Nombre del Trabajo: Análisis de la Seguridad en Redes Locales

Autores:

Prog. Nelson Rubén Rodríguez
Lic. Gustavo Alberto Quiroga
Lic. Héctor Alfredo Sanchez

Las personas nombradas son docentes e investigadores del Departamento e Instituto de Informática (Gabinete de Sistemas Operativos y Redes) de la Facultad de Ciencias Exactas, Físicas y Naturales de la Universidad Nacional de San Juan, cita en Cereceto y Meglioli - Rivadavia
(cp 5400) San Juan. Tel: 064- 231945 Fax: 064-234980

E-mail:NRODRIGUE@IINFO.UNSJ.EDU.AR
E-mail:GQUIROGA@IINFO.UNSJ.EDU.AR
E-mail:HSANCHEZ@IINFO.UNSJ.EDU.AR

Palabra Clave: Redes-Seguridad-Protección

Resumen:

Obviamente los términos seguridad y protección tienen que ver con el control de acceso de usuarios y procesos (sujetos) a recursos (objetos).

Los métodos de seguridad se basan en métodos de control de acceso y encriptado de datos.

La filosofía de trabajo varía según sean redes Peer-to-peer o Client-Server, no obstante cada producto implementa sus soluciones de forma diferente, lo que determina por ende distintas alternativas de seguridad.

A tal fin analizamos el modo de trabajo varios NOS, y al final presentamos dos tablas comparativas.

En sistemas operativos monousuarios no se puso énfasis en la protección, dado que se suponía que la computadora es personal y la maneja una sola persona. No obstante existe protección por la ROM BIOS, utilitarios como Disklock de Fifth Generation Systems Inc. y el sistema operativo DR 6.0 de Digital Research que permiten bloquear discos, archivos o directorios.

En algunos casos, el hecho de que el usuario esté presente, permite que utilice una señal digital para confirmar el acceso, como tarjeta con banda magnética o características personales como firma dinámica, combinada con una clave secreta. Lamentablemente esto no es posible de implementar en la mayoría de los casos.

Análisis de la Seguridad en Redes Locales

Primeramente vamos a definir un serie de conceptos

Protección:

- Se define como las reglas para restringir el acceso al uso de todo o parte de un sistema de computadora.
- Sinónimo de lockout.

Seguridad:

- Los conceptos, técnicas, medidas técnicas y administrativas usadas para proteger el hardware, software y datos de sistemas de computadoras desde error o daños deliberados a accidentales. Es el problema en general para proteger la información contra su uso no autorizado.

La Protección puede ser aplicada a datos, programas, el uso de la computadora, el uso del espacio de almacenamiento o periféricos; puede ser descripta como control de acceso a todas estos elementos. Se define mecanismo de protección como los mecanismos específicos del sistema Operativo que utiliza para salvaguardar información en la computadora.Los métodos de seguridad se basan en métodos de control de acceso y encriptado de datos.

Criptografía

La Criptografía computacional es el arte o ciencia de escribir en código un mensaje originalmente escrito con claridad, dejándolo incomprensible.

La criptografía da el soporte para proteger recursos controlando el acceso a los mismos. Las herramientas de seguridad de MainFrames no se pueden adaptar fácilmente a todas las redes, dado que en las mismas el control global es inexistente.

En equipos con subsistemas de interconexión abiertos, como redes WAN (Wasted Area Network) y conexiones telefónicas, radiales o satélite es imposible impedir el acceso de un extraño. Además las redes pueden están interconectadas con otras.

Ejemplos de aplicaciones son: transferencia electrónica de fondos, identificación de cajas automáticas, protección de información confidencial como datos policiales, médicos, militares o diplomáticos.

Los usuarios pueden requerir protección contra intentos maliciosos de otro usuario, ataque de virus y también fallas de soft y hard que pueden causar un efecto similar.

El modelo OSI (Open System Interconnection) de la International Standard Organization, describe una arquitectura de red basada en capas. La capa de presentación define varios servicios entre los que se encuentra la criptografía.

