49

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

FUNDAMENTOS DE SEGURIDAD DE LA INFORMACION

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACION

P R E S E N T A N:

CINTIA QUEZADA REYES

SERGIO ALBERTO GUTIERREZ RODRIGUEZ

DIRECTORA DE TESIS:

M C. MA. JAQUELINA LOPEZ BARRIENTOS

MEXICO, D. F. DICIEMBRE - 2001

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

"Cualesquiera que hayan sido nuestros logros,
alguien nos ayudó siempre a alcanzarlos."
Althea Gibson

A mis padres Luis Quezada y Náyade Reyes
Por el apoyo incondicional, sus esfuerzos, su amor y la continua motivación, todos estos elementos me han ayudado a cristalizar cada uno de mis sueños. Este éxito es de ustedes.

A mis tíos Sócrates Reyes (+), Elvia Santiago y Ceres Reyes
Por las palabras de aliento y el cariño brindado, sin éstos no habría podido seguir adelante. Mil gracias por creer en mí.

A mi hermana Aída Quezada
Por estar presente en cada uno de los momentos buenos y malos de mi vida, deseo de todo corazón que el presente sirva como incentivo para que también logres todas las metas que te has propuesto.

A mis amigos Ariadna Suárez, Carlos Torres, Juan Carlos Farfán, Hugo Cedillo, Carlos Aroche, Arturo Vidal, Raúl Mota, Moisés León, Daniel Hernández y Pablo Orozco
Porque su compañerismo y ayuda desinteresada en nuestra época estudiantil fue el inicio de lo que actualmente es una valiosa y entrañable amistad

A mis queridos maestros
Por el granito de arena que desinteresadamente aportaron en mi formación profesional Gracias por sus enseñanzas, son un gran tesoro

A mi amigo y compañero Sergio Gutiérrez
Por el apoyo, dedicación, esfuerzo y deseo de superación, no hay nada como el trabajo en equipo y el estímulo para alcanzar las metas y lograr el éxito en la vida Mil gracias por tu cooperación, amistad y sobre todo por tu cariño

A Dios
Por todo lo que me ha dado en la vida

Cintia Quezada Reyes

A mis padres Graciela Rodríguez y Regino Gutiérrez
Porque a través de su apoyo, cariño y comprensión me han guiado para encontrar el más grande tesoro que existe en la vida...el estudio. Estaré siempre endeudado con ustedes. Los quiero mucho.

A mis hermanas Graciela y Rocio Gutiérrez
Por compartir, conmigo, todos los días de su existencia y por ayudarme a conservar unida a la familia a la que pertenecemos. Sólo les recuerdo que todo lo que deseen en esta vida se puede lograr si son constantes.

A mis abuelitos Guadalupe Salazar y Adolfo Rodríguez.
Por apoyarnos en todo momento y más aún cuando los necesitamos. Mil gracias por estar conmigo en un logro más de mi vida. También quiero compartir con mis abuelitos ***Bruno Gutiérrez (+) y Socorro Alcántara*** este momento.

A mi tía Ma. de Jesús Rodríguez (+)
Por brindarnos todo su amor y tiempo cuando estuvo con nosotros. Desde el cielo, sé que me seguirás impulsando para que pueda lograr mis objetivos Gracias

A mis amigos
Por su amistad que es algo de lo más valioso y escaso en estos días Debemos recordar que "sólo quien sabe ser amigo puede tener amigos". Gracias

A mis maestros
Por contribuir con sus conocimientos y experiencias en mi formación académica Todos ustedes forman parte de este sueño alcanzado Gracias.

A mi amiga y compañera Cintia Quezada
Por permitirme estar contigo en uno de los momentos más anhelados de mi vida y sobre todo por cooperar con tu entusiasmo, dedicación y deseos de superación para hacer posible este éxito más en nuestras vidas Muchas gracias por existir y por dejarme entrar en tu corazón

A la M. en C. Ma. Jaquelina López Barrientos

Por su apoyo incondicional, sus valiosas enseñanzas, su calidad humana y la dirección recibida para alcanzar esta meta tan anhelada. Mil gracias por todo.

Cintia y Sergio

ÍNDICE

CAPÍTULO 1.
INTRODUCCIÓN

1. INTRODUCCIÓN

Es bien sabido que "El saber es poder", efectivamente el conocimiento nos permite, hasta cierto punto, un determinado control o "poder" sobre alguna actividad o tarea Considerando lo anterior, en el contexto informático se puede hablar de que quien tiene el conocimiento suficiente para entender todo lo que incluye el universo de la computación, podrá entrar a un mundo diferente donde se dará cuenta de que "Quien tiene la información tiene el poder".

Por lo tanto, se debe poner especial atención al valor de la información Porque después de los recursos humanos, la información es el activo más valioso de cualquier empresa o persona que la posea.

En general, lo valioso de la información depende de quién la tenga, por ejemplo, los altos ejecutivos de una organización que se dedican a tomar decisiones, entonces necesitarían información relacionada con su contabilidad o relacionada con los resultados que se obtuvieron durante su campaña de publicidad; de tal manera, que de acuerdo al análisis de la información emitirían una decisión. Sin embargo, si esa misma información cayera en manos de alguien que no está ligado absolutamente a los negocios no le daría valor alguno Por otro lado, si la misma información estuviera en manos de una organización que se dedica al mismo giro, le sería de mucha utilidad.

El anterior y muchos ejemplos más, revelan que cada persona u organización que posea información en sus computadoras deberá darle la protección y seguridad adecuada para que su activo más importante no se vea alterado, observado o robado

La seguridad de la información, es una cuestión que llega a afectar, incluso, la vida privada de las personas, de ahí que resulte obvio el interés creciente que día a día se da para proteger la información de cualquier amenaza o ataque

El inicio para reducir la inseguridad de la información es crear conciencia de que la seguridad no sólo es asignar una contraseña para acceder a una determinada aplicación o base de datos, ni tampoco es cuestión de sólo colocar un firewall en la red

Es necesario saber y comprender que lo más importante es proporcionar confidencialidad, integridad y disponibilidad a la información Para ello, aparte de los mecanismos, ya mencionados, no hay que olvidar la parte física (hardware) por la que fluye la información que se desea proteger Así que también hay que poner especial importancia a la seguridad de las redes

Por tales motivos, la finalidad de este trabajo es dar un panorama general acerca de la seguridad de la información y por consiguiente seguridad en las redes. Los puntos más sobresalientes, en términos generales, que se desean cubrir en este trabajo son:

- Definir cuáles son las principales amenazas y vulnerabilidades de un sistema informático, así como los distintos tipos de medidas que podemos utilizar para prevenirlas.
- Introducir los conceptos de seguridad, información y seguridad informática.
- Definir los servicios básicos involucrados en la seguridad informática, así como los mecanismos que se utilizan para su implementación
- Definir lo que es criptografía y los tipos existentes
- Definir qué se entiende por política de seguridad y tipos de modelos.
- Complementar la parte teórica a través de prácticas.

A continuación se muestra como está conformado el trabajo y se describe brevemente el contenido de cada capítulo

Debido a los grandes avances tecnológicos, la preocupación por las continuas amenazas que puedan afectar la información es aún más evidente. Para entender claramente cuáles son las posibles amenazas que ocasionan los diversos tipos de ataques, los tipos de individuos que son capaces de cometer delitos y el software que tiene efecto dañino en el sistema, el *capítulo 2* describe a detalle cada uno de estos puntos buscando así que el lector conozca estos aspectos y con ello pueda estar alerta en cualquier situación que pudiera representar un *ataque de seguridad informática*

Una vez que se tiene conocimiento de las posibles fuentes de amenazas – que son inherentes a la información –, el *capítulo 3* nos conduce a comprender qué es la seguridad y la importancia de la misma. Además se describe de manera detallada cuales son los niveles de seguridad actuales y su importancia internacional. Con lo anterior se pretende asentar los *fundamentos de seguridad*

Hasta este momento se sabe que siempre debe existir cierta protección, sin embargo, ésta debe ser la adecuada, por ello, antes de implementarla es necesario decidir para qué se quiere dicha protección o de quién se quiere proteger, esto es fácil averiguarlo con base en los siguientes intereses:

1 Que nadie se entere de la información.

2 Que la información no se destruya o se pierda.

3. Que la información no se altere

4. Que la información sea auténtica

Para plantear una seguridad específica según el interés, es importante distinguir los servicios ideales que se utilizan para tal propósito. Para asegurarse de no cometer error alguno en la selección, el *capítulo 4* describe a detalle cada uno de los *servicios de seguridad.*

Así como desde hace mucho tiempo se ha tratado de guardar los mensajes en secreto para mantener su privacía y ya en el pasado se recurría a técnicas de cifrado de información, actualmente el cifrado es el método más socorrido no sólo para mantener la confidencialidad de la información sino para cubrir otros servicios de seguridad como la integridad y la autenticación, por lo tanto el *capítulo 5* describe a detalle los métodos criptográficos más usados y se plantea un panorama general de lo que es la *criptografía*

Desafortunadamente, hoy en día, cualquier organización al momento de preocuparse por la seguridad de su información, sólo se basa en los nuevos productos que están en el mercado, sin analizar si éstos son los adecuados porque cumplen con su(s) política(s) de seguridad informática, de hecho, la mayoría ni siquiera cuenta con una política de seguridad informatica en la cual se determinan las normas que deben cumplirse dentro de la empresa con base en sus requerimientos específicos de seguridad para resguardar la información y con base en ellas, determinar entonces los mecanismos a adquirir para hacer cumplir ese conjunto de normas establecidas dentro de la organizacion, el *capítulo 6* plantea, los puntos que deben tomarse en cuenta para desarrollar una política de seguridad informática y a través de su aplicación obtener la *seguridad en una organización*

Una vez que se ha determinado el servicio de seguridad adecuado para la protección que ayuda a cumplir la política de seguridad, debe escogerse la técnica que pueda implementarlo, para esto, el *capítulo 7* detalla con sumo cuidado los *mecanismos de seguridad* más empleados.

Debido a que Internet es un medio muy utilizado hoy en día, que se ha convertido en la red más grande del mundo, el recurso de dominio público y de uso general más difundido, es necesario describir algunas de sus vulnerabilidades y mejorías de los protocolos que se utilizan, esto puede observarse en el *capítulo 8*, donde se detallan puntos de los más importantes o representativos que involucran la *seguridad en Internet*.

Además se incluyen cinco prácticas, las cuales tienen como objetivo reforzar los conceptos básicos expuestos en los capítulos que conforman el presente trabajo Aunado a las prácticas, se anexa una serie de reactivos – con la intención de evaluar los conocimientos adquiridos en cada capítulo – y una lista de lecturas recomendadas para que el lector pueda profundizar en aquellos temas que mayor interés le hayan causado.

Finalmente, en las conclusiones se mencionan los puntos a los que se llega tras la elaboración del presente trabajo ya que los temas que se tratan en los capítulos han sido diseñados con la finalidad de informar y crear conciencia sobre la importancia de la seguridad de la información y sobre todo para despertar el interés en aquellas personas que estén involucradas en el fascinante mundo de la computación y todo lo que ello implica

Los ataques tienen varios objetivos incluyendo el fraude, la extorsión, el robo de información, la venganza o simplemente el desafío de penetrar un sistema Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red

Un **escudo** es una técnica, procedimiento o cualquier otra medida que reduzca la vulnerabilidad, un escudo hace que las amenazas se vuelvan débiles o probablemente haya menos Algunos escudos son específicos para ciertas amenazas, otros protegen contra una amplia variedad de amenazas

Tipos de mal uso

Un ataque o caso de mal uso tiene un perpetrador, tal persona tiene una motivación (como una ganancia financiera o una revancha, inclusive la venganza) Algunas veces el motivo es complejo y difícil de entender El ataque tiene un método de operación – una manera de explotar una vulnerabilidad. Existe una misión (tal como una destrucción de datos) y un objetivo. Algunos ejemplos de los objetivos son archivos, contraseñas y mensajes.

Los incidentes de mal uso varían en sus resultados Los resultados pueden ser pérdidas de confidencialidad, pérdidas en la integridad de la información, robo en los servicios informáticos, robo de los recursos controlados por el sistema o denegación del servicio.

Los incidentes que violan la confidencialidad sólo son considerados como mal uso pasivo y en los casos que alteran los datos son mal uso activo

Los casos de mal uso también varían en los métodos o técnicas Las amenazas más comunes son los accidentes y los errores humanos No sólo se causan daño a ellos mismos, sino que proveen oportunidades para perpetradores maliciosos para causar otros daños Otro caso muy común es el abuso de autoridad por aquellos usuarios autorizados

Las amenazas de las personas externas a la empresa, incluyen virus, gusanos y diferentes tipos de software malicioso En muchos casos utilizan una combinación de métodos y solo algunas técnicas

Tipos de vulnerabilidades

Una vulnerabilidad es una debilidad que puede ser explotada para violar la seguridad. Las vulnerabilidades son también extremadamente variadas. Una administración pobre es un problema común que llega a ser grave cuando se acopla con una vulnerabilidad. Por ejemplo, los productos que son liberados con configuraciones inseguras. Un sistema operativo puede tener una arquitectura o un diseño defectuoso, muchos sistemas están expuestos a "agujeros" de seguridad que son explotados por los perpetradores para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" han sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de comunicación, navegadores de Internet, correo electrónico y toda clase de servicios en LAN's o WAN's. En lo que respecta al hardware, también puede tener defectos que puedan ser explotados para violar la seguridad

Perpetradores

Un perpetrador es un individuo que se basa en cualquier medio para cometer un delito o culpa grave

Los perpetradores pueden clasificarse en

a) Personas enteradas

Normalmente no se consideran hackers a los usuarios internos, lo cual es una postura acertada, siempre y cuando no se olvide el riesgo asociado que existe en los mismos, ya que un usuario interno es extremadamente más peligroso que un atacante externo

De tal manera, se asume que la intrusión se puede producir con un alto porcentaje de éxito si una persona enterada de información valiosa presta su ayuda desde el interior. La evolucion de técnicas existentes, como la emision de datos a través de protocolos de comunicacion, dificulta la deteccion de este tipo de acciones. Para finalizar este punto, cabe mencionar uno de los riesgos mas obvios: los antiguos empleados de la empresa

b) Hackers

Al comienzo del nuevo milenio, los hackers, se presentan con un cerebro desarrollado, curioso y con muy pocas armas: una simple computadora y una línea telefónica. Hackers, es una palabra que aún no se encuentra en los diccionarios pero que ya suena en todas las personas que alguna vez se interesaron por la informática o leyeron algún artículo relacionado a la computación

La palabra surge cuando un antiguo miembro del TMRC (Tech Model Railroad Club) y entonces profesor del MIT (Massachusetts Institute of Technology) hizo una visita al club y le preguntó a los miembros del Subcomité de Señales y Energía si les gustaría usar la TX-0. Ésta era una de las primeras máquinas que funcionaban con transistores en lugar de lámparas de vacío y había sido usada para ayudar en la puesta en marcha del gigantesco (para aquella época) TX-2

Dado que Tixo (como le llamaban) sólo tenía el equivalente a 9 KB de memoria, era fundamental optimizar al máximo los programas que se hacían para éste, por lo que una de las obsesiones fundamentales de los que lo usaban y se consideraban hábiles, era hacer los programas tan pequeños como fuera posible, eliminando alguna instrucción aquí y allá, o creando formas ingeniosas de hacer las cosas A estas habilidades ingeniosas se les llamaba "hacks" y de ahí es de donde viene el término "hacker", denominación que usaron entre los mismos compañeros

Hoy es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información considerada confidencial

Algunos de los puntos débiles que un hacker puede explotar son sistemas operativos defectuosos, una descuidada administración del sistema, la asignación tonta de los privilegios a un usuario, etc

El acceso se efectúa a menudo desde un lugar exterior, situado en la red El hacker puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema A menudo se hacen pasar por usuarios legítimos del sistema esto suele suceder con frecuencia en los

sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema

c) Espías

Un espía, es un individuo o proceso que ha sido enviado o implantado de manera secreta, para observar, escuchar, seguir a una persona, cosa o proceso, con el único propósito de recabar información. En la historia de la seguridad informática, el espionaje extranjero es el prototipo de la amenaza. Poca información está disponible públicamente.

Código malicioso

Se trata de cualquier software que entra en un sistema de cómputo sin ser invitado e intenta romper las reglas Esto incluye a los caballos de Troya, virus, gusanos, bombas lógicas y otros métodos de amenazas programadas El código malicioso explota los flujos de información en los sistemas operativos y software asociado, además explota la configuración insegura, la mayoría de los sistemas son entregados con configuración insegura y eso se debe a que es más fácil de instalar y utilizar.

Los tipos de código malicioso más comunes son caballos de Troya, virus y gusanos

a) Caballos de Troya

Los caballos de Troya fueron los primeros tipos de códigos ajenos al sistema, reconocidos y estimulados por los esfuerzos de seguridad de muchas computadoras Un caballo de Troya es un programa aparentemente útil que contiene funciones escondidas y además pueden explotar los privilegios de un usuario dando como resultado una amenaza hacia la seguridad Un caballo de Troya es más peligroso que un administrador del sistema o un usuario con ciertos privilegios

Un troyano comun es un programa que nos pide que se ejecute con privilegios de administrador, y cuando se ejecuta se dedica a borrar todo lo que puede

Recientemente, el término de caballo de Troya ha sido usado generalmente para incluir amenazas que no dependen de la cooperación de un usuario Por ejemplo, la penetración, en un sistema de utilidades estándar, puede sustituirse por una caballo de Troya o puede ser recibido en un correo electrónico para que éste pueda explotar los puntos débiles de los controles haciendo que causen su propia ejecución.

Un caballo de Troya es extremadamente peligroso, porque discretamente accede a los controles que son ineficaces contra él Muchas otras técnicas son construidas en un caballo de Troya.

Amenazas a la Integridad y la Confidencialidad

Como ha sido enfatizado, el caballo de Troya discretamente accede a los controles no protegidos contra él A través de un caballo de Troya no pueden derribarse los controles de mando, pero sí pueden violar su política Desde entonces más políticas también involucran controles discretamente

Se podría pensar que si se examinara cuidadosamente el origen del código, éste podría revelar un caballo de Troya, pero incluso con tal verificación es poco probable que se localice

Un caballo de Troya puede violar la integridad mucho más fácilmente que la confidencialidad Desde que el caballo de Troya tiene los derechos del usuario, puede modificar o destruir cualquier objeto que el usuario pueda modificar o destruir En efecto, el autor no necesita acceder a todos los sistemas del usuario, sino sólo necesita alguna manera de conseguir que el caballo de Troya sea ejecutado

Para violar la confidencialidad, el caballo de Troya debe mover la información a algún lugar donde el usuario pueda escribir y el autor pueda leer, tal vez ese lugar sea difícil de encontrar En algunos sistemas el autor puede crear un archivo escribible para el usuario

Si el software que lleva el control del acceso puede invocarlo por un programa (que generalmente puede hacerlo), el caballo de Troya puede modificar los derechos de los accesos a los archivos de los usuarios otorgando acceso de lectura al autor o al perpetrador

b) Virus

Los virus son la principal amenaza en la red Estos programas de extensión relativamente pequeña, son programas capaces de replicarse o copiarse a sí mismos. Internet aporta lo que se podría decir una vía rápida de infección de este tipo de programas dañinos. Antes, la distribución de los virus era una tarea lenta ya que sólo se contagiaban a través de discos de 3.5". Las tres vías de propagación más ampliamente conocidas son: un archivo anexo o adjunto al correo electrónico, una transferencia por FTP y descargar un archivo infectado desde una página web.

Además poseen particularidades que los hacen perfectamente reconocibles por la forma en que trabajan; el virus nace en la computadora del creador como subprograma ejecutable, después se inyecta o descarga en la red o se copia dentro de un programa comercial de gran difusión para asegurar un contagio rápido y masivo.

Cuando el virus se ejecuta, él intenta copiarse (o modificar su propia versión) en algún otro programa residente La nueva residencia del virus es modificada en memoria o en un disco, después el virus típicamente lleva a cabo una misión destructiva, tal como destruir el boot record o la tabla de asignación de archivos en un disco. Al principio eran programas pequeños que se copiaban (reproducían) a sí mismos por el simple hecho de ejecutar un programa infectado Esta similitud con los virus biológicos produjo su nombre

En efecto, la misión puede ser casi cualquier cosa, algunos virus simplemente tratan de exponerse a la vista de los demás mientras que otros son extremadamente destructivos La víctima experimenta un espantoso engaño, una herramienta confiable, de repente se comporta de manera arbitraria y perjudicial

Actualmente estos pequeños programas se han convertido en sofisticados códigos para impedir su detección Al principio se podrían detectar por el simple hecho de comprobar la modificación de los programas o su tamaño, pero los virus más modernos se las arreglan para ocultar sus modificaciones con metodos como tomar control sobre el sistema operativo y cuando se pide información del programa se muestra la original que fue almacenada en el momento de la infección

Los virus son peligrosos porque se propagan ellos mismos e infectan a otras computadoras. Los programas infectados usualmente realizan sus funciones normales Los virus pueden residir en discos o en cintas de respaldo y aparecen después de un largo tiempo de haber sido plantados o reaparecen después de mucho tiempo de ser supuestamente erradicados El predominio de algunos virus parece incrementarse linealmente por completo a lo largo del tiempo y después nivelarse a un bajo nivel.

c) Gusanos

El concepto de "gusano" (introducido en el libro de ciencia-ficción, "The Shockwave Rider", por John Brunner, 1975) fue desarrollado e implementado por John Shoch y Jon Hupp en la compañía Xerox El concepto es de "un programa o un cálculo que se puede mover de máquina en máquina, aprovechando los recursos que necesita, y se replica a sí mismo cuando es necesario".

Los gusanos son programas que se propagan ellos mismos, un gusano hace una copia de sí mismo y lo realiza cuando es ejecutado Los gusanos frecuentemente se propagan de una computadora a otra a través de las conexiones de la red Como los virus, los gusanos provienen de fuentes anónimas o no localizables. Los gusanos están frecuentemente equipados con descifradores de contraseñas basados en diccionarios y otras herramientas tipo "cracker" – el que rompe la seguridad de un sistema – que les permiten penetrar en otros sistemas Los gusanos con frecuencia roban, destruyen o modifican datos en una computadora.

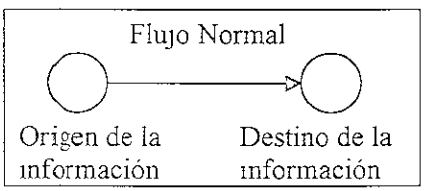
El ataque de un gusano puede involucrar diferentes programas que cooperan a través de la red A diferencia de los virus, un gusano no infecta un programa residente En espera de una orden para producir la ejecución de las réplicas de él mismo, un gusano necesita un sistema multitareas

Tienen como única misión la de colapsar cualquier sistema, ya que son programas que se copian en archivos distintos en cadena hasta crear miles de réplicas de sí mismos Así, un gusano de 866 Kb, puede convertirse en una cadena de archivos de miles de MB, que a su vez puede destruir información, ya que sustituye estados lógicos por otros no idénticos Suelen habitar en la red a veces como respuesta de grupos de hackers que pretenden obtener algo La existencia de uno de estos gusanos se hace notar cuando la red se alenta

considerablemente, ya que el proceso de autorreplicado llena el ancho de banda de trabajo de un servidor en particular.

Por otro lado, el cometido de los gusanos es el de devorar todos los datos de un archivo, hasta desplazarlos hacia otro archivo oculto.

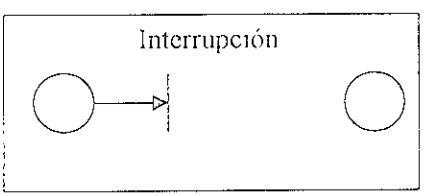
2.2 Clasificación General de amenazas inherentes a las redes



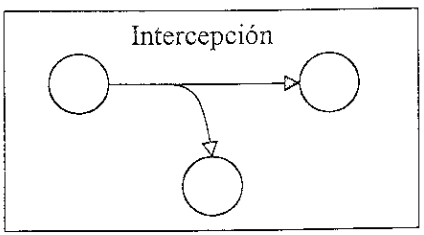
En el flujo normal de la información no debe existir ningún tipo de obstáculos para que la información llegue al destinatario.

Las cuatro categorías generales de amenazas o ataques son las siguientes:

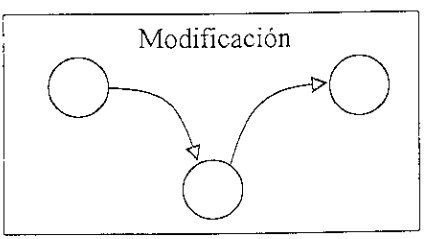
2.2.1 Interrupción: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la *disponibilidad* Ejemplos de este ataque son la destrucción de un elemento de hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos



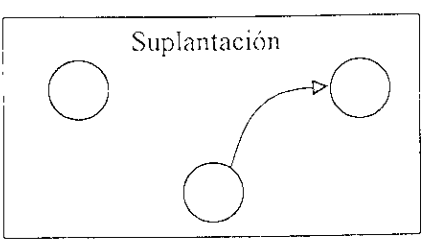
2.2.2 Intercepción: una entidad no autorizada consigue acceso a un recurso Este es un ataque contra la *confidencialidad* La entidad no autorizada podría ser una persona o un programa Ejemplos de este ataque son tener acceso a una línea para hacerse de datos que circulen por la red y la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de los paquetes para revelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad)



2.2.3 Modificación: una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la *integridad*. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.



2.2.4 Suplantación: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la *autenticidad*. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.



Estos ataques pueden asimismo clasificarse de forma útil en términos de ataques pasivos y ataques activos.

2.3 Otras clasificaciones

Otra forma de clasificar los ataques es tomando en cuenta si los perpetradores alteran o no la información.

2.3.1 Ataques pasivos

Los ataques pasivos reciben su nombre debido a que el atacante – también llamado perpetrador, oponente o persona que se entromete – no altera en ningún momento la información, es decir, únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida. Cualquier ataque pasivo tiene los siguientes objetivos principales:

2.3.1.1 Intercepción de datos: consiste en el conocimiento de la información cuando existe una liberación de los contenidos del mensaje.

2.3.1.2 Análisis de tráfico: consiste en la observación de todo el tráfico que pasa por la red.

Con los ataques pasivos se obtiene información que puede consistir en:

a) **Obtención del origen y destinatario** de la comunicación, esto se logra cuando el perpetrador lee las cabeceras de los paquetes que continuamente está monitoreando. Con ello se determina la localización y la identidad de los anfitriones (emisor, receptor)

b) **Control del volumen de tráfico** intercambiado entre las entidades monitoreadas, de esta forma se obtienen todos los datos necesarios para percatarse de la actividad o inactividad inusuales, se conoce la frecuencia y longitud de los mensajes

c) **Control de las horas habituales** de intercambio de datos entre las entidades de la comunicación, con ello se extraen los datos acerca de los períodos de actividad. El perpetrador conoce la frecuencia con la que se transmiten los mensajes

Desafortunadamente, los ataques pasivos son muy difíciles de detectar e interceptar, debido a que no provocan ninguna alteración de los datos. Aun cuando

su detección es prácticamente imposible, es necesario tomar en cuenta que puede evitarse el éxito de este tipo de ataques si se considera el uso del cifrado de la información, así como la existencia y utilización de otros mecanismos.

2.3.2 Ataques activos

Los ataques activos se nombran así debido a que implican algún tipo de modificación del flujo de datos transmitido (modificación de la corriente de datos) o la creación de un falso flujo de datos (creación de una corriente falsa).

Los ataques activos pueden clasificarse de la siguiente manera:

2.3.2.1 Enmascaramiento o Suplantación de identidad: en este caso, el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como el robar la contraseña de acceso a una cuenta.

2.3.2.2 Réplica o Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado debido a que se realiza una retransmisión subsecuente. Por ejemplo, se podría utilizar para ingresar dinero repetidas veces en una cuenta dada.

2.3.2.3 Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mismos mensajes son retardados o reordenados, esto provoca que se produzca un efecto no autorizado. Ejemplos de mensajes modificados:

Mensaje original: "Permitir a Javier Borja leer archivos de cuentas confidenciales"
Mensaje modificado: "Permitir a Joaquín Ríos leer archivos de cuentas confidenciales"

Mensaje original: "Ingresar un millón de pesos a la cuenta 92225909-2"
Mensaje modificado: "Ingresar un millon de pesos a la cuenta 92225909-5"

2.3.2.4 **Degradación fraudulenta del servicio:** este tipo de acción impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones (medios de comunicación). Entre estos ataques se encuentran los de **denegación de servicio**, los cuales consisten en paralizar temporalmente el servicio Por ejemplo: el intruso paraliza temporalmente el servicio de correo en el servidor de una red

2.4 Métodos de ataque

Un ataque en un sistema de cómputo contempla tres etapas principales:

1. **Preparación:** el método de ataque se plantea u otras preparaciones se realizan.

2. **Activación:** el ataque se activa o dispara

3. **Ejecución:** la misión[1] se lleva a cabo mediante la desviación de los controles de acceso, violación de secretos o integridad, denegación de servicio, robo de servicios, o simplemente dar a conocer el ataque

2.4.1 Preparación y planteamiento

Algunas formas para efectuar esta primera etapa se explican en este punto, siete de las más comunes se muestran a continuación

a) **Recolección de información:** es sabido que la información es el objetivo principal de los atacantes. Los individuos que poseen ciertos derechos sobre la información o flujos de información secreta, simplemente recolectan la del sistema que están autorizados a monitorear, sin embargo, las personas externas deben ingeniárselas para obtenerla, esto puede lograrse a través de engaños - basándose principalmente en convencer a la gente de que haga lo que en realidad no debería Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la contraseña con alguna excusa convincente Esto es común cuando en el Centro de Cómputo los administradores son amigos o conocidos

[1] Misión es el poder que se da a un enviado para desempeñar algun cometido La orden dada para determinado fin

b) **Caballo de Troya:** un usuario coloca un programa dentro de su dominio de protección, cuando el programa se ejecuta, obtiene los privilegios de dicho usuario, de esta manera se convierte en un cómplice inconsciente ya que envía y concede información a los perpetradores desde sus archivos (de forma no aparente). Se realiza una analogía con el caballo de Troya pues sin saberlo se está ayudando al atacante

c) **Propagación programada:** se refiere al código malicioso que se introduce en un equipo de cómputo ya que puede multiplicar su ámbito y daño. Los gusanos y virus se propagan por sí mismos

d) **Puerta trasera:** el software contiene mecanismos escondidos que permiten a los diseñadores (o quienes sepan el secreto) desviar los controles. Este tipo de mecanismo recibe el nombre de puerta trasera Un ejemplo clásico de puertas traseras se refiere a un programa en donde se requiera un nombre de usuario pero sin una contraseña válida

e) **Enmascaramiento o engaño:** significa que se pretende ser alguien más de tal manera que se pueden obtener los derechos de acceso de una persona. El enmascaramiento envuelve un ataque en los controles de autenticación, por lo que un sistema puede enmascararse como otro sistema para engañar al usuario y descubrir información

f) **Exploración:** antes de que el enmascaramiento se realice, el atacante necesita conocer las contraseñas, números telefónicos, etc , para ello es necesario hacer uso de la exploración, es decir, es necesario enviar una secuencia de información cambiante a una computadora, para encontrar valores que muestren respuestas positivas

g) **Mal uso de la autoridad:** si el atacante penetra de manera legítima al sistema, la preparación es mucho más fácil ya que está haciendo mal uso de la autoridad que posee dentro de la organización

2.4.2 Activación

En esta segunda etapa, la activación puede realizarse de las siguientes maneras

- Si el ámbito de preparación asume el control de una interrupción de un sistema operativo, el código de ataque es invocado cuando la interrupción se lleva a cabo, si no es así, el perpetrador puede invocar directamente un programa que lleve a cabo la misión.

- Un ataque más sofisticado impone un retardo entre la preparación y la activación, esto ocasiona que la identificación del atacante sea mucho más difícil, el retardo puede provocar que el ataque sea más destructivo, hablando específicamente de los virus.

- Una bomba de tiempo se encuentra arreglada para estallar a una hora y día determinados. Puede engancharse por sí sola a programas regulares de ejecución, verifica la hora designada y cuando ésta llegue, lleva a cabo la misión, aunque en ocasiones la bomba puede estar planteada en un programa cíclico de funcionamiento como un proceso de fin de mes. Una bomba de tiempo es un tipo de bomba lógica, ya que ésta se acciona por cualquier combinación de condiciones.

2.4.3 Misiones

Las misiones pueden ser:

a) **Mal uso activo:** un mal uso activo afecta la integridad de la información o disponibilidad de los servicios. Los archivos pueden ser destruidos o sutilmente alterados. Los mensajes pueden ser alterados, borrados o insertados, éstos pueden estar mal encaminados y su origen aparente puede estar modificado. Cualquier individuo que contenga información secreta puede destruir datos valiosos, instalar puertas traseras, alterar el estado de autorización, causar la caída del sistema y destruir la evidencia.

b) **Mal uso pasivo:** cuando la confidencialidad es violada pero el estado del sistema no es afectado, el mal uso es pasivo pero no por eso menos dañino, de hecho, podría resultar más letal que el activo. Algunas técnicas empleadas en el mal uso pasivo son las siguientes:

   1. **Fisgoneo (la intromisión no autorizada):** el fisgoneo abarca desde el escuchar de manera sofisticada lo que se transmite en una ruta de comunicación, hasta mirar por arriba del hombro de un usuario, lo que éste escribe con el teclado.

2. **Residuo:** la mayoría de las políticas de seguridad apuntan a la protección de la información y no a los objetos (discos, segmentos de memoria) que guardan dicha información Algunas amenazas explotan la relación imperfecta entre ambos puntos, ya que, en ocasiones el objeto es reutilizado por otro usuario sin que se le borre la información anterior. A este tipo de vulnerabilidad se le nombra "residuo" o "problema de objeto-reuso" y a la amenaza se le llama barrido, éste puede ocurrir fuera del sistema de cómputo en listados desechados del programa o en los resultados de las pruebas realizadas.

3. **Hojeo:** el hojeo se refiere a la búsqueda ociosa través del almacenaje (información disponible) sin saber exactamente qué información se busca o si existe. El hojeo y la búsqueda son efectivos en los sistemas abiertos o en aquéllos que se encuentran penetrados por otros medios. Debe notarse que la información considerada de uso histórico es igual de importante que la información vigente, desafortunadamente se le presta mayor atención a esta última y por ello se le da la preferencia en seguridad, lo cual es un grave error. ya que el descuido de cualquier tipo de información es de gran ayuda para que los perpetradores logren sus ataques

4. **Interferencia:** la técnica de interferencia junta piezas de información accesible para llegar a la información que se supone es secreta

5. **Canales encubiertos:** un sistema cuya política es el control del flujo de la información, es vulnerable al uso de canales encubiertos Según la política de seguridad multinivel, un usuario de nivel secreto, no puede transferir información secreta a un usuario de información confidencial ya que tanto la información como las personas tienen niveles de clasificación y cualquier persona autorizada recibe un permiso para un cierto nivel, por lo que puede tener acceso únicamente a la información que se encuentra hasta el nivel al que está autorizado los niveles de clasificacion son super secreto, secreto, confidencial y no clasificado , sin embargo, si ambos cooperan, pueden transferir informacion de maneras sutiles, utilizando canales que no son dedicados para esos propositos Pueden modificar la información almacenada o controlar el horario de los eventos, es decir, pueden utilizar canales de almacenamiento o canales de tiempo

c) **Denegación de servicio:** los ataques de denegación del servicio son los más fáciles de realizar. Las redes pueden abrumarse con tráfico, Cualquier tipo de caída traumática, interrupción de la energía o falla de una PC infectada por virus, deniega el servicio.

d) **Robo del servicio:** los hackers roban los servicios de cómputo y de comunicación de los sistemas en los que penetran. Los usuarios autorizados pueden estar jugando, enviar correo electrónico personal, mantener negocios personales y vender servicios a personas externas. Aun cuando muchas de estas actividades son inofensivas, son consideradas como un fraude, y ya que divide los recursos de cómputo, el robo de servicio en un sistema compartido hace que el servicio (proceso, flujo de información, etc.) se vuelva tan lento que llegue a la denegación de servicio

2.4.4 Ataques en escudos

Conforme la seguridad en cómputo madura, los atacantes invierten más esfuerzos para desarmar los escudos

a) **Autenticación:** un intruso debe pasar los controles de la conexión para progresar. La conexión en la mayoría de los sistemas de cómputo está protegida solamente por contraseñas. La persona que se conecta debe proveer un nombre de usuario o un identificador de cuenta más una contraseña asociada con tal identificador Desafortunadamente, las contraseñas son escudos débiles Los usuarios generalmente escogen sus contraseñas, si no se hiciera de esta forma, los usuarios tendrían problemas en recordarlas y las escribirían en lugares inconvenientes donde los intrusos pueden encontrarlas La mayoría de los usuarios escogen contraseñas fáciles de adivinar como sus nombres o identificadores de cuenta. Cuando esta tendencia se combina con la débil protección de los archivos de contraseñas, el resultado es una autenticación débil Algunos sistemas almacenan las contraseñas de una forma seudocifrada, el archivo de estas contraseñas transformadas puede ser leído por cualquier usuario y es imposible transformar las contraseñas desde su forma cifrada a su forma original Esta forma es más segura, el problema es que estas contraseñas son escogidas de un número limitado de nombres y letras Otros ataques pueden tener contraseñas en una forma clara (no cifrada), lo cual provoca que los atacantes primero penetren en

el sistema, enseguida obtengan el estado (condición) de privilegio y finalmente instalen el software que recolecta la información de todas las nuevas sesiones de la red, esta información incluye los identificadores de cuentas y las contraseñas de otras computadoras. La información se almacena para después tener acceso. Los atacantes tienen la oportunidad de comprometer más contraseñas ya que las comprometidas les dan acceso a otros sistemas Los ataques hacen evidente lo que se sabe: la contraseña familiar "reutilizable" es vulnerable y esto ocasiona que una vulnerabilidad del sistema sea otra vulnerabilidad del sistema. Otro problema es que algunas instalaciones se niegan a cambiar los identificadores y las contraseñas para las cuentas enviadas por un sistema operativo. El atacante que sabe esto puede darse de alta como programador del sistema o administrador de seguridad. Otros nombres de cuentas y contraseñas son difíciles de adivinar. Otro ataque empleado es el de la cuenta llamada INVITADO con la contraseña INVITADO.

b) **Ataques de tuneleo:** otra forma de derrotar a los escudos es atacando por debajo del nivel del escudo Si hay control de acceso en los archivos, se atacan los sectores del disco donde se almacena el archivo Si una aplicación de transacción tiene controles estrictos, se ataca el módulo del programa de la transacción Un ataque que va por debajo de los controles de esta forma, es llamado ataque de tuneleo. Este tipo de ataques utilizan herramientas del sistema que han sido creadas para ese propósito (desviación de procedimientos normales para corregir problemas de emergencia). Este tipo de ataque puede modificar el hardware o el microcódigo para permitir el desvío de los controles Este ataque se aprecia en la figura 2 1.

