VNIVERSIDAD NACIONAL
AVENOMA DE
MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGÓN

"SEGURIDAD CON IPSEC"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN
P R E S E N T A:

MARCELINO PIÑA FEREGRINO

ASESOR DE TESIS:
ING. ERNESTO PEÑALOZA

MÉXICO **2003**

A alguien muy especial mis padres:

"Por todo el cariño, amor y comprensión que durante toda la vida me han dado. Por la firmeza y valor que en mi inculcaron para realizar mis metas. !Gracias queridos padres!."

Jose Carmen y Alicia

A mi querido esposa: Blanquita

A quién tanto quiero y admiro, por que gracias a su cariño, sus exhortaciones constantes y su ayuda, finalice este trabajo.

A mis dos chiquitines:

Quienes me alientan una grandes ilusiones.

A Dios:

Por la vida que me dió y la oportunidad que me dá de convivir con toda esta maravillosa gente.

Y un agradecimiento muy especial al Ing Ernesto Peñaloza por que siempre me supo conducir para desarrollar esta Tesis.

CONTENIDO

Introducción

En la última década la creciente inversión y desarrollo de empresas en el país, y más generalmente en el mundo, así como el crecimiento de instituciones bancarias, educativas, de servicios y de Internet hace de las comunicaciones de datos la llave que les permite satisfacer fácilmente sus necesidades primordiales, como son: manejar grandes volúmenes de información y, al mismo tiempo, mantenerse informado de lo que ocurre en su empresa.

Otro aspecto muy importante, el cual esta influyendo para que las empresas adopten las comunicaciones de datos, es la interconectividad e interoperabilidad entre diferentes sistemas; esto es, modelos con arquitectura abierta, que constituye un verdadero sistema de integración empresarial conectando redes locales con redes privadas y redes públicas, como Internet.

Los nuevos negocios están manejando múltiples cambios en sus fases. El termino seguridad en redes empresariales están convirtiéndose mas común, de como los corporativos empiezan a entender y administrar los riesgos con el desarrollo de aplicaciones por Internet. La seguridad en redes es compleja por la abundancia de tecnologías en seguridad en todo el mundo.

La comunidad de Internet ha desarrollado aplicaciones con mecanismos de Seguridad en diferentes áreas como el correo electrónico (S/MIME, PGP) cliente-servidor (Kerberos) Web Access (SSL) y otros. El standard defacto utilizado por Internet para comunicarse es el stack TCP/IP y en lo que se refiere al tema de seguridad en redes, es el protocolo IPSec.

El propósito del presento trabajo es entender los fundamentos de seguridad del protocolo IPSec y realizar una implementación en una red empresarial entre dos puntos remotos a través de Internet. Veremos algunos detalles de como se compone el protocolo TCP/IP, algunos temas básicos de criptografía hasta llegar al standard IPSec revisándolo a detalle en Flexibilidad, independencia, seguridad, complejidad en su administración de llaves y escalabilidad. Finalmente implementaremos una infraestructura corporativa a través de Internet probando cada uno de las características anteriores, por lo que este trabajo se organizo de la siguiente manera:

Capitulo I. Se describe características de lo que es un protocolo en forma general para luego aplicarlo en especifico a los protocolos dentro de TCP/IP.

Capitulo II. Se desarrollan los fundamentos de la criptografía y sus aplicaciones en la seguridad en redes y los requerimientos para la seguridad de información dentro de cualquier organización, los cuales consisten en prevenir, detectar y corregir las alteraciones a causa de la transmisión de información.

El Capitulo III. El elemento central de Internet es TCP/IP, la seguridad en el nivel de red IP es importante en el diseño en un esquema de seguridad, en este capitulo veremos el desarrollo de los esquemas de seguridad en IP versión 4 (IPv4) utilizando la arquitectura IPSec. Detallaremos las tres áreas funcionales: autenticación, confidencialidad y administración de llaves.

La ultima parte, el Capitulo IV se implementa y se define una política de seguridad sobre un escenario en una red empresarial, con configuraciones especificas en equipos de comunicaciones marca Cisco. Estas configuraciones varían dependiendo de la política de seguridad pero sirven como una guía. Se muestran algunos líneas de monitoreo proveniente del Sistema Operativo en los equipos enrutadores Cisco, para entender sus funcionalidades observar que puede ser útil esta información para diagnostico de algún problema.

CAPITULO 1
PROTOCOLOS

1 Protocolos.

1.1 Concepto de Protocolo de Comunicación.

Los protocolos de comunicación son las reglas de información entre ellos. Pueden ser realizados por un programa de computadora y un conjunto de circuitos, dependiendo de la complejidad del protocolo. La palabra protocolo surgió en la década de los 70's, después de que Lynch y Barlett propusieron en 1968 y 1969 los primeros sistemas de control de línea, cuya finalidad principal era mejorar la confiabilidad en la transmisión.