Un caso particular de uso en redes, es la protección del correo electrónico, dado que su naturaleza lo hace muy vulnerable al tener archivos con formato estructurado conocido y contenido básicamente textual.

Por otro lado, la criptografía computacional da soporte para la obtención de métodos de check-sum convenientes para determinar el ataque de virus.

Se usa para garantizar:

- Secreto de la información: solo los usuarios autorizados (personas o procesos) tengan acceso a la información o consigan tenerla legible.
- Integridad de información: garantía ofrecida al usuario de que una información es correcta, original, no fue alterada, ni intencionalmente ni accidentalmente.
- Control de Acceso discrecional: regula quien tiene acceso a aplicaciones, archivos y servers. Se puede utilizar niveles de autorización para proteger aplicaciones, directorios y archivos contra uso y modificaciones no autorizadas.
- Autenticidad de remitentes: proceso que permite a un usuario certificar que un mensaje recibido fue en efecto enviado por el remitente, pudiendo probar, que un remitente envió dicho mensaje.
- Autenticidad de destinatario: consiste en tener una prueba de que el mensaje enviado fue como tal recibido por el destinatario.
- Autenticidad de actualización: consiste en probar que un mensaje es actual y no se trata de mensajes antiguos reenviados.

Para algunas organizaciones la seguridad no es más que un simple mecanismo de password, pero estos ofrecen una pequeña protección para acceso no autorizado. Hay que tener en cuenta que las redes involucran muchos componentes y se podrían dar las siguientes situaciones:

- Un usuario podría introducir un virus al usar cualquier disketera o sacar ilícitamente información de la red.
- Un usuario podría utilizar comandos destructivos como FORMAT
- Un usuario podría utilizar impresoras o puertas de comunicaciones sin derecho de acceso.

La filosofía de trabajo varía según si los NOS (Sistema Operativos de Red), son Peer-to-Peer o Client/Server, no obstante cada producto implementa sus soluciones de forma diferente los que determina por ende distintos niveles de seguridad.

Las Redes Peer-to-Peer no brindan un esquema de seguridad apropiado. El hecho de estar soportadas sobre DOS, que es un Sistema Operativo monousuario, monotarea y sin funciones de seguridad, deja abierta la posiblidad de que las máquinas sean inicializadas stand-alone, sumado al hecho de que cualquier estación puede ser server en cualquier momento.

Las Client/Server brindan esquemas más sofisticados.

Para los recursos a ser controlados por el Sistema Operativo de Red, el control de acceso es el mecanismo elegido, a través del uso de passwords.

En los casos donde el control de acceso no es posible, como workstation remotas donde la información viaja por canales inseguros, o el almacenamiento de claves que pudieran ser accedidas por el administrador, queda como único recurso el encriptado de datos.

Requerimiento de Administración en Redes

Administración de seguridad es concerniente con la generación, distribución y almacenamiento de claves encriptadas. Passwords y otras autorizaciones o información de control de acceso debe ser mantenida y distribuida. La administración de seguridad está relacionada también con el monitoreo y el control de acceso a redes de computadoras y accesos a toda o parte de la información de administración de red obtenidas desde nodos de la misma.

Los login son una herramienta de seguridad importante y además la administración de red involucra más que la colección, almacenamiento y examinación de registros de auditoría y logs de seguridad, así también como la habilitación y deshabilitación de estas facilidades de login. La seguridad es crítica para aplicaciones de transacciones y procesamiento. Un sistema de seguridad debe proveer más que un simple permiso o negativa de acceso a un archivo.