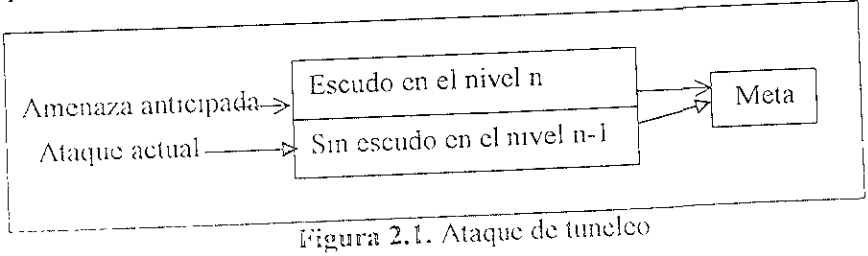


Figura 2.1. Ataque de tuneleo

c) **Compromiso de cifrado:** algunos métodos de cifrado son efectivos si las claves de cifrado se eligen cuidadosamente Una clave puede conocerla un intruso El sistema de cifrado puede romperse La implementación de

un algoritmo de cifrado puede contener errores El cifrado es parte de protocolos complejos empleados para resolver problemas de seguridad específicos, estos protocolos pueden tener errores. Finalmente el cifrado es utilizado en un largo contexto del sistema. El sistema total puede ser pobremente diseñado o pobremente manejado.

d) **Destrucción de la evidencia:** los procesamientos recaen en el registro del historial de la computadora. Los registros o rastros de intervención son valiosos porque generalmente están bien protegidos. Los registros en línea pueden ser desviados, alterados o destruidos (si sus controles son derribados) y los registros fuera de línea pueden ser destruidos (si físicamente la seguridad es floja)

e) **Subversión de los controles de aplicación:** muchos de los escudos más efectivos operan en el nivel de aplicación Ellos incluyen controles de cuentas, integridad y razón para controlar la entrada de datos y un esfuerzo para separar la responsabilidad Aun cuando no se tengan programas modificados, una persona enterada que conoce una aplicación íntima, puede explotar la debilidad de sus controles. Las personas que tienen acceso a la aplicación de los programas pueden alterarlos (durante su desarrollo o su mantenimiento) para generar transacciones fraudulentas, para desviar el control en ciertas entradas o para remover o alterar los expedientes de las transacciones. Un método es el ataque del salami, llamado así porque delgadas rebanadas son tomadas de vez en vez sin que se note la reducción del todo. Cada víctima pierde un poco de la cantidad y sus controles no son violados Una variedad del ataque del salami es el fraude bajo el redondeo que consiste en redondear las cantidades para quedarse con el sobrante

Lecturas recomendadas

[2]. Amenazas, ataques y vulnerabilidades

[3]. Amenazas, ataques, vulnerabilidades

[4]. Amenazas, servicios y mecanismos

[5]. Amenazas y ataques a la seguridad

[17]. Definiciones de hacker y cracker

[19]. Delitos informáticos: virus, gusanos..

[21]. Diferencia entre hacker y cracker

[57] Chapter 1. Introduction:
1.1 Attacks, services and mechanisms
1.2 Security attacks

[58]. Chapter 3 Threats

[66] Virus

CAPÍTULO 3.
FUNDAMENTOS DE SEGURIDAD

3.1 Definiciones

El concepto de **seguridad** se refiere a todo tipo de precauciones y protecciones que se llevan a cabo para evitar cualquier acción que comprometa a la información.

Se entiende por **información** a todo mensaje (conjunto de datos) que: al receptor le interese, le entienda o lo ignore antes de recibirlo.

Por consiguiente, el término **seguridad de la información** se refiere a la prevención y a la protección, a través de ciertos mecanismos, para evitar que ocurra de manera accidental o intencional, la transferencia, modificación, fusión o destrucción no autorizada de la información.

Existen dos nuevos conceptos que hay que considerar debido a que la seguridad de la información así lo requiere: seguridad informática y seguridad de la red.

Con la introducción de la computadora, la necesidad de herramientas automatizadas para proteger la información almacenada en la computadora se volvió más evidente, por lo que la **seguridad informática** es el nombre genérico dado a una colección de herramientas diseñadas para proteger datos y detener a los perpetradores, es decir, es la protección de los sistemas de cómputo para evitar amenazas de confidencialidad, integridad o disponibilidad

A continuación en la figura 3.1 se muestra el contexto de la seguridad informática, con lo cual se hace referencia a las condiciones que proponen las amenazas y que conforman el desarrollo y el uso de los escudos

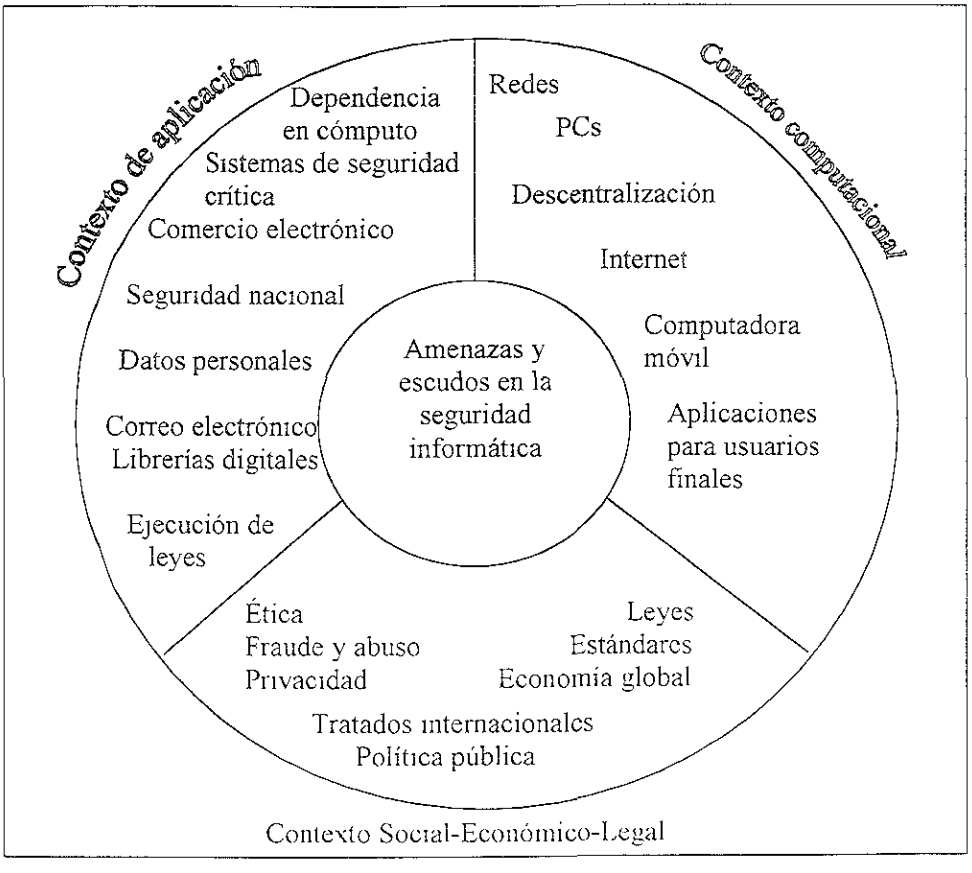


Figura 3.1. Contexto de la seguridad informática

El segundo concepto surge con la introducción de los sistemas distribuidos, aunado al uso de redes y las facilidades que el desarrollo de la tecnología proporciona a la comunicación, ya que con ésta se obtienen los elementos necesarios para transportar los datos entre una terminal de usuario y una computadora o entre una computadora y otra. Dado el avance de la tecnología de red, la cual ha permitido que las computadoras de todo el mundo se encuentren interconectadas, las amenazas de seguridad son una gran preocupación para las organizaciones y los usuarios. La protección de los recursos de la red, la información y servicios en contra de las amenazas de seguridad recibe el nombre de

seguridad de la red, cualquier medida realizada tiene como objetivo proteger los datos durante su transmisión

El principio de la seguridad de la red es proteger el entorno de cualquier tipo de amenazas de seguridad mediante servicios de seguridad, mecanismos, y técnicas para hacer cumplir una política de seguridad.

3.2 Niveles de seguridad

La palabra seguridad, en cualquier ámbito, siempre ha llevado consigo la idea implícita de confianza o tranquilidad para realizar diferentes actividades. Cuando se habla de seguridad la relacionamos, la mayoría de las veces, con Seguridad Social[2].

El simple hecho de vivir, de ninguna manera, nos garantiza estar seguros, bajo esta premisa se puede concluir que el riesgo en cualquier actividad humana puede ser medida con determinado porcentaje.

Por lo tanto, toda actividad tendrá riesgos y beneficios posteriores a su desarrollo, dando pauta para evaluar la relación existente entre los riesgos (costos) y los beneficios

Tomando en cuenta la premisa mencionada, podemos afirmar que la seguridad informática no existe en su totalidad, debido a que toda nuestra información se encuentra almacenada en la computadora y ésta se compone de estructuras (conjunto de elementos electrónicos) que se mueven bajo un concepto de riesgo estadístico

Dicho riesgo estadístico, nos indica la probabilidad de que un suceso ocurra (medido generalmente en horas) y si ocurre, en qué porcentaje va a afectar sus funciones De esta manera la mayoría de las piezas que componen una computadora (hardware) tienen una medida, llamada MTBF (Meaning Time Between Failures) o tiempo esperado entre fallas

Como se ha venido mencionando, no tenemos garantizada totalmente la seguridad en un sistema informático pero lo que sí podemos hacer es tratar de

[2] Conjunto de leyes y de los organismos que las aplican, que tienen por objeto proteger contra determinados riesgos sociales (accidentes, enfermedad, vejez, etc.)

reducir las probabilidades de fallas en el sistema cuando se presenten ataques o sucesos inesperados de inoperabilidad en los equipos que conforman al sistema.

La seguridad de un sistema informático[3], estará siempre ligada a los dos elementos que lo componen, es decir, al software y al hardware. En general la seguridad del sistema no se limitará únicamente a evitar la modificación de la información o de restringir el acceso a personas no autorizadas, sino que deberá también preocuparse por la protección de los equipos donde se opera y almacena la información

Ambos elementos deben tener la misma importancia en lo que respecta a seguridad, sin embargo, las estadísticas[4] de 1989 nos muestran que errores intencionales de los empleados fueron responsables del 65% de pérdidas financieras debido a fallas en la seguridad informática. La deshonestidad de los empleados arroja el 13%; cuando no están a gusto con su jefe o su trabajo, provocan pérdidas por un 6% y el 3% lo realizan personas ajenas. Mientras que el 13% restante se debe a factores tales como fallas en la energía eléctrica o daños causados por la lluvia

Otros estudios encontraron diferentes motivos, de los empleados, que ocasionan pérdidas:

- La necesidad de resolver intensos problemas personales.
- Presiones y retos.
- Idealismo o defensa extrema
- Ganancia financiera

Un punto a destacar, también, es que los encargados de la seguridad del sistema están mas preocupados por el ataque de un experto para filtrarse en su información y que éste haga estragos en ella, que preocuparse por si los equipos que componen al sistema pueden llegar a fallar y puedan dejar de funcionar por un determinado tiempo

[3] Conjunto de dispositivos y programas que funcionen bajo un fin

[4] Summers, Rita *Secure Computing Threats and Safeguards* 1 U. A., Mc Graw Hill, 1997 p 76

De tal manera que las tendencias han hecho que la seguridad de la información se incline más por el lado del software que del hardware.

Para que haya equilibrio en la importancia que se le debe dar a la seguridad tanto en el software como en el hardware, fue necesario implementar niveles de seguridad.

El método para determinar los requerimientos de seguridad del hardware y el software de un sistema, se basa en

- La capacidad disponible de procesamiento para un usuario del sistema.
- El tipo de encaminamiento de la comunicación entre el dispositivo local del usuario y los componentes del sistema primario.
- La flexibilidad de la capacidad de procesamiento que el sistema provee al usuario
- El entorno en el cuál el sistema fue desarrollado.
- La diferencia entre los máximos y los mínimos permisos del usuario del sistema y la clasificación de los datos más susceptibles procesados por el sistema.

Este método puede ser entendido como una evaluación del riesgo de un sistema que puede ser conducido en una fase muy cercana al ciclo de vida de un sistema. Las estructuras y funciones del sistema cambian durante el desarrollo y la operación

Dependiendo del riesgo inherente que un sistema (o diseño del sistema) represente, se necesitan diferentes niveles de seguridad que pueden ser impuestos en un orden tal que reduzcan el riesgo operacional del sistema a un nivel aceptable

Tal equilibrio hace crear un estándar de seguridad en las computadoras, para proteger de un ataque al hardware, al software y por consiguiente a la información guardada

El estándar ha sido clasificado en niveles de seguridad y ellos están especificados en los Criterios Comunes para Evaluación de Seguridad de Tecnología de la Información versión 2.1

Criterios comunes

El TCSEC (Trusted Computer Security Evaluation Criteria or Orange Book creado a mediados de los 80's) proveía niveles que requerían una funcionalidad de seguridad específica que era conveniente para un entorno específico El ITSEC (Information Technology Security Evaluation Criteria por los gobiernos de Francia, Alemania, los Países Bajos y el Reino Unido), a principios de los 90's, proveía niveles de seguridad donde la funcionalidad del producto desarrollado se definía. Al final ambos probaron que no eran satisfactorios y las iniciativas se combinaron para producir un nuevo esquema. El nuevo esquema de evaluación de seguridad que reemplaza al TCSEC y al ITSEC, a finales de 1998, es llamado "Criterios Comunes para Evaluación de Seguridad de Tecnología de la Información" (Common Criteria for Information Technology Security - CCITSE) mejor conocido como CC

El nuevo esquema fue originado con proyectos cooperativos que estaban relacionados con la Organización Internacional de Estándares (ISO) La versión 2 0 de CC tenía el mismo contenido que la Redacción Final del Comité (FCD) 15408, la cual fue llevada a votación por parte de la ISO en el verano de 1998.

CCITSE versión 2.1, aprobada en agosto de 1999, fue adoptada por (ISO) como "Tecnología de información – Técnicas de seguridad – Criterios de evaluación para la seguridad de IT" (ISO/IEC 15408) en diciembre de 1999

En Octubre de 1998, Canadá, Francia, Alemania, el Reino Unido y los Estados Unidos firmaron un acuerdo de reconocimiento mutuo (MRA) de las evaluaciones basadas en los Criterios Comunes (CC) En mayo del 2000 un nuevo acuerdo de reconocimiento mutuo fue firmado, aquí se incluyó a Australia, Nueva Zelanda, Finlandia, Grecia, Italia, Holanda, Noruega y España Este acuerdo es un paso adelante significativo para el gobierno y la industria en el área de los productos de Tecnología de la Información (IT) y los perfiles de protección de las evaluaciones de seguridad El reconocimiento mutuo que este acuerdo provee significa que un certificado CC obtenido en un país es reconocido por los demas países firmantes

Los CC son una norma internacional para evaluar la seguridad de los productos de tecnología de la información (IT) basados en los criterios europeos, norteamericanos y canadienses existentes para la evaluación de la seguridad de la IT, por ello, los resultados obtenidos al realizar una evaluación – la evaluación la realiza una autoridad específica del país – siguiendo los CC, son reconocidos internacionalmente. Además tienen como objetivos principales proporcionar protección a la información, como por ejemplo: no revelar secretos sin autorización, perder información por el uso y modificar la información.

En la evaluación de las propiedades de seguridad de los productos, existen tres grupos que tienen interés general en la misma: los consumidores, los desarrolladores y los evaluadores.

Bajo los CC, las clases de productos son evaluadas basándose en los puntos de los Perfiles de Protección (PP) que especifican los requerimientos funcionales de seguridad. Los PP deben ser desarrollados para aplicarse en los sistemas operativos, firewalls, tarjetas inteligentes y otros productos que se espera cuenten con requerimientos de seguridad. Los CC especifican una serie de evaluación de niveles de confianza (Evaluation Assurance Levels - EAL) para los productos evaluados Un nivel alto de EAL especifica un nivel alto de confianza de que las funciones de seguridad del producto serán ejecutadas de manera correcta y efectiva Para los consumidores y los desarrolladores de productos IT, los CC proveen un conjunto de criterios y están diseñados de tal manera que los aspectos de seguridad del producto IT pueden ser medidos de manera respetable, reproducible e independiente con la libertad de resultados favorables

En una evaluación de CC un producto IT es evaluado contra un conjunto aprobado de criterios de evaluación de seguridad de la información El conjunto de evaluación de seguridad de los CC puede estar acostumbrado a evaluar todo tipo de productos IT Generalmente esto significa que para un producto IT específico, en una evaluación de CC, los siguientes aspectos se revisan

- Si los requerimientos del producto son definidos correctamente
- Si los requerimientos son implementados correctamente

- Si el proceso de desarrollo y documentación del producto cumple con ciertos requerimientos

Debido a que los CC son un medio para definir los recursos y la medida de los aspectos de la seguridad de los productos IT, proveen:

1. Un conjunto de criterios para las facilidades de prueba (llamadas facilidades de evaluación) para asegurar que dichas facilidades pueden ejecutar una prueba de seguridad bajo un sistema de calidad clara y definida

2. Un marco para la especificación de funcionalidad que:

   - Permite a los consumidores claramente especificar el problema de su seguridad

   - Permite a los desarrolladores claramente especificar su solución de seguridad

   - Permite a los consumidores comparar varias soluciones de seguridad para su problema

   - Permite a los evaluadores determinar sin equivocaciones qué es lo que un producto hace

3. Un marco para la prueba de especificación que

   - Permite a los consumidores definir qué tan seguros están de querer saber si su producto es seguro

   - Permite a los desarrolladores saber anticipadamente qué entregas necesitan proveer y cuál debe ser el contenido de estas entregas

   - Permite a los evaluadores cumplir con las pruebas de una manera muy bien definida

Contenidos de la norma

Los CC versión 2.1 está formada por tres partes:

1. Introducción y Modelo General

Esta parte está destinada a la gente que tiene indicios acerca de la evaluación de seguridad ya que introduce los conceptos generales y el formato de los Criterios Comunes. En esta parte se describe cómo los CC son establecidos y para quién están destinados Además elabora sobre la definición de funcionalidad de seguridad, requisitos de confiabilidad y las estructuras de Perfiles de Protección y Metas de Seguridad.

2. Requerimientos de Seguridad Funcional

Esta parte está destinada a los usuarios y desarrolladores pues establece un conjunto de componentes de seguridad funcional como un estándar que expresa los requerimientos de seguridad funcional para los productos IT. Los componentes funcionales presentados son para utilizarse en los Perfiles de Protección y Metas de Seguridad

3. Requerimientos de Seguridad Confiable

Esta parte está destinada a los desarrolladores ya que define el criterio de confiabilidad que los evaluadores usan para verificar el desempeño de los desarrolladores y sus productos Introduce siete niveles de evaluación de confiabilidad (EALs) que define la escala de los CC para clasificar la evaluación de confiabilidad obtenida por los productos

Perfiles de Protección y Metas de Seguridad.

Los Perfiles de Protección y Metas de Seguridad, conocidos como PP y ST, son elementos muy esenciales del armazón de los CC Cuando se terminaron los documentos ST/PP eran muy similares Sin embargo, sirven a diferentes roles en el proceso de evaluación

- Un Perfil de Protección es un requerimiento que define un problema de seguridad general de un consumidor o grupo de consumidores. Básicamente un Perfil de Protección establece: Esto es lo que se necesita.

- Una Meta de Seguridad es una especificación que define una solución general de un desarrollador para un problema de seguridad Básicamente una Meta de Seguridad establece. Esto es lo que se ha construido o se construirá en el futuro

En el mundo ideal, un consumidor escribe un Perfil de Protección reflejando su problema de seguridad y lo envía al mundo. Uno o más desarrolladores producen Metas de Seguridad reflejando su solución al problema y lo envían al consumidor. Basado en esto, el consumidor selecciona una de ellas y compra el sistema de ese desarrollador.

Beneficios

Los CC ofrecen varias ventajas tanto a los usuarios como a los desarrolladores de productos IT

a) **Para los usuarios:** los CC proveen medios para comparar productos de varios desarrolladores – a través de la llamada Meta de Seguridad Además, un esquema es provisto por usuarios que pueden especificar sus necesidades de seguridad de tal forma que los desarrolladores pueden entender de manera clara y sin ambiguedades – por medio de una lista de verificación de los requerimientos de seguridad resultantes en un perfil de protección Al utilizar productos evaluados, un usuario incrementa su confiabilidad en la funcionalidad de seguridad de sus productos, porque una opinión experta independiente es dada sobre el producto de acuerdo a un conjunto de criterios internacionales y reconocidos

b) **Para los desarrolladores:** los CC proveen medios para mostrar al mundo que se tiene un producto adecuado y seguro ventajas competitivas del producto Los CC proveen una guía de la información requerida exactamente, interpretacion de

requerimientos de seguridad y un armazón que especifica qué es lo que el producto provee en términos de seguridad. La opinión independiente y experta del producto es dada sobre un criterio público predefinido que indica lo bien organizados que están tanto el producto como el diseño.

Identificación de los factores de riesgo

Los siguientes párrafos explican los factores que deben ser tomados en cuenta. Para cada factor, los diferentes niveles de riesgo están definidos, por lo que la diferencia entre dos niveles adyacentes en cada factor representan un incremento (o decremento) comparable aproximado en riesgo. Los factores están definidos así que son de manera general independientes – un cambio en un factor no implica un cambio en otro factor. Estas propiedades permiten numerar los niveles de riesgo y combinarlos en la mayoría de los casos utilizando una suma.

Algunas veces el riesgo no puede ser cuantificado de manera precisa por ser abstracto. El esquema descrito posteriormente captura la intuición y experiencia de los practicantes de la seguridad de cómputo y es preferible simplemente establecer estas consideraciones aparte debido a que no están hechas de manera precisa.

a) **Capacidad de procesamiento local:** algunos sistemas tiene terminales sólo de recepción, los usuarios de estas terminales no tienen manera de entrar directamente a los comandos del sistema. Estas terminales representan un nivel de riesgo más bajo que las terminales que permiten la emisión y recepción de información Al reemplazar una terminal interactiva con una función determinada por una terminal programable, una PC u otro dispositivo programable, introduciría un nivel muy alto de riesgo ya que el usuario puede programar su terminal para introducir los comandos por él Un usuario que tiene acceso a un sistema de terminal de función determinada pero por la vía de una computadora anfitrión programable se considera que tiene la misma capacidad de procesamiento local que uno que utilizara una computadora personal como terminal Los niveles de riesgo identificados para la capacidad de procesamiento local son

- Nivel 1 terminal de solo recepcion

- Nivel 2: terminal interactiva de función determinada
- Nivel 3: dispositivo programable (Acceso vía computadora personal o anfitrión programable)

b) **Ruta de comunicación:** la ruta de comunicación entre una terminal y el anfitrión puede afectar el riesgo del sistema. Una terminal que tiene una liga simple de recepción hacia su anfitrión vía red abastecedora y retransmisora posee menor riesgo que otra que se encuentra conectada vía liga dúplex abastecedora y retransmisora, ya que la ruta simple previene a los usuarios de las peticiones presentadas al sistema. Las terminales que están conectadas al anfitrión ya sea de forma directa, red de transporte largo de paquetes o a través de una LAN ofrecen un decremento en las posibilidades de penetración y mal uso sobre aquéllas que se encuentran conectadas sólo a través de una red abastecedora y retransmisora debido al incremento del ancho de banda y a la interacción más cercana anfitrión-terminal que permiten Los niveles de riesgo identificados para la ruta de comunicación son

- Nivel 1 abastecimiento/retransmisión, sólo receptor
- Nivel 2 abastecimiento/retransmisión, emisor/receptor
- Nivel 3: interactiva, vía conexión directa, LAN, red de transporte largo de paquetes

c) **Capacidad del usuario:** a pesar del procesamiento local disponible a un usuario o la ruta de comunicación por la cual él tiene acceso a un anfitrión, si este anfitrión está programado sólo para proveer salidas predefinidas a pesar de las entradas que el usuario presenta, es menos arriesgado que un sistema que responda a las transacciones del usuario El sistema que genera la cinta del indicador automático para una bolsa de acciones es menor en riesgo a las terminales que despliegan la cinta, como un sistema interactivo electrónico de banco es a una máquina automatizada de cobro Finalmente un sistema basado en la transacción es menos riesgoso para sus usuarios que un sistema que permita a sus usuarios capacidades de una completa programación Los niveles de riesgo identificados para la capacidad del usuario son

- Nivel 1: sólo salidas
- Nivel 2: procesamiento de transacción
- Nivel 3: programación completa

d) **Entorno de desarrollo y mantenimiento:** un sistema que ha sido desarrollado y es mantenido por individuos bajo un control de configuración cerrada (entorno cerrado) debería plantear un riesgo menor que uno que no es desarrollado y mantenido de esta manera (entorno abierto). Esta distinción ha sido propuesta en la teoría del plan de aplicación. Parece razonable, pero algunos ejemplos de sistemas desarrollados y mantenidos de acuerdo a la definición propuesta como "entorno cerrado" han sido identificados fuera de la comunidad inteligente. Por simplicidad se asume que los sistemas son desarrollados y mantenidos en un entorno abierto.

e) **Exposición de datos:** Un sistema que tiene una gran disparidad entre el permiso del usuario de menor rango y la clasificación de los datos, presenta un proceso que se encuentra en más riesgo que otro que tenga una disparidad menor, de manera que la teoría del plan de aplicación propone un esquema para numerar y clasificar el rango de riesgo, al cual se le llama exposición de datos para distinguirlo de otros factores de riesgo. Los niveles de permisos se definen como:

- Nivel 0: no aclarados
- Nivel 1: no aclarados, pero acceso autorizado a información delicada no clasificada
- Nivel 2: permiso confidencial
- Nivel 3: permiso secreta
- Nivel 4: ultrasecreto/investigación de fondo
- Nivel 5: ultrasecreto + investigación especial de fondo

- Nivel 6: ultrasecreto / investigación especial de fondo, con autorización para una división
- Nivel 7: ultrasecreto / investigación especial de fondo, con autorización para más de una división

Los niveles de clasificación se numeran de la siguiente manera

- Nivel 0. no clasificado
- Nivel 1: información delicada no clasificada
- Nivel 2: confidencial
- Nivel 3: secreta
- Nivel 4: secreta con una categoría
- Nivel 5: ultrasecreta sin categorías o secreta con dos o más categorías
- Nivel 6 ultrasecreta con una categoría
- Nivel 7 ultrasecreta con dos o más categorías

La exposición de datos es calculada como la diferencia entre el nivel del usuario menor de un sistema y el máximo nivel de los datos procesados por el sistema Esto coloca un valor entre 0 (todos los usuarios certifican para todos los datos) y 7 (el sistema procesa los datos ultrasecretos con dos o más categorías y algunos usuarios no están certificados)

Aplicación de los factores de riesgo

Para un sistema en particular cada uno de los factores de riesgo necesita ser evaluado de manera que determine el riesgo total Con menores excepciones, el riesgo del sistema es sencillamente la suma de los riesgos de los factores individuales de riesgo Basándose en el riesgo del sistema y la exposición de datos, los requerimientos de seguridad pueden determinarse En un sistema dado, las diferentes terminales pueden proveer diferentes funciones, ganados a diferentes

Lecturas recomendadas

[6]. II. Aspectos generales de la seguridad de la información

[11]. Common criteria version 2.1 / ISO IS 15408

[12]. Common Criteria

[13] Common Criteria

[14]. Common Criteria

[18]. Chapter 2. A theory of information warfare·
Information Security and information assurance

[20]. Determining Security Requirements for complex systems with the Orange Book

[35] Chapter 1. Business fundamentals of security.
Principles of security

[53] Seguridad informática, definiciones

[57]. Chapter 1 Introduction

[58] Chapter 1 Introduction
Concepts

[58] Chapter 2. The context for computer security
The changing context

CAPÍTULO 4.
SERVICIOS DE SEGURIDAD

Un servicio de seguridad es aquél que mejora la seguridad de un sistema de información y el flujo de la información de una organización. Los servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio.

4.2 Clasificación

Una clasificación muy utilizada de los servicios de seguridad es la siguiente:

1. Confidencialidad
2. Autenticación
3. Integridad
4. No repudio
5. Control de acceso
6. Disponibilidad

4.2.1 Confidencialidad

La privacía o la confidencialidad es la capacidad de asegurar que sólo las personas autorizadas tienen acceso a algo. La forma más común de proteger las cosas en el mundo físico es con el uso de candados y cerraduras. Muchos objetos tienen llaves como cajas de seguridad, casilleros, oficinas, automóvil, casa, etc. Generalmente las llaves de las oficinas, casas, etc. están en posesión de múltiples personas. En algunas circunstancias dos personas requerirán emplear su llave, al mismo tiempo, para activar una cerradura. Si se desea más seguridad, se emplearán múltiples cerraduras.

La confidencialidad es un aspecto primario y sumamente importante de la seguridad, significa mantener la información secreta para proteger los recursos y la información contra el descubrimiento intencional o accidental por personal no autorizado, es decir, es la protección de los datos transmitidos de cualquier ataque pasivo.

La confidencialidad es algo a lo que se enfrenta la gente y las organizaciones en su vida diaria, la privacía de la información personal debe estar asegurada. La confidencialidad es importante porque la consecuencia del descubrimiento no autorizado puede ser desastroso. No es difícil imaginar qué tan serio puede ser el daño si cualquier individuo conociera la información privada de uno o si una persona perteneciente a una cierta compañía fuera capaz de tener acceso a la información secreta de la compañía competidora, como los datos financieros y los planes de desarrollo de un producto.

El control de la seguridad depende de lo que se desea proteger, en qué medida puede afectar su confidencialidad y qué tan peligroso puede ser en manos desconocidas. Nosotros finalmente controlamos y no involucramos a la otra parte que no requiere de autorización o permiso para el cambio Por ejemplo, si somos propietarios de una casa, podemos cambiar las cerraduras y las llaves tantas veces como nos parezca conveniente, pues esta acción no podrá tener lugar si se estuviera en condición de inquilino, en donde no se puede cambiar las chapas sin autorización del propietario.

La posesión de una llave permite la autenticación y la autorización, y por consiguiente la confidencialidad. Por ejemplo, si alguien robó nuestras llaves, ellos tienen acceso a todas las cosas que las llaves abren y nuestra "confidencialidad" será infringida. El ladrón tendrá acceso, a no ser que cambiemos las cerraduras. En el mundo físico se puede advertir la pérdida de las llaves y nos pone en alerta para tomar medidas necesarias tal como cambiar las cerraduras, pero esto no ocurre en el mundo de las redes, es posible que alguien tome las "llaves" sin nuestro conocimiento, simplemente haciendo una copia de ellas A causa de la conectividad de una red, si alguien puede conseguir el acceso a nuestras claves, es posible que pueda copiarlas

Existen personas que desean tener acceso a la información no autorizada y a los recursos por varias razones tales como adquirir ventajas competitivas, publicidad o revancha entre otras

Los servicios de confidencialidad proveen protección de los recursos y de la información en términos del almacenamiento y la información, para asegurar que

- Nadie pueda leer, copiar, descubrir o modificar la información sin autorización

- Nadie pueda interceptar las comunicaciones o los mensajes entre entidades.

Estos dos aspectos de la confidencialidad son llamados **confidencialidad de contenido** y **confidencialidad de flujo del mensaje**.

a) **Servicios de confidencialidad de contenido:** estos servicios son provistos sobre un principio fundamental por recurso utilizando una técnica de cifrado para prevenir el descubrimiento no autorizado del contenido de un recurso de la red como un mensaje, un archivo o un registro de datos. Varios niveles de protección pueden identificarse. El servicio más amplio protege todos los datos del usuario transmitidos entre dos usuarios en un cierto período de tiempo. Las formas más estrechas de este servicio pueden definirse, incluyendo la protección de un solo mensaje o campos específicos dentro de un mensaje. Estos refinamientos son menos útiles que el amplio acercamiento y pueden ser más complejos y caros de implementar

b) **Servicios de confidencialidad de flujo del mensaje:** dichos servicios son provistos a través del cifrado y una técnica de envoltura para permitir al creador del mensaje ocultar el flujo de un mensaje lo cual procura que la información sea prevenida de una observación Este servicio protege a los flujos de mensaje contra la amenaza del análisis de tráfico. Esto es, un atacante no debe ser capaz de observar la fuente y el destino, la frecuencia, la longitud u otras características del tráfico en un recurso de comunicación

La criptografía es utilizada para proveer los servicios de confidencialidad De manera más sofisticada los métodos de cifrado basados en la criptografía son los mecanismos para asegurar que el descubrimiento no autorizado de la información sea computacionalmente imposible

4.2.2 Autenticación

La autenticación es uno de los servicios más fáciles de comprender Es simplemente "verificar" la identidad En la vida diaria generalmente la autenticación se hace de manera informal y en ocasiones, sin pensarlo Todos inconscientemente autenticamos gente, compañías y ubicaciones todo el tiempo

Por ejemplo, cuando uno va a casa, autentica su hogar comparándolo con su memoria. Si se visita el hogar de un amigo, se verifica que está en la ubicación correcta comprobando la dirección dada por la calle y el número sobre la casa. Cuando se entra a una sucursal de un banco, lo autentica por su logotipo y colores.

La forma más popular de autenticación individual es una firma. Una firma se usa para autenticar al titular de la cuenta en el banco, para comprometer a una persona para alojarse en un hotel y para autenticar al titular de la tarjeta de crédito al realizar alguna compra. La firma se usa no solamente para autenticar la identidad, sino también para dar autorización.

El servicio de autenticación trata de asegurar que una comunicación sea auténtica En el caso de un solo mensaje como una señal de alarma o una advertencia, la función del servicio de autenticación asegura al receptor que el mensaje proviene de la fuente que éste espera que provenga.

En el caso de una interacción en curso como la conexión de una terminal a un anfitrión, dos aspectos son envueltos

- Al momento en el que la conexión se inicia, el servicio verifica que las dos entidades sean auténticas (esto significa que cada entidad es en realidad la que se supone que debe ser)

- El servicio debe asegurar que la conexión no pueda ser interferida por un tercer individuo que pueda enmascararse como una de las dos entidades legítimas con el único propósito de realizar una transmisión o recepción no autorizada.

La autenticación es utilizada para proporcionar una prueba al sistema de que en realidad se es la entidad que se pretende ser El sistema verifica la información que alguien provee contra la información que el sistema sabe sobre esa persona

La autenticación es realizada principalmente a través de

a) **Algo que se sabe:** una contraseña o un número personal de identificación, es algo que se sabe Cuando se le provee al sistema, éste lo verifica contra la copia que esta almacenada en el sistema para determinar si la autenticación es exitosa o no

b) **Algo que se tiene:** una tarjeta o un pasaporte es un ejemplo de algo que se tiene, lo cual es utilizado por el sistema para verificar la identidad

c) **Algo que se es:** la voz, la retina, la imagen del rostro o una huella digital pueden identificar de quién se trata y pueden ser utilizadas en el proceso de autenticación

4.2.3 Integridad

En la integridad de los datos algo de lo más utilizado son los sellos, especialmente en el área comercial. Por ejemplo, los funcionarios de aduana en un país registran una caja de la mercancía, para asegurar que contiene lo que dice en la lista, entonces la sellan Si los funcionarios de la aduana destino ven que el sello está todavía intacto, ellos saben que nadie ha alterado la carga en el tránsito de lo contrario, saben que su integridad ha sido violada.

En el mundo físico generalmente la verificación de la integridad de los "datos" se ha hecho en forma visual. La ausencia de señales de alteración significa que los datos no han sido cambiados. Cuando se firma un contrato, cualquier cambio hecho en la página impresa debe ser iniciado por ambas partes, para asegurar que ellos son una parte del acuerdo y no una señal de alteración que ocurrió después de la firma

El poner algún tipo de sello como en los ejemplos anteriores, no sería tan fácil de realizar en un sistema de información, pues la duplicación de un dato es fácil y cada copia de los datos está virtualmente en todos lados Pueden alterarse fácilmente los datos cuando se almacenan en una computadora y muchas personas podrían potencialmente ganar acceso, haciendo la integridad de datos mucho más difícil en el mundo de la red Para asegurar la integridad de datos, se necesita de algún modo crear un sello que no pueda alterarse y pueda ser usado para verificar que los datos no han sido cambiados

La integridad de datos provee controles que aseguran que el contenido de los datos no haya sido modificado, y que la secuencia de los datos se mantenga durante la transmisión Al proporcionar la integridad de los datos se evita la inserción, borrado o cualquier otra modificación no autorizada Los usuarios no autorizados son o no capaces de leer los datos pero la protección debe existir para prevenir que los usuarios no autorizados añadan, borren o modifique cualquier parte de los

datos. Si la integridad no existe, cualquier persona puede manipular los datos según su conveniencia.

Puede aplicarse a una secuencia de mensajes, a un solo mensaje o campos seleccionados dentro de un mensaje. La aproximación más útil y directa es la protección total de la secuencia.

Un servicio de conexión orientada de la integridad que trata con una secuencia de mensajes, asegura que los mensajes se reciban como fueron enviados sin duplicación, inserción, modificación, ni denegación de servicio.

Se puede hacer una distinción entre el servicio con o sin recuperación, porque el servicio de integridad se relaciona con los ataques activos, se refiere a la detección más que a la prevención. Si una violación a la integridad es detectada, entonces el sistema reporta esta violación y otra parte del software o la intervención humana es requerida para recuperarse de la violación. De manera alternativa, hay mecanismos disponibles para reponerse de una pérdida de integridad de datos, la incorporación de mecanismos de recuperación automáticos, es la alternativa más efectiva.