1.1.1 Fases de un Protocolo de Comunicación.

En general, cualquier nivel de protocolo de comunicaciones puede decirse que consta de tres fases que son:

1. Establecimiento.
2. Transferencia de la información.
3. Liberación.

Cualquiera de los 7 niveles de la estructura de OSI, se mencionará posteriormente, puede definirse en función de estas tres fases. Ahora que un nivel determinado, puede requerir de los servicios del nivel inferior, para poder completar una determinada fase.

1.1.2 Sintaxis y Semántica.

En general, podemos decir que la especificación o definición de un protocolo se obtiene determinando como deben realizarse las tres fases antes aludidas. Dicha definición tiene dos aspectos que son la sintaxis o formato con que deben transmitirse las unidades de intercambio de la información y la semántica o significado que tienen los distintos tipos de unidad de intercambio de información y los campos de control de las unidades que maneja el protocolo.

La sintaxis del protocolo representa la estructura que deben tener los encabezados y terminaciones aludidas y la semántica representa el significado de cada uno de los elementos de control que acompañan a la información y el significado de los mensajes de control que pueden intercambiar los protocolos, además de la información.

1.1.3 Funciones.

Algunas de las funciones más comunes de los protocolos de comunicación son:

1. Fragmentación y reensamble.
2. Encapsulado.
3. Control de conexión.
4. Control de flujo.
5. Control de errores.
6. Sincronización.
7. Control de secuencia.
8. Multiplexaje[1].

[1] Networking Standars
William Stallings
Addison-Wesley
1994

1.1.3.1 Fragmentación y Reensamble.

La información se tiene que fragmentar por alguna o algunas de las siguientes razones:

- La arquitectura del software y/o del hardware del sistema sólo permiten manejar mensajes de una determinada longitud máxima.
- La eficiencia en la transferencia de información, en un canal de datos que introduce errores, es función de la longitud del mensaje.
- Se puede lograr el acceso a medios de comunicación compartidos, como los de las redes locales, de sistemas de radiocomunicación o de satélites, de manera más equitativa.

En la **figura No 1.1** se muestra un esquema del proceso de fragmentación y ensamble. En dicha figura, se le llama entidad al proceso que realiza o ejecuta el protocolo, una de cuyas funciones es la fragmentación. Como puede apreciarse, la entidad A, fragmenta la unidad de información que le entregó el usuario; mientras que la entidad B tiene que reensamblar los fragmentos y entregar al usuario B la unidad de información tal como se la entregó el usuario A a la entidad A[2].

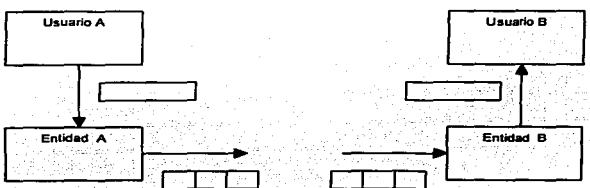


Figura No 1.1. Procesos de Fragmentación y Reensamble

[2]Internetworking with TCP/IP Volume III Comer, Douglas E. and Stevens, David L. Prentice Hall, New Jersey, 1993.

1.1.3.2 Encapsulado.

Encapsular información significa: envolver a la unidad de información del protocolo llamado encabezado, que permiten controlar distintos aspectos de la transferencia de información. Entre otras cosas, la información de control que se agrega está relacionada con:

- Las direcciones de origen y destino de la información.
- Información de control para detectar y corregir posibles errores en la transmisión, como se menciona posteriormente. La información de control para realizar las distintas funciones de control del protocolo. Por ejemplo, contadores de secuencia, bits de control de fragmentación, etc.

Se realiza el encapsulado de la información prácticamente en todos los niveles, tal como lo denota la **figura No 1.2** ilustra el proceso de encapsulado.

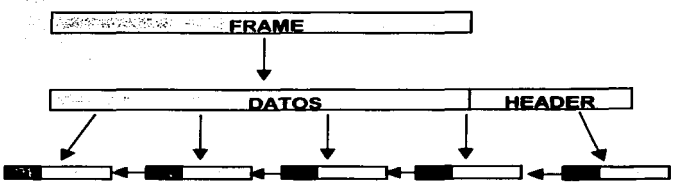


Figura No 1.2. Fragmentación en varios niveles.

1.1.3.3 Control de la conexión.

El control de la conexión se realiza en tres fases, que son: la fase de establecimiento, la fase de transferencia y la fase de desconexión. En la **figura No 1.3** se muestra esquemáticamente esta función.