Los mecanismos de protección de redes se utilizan para:

- Impedir acceso de intrusos
- Impedir acceso a recursos
- Proveer normas de seguridad

Los aspectos que podemos nombrar como claves en un análisis serían:

- Protección de unos usuarios con otros
- Protección de tareas con otras (Esto lo debe garantizar cualquier sistema multitarea, fundamentalmente protección en el uso de recursos como memoria).
- Tolerancia a Fallos (pueden ser Hard y Soft)
- Cortes del Fluido Eléctrico (UPS)
- Fallas en el disco
- Hot Fix
- Espejado de Disco
- Duplicación de Disco
- Fallas en el Server
- Fallas en las Transacciones
- Buena administración de recursos y de los usuarios (Derechos sobre archivos, directorios y usuario).
- Monitoreo de Red
- Autenticación de Usuarios
- Protección de búsqueda y destrucción de virus
- Aplicaciones de seguridad provisto por otra compañias

La seguridad refleja los servicios de supervisión del NOS y la habilidad de un administrador en usarlos para crear nombres de usuario y un Bindery (base de Datos) de información de seguridad. Los servicios de supervisión deben permitir al administrador ver la contraseña de cada usuario, escribir por encima de contraseñas encriptadas y forzar a los usuarios a cambiar periódicamente de contraseña o en conexiones subsiguientes.

Además, los supervisores de red deben poder crear nombres de usuarios, contraseñas de usuarios y recursos publicados para Pcs locales. Los administradores también deben poder almacenar los recursos publicados de cada usuario en un guión de conexión y generar una lista de recursos bajo uso, una lista de usuarios y un registro de errores.

Protección de unos usuarios con otros

Para mantener varios usuarios en Red, accediendo a distintos recursos y con distintas alternativas de acceso, se definen niveles de Usuarios.

En un sistema de cierta dimensión, resulta muy conveniente separar las funciones de administración del Sistema de las de seguridad. El primero podría manejar la definición de usuarios, controles de acceso y configuraciones de los programas de aplicación, mientras que el administrador de seguridad se encargaría de la asignación y manejo de las palabras claves, auditoría y otros mecanismos específicos de seguridad.

Un segundo nivel es el contituído por los diferentes grupos que manejan proyectos específicos. Finalmente en un nivel inferior están los usuarios para ingreso de datos (data entry) o incluso usuarios ocacionales (invitados), los cuales deben tener acceso bastante restringido.

Supervisor (SuperUsuario)

Posee un acceso completo a los archivos del sistema y un control pleno sobre el sistema de seguridad. Fija las restricciones sobre las cuentas y puede designar a algunos usuarios como responsables de grupos de trabajo, responsable de cuentas de usuario y operadores. En grandes redes también se ocupa del mantenimiento y monitoreo de la red y es posible que tenga que delegar las labores de creación de los usuarios.

Usuario

Es una persona que posee derechos limitados en el sistema al menos que sea el supervisor.

Los usuarios se restringen y controlan por medio de:

- Restricciones de conexión
- Derechos de acceso a Directorios
- Derechos de acceso a Archivos

Grupos

Los grupos son conjuntos de usuarios que se agrupan para facilitar las actividades de administración. Se corresponde generalmente con un grupo de trabajo y se les da derechos a unos directorios específicos y a los archivos que contienen. Asignar los derechos de acceso a grupos en vez de a usuario simplifica la administración.

Responsable de Grupo y de Cuenta de Usuario

Son usuarios que se definen para relevar al administrador de algunas tareas de gestión. Reciben el control sobre uno o más usuarios o grupos y los directorios. Pueden definir o suprimir usuarios, crear nuevos subdirectorios, cargar programas y realizar otras tareas de administración. El responsable a su vez también puede definir a otros responsables que le ayuden en la tarea de administración, pero estos estaran restringidos al ámbito del responsable.

Protección de unas tareas con otras

Por ser un Sistema Operativo Multitarea debe proveer protección de unas con otras, es quizás la función más dificil de llevar a cabo. El Sistema Operativo es el responsable de brindar todas las funciones necesarias para la protección de los programas de usuarios a la vez que debe cuidar que esas funciones no perjudiquen a otros usuarios o al propio Sistema Operativo. En combinación con el hard, el Sistema Operativo protege la operación del equipo, previniendo la invasión de sectores de memoria no accesibles, la ejecución de instrucciones privilegiadas o el uso de recursos para los que no se cuenta con la debida autorización.