Existen dos tipos de servicios **servicio de integridad del contenido** y **servicios de integridad de la secuencia del mensaje**

a) **Servicios de integridad del contenido:** éstos proveen pruebas de que el contenido no ha sido alterado o modificado por inserción o supresión

b) **Servicios de integridad de la secuencia del mensaje:** proporcionan pruebas de que el orden de una secuencia de mensajes ha sido mantenida durante su transmisión. Este servicio es provisto por el receptor para proteger los mensajes contra las amenazas de secuencia del mensaje como la réplica y el reordenamiento del mensaje

Los servicios de integridad de los datos pueden ofrecerse a través de varios mecanismos de seguridad

- **Código de detección de modificación:** es una suma de comprobación de los datos generada utilizando un algoritmo criptográfico. Es decir, a los datos a enviar se les aplica un cierto algoritmo que genera una secuencia de bits y ésta se adiciona a dichos datos, de manera que al llegar a su

destino se efectúa la prueba de comprobación y si la secuencia de bits generada es la misma, entonces se sabe que los datos llegaron sin modificación alguna.

- **Código de autenticación del mensaje:** es una suma de comprobación cifrada de los datos generada con base en la criptografía. Es decir, a los datos a enviar se les aumenta una secuencia de bits que resulta de aplicarles un algoritmo. Al llegar a su destino debe efectuarse una prueba de comprobación y si la secuencia de bits generada es la misma, entonces se sabe que los datos provienen de quien se supone los envió sin sufrir modificación alguna.

- **Firma digital:** es una pieza de información asociada con los datos que únicamente puede ser creada por el firmante y puede ser verificada por cualquier persona. Esto es, se cifra la unidad de datos junto con alguna componente secreta del firmante, y se obtiene un valor de control ligado al resultado cifrado.

- **Número de secuencia del mensaje:** identifica la posición del mensaje en la secuencia Este número es transferido con el mensaje de manera normal o de manera cifrada Esto es, cuando un mensaje es dividido en varios paquetes para su envío, al receptor le deberá llegar la misma cantidad de paquetes y en la misma secuencia en que fueron enviados Para ello, será necesario agregar, a cada paquete, una secuencia de bits la cual contendrá el número de secuencia del mensaje y dicho número podrá ser enviado como texto claro o cifrado El receptor deberá comprobar, al momento de descifrar, que la secuencia de bits agregada al mensaje original efectivamente coincide con el paquete y el orden en que fue enviado Garantizando de esta manera que el mensaje llegó a su destino sin modificación alguna y que además ningún mensaje fue adicionado o sustraído por un ente ajeno al emisor.

4.2.4 No repudio

El no repudio previene a los emisores o a los receptores de negar un mensaje transmitido Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el

presunto receptor. Esto es, el no repudio ofrece protección a un usuario frente a otro usuario que niegue, posteriormente, haber realizado cierta comunicación o recepción de un mensaje enviado. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa.

El no repudio se aplica al problema de la denegación falsa de la información que se recibe de otros o de la que uno ha enviado a otros. Los servicios de no repudio suministran pruebas que pueden ser demostradas a una tercera entidad. Los siguientes servicios son los que pueden ser proporcionados:

a) **No repudio de origen:** provee pruebas del origen de los datos, con ello se previene a la entidad de origen de cualquier denegación falsa al suministrar los datos, es decir, el no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje

b) **No repudio de envío:** provee pruebas del envío de los datos, por lo tanto previene a quien recibe los datos de cualquier denegación falsa al recibir los datos

c) **No repudio de presentación**: provee pruebas de presentación de los datos, con ello protege contra cualquier intento falso de negar que los datos fueron presentados para el envío.

d) **No repudio de transporte:** provee pruebas del transporte de los datos con lo que protege contra cualquier intento de negar que los datos fueron transportados.

e) **No repudio de recepción:** provee pruebas de recepción de los datos con esto se protege al emisor de que el receptor niegue haber recibido el mensaje.

Para proporcionar los servicios de no repudio, las firmas digitales son utilizadas porque éstas tienen la propiedad de que pueden ser creadas por los firmantes y verificadas por otros.

4.2.5 Control de acceso

El acceso a un medio de información puede ser controlado ya sea a través de un dispositivo pasivo tal como una puerta cerrada o a través de un dispositivo activo como lo puede ser un monitor. Un monitor de control de acceso, determina qué usuario está autorizado para usar un recurso de manera requerida. Antes de otorgar el acceso, el monitor puede validar la identidad del usuario. En algunos casos, los procesos para determinar la autorización está combinada con la autenticación.

En el contexto de seguridad de la red, el control de acceso es la habilidad para limitar y controlar el acceso a los sistemas anfitriones y las aplicaciones mediante los puentes de comunicación. Para lograr este control, cada entidad que trata de ganar acceso, debe identificarse primero o autenticarse, así que los derechos de acceso pueden ser adaptados de manera individual.

Un control de acceso se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que entonces le sea permitido el acceso.

Los componentes básicos de un mecanismo de control de acceso son las entidades de red, los recursos de la red y los derechos de acceso. Los derechos de acceso describen los privilegios de la entidad o los permisos bajo cuáles condiciones las entidades pueden tener acceso a un recurso de la red y cómo estas entidades son permitidas para tener acceso a un recurso de la red

Ejemplos de los privilegios o permisos de una entidad:

- Creación o destrucción
- Lectura o escritura
- Adición, supresión o modificación del contenido
- Exportación o importación
- Ejecución

Los privilegios o permisos pueden ser revocados y/o cambiados por el administrador autorizado de la red o del sistema en cuestión.

Los usuarios, los recursos y la información pueden ser clasificados al asignarse diferentes niveles de seguridad, cualquier usuario permitido recibe autorización para un cierto nivel, por lo que puede tener acceso únicamente a la información que se encuentra clasificada en el nivel autorizado y niveles inferiores pero nunca podrá tener acceso a los niveles superiores al que está autorizado.

El control de acceso puede ejecutarse de acuerdo a los niveles de seguridad y en recursos de la red particulares, pueden ejecutarse mediante la administración de la red o por una entidad individual de acuerdo a las políticas de control de acceso.

Una lista de control de acceso (LCA) puede ser empleada para la protección de los recursos individuales Una LCA es una lista de permisos que determinan quién puede tener acceso a los recursos individuales de la red y qué puede hacerse con los recursos, esta lista deja que el propietario de un recurso permita o deniegue el acceso a los recursos a una entidad o a un grupo de entidades

4.2.6 Disponibilidad

La disponibilidad se cumple si las personas autorizadas pueden acceder a la información deseada cuando lo requieran y tantas veces como sea necesario

El disponer de la información después del momento necesario puede equivaler a la no disponibilidad Es importante aclarar que la disponibilidad se refiere únicamente al tiempo para obtener la información y no importa si la información es correcta o no.

Otro caso grave es la no disponibilidad absoluta, por haberse producido algún desastre. En ese caso a medida que pasa el tiempo el impacto será mayor, hasta llegar a suponer la no continuidad de la entidad, como ha pasado en muchos de los casos producidos ya que las incidencias son frecuentes. En relación con ello deben existir soluciones alternativas, basadas en medios propios o contratados, copias actualizadas de la información crítica y de programas en un lugar diferente,

y un verdadero plan de continuidad[5] que permita restablecer las operaciones en un tiempo inferior o igual al prefijado.

Una variedad de ataques puede resultar por la pérdida o reducción en la disponibilidad. Algunos de estos ataques son favorables para las contramedidas automatizadas, tales como la autenticación y cifrado, mientras que otras requieren algunas clases de acciones físicas para prevenir o recobrarse de la pérdida de disponibilidad de los elementos de un sistema distribuido.

[5] Plan de continuidad es un conjunto de pasos a seguir para que una entidad tenga disponibilidad continua cuando exista algún imprevisto al momento de acceder a la información. Para elaborar un plan de continuidad, los usuarios habrán determinado previamente qué aplicaciones son las más críticas y el impacto en sus áreas, y a un nivel corporativo, idealmente por parte de un comité, se habrán determinado las prioridades.

Lecturas recomendadas

[8]. Autenticación

[18] Chapter 12. How to tell a fake

[18]. Chapter 13. Monitors and gatekeepers:
Access controls
Access control monitors

[31]. Integridad

[35]. Chapter 1. Business fundamentals of security
1.2 Identification and Authentication
1.3 Access control
1.4 Confidentiality
1.5 Data integrity
1 6 Non-repudiation

[48] Privacidad y confidencialidad

[54] Servicios de seguridad

[55] Servicios de seguridad

[57] Chapter 1. Introduction
1 3 Security services

[58] Chapter 1 Introduction.
Framework for technical safeguards

CAPÍTULO 5.
CRIPTOGRAFÍA

5.1 Principios de criptografía

El uso de las redes de computadoras, requiere la transferencia de mensajes de datos a través de medios que pueden estar a salvo de personas malintencionadas que desean obtener o alterar información, a la cual no tienen acceso. Por lo tanto, mensajes y datos necesitan ser protegidos, de tal forma que solamente las personas y procesos autorizados consigan utilizarlos, evitando la alteración fraudulenta de la información, la destrucción de la misma o la creación de información falsa.

Dicha información necesita protección contra diversos ataques en los servicios como la confidencialidad, integridad, autenticación, no repudio y el control de acceso. La protección de la información se puede llevar a cabo por medio de la criptografía. La criptografía es una rama de la **criptología** – un campo que trata con las comunicaciones seguras, la criptología es un arte tan antiguo como lo fue la propia escritura, permaneció durante muchos siglos relacionada muy directamente en el ámbito militar y diplomático, dado que éstos eran los únicos que en principio tenían auténtica necesidad de ella – , la otra rama de la criptología es el **criptoanálisis** éste se refiere a la ruptura o derrota de la criptografía, es decir, es el proceso que intenta descubrir el texto o la clave, la estrategia utilizada por el criptoanalista depende de la naturaleza del esquema de cifrado y de la información que tenga disponible Por lo tanto, la criptografía y el criptoanálisis siempre están unidos.

La **criptografía**[6] es el arte y la ciencia de transformar la información para asegurar su secreto, su autenticidad o ambas y prevenir a los usuarios de acciones no autorizadas o ilegales en contra de la información, los recursos de red y los servicios, es decir, es la encargada del diseño de procedimientos, controlados por una clave, para cifrar o enmascarar una determinada información de carácter confidencial. A través de la criptografía la información puede ser protegida contra el acceso no autorizado, la fusión, la modificación y la inserción, también puede ser usada para prevenir el acceso y uso no autorizado de los recursos de la red y para prevenir a los usuarios de la negación de los servicios a los que están permitidos La criptografía es la metodología para proveer la seguridad de la red, por ello, trata con todos los aspectos de la seguridad en un ambiente seguro de red, incluyendo la

[6] Criptografía (kryptos – escondido, oculto, graphé – grafía, escritura) el arte o ciencia de escribir en cifra o en código, de tal forma que permita que sólo el destinatario lo descifre y comprenda

identificación de entidades y autenticación, el control de acceso a los recursos, la confidencialidad del mensaje, la integridad del mensaje y el no repudio.

La criptografía está íntimamente relacionada con la seguridad y asume un papel cada vez más importante debido a la gran cantidad de información que las organizaciones actualmente necesitan generar, procesar, almacenar y/o distribuir de manera segura (confidencial e íntegra); proceso en el que es de gran importancia el uso de las redes de computadoras. Éstas transportan informaciones cada vez más valiosas y vitales para las más diversas organizaciones. La seguridad de los datos, más que nunca, se está tornando en un problema crítico.

Por miles de años la criptografía ha sido utilizada para secretos militares y diplomáticos. Actualmente la criptografía es utilizada entre otras muchas actividades para:

- Autenticar transacciones comerciales y bancarias.
- Autenticar transacciones entre negocios o entre gobiernos y negocios.
- Proteger la integridad de las transferencias electrónicas de fondos
- Proteger el secreto de las comunicaciones personales, militares y comerciales.
- Proveer el secreto y la integridad de las transacciones por Internet.
- Proteger la integridad del software y de las bases de datos
- Autenticar la identidad de los usuarios de la red y las entidades

La criptografía intenta garantizar:

- **Discreción:** solamente los usuarios autorizados tienen acceso a la información
- **Integridad de la información:** garantía ofrecida a los usuarios de que la información original, no será alterada, ni intencional ni accidentalmente

- **Autenticación de usuario:** es un proceso que permite al sistema verificar si el usuario que pretende acceder o hacer uso del sistema es quien dice ser.

- **Autenticación de remitente:** es el proceso que permite a un usuario certificar que el mensaje recibido fue de hecho enviado por el remitente.

- **Autenticación del destinatario:** es el proceso que permite garantizar que la información enviada sólo podrá ser leída por el destinatario.

- **Autenticación de actualidad:** consiste en probar que el mensaje es actual, y que no se trata de un mensaje antiguo reenviado.

En la criptografía, los mensajes originales se conocen como **texto en claro o texto fuente** y a la operación con la cual los símbolos básicos se transponen o sustituyen para transformar los datos, se denomina **puesta en cifra**. El resultado (mensaje cifrado) de la puesta en cifra se conoce como **texto cifrado** o **criptograma**, que luego es transmitido por un canal público A este conjunto de elementos se le denomina **criptosistema o sistema criptográfico.**

En el proceso de transmisión, el mensaje cifrado (criptograma) puede sufrir el ataque de un criptoanalista, el cual intentará realizar la labor de descriptado [7] del mensaje original

En la figura 5 1 se presenta el esquema de un proceso criptográfico (cifrar y descifrar). Siguiendo el flujo (de izquierda a derecha) del mensaje original, se tiene que el texto en claro pasa al proceso de puesta en cifra, dando como resultado un criptograma Después se envía el criptograma a través de un canal público, durante el trayecto puede presentarse el ataque de un criptoanalista, quien intentará el descriptado del criptograma. Sin embargo, a diferencia del receptor, dicho intruso no conoce la clave y por lo tanto, se le dificultará obtener el mensaje original

[7] Intentar a partir del criptograma y sin conocimiento de la clave, recuperar el mensaje original

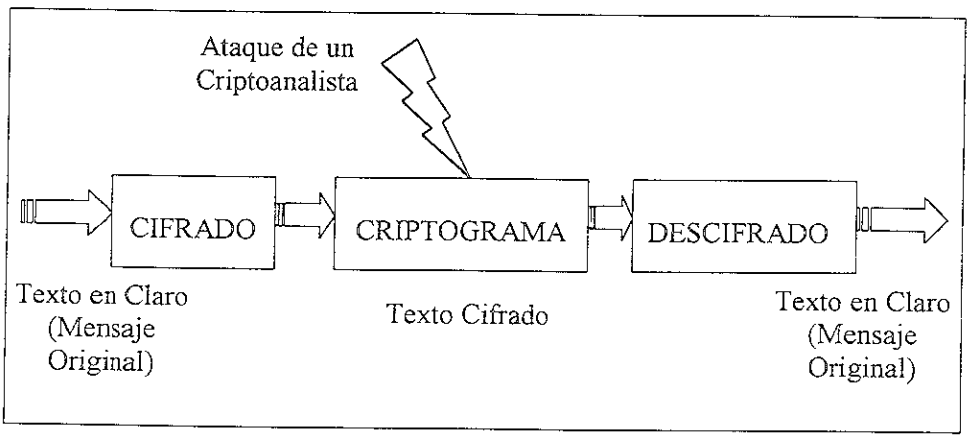


Figura 5.1. Proceso criptográfico

Los sistemas criptográficos se clasifican de acuerdo a

1. **El tipo de operaciones utilizadas para transformar el texto en claro en texto cifrado:** todos los algoritmos de cifrado se basan en dos principios generales:

   a) **Sustitución:** en el cual cada elemento del texto (bit, letra, grupo de bits o letras) es cambiado por otro elemento. La sustitución consiste en determinar una correspondencia entre las letras del alfabeto en que está escrito el mensaje original y los elementos de otro conjunto, el cual puede ser el mismo o diferente alfabeto. De tal manera, cada letra del mensaje original se sustituye por su símbolo correspondiente en la elaboración del criptograma. El receptor, que conoce asimismo la correspondencia definida, recupera el mensaje original sustituyendo cada símbolo del criptograma por el símbolo correspondiente del alfabeto original.

      i) **Sustitución monoalfabética**

      El procedimiento de sustitución más antiguo que se conoce es el **cifrado de César**, en él la letra A se representa por la letra D, B por E, C por F, ..., así para cada letra del abecedario hasta sustituir Z por C (ver tabla 5.1). Una generalización sencilla de este método permite que el alfabeto cifrado se desplace *k* letras, en lugar de 3, por

este caso, k se convierte en una clave para el método general de alfabetos desplazados en forma circular.

Texto en claro:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Texto cifrado:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tabla 5.1. Cifrado de César

Un mensaje cifrado con este método puede ser sujeto de un exitoso criptoanálisis analizando la frecuencia de cada carácter del texto cifrado y comparando estas frecuencias con aquéllas que normalmente aparecen en un determinado idioma. Las vocales tienen mayor frecuencia que las consonantes y algunos caracteres poseen frecuencia muy baja con relación a las demás

Una mejora de este método consiste en relacionar cada uno de los símbolos del texto en claro con alguna otra letra como se aprecia en la tabla 5.2.

Texto en claro:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Texto cifrado	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Tabla 5.2. Sustitución monoalfabética

A este sistema se le conoce como sustitución monoalfabética, en el cual la clave se constituye por una cadena de 26 letras, correspondiente al alfabeto completo Un ejemplo, utilizando una sustitución monoalfabética, se muestra a continuación:

Utilizando la tabla 5.2, cifrar la palabra "seguridad"

Texto en claro	s	e	g	u	r	i	d	a	d
Texto cifrado	L	T	U	X	K	O	R	Q	R

Aparentemente, este sistema puede ser seguro porque aun cuando el criptoanalista conociera el sistema general (sustitución letra por letra), tendría que realizar las posibles combinaciones de claves

(26!) para descriptar el mensaje. No es factible probar todas las claves como en el cifrado de César.

En una sustitución monoalfabética, cada letra del texto original es cambiada por otra de acuerdo con una tabla y con su posición del texto. La sustitución de César es un ejemplo de sustitución monoalfabética, que consiste en cambiar cada letra por otra que está en orden alfabético 3 letras adelante.

Se pueden usar otros valores en vez de 3, lo que constituye una clave para cifrar. Existen apenas 26 claves, pero este método basta para proteger textos con pequeño grado de confidencialidad. Se tiene una clave que dice cuál de las tablas será usada para cada letra del texto original. Por lo tanto, cuanto mayor sea la clave, más seguro es el método. Entretanto, es suficiente descubrir el tamaño de la clave *k* y analizar bloques de *k* caracteres del texto, verificando la frecuencia de repetición de los caracteres.

ii) Sustitución por desplazamiento

En una sustitución por desplazamiento una clave indica cuántas posiciones alfabéticas se deben avanzar para sustituir cada letra (ver tabla 5 3) Sería diferente a la sustitución de César, las letras no son cambiadas siempre por una letra cada *n* posiciones del alfabeto Es decir, el desplazamiento es variable, mientras que en el método César es fijo.

Alfabeto	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Posición	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Tabla 5.3. Sustitución por desplazamiento

Hay que resaltar que cada dos dígitos de la clave corresponde al desplazamiento hacia delante que se va a realizar con respecto a la letra del texto cifrado Se toman los dígitos de dos en dos debido a que el alfabeto que se utiliza es de 26 letras, por lo tanto, se necesitan dos dígitos para formar el desplazamiento

A continuación se da un ejemplo:

Utilizando la tabla 5.3, descifrar el siguiente texto cifrado ACFOOJDAAIA, donde la clave es 02150301050503170004 00.

El texto en claro, se obtiene de la siguiente manera.

Trabajando con el texto cifrado, se toma la primera letra *A* – de izquierda a derecha – y se toman los primeros dos dígitos de la clave 02 – también de izquierda a derecha. En la tabla 5.3, se verifica la posición que toma la letra *A* que es 01 y se suma (se desplaza hacia delante) el valor de la clave 02 dando como resultado 03. Después se verifica en la misma tabla la letra que corresponde al resultado, en este caso es *C*, de esta manera se ha encontrado la primera letra que corresponde al texto en claro. Se tiene que realizar el mismo procedimiento para obtener cada letra del texto original En la tabla 5.4 se observa el texto original

Texto en claro:	c	r	i	p	t	o	g	r	a	M	a
Texto cifrado:	A	C	F	O	O	J	D	A	A	I	A
Clave	02	15	03	01	05	05	03	17	00	04	00

Tabla 5.4. Texto original

iii) Sustitución polialfabética

Otro sistema de sustitución que se conoce es el polialfabético, que es el resultado de introducir múltiples alfabetos de cifrado que se utilizan en rotación de acuerdo con un criterio o clave, su objetivo es adecuar las frecuencias del texto cifrado de tal forma que las letras con mayor frecuencia de aparición no sobresalen tan claramente

Dentro de este sistema se tiene el **cifrado Vigenère**, que consiste de una matriz cuadrada que contiene 26 alfabetos de César El primer renglón llamado renglón *A* es ABCDEFGH XYZ El siguiente renglón, llamado renglon *B* es BCDEFGHI YZA Finalmente el último renglón llamado renglon *Z* es ZABCDEFG WXY

De forma similar al cifrado monoalfabético, este cifrado también tiene una clave, pero ya no es una cadena de 26 caracteres diferentes sino una palabra o frase corta y fácil de recordar.

A continuación se describe un ejemplo del cifrado Vigenère:

Clave a utilizar: mundo

Texto en claro: computadora descompuesta

Para obtener el criptograma del texto claro, primero hay que poner la clave, en forma repetida, encima del texto en claro.

Así:

m	u	n	d	o	m	u	n	d	o	m	u	n	d	o	m	u	n	d	o	m	u	n
c	o	m	p	u	t	a	d	o	r	a	d	e	s	c	o	m	p	u	e	s	t	a

La palabra *mundo* que se encuentra sobre el texto en claro indica el renglón que se debe utilizar para la puesta en clave. Es decir, la letra *c* – primera letra del texto "computadora descompuesta" – se pone en clave usando el alfabeto de César del renglón *m*, la *o* – segunda letra del texto "computadora descompuesta" – usando el renglón *u*, la letra *m* – tercera letra del texto "computadora descompuesta" – usando el renglón *n*, así sucesivamente hasta terminar con las letras del mensaje original – "computadora descompuesta".

El criptograma se obtiene de la siguiente manera

Se toma la primera letra del texto claro *c* y se observa que le corresponde la letra *m* de la clave. La letra cifrada es la letra que resulta de intersectar el renglón *m* con la columna *c*. De acuerdo con la tabla 5.5, la letra resultante es *o*

Para la segunda letra del texto claro *o*, se observa que le corresponde la letra *u* de la clave. La letra cifrada es la letra que

resulta de intersectar el renglón *u* con la columna *o*. De acuerdo con la tabla 5.5, la letra resultante es *i*.

Se realiza el mismo procedimiento para cada una de las letras del texto en claro.

Realizando lo anterior y basándose en la tabla 5.5, se obtiene el siguiente criptograma:

oizsifuqrfmxrvqagcxsemn

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Tabla 5.5. Matriz cuadrada

A continuación se describe el descifrado del ejemplo anterior

Clave utilizada. mundo

Texto cifrado: oizsifuqrfmxrvqagcxsenn

Para obtener el texto en claro, primero hay que poner la clave, en forma repetida, encima del texto cifrado.

Así:

m	u	n	d	o	m	u	n	d	o	m	u	n	d	o	m	u	n	d	o	m	u	n
o	i	z	s	i	f	u	q	r	f	m	x	r	v	q	a	g	c	x	s	e	n	n

La palabra *mundo* que se encuentra sobre el texto cifrado indica el renglón que se debe utilizar para descifrar Es decir, se toma el renglón de la letra *m* – primera letra de la clave – y en ese mismo renglón se busca la letra *o* – primera letra del texto cifrado – una vez encontrada ésta, la letra del texto en claro será la correspondiente a esa columna De acuerdo con la tabla 5.5, la letra resultante es *c*

Para la siguiente letra del criptograma, nuevamente se toma el renglón correspondiente a la segunda letra de la clave *u* y en ese mismo renglón se busca la letra *i* – segunda letra del texto cifrado – una vez encontrada ésta, la letra del texto en claro será la correspondiente a esa columna De acuerdo con la tabla 5 5, la letra resultante es *o*

Se realiza el mismo procedimiento para cada una de las letras del texto cifrado.

Realizando lo anterior y basándose en la tabla 5 5, se obtiene el texto en claro original

computadora descompuesta

Un cifrado polialfabético puede ser muy eficaz si se usan cifrados monoalfabéticos arbitrarios para los renglones, en lugar de restringirlos al cifrado de César, aunque tiene el inconveniente de que

la matriz de 26x26 también se convierte en parte de la clave y se deberá memorizar o escribir.

Otra de las formas de dar mayor complejidad al cifrado es utilizar una clave que sea de mayor longitud que la del texto en claro El **cifrado Vernam** representa el caso límite del cifrado de Vigenère pues emplea un alfabeto binario y escoge como clave una cadena de bits aleatoria. Después, se convierte el texto en claro en una cadena de bits (la cual puede ser su representación en ASCII). Después, se aplica un OR-exclusivo[8] , bit por bit, con estas 2 cadenas; de este modo, el texto cifrado no puede desbaratarse puesto que todos los posibles textos en claro son candidatos, igualmente probables y no le proporcionará ninguna información al criptoanalista. Para recuperar el mensaje original se realiza la operación OR-exclusivo de la secuencia aleatoria – clave – con el criptograma

Enseguida se muestra cómo quedaría cifrado el siguiente mensaje: "VERNAM", utilizando el cifrado Vernam

Primero es necesario encontrar el equivalente de cada letra en código ASCII [9] y anotar su equivalente en bits [10]

V = 86 = 1010110
E = 69 = 1000101
R = 82 = 1010010
N = 78 = 1001110
A = 65 = 1000001
M = 77 = 1001101

Después se propone una cadena arbitraria, de la misma cantidad de bits que el texto claro, la cual va a ser la clave Quedando de la siguiente manera

[8] Ver tabla XOR en el Apéndice A
[9] Ver tabla del código ASCII en el Apéndice A
[10] Se puede establecer cualquier otra equivalencia de la letra en bits, es decir no necesariamente es su equivalencia en ASCII

Texto claro: 10101101000101101001010011101000001100l101
Clave: 11111110101001111000100001011010101010101010

A continuación para obtener el texto cifrado se realiza la operación OR-exclusivo, bit a bit, entre el texto claro y la clave.

Texto claro: 10101101000101101001010011101000001100l101
Clave: 11111110101001111000100001011010101010101010
Texto cifrado: 01010011101100010001110010110010100l100111

Para obtener el texto claro, se debe realizar la operación OR-exclusivo, bit a bit, entre la clave y el texto cifrado. Después se obtiene su equivalencia en código ASCII de cada letra

Las ventajas que tiene este método, conocido como clave de una sola vez, son las siguientes:

- Debido a que la clave es arbitraria y de la misma longitud del texto en claro, cuando no se tiene la clave y se desea obtenerla será necesario probar con cada una de las combinaciones posibles que nos permita la longitud de la clave. Es decir, que se tendrían que probar 2^n claves para poder descifrar el criptograma.

- No sólo se puede utilizar el código ASCII, sino que se puede establecer cualquier otro código de tal manera que cada letra no siempre tendrá la misma equivalencia que la del código ASCII

- Con los puntos anteriores se puede decir que este cifrado es más completo y complejo en comparación a los cifrados descritos anteriormente

b) **Transposición:** los elementos del texto son reacomodados La transposición consiste en intercambiar los símbolos del mensaje original, de tal forma que el criptograma tenga los mismos elementos que el mensaje original pero que sea difícil de comprender A diferencia de los métodos de sustitución, que reemplazan los elementos del texto en claro por símbolos, los métodos de

transposición reordenan las letras. Se cambia la posición de los caracteres en un mensaje. Por ejemplo, se puede reescribir un texto corrido o por columnas. También, se puede definir el tamaño para un vector de cambios y un orden en el que los cambios son hechos. Se puede usar una clave para ello.

El ejemplo más simple de la transposición – transposición sencilla – es escribir el texto original al revés. Para el caso del texto original: SECRETO PERFECTO, el texto cifrado quedaría: OTCEFREP OTERCES.

Ejemplo: en un vector de tamaño 6 se puede cambiar el primer carácter por el tercero, el segundo por el quinto y el cuarto por el sexto. La clave es una palabra o frase que no contiene una letra repetida.

La finalidad de la clave es la de enumerar las columnas, siendo la columna uno la que queda bajo la letra de la clave más cerca al inicio del alfabeto y así sucesivamente.

El texto en claro se escribe horizontalmente en renglones y el texto cifrado, se lee por columnas comenzando en la columna cuya letra clave tiene el valor inferior Es decir, se intercala entre renglones y éstos se leen en forma secuencial

Para el caso de dos renglones, el mensaje: SECRETO PERFECTO.

Quedaría de la siguiente forma

S C E O E F C O
E R T P R E T

Puesto en forma secuencial

S C E O E F C O E R T P R E T

Si se desea complicar más, el método se puede aplicar nuevamente.

S E E C E T R T
C O F O R P E

Puesto en forma secuencial:

S E E C E T R T C O F O R P E

El requerimiento principal es que la información no se pierde, lo cual indica que las operaciones son reversibles.

2. **El número de claves utilizadas:** si el emisor y el receptor usan la misma clave, el sistema es llamado cifrado simétrico, de clave simple, de clave secreta o convencional. Si el emisor y el receptor utilizan diferentes claves, el sistema es llamado cifrado asimétrico, de doble clave o de clave pública

3. **La manera en la que el texto es procesado:** si el texto es procesado mediante un cifrador de bloque que opera sobre grupos o bloques de bits u octetos, generalmente 64 bits u 8 octetos, entonces un bloque de código procesa la entrada de un bloque de elementos a la vez, produciendo un bloque de salida por cada bloque de entrada. Esto se aprecia en la figura 5.2.

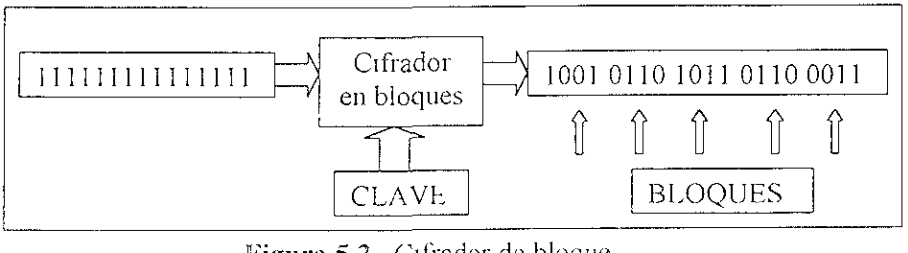


Figura 5.2. Cifrador de bloque

Si se procesa el texto mediante un cifrador continuo que opera con cadenas continuas de datos, generalmente bits u octetos, entonces una secuencia de código procesa los elementos de entrada de manera

continua, produciendo un elemento de salida a la vez El cifrador continuo se observa en la figura 5.3.

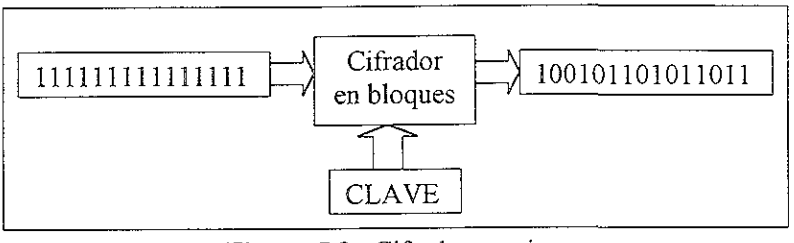


Figura 5.3. Cifrador continuo

Los sistemas criptográficos proveen las propiedades de seguridad: el secreto y la autenticidad, lo cual incluye integridad, además pueden proveer no repudio. Mantener en secreto la información es la meta histórica de la criptografía y ésta se alinea con las metas de la seguridad informática la confidencialidad y la integridad. La autenticidad implica que el receptor de un mensaje debe ser capaz de determinar:

a) El origen del mensaje

b) Que el mensaje no fue modificado.

La seguridad de un sistema criptográfico no puede basarse únicamente en los algoritmos de cifrado y descrifado, sino que también debe darle importancia a la clave Por ello, las técnicas de cifrado deben tener las siguientes propiedades

- Para los usuarios autorizados debe ser relativamente sencillo cifrar y descifrar el mensaje.

- El esquema de cifrado no depende de mantener en secreto el algoritmo, sino de un parámetro del algoritmo llamado clave de cifrado.

- Para un intruso (criptoanalista) debe ser muy difícil determinar cuál es la clave de cifrado

Secreto Perfecto

Shannon determinó las condiciones del Secreto Perfecto basándose en dos hipótesis principalmente.

1. Utilizar una sola vez la clave secreta.

2. El criptoanalista puede acceder únicamente al criptograma, por lo tanto, está limitado a realizar un solo ataque sobre el texto cifrado.

Shannon, de acuerdo a sus hipótesis anteriores enunció las condiciones de secreto perfecto: Si el texto claro *X* es estadísticamente independiente del texto cifrado *Y*, entonces se puede expresar como: $P(X = x \mid Y = y) = P(X = x)$, para todos los posibles valores criptogramas $x = (x_1, x_2, ..., x_m)$ y todos los posibles criptogramas $y = (y_1, y_2, y_3, ..., y_n)$. Lo anterior significa que la probabilidad de saber el texto claro dado el criptograma es nula, debido a que el criptoanalista no puede hacer una estimación de *X* (texto claro) con conocimiento de *Y* (criptograma) que la que haría sin su conocimiento.

5.2 Criptografía simétrica o de clave secreta (DES e IDEA)

Los métodos simétricos son aquéllos en los que la clave de cifrado es la misma que la clave de descifrado. Para ello, es necesario que la clave únicamente sea conocida por el emisor y el receptor. Dado que la misma clave es usada para cifrar y descifrar el mensaje, a este método de criptografía se le llamó "secreto compartido", el término más formal para este método es la criptografía simétrica Es importante mencionar que el cifrado convencional también es llamado cifrado simétrico, de clave secreta o de clave sencilla, y éste fue el primer tipo de cifrado en utilizarse a principios de 1970

Un esquema de cifrado convencional cuenta con cinco elementos principales.

1. **Texto en claro:** es el mensaje original o los datos que son alimentados como entrada al algoritmo

2. **Algoritmo de cifrado:** el algoritmo ejecuta varias sustituciones y transformaciones sobre el texto en claro

3. **Clave secreta:** es también una entrada al algoritmo. Las sustituciones y transformaciones exactas dependen de la clave.

4. **Texto cifrado o criptograma:** es el mensaje que se produce como salida. Depende del texto y de la clave secreta. Para un mensaje dado, dos claves diferentes producen dos textos cifrados diferentes.

5. **Algoritmo de descifrado:** se trata del algoritmo de cifrado ejecutado en reversa. Toma el texto cifrado y la misma clave secreta y produce el texto original.

Existen dos requerimientos para el uso seguro del cifrado convencional:

a) Se necesita un algoritmo de cifrado fuerte. Como mínimo el algoritmo debe ser tal que un oponente que sepa el algoritmo y que tenga acceso a uno o más textos cifrados sea incapaz de descifrar el texto o encontrar la clave.

b) *El emisor y el receptor deben tener copias de la clave secreta en un lugar* secreto y deben mantenerla segura

Es importante notar que la seguridad del cifrado convencional depende de lo secreta que sea la clave y no de qué tan secreto sea el algoritmo, es decir, el algoritmo no debe mantenerse en secreto, pero la clave sí pues no se puede descifrar un texto sólo partiendo de la base de que se conoce el algoritmo La clave utilizada en el cifrado convencional es llamada **clave secreta**

En la criptografía simétrica el cifrado y descifrado se expresan a través de las siguientes funciones:

Cifrado E(K,P)=C Descifrado: D(K, C)=P

Donde E(K,P) es una función de cifrado, *K* es la clave secreta, *P* es el texto, C es el texto cifrado y D(K, C) es la función correspondiente de descifrado. Debido al inconveniente de la criptografía simétrica, de que si se deduce la clave, con ella se puede descifrar el mensaje y también se podrían crear nuevos mensajes usando la misma, el requerimiento para un cifrado de clave secreta es que la seguridad del sistema dependa sólo de mantener en secreto la clave de la información, lo cual

indica que las funciones de cifrado y descifrado pueden ser públicas sin degradar la seguridad del sistema.