La función de control de la conexión es aplicable a servicios de transferencia de datos orientados a conexión. Existen también otro tipo de servicios que son orientados a la transferencia de datos sin conexión. En este último caso no se realiza las fases de establecimiento y desconexión sino únicamente la fase de transferencia. Tal es el caso de los servicios de datagrama que se utilizan en distintas redes locales.

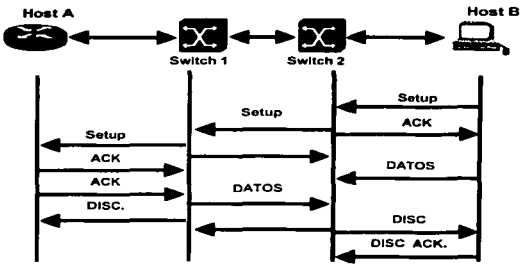


Figura No 1.3. Control de conexión.

1.1.3.4 Control de flujo.

Se controla el flujo de información entre dos entidades por varias razones:

- Para sincronizar la transferencia de manera que se adapte a las velocidades de procesamiento de ambas entidades.
- Para evitar bloqueo por exceso de tráfico en la red.
- Para aprovechar al máximo la capacidad del canal y evitar retrasos indeseables, para lo cual se emplea el mecanismo de ventana que también es un elemento de control de flujo, además de un elemento de control de errores.

1.1.3.5 Control de errores.

Hay diversos tipos de error que una entidad de protocolo puede detectar. Podemos decir que los principales son:

- Pérdida total de una entidad de información.
- Alteración de la información durante la transmisión.
- Alteración de la información de control.

1.1.3.6 Sincronización.

Dos entidades que se comunican por medio de un protocolo, deben sincronizarse adecuadamente. Para esto, deben encontrarse en un estado definido y de acuerdo con los procedimientos del protocolo, por ejemplo: inicialización, verificación, terminación, etc. El estado del protocolo, está determinado por los valores de parámetros como el tamaño de ventana, los valores de los contadores de secuencia, la fase en que se encuentra la conexión, el tiempo restante en un temporizador, etc. Estos parámetros constituyen lo que se conoce como variables de estado. Si no están sincronizadas las dos entidades, obviamente no podrá realizarse la comunicación, ya que los mensajes no tendrán el sentido correcto, por que las entidades se encontrarán en estados en los cuales no le podrán dar la interpretación.

1.1.3.7 Control de secuencia.

Se realiza el control de secuencia por 3 razones importantes:
- Entrega ordenada.
- Control de flujo.
- Control de errores.

La entrega ordenada es una característica fundamental del servicio de circuito virtual ofrecido en cualquier protocolo. La entrega ordenada, en este nivel, facilita los procedimientos de reensamble y almacenamiento temporal de la transmisión de datos, sirve como control de flujo y errores debido a que se identifica a cada paquete que se espera recibir y/o enviar; dicha solicitud se realiza mediante una trama de control de reenvío de trama.

1.1.3.8 Multiplexaje

Como se hizo notar con anterioridad los nombres de conexión sirven de base para podar contar con servicios de multiplexaje. En general, las direcciones, los nombres de conexión y algunos otros elementos de código que permiten etiquetar de alguna manera el flujo de información, se utilizan para desarrollar los servicios de multiplexaje[3]. Como se observa en la figura No 1.4.

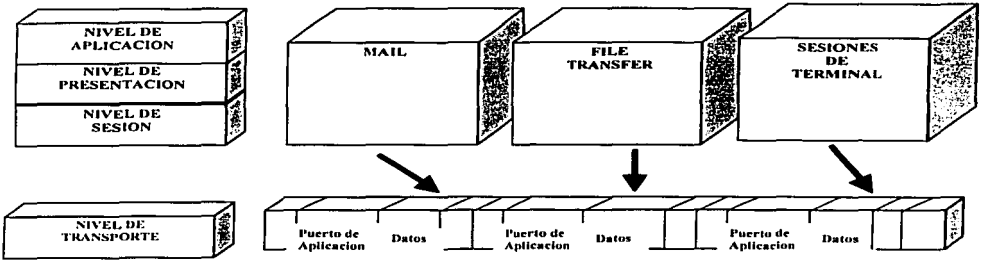


Figura No 1.4. Multiplexaje.

[3] Enhanced IP Services
Donald C Lee
Cisco System
1999

1.2 ARQUITECTURAS

1.2.1 Estructura jerárquica de los Protocolos.

Una de las técnicas que los ingenieros tradicionalmente han usado, para atacar sistemas complejos es subdividirlos y atacar los subproblemas separadamente y después integrar las soluciones parciales. Los protocolos de comunicación son sistemas complejos y para su diseño especificación y entendimiento se han organizado utilizando el concepto de jerarquización. El número de niveles jerárquicos, los nombres de estos niveles y las funciones que realizan han variado, en los distintos desarrollos de redes de computadoras. No obstante la Organización Internacional de Normalización introdujo una estructura que ha orientado el diseño por la mayor parte de los sistemas, como se observa en la figura No 1.5.