Soporte para UPS

Tiene que ver con la habilidad del Sistema Operativo en administrar una fuente de alimentación ininterrumpible conectada al server.

Con el programa de administración de la UPS, se puede fijar una alarma que lo alerta cuando se interrumpe el fluido eléctrico y fijar un nivel de voltaje donde el server ejecuta un apagado organizado,si el corte de energía se prolonga por un período especificado. Además el

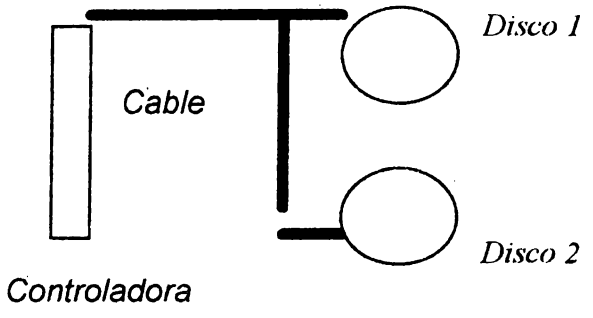
Sistema Operativo debe mostrar mensajes de advertencias en las pantallas del servidor y de las estaciones clientes antes de apagarse.

Hot Fix

El Sistema Operativo realiza una verificación de lectura tras escritura, de tal forma que al escribir un bloque de datos, inmediatamente se lee del disco y se compara con los datos originales. Si coinciden los datos la operación es correcta, si no coinciden es probable que hay problemas con el disco, entonces entra en acción la técnica Hot Fix para evitarlo. El Hot Fix permite que el disco fijo mantenga su integridad reservando una pequeña porción del área de almacenamiento del disco como área de redirección Hot Fix y manda a ese sector los bloques de datos que se intentan escribir.

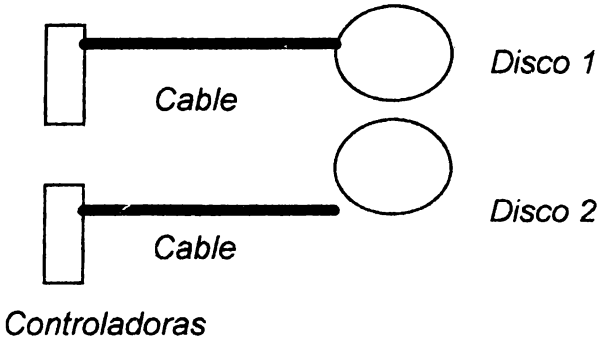
Espejado de Disco

El Sistema Operativo posee una opción de *espejado de disco (Disk Mirroring)* que permite que los datos de un dispositivo primario quedan duplicados en el secundario.Los bloque de datos quedan duplicados en ambos discos funcionando como un tándem al actualizar los archivos. Al fallar uno de los discos el otro sigue funcionando perfectamente.



Duplicación de Canal

La duplicación de canal (Disk Duplexing) es un paso más en la protección ante fallos. Igual que en el caso anterior existen dos discos iguales, pero en este caso no comparten la controladora ni el cable, osea que se duplica el canal completo (controladora, cable y disco). Otra de las ventajas es el *reparto de búsqueda*, ante una petición de lectura el sistema podra leer de los dos discosa la vez.



Fallas en el Server

El Sistema Operativo provee la posibilidad del "Sistema tolerante a fallas" con el cual se permite duplicar el servidor por completo coexistiendo ambos en la red.

Fallas en las Transacciones

El TTS evita la corrupción de las bases de datos en caso de que ocurra un error mientras se esta escribiendo en el disco. Al esta activo el TTS una secuencia de transacciones se ve como un solo evento que debe completarse o anularse. Si el evento no se completo se vuelve al estado anterior perdiendo esa ultima transacción pera manteniendo la base intacta

Monitoreo de Red

Las redes incluyen componentes de diferentes proveedores, cada uno con sus propios controles, parámetros y opciones de configuración, lo que obliga a los usuarios a adquirir y administrar múltiples herramientas de administración. Una heterogeneidad de este tipo puede volverse un obstáculo insalvable en el crecimiento de una instalación.