Un ejemplo de la criptografía simétrica se presenta en la tabla 5.6:

Texto en claro	Clave	Criptograma	Texto en claro nuevamente
Nosotros estamos seguros	Sustitución del texto por palabras. Nosotros = XXX, estamos=YYY, seguros=ZZZ.	XXX YYY ZZZ	Nosotros estamos seguros
Nosotros estamos seguros	Incluir palabras al mensaje y cada tres palabras se toma dicha palabra para formar el mensaje original.	¿Que si nosotros sabemos que estamos realmente muy seguros de comer?	Nosotros estamos seguros

Tabla 5.6. Ejemplo de método simétrico

Norma de cifrado de datos (DES)

La Norma de Cifrado de Datos (DES – Data Encryption Standard) es un algoritmo para cifrar desarrollado por IBM e introducido en 1977 por el Instituto Americano de Estandarización y Tecnología, fue aprobado por la Oficina Nacional de Normas de los Estados Unidos como una Norma Oficial para la información no clasificada y para ser usada por los sistemas de comunicaciones de los sectores privado y gubernamental

El DES es un algoritmo de cifrado de bloque, donde la longitud de bloque es de 64 bits y la longitud de la clave es de 56 bits, si el texto es más grande entonces se procesa en bloques de 64 bits. La norma pide obligatoriamente que el DES se implemente mediante un circuito integrado electrónico. El esquema total del DES se ilustra en la figura 5.4

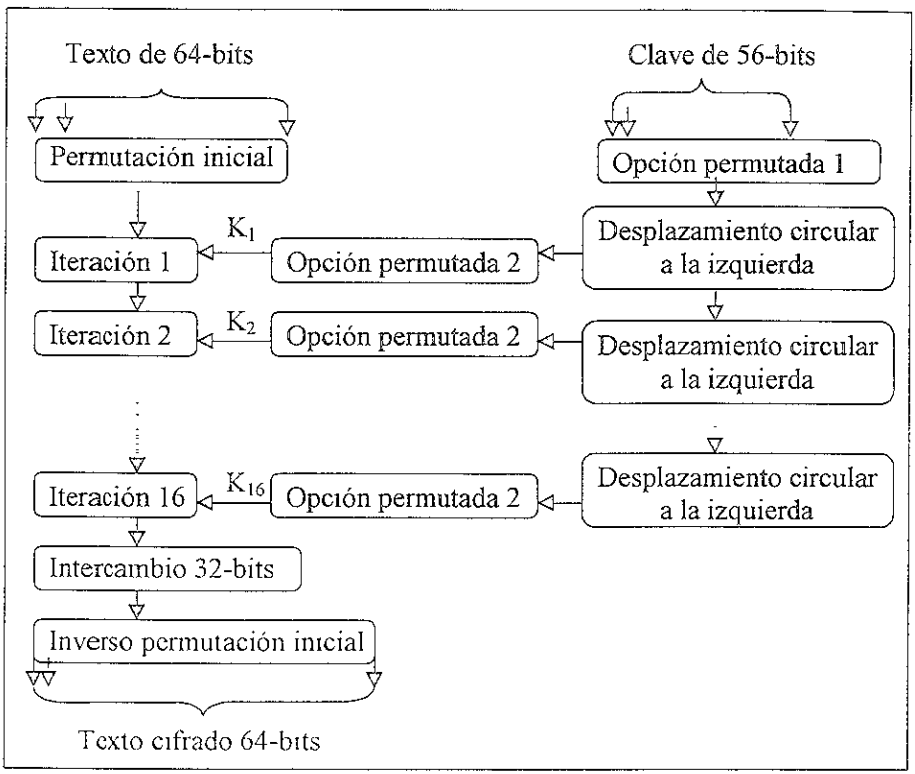


Figura 5.4. Algoritmo DES

La parte izquierda de la figura 5.4 muestra que el procedimiento para cifrar se realiza en tres fases

a) El texto de 64 bits pasa a través de una permutación inicial que reacomoda los bits para producir la entrada permutada.

b) Consiste en 16 iteraciones de la misma función, la salida de la iteración número 16 contiene 64 bits que es una función del texto entrante y la clave, las mitades izquierda y derecha de la salida son intercambiadas para producir la pre-salida

c) La pre-salida pasa a través de una permutación que es el inverso de la función de permutación inicial para producir el texto cifrado de 64 bits

La parte derecha muestra la forma en la cual la clave de 56 bits es utilizada Inicialmente la clave pasa a través de una función de permutación, luego, para cada una de las iteraciones una subclave (K_i) es producida por la combinación de un desplazamiento circular a la izquierda y una permutación La función de permutación es la misma para cada iteración, pero una subclave diferente se produce debido al desplazamiento repetido de los bits de la clave.

El proceso de descifrado con DES es igual al proceso de cifrado, sólo que la regla es como sigue: se utiliza el texto cifrado como la entrada al algoritmo DES y se usan las claves K_i en orden inverso, esto es, en la primera iteración K_{16}, K_{15} en la segunda , así hasta que K_1 sea usada en la iteración número 16.

De manera más detallada el funcionamiento del DES se basa en los siguientes pasos:

1 Del bloque original de 64 bits, se realiza una permutación inicial fija.

2 Se divide el bloque resultante en dos mitades de 32 bits cada una. Bloque derecho y bloque izquierdo

3 Se aplica una función *f* en 16 ocasiones. Calculando L_iR_i para $1 < i < 16$ de la siguiente forma:
$L_i = R_{i-1}$ $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ donde $\oplus$ representa la operación OR EXCLUSIVA de dos bloques de bits. Las K_i son obtenidas a partir de la clave *K*.

4 En la iteración 16 se omite el intercambio, pero termina el algoritmo con una permutación final (que es la inversa de la permutación inicial). De esta manera se regresa al bloque original.

El DES utiliza las técnicas que fueron sugeridas por Shannon:

a) **Confusión:** el DES crea confusión por sustitución, utilizando dispositivos de sustitución no lineales llamados cajas-S

b) **Difusión:** la difusión en DES se basa en la permutación utilizando cajas-P que definen las permutaciones

c) **Cifras de producto:** el DES es una cifra de producto, con cifrado aplicado 16 veces.

d) **Transformaciones mezcladas:** son aquéllas que difunden mensajes de alta probabilidad de un espacio de mensaje uniformemente a través del espacio.

Esta norma (DES), es una transformación producto, es decir, que utiliza los conceptos de transposición y sustitución, cuyo objetivo es el de hacer un algoritmo de cifrado tan complicado, de modo que un criptoanalista no tenga ninguna posibilidad de obtener información alguna de un texto cifrado.

Existen dos maneras para fortalecer la norma DES:

1. Incluir caracteres aleatorios en el texto en claro, por medio de una regla definida. Por ejemplo, todos los n-ésimos caracteres son reales y el resto son sólo ruido. Además, se pueden insertar mensajes de relleno entre los que son reales. Este principio se conoce como **cifrador nulo**, por el cual se tiene un desperdicio de ancho de banda pero cuyo descifrado es muy difícil porque la posición de los caracteres reales y de los mensajes se conserva en secreto y se cambia cuando se modifica la clave.

2 Otra manera más difícil, es hacerla funcionar como un **cifrador de flujo**, en el que tanto el transmisor como el receptor operan sus circuitos integrados DES en modo de cifrado (opuesto al descifrado)

Algoritmo internacional de cifrado de datos (IDEA)

El algoritmo internacional de cifrado de datos (IDEA – International Data Encryption Algorithm) es un cifrado de bloque simétrico que fue desarrollado por Huejia Lai y James Massey del Instituto Federal Suizo de Tecnología en 1991, está diseñado para ser más seguro que el DES contra los ataques de fuerza bruta y diferentes tipos de criptoanalistas. IDEA difiere del DES tanto en la función iterativa como en la función generadora de subclaves. La efectividad de este tipo de cifrado está basada en el concepto de mezclar operaciones aritméticas de grupos algebraicos diferentes. La clave es de 128 bits, lo que hace que la búsqueda sea más difícil que para la clave de 56 bits del DEA debido a que la longitud de la clave es mayor y por lo tanto aumenta el número de operaciones aritméticas. La clave de 128 bits es utilizada para generar 16 subclaves. Como en el DES, la entrada es un

bloque de 64 bits, que se separa en sub-bloques de 16 bits Existen ocho iteraciones más una transformación final. Cada iteración opera sobre cuatro sub-bloques del texto y seis subclaves, y la transformación final utiliza cuatro subclaves. Para la función iterativa, IDEA no utiliza cajas-S. Como el DES, IDEA hace buen uso de la confusión y la difusión DES utiliza únicamente operaciones de OR-exclusiva recayendo en las cajas-S para la confusión . IDEA mezcla tres diferentes operaciones:

1. OR-exclusiva.

2. Módulo de adición 2^{16} (Suma binaria de enteros de 16 bits).

3. Módulo de multiplicación $2^{16} + 1$ (Multiplicación binaria de enteros de 16 bits)

Esto quiere decir que existen operaciones durante el proceso de cifrado, dichas operaciones se utilizan en tres grupos artiméticos diferentes sobre pares de sub-bloques con longitud de 16 bits. Los grupos son:

1 Grupo Multiplicativo en el cuerpo $Z_{2^{16}-1}$ y se representa con el símbolo "$\otimes$ ".

2. Grupo Aditivo en $Z_{2^{16}}$ y se representa con el simbolo "+"

3 Grupo aditivo en Z_2 de las 16-tuplas, que son bit a bit, y se representa con el símbolo "$\oplus$"

Las funciones son combinadas de tal manera que se produce una transformación compleja que es difícil de analizar y por consiguiente difícil de criptoanalizar El algoritmo de generación de subclaves recae en el uso de desplazamientos circulares y se utilizan de una forma compleja para generar un total de seis subclaves por cada una de las ocho iteraciones de IDEA

IDEA está diseñado para ser más seguro que DES y parece que será altamente resistente al criptoanálisis IDEA es utilizado en el PGP (Pretty Good Privacy system) como una alternativa

En la tabla 5.7 puede observarse una comparación entre ambos algoritmos

Algoritmo	Tamaño de la clave	Número de iteraciones	Operaciones matemáticas
DES	56 bits	16	XOR, cajas-S
IDEA	128 bits	8	XOR, suma, multiplicación

Tabla 5.7. Algoritmos DES e IDEA

5.3 Criptografía asimétrica o de clave pública (Diffie-Hellman y RSA)

Los métodos asimétricos son aquéllos en los que la clave de cifrado es diferente a la de descifrado. En términos generales, la clave de cifrado es conocida por todo el público, mientras que la de descifrado sólo es conocida por el usuario.

Los investigadores Whitfield Diffie y Martin Hellman, desarrollaron el uso de una clave asimétrica en 1975 para resolver el problema de poseer una sola clave simétrica. De esa manera, todos los que quieran comunicarse posiblemente tienen un par de claves. Las dos claves utilizadas en un cifrado de clave pública son llamadas **clave pública** y **clave privada**. Haciendo una analogía con una cerradura, se necesitaría una clave para cerrarla y otra clave para abrirla.

A este método asimétrico se le conoce como criptografía de clave pública. Existe un algoritmo de clave pública que está hoy día teniendo una gran aceptación. Éste es llamado RSA, nombrada por sus inventores, Ron Rivest, Adi Shamir y Leonard Adelman

En la criptografía de clave pública una de las claves es distribuida ampliamente (su conocimiento se hace público) Esto no compromete su clave privada, ya que ésta no puede derivarse a partir de la clave pública. La clave pública se da a la persona con quien se quiere mantener comunicación. Ahora cada persona tiene su propio par de claves (pública y privada), de esta manera la probabilidad de que alguien divulgue una clave es menor, es decir, la clave pública del par es pública para que otros la utilicen, mientras que la clave privada sólo la conoce su dueño. Un propósito general del algoritmo criptográfico de clave pública recae en que se utiliza una clave para el cifrado y otra diferente para el descifrado.

Un cifrado de clave pública puede ser expresado a través de las siguientes funciones.

Cifrado: E(X,P)=C Descifrado: D(Y,C)=P

Donde E(X,P) es una función de cifrado de clave pública, *X* es la clave pública, *P* es el texto, *C* es el texto cifrado, D(Y,C) es la función de descifrado correspondiente , *Y* es la clave privada y *X* es diferente de *Y*.

El requerimiento fundamental para un cifrado de clave pública es que la función de cifrado E(X,P) debe ser una función de puerta falsa de un solo sentido para el cual es fácil realizar con una clave pública, pero difícil invertirlo sin la clave privada. El otro aspecto de los algoritmos de clave pública es que están designados de tal forma que es difícil deducir la clave privada a partir de la clave pública.

Un esquema de cifrado de clave pública contiene los siguientes elementos.

1. **Texto en claro:** es el mensaje o los datos de entrada al algoritmo, es decir, el texto a cifrar

2. **Algoritmo de cifrado:** el algoritmo de cifrado ejecuta varias transformaciones sobre el texto en claro.

3. **Clave pública y privada:** son un par de claves que han sido seleccionadas, de tal forma que si una ha sido seleccionada para cifrar, la otra es utilizada para descifrar

4. **Texto cifrado:** este es el mensaje que se produce como salida Depende del texto original y de la clave

5. **Algoritmo de descifrado:** este algoritmo acepta el texto cifrado y la clave dada y produce el texto original

Los pasos esenciales de este algoritmo son los siguientes

1 Cada usuario genera un par de claves para que sean usadas en el cifrado y descifrado de mensajes

2. Cada usuario coloca una de las dos claves en un registro público u otro archivo accesible, a ésta se le llama clave pública. La otra clave se mantiene en privado, cada usuario mantiene una colección de claves públicas que obtiene de otros.

3. Si el individuo *B* desea enviar un mensaje privado al individuo *A*, entonces *B* cifra el mensaje utilizando la clave pública de *A*.

4. Cuando *A* reciba el mensaje, lo descifrará utilizando su clave privada. No existe otro receptor que pueda descifrar el mensaje porque sólo *A* conoce la clave privada de *A*.

Todos los participantes tienen acceso a las claves públicas, y las claves privadas son generadas localmente por cada participante y nunca son distribuidas. Si el participante protege su clave privada, la comunicación es segura, en cualquier momento el usuario puede cambiar la clave privada y publicar la clave pública para reemplazar a la antigua.

Los sistemas criptográficos asimétricos pueden clasificarse, dependiendo de su uso, en tres categorías:

a) **Cifrado y descifrado:** el emisor cifra un mensaje con la clave pública del receptor

b) **Firma digital:** el emisor "firma" un mensaje con su clave privada La firma es realizada por un algoritmo criptográfico aplicado al mensaje o al bloque de datos que es una función del mensaje

c) **Intercambio de claves:** dos lados cooperan para intercambiar una clave de sesión

Algunos algoritmos son convenientes para las tres aplicaciones, mientras que otros sólo pueden ser utilizados para una o dos de las aplicaciones, la tabla 5 8 indica las aplicaciones soportadas por los algoritmos RSA y Diffie-Hellman

Algoritmo	Cifrado/Descifrado	Firma digital	Intercambio de claves
RSA	Sí	Sí	Sí
Diffie-Hellman	No	No	Sí

Tabla 5.8. Aplicaciones para los sistemas criptográficos de clave pública

Algoritmo RSA

Uno de los primeros esquemas de clave pública es el algoritmo RSA desarrollado por Ron Rivest, Adi Shamir y Len Adleman en MIT 1978. El algoritmo está basado en la dificultad para realizar factorizaciones de números largos. RSA es un bloque cifrador en el cual el texto original y el texto cifrado son enteros entre el 0 y n-1 para cualquier n.

El cifrado y descifrado son de la siguiente manera para algún bloque de texto M y un bloque de texto cifrado C:

$C = M^e \bmod n$
$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Tanto el receptor como el emisor deben saber los valores de n y e, y sólo el receptor conoce el valor de d Este es un algoritmo de cifrado de clave pública con una clave pública de KU= {e,n} y una clave privada de KR={d,n} Para que este algoritmo satisfaga el cifrado de clave pública, deben cumplirse los siguientes requerimientos:

1. Es posible encontrar valores de e, d, n tal que $M^{ed} = M \bmod n$ para toda $M<n$

2. Es relativamente fácil calcular M^e y C para todos los valores de $M<n$.

3. No es factible determinar d dados e y n

Los dos primeros requerimientos son fáciles de cumplir y el tercero se logra cuando los valores de e y n son muy grandes

Los pasos del algoritmo RSA son los siguientes

1. Se seleccionan dos números primarios, p y q

2. Se calcula el producto $n= p \times q$, el cual es el módulo para cifrar y descifrar.

3. Se obtiene $\phi(n)$, que es el número de enteros positivos menores que n y relativamente primos de n.

4. Se selecciona un entero e que es relativamente primo a $\phi(n)$[11] El máximo común divisor (mcd) de e y $\phi(n)$ es 1.

5. Finalmente se calcula d como el inverso multiplicativo de e, módulo $\phi(n)$.

El algoritmo RSA se resume en la figura 5.5.

Generación de la clave	
Seleccionar p,q	p y q son primos
Calcular $n= p \times q$	
Calcular $\phi(n) = (p-1)(q-1)$	
Seleccionar el entero e	$mcd(\phi(n),e) =1 \; ; \; 1<e< \phi(n)$
Calcular d	$d=e^{-1} \bmod \phi(n)$
Clave pública	KU={e,n}
Clave privada	KR={d,n}
Cifrado	
Texto original:	M<n
Texto cifrado:	$C=M^e \pmod n$
Descifrado	
Texto cifrado.	C
Texto original	$M=C^d \pmod n$

Figura 5.5. Algoritmo RSA

[11] El entero e debe ser un número primo sin ser divisor de $\phi(n)$

Algoritmo Diffie-Hellman

El primer algoritmo de clave pública que definía la criptografía de clave pública – generalmente se hace referencia a este algoritmo como el intercambio de clave de Diffie-Hellman – , fue introducido por Diffie y Hellman en 1976, los cuales propusieron que se utilizara dicha idea para distribuir las claves secretas de cifrado.

El propósito del algoritmo es habilitar a los dos usuarios para intercambiar una clave secreta de manera más segura que puede ser utilizada para el subsecuente cifrado de mensajes. El algoritmo sólo se limita al intercambio de claves.

El algoritmo Diffie-Hellman basa su efectividad en la dificultad de lograr el cálculo de logaritmos discretos. Brevemente se puede definir el logaritmo discreto de la siguiente manera, primero se define una raíz primitiva de un número primo p como aquélla que genera todos los enteros de 1 a p-1. Esto es, si a es una raíz primitiva del número primo p, entonces los números:

$a \bmod p$, $a^2 \bmod p$, . . $a^{p-1} \bmod p$

son distintos y contienen los enteros de 1 a p-1 en alguna permutación.

Para cualquier entero b y la raíz primitiva a del número primitivo p, uno puede encontrar un único exponente i tal que $b=a^i \bmod p$ donde $0 \leq i \leq (p-1)$

El exponente i es referido al logaritmo discreto o índice de b para la base a, mod p Este valor es denotado como $\mathrm{ind}_{a,p}(b)$

En el algoritmo Diffie-Hellman existen dos números, uno es un número primo q y el otro un entero α que es una raíz primitiva de q Suponiendo que los usuarios A y B desean intercambiar una clave. El usuario A selecciona un entero de manera aleatoria $X_A<q$ y calcula $Y_A=\alpha^{X_A} \bmod q$ De manera similar, el usuario B de manera independiente selecciona un número entero aleatorio $X_B<q$ y calcula Y_B $\alpha^{X_B} \bmod q$ Cada lado mantiene el valor de X en privado y hace que el valor de Y sea conocido por el lado contrario El usuario A calcula K $(Y_B)^{X_A} \bmod q$ y el usuario B calcula la clave como K $(Y_A)^{X_B} \bmod q$ Estos cálculos producen

resultados idénticos. Debido a que X_A y X_B son privadas, un oponente sólo puede trabajar con: q,a, Y_A y Y_B. Entonces el oponente está forzado a tener el logaritmo discreto para determinar la clave, el logaritmo discreto no es computacionalmente factible, excepto para ciertos valores de q. La seguridad del algoritmo recae en el hecho de que es difícil calcular los logaritmos discretos.

El algoritmo de Diffie-Hellman se resume en la figura 5.6.

Elementos públicos globales

q	número primo
α	$\alpha<q$ y una raíz primitiva de q

Generación de la clave del usuario A

Seleccionar X_A privada	$X_A<q$
Calcular Y_A pública	$Y_A = \alpha^{X_A} \bmod q$

Generación de la clave del usuario B

Seleccionar X_B privada	$X_B<q$
Calcular Y_B pública	$Y_B = \alpha^{X_B} \bmod q$

Generación de la clave secreta por el usuario A

$K=(Y_B)^{X_A} \bmod q$

Generación de la clave secreta por el usuario B

$K=(Y_A)^{X_B} \bmod q$

Figura 5.6. Algoritmo Diffie-Hellman

Lecturas recomendadas

[1]. Algoritmo DES

[9]. Capítulo 9. Seguridad en el Web:
Introducción a los sistemas de cifrado

[16]. Criptografía simétrica

[28]. Capítulo 1. La Criptología
1. Introducción
2. Procedimientos clásicos de cifrado
2.1Principios de sustitución y de transposición
2.2Ejemplos históricos de cifrado por sustitución
2.3Condiciones de Secreto Perfecto

[28]. Capítulo 3 Criptografía de clave secreta: Métodos de cifrado en bloque
3 DES
3.1Estructura del DES
6. IDEA

[34]. Introduction to Modular arithmetic

[35] Chapter 2 Technical Fundamentals of security
2.1 Secret and Public Key cryptography
2.2 Secret Key Encryption

[47] Principios de criptografía, definiciones

[49] V Protección especial de la información

[57]. Chapter 2 Conventional Encryption & Message Confidenciality:
2.1 Conventional Encryption principles
2.2 Conventional Encryption Algorithms

[57] Chapter 3 Public key Cryptography & Message Authentication
3.4 Public Key Cryptography Algorithms

[58]. Chapter 5. Cryptography:
The Data Encryption Standard
IDEA
Overview

[59]. Sustitución, Transposición, Cifrado Vigenère

CAPÍTULO 6.
SEGURIDAD EN UNA ORGANIZACIÓN

6.1 Misión de la organización (sus objetivos)

En la actualidad, la dependencia de las organizaciones en su información ha crecido al punto de ser considerada como uno de sus activos más importantes. A través del tiempo, las necesidades del intercambio electrónico de información ha sido uno de los principales retos de cualquier organización, como respuesta a dichas necesidades se establece una infraestructura que permita brindar los servicios necesarios a sus clientes, socios comerciales y empleados. Esta infraestructura se basa, principalmente, en el establecimiento de redes, que son grupos de computadoras y dispositivos periféricos relacionados (impresoras, unidades de CD-ROM, etc.) – conectados a través de un canal de comunicaciones – los cuales son capaces de compartir archivos y otros recursos entre varios usuarios

El principal objetivo[12] informático de la organización es dar protección y seguridad a su información, para ello es necesario establecer las normas, políticas y estándares de seguridad para los sistemas distribuidos que procesan, almacenan y transmiten información, a fin de minimizar riesgos en su integridad, confidencialidad y disponibilidad.

Las ventajas que ofrece el plantear objetivos o misiones[13] en la organización, garantiza que la información manejada dentro y fuera del sistema central de la organización, cuente con los elementos necesarios para asegurar su protección contra alteración, divulgación, malversación o negación de acceso no autorizados, permitiendo la continuidad de las operaciones en las áreas de negocio principalmente o en áreas donde se maneja información sensitiva [14].

6.2 Definición de política

La **política de seguridad**, en el mundo real, es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma

[12] Objetivo: fin, objeto, término de un acto

[13] Misión: apostolado, predicación. Deber moral que a cada hombre le impone su condición o estado

[14] La información sensitiva es aquélla que es clasificada como secreta, confidencial o privada

La política define la seguridad de la información en el sistema central de la organización, por lo tanto, un sistema central es seguro si cumple con las políticas de seguridad impuestas para esa organización. La política especifica qué propiedades de seguridad el sistema debe proveer. De manera similar, la política define la seguridad informática para una organización, especificando tanto las propiedades del sistema como las responsabilidades de seguridad de las personas.

Una **política de seguridad informática** debe fielmente representar una política del mundo real y además debe interactuar con la política de recursos, por ejemplo, políticas en el manejo de bases de datos o de transacciones. En ella, se deben considerar las amenazas contra las computadoras, especificando cuáles son dichas amenazas y cómo contraatacarlas. Así mismo debe ser expresada en un lenguaje en el que todas las personas involucradas (quienes crean la política, quienes la van a aplicar y quienes la van a cumplir) puedan entender.

6.2.1 Principios fundamentales

A través de las leyes, reglas y prácticas que reflejen las metas y situaciones de la organización, ellas también reflejan los principios que se aplican en general, éstos se detallan a continuación

a) **Responsabilidad individual:** las personas son responsables de sus actos El principio implica que la gente que está plenamente identificada debe estar consciente de sus actividades, debido a que sus acciones son registradas, guardadas y examinadas.

b) **Autorización:** son reglas explícitas acerca de quién y de qué manera puede utilizar los recursos

c) **Mínimo privilegio:** la gente debe estar autorizada única y exclusivamente para acceder a los recursos que necesita para hacer su trabajo

d) **Separación de obligaciones:** las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad o función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado. La separación de obligaciones funciona mejor cuando cada una de las personas involucradas tiene diferentes actividades y puntos de vista

e) **Auditoría:** el trabajo y los resultados deben ser monitoreados durante su inicio y hasta después de ser terminado. Una revisión de los registros,

donde se guardan las actividades, ayuda para realizar una reconstrucción de las acciones de cada individuo.

f) **Redundancia:** el principio de redundancia afecta al trabajo y a la información. Múltiples copias son guardadas con importantes registros y dichas copias son frecuentemente almacenadas en diferentes lugares.

g) **Reducción de Riesgo:** esta estrategia debe reducir el riesgo a un nivel aceptable, haciendo que el costo de la aplicación sea proporcional al riesgo.

Roles, papeles o funciones en el mundo real, de la política de seguridad

La política de seguridad involucra papeles que se repiten en muchas situaciones y también en aplicaciones específicas. Para documentos realizados en papel, se aplican los siguientes roles genéricos:

a) **Originador (autor):** es la persona que publica un documento, frecuentemente el autor o el director, es el responsable de la unidad.

b) **Autorizador:** es la persona que tiene el control sobre el documento y quien puede autorizar o denegar el acceso al mismo para editar, copiar, leer, etc. El autorizador puede o no ser el autor

c) **Custodio:** es la persona que físicamente guarda el documento y lleva a cabo los propósitos del autorizador sobre la manera de accederlo

d) **Usuario:** es la persona que lee y/o modifica el documento

Si el medio no es un documento pero sí es una transacción comercial, otros roles o funciones entran en acción, incluyendo

a) **Creador:** es la persona que diseña la transacción y escribe las reglas sobre los pasos a seguir.

b) **Cliente:** es la persona que en su nombre se lleva a cabo la transacción

c) **Ejecutor:** es la persona que efectivamente realiza la transacción en nombre del cliente, paga un cheque, abre una cuenta, etc.

d) **Supervisor:** es la persona que verifica que las acciones, resultados y controles se hayan llevado a cabo conforme a lo establecido por el creador.

Políticas en el mundo real, para confidencialidad

De las tres propiedades de seguridad más importantes (confidencialidad, integridad y disponibilidad), las dos primeras reflejan claramente las propiedades en el mundo real. Algunos documentos importantes son guardados en secreto para cualquiera, excepto para el propio creador. Típicamente, los documentos son agrupados o clasificados de acuerdo al tipo de confidencialidad que se necesite.

La política puede ser indicada como una relación entre la clasificación del documento y la posición o cargo de la persona. Por ejemplo, en la política de confidencialidad militar de Estados Unidos, tanto los documentos como las personas tienen diferentes niveles de clasificación· Super secreto (top secret), secreto (secret), confidencial (confidential) o no clasificado (unclassified)

Políticas y controles para la integridad

La administración en el control de la política está dirigida principalmente a la integridad más que a la confidencialidad y esto se ha dado principalmente porque para la mayoría de las aplicaciones empleadas en el mundo real - comerciales, militares, de tipo médico, sistemas financieros – es más importante mantener la integridad de los datos ya que cada vez se necesita automatizar más actividades – sistemas de comunicación, control del tráfico de aire, lanzamiento de misiles, tratamientos con radiación - que requieren de dispositivos y aplicaciones más complejos, de tal manera que también es necesario mantener la integridad de éstos y la integridad de los datos que procesan [15] A

[15] Summers, Rita *Secure Computing, Threats and Safeguards* EUA, Mc Graw Hill, 1997, p 107

continuación se mencionan algunas de las políticas de integridad más comunes e importantes:

a) **Política de acciones autorizadas:** establece que la gente puede realizar las acciones para las que está autorizada, esta política aplica para importantes medios, tales como el dinero que está en la caja registradora de un restaurante (por ejemplo); cualquiera puede recoger una servilleta del suelo, pero no todos pueden meter mano a la caja registradora.

b) **Política de control supervisor:** ciertas acciones deben ser aprobadas por un supervisor.

c) **Política de rotación de obligaciones:** una tarea no debe ser realizada siempre por la(s) misma(s) persona(s).

d) **Política de control de "n" personas:** requiere que la gente coopere para llevar a cabo una acción.

e) **Política de secuencia de operaciones:** requiere que los pasos de alguna tarea deben llevarse a cabo en un orden específico. Frecuentemente esta política es combinada con la separación de obligaciones y "n" personas de control, así que una persona o grupo diferente realiza cada paso de la secuencia.

f) **Política de cambio restringido:** requiere que la información sea cambiada siempre en la forma prescrita y estructurada, es decir, que desde que se diseña la política hay que considerar que se pueden presentar cambios y éstos pueden realizarse respetando y siguiendo determinados procedimientos que se hayan elaborado previamente

g) **Política de atribución de cambios:** tiene como objetivo verificar la validez de la información

Políticas de seguridad en el mundo real, de la computación

Primero, la política de seguridad debe reflejar fielmente el mundo real Esto significa que debe ser especificada sin ambigüedades Segundo, las políticas seleccionadas deben ser hechas sobre la situación actual de los sistemas conectados en red Una política de seguridad debe estar especificada en un documento especial para tal propósito redactada en un lenguaje natural,

claramente y sin ambigüedades posibles. El documento deberá especificar qué propiedades de seguridad se pretenden cubrir con la aplicación de las políticas y la manera de usarlas.

6.3 Definición de modelos

Un **modelo de seguridad** es la presentación formal de una política de seguridad ejecutada por el sistema. El modelo debe identificar el conjunto de reglas y prácticas que regulan cómo un sistema maneja, protege y distribuye información delicada.

Los modelos de seguridad pueden ser de dos tipos:

1. **Modelo abstracto:** se ocupa de las entidades abstractas como sujetos y objetos. El modelo Bell LaPadula es un ejemplo de este tipo.

2. **Modelo concreto:** traduce las entidades abstractas a entidades de un sistema real como procesos y archivos.

Además los modelos sirven a tres propósitos en la seguridad informática:

1. Proveer un sistema que ayude a comprender los diferentes conceptos. Los modelos diseñados para este propósito usan diagramas, analogías, cartas. Un ejemplo es la matriz de acceso

2. Proveer una representación de una política general de seguridad formal y clara. Un ejemplo es el modelo Bell-LaPadula.

3. Expresar la política exigida por un sistema de cómputo específico

Es importante mencionar que los modelos formales se basan en métodos de lógica matemática y algunos campos de matemáticas aplicadas, lo cual incluye teoría de información, teoría autómata, teoría compleja y estadística.

6.3.1 Criterios

Al asumir que la política de seguridad es realmente la apropiada, existen criterios que un modelo de seguridad debe seguir a medida que se va desarrollando para considerarse un buen modelo. Por lo tanto, un modelo de seguridad debe

1. **Representar de manera válida y precisa la política de seguridad**: los creadores del modelo deben explicar de manera clara cómo el modelo corresponde a la política y deben justificar la validez de las correspondencias.

2. **Ayudar a entender a través de expresiones enfocadas y exactas y pruebas de propiedades**: un modelo ayuda a la comprensión tras aclarar conceptos y expresarlos de manera precisa, lo cual enfoca la atención sobre lo esencial. Se entiende el problema con lo que se deriva de los axiomas del modelo.

3. **Soportar un análisis de seguridad**: un modelo debe soportar decisiones sobre seguridad y la pregunta de si existe algún estado del modelo en donde una propiedad específica de seguridad no se mantiene. Desafortunadamente existe una tensión entre la seguridad y la precisión, si el modelo está restringido de manera que la seguridad puede decidirse, no se representará una política de seguridad demasiado precisa.

4. **Soportar la creación y verificación del sistema:** un sistema basado en un modelo debe ser razonable para construirse y debe trabajar de manera adecuada.

5. **Permitir que los sistemas sean modelados en partes y después unirlas:** debe ser posible modelar sistemas complejos en partes y después unir estas partes, de esta manera cada parte será más clara y su verificación simple y correcta.

6.3.2 Modelos de control de acceso

Los modelos de control de acceso identifican las reglas necesarias para que un sistema lleve a cabo el proceso que asegura que todo acceso a los recursos, sea un acceso autorizado. Estos modelos refuerzan el principio fundamental de seguridad de autorización, ya que éste protege tanto a la confidencialidad como a la integridad

Los modelos de control de acceso son

6.3.2.1 Modelo de la matriz de acceso

Este modelo fue desarrollado a principios de los años 70's para los sistemas operativos debido a los problemas de protección presentados en los sistemas multiusuarios. Se trata de un modelo simple e intuitivo y permite expresar varias políticas de protección. El modelo de la matriz de acceso relaciona sujetos, objetos y derechos. Estos elementos se describen a continuación:

a) **Objetos:** representan los recursos que serán controlados como archivos o áreas de memorias.

b) **Sujetos:** son las entidades activas del modelo como los usuarios o los procesos ejecutados por el usuario.

c) **Derechos:** representan un tipo de acceso hacia el objeto como leer, escribir o ejecutar.

La matriz de acceso está formada por un renglón para cada sujeto y una columna para cada objeto, la celda especifica los derechos que el sujeto *s* tiene sobre el objeto *o* - la notación empleada es AM[s,o]. Por lo que un renglón de la matriz de acceso corresponde a una **lista de capacidad** (lista de todos los derechos del sujeto) y una columna corresponde a una **lista de control de acceso** (lista de todos los derechos que tiene el sujeto sobre el objeto) Lo descrito se muestra de manera clara en la figura 6.1.

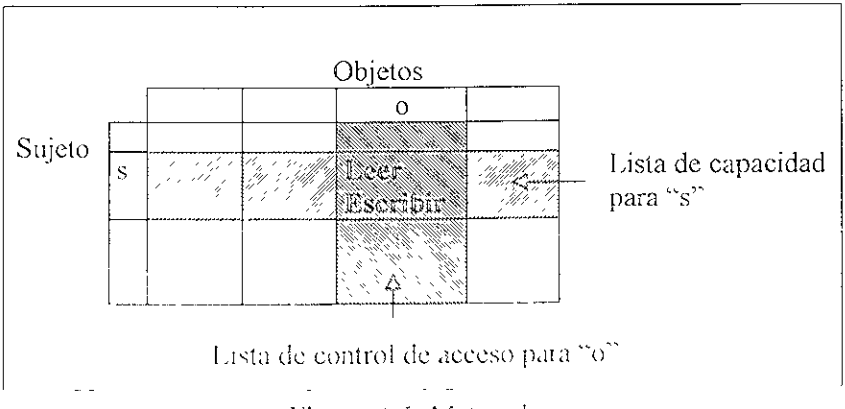


Figura 6.1. Matriz de acceso

Este modelo puede representar muchas políticas de control de acceso que aseguran la confidencialidad (esto se logra controlando la lectura de los objetos) y la integridad (tras controlar las modificaciones a los objetos y la invocación de los programas). Maneja lo que se conoce como control de acceso discreto (DAC) ya que la matriz de acceso puede ser cambiada de manera discreta por aquéllos que autorizan. En este modelo se especifica quién eres y con quién estás relacionado además de que el sistema indica lo que te está permitido hacer.

Para que un sistema sea más útil, la matriz de acceso no debe ser estática, entonces los sujetos, los objetos y los derechos suelen ser cambiantes. Esto indica que el modelo debe incluir operaciones para cambiar la matriz de acceso, es decir, ciertas operaciones para crear o destruir sujetos y objetos y para crear o borrar derechos. Sin embargo, debe tomarse en cuenta lo que un cambio en el modelo implica y lo que puede lograr el sujeto con dichos cambios

Modelo HRU

El modelo HRU fue creado por Harrison, Ruzzo y Ullman en 1976 al tratar de mejorar el modelo de la matriz de acceso, debido a que éste era débil con respecto a la seguridad ya que de manera general no toma en cuenta lo que un cambio en el modelo implica.

El modelo HRU define un sistema de protección que se encuentra constituido por dos elementos

a) **Un conjunto de derechos genéricos:** donde ese conjunto representa los tipos de acceso del sujeto hacia el objeto como leer, escribir, borrar, modificar, ejecutar.

b) **Un conjunto de comandos**: donde un comando cuenta con una parte condicional y una principal, la condicional prueba la presencia de ciertos derechos en la matriz de acceso, si la prueba es exitosa la parte principal se ejecuta realizando una serie de operaciones primitivas que cambian la configuración de protección. Las operaciones primitivas crean y destruyen objetos y sujetos, añaden o borran derechos en la matriz de acceso

El modelo HRU es sencillo y se encuentra diseñado para contestar preguntas fundamentales. Además, mejora la seguridad puesto que verifica si realmente se trata de un sujeto autorizado y contempla que un cambio en la matriz de acceso no permite a sujetos no autorizados obtener derechos.

El resultado importante del modelo es que no está a discusión si una configuración dada es segura para un determinado derecho. Aún cuando este resultado acerca de la matriz de acceso es fundamental, sólo aplica a un sistema de protección general y no restringido ya que para un sistema restringido monoperacional (donde cada comando se compone de una sola operación primitiva) la seguridad está a discusión pero el procedimiento de decisión es computacionalmente complejo, lo cual no es práctico.

Otros rasgos del modelo de la matriz de acceso

Los siguientes rasgos aparecen en diferentes versiones del modelo de la matriz de acceso:

1. **Transferencia de derechos:** en algunos sistemas los sujetos pueden recibir derechos que son transferibles, es decir, el sujeto puede transferir el derecho a otro sujeto. Esta transferencia es descrita como una copia de bandera, si dicha copia se añade a un derecho en una celda, significa que un sujeto puede copiar ese derecho a otra celda en la columna *o*, escogiendo si se puede o no copiar la bandera también

2. **El monitor de referencia:** algún mecanismo que monitorea todos los accesos a los recursos. Este mecanismo asegura que cada acceso sea autorizado por la matriz

3. **Petición y decisión de acceso:** una petición es el evento sobre el cual el monitor de referencia interviene. Esto es, el sujeto *s* pide acceso de tipo *r* sobre el objeto *o*. La decisión permite o niega la petición o la convierte en otra petición. En este punto, otros elementos deben ser tomados en cuenta

a) **Reglas de validación de acceso:** especifican cómo el monitor de referencia decide el destino de la petición, es decir, cómo realiza la decisión.

b) **Reglas de autorización:** especifican cómo la matriz de acceso puede ser modificada.

En la figura 6.2 puede observarse una petición de acceso y la forma en la que el monitor de referencia interviene.