1.3 Descripción de la Estructura OSI

Debido a estas circunstancias, en el seno de la Organizacíón Internacional de Normalización (ISO) se propuso y aprobó el modelo para la interconexión de sistemas abiertos. El objetivo que ISO pretende al desarrollar su modelo de referencia es simplemente definir un conjunto de mecanismos que hagan posible la interconexión de sistemas informáticos heterogéneos, utilizando los medios públicos de transmisión de datos. Se trata pues de una forma de asentar bases suficientemente amplias y al mismo tiempo bien definidas que faciliten el desarrollo de sistemas de interconexión. ISO ha procurado que su arquitectura permita la utilización de las normas emitidas por otros organismos internacionales, como el CCITT.

Las diferentes funciones previstas en la arquitectura ISO han sido estructuradas de una forma jerarquizada en siete niveles a los cuales se les asignan distintas funciones complementarias: uno de ellos se ocupa de las relaciones con las aplicaciones que utilizan el sistema de interconexión (nivel de aplicación) los tres siguientes se ocupan de materializar las relaciones con los sistemas informáticos (Niveles de presentación, sesión y transporte) y los tres últimos están orientados a la solución de los problemas de las comunicaciones (Niveles de Red, Enlace y Físico).

Un protocolo en un determinado nivel está definido por los servicios que puede proporcionar a los niveles superiores de la jerarquía, por los que a su vez requiere de las capas inferiores y por los procedimientos de interacción con la capa de su nivel en el software del equipo terminal corresponsal. Esto está indicado en la **figura No 1.6** por las líneas de interfaz entre capas y las líneas de diálogo entre capas del mismo nivel. A continuación se describe en forma breve las funciones que tienen asignadas, los 7 niveles de la estructura OSI.

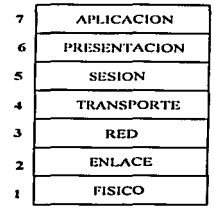


Figura No 1.5. Modelo OSI

Los sistemas desarrollados de acuerdo al modelo de referencia de la ISO tienen una estructura jerárquica de niveles o estractos, como lo indica el esquema de **la figura No 1.6.** Estas formados por un conjunto de bloques situados diferentes niveles estructurales, denominados estractos. Los bloques de un determinado nivel N interactúan utilizando un determinado protocolo de nivel n y los servicios de este nivel n utilizan los servicios de nivel n - 1 proporcionados por los bloques de nivel inferior, mediante un acceso a ellos. La estructura de los niveles inferiores es desconocida para el nivel N y solo toma en cuenta los servicios proporcionados por el nivel n - 1 los entes de un nivel n realizan determinadas funciones n utilizando los servicios de los bloques del nivel N – 1 y proporcionando a su vez servicios a los bloques del nivel N+1.

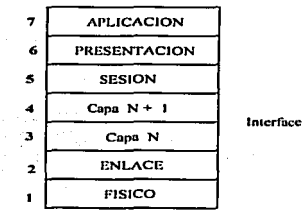


Figura No 1.6. Estructura por bloques de los sistemas abiertos

1.3.1 Nivel de Aplicación (Nivel 7)

El nivel de aplicación es el nivel superior del modelo OSI y proporciona los servicios de comunicación entre los diferentes procesos de aplicación que constituyen el sistema.

Los Procesos se comunican con otros procesos, a través de los servicios de comunicación entre procesos que brinda el sistema operativo cuando los procesos se encuentran residiendo en la misma máquina; sin embargo, en el caso de que los procesos se encuentren en máquinas distintas será necesario hacer intervenir al sistema de interconexión constituido por protocolos de aplicación.

1.3.2 Nivel de Presentación (Nivel 6)

El objetivo de este nivel es proporcionar un conjunto de servicios a los entes del nivel de aplicación, orientados a la interpretación de la estructura de la información intercambiada. Algunos de estos servicios son:

- La selección del tipo de terminal.
- La gestión de los formatos de presentación de los datos.
- Ordenes de manejo y formateado de los archivos.
- Conversiones de códigos de los datos

1.3.3 Nivel de Sesión (Nivel 5)

Este nivel proporciona el soporte a la comunicación entre los entes del nivel presentación. Los entes del nivel sesión utilizan a su vez los servicios del nivel Transporte de acuerdo con la estructura jerarquizada del modelo de referencia de la ISO.