Los requerimientos de administración necesitan de un monitoreo y control de extremo a extemo de la red.

Los protocolos normalizados tratan de proveer un canal común de comunicación a través del cual componentes y software de diferentes proveedores puedan intercambiar información de una manera consistente.

Una plataforma de Monitoreo de Red debe identificar y reemplazar los equipos que fallan. Estas plataformas son sistemas integrados que pueden tomar datos desde una variedad de aplicaciones de terceras partes y los presenta en una interface consistente, ofreciendo un conjunto de servicios como display de todos los equipos conectados.

La ISO desarrolló una serie de especificaciones denominada CMIP (Protocolo de Información de Administración Común) y CMIS (Sistema de Información de Administración Común). Luego la IETF (Internet Engineering Task Force) basándose en los anteriores genera SNMP (Protocolo de Administración de Red Simple) que no incluye facilidades de seguridad, debido a esto en Carnegie Mellon se desarrolla SNMP2. SNMP fué diseñado para proveer administración en la capa de Red y Transporte, con lo que cubre dispositivos como puentes, routers y concentradores. Cada característica del agente a ser administrado se define como un objeto en la base de datos llamada MIB (Base de Información para la Administración).

Actualmente se está definiendo una extensión a SNMP MIB (Mobile MIB), para actividad no cableada (wireless) por Xircom Inc. y Epilogue Technology Corp., agregando especificaciones como tiempo de batería, administración de potencia, servicios de socket y card, etc.

Entre las plataformas de monitoreo tenemos: SunNet Manager (SunSoft), OpenView (Hewlett Packard) e IBM NetView para AIX.

Administración de Archivos y Usuarios
Derechos de Directorios y Archivos en Netware

Dado que el NOS permite que mucha gente acceda al mismo archivo a la vez, la seguridad de archivos es esencial. Las facilidades de seguridad previenen accesos no autorizados a los archivos en el server. Netware provee la seguridad de archivo a través del uso de derechos de archivos y directorios.

Los archivos del NOS son distintos de los de DOS y Macintosh. Los archivos almacenados en el server son guardados en un formato que es nativo de Netware. Cuando un usuario requiere un archivo, el software del server presenta el archivo de dato en un formato compatible con el Sistema Operativo de la workstation sea DOS, OS/2, Mac o UNIX.

Tipo de Derecho

Los NOS proveen la facilidad de otorgar derechos a los directorios y archivos.

Los derechos y restricciones de un usuario sobre un directorio pueden ser los derechos que se le han asignados y los derechos que heredan de su directorio padre. Los derechos asignados se superponen sobre otros, pero los derechos heredados pueden ser bloqueados.

Atributos de Directorios

Normal, No Borrar, No Renombrar, Purgado, Oculto, Sistema y Visible (para suarios Mac).

Atributos de Archivos

Sirven para proteger a los archivos de un directorio y son:

Archivo, Restringe copia, Restringe borrado, Ejecuta solamente, Oculto, Purgado, Auditoria de Lectura, Lectura y Escritura, Deshabilita Renombrado, Compartido, Sistema, Transaccional y Auditoria de Escritura.

Protección de búsqueda y destrucción de virus

Los virus en redes de computadoras son bastantes problemáticos y pueden afectar a archivos COM, EXE y areas de boot. No obstante las facilidades provistas por los NOS, algunos virus como One Half, afectan a archivos EXE que estaban protegidos con derechos RO (Read Only) e inclusive en directorios donde los usuarios no tenían acceso de escritura. Otro problema son los virus stealth.