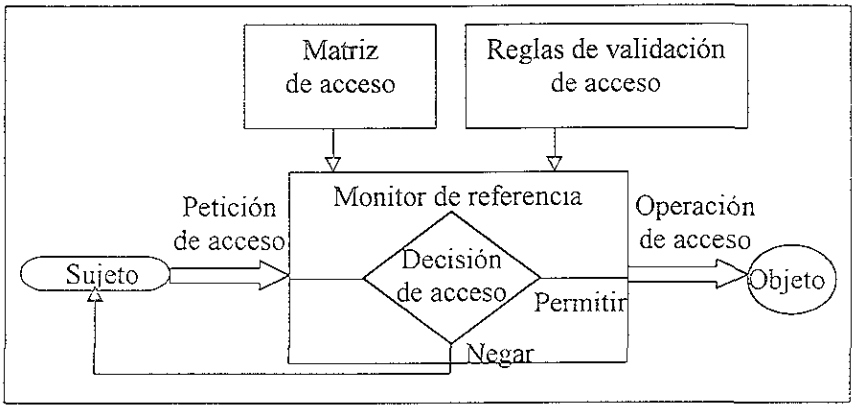


Figura 6.2. Monitor de referencia

6.3.2.2 Modelo Take-Grant

Ya que un renglón de la matriz de acceso puede ser visto como una lista de capacidades especificando todos los derechos del sujeto asociado con ese renglón Existen dos maneras principales para implementar el control de acceso

a) **Listas de control de acceso:** una lista de control de acceso contiene todos los derechos que tiene el sujeto sobre el objeto

b) **Capacidades:** una capacidad se define como (*objeto, derechos, número aleatorio*), el número asegura que no haya falsificación de capacidades

Debido a que las capacidades no pueden ser falsificadas, pueden pasar sin la intervención de un monitor, esta propiedad de las capacidades contribuye a dar gran importancia a la flexibilidad en el diseño de sistemas, los sistemas operativos y las arquitecturas de hardware han sido diseñados con base en las capacidades.

Los modelos Take-Grant se encuentran estrechamente identificados con los sistemas de capacidad. Estos modelos representan el estado de protección mediante una gráfica dirigida, los elementos utilizados en este modelo son:

a) **Vértice sólido:** representa un sujeto. El símbolo que lo representa es ○. Ej. Vértice b

b) **Vértice abierto:** representa un objeto Se representa mediante el símbolo ○. Ej Vértice c

c) **Línea dirigida:** va de un vértice a otro y representa un derecho que el sujeto tiene sobre el objeto. Ej α

d) **Vértice mixto:** representa a un sujeto o a un objeto. Su símbolo es $\otimes$.

Algunos de los elementos mencionados se observan en la figura 6.3

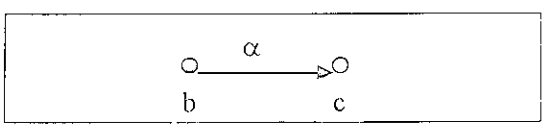


Figura 6.3. Elementos del modelo Take-Grant

Un modelo Take-Grant especifica un conjunto de reglas para transformar las gráficas de protección Estas reglas controlan la forma en la que los derechos pueden ser pasados de un sujeto a otro Al variar las reglas se obtienen diferentes modelos Take-Grant, por ejemplo, cuando se emplean las reglas Create (crear) y Remove (remover), el modelo indica cómo los vértices se *añaden* y se *quitan*, pero si se emplean las reglas Grant (conceder)

y Take (tomar), entonces se indica cómo un sujeto *concede* derechos a otro o cómo *adquiere* los derechos de otros.

En este modelo existen dos reglas principales:

a) **Regla Grant:** ésta añade una nueva línea (β) de un vértice (y) a otro (z), esto es posible porque un primer vértice (x) concede al segundo (y) la habilidad de crear la nueva línea (β) hacia el tercer vértice (z), esto se debe a que el primer vértice (x) concede el derecho al segundo (y) porque la línea (β) está incluida en los derechos del primero (x) sobre el tercer vértice (z) . La figura 6.4 representa esta regla.

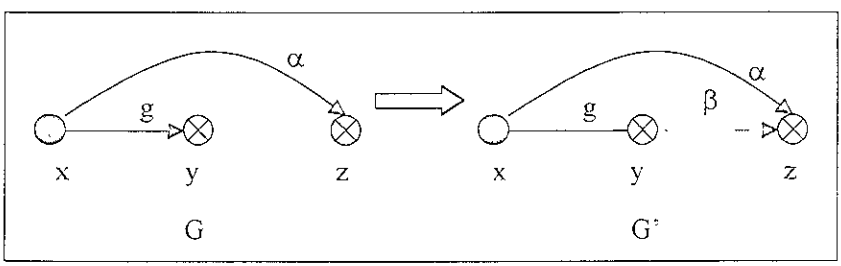


Figura 6.4. Regla Grant

b) **Regla Take:** añade una línea (β) del primer vértice (x) hasta el tercero (z), esto se debe a que el primer vértice (x) toma del segundo (y) el derecho de realizar la línea (β) hasta el tercero (z). Esta regla puede observarse en la figura 6 5

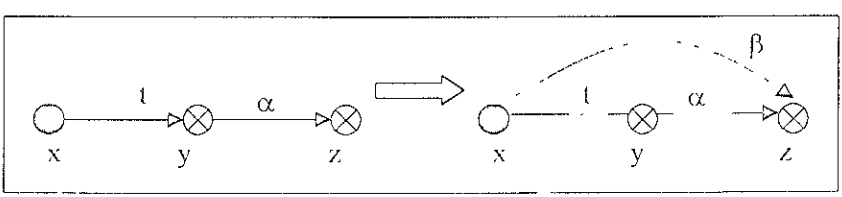


Figura 6.5. Regla Take

El modelo Take-Grant es más restrictivo debido a que tiene reglas particulares para transformar la gráfica de protección, lo cual logra que las decisiones de seguridad sean posibles

6.3.2.3 Modelo Bell-LaPadula

Una de las limitaciones del control de acceso discreto (DAC) es su vulnerabilidad a los ataques de los Caballos de Troya, esto se debe a que el Caballo de Troya se ejecuta con los derechos del usuario que lo invoca sin desearlo ni saberlo, por lo tanto el control de acceso es incapaz de protegerse contra esto. Para intentar resolver dicho problema, se recurre a un modelo mandatario de control de acceso (MAC), el cual restringe lo que pueden hacer los que autorizan. Este modelo recibe el nombre de Bell-LaPadula ya que fue desarrollado por D. E Bell. y L. J. LaPadula en 1976.

El modelo Bell-LaPadula (BLP) formaliza la política de seguridad multinivel (la política multinivel es aquélla que clasifica la información en cuatro niveles: no clasificado, confidencial, secreto y ultra secreto. La información es descrita en términos de compartimentos los cuales representan el asunto del sujeto. El nivel de seguridad o clase de acceso de un documento es la combinación de su nivel y conjunto de compartimentos Cualquier persona autorizada, recibe un permiso para un cierto nivel, de esta manera tanto las personas como la información, tienen niveles de seguridad o clases de acceso. La política indica que las personas pueden tener acceso a la información que se encuentra hasta su nivel autorizado) y esta política tiene como objetivo controlar el flujo de la información, el modelo también ayuda en la construcción de sistemas cuya seguridad puede ser verificada.

BLP es un modelo de máquina de estado como muchos modelos de seguridad de computadora donde se ve a los sistemas como una tripleta (S, I, F) donde se tiene un conjunto de estados S, un conjunto de posibles entradas I y una función de transición F que transfiere al sistema de un estado a otro

El modelo contiene los siguientes elementos:

a) **Sujetos**

b) Objetos

c) Modos de acceso: como leer y escribir

d) Niveles de seguridad

Un estado de seguridad se encuentra definido por tres propiedades que intentan expresar la política de seguridad:

a) **Propiedad de seguridad simple (ss-property):** expresa la política de autorización-clasificación.

b) **Propiedad estrella (star-property):** representa la política del flujo de información no autorizado de un nivel alto a uno bajo.

c) **Propiedad de seguridad discrecional:** refleja el principio de autorización y se expresa en una matriz de acceso.

Se observa que un estado del sistema satisface la propiedad de seguridad simple si para cada elemento del conjunto de acceso actual, el nivel de seguridad del sujeto domina el nivel de seguridad del objeto. La propiedad estrella se satisface si para cada acceso de escritura en el conjunto de acceso actual, el nivel del objeto es igual al nivel actual del sujeto y para cada acceso de lectura, el nivel del sujeto domina al nivel del objeto. Esta propiedad asegura que si el sujeto tiene acceso de lectura a un objeto y acceso de escritura a otro, entonces el nivel del primero se encuentra dominado por el nivel del segundo La propiedad estrella representa la política de que un sujeto no puede copiar información de un nivel más alto a un objeto de nivel inferior

El modelo BLP se ha utilizado como base para muchos sistemas concretos ya que estos modelos deben ser una interpretación válida del modelo abstracto BLP.

Algunas consideraciones del modelo son

1. **Limitaciones de los modelos de control de acceso:** un modelo de control de acceso sólo puede expresar de un modo general la política multinivel, es decir, un modelo de este tipo no puede ser tan preciso en este aspecto como lo es un modelo de flujo de información

2. **Restricciones de la propiedad estrella:** BLP prohibe el flujo de información de un alto nivel a uno inferior La suposición es que cualquier flujo es equivalente a fusionar diversas secciones

3. **Sujetos confiables:** el modelo muestra que no hay presiones sobre cómo los procesos confiables pueden violar la propiedad estrella, cada sistema que es desarrollado realiza sus propias reglas sobre lo que pueden realizar los sujetos confiables

4. **Estado incompleto del modelo:** el modelo BLP trabaja con el conjunto de acceso actual, el cual no modela de manera explícita las lecturas y escrituras actuales, para lo cual se necesitan modelos suplementarios que aseguren que las lecturas y escrituras sean consistentes con el conjunto de acceso actual.

5. **Canales encubiertos:** el modelo no trabaja con información que es transmitida de manera indirecta, mejor conocida como canales encubiertos. Un sujeto puede transmitir información a otro a través de recursos que estén compartiendo.

6. **Transición segura de estado:** un sistema puede ser seguro según el modelo BLP, pero aún muestra transiciones no seguras, este problema puede corregirse si se añaden al modelo condiciones necesarias para transiciones seguras del estado.

6.3.3 Modelos de flujo de información

Una meta de las políticas de seguridad es proteger la información. Los modelos de control de acceso se aproximan a dicha meta indirectamente, sin relacionarse con la información pero sí con objetos (tales como archivos) que contienen información.

Teoría de la información

La teoría de la información, la cual fue desarrollada por Claude Shannon para tratar con la comunicación, provee una visión sistemática de la información. La teoría de la información ha sido usada en los modelos de flujo de información y está relacionada con otros problemas y métodos de la seguridad de las computadoras.

La teoría de la información define la información en términos de incertidumbre. Al proporcionar información se elimina la incertidumbre. Por ejemplo: Una carrera entre tres competidores, con una categoría mayor, es más incierta que una carrera entre dos competidores. El concepto de la

entropía captura esta idea. Los elementos que considera la teoría de la información son:

a) **Entropía:** una variable aleatoria, tal como el resultado del lanzamiento de un dado, tiene un conjunto de posibles valores, tales como 1,2,3,4, 5 y 6. La entropía de una variable aleatoria depende de las probabilidades de dichos valores. Supongamos que X es una variable aleatoria y que toma un conjunto finito de valores con probabilidades:

$p_1, \ldots, p_k, \ldots, p_n$ La entropía H de X está definida como:

$$H(X) = \sum_k p_k \log_2 p_k \quad \text{o}$$

$$H(X) = \sum_k p_k \log_2 \left(\frac{1}{p_k} \right)$$

Ejemplo: Una carrera que tiene dos competidores, A y B, los cuales tienen las mismas posibilidades de ganar, así que la $P_A = 0.5$ y la $P_B = 0.5$ El log de (1/0.5) es igual a log de (2) por lo tanto el resultado es 1

Sustituyendo los valores en la fórmula de arriba, se tiene que:

H(X) = 0.5 x 1 + 0.5 x 1 = 1

La entropía es siempre una cantidad positiva El límite superior de H está dado por el log n

H es igual a log n cuando todas las probabilidades son iguales, como en el ejemplo La unidad de la entropía es un bit Cuando se aprende quién gana la mayoría de las carreras, se habría ganado un bit de información, el cual podría ser representado en una computadora por un campo de un bit Es decir, si se cuenta con

suficiente información y se tiene una probabilidad alta, la incertidumbre disminuye, lo cual ocasiona que la entropía aumente y finalmente indique la cantidad de bits que se ganan de información. La incertidumbre es inversamente proporcional a la entropía.

b) **Entropía Condicional:** un importante concepto para el modelo de flujo de información es la entropía condicional. La entropía condicional de X dado Y es una medida de la incertidumbre de X dado el conocimiento acerca de Y. Para cada valor y_j de Y, existe una entropía condicional de X dado y_j.

$$H(X \mid Y) = -\sum_k p\left(x_k \mid y_j\right) \log p\left(x_k \mid y_j\right)$$

donde $p(x_k \mid y_j)$ es la probabilidad condicional de que $X = x_k$ da a $Y = y_j$. La entropía condicional de X dado Y está definida como:

$$H(X \mid Y) = \sum_J H\left(X \mid y_J\right) p\left(y_J\right)$$

Esto es, H(X | Y) es la entropía de X dado un valor particular de Y, promediado sobre los posibles valores de Y.

La entropía condicional mide cuánta información de X puede obtenerse a través del conocimiento de Y. Si X y Y son independientes, el conocimiento de Y no tiene efecto en la entropía de X. La entropía condicional nunca puede ser mayor que la entropía.

c) **Canales:** un canal es una caja negra que acepta cadenas de símbolos desde alguna entrada alfabética y emite cadenas de símbolos desde alguna salida alfabética. La teoría de la información define diferentes tipos de canales

- Un *canal discreto* puede transmitir sólo símbolos desde un número finito de entradas alfabéticas

- En un *canal sin memoria* la salida es independiente de cualquier entrada o salida anterior.

- Un *canal discreto sin memoria* emite una cadena de la misma longitud que la cadena de entrada.

La capacidad de un canal es una medida de la habilidad del canal para transmitir información. Ésta es expresada (dependiendo del contexto) como un bit por segundo o bits por símbolo.

Un modelo enrejado del flujo de información

Una política del flujo de información define las clases de información que un sistema puede tener y cómo la información puede fluir entre esas clases. Un modelo de flujo de información desarrollado por Dorothy Denning puede expresar la política de multinivel en términos del flujo de información mejor que el control de acceso. Puede también expresar otras políticas más útiles. La política del flujo está definida por un enrejado.

Un enrejado es una estructura matemática que representa el significado de los niveles de seguridad. Un enrejado consiste de un conjunto extra, ordenado parcialmente, del menor límite superior (representado por el operador $\oplus$) y el mayor límite inferior (representado por el operador $\otimes$) En un modelo de flujo de información, el enrejado $(SC, \leq, \oplus, \otimes)$ representa un conjunto de clases de seguridad SC y una relación con la clasificación $\leq$ sobre las clases.

Si se tienen las clases A, B y C $A \leq B$ y $B \leq C$ implica que $A \leq C$

Una operación causa información del flujo de X a Y si se reduce la entropía condicional de X dado Y Esto es, la nueva información acerca de X puede obtenerse de Y. La cantidad de información que fluye es medida por la reducción en la entropía condicional $H(X \mid Y)$ Un flujo potencial es un canal cuya capacidad es la máxima información que puede ser transferida por el flujo

Una definición precisa de una restricción del flujo de información se encuentra en el concepto de no interferencia Un grupo de usuarios no interfiere con otro grupo si las acciones del primer grupo al utilizar ciertos

comandos no tienen efecto sobre lo que el segundo grupo puede ver. La no interferencia fue introducida por Joseph Goguen y José Meseguer entre 1982 y 1984.

Consideraciones en la seguridad del flujo de información

Debido a que la no interferencia restringe el flujo de información, se observan varios problemas:

1. Los sistemas son modelados como máquinas de estado determinísticas aunque los sistemas frecuentemente son diseñados sin determinismo.

2. Algunos problemas prácticos no pueden ser manejados, como la política de que la información puede fluir a un nivel más bajo al pasar por un degradador confiable.

3. La no interferencia no está permitida para la generación de datos de alto nivel desde entradas de bajo nivel.

4 La no interferencia es un requerimiento muy fuerte y los modelos deben ser capaces de expresar una medida cuantificada de interferencia

6.3.4 Modelos de integridad

Recordando que la integridad se refiere a que la información no sufre modificaciones si éstas no se autorizan, aunado a que es consistente internamente y con los objetos del mundo real que representa y que el sistema ejecuta correctamente, en términos generales, la integridad se define como toda la seguridad exceptuando la confidencialidad y la disponibilidad que son los principales tres factores que la componen

Los sistemas de integridad tienen que ver con la conducta del sistema de acuerdo a las expectativas aun cuando tengan que enfrentar ataques La integridad de los datos incluye dos tipos de consistencia, ya que éstos deben ser internamente consistentes y consistentes con las entidades del mundo real que representan Un concepto mas amplio de la integridad de los datos es la calidad de los datos, esta calidad incluye atributos como oportuno, genealogía y entereza

La integridad de los datos tiene las siguientes metas:

- Prevenir las modificaciones no autorizadas.
- Mantener la consistencia interna y externa.
- Mantener otros atributos de calidad de los datos.
- Prevenir las modificaciones autorizadas pero impropias.

Los modelos de integridad tienen como objetivo lograr estas metas Existen dos tipos de modelos:

6.3.4.1 Modelo Biba

Creado por K. J. Biba en 1977, el modelo de integridad supone un enrejado de niveles de integridad (análogo a los niveles de seguridad) con una relación ordenada menor o igual Los objetos son asignados a clases de integridad de acuerdo al daño que sufrirían si fueran modificados de manera inapropiada. Los usuarios son asignados a clases de integridad basados en su veracidad. Los compartimentos de integridad son interpretados como compartimentos de confidencialidad El nivel de integridad de un sujeto está basado en el nivel de integridad del usuario que representa y en sus necesidades, de acuerdo al principio del último privilegio.

Biba presenta varios modelos, todos basados en las mismas entidades pero representando diferentes políticas de integridad El modelo representa la política de integridad estricta el cual intenta ser un doble de la política de confidencialidad Bell-LaPadula. Las entidades del modelo son:

a) S, O, I: conjunto de sujetos, objetos y niveles de integridad.

b) il: una función que define el nivel de integridad de cada sujeto y objeto

c) leq: relación parcial ordenada sobre los niveles de integridad, menor que o igual

d) **min:** una función que regrese el límite inferior del conjunto de I especificado.

e) **o, m:** relaciones que definen la habilidad de un sujeto s para observar (o) o modificar (m) un objeto o

f) **i:** una relación que define la habilidad de un sujeto s_1 para invocar a otro sujeto s_2

La política de integridad estricta se caracteriza por tres axiomas.

1. Para que un sujeto observe a un objeto, el sujeto debe tener un nivel de integridad menor o igual que el nivel de integridad del objeto.

2. Para que un sujeto modifique un objeto, el objeto debe tener un nivel de integridad menor o igual que el nivel de integridad del sujeto

3. Para que un sujeto 1 invoque a un sujeto 2, el sujeto 2 debe tener un nivel de integridad menor o igual que el nivel de integridad del sujeto 1.

Los primeros dos axiomas indican que un sujeto no puede observar a un objeto de menor integridad y no puede modificar a un objeto de más alta integridad, el tercero establece que un sujeto no puede invocar a otro sujeto de más alta integridad, dicho axioma trata de prevenir al sujeto invocado de cualquier modificación indirecta de objetos de más alta integridad.

El modelo Biba prueba que bajo los axiomas de integridad estricta, si existe una ruta de transferencia de un objeto o_1 a un objeto o_{n+1} entonces el nivel de integridad del objeto o_{n+1} es menor o igual que el nivel de integridad del objeto o_1, lo cual indica que la información no se transmite a un nivel de integridad más alto

El modelo Biba no se ha utilizado mucho porque no corresponde a una política del mundo real establecida

6.3.4.2 Modelo de Clark-Wilson

El modelo de integridad de David Clark y David Wilson desarrollado entre 1987 y 1989 comenzó una revolución en la investigación de la seguridad informática. Aunque no es un modelo altamente formal, es un armazón para describir los requerimientos de la integridad. Clark y Wilson demostraron que para la mayoría del cómputo relacionado con las operaciones de negocios y el control de los recursos, la integridad es más importante que la confidencialidad. Ellos argumentaban que las políticas de integridad demandan modelos diferentes a los modelos de confidencialidad y diferentes mecanismos ya que se enfocan en dos controles que son centrales en el mundo comercial:

a) Las transacciones bien formadas.

b) Separación de la obligación.

Las entidades del modelo son:

1. **Elementos de datos restringidos (CDIs):** se trata de los elementos cuya integridad debe mantenerse.

2. **Procedimientos de transformación (TPs):** estos procedimientos del modelo representan las transacciones bien formadas, manipulan a los CDIs ya que transforman un conjunto de éstos de un estado válido a otro.

3. **Procedimiento de verificación de integridad (IVP):** tiene el propósito de confirmar que todos los CDIs están en un estado válido, esto es, ellos reúnen los requerimientos de integridad. El IVP sirve para la consistencia interna y para la consistencia con la realidad externa de acuerdo a la visión de esa realidad. La visión particular de la realidad es llamada dominio de integridad.

4. **Elementos de datos no restringidos (UDIs):** como datos de entrada son relevantes porque pueden ser transformados en CDIs.

El sistema debe asegurar que sólo los TPs pueden manipular a los CDIs. Los TPs y los IVPs deben estar certificados con respecto a una política

de integridad específica. Un TP debe reunir sus especificaciones y éstas deben ser correctas

El modelo cuenta con reglas que definen un sistema de aplicación de integridad, a continuación se mencionan estas reglas.

a) **Reglas de ejecución (E):** son de aplicación independiente, son fáciles de implementar en el sistema.

b) **Reglas de certificación (C):** envuelven el análisis humano y la decisión tomada hasta que alguna automatización sea posible.

Las reglas siguientes relacionan la consistencia interna y externa:

1. **C1:** todos los IVPs deben asegurar de manera apropiada que todos los CDIs están en un estado válido al momento de que el IVP está corriendo.

2. **C2:** todos los TPs deben estar certificados para ser válidos. Esto indica que transforman un CDI a un estado final válido, si el CDI está en un estado válido al inicio. Cada TP debe estar certificado para un conjunto específico de CDIs

3. **E1:** el sistema debe mantener una lista de las relaciones de la regla C2 y debe asegurar que cualquier manipulación de un CDI es mediante un TP y está autorizado por alguna relación

Las reglas adicionales que se necesitan para la separación de la obligación son:

1. **E2:** el sistema debe mantener una lista de relaciones que enlacen al usuario, al TP y los CDIs que el TP debe manipular a favor de ese usuario.

2. **C3:** la lista de relaciones de E2 debe estar certificada para conocer la separación de la obligación requerida

Otras cuatro reglas completan el modelo. Éstas especifican que:

1. **E3:** los usuarios que invocan TPs deben ser autenticados.

2. **C4:** todos los TPs deben certificar para que pueda tener acceso de entrada.

3. **C5:** los TPs que transforman UDIs a CDIs deben estar certificados.

4. E4: sólo ciertos usuarios designados deben especificar las relaciones

Estas reglas ejecutan una política obligatoria de integridad.

Este armazón para la integridad conlleva a un conjunto de requerimientos para los servicios de seguridad informática:

a) **Cambio de registros y etiquetas de integridad:** la autoría debe ser guardada con los datos (para soportar la política de atribución de cambio), la etiqueta de integridad registra que los datos fueron certificados por un IVP y qué dominio de integridad fue utilizado

b) **Soporte del acceso triple:** para ejecutar la política de cambio restringido, el control de acceso triple enlaza al usuario, al programa y a los datos

c) **Autenticaciones mejoradas de usuarios:** aunque la autenticación es necesaria para la confidencialidad, tiene una importancia especial para la integridad en particular con la política de separación de la obligación Las contraseñas son inadecuadas, ya que pueden ser reveladas u observadas, permitiendo así que alguien actúe como dos personas diferentes, violando las reglas de separación de la obligación

d) **Control de los usuarios privilegiados:** la separación de la obligación debe ser ejecutada por la gente que mantiene los accesos triples o quienes certifican TPs

e) **Control del programa de aplicación:** un sistema necesita herramientas automatizadas para manejar las aplicaciones de software y asegurar su integridad.

f) **Separación dinámica de la obligación relacionada a los TPs:** la separación de la obligación seguido requiere que los diferentes pasos en una secuencia se cumplan por diferentes personas. Aunque una tarea estática puede reunir este requerimiento, un acercamiento más flexible es para que el sistema mantenga la pista de quién ha ejecutado cada paso y realizar la separación de la obligación a cada paso. Esto es parecido a lo que pasa en el mundo real.

Lecturas recomendadas

[46]. IV. Políticas de seguridad

[58]. Chapter 4. Policies and models.

CAPÍTULO 7.
MECANISMOS DE SEGURIDAD

Los mecanismos de seguridad son el tercer aspecto que se considera en la seguridad de la información – cabe recordar que el primer aspecto es el ataque de seguridad y el segundo los servicios de seguridad.

Un **mecanismo de seguridad** es una técnica que se utiliza para implementar un servicio, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o recobrarse de un ataque de seguridad. Los mecanismos de seguridad implementan varios servicios básicos de seguridad o combinaciones de estos servicios básicos – los servicios de seguridad especifican "qué" controles son requeridos y los mecanismos de seguridad especifican "cómo" deben ser ejecutados los controles.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los diferentes servicios de seguridad. Conviene resaltar que los mecanismos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, y generación de números aleatorios
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo

No existe un único mecanismo capaz de proveer todos los servicios, sin embargo, la mayoría de ellos hace uso de técnicas criptográficas basadas en el cifrado de la información. Los mecanismos pueden ser clasificados como preventivos, detectivos, y recuperables.

7.1 Tipos

Los mecanismos de seguridad se pueden clasificar en dos categorías:

a) Mecanismos de seguridad generalizados

b) Mecanismos de seguridad específicos

Mecanismos de seguridad generalizados

Los mecanismos de seguridad generalizados se relacionan directamente con los niveles de seguridad requeridos y algunos de estos mecanismos están relacionados al manejo de la seguridad, es decir, a la administración de seguridad y permiten determinar el grado de seguridad del sistema ya que se aplican a éste para cumplir la política general.

Dentro de este tipo se encuentran:

1. **Funcionalidad de confianza:** es utilizada para extender los otros mecanismos de seguridad. La funcionalidad digna de confianza puede proveer protección de asociaciones encima de la capa en la cual la protección es aplicada o ejercida, con esto permite determinar el grado de confianza de un determinado servicio o persona.

2. **Etiquetas de seguridad:** se asocian a los recursos para indicar el nivel de sensibilidad, se trata de números que permiten graduar la sensibilidad de determinados datos clasificando la información por niveles de seguridad secreta, confidencial, no clasificada, etc. Estas etiquetas pueden ser transmitidas con los datos o pueden estar implícitas. Ejemplos de etiquetas de seguridad implícitas son aquéllas implicadas en el uso de una clave específica para cifrar los datos

3. **Detección de eventos:** incluye la detección de violaciones de la seguridad y de manera opcional la detección de eventos normales como el acceso realizado de manera exitosa La detección de eventos puede accionar una o más acciones como el reporte local de un evento, el reporte remoto de un evento, la terminación del evento y la acción recobrada, es decir, este mecanismo detecta movimientos peligrosos o normales dentro del sistema

4. **Seguimiento de auditorías de seguridad:** cualquier seguimiento se refiere a resúmenes independientes y análisis de los registros tanto del sistema como de las actividades datos que se adquieren y que potencialmente facilitan las auditorías sobre seguridad El propósito de un seguimiento de auditoría de seguridad es probar que tan adecuados son los controles del sistema para asegurar la complacencia de las políticas establecidas y los procedimientos operacionales Una auditoría de

seguridad envuelve los registros de información relevante de seguridad y el análisis de la información obtenido en un seguimiento de auditoría de seguridad.

5. **Recuperación de seguridad:** toma acciones para satisfacer las peticiones de los mecanismos como el manejo de los eventos y las funciones de administración, es decir, realiza acciones de recuperación basadas en la aplicación de una serie de reglas. Las acciones de recuperación pueden ser inmediatas – como la desconexión –, temporales – invalidación temporal de una entidad – o de largo plazo – intercambio de clave

Mecanismos de seguridad específicos.

Los mecanismos de seguridad específicos definen la implementación de servicios concretos. Los más importantes son los siguientes

7.1.1 Intercambio de autenticación

Mientras que la autenticación física es más fácil, en lo que respecta a la autenticación a través de la red, ésta no lo es debido a que la comprobación visual no es práctica sobre las redes porque la *persona no está allí* La autenticación tiene como meta principal obtener un *muy elevado grado de confianza* sobre el intercambio de información

El mecanismo de intercambio de autenticación trata con la autenticación de las entidades de la red. Hace uso de información de autenticación, técnicas criptográficas y características y/o posesiones de la entidad.

El mecanismo de intercambio de autenticación se utiliza para verificar la supuesta identidad de quienes envían los mensajes y/o los datos, corroborando así que una entidad, ya sea origen o destino de la información, es la deseada. Los mecanismos de este tipo pueden ser

a) **Fuertes:** comúnmente llamados de autenticación fuerte porque emplean técnicas criptográficas propiedades de los sistemas criptográficos de clave publica para proteger los mensajes que se van a intercambiar Un usuario se autentica mediante su identificador y su clave privada Su interlocutor debe verificar que aquel, efectivamente, posee la clave privada, para lo cual debe obtener de algún modo, la clave pública de

primero. Para ello deberá obtener su certificado, un certificado es un documento firmado por una Autoridad de Certificación (una tercera parte de confianza) y válido durante el período de tiempo determinado, que asocia una clave pública a un usuario.

b) **Débiles:** generalmente llamados de autenticación simple ya que se basa en técnicas de control de acceso. El emisor envía su identificador y una contraseña al receptor, el cual los comprueba.

Este mecanismo funciona de la siguiente manera: se corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, la computadora *A* envía un número aleatorio cifrado con la clave pública de la computadora *B*, *B* lo descifra con su clave privada y se lo reenvía a *A*, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos mecanismos, ya que existen ataques para desbaratarlos

Debe ser utilizado con sellos de horario, relojes sincronizados y servicios de no repudio.

7.1.2 Integridad de datos

Los mecanismos de integridad de datos aseguran que los datos no sean alterados o destruidos. Estos mecanismos tratan con la integridad de una unidad o campo de datos simples y la integridad de una secuencia de unidades o campos de datos

La manera en que funciona el mecanismo de integridad de datos implica el cifrado de una cadena (compactada) de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV) Este mensaje se envía al receptor junto con los datos ordinarios El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados

Existen dos procesos para determinar la integridad de una unidad o campo de datos simples El primer proceso genera un valor en la entidad emisora y lo adiciona a la unidad o campo de datos Este valor es un código de verificación de datos o una cantidad criptográfica que se calcula en función de los datos y que se manda como información suplementaria El segundo proceso genera el valor

correspondiente de la unidad o campo de datos recibido en la entidad receptora, y lo compara con el valor recibido.

Para la integridad de una secuencia de unidades o campos de datos, se requieren protecciones adicionales. Si la transferencia de datos está en modo de conexión, la orden explícita como la secuencia numérica, sellos de tiempo o la cadena criptográfica deben ser utilizados, si la transmisión de datos es sin conexión, una forma limitada de protección contra el reenvío de unidades individuales de datos se puede proporcionar a través sellos de tiempo.

Para resguardar la integridad de los datos se puede realizar una auditoría a los datos Esta herramienta, la auditoría, se tomó del mundo real cuando las compañías emplean auditores externos para asegurar que sus libros de contabilidad afirmen correctamente la posición fiscal de la compañía. La auditoría puede ser una herramienta valiosa para mantener los sistemas y la integridad de los datos también en el mundo real de la red

7.1.3 Firma digital

En los sistemas con clave pública, cualquier persona puede cifrar un mensaje, y solamente el destinatario del mensaje puede descifrarlo Invirtiendo la manera del uso de las claves públicas se tiene un mensaje que sólo puede ser cifrado por una persona y descifrado por cualquier otra, obteniéndose así un efecto de personalización del documento semejante a una firma. Un sistema de ese tipo es denominado **firma digital** La firma digital se puede definir como un conjunto de datos – como códigos o claves criptográficas privadas – que se añaden a una unidad de datos de modo que protejan a ésta contra cualquier falsificación, permitiendo al receptor comprobar el origen y la integridad de los datos. Para ello, se cifra la unidad de datos junto con alguna componente secreta del firmante y se obtiene un valor de control ligado al resultado cifrado

La manera en que funciona la firma digital se describe a continuación para personalizar un mensaje, un determinado usuario *A (Alicia)* cifra un mensaje utilizando su clave secreta y lo envía al destinatario Únicamente la clave pública de *A (Alicia)* permitirá descifrar el mensaje, por lo tanto, se comprueba que efectivamente *A (Alicia)* fue quien envió el mensaje Un mensaje así puede ser descifrado por cualquiera que tenga la clave pública de *A (Alicia)*

Una firma digital tiene las siguientes ventajas

a) **La firma es auténtica:** porque cuando un usuario usa una clave pública de *A* para descifrar un mensaje, él confirma que fue *A* y solamente *A* quien envió el mensaje.

b) **La firma no puede ser violada:** porque solamente *A* conoce su clave secreta.

c) **El documento firmado no puede ser alterado:** porque en caso de existir cualquier alteración en el mensaje cifrado, éste no podría ser restaurado (descrifrado) con el uso de la clave pública de *A*

d) **La firma no es reutilizable:** debido a que la firma es una función del documento y no puede ser transferida para otro documento.

La firma digital, aunque tiene varias ventajas y cada usuario tenga un par de claves únicas, existe el riesgo de que se presente un ataque a la integridad de los datos. En caso de que se cometa un ataque, el receptor no puede estar seguro de que el emisor del mensaje realmente lo envió Para verificar que efectivamente el emisor envió el mensaje y utilizó su clave privada, existen las Autoridades de Certificación

Cuando se firma un documento en papel, se tiene entendido que

- La firma compromete a lo estipulado en el documento.
- El documento no se cambiará después de la firma
- Su firma no se transferirá a otro documento.

Hay leyes y convenciones que hacen estas suposiciones válidas en el mundo real, mientras que para el mundo de la red se necesita también una convención para asegurarse de que el mensaje no ha sido cambiado (integridad de datos) e impedir que alguien, simplemente, pase la firma a otro documento que nunca se ha destinado para firmar

Lo anterior, podría hacerse usando la clave privada para cifrar el documento entero Sin embargo, el proceso consumiría demasiado tiempo-máquina cuando se utilicen algoritmos de claves públicas Existen algoritmos que reducen documentos al mismo y este tipo de algoritmo se le conoce como "mensaje reducido" y es una

manera de confundir al atacante. Estos algoritmos se usan para tomar cualquier tamaño de documento y crear una reducción única, la cuál tendrá siempre la misma longitud.

Un mensaje reducido no puede revertirse, por lo tanto, alguien debe tener el documento original que creó la reducción. Desde estas reducciones que son bastante pequeñas, toma mucho menos tiempo para cifrar la reducción con un algoritmo de clave privada y una clave pública.

La firma digital basada en la reducción funciona de la siguiente manera:

1. El emisor crea una reducción del mensaje y cifra dicha reducción (usando la clave privada)

2. Después firma el documento, es decir, cifra el mensaje original (usando la clave privada)

3. Tanto el mensaje cifrado, que está contenido en el documento firmado, como la reducción cifrada se envían al destinatario

4 El destinatario aplica la clave pública, del remitente (emisor), a las dos firmas digitales que recibió (la firma digital que contiene el mensaje original y la firma digital que contiene la reducción del mensaje).

5 Después el destinatario crea una nueva reducción del mensaje utilizando el mensaje original que recibió y compara la longitud obtenida, con la longitud de la reducción que estaba dentro de la firma digital. Si las longitudes de las reducciones son iguales, entonces el mensaje fue verdaderamente enviado por el remitente y ha llegado sin haber sido alterado.

Todos los pasos mencionados, son usados por el software para firmar y enviar, o recibir y verificar. El usuario puede ver algún indicio sobre la pantalla de que estas acciones se están realizando, pero las tareas son totalmente automatizadas. El usuario simplemente ve el documento que recibe y verifica.

Se puede enviar un mensaje a alguien y tener la confianza de que no será cambiado. Si no se quiere que alguien sea capaz de leer el mensaje, se puede cifrar tanto el mensaje como la firma para protegerlos.

El mecanismo de firma digital soporta los siguientes servicios de seguridad:

a) **Autenticación:** la seguridad de que el remitente es el único que pudo haber enviado el mensaje.

b) **Integridad del mensaje:** la seguridad de que el mensaje llegó sin cambios durante el trayecto.

c) **No repudio:** porque el par de claves son únicas, la confianza de que sólo el remitente pudo haber firmado la reducción del mensaje, el remitente no puede negar que envió el mensaje.

Para que se pueda proporcionar el servicio de no repudio con prueba de entrega, hay que forzar al receptor para que envíe un acuse de recibo firmado digitalmente.

7.1.4 Control de acceso

El mecanismo de control de acceso se utiliza para autenticar las capacidades de una entidad para acceder a un recurso dado, se puede llevar a cabo en el origen o en un punto intermedio, y se encarga de asegurar que el emisor está autorizado a comunicarse con el receptor o a usar los recursos de comunicación Este mecanismo soporta el servicio de control de acceso y está muy ligado a la autenticación y confianza

Detrás de este mecanismo de seguridad es importante la "confianza" En el mundo de la red, la "confianza" es la capacidad para autenticar a las compañías y a los individuos que intercambian información a través de la red, además es un punto fuerte en el comercio, mientras que en el mundo real, es más fácil autenticar a las compañías y a los individuos con quienes se tiene una relación establecida o con quienes son presentados por alguien de confianza

Por ejemplo, si se observa un librero que está tambaleante, no se podrá confiar en que pueda resistir el peso cuando se pongan más libros La confianza en la seguridad de la red es exactamente lo mismo Si los mecanismos que actualmente se utilizan para la autenticación, confidencialidad, integridad y no repudio, no se aplican en forma robusta para los usuarios, ellos dudarán en usarlos Hoy en día uno de los problemas mas grandes de confianza sobre la red es que la

gente simplemente no comprende el término confianza[16] o lo confunde con el término confidencial[17]. Este problema de comprensión es una barrera crítica que debe superarse.