Al establecer la comunicación entre dos procesos de sistemas distintos, se establece una sesión entre los correspondientes entes de presentación. La sesión regula el diálogo entre ellos y deja de existir cuando éste finaliza. Así que una sesión es una relación de cooperación entre dos entes del nivel presentación para permitir la comunicación entre ellos. En el establecimiento de una sesión intervienen dos etapas bien definidas que son: la orden de establecimiento de la sesión dirigida a un "buzón" específico situado en un sistema informático y una vez establecida la sesión se procede al intercambio de información de control y de datos. La sesión puede permitir una comunicación bidireccional o bien únicamente unidireccional.

1.3.4 Nivel de Transporte (Nivel 4)

Este nivel proporciona el servicio de transporte de la información a través del sistema. El servicio debe ser transparente para los usuarios (elementos del nivel sesión) liberándolos de ese modo de todo lo referente a la forma de realizar el transporte de la información de un sistema

a otro.
Proporciona tres tipos de servicios que son: los orientados hacia el establecimiento de una conexión, los orientados a la realización de transacciones de información y los orientados a la difusión de información a múltiples destinatarios.

Como se menciono con anterioridad, a partir del nivel 4 los protocolos son de extremo a extremo, es decir, se trata de programas de control de diálogos entre procesos corriendo en DTE's de los extremos del enlace (**ver figura 1.7.**); desde luego, para su funcionamiento, necesitan de los niveles inferiores, los cuales les proporcionan los servicios necesarios para que puedan llevarse a cabo los protocolos extremo - extremo.

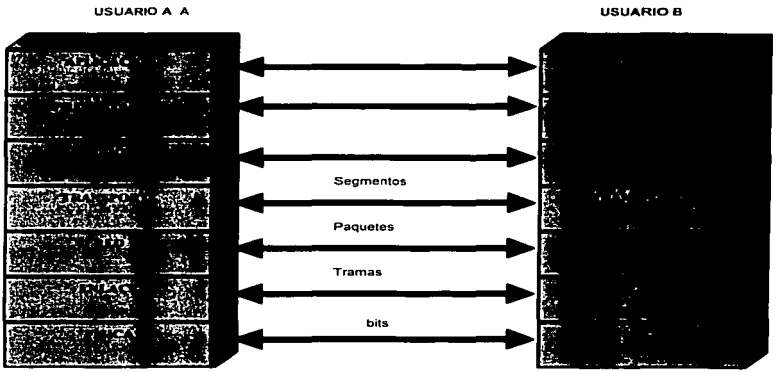


Figura No 1.7. Protocolos en el Modelo OSI

1.3.5 Nivel de Red (Nivel 3)

Este nivel se utiliza para establecer mantener y liberar las comunicaciones, especialmente cuando estas se realizan a través de una red. Un servicio muy importante en el caso de las redes de conmutación de paquetes, es el servicio de llamada virtual, el cual permite establecer a través de un mismo enlace físico a la red un gran número de comunicaciones simultáneas. Adicionalmente el nivel de red proporciona los elementos para gestionar servicios de red, como son los de grupo cerrado de usuarios con o sin acceso de salida o entrada (redes privadas virtuales), los de difusión general, modificación de velocidad de transmisión o longitud de paquete para mejorar la eficiencia de transmisión, los de petición de trayectoria de encaminamiento, etc.

1.3.6 Nivel de Enlace (Nivel 2)

Uno de los objetivos principales del nivel de enlace es mejorar la confiabilidad de la comunicación. No obstante, además de que el nivel de enlace permite que la transmisión de información a través de un enlace de datos sea confiable, también proporciona los medios para administrar adecuadamente, la de información y controlar el flujo de datos, y los procedimientos de inicialización y liberación del enlace. Los servicios principales que tiene nivel son: sincronía a nivel de trama, palabra y octeto; control de línea (enlaces punto a punto o multipunto, dúplex o semidúplex), control y corrección de errores (corrección directa o por repetición) control de secuencia (para sincronización de velocidades de proceso, control de bloqueos, etc.), recuperación en caso de errores (pérdida del enlace, errores en los campos de control de las tramas, etc.) , y transparencia (facilidad de transmitir información cualquiera, en el campo de información, no importando el código que la represente).

El protocolo de nivel de enlace se realiza en un enlace físico entre dos terminales conectadas a él y también debe inicializarse y liberarse cuando se deja de usar.

1.3.7 Nivel Físico (Nivel 1)

El nivel físico define las características lógicas, funcionales, eléctricas y mecánicas del enlace físico entre el equipo de cómputo y la red de telecomunicaciones[4].