Entre las consideraciones a tener en cuenta están: usar una estrategia antivirus multiparte, tal como virus scanning NLM en tiempo real, un scanner antivirus basado en workstation y programas que periódicamente observan los cambios a los archivos ejecutables en workstation y servers. Considerar algún procedimiento para chequear cada nueva pieza de software antes de instalarla al sistema, cada paquete es sospechoso: shareware, demos, etc.

Asegurarse que los usuarios tienen solamente los derechos de seguridad necesarios para ejecutar sus programas (aunque muchos virus pueden evadir los mismos). Agregar los cuidados para protección antivirus stand-alone (disco de boot sano, versiones de bases de datos de virus actualizadas, etc.).

Autenticación de Usuarios

Para ingresar al Sistema cada usuario debe introducir su clave de acceso.

Las plataformas que utilizan UNIX con BSD (Berkeley Software Distribution) con TCP/IP, tienen un buen sistema de seguridad en su Sistema Operativo y plataforma. Alternativas UNIX como Telnet y Rlogin no encriptan la transmisión del login. Por lo tanto proceder con login de Netware (esto es combinando ambos sistemas Operativos) es más seguro que muchos ambientes NFS, los cuales transmiten passwords no encriptados.

Algunos NOS como Vines envian solamente las palabras claves en forma encriptada, otros como 3+Open y LanServer usan un sistema de registro en que una palabra clave se envía a través de la red, sino un sistema de desafío y respuesta. El carácter desafío se combina con la palabra clave encriptada y la estación envía el resultado al servidor. Este, en tanto, ha realizado el mismo trabajo y compara los resultados.

Las palabras claves deberían tener no menos de 8 caracteres e incluso ser mezclas de mayúsculas y minúsculas.

Si bien los passwords ofrecen adecuada protección, a menudo son facilmente penetrado por hackers oportunos

En Sistemas de Empresas, el usuario puede necesitar de múltiples passwords. Existen 3 productos comerciales que pueden generar passwords más seguros: SmartPass for Netware (Software Inc) Acces Data (Access Data Corp) y Pretty Good Privacy (PGP) (ViaCryt).

SmartPass opera como NLM identifica passwords de red que pueden ser facilmente adivinados por comparación de passwords de cada usuario (incluyendo el supervisor) contra una base de datos de 150.000 password vulnerables.

Una vez que realiza el análisis genera una lista de passwords débiles encontrados en el server y sugiere palabras claves más seguras para usos futuros. Tiene además otras facilidades. Acces Data tiene un conjunto de utilidades que revisa los passwords usados para bloquear archivos de varios paquetes como Excel, Lotus,Symphony, Paradox, WordPerfect, Quattro Pro, PkZip y otros.

PGP es un algoritmo de cifrado por software, que ofrece alta seguridad, grado militar (configurable) sobre DOS,Windows, UNIX, VAX/VMS y otras plataformas. PGP permite que se intercambie archivos o mensajes con privacía y autenticación y es utilizado ampliamente en la comunidad internet.

Otras consideraciones

Un problema crítico en la seguridad son las interredes, dado que resulta bastante molesto ir avanzado en las mismas por medio de password, lo que significa que un usuario deba recordar varias palabras claves y no procure llevar a cabo normas de seguridad como cambio periódico de las mismas.

La seguridad también se debe mantener al cambiar la versión de un producto. Por Ej. cuando se transfiere información de bindery de un servidor Netware 2.x a 3.x, se pasan al nuevo sistema todos los derechos de usuarios, grupos, directorios y archivos, excepto las contraseñas. Debido a que las mismas residen encriptadas y Novell tiene un esquema de seguridad por lo cual, ni aquellas pueden pasarse como parte del bindery. Por lo tanto el supervisor tendrá que volver a entrar las contraseñas, o el sistema permitirá entrar la misma u otra cuando los usuarios se registren por primera vez en el nuevo sistema.

Aplicaciones de Seguridad Provistos por Otras Compañias

Otras empresas han generado distintas aplicaciones que ofrecen seguridad adicional ya sea para complementar versiones nuevas o mejorar la anteriores.