Generalmente, la confianza se aplica también en la confidencialidad. Por ejemplo, la gente no depositará dinero, en una institución financiera, que no emplea una adecuada protección contra los ladrones que intenten robar los fondos del banco Lo mismo es aplicado para la integridad de datos: si un consumidor teme que un producto pudo haber sido alterado después de la fabricación, él no lo comprará

7.1.5 Tráfico de relleno

El tráfico de relleno – también conocido como mecanismo de relleno de tráfico – es un mecanismo que provee una generación de tráfico falso, esto se logra enviando por la red mensajes sin contenido (basura) para obtener un flujo constante de mensajes – un tráfico constante – o la longitud del mensaje constante, esto significa que se envía tráfico falso junto con los datos válidos, esto es de gran valía ya que en una situación en la que haya necesidad de mantener un vasto intercambio de información entre nodos que regularmente apenas si tienen alguna comunicación ocasional, el incremento de actividad en el canal podría entonces ser motivo de un análisis de tráfico por parte de atacantes para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo, dificultando así el análisis de flujo de tráfico ya que inyectan tráfico sin información en las redes para confundir a los observadores de la red

Este mecanismo evita que alguien que conozca la estructura obtenga información de una determinada posición tras realizar un análisis del flujo de datos Cualquier mecanismo de tráfico de relleno se usa para proteger contra ataques de análisis de tráfico Se llaman rellenos porque consisten en generar eventos de comunicación, unidades de datos y datos falsos, en forma semi-aleatoria, con el fin de "confundir" a un analizador de tráfico Lo que hace el tráfico de relleno es generar una salida de texto cifrado continuamente, incluso en ausencia de texto original, de este modo es imposible que un atacante distinga entre el flujo de datos verdadero y el ruido, con lo que resulta imposible deducir la cantidad de tráfico real

[16] Confianza: creer, tener firme esperanza en una persona o cosa
[17] Confidencial: que se hace en secreto

El mecanismo de tráfico de relleno puede ser utilizado para proveer varios niveles de protección contra el análisis de tráfico.

7.1.6 Control de encaminamiento

El control de encaminamiento también es conocido como control de ruta, como su nombre lo indica, está destinado a seleccionar de manera física cada una de las rutas alternativas que pueden utilizarse según el nivel de seguridad y la información que se esté transmitiendo ya que permite enviar determinada información por ciertas zonas que se consideran clasificadas o calificadas para llevar a cabo la transmisión de la información, es decir, este mecanismo de seguridad cubre todos los aspectos de la ruta que siguen los datos en la red.

Este mecanismo permite que se soliciten y utilicen otras rutas para el envío de datos, en caso de que se detecten continuas violaciones de integridad en una ruta determinada. El control de encaminamiento, durante el proceso de conmutación, selecciona para una cierta comunicación determinados enlaces, redes o repetidores, buscando una mayor confidencialidad, para esto se lleva a cabo una recodificación de rutas y tablas del sistema para evitar líneas o máquinas comprometidas Cualquier mecanismo de control de encaminamiento se usa para lograr la selección dinámica o pre-establecida de rutas específicas para la transmisión de datos, por esto, a los datos con determinadas etiquetas de seguridad se les prohibe pasar por ciertas subredes o líneas. Algunos mecanismos, más sofisticados, de este tipo incluso reaccionan ante la insistencia de ataques a una ruta determinada, dejando esta ruta fuera de las posibles selecciones.

Los sistemas finales establecen una conexión por medio de una ruta diferente para prevenir los ataques constantes de manipulación. Las rutas preestablecidas a través de redes físicamente seguras suelen escogerse en lugar de las rutas dinámicas

7.1.7 Unicidad

La unicidad consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se logra que la información tenga una secuencia única, esto evita que los datos enviados sean reacomodados o repetidos

7.1.8 Cifrado

El cifrado puede realizarse mediante el uso de sistemas criptográficos simétricos o asimétricos y puede aplicarse extremo a extremo o a cada enlace del sistema de comunicaciones.

El mecanismo de cifrado soporta el servicio de confidencialidad de los datos y puede complementar a otros mecanismos para conseguir diversos servicios de seguridad. El cifrado es la clave del mecanismo de seguridad que puede proveer confidencialidad a los datos o al flujo de tráfico. Aquí se hace uso de la criptografía ya que ésta envuelve los principios, significados, y métodos para la transformación matemática de los datos para esconder los contenidos de información, previniendo así la alteración o el uso no autorizado. Este mecanismo es requerido por muchos sistemas de seguridad y puede ser usado como parte de un cifrado, integridad de datos, autenticación de los datos y almacenaje de la contraseña.

El cifrado garantiza que la información es secreta para individuos, entidades o procesos no autorizados – confidencialidad. Un algoritmo de cifrado puede ser reversible o irreversible Un algoritmo de cifrado consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado.

Un algoritmo de cifrado reversible simétrico utiliza una clave de cifrado secreta y el conocimiento de esta clave implica el conocimiento de la clave de descifrado, esto es, cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el sistema criptográfico es simétrico Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos Se pueden dividir en dos categorías: cifradores de bloque, que cifran los datos en bloques de tamaño fijo – generalmente bloques de 64 bits –, y cifradores en flujo, que trabajan sobre flujos continuos de bits

Un algoritmo de cifrado irreversible asimétrico utiliza una clave pública y el conocimiento de esta clave no implica el conocimiento de la clave privada para el descifrado, esto es, cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el sistema criptográfico es asimétrico o de clave pública Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, puede ser conocida por todos De forma general, las claves públicas se utilizan para cifrar y las privadas para descifrar El sistema tiene la propiedad de

que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los sistemas criptográficos de clave pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales.

7.1.9 Notarización

El mecanismo de notarización provee los elementos necesarios para asegurar las propiedades de la comunicación de datos entre dos o más entidades, como la integridad de datos, origen, tiempo y destino. Esto es provisto por una tercera entidad de confianza – llamado notario, el cual tiene credibilidad por las entidades comunicantes y tiene la información necesaria para proveer el seguro requerido de una forma que puede ser testado – que realiza la certificación para asegurarse de ciertas propiedades de los datos comunicados entre las entidades El mecanismo de notarización también es conocido como mecanismo de certificación ya que se recurre a terceras personas físicas o jurídicas que confirman la seguridad de procedencia e integridad de los datos además garantizan el origen, el destino, las entidades involucradas, el tiempo de tránsito, etc

Cada instancia de comunicación debe ser protegida utilizando una firma digital, cifrado, integridad o cualquiera de los mecanismos que sean apropiados para los servicios de notariado. Los datos son comunicados entre las entidades mediante este tipo de instancia de protección cuando un mecanismo de notarización es utilizado ya que el uso de las redes está llegando a ser socialmente más aceptable, lo que constituye parte del problema sobre la seguridad en las redes, en donde nadie realmente conoce con quiénes se comunican Sin embargo, los bancos, las compañías de tarjetas de crédito, y corporaciones importantes, están desarrollando activamente una herramienta que permite a la gente aplicar la firma digital para asegurar que éstas, en un momento dado, sirvan dentro del tribunal de leyes

Los bancos y los prestamistas no solamente son los únicos interesados en las firmas electrónicas. Muchas compañías están experimentando con firmar todo documento en la red (Internet) desde un correo electrónico Las firmas pueden proveer un nivel de integridad y no repudio que interesa para cualquier inquietud de falsificación de datos

Se necesita que alguien de fe de la identidad del remitente Además, se debe tener alguna forma para enlazar a una persona u organización a la clave privada La

solución a este problema está en tener a otra persona que "certifique" que la clave privada pertenece al remitente.

El vínculo de identidad que posee la clave particular se ha hecho usando un "certificado" que da testimonio de la identidad del propietario, que es emitida por una **Autoridad de Certificación** – una organización que verifica las identidades y emite los certificados que comprometen al par de claves de esa identidad.

Las funciones primarias de una Autoridad de Certificación son:

- Aceptar aplicaciones para certificados.
- Verificar la identidad de la persona o la compañía empleada para el certificado.
- Emitir certificados.
- Revocar certificados
- Proveer la información del estado sobre los certificados que se han emitido

Lecturas recomendadas

[7] Ataques, servicios y mecanismos de seguridad

[10]. Certificación

[15]. Control de acceso

[27] Firma digital

[29]. Glosario de términos de criptología

[32]. Integridad de datos

[33]. Intercambio de autenticación

[35]. Chapter 3 Security Architecture Standard:
3.4 Security mechanisms

[36] Mecanismos de seguridad

[37] Mecanismos de seguridad

[38] Mecanismos de seguridad

[39] Mecanismos de seguridad

[40] Mecanismos de seguridad

[41] Mecanismos de seguridad

[42] Mecanismos de seguridad

[43] Mecanismos de seguridad

[44] Mecanismos de seguridad

[51] ¿Que mecanismos de seguridad existen?

[52]. Seguridad en Internet

[56]. Servicios y Mecanismos de seguridad

[57]. Chapter 1. Introduction:
1.1 Attacks, services and mechanisms

[58]. Chapter 1. Introduction
Framework for technical safeguards

A mediados de los 90's, el número de entradas a Internet fue creciendo en un 70% cada año[18]. Tan pronto como el potencial de Internet para el comercio electrónico se volvió evidente, la vulnerabilidad de Internet se convirtió en la noticia primordial. Internet conecta muchos anfitriones que están configurados y administrados de manera insegura y eso minimiza el uso de medidas para evitar cualquier ataque. Muchos de los delitos se deben a la vulnerabilidad de los proveedores, de los sistemas que no están bien configurados y de las claves de acceso por omisión o que son fáciles de adivinar

8.1 Vulnerabilidades

Los protocolos TCP/IP (Transmission Control Protocol/ Internet Protocol) protegen contra algunas amenazas; pero esta suite de protocolos no está desarrollada con ese fin, ahora bien, algunas sumas de comprobación protegen contra las modificaciones que puedan existir en las cabeceras de los paquetes, y aun cuando en TCP, la secuencia de los números protegen contra los paquetes perdidos o duplicados y otras medidas protegen contra el reuso de los paquetes, las protecciones son débiles, además TCP se encarga sólo de formar los paquetes en salida y reensamblarlos en llegada, el envío de éstos queda a cargo de IP, el usuario no puede determinar la ruta por la que deberán transitar los paquetes, ni siquiera existe la posibilidad de especificar por donde precisamente es que no deben pasar (por razones de seguridad), aunado a esto los paquetes IP no acarrean autenticadores de su carga de datos (una debilidad corregida en la nueva versión de IP) No existe un lugar común para la identificación y autenticación de la información o los servicios Para la mayoría, las aplicaciones deben realizar su propia autenticación. La autenticación del Telnet y FTP recae en las contraseñas transmitidas en el texto en claro, ambos son riesgosos para un anfitrión que no está bien asegurado. Las aplicaciones y los accesorios son más fáciles de explotar. De manera que Internet es una red inherentemente insegura, desde su desarrollo la seguridad no fue un objetivo que se persiguiera

Las principales vulnerabilidades son las siguientes:

1. **Suplantación de IP** Muchos ataques de Internet se basan en la suplantación de IP, la cual permite que un anfitrión se disfrace como otro

[18] Summers, Rita *Secure Computing: Threats and Safeguards* EUA, Mc Graw Hill, 1997, p. 56

Un paquete es enviado por un anfitrión, pero la dirección fuente en el paquete es la de otro anfitrión Esto es peligroso ya que las aplicaciones comúnmente utilizan las direcciones fuente para identificar las peticiones de los anfitriones que son confiables, De esta forma el atacante en el anfitrión *A*, de quien el destino es el anfitrión *B*, suplanta al anfitrión *T* el cual es confiable para *B*. Un ataque común explota una característica IP llamada **encaminamiento de fuente**, la cual permite al emisor de un paquete especificar su ruta y la ruta de regreso. Si la ruta es *A, B, C*, entonces *C* debe utilizar la ruta de regreso *C, B, A*. Para que el ataque sea exitoso, el paquete enviado desde *A* debe parecer que fue enviado desde *T*, además, si el ataque es para completar algo, la réplica de *B* debe dirigirse a *A* no a *T*. Primero el atacante toma control del anfitrión *A* y cambia su dirección IP a *T*, entonces envía un paquete a *B*, especificando la ruta de la fuente con *A* como último trayecto de la ruta. El anfitrión *B* acepta la petición como si viniera de *T* y reenvía su paquete hacia *A* Un firewall puede proteger una red interna contra los ataques de suplantación de IP mediante el rechazo de los paquetes entrantes direccionados desde cierta fuente Los anfitriones dentro del firewall no deben especificar a algún anfitrión externo para que sea confiable y el firewall debe rechazar cualquier paquete entrante cuya dirección fuente se encuentra dentro de la red interna El firewall debe bloquear los paquetes salientes cuya dirección fuente no está dentro de la red interna, esto es para evitar que se convierta en el origen de un ataque

2. **Conexiones secuestradas:** un atacante que gana el control de una sesión activa gana los derechos del usuario legítimo. La autenticación y los servicios de control de acceso no son útiles ya que se toma posesión de la sesión después de la autenticación y de que el control de acceso asume que el usuario es el que está autenticado En los sistemas UNIX en Internet el atacante penetra al sistema utilizando cualquier método, modifica el kernel para permitir el secuestro de cualquier sesión activa

3. **Ataques por husmeo:** Internet ha sufrido ataques que recolectan contraseñas u otra información que puede ser utilizada por usuarios no autorizados A estos ataques se les llama **ataques por husmeo** ya que utilizan herramientas monitoras de red llamadas husmeadoras (sniffers) El monitoreo se basa en una característica de interfase de red llamada modo promiscuo, la cual es útil para la administración de la red pero no para la seguridad. Una computadora cuya unidad de interfase de red se

encuentra en modo promiscuo puede leer todos los paquetes que pasan por la red. Un atacante que tome posesión de una computadora así, ejecuta un programa que captura los primeros datos transmitidos para cada sesión de la red (como el Telnet y el FTP). Los datos incluyen el nombre del anfitrión remoto, el nombre de la cuenta y la contraseña.

8.2 Firewalls

Un firewall es un conjunto de componentes de hardware – un encaminador, un anfitrión, una combinación de encaminadores, computadoras, redes – que están configurados específicamente para proteger la información que fluye entre dos redes, lo cual indica que un firewall refuerza la política de control de acceso entre dos redes. Ver figura 8.1

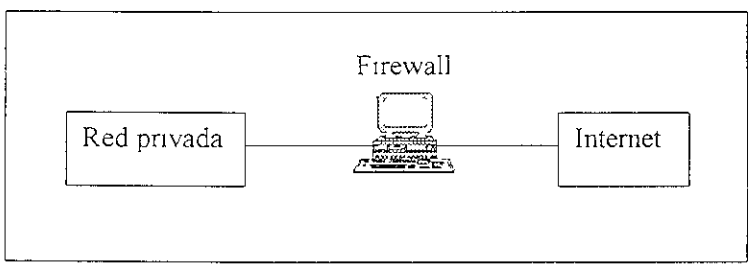


Figura 8.1. Firewall

Un firewall puede clasificarse dentro de uno de los siguientes tipos o como una combinación de los mismos

a) **Filtrado de paquetes:** el sistema de filtrado de paquetes encamina paquetes entre anfitriones internos y externos, pero de manera selectiva Permite bloquear cierto tipo de paquetes de acuerdo con la política de seguridad de la red El tipo de encaminamiento usado para filtrar paquetes en un firewall es conocido como *encaminamiento de protección* el paquete es analizado detalladamente y se determina si éste puede ser encaminado o no a la dirección destino y si debe o no ser encaminado con base en la política de seguridad Realizar el encaminamiento y la decisión de encaminar es la única protección al sistema Si la seguridad falla, la red interna esta expuesta Un encaminamiento de protección puede permitir o denegar un servicio, pero no puede proteger operaciones

individuales dentro del servicio. Las firewalls de este tipo trabajan a nivel de red ya que generalmente, toman las decisiones basándose en el origen, dirección de destino y puertos que leen en la cabecera de los paquetes IP Ejemplos de un firewall de este tipo son:

1. **Firewall de anfitrión protegido:** se accede a y desde un único anfitrión el cual es controlado por un encaminador que está operando a nivel de red. El anfitrión es como una defensa, dado que está muy protegido y es un punto seguro para refugiarse contra los ataques. Este tipo de firewall se observa en la figura 8.2

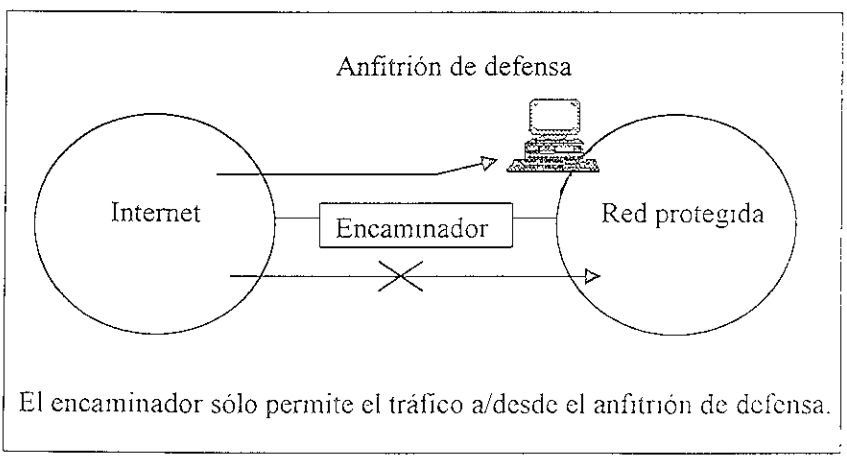


Figura 8.2. Firewall de anfitrión protegido

2. **Firewall de subred protegida:** se tiene acceso a y desde una red, la cual es controlada por un encaminador que opera a nivel de red Ver figura 8 3

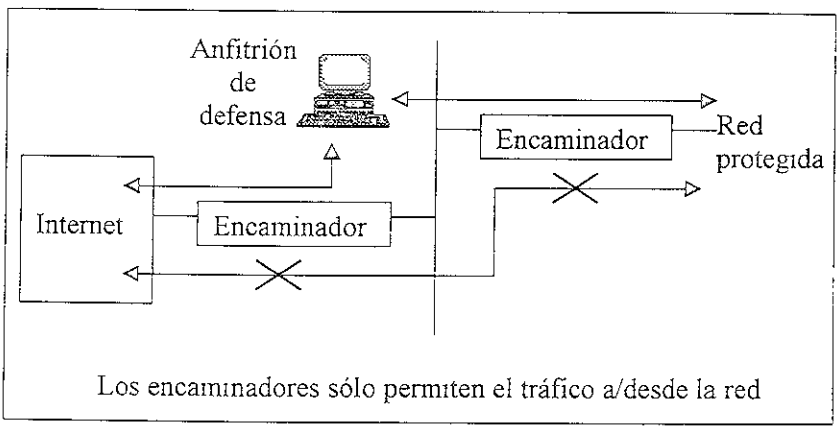


Figura 8.3. Firewall de subred protegida

b) **Servicio proxy:** son aplicaciones o programas servidores intermediarios entre anfitriones internos de una red y los anfitriones de Internet de tal forma que reciben las requisiciones de unos y se las pasan a los otros previa verificación de accesos y privilegios Los firewalls de este tipo trabajan a nivel de aplicación pues generalmente son anfitriones que corren bajo servidores proxy que no permiten tráfico directo entre redes y que auditan el tráfico que pasa a través de ellas Ejemplo de un firewall de este tipo

I **Gateway doblemente dirigido:** es un anfitrión de alta seguridad que corre bajo software proxy Consta de dos interfaces de red - cada una se encuentra conectada a una red diferente -, éstas actúan generalmente como bloqueo o filtrador de parte o del total del tráfico que intenta pasar La figura 8 4 muestra este tipo de firewall

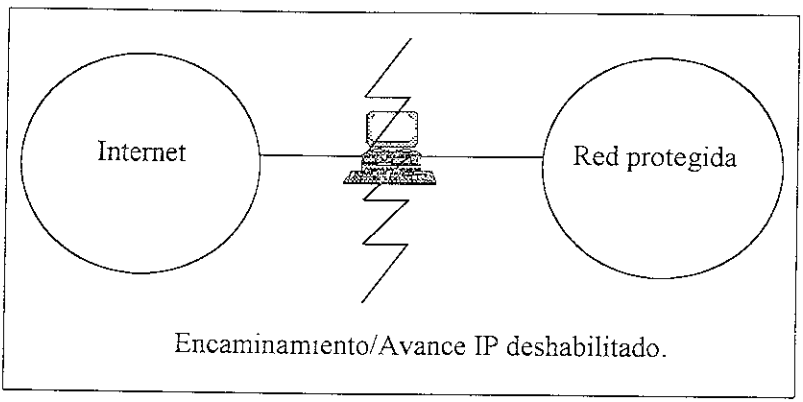


Figura 8.4. Gateway doblemente dirigido

Un firewall en un edificio provee una barricada de fuego entre partes del edificio, haciendo que una parte sea más resistente al fuego y evite que se disperse a otras partes. De manera similar, un firewall de red está construido alrededor de una red o subred para protegerla del exterior Tal como un firewall de un edificio debe tener puertas, el firewall de la red debe tener aberturas que permitan de manera selectiva el paso de información Steven Bellovin y William Cheswick (1994) definen un firewall como una colección de componentes colocados entre una red interna y una red externa para alcanzar las siguientes metas:

a) Todo el tráfico puede pasar a través del firewall

b) Sólo el tráfico que es autorizado por la política de seguridad de la red interna está permitido para pasar

c) El firewall no puede ser penetrado

El firewall debe proteger una red pobremente segura de amenazas externas o debe proteger a una red altamente segura de una menor La mayoría de las redes empresariales que se conectan a Internet limitan su exposición con los firewalls Los mecanismos más importantes de firewall son el **filtrado de paquetes** y los **gateways de aplicación** La mayoría de los firewalls utilizan ambos Los firewalls continuamente proveen servicios de autenticacion

Ejemplos de políticas que un firewall puede hacer cumplir son:

- Permitir el tráfico de ambos lados sólo con anfitriones en el mismo nivel de clasificación.

- Limitar el tráfico exterior a correo electrónico.

La mayoría de los servicios útiles son vulnerables. Su uso a través del firewall puede prevenirse, mientras que el uso dentro del firewall está permitido. Un firewall puede proteger contra los ataques basados en la ruta, puede proveer autenticación para todos los accesos externos utilizando contraseñas de una sola vez. El software de autenticación sólo tiene que ser instalado en los componentes del firewall y no en cada anfitrión. Un firewall puede ayudar a un lugar a ocultar información que puede ser útil a los intrusos. Un firewall puede mantener una auditoría de las conexiones de la red y puede detectar posibles intrusiones

Los firewalls para seguridad están construidos en mecanismos que fueron desarrollados para otras funciones **encaminadores** y **gateways** Cada uno de estos mecanismos conecta las redes y controla el tráfico de la red que pasa a través de él Un encaminador utiliza una dirección de destino e instrucciones de direccionamiento posible para determinar una ruta hacia el destino Un gateway puede conectar dos redes que utilizan diferentes protocolos ya que puede traducir de un protocolo a otro

Los componentes del firewall pueden ser manejados cuidadosamente, un firewall no es un sustituto para una seguridad interna buena, pero puede adicionar una capa de protección ya que puede ser la única forma práctica para ganar los beneficios de una conexión de red

Filtrado de paquetes

El filtrado de paquetes permite a ciertos paquetes pasar a través del firewall, el criterio utilizado para filtrar puede incluir cualquier cosa en la cabecera de la capa de red, para TCP/IP, es la cabecera IP, la cual contiene las direcciones anfitrionas fuente y destino El **filtrado de direcciones** utiliza las direcciones fuente y destino como criterio En la práctica, el filtrado de paquetes continuamente utiliza la información TCP de cabecera, especialmente el identificador del puerto destino Los números de puerto pueden ser usados para filtrar paquetes basados en

la aplicación si las redes TCP/IP usan números arreglados de puertos (puertos bien conocidos) para las aplicaciones. El filtrado de paquetes hace cumplir el control de acceso, el anfitrión fuente identifica a un sujeto y el destino (anfitrión, puerto) identifica un objeto. Algunas de las políticas que el filtrado comúnmente hace cumplir son:

- Permitir los servicios de correo electrónico y de directorio de ambos lados, el Telnet saliente, denegar todo lo demás.
- Permitir la comunicación sólo con un conjunto designado de anfitriones
- Denegar el tráfico entrante a un conjunto designado de puertos (ya que proveen servicios que son riesgosos)
- Permitir sólo los servicios de correo electrónico y directorio

Los encaminadores son utilizados para construir firewalls de filtrado de paquetes alrededor de las LANs Las cajas comerciales que cuestan casi lo mismo que una estación de trabajo permite a los administradores de la LAN especificar sus propias políticas de firewall Los encaminadores se ejecutan bien y son transparentes para los usuarios Un encaminador puede redireccionar un paquete, así el tráfico de un usuario remoto va a través de una computadora de entrada que implementa la autenticación más compresiva y audita antes que permitir a un usuario remoto tener acceso al anfitrión destino El filtrado de paquetes tiene varias desventajas serias, esto recae en las direcciones cuya integridad no puede ser garantizada; la suplantación de IP puede derrotar cualquier control de acceso basado en el anfitrión fuente Si la política de seguridad no es muy simple, las reglas de filtrado de paquetes se vuelven complejas y difíciles de escribir correctamente

Gateways de aplicación

Comparado con el filtrado de paquetes, un gateway de aplicación utiliza el más alto protocolo de la capa de información e implementa servicios adicionales de seguridad Es típicamente implementado en una o más computadoras anfitrionas y envuelven software personalizado y desarrollado para la organización Un gateway

de aplicación provee servicios proxy[19] que controlan el acceso a los servicios reales como el Telnet, FTP y X Windows. Para el Telnet, esto trabajaría como sigue:

1. Un usuario hace un Telnet al gateway y entra el nombre de un anfitrión destino

2. El gateway verifica la dirección IP de la fuente y acepta o rechaza el intento.

3. El usuario es autenticado.

4. El servicio proxy crea una conexión Telnet entre el gateway y el anfitrión destino

5 El servicio proxy pasa datos entre las dos conexiones.

6 El gateway registra la conexión

Muchas organizaciones utilizan gateways de correo Un gateway puede ejecutar la identificación del usuario y la autenticación para los usuarios remotos. Puede permitir el tráfico limitado entre dos subredes. Un gateway puede controlar el flujo de información saliente. Una desventaja de los gateways de aplicación es su incompatibilidad con el cifrado extremo a extremo que se realiza en la transportación o capa de red El gateways necesita el más alto protocolo de la capa de información así tendría que descifrar y volver a cifrar, entonces el cifrado no puede ser extremo a extremo

Consideraciones y problemas de firewall

Un firewall está muy alejado de una solución completa de los problemas de seguridad No provee protección contra el mal uso interno De manera adicional, una persona enterada puede cooperar con una persona externa para tunelear bajo el firewall Tunelear significa encapsular una unidad de datos de un protocolo a una unidad de datos de otro protocolo (o del mismo) Por ejemplo, los paquetes IP

[19] La función principal de los servicios proxy es la de acelerar las peticiones mediante mecanismos de cache (memoria intermedia), evitando así la conexión al servidor remoto y haciendo mas rapida por tanto la obtencion de la información

pueden ser escondidos en paquetes TCP, cualquier módem puede proveer una puerta trasera a través del firewall. El firewall no previene ataques en los cuales el contenido de un mensaje active la vulnerabilidad de un servicio. No protege contra el ataque de datos manejados, en el cual el anfitrión ejecuta algo que recibe.

8.3 Mejorías en los protocolos

Un paso significativo para la seguridad de Internet es la adopción de un protocolo estándar reforzado, IPv6. Este protocolo soporta la autenticación del origen de los datos, la integridad de los datos y el cifrado para la confidencialidad. Todas las implementaciones de IPv6 deben proveer todas las características y los componentes de confidencialidad pueden ser borrados para satisfacer las restricciones de exportación. IPv6 provee dos mecanismos que pueden ser utilizados de varias maneras. Una **cabecera de autenticación** soporta integridad y la autenticación del origen de los datos; una **carga encapsulada de seguridad** (ESP) soporta estos servicios y el cifrado para la confidencialidad. El nuevo protocolo puede interoperar con la versión previa IPv4.

IPv6 utiliza el concepto de una **asociación de seguridad**, la cual es la información de seguridad necesaria para una conexión de red o un conjunto de conexiones Por ejemplo, un anfitrión probablemente tiene una asociación de seguridad para todos sus usuarios, para una dirección de destino específica o probablemente tiene una asociación de seguridad por cada usuario y destino. La asociación de seguridad incluye información como el algoritmo de seguridad que está siendo utilizado, el algoritmo de cifrado, las claves criptográficas y el nivel de clasificación como Secreto o No clasificado. Un anfitrión receptor puede verificar si la dirección fuente del paquete es compatible con su asociación de seguridad

La ESP tiene dos modos de uso El **modo túnel** cifra un paquete IP entero, incluyendo las cabeceras, con otro paquete IP. Con el **modo transporte** (utilizado por marcos de protocolos de transporte de capas como el TCP o el UDP) la cabecera original no es cifrada El algoritmo predeterminado para la integridad es el MD5, para la confidencialidad es el DES

8.4 Seguridad en WWW

WWW (World Wide Web) rápidamente llegó a convertirse en la forma para navegar Internet El usuario ve un hipertexto o documento hipermedia con ligas a

recursos que pueden residir en cualquier lugar de Internet Los recursos pueden ser de muchos tipos, incluyendo FTP, Gopher, Telnet y los archivos. Un **localizador universal del recurso** (URL – Universal Resource Locator) especifica cada tipo del recurso, anfitrión y locación del anfitrión. Los clientes del Web y los servidores cooperan utilizando el **protocolo de transferencia de hipertexto** (HTTP – Hypertext Transfer Protocol). Un tipo de cliente es el **explorador** gráfico.

Amenazas de seguridad

Tanto los clientes como los servidores están expuestos a las amenazas de seguridad Los sistemas cliente están expuestos a las amenazas usuales de la red que son numeradas por las medidas de autenticación, integridad y confidencialidad Son vulnerables a los ataques de los caballos de Troya, ya que el software del cliente ejecuta los recursos del Web recibidos de los servidores como los subprogramas escritos en el lenguaje de programación Java. Puesto que un cliente puede escribir datos en un servidor e invocar las transacciones del servidor, un servidor con seguridad débil puede ser destruido o dañado.

Comercio electrónico

Los protocolos del Web están emergiendo como una probable base para realizar negocios en Internet Los requerimientos de seguridad para las transacciones electrónicas incluyen:

a) Integridad de la transacción

b) Confidencialidad de todas las partes de la transacción

c) Mutua autenticación de las partes (como el cliente, el comerciante y el banco)

d) No repudio

e) Servicio oportuno

f) Mantenencia del registro

g) Protección del sistema participante contra intrusión y abuso interno

Mejorías de los protocolos

Dos mejorías de seguridad de los protocolos del Web están siendo utilizadas: SSL (Secure Socket Layer) y S-HTTP (Secure Hypertext Transfer Protocol). SSL se encuentra entre TCP y HTTP (u otros protocolos de aplicación). Utilizando la tecnología de clave pública RSA, SSL provee autenticación de servidor, integridad de mensajes y cifrado. S-HTTP es una versión reforzada de HTTP Provee mayor flexibilidad que el SSL permitiendo para la negociación entre el cliente y el servidor alrededor de los métodos de administración de clave, políticas de seguridad, algoritmos criptográficos y formatos de mensaje. S-HTTP provee autenticación del cliente y el servidor. Integridad de mensaje y cifrado. Cada uno de estos servicios deben ser seleccionados (o no) de manera independiente.

Efectivo digital

Las transacciones de tarjeta de crédito son demasiado costosas. Una manera menos costosa de comercio en red es necesario para la venta de productos baratos como los documentos pequeños o los pequeños productos de software. Ecash es un sistema desarrollado por DigiCash, es utilizado como efectivo pero se implementa de manera diferente. Un banco está envuelto en una transferencia de efectivo entre dos partes Una compra envuelve un comprador, un vendedor y al banco, cada parte corre el software ecash. El efectivo es representado como monedas digitales, cada uno revela un número serial único y la firma digital del banco Cuando *A* saca monedas digitales de su banco, el banco le envía mensajes que representan cada moneda y el software ecash de *A* almacena las monedas en su disco duro. Para pagar una compra de *B*, *A* le envía algunas de sus monedas El software ecash de *B* las envía al banco para validación y depósito. El involucramiento del banco es necesario para prevenir abusos como el gasto de una moneda dos veces El banco mantiene una base de datos de monedas gastadas en el cual puede tener acceso por el número serial de la moneda. Si las monedas pagadas por *A* son válidas, el banco las mantiene en la base de datos y le informa a *B* que el pago es válido *B* puede escoger "mantener" las monedas, en cuyo caso el banco le envia nuevas como equivalente

Las firmas ciegas - permiten a una entidad firmar un mensaje sin conocer su contenido permiten que el banco firme las monedas digitales que no son rastreadas Para el anonimato, ecash en la computadora de *A* crea una moneda con un número serial aleatorio y lo oculta en un sobre digital y lo envía al banco El banco coloca su firma digital en el exterior del sobre y se lo regresa a *A* El

software de A remueve la moneda de su sobre. El banco no tiene manera de reconocer la moneda que fue puesta en circulación a A.

CAPÍTULO 9.
CONCLUSIONES

9. CONCLUSIONES

Dado que la seguridad es uno de los temas que más "preocupan" a quienes están involucrados en los negocios electrónicos, desafortunadamente hoy en día, en cuestiones de presupuesto, es raro que la seguridad sea una de las prioridades de la inversión. Generalmente las empresas funcionan bajo un contexto de "confianza relativa", es decir, esperan que no suceda nada grave que pueda poner en peligro su información. Sin embargo, para poder competir con éxito en un entorno digital, debe asumirse la seguridad como parte integral-esencial del negocio.

Por otro lado, el tema de la seguridad de la tecnología de la información, en el nivel educativo, debe ser considerado como un tema aún más importante que en los negocios. ¿Por qué? Porque si consideramos que los egresados de nuestra facultad serán los futuros directivos, dueños de empresas, administradores de centros de cómputo o de redes de computadoras, o bien diseñadores y o desarrolladores de cualquier tipo de productos de tecnología de la información, ellos necesitarán tener conocimientos acerca de la seguridad para poder resguardar y manipular la información que transita por las redes de manera confiable e integra De esta manera, los egresados serán más eficaces en el cumplimiento de sus actividades y por consiguiente nuestro país contará cada vez más con empresas y organizaciones seguras y competitivas

Ante tal situación, se concluye lo siguiente:

- La mayoría de las personas que tienen conocimientos afines con la carrera de computación, aún no se han dado cuenta de la importancia que tiene la seguridad y que a largo plazo representa pérdida de información y sobretodo una constante inseguridad cada vez que se presenta una falla en la red Por lo tanto, creemos que un punto fundamental es crear conciencia sobre la importancia de la seguridad de las redes esta seguridad debe comprender políticas, procedimientos y sobretodo una disciplina corporativa. – y de la información que en ellas fluye ya que la seguridad es responsabilidad de todos, pues ésta no pertenece únicamente a una persona – administrador de la red - o grupos específicos, sino a todos y cada uno de los que están en contacto con la información directivos, gerentes, secretarias, administradores, alumnos, jefes de área, etc , porque lamentablemente, en términos generales, no existe en México la conciencia de la importancia mayúscula que tiene el amplio, vasto y maravilloso mundo de la seguridad

- Una vez que se tiene conciencia sobre lo trascendental que tiene el conocimiento de la seguridad de la información, ahora será necesario transmitir, a los alumnos, los conocimientos fundamentales sobre la seguridad de la información.

- Conforme se vayan transmitiendo dichos conocimientos a las siguientes generaciones se considera que los futuros egresados saldrán de la Facultad mejor preparados aún, y con la capacidad de llevar a la práctica (a la vida profesional) los conocimientos adquiridos en términos de seguridad informática a través de las notas y de las prácticas que se plantean en este trabajo, para así poder crear y ver en México, a la seguridad como una cultura.

CAPÍTULO 10.
APÉNDICES

APÉNDICE A.
TABLAS

A	*B*	*XOR*
0	0	0
0	1	1
1	0	1
1	1	0

Tabla OR EXCLUSIVO

	0	1	2	3	4	5	6	7	8	9
0	nul	soh	stx	etx	eot	enq	ack	bel	bs	ht
1	nl	vt	ff	cr	so	si	dle	dc1	dc2	dc3
2	dc4	nak	syn	etb	can	em	sub	esc	fs	gs
3	rs	us	sp	!	"	#	$	%	&	'
4	(	)	*	+	,	-	.	/	0	1
5	2	3	4	5	6	7	8	9	:	;
6	<	=	>	?	@	A	B	C	D	E
7	F	G	H	I	J	K	L	M	N	O
8	P	Q	R	S	T	U	V	W	X	Y
9	Z	[	\	]	^	_	`	a	b	c
10	d	e	f	g	h	i	j	k	l	m
11	n	o	p	q	r	s	t	u	v	w
12	x	y	z	{	|	}	~	del		

Los dígitos a la izquierda de la tabla son los dígitos izquierdos del equivalente decimal del código de caracteres, y los dígitos en la parte superior de la tabla son los dígitos derechos del código de caracteres. Por ejemplo, el código de carácter para 'F' es 70, y el correspondiente para & es 38.

Tabla del código ASCII

APÉNDICE B.
REACTIVOS

Capítulo 2. Ataques de seguridad

1. ¿Qué es una amenaza y de qué fuentes proviene?
2. ¿Cuáles son los tres elementos que se necesitan para efectuar un ataque?
3. ¿Qué es un escudo?
4. ¿Qué es una vulnerabilidad y por qué se produce?
5. Un perpetrador es un individuo que se basa en cualquier medio para cometer un delito o culpa grave; los perpetradores pueden clasificarse en personas enteradas, hackers y espías. Según su punto de vista ¿cuál(es) cree que represente(n) una amenaza mayor y por qué?.
6. Entre las amenazas que existen para un flujo de información se encuentran la interrupción, intercepción, modificación y suplantación Explicar y dar un ejemplo de cada una de las amenazas mencionadas.
7. Se sabe que existen ataques activos y ataques pasivos ¿Cuál de estos dos tipos considera que es más peligroso?. Justifique su respuesta.
8. ¿Cuáles son las tres etapas principales para atacar un centro de cómputo?
9. ¿ Cuál cree que sean las misiones de un ataque más comunes observadas en el mundo real? Elabore una lista.

