifica o bien los reemplaza por completo.

Caballo de Troya.- El penetrador coloca código en el sistema que le permitirá un acceso posterior no autorizado. El Caballo de Troya puede dejarse en el sistema permanentemente o puede borrar todos los indicios de su existencia después de una penetración.

Parámetros inesperados.- El penetrador suministra valores inesperados en una llamada al supervisor para aprovechar un punto débil en los mecanismos de verificación de legalidad del sistema.

La confidencialidad de un computador no existe.
Aquí la idea es: Si no quieres que lean algo
no lo metas en el sistema.