[4] Networking Standars
William Stallings
Addison-Wesley
1994

1.4 REDES DE AREA LOCAL (LOCAL AREA NETWORKS).

1.4.1 Servidor.

Es una microcomputadora designada como administrador de los recursos comunes. En este, todos los usuarios pueden tener acceso a la misma información compartir archivos y contar con niveles de seguridad, además en el concepto de servidor de archivos un usuario no puede accesar indistintamente los discos que se encuentran en otras microcomputadoras, al hacer esto se logra una verdadera eficiencia en el uso de estos, así como una total integridad de los datos.

1.4.2 Topología.

Se le llama así a la forma física de conectar cada uno de los componentes de la red. Existiendo 3 topologías básicas: estrella, anillo y bus.

1.4.2.1 Topología estrella.

En la topología estrella cada estación se conecta con su propio cable a un dispositivo de conexión central, bien sea un servidor de archivos, un concentrador o repetidor. Esta topología utiliza mas cable que la topología en bus, pero en esta es mucho más fácil aislar las fallas. Si una estación funciona mal en la red, solamente se apaga la estación individual afectada. El resto de la red continua operando sin interferencia. La topología en estrella es ideal par muchas estaciones que se localizan a gran distancia de las otras.

La flexibilidad de la estrella permite hacer una fácil instalación y hace fácil agregar, relocalizar o renovar estaciones de la red, como en la **figura No 1.9.**

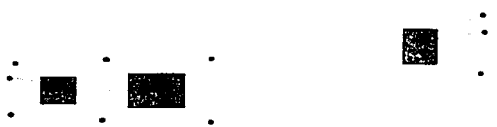


Figura No 1.9. Topología Estrella.

1.4.2.2 Topología anillo.

En las topologías en anillo las estaciones se conectan físicamente en anillo, terminando el cable en la misma estación donde se origino. Esto hace a esta topología más difícil de instalar que las topologías estrella o bus. En esta topología cada estación repite activamente todos los mensajes, por lo que la falla de una estación rompe el anillo causando que toda la red se apague, a menos que se integre una costosa de redundancia en el sistema. En la actualidad la topología en anillo ha dejado de ser popular cediendo su paso a la topología en anillo modificado, en la cual la caída de una estación, no significa la caída de la red.

Arcnet y Token Ring son muestra de lo que se considera anillo modificado o anillo de estrellas. Como se muestra en la **figura No 1.10.**

Figura No 1.10. Topología Anillo.

1.4.2.3 Topología bus.

En esta topología también llamada lineal, todas las estaciones son conectadas a un cable central, llamado bus o troncal. Este tipo de topología es fácil de instalar y requiere de menos cable que la topología en estrella, como se observa en la figura No 1.11.

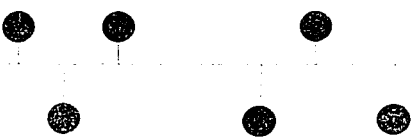


Figura No 1.11. Topología Bus

1.4.3 Estación de trabajo (workstation).

Se le llama así a una computadora personal conectada a un sistema operativo de la red y usada para realizar sus tareas a través de programas de aplicación y/o utilerías.

1.4.4 Enrutador.

Se llama así aquella que permite el enlace entre dos redes, además un enrutador permite el enlace entre diferentes protocolo, usando protocolos standard como lo son por ejemplo: TCP/IP, X.25, SNA, etc. Estos equipos contienen procesos robustos para implementar Seguridad en datos.

1.4.5 Firewall.

Dispositivo que ayudará a la interconexión de redes externas con Redes Internas, es decir, Redes Públicas (Internet) contra Redes Privadas, respectivamente. Estos dispositivos son utilizados para este tipos de conexiones a Internet y actualmente son empleados en apoyo a la Seguridad de nuestra red. Es posible activar diversos procesos para lograr lo antes mencionado algunos muy simples y otros complejos.

1.4.6 Conmutador de Red LAN.

Dispositivos tambien conocidos como Switches LAN, utilizados para conformar redes Jerárquicas. Estos equipos pueden ayudar en la Seguridad de las organizaciones en la parte Central de la red con nuevas mejoras para la optimización del tráfico local, conocidas como Redes Virtuales y aplicadas a la Seguridad en los Sistemas.

1.4.7 Hub.

Se llama así al elemento que modifica la señal de transmisión, permitiendo a la red ser mas larga ó extenderse con adicionales workstations. Existen dos tipos de hubs. Equipos que ayudan a los intrusos a monitorear y/o capturar informacion confidencial para su analisis.

1.4.7.1 Hubs Activos.

Un Hub activo amplifica la señal de transmisión, y es usado para adicionar workstations a la red o para extender la distancia entre las estaciones y el servidor.

1.4.7.2 Hubs Pasivos

Es un elemento usado en ciertas topologías par dividir la señal de transmisión, permitiendo adicionar workstations. Un Hub pasivo no puede amplificar la señal, pero si puede ser usado para conectar directamente a una estación o un Hub activo.