Capítulo 3. Fundamentos de la seguridad

1. ¿Qué entiende por seguridad? y ¿Cuál considera que sea su importancia?
2. Mencione los puntos en los que se basa el método para determinar los requerimientos de seguridad del software y el hardware
3. ¿Qué son los criterios comunes y cuál es su importancia?
4. Al realizar una evaluación de las propiedades de seguridad de los productos ¿Quiénes son los principales interesados en dicha evaluación?
5. ¿Cuáles son los dos elementos esenciales de los criterios comunes y para qué sirve cada uno?

Capítulo 4. Servicios de seguridad

1. ¿Que es un servicio de seguridad?
2. De los servicios de seguridad – confidencialidad, autenticación, integridad de datos, no repudio, control de acceso y disponibilidad – desde su punto de vista ¿Cuál(es) cree que es(son) más empleado(s) en el mundo real y por qué? Justifique su respuesta

3. Un nuevo banco acaba de contratar a un administrador para la red A éste último se le encomendó realizar una lista con los servicios de seguridad que aplicaría, por qué y en qué casos. Si estuvieras en su situación ¿cómo quedaría la lista?
4. Dé ejemplos de cada uno de los servicios de seguridad.

Capítulo 5. Criptografía

1. ¿Qué entiende por criptografía? y ¿Cuál considera que sea su importancia?
2. ¿ Qué diferencia existe entre la criptografía y el criptoanálisis?
3 ¿Cuáles son los dos principios generales en los que se basan todos los algoritmos de cifrado? Explique cada uno.
4. ¿Cuál es la principal diferencia entre un cifrado simétrico y un cifrado asimétrico? ¿Qué elementos en común tienen? Explique.
5 ¿Cuáles son las dos hipótesis en las que se basa el Secreto Perfecto?
6 ¿Cuál es la diferencia entre el algoritmo DES y el IDEA?
7. Cree un método de cifrado justificando el planteamiento y la seguridad que ofrece
8 Haciendo uso del cifrado Vigenère y la tabla 5.5 del capítulo 5:
   a) ¿Cuál sería el criptograma si el texto original es: "Código malicioso" y se utiliza la clave "datos"?
   b) Descifre el siguiente criptograma "vbrkmzagukddfm" usando la clave: "virus"

Capítulo 6. Seguridad en una organización

1 ¿Qué es una política de seguridad?
2 ¿Qué aspectos se deben considerar para crear una política de seguridad informática?
3 ¿Qué principios fundamentales se aplican en general en las metas de una organización? Explique
4 ¿Qué es y para que sirve un modelo de seguridad?
5 Sabiendo que existen varios modelos de seguridad y que cada uno de ellos tiene limitaciones, ¿Cree que sería buena opción combinar algunos de ellos para obtener una mayor seguridad o lo mejor sería diseñar un nuevo modelo? Justifique su respuesta y haga el desarrollo correspondiente

Capítulo 7. Mecanismos de seguridad

1. ¿Qué es un mecanismo de seguridad?
2. ¿Cuáles son los tres componentes principales de un mecanismo de seguridad en general?
3. ¿Cuáles son las dos categorías en que se pueden clasificar los mecanismos de seguridad?, explique cada una y dé un ejemplo de cada uno de los mecanismos que se observan en cada categoría.

Capítulo 8. Seguridad en Internet

1. ¿Cuáles son las principales vulnerabilidades que se observan en Internet?
2. ¿Qué es un firewall y cuáles son las desventajas que presenta en cuanto a la seguridad?
3. ¿Qué características importantes ofrece el protocolo IPV6 para mejorar el protocolo IPV4?
4. Basándose en lo mencionado en el capítulo 8 ¿Cree que Internet es segura actualmente? sí, no, ¿por qué? Justifique su respuesta, dando con ello sus propuestas de solución (el qué y el cómo)

APÉNDICE C.
PRÁCTICAS

PRÁCTICA 1. ATAQUES PASIVOS

Objetivo: El alumno conocerá y comprenderá los ataques pasivos así como la información que puede obtener de éstos

Introducción:

¿Qué son los ataques activos?

Las amenazas se encuentran en cualquier parte de nuestro entorno informático, sin embargo, cuando se presenta una oportunidad de realizar algún tipo de violación, automáticamente se está llevando a cabo un **ataque de seguridad**

Los ataques tienen varios objetivos incluyendo el fraude, la extorsión, el robo de información, la venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red

Los ataques pasivos reciben su nombre debido a que el perpetrador no altera en ningún momento la información, es decir, únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida Cualquier ataque pasivo tiene los siguientes objetivos principales

a) **Intercepción de datos:** consiste en el conocimiento de la información cuando existe una liberación de los contenidos del mensaje.

b) **Análisis de tráfico:** consiste en la observación de todo el tráfico que pasa por la red

Con los ataques pasivos se obtiene información que puede consistir en

a) **Obtención del origen y destinatario** de la comunicación, esto se logra cuando el perpetrador lee las cabeceras de los paquetes que continuamente está monitoreando Con ello se determina la localizacion y la identidad de los anfitriones (emisor, receptor)

b) Control del volumen de tráfico intercambiado entre las entidades monitoreadas de esta forma se obtienen todos los datos necesarios

para percatarse de la actividad o inactividad inusuales, se conoce la frecuencia y longitud de los mensajes.

c) **Control de las horas habituales** de intercambio de datos entre las entidades de la comunicación, con ello se extraen los datos acerca de los períodos de actividad. El perpetrador conoce la frecuencia con la que se transmiten los mensajes.

Los ataques pasivos son muy difíciles de detectar e interceptar, debido a que no provocan ninguna alteración de los datos.

¿Cómo funciona un cajero automático?

Un cajero automático es un dispositivo mediante el cual se pueden realizar transacciones bancarias – disposición de efectivo, pago de servicios, consulta de saldos, etc. – y es el mediador entre el cliente y la institución bancaria.

Dicho dispositivo – cajero automático – tiene una interfaz gráfica que permite interactuar con el cliente, es decir, el cajero recibe las peticiones del cliente y prepara la información (petición) para enviarla al anfitrión del banco Una vez que el anfitrión valida y autoriza la información la regresa al cajero, éste realiza determinadas acciones – dependiendo de la información que le envió el anfitrión – y da una respuesta al cliente

A continuación se muestra – en la figura 1 – a grandes rasgos el flujo de la información entre el cajero y el anfitrión de un banco.

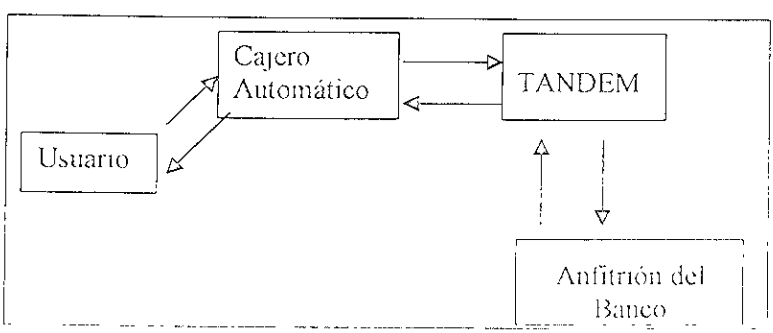


Figura 1. Flujo de la información

El flujo de la información es la siguiente:

1. El cliente realiza cualquier transacción – disposición de efectivo, pago de un servicio – a través del cajero automático.

2 El cajero automático se encarga de tomar la petición del cliente y dicha petición la transforma en un mensaje (trama) que contiene los datos necesarios para que el anfitrión del banco pueda atender la petición del cliente. Sin embargo, antes de llegar al anfitrión el mensaje debe llegar a un servidor – llamado TANDEM – El servidor TANDEM toma la trama que elaboró el cajero en su lenguaje propio y la convierte para que el anfitrión del Banco pueda entender la petición que solicitó el cajero automático

3 Cuando llega el mensaje al anfitrión del Banco, éste toma el mensaje y de acuerdo a la información contenida en él, empieza a realizar las validaciones y operaciones correspondientes a la petición del cliente.

4 El anfitrión del Banco cuando ya tiene la respuesta para el cliente, genera un mensaje y lo envía hacia el servidor TANDEM

5. El servidor TANDEM convierte ahora el mensaje del anfitrión y genera un mensaje con el lenguaje propio del cajero y se lo envía a este último.

6 El cajero de acuerdo a la respuesta que le envió el anfitrión del Banco, le indica los resultados al cliente Los resultados pueden ser la entrega de dinero, la impresión de una consulta de saldo, informar al cliente que su datos no fueron válidos, etc

¿Cómo funciona el cajero automático de la aplicación?

Comunicación entre el cajero automático y el anfitrión.

La comunicación entre el cajero automático y el anfitrión consistirá siempre en recibir y enviar un mensaje (trama) Se manejarán cuatro tramas en la aplicación, a continuación se describe el contenido de cada trama

TRAMA 1 (DATOS QUE SE ENVIAN PARA COMUNICARSE AL ANFITRIÓN)

Campo	No. Tarjeta	NIP	Status	Terminal	Fecha	Hora
Longitud	16	4	2	2	8	4

TRAMA 2 (DATOS QUE ENVIA – COMO RESPUESTA – EL ANFITRIÓN AL CAJERO)

Campo	No. Tarjeta	NIP	Status	Terminal	Fecha	Hora
Longitud	16	4	2	2	8	4

Elementos utilizados en las tramas 1 y 2

a) **No. Tarjeta:** es el número de la tarjeta con la que se realizarán las operaciones y es de una longitud de 16 dígitos.

b) **NIP:** es el Número de Identificación Personal que se utilizará como password y es de una longitud de 4 dígitos.

c) **Status:** Su longitud es de 2 dígitos e indicará los siguientes estados
   00 Envío de Datos
   10 Datos Inválidos
   11 Datos Válidos

d) **Terminal:** corresponderá a la terminal en la que se está efectuando la operación y tiene una longitud de 2 dígitos. El único valor posible es. 01

e) **Fecha:** es la fecha en que se está efectuando la operación

f) **Hora:** es la hora en que se está efectuando la operación

TRAMA 3 (DATOS QUE SE ENVIAN AL ANFITRIÓN PARA PROCESAR TRANSACCIÓN)

Campo	No. Tarjeta	Status	Termina l	Fecha	Hora	Clave Operación	Importe
Longitud	16	2	2	8	4	3	14

TRAMA 4 (DATOS QUE ENVÍA – COMO RESPUESTA – EL ANFITRIÓN AL CAJERO)

Campo	No. Tarjeta	Status	Termina l	Fecha	Hora	Clave Operación	Importe
Longitud	16	2	2	8	4	3	14

Elementos utilizados en las tramas 3 y 4:

a) **No. Tarjeta:** es el número de la tarjeta con la que se realizarán las operaciones y es de una longitud de 16 dígitos

b) **Status:** Su longitud es de 2 digitos e indicará los siguientes estados.
00 Envío de Datos
10 Operación No Efectuada
11 Operación Efectuada

c) **Terminal:** corresponderá a la terminal en la que se está efectuando la operación y tiene una longitud de 2 dígitos El único posible valor es 01

d) **Fecha:** es la fecha en que se está efectuando la operación

e) **Hora:** es la hora en que se está efectuando la operación

f) **Clave de Operación:** tiene una longitud de 3 dígitos y pueden ser tres posibles valores

501 Cargo a la cuenta
601 Abono a la cuenta
102 Saldo de la cuenta

g) **Importe:** tiene una longitud de 14 dígitos y corresponderá al monto que se desea cargar o abonar a la cuenta.

Las cuatro tramas mencionadas, contienen la información necesaria para mantener una comunicación y se puedan ejecutar las transacciones

Nota: En esta simulación sólo existirá comunicación entre el cajero automático y el anfitrión.

Operatividad del cajero automático de la aplicación

1ª Etapa

- Se ingresa un No. de tarjeta de 16 dígitos.
- Se indica el NIP asociado al No de Tarjeta ingresado.
- Se presionará el botón ACEPTAR y se establecerá comunicación con el anfitrión.
- Si el No. de Tarjeta y el NIP son válidos se continúa con la sesión. En caso contrario de que cualquiera de los datos sea incorrecto mandará un mensaje indicándolo

2ª Etapa

- Se continúa la sesión cuando la aplicación se enlaza a la pantalla del menú, en ella se muestran tres posibles transacciones a efectuar

  1 Disposición de efectivo

  - Se mostrarán las posibles cantidades ($50, $100, $200, $500, $1000 y $3000)
  - Cuando se realiza una petición para solicitar efectivo, vuelve a existir una comunicación al anfitrión sólo que ahora se estará procesando la transacción de disposición de efectivo

- Se realiza el cargo a la cuenta asociada al No. de Tarjeta ingresada desde el principio y aparece un mensaje indicando el saldo actual de la cuenta.

- Se regresa a la pantalla de menú.

2. Traspasos a otra Cuenta

- Se mostrará el No. de Tarjeta ingresado, el No. de Cta y el titular de la cuenta.
- Se debe seleccionar desde el combo box la cuenta a la que se le realizará un traspaso –cuenta destino.

- Una vez realizada la selección de la cuenta aparecerá el titular de dicha cuenta

- Se debe indicar el importe que se desea abonar a la cuenta destino y dar "ACEPTAR". En ese momento el cajero se vuelve a comunicar con el anfitrión y le envía los datos para poder realizar el traspaso entre las cuentas.

- Enseguida aparecerá el saldo disponible de la cuenta origen y después el de la cuenta destino

- Se regresa a la pantalla de menú

3 Consulta de Saldos

- Al solicitar una consulta, el cajero se vuelve a comunicar con el anfitrión y le envía los datos para poder realizar la consulta Se mostrará el Número de Tarjeta, Número de Cuenta, Titular, Saldo Actual, Fecha, Hora y Terminal.

Desarrollo:

1. Tomando como base la operatividad del cajero automático de la aplicación:

   a) Ingresar Número de Tarjeta y NIP – dar click en los números que aparecen en la aplicación para ingresar el NIP –, después dar ACEPTAR. En la tabla 1 se indican las combinaciones de números de tarjeta y NIP's que se deben ingresar.

No. De Tarjeta	Tarjeta Válida	NIP	NIP Válido	Respuesta Esperada
4913500010000001	No	9510	No	Mensaje de error
5513600010000015	No	4562	No	Mensaje de error
4521025514500110	No	5410	No	Mensaje de error
4913500010000000	Sí	3000	No	Mensaje de error
4913500010000000	Sí	2130	No	Mensaje de error
4913500010000000	Sí	4200	Sí	Continúa la sesión

Tabla 1. Números de tarjetas y NIP's

   b) Realizar tres consultas del saldo de la cuenta. Para cada consulta de saldo se requiere oprimir la tecla *C* dos veces (una vez para CONSULTA DE SALDO y otra para TERMINAR)

   c) Realizar una disposición de efectivo de cada valor –$50, $100, $200, $500, $1000 y $3000. Para cada disposición se requiere oprimir primero la tecla *A* e inmediatamente la tecla correspondiente al valor (A, B, C, D, E o F)

   d) Realizar tres traspasos a otras cuentas con diferentes importes Para cada traspaso es necesario oprimir la tecla *B*, escoger la CUENTA DE ABONO e ingresar la cantidad no mayor a $10000 cada vez – para ello dar click en los números que aparecen en la aplicación –, finalmente oprimir la tecla *C*

   e) Oprimir el botón PASIVOS Se mostrará la pantalla donde se indicarán todos los movimientos – las tramas - que se realizaron

2. Tomando en cuenta la tabla 2, crear una tabla similar a la tabla 1, de tal manera que solo una combinación tenga un número de tarjeta y un NIP válidos

No Tarjeta	NIP
4913500010000000	4200
4913500110000001	4201
4913500210000002	4202
4913500310000003	4203
4913500410000004	4204
4913500510000005	4205

Tabla 2. Relación de cuentas

3. Con ayuda de la tabla creada en el punto anterior, repetir los pasos descritos en el punto 1.

4. Apuntar las tramas que se muestran en la pantalla que aparece después de oprimir el botón PASIVOS

5. De las tramas obtenidas en el punto anterior, escribir – para cada una – a qué número de trama se refiere (1, 2, 3 ó 4) y porqué, tomando en cuenta la comunicación entre el Cajero Automático y el anfitrión

Cuestionario:

1. Si no supiera cómo están conformadas las tramas, ¿Qué contendrían éstas: datos o información? y ¿Por qué lo considera así?.

2 En la pantalla donde se muestran todos los movimientos que realizó una cuenta en el cajero automático – Ver puntos 1 e y 4 – ¿Qué tipo de información se puede obtener de ella?

3. Tomando como base las tramas que se utilizaron para la práctica, ¿Qué modificaría agregar o quitar campos – de las tramas, con el objetivo de proporcionar mayor seguridad en los datos que se envían y/o reciben? y ¿Por qué?

4 Dé sus conclusiones

PRÁCTICA 2. ATAQUES ACTIVOS

Objetivo: El alumno conocerá y comprenderá los ataques activos que existen.

Introducción:

¿Qué son los ataques activos?

Los ataques activos se nombran así debido a que implican algún tipo de modificación de la corriente de datos o la creación de una corriente falsa.

Los ataques activos pueden clasificarse de la siguiente manera.

a) **Degradación fraudulenta del servicio:** este tipo de acción impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones (medios de comunicación) Entre estos ataques se encuentran los de **denegación de servicio**, los cuales consisten en paralizar temporalmente el servicio.

b) **Enmascaramiento o Suplantación de identidad:** en este caso, el intruso se hace pasar por una entidad diferente Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como el robar la contraseña de acceso a una cuenta.

c) **Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mismos mensajes son retardados o reordenados, esto provoca que se produzca un efecto no autorizado

d) **Réplica o Reactuación:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado debido a que se realiza una retransmisión subsecuente Por ejemplo, se podría utilizar para ingresar dinero repetidas veces en una cuenta dada

Desarrollo:

1. Tomando como base la operatividad del cajero automático de la aplicación vista en la práctica No.4:

MODIFICACIÓN DE DATOS

a) En la tabla 1 se indica las combinaciones de números de tarjeta y NIP's que se utilizarán.

No. de Tarjeta	Tarjeta Válida	NIP	NIP Válido
4913500310000003	Sí	4203	Sí
4913500410000004	Sí	4204	Sí

Tabla 1. Números de tarjetas y NIP's

b) Ingresar la primera combinación de datos –No. De Tarjeta y NIP (dar click en los números que aparecen en la aplicación para ingresar el NIP). No oprima el botón "ACEPTAR"

c) Oprimir el botón "MODIFICACIÓN". Aparecerá el siguiente mensaje: "Hay que seleccionar una trama".

d) Seleccionar la trama 1 y después dar click en el botón "ACEPTAR"

e) Como consecuencia aparecerá la pantalla de ataques activos correspondiente a "Modificación de Datos". En ella se muestran los datos de la trama 1 (únicamente están habilitados los campos de No. De Tarjeta y el campo del NIP)

f) Modificar el número de tarjeta por el siguiente 5412500310078943 El NIP no debe modificarse (debe permanecer el número 4203).

g) Oprimir el botón "REENVIAR DATOS" En ese momento se establecerá la comunicación con el anfitrión y se mostrará el siguiente mensaje: "No existe No. De Tarjeta"

h) Ingresar nuevamente los datos de la primera combinación, debido a que el No De Tarjeta ya está escrito, entonces sólo hay que teclear el NIP (4203) y repetir los pasos c, d y e.

i) Modificar el NIP por el siguiente: 9999 El número de tarjeta no debe modificarse (4913500310000003).

j) Oprimir el botón "REENVIAR DATOS". En ese momento se establecerá la comunicación con el anfitrión y se mostrará el siguiente mensaje: "NIP INVÁLIDO".

k) Ingresar nuevamente los datos de la primera combinación, debido a que el No. De Tarjeta ya esta escrito, entonces sólo hay que teclear el NIP (4203) y repetir el paso c.

l) Seleccionar la trama 2 y después dar click en el botón "ACEPTAR".

m) Como consecuencia aparecerá la pantalla de ataques activos correspondiente a "Modificación de Datos". En ella se muestran los datos de la trama 2 (únicamente están habilitados los campos de No. De Tarjeta y el campo del NIP).

n) Modificar el número de tarjeta y el NIP, para esto hay que cambiarlos por la segunda combinación mostrada en la tabla 1 (4913500410000004 y 4204)

o) Oprimir el botón "REENVIAR DATOS" En ese momento el anfitrión establecerá la comunicación con el cajero y se continuará con la sesión

p) Realizar una consulta de saldo – para esto oprimir la tecla (' --, se observará que el número de la tarjeta inicial – 4913500310000003 – tiene un saldo de $50,000 00 Oprimir nuevamente la tecla (' para terminar la consulta y poder realizar otra operación

q) Realizar una disposición de efectivo de $3,000.00 para ello hay que oprimir la tecla 4 y enseguida la tecla (', aparecerá el saldo disponible de la cuenta Realizar una segunda consulta de la cuenta, se observara que el número de la tarjeta inicial 4913500310000003 tiene un saldo de $50,000 00

r) Realizar un traspaso a la cuenta 10000005 por un importe de $5,000.00 (para esto hay que oprimir la tecla *B*, enseguida seleccionar la cuenta 10000005, dar click en los números que aparecen en la aplicación para ingresar el importe de $5,000.00 y finalmente oprimir la tecla *C* para que se acepte la información). Aparecerá el saldo disponible de la cuenta – $42,000.00 – y el saldo disponible de la cuenta destino –$55,000.00.

s) Realizar una tercera consulta de la cuenta, se observará que el número de la tarjeta inicial – 4913500310000003 – tiene un saldo de $50,000.00

t) Oprimir el botón "REINICIAR CAJERO".

REPLICACIÓN DE DATOS

a) Ingresar el siguiente número de tarjeta: 4913500210000002 y el NIP 4202. Después presionar el botón "RÉPLICA", aparecerá el mensaje: "HAY QUE SELECCIONAR EL No. DE RÉPLICAS".

b) Seleccionar como número de réplicas el 5 y también seleccionar la cuenta 10000005 como No. de cuenta a atacar

c) Dar click al botón "ACEPTAR"y enseguida se continuará con la sesión.

d) Realizar una disposición de efectivo por $1,000 00. Enseguida se mostrará la pantalla correspondiente a Réplica de Información, en ella se indican diversos datos, entre ellos el número de la cuenta atacada – 10000005 – y el saldo de la misma después de cada ataque – 5 réplicas o ataques. Dar click al botón "CERRAR"

e) Realizar una consulta de la cuenta, se observará que el número de la tarjeta inicial – 4913500210000002 – tiene un saldo de $50,000 00

f) Realizar un traspaso a la cuenta 10000004 por un importe de $2,000.00

g) Enseguida se mostrará la pantalla correspondiente a Réplica de Información, en ella se indican diversos datos entre ellos el número de la cuenta atacada 10000005 y el saldo tanto de la cuenta atacada como el saldo de la cuenta destino después de cada ataque 5 réplicas o ataques

h) Dar click al botón "CERRAR".

i) Realizar una segunda consulta de la cuenta, se observará que el número de la tarjeta inicial – 4913500210000002 – sigue teniendo un saldo de $50,000.00

j) Para terminar la práctica, oprimir el botón "REGRESAR AL MENÚ" o el botón "REINICIAR CAJERO".

Cuestionario:

1. En la trama 1 se modificaron datos – número de tarjeta y el NIP – antes de que la trama 1 llegara al anfitrión. ¿Qué cree que se podría hacer (programar, aumentar campos en la trama, etc.) para identificar y contraatacar la modificación de datos?

2. Comparando los ataques vistos en la práctica 1 con los ataques realizados en esta práctica ¿Cuál cree que son más peligrosos? y ¿Por qué?

3. Cuando se realizaron modificaciones a la trama 2 (número de tarjeta y el NIP), después se realizó la disposición de efectivo por $3,000.00 y también se realizó una segunda consulta de la cuenta – punto 1.q – ¿Por qué razón el saldo de la cuenta indica $50,000.00?

4. En los puntos 1.r y 1.s se llevó a cabo un traspaso a otra cuenta por una cantidad de $5,000.00 y después se revisó el saldo de la cuenta original y se mostró la cantidad de $50,000.00. Es decir, que aun cuando la cuenta original acaba de realizar un traspaso por $5,000.00 debería tener de un saldo de $45,000.00, sin embargo , conserva su saldo con $50,000.00. De tal situación ¿En qué otro tipo de ataque activo - a parte de la modificación de datos – se está incurriendo? y ¿Por qué?

5. En la sección de la práctica referente a replicación de datos, ¿Cómo cree que se podrían evitar o qué medidas tomaría para que este tipo de ataques no se presentaran si usted fuera el encargado de supervisar las transacciones que se realizan entre un cajero automático y el banco donde trabaja? Explique

6. Dé sus conclusiones

PRÁCTICA 3. SUSTITUCIÓN Y TRANSPOSICIÓN

Objetivo: El alumno conocerá, comprenderá y manejará los dos principios generales de los algoritmos de cifrado: la sustitución y la transposición.

Introducción:

¿Qué son la sustitución y la transposición?

Todos los algoritmos de cifrado se basan en dos principios generales:

1. **Sustitución:** en el cual cada elemento del texto (bit, letra, grupo de bits o letras) es cambiado por otro elemento. La sustitución consiste en determinar una correspondencia entre las letras del alfabeto en que está escrito el mensaje original y los elementos de otro conjunto, el cual puede ser el mismo o diferente alfabeto La sustitución es empleada para causar confusión Uno de los sistemas de sustitución que se conoce es el polialfabético, que es el resultado de introducir múltiples alfabetos de cifrado que se utilizan en rotación de acuerdo con un criterio o clave, su objetivo es adecuar las frecuencias del texto cifrado de tal forma que las letras con mayor frecuencia de aparición no sobresalen tan claramente. Dentro de este sistema se tiene el **cifrado Vigenère.**

   Para cifrar utilizando el **cifrado Vigenère** se utiliza la matriz cuadrada que se muestra en la tabla 1

   Por ejemplo, para cifrar el texto: "el perro ladra muy fuerte", empleando la clave. conducta.

   Primero hay que poner la clave, en forma repetida, encima del texto en claro

c	o	n	d	u	c	t	a	c	o	n	d	u	c	t	a	c	o	n	d	u
e	l	p	e	r	r	o	l	a	d	r	a	m	u	y	f	u	e	r	t	e

   El criptograma se obtiene de la siguiente manera

   - Se toma la primera letra del texto claro *e* y se observa que le corresponde la letra *c* de la clave La letra cifrada es la letra que resulta de intersectar el

renglón *c* con la columna *e*. De acuerdo con la tabla 1, la letra resultante es *g*.

- Se toma la segunda letra del texto claro *l* y se observa que le corresponde la letra *o* de la clave. La letra cifrada es la letra que resulta de intersectar el renglón *o* con la columna *l*. De acuerdo con la tabla 1, la letra resultante es *z*.

- Se toma la tercera letra del texto claro *p* y se observa que le corresponde la letra *n* de la clave. La letra cifrada es la letra que resulta de intersectar el renglón *n* con la columna *p*. De acuerdo con la tabla 1, la letra resultante es *c*.

Se realiza el mismo procedimiento para cada una de las letras del texto en claro, hasta que finalmente se obtiene el siguiente criptograma: **gzchlthlcredgwrfwsewy.**

Para descifrar el criptograma también hay que poner la clave, en forma repetida, encima del texto cifrado

c	o	n	d	u	c	t	a	c	o	n	d	u	c	t	a	c	o	n	d	u
g	z	c	h	l	t	h	l	c	r	e	d	g	w	r	f	w	s	e	w	y

Y el texto original se obtiene de la siguiente manera

- Se toma el renglón de la primera letra de la clave *c* y en ese mismo renglón se busca la primera letra del texto cifrado *g* una vez encontrada ésta, la letra del texto en claro será la correspondiente a esa columna. De acuerdo con la tabla 1, la letra resultante es *e*.

- Se toma el renglón de la segunda letra de la clave *o* y en ese mismo renglón se busca la segunda letra del texto cifrado *z* una vez encontrada ésta, la letra del texto en claro será la correspondiente a esa columna. De acuerdo con la tabla 1, la letra resultante es *l*

- Se toma el renglón de la tercera letra de la clave *n* y en ese mismo renglón se busca la tercera letra del texto cifrado *c* una vez encontrada esta, la letra

del texto en claro será la correspondiente a esa columna. De acuerdo con la tabla 1, la letra resultante es *p*.

Se realiza el mismo procedimiento para cada una de las letras del criptograma hasta que finalmente se obtiene el texto en claro: **el perro ladra muy fuerte**

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Tabla 1. Matriz cuadrada

2. **Transposición:** los elementos del texto son reacomodados. La transposición consiste en intercambiar los símbolos del mensaje original, de tal forma que el criptograma tenga los mismos elementos que el mensaje original pero que sea

difícil de comprender. La transposición es utilizada para la difusión, pues el mensaje original se difumina sin que se pierda la información.

Por ejemplo, se requiere cifrar el siguiente mensaje empleando la transposición. "clase de aritmética", para ello se utiliza la siguiente clave. escribir el mensaje horizontalmente de tal manera que se formen cuatro renglones, colocar los renglones obtenidos de manera secuencial.
El criptograma se obtiene de la siguiente manera:

c	e	r	e	a
l	d	i	t	
a	e	t	i	
s	a	m	c	

Puesto en forma secuencial:

cerealditaetisamc

Desarrollo:

1. Tomando como base la explicación de la sustitución

   a) Plantear un nuevo texto en claro

   b) Plantear una nueva clave.

   c) Haciendo uso del cifrado Vigenère, cifre el texto del inciso a) con la clave del inciso b).

   d) Ahora cifre el texto del inciso a) con la clave proporcionada por el profesor

   e) Intercambie con otro equipo las claves de los incisos b) y d) y los criptogramas obtenidos en el inciso anterior

   f) Haciendo uso del cifrado Vigenère descifre los criptogramas dados por el otro equipo

2. Tomando como base la explicación de la transposición

a) Plantear un nuevo texto en claro.

b) Escribir la forma en la que será cifrado (clave)

c) Cifrar el texto del inciso a)

d) Intercambie con otro equipo la clave del inciso b) y el criptograma obtenido en el inciso anterior.

e) Descifre el criptograma proporcionado por el otro equipo

Cuestionario:

1. ¿Por qué se dice que la confusión se basa en la sustitución?

2. ¿A qué tipo de sustitución pertenece el cifrado Vigenère? ¿Por qué?

3 ¿Los criptogramas obtenidos en el inciso 1.d son iguales? Sí o no y ¿Por qué?

4. ¿Por qué se dice que la difusión se basa en la transposición?

5. Si en el punto 2 d no se hubiera proporcionado la clave, podría realizarse el punto 2 c? ¿Por qué?

6 Dé sus conclusiones

PRÁCTICA 4. ALGORITMO DES (DATA ENCRYPTION STANDARD)

Objetivo: El alumno conocerá, comprenderá y manejará el funcionamiento del algoritmo DES utilizando una aplicación que cifra y descifra mensajes con dicho algoritmo.

Introducción:

¿Cómo funciona el algoritmo DES?

El cifrado se lleva a cabo en dos pasos principalmente:

a) El primero consiste en crear 16 subclaves, cada una con una longitud de 48 bits, partiendo de la clave original (64 bits).

b) El segundo consiste en cifrar el mensaje (bloque de 64 bits) utilizando las subclaves del primer paso.

Utilizando como mensaje original (M) el siguiente texto

M = 0123456789ABCDEF

M está en hexadecimal (máximo 16 dígitos), así que se pasará a binario; quedando de la siguiente manera

M=0000000100100011010001010110011111000100110101011110011011111011111

También es necesario contar con una clave original (K) que deberá ser de 16 dígitos hexadecimales, así que: K=133457799BBCDFF1. *K* está en hexadecimal, así que se pasará a binario; quedando de la siguiente manera:

K=0001001100110100010101110111100110011011101111001101111111110001

PASO 1: Creación de las 16 subclaves.

1. Se debe reducir la clave original "K" a 56 bits. Para ello, se realizará una permutación de K de acuerdo a la tabla PC-1. El primer elemento de la tabla es "57", dicho número corresponde al bit 57 de K y este bit será el primer bit de la clave permutada que se llamará "K+". El segundo elemento de la tabla es "49" se localiza el bit 49 de K y dicho bit corresponderá al segundo bit de K+. El último elemento de la tabla es "4" se localiza el bit 4 de la clave original y corresponderá al último bit de K+. Este mismo proceso se realizará con todos los elementos de la tabla - la tabla se recorre por renglones de arriba hacia abajo, donde cada renglón se lee de izquierda a derecha.

   Nota: sólo 56 bits de la clave original aparecen en la clave permutada K+

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Tabla PC-1

Después de realizar la permutación a K se obtiene:

K+=1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

2 Se divide K+ en dos bloques de 28 bits cada uno Quedando así

C_0 = 1111000 0110011 0010101 0101111
D_0 = 0101010 1011001 1001111 0001111

Con C_0 y D_0 definidos, se crean 16 bloques C_n y D_n, 1 n 16 Cada par de bloques C_n y D_n se forma a partir del par previo C_{n-1} D_{n-1}, respectivamente, para n 1, 2, , 16, utilizando la siguiente lista de "desplazamientos izquierdos" del bloque previo Para realizar un desplazamiento izquierdo, se

mueve cada bit un lugar a la izquierda excepto el primero que se coloca al final del bloque.

Número de iteración	Número de desplazamientos a la izquierda
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Esto indica, por ejemplo, que C_3 y D_3 se obtienen de C_2 y D_2, respectivamente, por dos desplazamientos a la izquierda, y C_{16} y D_{16} se obtienen de C_{15} y D_{15}, respectivamente, por un desplazamiento a la izquierda. En todos los casos, un desplazamiento a la izquierda significa una rotación de bits un lugar a la izquierda, así que después de un desplazamiento a la izquierda los bits en las 28 posiciones son los bits que estaban previamente en las posiciones 2, 3, ..., 28, 1.

Siguiendo la lista y usando el par C_0 and D_0 se obtiene.

C_0 = 1111000011001100101010101111
D_0 = 0101010101100110011110001111
C_1 = 1110000110011001010101011111
D_1 = 1010101011001100111100011110

$C_2 = 11000011001100101010101111111$
$D_2 = 01010101100110011111000111101$
$C_3 = 00001100110010101010111111111$
$D_3 = 01010110011001111100011110101$
$C_4 = 00110011001010101011111111100$
$D_4 = 01011001100111110001111010101$
$C_5 = 11001100101010101111111110000$
$D_5 = 01100110011111000111101010101$
$C_6 = 00110010101010111111111000011$
$D_6 = 10011001111000111101010101101$
$C_7 = 11001010101011111111100001100$
$D_7 = 01100111110001111010101010110$
$C_8 = 00101010101111111110000110011$
$D_8 = 10011110001111010101010110011$
$C_9 = 01010101011111111100001100110$
$D_9 = 00111100011110101010101100011$
$C_{10} = 01010101111111110000110011001$
$D_{10} = 11110001111010101010110011001$
$C_{11} = 01010111111111000011001100101$
$D_{11} = 11000111101010101011001100111$
$C_{12} = 01011111111100001100110010101$
$D_{12} = 00011110101010101100110011111$
$C_{13} = 01111111110000110011001010101$
$D_{13} = 01111010101010110011001111100$
$C_{14} = 11111110000110011001010101011$
$D_{14} = 11101010101011001100111100011$
$C_{15} = 11111000011001100101010101111$
$D_{15} = 10101010101100110011111000111$
$C_{16} = 11110000110011001010101011111$
$D_{16} = 01010101011001100111100011111$

3 Se forman las claves K_n, para $1<=n<=16$, al aplicar la tabla de permutación PC-2 a cada uno de los pares C_nD_n. Cada par tiene 56 bits, pero PC-2 sólo utiliza 48

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Tabla PC-2

Por lo tanto, el primer bit de K_n es el bit 14 de C_nD_n, el segundo bit es el 17, y así sucesivamente hasta terminar con el bit 48 de K_n que es el bit 32 de C_nD_n.

Para obtener la primera clave se tiene:

C_1D_1=111000011001100101010101111111010101011001100111100011110

Después de aplicar la permutación de obtiene.

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

Las otras claves que se obtienen de la misma forma son:

K_2 = 011110 011010 111011 011001 110110 111100 100111 100101
K_3 = 010101 011111 110010 001010 010000 101100 111110 011001
K_4 = 011100 101010 110111 010110 110110 110011 010100 011101
K_5 = 011111 001110 110000 000111 111010 110101 001110 101000
K_6 = 011000 111010 010100 111110 010100 000111 101100 101111
K_7 = 111011 001000 010010 110111 111101 100001 100010 111100
K_8 = 111101 111000 101000 111010 110000 010011 101111 111011
K_9 = 111000 001101 101111 101011 111011 011110 011110 000001
K_{10} = 101100 011111 001101 000111 101110 100100 011001 001111
K_{11} = 001000 010101 111111 010011 110111 101101 001110 000110
K_{12} = 011101 010111 000111 110101 100101 000110 011111 101001
K_{13} = 100101 111100 010111 010001 111110 101011 101001 000001
K_{14} = 010111 110100 001110 110111 111100 101110 011100 111010
K_{15} = 101111 111001 000110 001101 001111 010011 111100 001010
K_{16} = 110010 110011 110110 001011 000011 100001 011111 110101

PASO 2: Codificación de cada uno de los bloques de datos de 64 bits.

1. Existe una permutación inicial (IP) de los 64 bits del mensaje de datos M. Ésta reacomoda los bits de acuerdo a la tabla siguiente, denominada tabla IP, donde las entradas muestran el nuevo arreglo de los bits. El bit 58 de M es el primer bit de IP. El bit 50 de M es el segundo bit de IP. El bit 7 de M es el último bit de IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Tabla IP

Tras aplicar la permutación inicial al bloque de texto M se obtiene:

M=0000000100100011010001010111001111000100110101011110011011111101111
IP=1100110000000000110011001111111111111110000101010101111000010101010

2 Se divide el bloque permutado IP en una mitad izquierda L_0 de 32 bits, y una mitad derecha R_0 de 32 bits

L_0 = 1100 1100 0000 0000 1100 1100 1111 1111
R_0 = 1111 0000 1010 1010 1111 0000 1010 1010

Se procede mediante 16 iteraciones, para 1<=n<=16, utilizando una función f la cual opera sobre dos bloques — un bloque de datos de 32 bits y una clave K_n de 48 bits — a producir un bloque de 32 bits. El símbolo + denota la adición XOR, (la adición bit a bit módulo 2). Entonces para n de 1 a 16 se calcula.