Password Coach 1.0 (Baseline Software) que corre Netware y provee los siguientes servicios: Control de Indentificación y Password, Protección de archivos de datos (Control de Acceso) y Seguridad en Comunicaciones.

PC/DACS (Mergent International Inc) ofrece control de identificación y password, protección de virus, auditoría, seguridad en comunicaciones y encriptado DES y propietario, para Netware, Vines , Lan Manager y otras.

Path Key Secure Communications , provee DES, es un dispositivo serial en línea que reside entre una computadora y un modem.

MiraLink y Vinca son ambos productos de mirroring remoto diseñados para recuperación, servicio de backup y aplicaciones de administración centralizada. Estas soluciones están disponibles para Netware 3.x o servidor de archivo mayor a servidores remotos usando soluciones desde Novell, aún para el NOS Netware 4.1 SFT III que puede espejar hasta 8 servers, dado que este producto no soporta mirroring remoto.

Clasificación de los Sistemas de Seguridad

En 1983 el DOD propone una serie de medidas para evaluar la seguridad técnica en sistemas de computadoras.

Las 4 clases son:

- D - Protección Mínima
- C - Protección Discrecional
- C1 - Protección de Seguridad Discrecional
- C2 - Protección de Acceso Controlado
- B - Protección de Mandatario
- B1 - Protección de seguridad Cargada
- B2 - Protección Estructurada
- B3 - Dominio de Seguridad
- A - Protección Verificada
- A1 - Diseño verificado

Clase D: Esta clase se reserva para aquellos sistemas que han sido evaluados pero que fallan para satisfacer los requerimientos para una clase de evaluación alta.

Clase C1: El Sist. satisface los requerimientos de seguridad discrecional para proveer separación de usuarios y datos. Incorpora alguna forma de controles creíbles aptos para limitar el acceso en una base individual, es decir, ostensiblemente confiable para permitir a los usuarios estar habilitados para proteger proyectos o información privada y para guardarse de otros usuarios de lectura accidental o destruir sus datos.

Clase C2: El Sist. en esta clase se esfuerza por lograr un acceso de control discrecional más sutil que C1, crenado cuentas de usuarios individualmente para sus acciones a través de procedimientos de login, auditoría de eventos relevantes a seguridad y aislación de recursos.

Clase B1: Tiene todas las facilidades de la clase C2. Además una presentación informal del modelo de política de seguridad, rotulación de datos y control de acceso obligatorio sobre sujetos y objetos. La capacidad debe existir para que la información exportada sea rotulada con exactitud. Cualquier defecto identificado por testeo debe ser removido.

Clase B2: Está basada en un modelo de política de seguridad formal documentada y claramente definida que requiere la discrecionalidad y control de acceso obligatorio encontrado en clase B1 y son extendidos a todos los sujetos y objetos en el sistema. Debe ser cuidadosamente estructurado en elementos de protección crítica y no crítica.

La interface está bien definida y el diseño e implementación habilita a estar sometido a un testing más cuidadoso y una revisión más completa.

Clase B3: Debe satisfacer los requerimientos del monitor de referencia que media todos los accesos de sujetos a objetos. Un administrador de seguridad es soportado, mecanismos de auditoría son expandidos a eventos relevantes a la seguridad, y procedimientos de recuperación de sistema. El Sist. es altamente resistente a la penetración.

Clase A1: Son funcionalmente equivalentes a aquellos de la clase B3 a los cuales se les agrega facilidades de arquitectura adicional o políticas de requerimientos. Las facilidades distinguibles del sist. en esta clase es el análisis derivado de especificaciones de diseño formal y técnicas verificadas y el alto grado de seguridad resultante que está correctamente implementada. Esta confianza está desarrollada en forma natural, comenzando con un modelo de política de seguridad formal y una especificación formal del nivel tope de diseño.