1.5 MEDIOS DE TRANSMISION.

1.5.1 Par Trenzado (blindado o no blindado).

Es usado primordialmente en topología en estrella, ya que es menos rígido que el cable coaxial y fibra óptica, además de que el par trenzado puede ser fácilmente instalado, además los ductos del cableado telefónico instalado en la mayor parte de oficinas son adecuados para la instalación del par trenzado, por lo que es menos costoso instalar adicional par trenzado en la ductería, para propósito de transmisión de datos, que instalar nuevos ductos para cable coaxial o fibra.

Existe un limite máximo en la longitud del par trenzado dependiendo de la velocidad de transmisión usada. Típicamente él limite es 100 mts para 1 MBPS o con la ayuda de circuitos adicionales para las interferencias, 100 mts para 10 MBPS.

1.5.2 Cable coaxial.

Es también ampliamente usado para LAN's, primordialmente utilizado con redes con topología en bus, con topología en bus operando ya sea con transmisión en banda base o en banda ancha. Dos tipos de cable son usados en banda base: uno conocido como thinwire y el otro como thickwire. Los términos se refieren al diámetro del cable. Thinwire es de 0.25 pulgadas de diámetro y thickwire a 0.5 pulgadas de diámetro. Normalmente ambos operan a la misma bit rate 10 MBPS pero el thinwire tiene mayor atenuación, la máximo longitud del thinwire entre cada repetidor es de 200 mts y para el thickwire es de 500 mts. Debe recordarse que un repetidor es usado para regenerar una señal recibida a su forma original. Los dos modos de operación alternos son conocidos como 10 Base 2, lo que significa 10 Mbps, banda base, 200 mts de longitud máxima, 10 Base 5, significa 10 Mbps banda base, 500 mts de longitud máxima.

1.5.3 Coaxial delgado.

Es continuamente usado para interconectar workstations en la misma oficina o laboratorio. El conector físico para cable coaxial une directamente a la tarjeta de interfase de la workstation.

1.5.4 Coaxial grueso.

En contraste, el coaxial grueso, debido a que su estructura es más rígida, es normalmente instalada fuera de la workstation, por ejemplo en un corredor. Cableado adicional - conocido como un drop cable - y circuitos electrónicos como lo son el transmisor y el receptor - conocido como un transceiver - deberá ser usado entre el punto de derivación (conexión) del cable coaxial principal - conocido como la unidad de interfase de acoplamiento attachment unit interfase AUI - y el punto de acoplamiento de cada workstation. Este arreglo es mas caro y es usado primordialmente cuando las workstation están cada una localizadas en oficinas diferentes. Ver figura No 1.12.

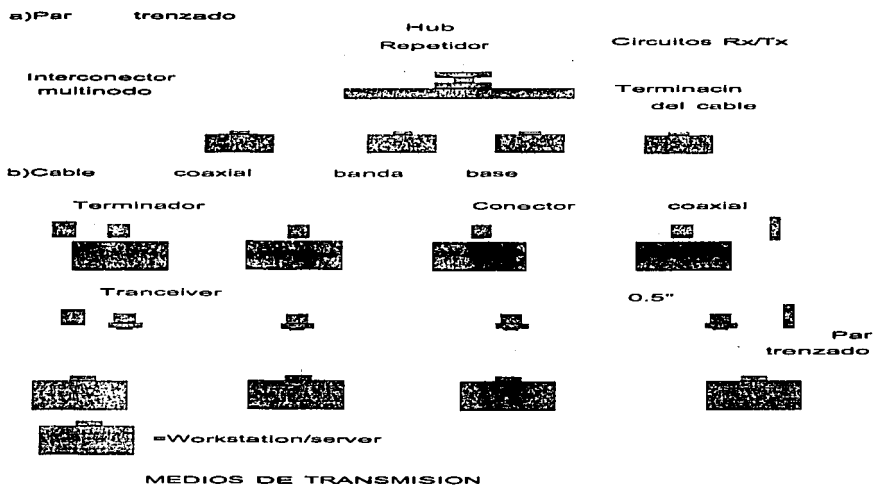


Figura No 1.12. Medios de Transmisión

1.5.5 Fibra óptica

Para transportar cualquier señal es necesario un medio de transmisión, por ejemplo para transportar voz podemos utilizar microondas, señales eléctricas, etc. Pero en el caso de transportar señales que llevan información importante, debemos de elegir un medio seguro para hacerlo. Ver figuran No 1.13.

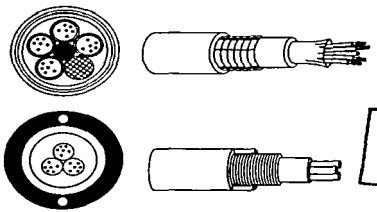


Figura No 1.13. Cables OSP y de cinta vertical.