L_n R_{n-1}
R_n L_{n-1} $f(R_{n-1},K_n)$

Esto da como resultado un bloque final, para n = 16, de $L_{16}R_{16}$. Esto es, en cada iteración se toman los 32 bits derechos del resultado previo y se convierten en

los 32 bits izquierdos del paso actual. Para los 32 bits derechos del paso actual, se realiza el XOR de los 32 bits izquierdos del paso previo con el cálculo de f.

Para $n = 1$, se tiene:
K_1 = 000110 110000 001011 101111 111111 000111 000001 110010
$L_1 = R_0$ = 1111 0000 1010 1010 1111 0000 1010 1010
$R_1 = L_0 + f(R_0, K_1)$

Para calcular f primero se expande cada bloque R_{n-1} de 32 bits a 48 bits. Esto se hace utilizando una tabla seleccionada que repite algunos de los bits en R_{n-1} A esta tabla seleccionada se le llama la función E. Entonces $E(R_{n-1})$ tiene un bloque de entrada de 32 bits y un bloque de salida de 48 bits.

E es tal que los 48 bits de su salida, escritos como 8 bloques de 6 bits cada uno, se obtienen al seleccionar los bits en sus entradas en orden de acuerdo a la siguiente tabla denominada tabla E.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Tabla E de selección de bit

Entonces los tres primeros bits de $E(R_{n-1})$ son los bits en las posiciones 32, 1 y 2 de R_{n-1} mientras que los 2 últimos bits de $E(R_{n-1})$ son los bits en las posiciones 32 y 1

Se calcula $E(R_0)$ de R_0 como sigue.

R_0 = 1111 0000 1010 1010 1111 0000 1010 1010
$E(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 010101

Hay que notar que cada bloque original de 4 bits ha sido expandido a un bloque de 6 bits de salida

En el cálculo de f se realiza un XOR de la salida $\mathbb{E}(R_{n-1})$ con la clave K_n: $K_n + \mathbb{E}(R_{n-1})$.

Para K_1 , $\mathbb{E}(R_0)$, se tiene:

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010
$\mathbb{E}(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 010101
$K_1+\mathbb{E}(R_0)$ = 011000 010001 011110 111010 100001 100110 010100 100111.
Aún no se termina el cálculo de la función f . Hasta este momento se expandió R_{n-1} de 32 bits a 48 bits, utilizando la tabla seleccionada, y realizando XOR al resultado con la clave K_n. Ahora se tienen 48 bits, u ocho grupos de seis bits. Se utilizan los grupos de seis bits como direcciones en las tablas llamadas "cajas-S" Cada grupo de seis bits da una dirección en una caja-S diferente. Localizado en esa dirección existe un número de 4 bits, el cual reemplaza al original de 6 bits. El resultado es, que los ocho grupos de 6 bits son transformados en grupos de 4 bits (las salidas de 4 bits de las cajas-S) para un total de 32 bits.

Se escribe el resultado previo, el cual es de 48 bits.
$K_n + \mathbb{E}(R_{n-1}) = B_1B_2B_3B_4B_5B_6B_7B_8$, donde cada B_i es un grupo de seis bits.

Ahora se calcula $S(B) = S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$ donde $S_i(B_i)$ se refiere a la salida de la i-ésima caja-S
Para repetir, cada una de las funciones $S1$, $S2$,..., $S8$, se toma un bloque de 6 bits como entradas y arroja un bloque de 4 bits como salida. La tabla para determinar S_1 se muestra y explica a continuación.

		Número de columna															
		0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
Número de renglón	*0*	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Tabla S1

Si S_1 es la función definida en esta tabla y B es un bloque de 6 bits, entonces $S_1(B)$ esta determinada como sigue: El primero y el último bit de B representa en base 2 un número en el rango decimal 0 a 3 (en binario 00 a 11). Permitiendo que ese número sea i. Los 4 bits intermedios de B representan en

base 2 un número en el rango decimal 0 a 15 (en binario 0000 a 1111). Ese número será *j* A continuación se debe buscar en la tabla el número en el renglón *i*-ésimo y la columna *j*-ésima, es un número en el rango 0 a 15 y está representado únicamente por un bloque de 4 bits. Ese bloque es la salida el bloque es la salida $S_1(B)$ de S_1 para la entrada B. Por ejemplo, para el bloque de entrada B = 011011 el primer bit es "0" y el último bit "1" dando 01 como el renglón (este es el renglón 1). Los cuatro bits intermedios son "1101". Este es el equivalente binario del decimal 13, así que la columna es la columna número 13. En el renglón 1, columna 13 aparece el 5. Esto determina la salida; 5 es en binario 0101, así que la salida es 0101. Por consiguiente $S_1(011011) = 0101$.
Las tablas que definen las funciones $S_1,...,S_8$ son las siguientes:

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Tabla S1

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Tabla S2

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Tabla S3

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Tabla S4

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Tabla S5

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Tabla S6

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Tabla S7

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Tabla S8

Para la primera iteración, se obtiene como la salida de las ocho cajas-S:

$K_1 + \mathbb{E}(R_0) = 011000\ 010001\ 011110\ 111010\ 100001\ 100110\ 010100\ 100111.$
$S(B) = S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$
$S(B) = 0101\ 1100\ 1000\ 0010\ 1011\ 0101\ 1001\ 0111$

La fase final en el cálculo de f es hacer una permutación P de la salida de la caja-S para obtener el valor final de f.

$$f \quad P(S_1(B_1)S_2(B_2)...S_8(B_8))$$

La permutación P esta defina en la siguiente tabla denominada tabla S. P produce una salida de 32 bits a partir de una entrada de 32 bits al permutar los bits del bloque de entrada

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Tabla S

De la salida de las ocho cajas-S:

$S(B) = S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$

$S(B)$ = 0101 1100 1000 0010 1011 0101 1001 0111

Se obtiene

f = 0010 0011 0100 1010 1010 1001 1011 1011

$R_1 = L_0 + f(R_0, K_1)$

R_1= 1100 1100 0000 0000 1100 1100 1111 1111
+ 0010 0011 0100 1010 1010 1001 1011 1011

R_1= 1110 1111 0100 1010 0110 0101 0100 0100

En la siguiente iteración se tiene $L_2 = R_1$, que es el bloque que se calculó, y enseguida se calcula $R_2 = L_1 + f(R_1, K_2)$, y así para las 16 iteraciones

3 Al final de la iteración 16 se tienen los bloques L_{16} y R_{16}. Entonces se invierte el orden de los dos bloques dentro del bloque de 64 bits $R_{16}L_{16}$ y se aplica una permutación final IP^{-1} como está definida por la tabla siguiente denominada tabla IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Tabla IP^{-1}

Esto es, la salida del algoritmo tiene el bit 40 del bloque de presalida como su primer bit, el bit 8 como su segundo bit, y así hasta que el bit 25 del bloque de presalida es el último bit de salida.

Si se procesan todos los 16 bloques se obtiene en la iteración 16

L_{16} = 0100 0011 0100 0010 0011 0010 0011 0100
R_{16} = 0000 1010 0100 1100 1101 1001 1001 0101

Si se invierte el orden de estos dos bloques y se le aplica la permutación se obtiene·

$R_{16}L_{16}$=00001010010011001101100110010101010000110100001000110010001101000
IP^{-1}=10000101111010000001001101010100000011111000010101011010000000101

Que en hexadecimal es 85E813540F0AB405.
La forma cifrada del mensaje en claro M = 0123456789ABCDEF, es el mensaje cifrado C = 85E813540F0AB405.

El descifrado es simplemente el inverso del cifrado, esto se logra al seguir paso a paso los puntos descritos en el paso 2, sólo que se utiliza C en lugar de M y se invierte el orden en el cual las subclaves son aplicadas, es decir, la primera subclave que se aplica es K_{16}, la segunda K_{15} y así hasta que la última en aplicarse es K_1.

Desarrollo:

1 Tomando como base la explicación de cifrado del algoritmo DES

a) Plantear un nuevo mensaje M

b) Plantear una nueva clave K

c) Realizar el PASO 1 para obtener las 16 subclaves

d) Realizar el PASO 2 para obtener el criptograma

2 Comprobar con la aplicación lo obtenido en el punto anterior, para ello realizar lo siguiente

a) Escribir el mensaje M en hexadecimal, dicho mensaje debe tener como máximo 16 dígitos.

b) Presionar el botón "Leer Mensaje".

c) Ingresar la clave K en binario, cuya longitud debe ser forzosamente de 64 bits.

d) Oprimir el botón "Cifrar Paso 1", comparar las subclaves obtenidas en el punto 1.c con las que se muestran en pantalla.

e) Oprimir el botón "Cifrar Paso 2", comparar el criptograma obtenido en el punto 1.d con el que se muestra en pantalla.

f) Oprimir el botón "Descifrar" para observar la segunda parte del algoritmo.

3. Haciendo uso de la aplicación:

a) Escribir el mensaje M en hexadecimal, planteado en el punto1 a

b) Presionar el botón "Leer Mensaje".

c) Ingresar una nueva clave K en binario u oprimir el botón "Crear clave"

d) Oprimir el botón "Cifrar Paso 1".

e) Oprimir el botón "Cifrar Paso 2" y anotar el criptograma que se muestra en pantalla

f) Oprimir el botón "Descifrar" para observar la segunda parte del algoritmo.

Cuestionario:

1. ¿A que tipo de criptografía pertenece el algoritmo DES? ¿Por qué?

2. ¿En qué favorece, al algoritmo DES, que la clave K sea de 64 bits?

3. En el punto 2 se obtuvo un criptograma diferente al del punto 3 ¿A que se debe dicho resultado?

4. ¿Cuál es la importancia de la opción "crear la clave" en el punto 3.c? , para que esta opción sea segura ¿qué aspectos deben cuidarse?

5. Dé sus conclusiones.

PRÁCTICA 5. POLÍTICAS DE SEGURIDAD

Objetivo: El alumno planteará algunas políticas de seguridad que se deben seguir para el buen manejo de la información dentro de una empresa con base en los objetivos de ésta.

Introducción: ¿Qué es una política de seguridad?

La **política de seguridad**, en el mundo real, es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma

Una **política de seguridad informática** debe fielmente representar una política del mundo real y además debe interactuar con la política de recursos, por ejemplo, políticas en el manejo de transacciones, aplicaciones, bases de datos En ella, se deben considerar las amenazas contra las computadoras, especificando cuáles son dichas amenazas y cómo contraatacarlas.

En la actualidad, se ha incrementado la dependencia de una organización en su información, la cual es considerada como uno de sus activos más valiosos El procesamiento, almacenamiento y distribución de información, son llevados a cabo por personas, quienes deben observar cierta conducta y conciencia en el manejo de información.

Esta dependencia en la información, ha impulsado la necesidad de contar con lineamientos que conduzcan a su buen uso y cuidado, por lo que se debe desarrollar un documento, a fin de que todos los involucrados en el manejo de información, observen las normas de seguridad indicadas, dicho documento debe ser redactado en un lenguaje natural, claramente y sin ambigüedades posibles El documento deberá especificar qué propiedades de seguridad se pretenden cubrir con la aplicación de las políticas y la manera de usarlas.

A continuación se presenta la *política de seguridad que se utiliza para la protección de la información* de una organización que tiene como **objetivo** Establecer los lineamientos de seguridad para garantizar la integridad, confidencialidad y disponibilidad de los datos que son procesados fuera de su sistema central y aquellos obtenidos a partir de este para ser explotados en otras plataformas, equipos o sistemas de procesamiento de datos

Y con base en este objetivo se pretende obtener los siguientes beneficios: Garantizar que la información manejada fuera del sistema central, cuente con los elementos necesarios para asegurar su protección contra alteración, divulgación, malversación o negación de acceso no autorizados, permitiendo la continuidad de las operaciones en las áreas de negocio donde se maneja información sensitiva[1].

Con dicho objetivo, con los beneficios que se lograrán y considerando los siguientes puntos: obtención extracción, acceso, clasificación y copias de la información, enseguida se detallan las políticas de seguridad que se utilizarán para la protección de la información:

1. *Autorización para obtención de información.*
   La obtención de información del sistema central, deberá ser bajo autorización expresa de su propietario.

2. *Responsabilidad de clasificación de información.*
   El propietario de la información, es el responsable de realizar la clasificación de información, de acuerdo a su sensibilidad como secreta, confidencial, privada y no clasificada

3. *Autorización para realizar copias de información.*
   No deben realizarse copias o impresiones adicionales de información sensitiva, sin la autorización del propietario.

4. *Numeración secuencial en documentos con información sensitiva.*
   Con la finalidad de evitar fugas de información y asegurar que la información está completa, todos los documentos impresos que contengan información sensitiva, deben indicar el número de página actual y aquél correspondiente al total de páginas del documento (ejemplo "página X de Y")

5. *Etiquetado externo de documentos con información sensitiva.*
   Con la finalidad de concientizar a los empleados respecto al manejo que se debe dar a la información, conforme a su nivel de sensibilidad, las cintas, disquetes, CD's y otros medios magnéticos de almacenamiento que contengan información sensitiva, deben ser marcados (etiquetados) externamente, con la clasificación correspondiente

[1] La información sensitiva es aquélla que es clasificada como secreta, confidencial o privada

6. Uso de mecanismos para el control de acceso.

La información considerada como sensitiva, residente en un sistema de cómputo, debe estar provista por mecanismos de control de acceso para asegurar que no sea revelada, modificada, eliminada o transformada a un estado inservible, por acciones impropias o no autorizadas.

7. Extracción de información sensitiva de la organización

No debe extraerse de la organización, la información sensitiva, salvo autorización del propietario Se hace excepción para enviar esta información a los sitios de respaldo autorizados.

8. Sistemas que requieren control de acceso basados en contraseñas.

Cuando se maneje información sensitiva en un sistema menor (PC, LAN, etc), éste deberá proveer y mantener controles de acceso basados en contraseñas (passwords)

9. Estado físico de las computadoras con información sensitiva.

Las computadoras que contengan o procesen información sensitiva, deberán recibir mantenimiento constante con el fin de evitar posibles fallas que provoquen la no disponibilidad de la información

10. Escritorios y áreas de trabajo con información sensitiva.

Los usuarios que utilicen información sensitiva, tienen la obligación de resguardarla bajo llave durante horarios no laborables Los documentos, disquetes, cintas, etc., que contengan este tipo de información, no deben permanecer sobre escritorios y áreas de trabajo durante los períodos no laborables

11. Restricción de acceso.

Los privilegios de los usuarios y programas deberán ser restringidos, de acuerdo a las aplicaciones que deben utilizar para llevar a cabo sus actividades laborales

12. Negación de acceso predeterminada.

Los permisos de control de acceso a datos y programas, deben establecer de manera predeterminada el "no acceso" a usuarios no autorizados, es decir, un usuario que pertenece a un área determinada no podrá tener acceso a la información de otras áreas a menos que éstas necesiten compartirla

13. Utilerías de sistemas residentes en medios de almacenamiento con información sensitiva.

Los discos y otros medios de almacenamiento de información en línea, utilizados, no deben contener compiladores, ensambladores, editores de texto, procesadores de texto u otras utilerías de uso general que pudieran ser utilizadas para comprometer la seguridad de la información.

Desarrollo:

1. Tomando como base el objetivo y los beneficios que se plantearon en la introducción:

   a) Proponer y plantear una *política de seguridad para distribuir la información* (de la misma manera como se obtuvo la *política de seguridad para la protección de la información* descrita en la introducción). Tomar en cuenta los siguientes puntos: mensajería, correo electrónico, fax, conversaciones telefónicas, equipos portátiles para la distribución.

   b) Proponer y plantear una *política de seguridad para respaldar la información* (de la misma manera como se obtuvo la *política de seguridad para la protección de la información* descrita en la introducción) Considerar número de respaldos, alternativas de respaldo, bitácoras, ubicaciones físicas de los respaldos, pruebas de respaldos, pérdidas por deterioro de los respaldos

2 Establecer el objetivo, los beneficios y la política de seguridad para prevenir la infección de equipos PC's por código malicioso Para la creación de dicha política, hay que considerar los siguientes puntos: antivirus, informar existencia de virus, descompresión de archivos, instalación de aplicaciones dudosas y que no estén permitidas, erradicación de virus

Cuestionario:

1. ¿Por qué cree que es importante que la política de seguridad de una organización esté fundamentada en la misión que tenga dicha organización?

2 ¿Por que cree que una política de seguridad debe ser redactada de manera clara y sin ningun tipo de ambiguedades?

3 De sus conclusiones

APÉNDICE D.
RESPUESTAS DE LAS PRÁCTICAS

Práctica 1. Ataques pasivos

1 Si no supiera cómo están conformadas las tramas, ¿Qué contendrían éstas datos o información? y ¿Por qué lo considera así?

Datos, porque si a la cadena mostrada no se le puede dar una interpretación correcta, se ignora o no se entiende el significado del contenido del mensaje, realmente no serviría de nada el análisis del tráfico si el objetivo principal es enterarme de la información que está circulando.

2. En la pantalla donde se muestran todos los movimientos que realizó una cuenta en el cajero automático – Ver puntos 1.e y 4 – ¿Qué tipo de información se puede obtener de ella?

a) El número de tarjeta que ingresa al cajero.

b) El número de identificación personal

c) La indicación de si existe un envío de datos o si una operación se efectúa o no.

d) El número del cajero automático que está efectuando las transacciones

e) La fecha en que se lleva a cabo la transacción

f) La hora en que se lleva a cabo la transacción

g) Las operaciones que se realizan saldo, disposición de efectivo, traspaso

h) La cantidad de las operaciones realizadas

3 Tomando como base las tramas que se utilizaron para la práctica, ¿Qué modificaría - agregar o quitar campos de las tramas, con el objetivo de proporcionar mayor seguridad en los datos que se envían y/o reciben? y ¿Por qué?

En la trama 2 sería conveniente eliminar los campos correspondientes al número de tarjeta y NIP para que sólo se manden los campos status, terminal, fecha y

5. En la sección de la práctica referente a replicación de datos, ¿Cómo cree que se podrían evitar o qué medidas tomaría para que este tipo de ataques no se presentaran si usted fuera el encargado de supervisar las transacciones que se realizan entre un cajero automático y el banco donde trabaja? Explique

   Se podrían adoptar varias medidas, por ejemplo las siguientes:

   - No se permitiría realizar más de tres transacciones en un intervalo de tiempo muy corto.
   - En caso de reincidir en el intento de realizar muchas transacciones entonces se bloquearía automáticamente la cuenta.
   - En caso de que la transacción sea una disposición de efectivo o traspaso a otra cuenta se pondría una cantidad límite por día.

6 Dé sus conclusiones

Práctica 3. Sustitución y transposición

1 ¿Por qué se dice que la confusión se basa en la sustitución?

Se dice que la confusión se basa en la sustitución porque al tratar de evitar que el texto en claro pueda entenderse fácilmente, cada elemento del texto (bit, letra, grupo de bits o letras) es cambiado por otro elemento, de tal manera que al momento de observar el criptograma, en primera instancia causa una gran confusión, pues al no estar el texto en claro, no se entiende lo que está escrito..

2 ¿A qué tipo de sustitución pertenece el cifrado Vigenère? ¿Por qué?

El cifrado Vigenère pertenece a la sustitución polialfabética porque se introducen múltiples alfabetos de cifrado que se utilizan en rotación de acuerdo con un criterio o clave, el objetivo de este tipo de sustitución es evitar que las letras con mayor frecuencia de aparición no sobresalgan tan claramente

3. ¿Los criptogramas obtenidos en el inciso 1.d son iguales? Sí o no y ¿Por qué?

   No son iguales debido a que la clave empleada para cifrarlos es diferente, lo cual ocasiona que se utilicen renglones distintos de la matriz para cifrar los mensajes, dando así como resultado criptogramas que no son iguales.

4. ¿Por qué se dice que la difusión se basa en la transposición?

   Se dice que la difusión se basa en la transposición porque al tratar de evitar que el texto en claro pueda entenderse fácilmente, se reordenan las letras, es decir, se cambia la posición de los caracteres en un mensaje sin que se cambien por otro elemento, de tal forma que sólo se difumina el mensaje de tal manera que al no estar el texto en claro, no se entiende lo que está escrito.

5 Si en el punto 2.d no se hubiera proporcionado la clave, podría realizarse el punto 2.e? ¿Por qué?

   No, esto se debe a que cada equipo crea su clave, por lo tanto sería muy difícil encontrar los pasos exactos que se utilizaron para cifrar un mensaje, de ahí la importancia de mantener en secreto la clave para evitar que un mensaje sea descifrado por una persona no autorizada.

6 Dé sus conclusiones.

Práctica 4. Algoritmo DES

1 ¿A qué tipo de criptografía pertenece el algoritmo DES? ¿Por qué?

   El algoritmo DES pertenece al tipo de criptografía de clave simétrica o de clave secreta ya que la clave que se emplea para cifrar es la misma que se emplea para descifrar.

2 ¿En qué favorece, al algoritmo DES, que la clave K sea de 64 bits?

   Cuando no se tiene la clave y se desea obtenerla será necesario probar con cada una de las combinaciones posibles que nos permita la longitud de la clave. Es decir, que se tendrían que probar 2^{64} (18,446,744,073,709,551,616) claves para poder descifrar el criptograma. Aunque el número de combinaciones es

demasiado alto, sería posible programar un algoritmo que permita obtener y probar cada una de las combinaciones pero se necesitaría contar con un hardware poderoso, el cuál sería demasiado sería costoso Por lo tanto, si no se conoce la clave secreta sería muy difícil descifrar el mensaje favoreciendo de esta manera que sea robusto el algoritmo DES.

3. En el punto 2 se obtuvo un criptograma diferente al del punto 3 ¿A qué se debe dicho resultado?

   Se debe a que no se está utilizando la misma clave Hay que recordar que: el primer paso para cifrar utiliza la clave original y ésta se emplea para generar las 16 subclaves que se utilizarán a lo largo del algoritmo. Entonces, si se cambia la clave original se realiza el algoritmo, pero se obtendría un criptograma diferente.

4. ¿Cuál es la importancia de la opción "crear la clave" en el punto 3.c? , para que esta opción sea segura ¿qué aspectos deben cuidarse?

   La importancia de esta opción se debe a que de esta forma se puede contar con una clave aleatoria y por lo tanto libre de manipulaciones. Para que esta opción sea segura es necesario que se utilice una clave distinta cada vez que se vaya a cifrar un texto sólo así se evita la posibilidad de repetir claves utilizadas con anterioridad, ya que esto ocasiona que al realizar el análisis del texto cifrado sea fácil notar la frecuencia con la que aparecen ciertas letras, favoreciendo de esta forma a la persona no autorizada, que descripte con menor dificultad dicho criptograma

5 Dé sus conclusiones

Práctica 5. Ataques pasivos

1. ¿Por qué cree que es importante que la política de seguridad de una organización esté fundamentada en la misión que tenga dicha organización?

Porque de acuerdo a la misión que tenga la organización es como se plantean las reglas más adecuadas para dirigir, proteger y distribuir tanto los recursos como la información que se maneja dentro y fuera de la organización, asegurando de esta manera la protección de la información, es decir una

política de seguridad debe garantizar que la misión de la organización se lleve a cabo

2. ¿Por qué cree que una política de seguridad debe ser redactada de manera clara y sin ningún tipo de ambigüedades?
   Debe ser expresada claramente y sin ambigüedades para que tanto las personas que crean la política como quienes la van a aplicar y cumplir la entiendan y no le den interpretaciones que distorsionen el propósito original de la política de seguridad

3 Dé sus conclusiones.

APÉNDICE E.
GLOSARIO DE TÉRMINOS

Amenaza: todo aquello que intenta o pretende destruir, las amenazas provienen de diversas fuentes.

Ataque activo: se nombran así debido a que implica algún tipo de modificación del flujo de datos o la creación de un falso flujo de datos.

Ataque de seguridad: es la realización de una amenaza, un ataque tiene diversos objetivos.

Ataque pasivo: recibe su nombre debido a que el atacante no altera en ningún momento la información, es decir, únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida.

Caballo de Troya: es un programa malicioso que aparenta ser un programa benigno. Puede robar contraseñas, infectar una computadora con un virus o incluso actuar como puerta trasera para espiar a los usuarios, registrando las pulsaciones de teclas y transmitiéndolas a un tercero a través de TCP/IP.

CCITSE (Common Criteria for Information Technology Security). Criterios Comunes para Seguridad de Tecnología de la Información desarrollados en enero de 1996 por Estados Unidos, el Reino Unido, Alemania, Francia y los Países bajos

Código malicioso: cualquier software que entra en un sistema de cómputo sin ser invitado e intenta romper las reglas para robar, destruir o alterar la información

Cracker: persona que irrumpe dentro de un sistema de cómputo ajeno para utilizarlo sin autorización, esta intrusión puede realizarse por beneficio, venganza o sólo porque se da la oportunidad

Criptoanálisis: se refiere a la ruptura o derrota de la criptografía, es decir, es el proceso que sin tener la autorización correspondiente intenta descubrir el texto o la clave

Criptoanalista: es la persona no autorizada que intenta conocer la clave o el mensaje original utilizando para ello el criptoanálisis

Criptografía: es el arte y ciencia de transformar la información para asegurar un secreto, la autenticidad de éste o ambas y prevenir a los usuarios de acciones no autorizadas o ilegales en contra de la información.

Criptograma: es el texto o mensaje cifrado.

Criptólogo: es la persona que hace uso de la criptografía para desarrollar algoritmos, técnicas y mecanismos para cifrar y descifrar información.

DES: Data Encryption Standard, es un algoritmo de cifrado en bloques, introducido en 197, donde la longitud de cada bloque es de 64 bits y la longitud de la clave es de 56 bits

Diffie-Hellman: el primer algoritmo de clave pública que definía la criptografía de clave pública, fue introducido por Diffie y Hellman en 1976, los cuales propusieron que se utilizara dicha idea para distribuir las claves secretas de cifrado.

Encaminador: Es un dispositivo de red que posee dos o más puertos de conexión y que comunica dos redes distintas, además es capaz de determinar en qué red se encuentra el dispositivo al que se desea conectar (también conocido como router)

Escudo: técnica, procedimiento o cualquier otra medida que reduce la vulnerabilidad

Firewall: colección de componentes colocados entre una red interna y una red externa para que sólo el tráfico que es autorizado por la política de seguridad de la red interna esté permitido para pasar

Gateway: es un nodo de interconexión entre dos redes incompatibles, es decir, es un sistema capaz de enviar información entre dos o más redes con estándares, arquitecturas y protocolos diferentes, la función principal de dicha herramienta es interceptar los datos para traducirlos al lenguaje o protocolo que utiliza la conexión de entrada

Gusano: es un programa que se propaga a sí mismo por una red, normalmente a través de correo electrónico, TCP/IP o una unidad de disco. Se reproduce a sí mismo a medida que se ejecuta

Hacker: Persona que disfruta con la exploración de los detalles de los sistemas programables y cómo aprovechar sus posibilidades; a diferencia de la mayoría de los usuarios, que prefieren aprender sólo lo imprescindible

IDEA: International Data Encryption Algorithm, es un cifrado de bloque simétrico, donde la clave de 128 bits es utilizada para generar 16 subclaves.

Información: todo mensaje (conjunto de datos) que: al receptor le interese, le entienda o lo ignore antes de recibirlo

IP: Internet Protocol.

IT: Tecnología de la información.

Mecanismo de seguridad: conjunto de elementos o procesos que implementan un servicio de seguridad, es decir, es aquel mecanismo que está diseñado para detectar, prevenir o recobrarse de un ataque de seguridad

Método asimétrico: es aquél método que para cifrar utiliza funciones unidireccionales, esto es, que requiere de dos claves, una para cifrar y otra para descifrar

Método simétrico: es aquél método que para cifrar utiliza funciones bidireccionales esto es, que requiere de una sola clave para cifrar y descifrar

Misión: es el poder que se da a un enviado para desempeñar algún cometido Es la orden dada para determinado fin.

Modelo de seguridad: es la presentación formal de una política de seguridad ejecutada por el sistema

Perpetrador: es un individuo que se basa en cualquier medio para cometer un delito o culpa grave

Política de seguridad: conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad

E. GLOSARIO DE TÉRMINOS

Proxy: es un sistema intermediario entre anfitriones internos de una red y los anfitriones de Internet de forma tal que recibe las requisiciones de unos y se las pasa a los otros previa verificación de accesos y privilegios.

RSA: algoritmo de clave pública desarrollado por Ron Rivest, Adi Shamir y Len Adleman en MIT 1978. El algoritmo está basado en la dificultad para realizar factorizaciones de números largos (128 dígitos)

Seguridad: Confianza, tranquilidad, certidumbre procedente de la idea de que no hay peligro que temer, todo está bien.

Seguridad de la información: se refiere a la prevención y a la protección, a través de ciertos mecanismos, para evitar que ocurra de manera accidental o intencional, la transferencia, modificación, fusión o destrucción no autorizada de la información con la que se obtiene confianza en que la información está debidamente resguardada y que no hay peligro que temer

Seguridad de la red: es la protección de los recursos de la red, la información y servicios en contra de las amenazas de seguridad.

Seguridad informática: nombre genérico dado a una colección de herramientas diseñadas para proteger datos y detener a los perpetradores.

Servicio de seguridad: es aquél que está dirigido a evitar ataques de seguridad desde un aspecto muy particular buscando la seguridad de un sistema de información y el flujo de la información de una organización Los principales servicios de seguridad son control de acceso, confidencialidad, integridad, disponibilidad y no repudio

Servicios proxy: su función principal es la de acelerar las peticiones mediante mecanismos de caché (memoria intermedia), evitando así la conexión al servidor remoto y haciendo más rápida por tanto la obtención de la información

S-HTTP: Secure Hypertext Transfer Protocol

SSL: Secure Socket Layer

TCP/IP: Transmission Control Protocol Internet Protocol

TCSEC: Trusted Computer Security Evaluation Criteria or Orange Book.

URL: Universal Resource Locator.

Virus: los virus son programas que infectan documentos o sistemas mediante la inserción o la agregación de una copia de sí mismo o mediante la reescritura de archivos completos. Los virus trabajan sin el conocimiento ni la autorización del usuario.

Vulnerabilidad: es una debilidad que puede ser explotada para violar la seguridad.

WWW: World Wide Web.

CAPÍTULO 11.
BIBLIOGRAFÍA

[1]. Algoritmo DES
http://www.inei gob.pe/cpi/bancopub/libfree/lib620/cap0505.htm

[2]. Amenazas, ataques y vulnerabilidades
http://it.unex.es/sypi/articulo/ataques.htm

[3]. Amenazas, ataques, vulnerabilidades
http://spisa.act.uji.es/SPI/TEORIA/Temario/tema1/

[4]. Amenazas, servicios y mecanismos
http.//www.iec.csic.es/criptonomicon/seguridad.html

[5]. Amenazas y ataques a la seguridad
http.//ttt.epsg.upv.es/~juamelju/Seguridad/paginas/pag_seguridad htm

[6]. Aspectos generales de la seguridad de la información
http://www inei gob.pe/cpi/bancopub/libfree/lib611/0300.HTM

[7] Ataques, servicios y mecanismos de seguridad
http //ttt.epsg upv es/~juamelju/Seguridad/paginas/pag_seguridad htm

[8] Autenticación
http //www.inei.gob.pe/cpi/bancopub/libfree/lib620/cap0402.htm

[9] Bobadilla, Jesús *Superutilidades para webmasters*. España, Mc-Graw Hill, 1999

[10]. Certificación
http.//www inei gob pe/cpi/bancopub/libfree/lib620/cap0507.htm

[11] Common criteria version 2 1 / ISO IS 15408
http.//csrc nist.gov/cc/ccv20/ccv2list htm

[12] Common Criteria
http //www microsoft com/TechNet/security/secureev asp

[13] Common Criteria
http · www tno nl instit fel refs info html

[14]. Common Criteria
http://www.commoncriteria.org

[15]. Control de acceso
http://www.inei.gob.pe/cpi/bancopub/libfree/lib620/cap0507.htm
http://www.inei.gob.pe/cpi/bancopub/libfree/lib620/cap0406.htm

[16]. Criptografía simétrica
http://www.inei.gob.pe/cpi/bancopub/libfree/lib620/cap0506.htm

[17]. Definiciones de hacker y cracker
http://www.seguridadcorporativa.org/seguridadcorporativa/perfilesamenazas.html

[18]. Denning Dorothy. *Information Warfare and Security.*E.U A. Adisson Wesley. 2000

[19] Delitos informáticos: virus, gusanos.
http://tiny.uasnet.mx/prof/cln/der/silvia/tipos.htm

[20] Determining Security Requirements for complex systems with the Orange Book
http://chacs.nrl.navy.mil/publications/CHACS/Before1990/1985landwehr-ncsc.html

[21]. Diferencia entre hacker y cracker
http://bbs.seker.es/~alvy/Hacker-Cracker.html

[22] FAQ Firewalls
http://www.interhack.net/pubs/fwfaq/

[23] Firewalls
http://www.adm.salvador.edu.ar/sistemas/teleinformatica/seguridad.htm

[24] Firewalls
http://penta2.ufrgs.br/gereseg/unlp/t12home.htm

[25] Firewalls
http://www.tempel.es/tempelredcom/tutor/firewall.html

[26] Firewalls-FTP
http://oocity.umu.es/[illegible]/telecom/sist.red/public.htm/ftp.htm

[27] Firma digital
http://www inei.gob pe/cpi/bancopub/libfree/lib620/cap0507.htm

[28] Fúster, Amparo. *Técnicas Criptográficas de protección de datos*. Colombia, Alfaomega, 1998

[29]. Glosario de términos de criptología
http://www.cita.es/textos/glosar htm

[30]. Información descriptiva de firewalls
http //www.carsoft.com ar/Firewall htm

[31]. Integridad
http //www.inei gob pe/cpi/bancopub/libfree/lib620/cap0405.htm

[32]. Integridad de datos
http //www.inei gob pe/cpi/bancopub/libfree/lib620/cap0405 htm

[33] Intercambio de autenticación
http //www inei gob pe/cpi/bancopub/libfree/lib620/cap0402 htm

[34] Introduction to Modular arithmetic
http //www cs usask.ca/resources/tutorials/csconcepts/numbertheory/tutorial/trail/tp03 html

[35] Kou, Weidong *Networking Security and standards* E U A Kluwer Academic Publishers, 1997.

[36] Mecanismos de seguridad
http //www iec csic es/criptonomicon/mecanism html

[37] Mecanismos de seguridad
http //a01-unix.lab inf uc3m es/~sblanco/Seg_Redes/Seg_Redes_Mecanis_Seg htm

[38] Mecanismos de seguridad
http //www geocities com/CapeCanaveral/2566/intro/mecanism html

[39] Mecanismos de seguridad
http www disc ua es asignaturas/rc trabajos/criptografia paginas mecanis html

[40]. Mecanismos de seguridad
http://www.svnet.org.sv/lpgcol61.html

[41]. Mecanismos de seguridad
http://det.bi.ehu.es/~isa/asignaturas/tema7/pagina2.html

[42]. Mecanismos de seguridad
http://det.bi.ehu.es/~isa/asignaturas/tema8/servicios.htm

[43]. Mecanismos de seguridad
http://www.el-mundo.es/su-ordenador/SORnumeros/98/SOR147/SOR147mensaje.html

[44]. Mecanismos de seguridad
http://ulises.umh.es/te/docencia/proyectos/Trabajos_Redes/onblur/sei/cripto.htm

[45]. Pérez, Judith "La seguridad en línea es vital". En El Universal, Universo de la computación. 11 de junio de 2001

[46] Políticas de seguridad
http //www inei.gob.pe/cpi/bancopub/libfree/lib611/0300 HTM

[47] Principios de criptografía, definiciones
http://www inei gob.pe/cpi/bancopub/libfree/lib620/cap0501.htm

[48] Privacidad y confidencialidad
http //www.inei.gob pe/cpi/bancopub/libfree/lib620/cap0404.htm

[49] Protección especial de la información
http //www inei gob.pe/cpi/bancopub/libfree/lib611/0300 HTM

[50] ¿Qué es un firewall?
http //www baja gob mx/organizacion/dgi/biblioteca/ei/ei10/art_11.htm

[51] ¿Qué mecanismos de seguridad existen?
http //www uah es/servicios/ssii/Seguridad/FAQs shtm

[52] Seguridad en Internet
http www inei gob pe cpi bancopub libfree lib620 indice htm

[53]. Seguridad informática, definiciones
http://spisa.act.uji.es/SPI/TEORIA/Temario/tema1/

[54]. Servicios de seguridad
http://a01-unix.lab.inf.uc3m.es/~sblanco/Seg_Redes/Pagina_Redes.htm

[55]. Servicios de seguridad
http://www.onnet.es/03003001.htm

[56]. Servicios y Mecanismos de seguridad
http://www.dat.etsit.upm.es/~mmonjas/cripto/01 html

[57]. Stallings, William. *Network Security Essentials: Applications and Standars*. E.U.A., Prentice Hall, 2000.

[58] Summers, Rita. *Secure Computing, Threats and Safeguards*. E U A., Mc Graw Hill, 1997

[59]. Sustitución, Transposición, Cifrado Vigenère
http //www.inei.gob.pe/cpi/bancopub/libfree/lib620/cap0504 htm

[60] Versión 6 de IP (IPV6)
http://faq.v6.wide.ad jp/index html

[61] Versión 6 de IP (IPV6)
http://www.v6.sfc.wide ad jp/index html

[62] Versión 6 de IP (IPV6)
http //www.ipv6.org/

[63] Versión 4 y 6 de IP (IPV4 e IPV6)
http //www.disc ua.es/asignaturas/rc/trabajos/ip/indice.html

[64] Versión 6 de IP (IPV6)
http //members nbci com/newtech/ip6 html

[65] Versión 6 de IP (IPV6)
http info telecom-co net unidadtrans gruposrd internet temas ipv6 htm

[66] Virus
http.//tejo.usal es/~nines/d alumnos/virus/virus2.htm

[67]. Wyatt, Allen *La magia de Internet.* México, Mc Graw Hill, 1994