Tablas Comparativas (Peer-to-Peer)

	Lantastic 6.0	Windows for WorkGroups 3.11	Personal Netware 1.0	Power Lan 3.11
Restricciones de log-time	X	X	X	X
Fecha de expiración	X			X
Grupos de usuarios	X		X	X
Password a nivel de archivo	X			

De todas la peer-to-peer Lantastic es la que provee mayor seguridad. Después de crear cada usuario de red, Ud. apunta y hace clik para otorgar permisos y derechos. Puede proteger con password drive de disco, directorios o archivos individuales.

Tablas Comparativas (Client/Server)

	IBM OS/2 4.0	Windows NT 3.5	Netware 4.02
Monitoreo de UPS	X	X	X
Mirroring Disk	X	X	X
Duplexing Disk	X	X	X
Server Duplexing			X
Hot Fix	X	X	X
RAID nivel 5		X	
Seguridad basada en usuario	X	X	X
Fecha de expiración de cuenta	X	X	X
Restricción de Tiempo	X	X	X
Encriptado de Passwords	X	X	X
Seguridad C2		X	X

La versión 3.12 de Netware agrega mejoras a la seguridad por medio del paquete de firma NCP. No obstante no cumple con la especificación de la Clase C2.

La versión 4 extiende los servicios de Netware con:

- Auditoría de Seguridad
- Servicio de Tolerancia a Fallos
- Servicio de directorio Netware

- Provee Clave RSA pública/privada
- Login restricto a una específica dirección Mac

Bibliografía:

Data Encryption Standard - FIPS Publication 46 - NBS, U.S. Department of Commerce-1977.
- Tanembaum A. - Computer Networks - Prentice Hall.
- LeLann G. - Motivations, Objetives and Characterization of distributed Systems - Springer-Verlag.
- K.Zeng-C.Yang-D.Yea-T.Rao - Pseudorandom bit generators in stream cipher cryptography - Computer IEEE - Feb 1991
- Shannon C. - Communication Theory of Secrecy Systems - Bell System Tech. Journal - Vol 28 - 1949
- Rodriguez Prieto - Protección de la Información diseño de criptosistemas informáticos - Paraninfo 1986
- Denning D. - Cryptography - Communication ACM - Mar 1993
- Lucchesi Claudio - Introducao a la Criptografia Computacional -Papirus
- Seberry J. Pieprzyk J. - Cryptography An Introduction to Computer security - Prentice Hall
- Borsook P. - En busca de la seguridad - Byte Arg. - Mayo 93
- Wayner P. - Se debe regular la encriptación ? - Byte - Mayo 93
- Stallings William - Pretty Goood Privacy - Byte - Julio 1994
- Stallings William - Local and Metropolitan Area Networks - 4° Edition - Mac.Millan Inc.
- Appleton Elaine - Seguridad: qué tan vulnerable es su red? - Datamation - Mar 1994
- Earley John - Security Solutions for Networks - Telecomunications Iternational Edition - Feb 1990
- Kent S. - Internet Privacy Enhaced Mail - Commun ACM - Agosto 1993
- Hoffman L. - Who holds the cryptographic keys? The government key escrow iniciative of 1993 - Computer IEEE - Nov 1993
- M. Chris - OSI and X.400 Security - Telecomunications International Edition - May 90
- N. Willet - Deliberate Noise in a Modern Cryptographic System - IEEE Transactions on Information Theory - Enero 1990
- Rodriguez,Klenzi,Rueda,Ortega - Protección y seguridad computacional con algoritmos criptográficos simétricos - 2° Congreso Internacional de Informática - Informática 94. Mendoza Junio 94
- Needham R. - Denial of Service: An Example - Communication ACM - Nov 94
- Simmons G. - Cryptoanalisys and Protocol Failures - Communication ACM - Nov 94.
- Tadesse Giorgis - Networks for the Enterprise - Byte - Feb 95
- Lan Times - Nros varios - Mc Graw Hill
- Lan & Wan and Anything in Between - Nros varios - Ed. Canaima
- Russell Kay - Distributed and Secure - Byte - Jun 94
- Corporate Connections 94 - Novell