La esencia de la fibra óptica es la canalización de los rayos de luz a través de "caminos de fibra óptica" y la generación de frecuencias de luz apropiadas.

Una de las tecnologías más importantes en transmisión de información ha sido el desarrollo de sistemas de comunicación por fibra óptica. Las partes principales de los sistemas de comunicación de fibra óptica son el transmisor, la fibra y el receptor.

1.5.5.1 Descripción física

La fibra óptica es una especie de filamento mucho más delgado que un cabello, generalmente las fibras estan hechas de sílice (combinación de silicio y oxigeno), y algún tipo de vidrio, pero este vidrio es de muy alta calidad, el cual es capaz de transportar rayos de luz en su interior de una manera determinada.

La fibra óptica consiste de dos porciones sólidas: el núcleo y el revestimiento, estas dos porciones no pueden ser separadas. La luz viaja a través del núcleo mientras el revestimiento guarda la luz contenida dentro del núcleo. Esto es realizado para tener índices diferentes de refracción entre el núcleo y el revestimiento.

El núcleo que consiste de vidrio o cuarzo, tiene un índice de refracción mas alto que el revestimiento de vidrio, cuarzo o plástico que lo rodea.

A su vez la superficie del revestimiento esta protegida por otras 4 capas más que son: Recubrimiento primario, aire o petrolato, recubrimiento secundario y una cubierta protectora.

Recubrimiento primario. Cuando la fibra es manufacturada, esta es inicialmente protegida con un recubrimiento primario. Este es típicamente hecho de acrílico y existe sobre todas las fibras virtualmente.

El tamaño de la fibra óptica es dado con dos números: El diámetro del núcleo y el diámetro del revestimiento respectivamente. Por ejemplo 62.5/125 μm es una fibra con un núcleo de 62.5 μm y tiene un diámetro de revestimiento de 125 μm. Ver figura No. 1.14.

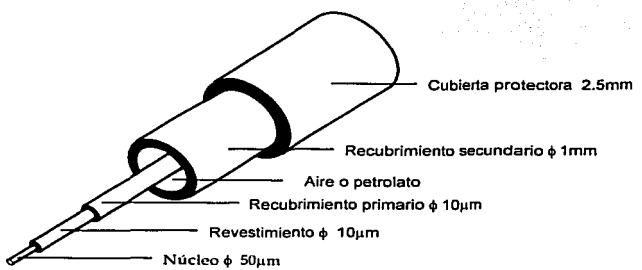


Figura No 1.14. Descripción física de un cable de fibra óptica

1.5.5.2 Transmisión

La fibra óptica transmite una señal codificada irradiando luz por medio de reflexión interna total. Esta puede ocurrir en cualquier medio transparente que tenga un índice alto de refracción que lo rodee, en efecto, la fibra óptica actúa como una guía de onda para frecuencias en el rango de 10^{14} a 10^{15} Hz el cual cubre el espectro visible y parte del espectro infrarrojo.

La forma de propagación es llamada multimodo porque se refiere a la variedad de ángulos que refleja. Cuando el radio del núcleo de la fibra es reducido pocos ángulos serán reflejados. Para reducir el radio del núcleo al de una guía de onda, solamente un ángulo o un modo podrá pasar.

Los modos de transmisión de la fibra óptica se observan en la figura No 1.15.

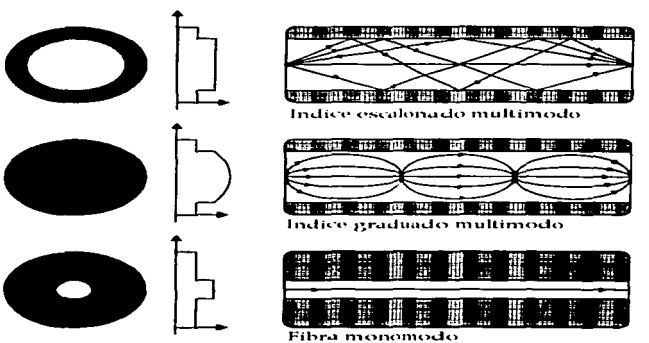


Figura No 1.15. Índice escalonado multimodo, Índice graduado Multimodo y fibra monomodo.

1.5.5.3 Tipos de fibras ópticas.

Monomodo.- Se dice que una fibra óptica es monomodo cuando sólo consideramos una frecuencia de luz para transmitir, ya que el diámetro del núcleo es muy pequeño.

Multimodo.- Se dice que una fibra óptica es multimodo, si bien el diámetro del núcleo o los índices de refracción del núcleo y de la cubierta son mayores que los límites establecidos para la operación en monomodo.

Cuando se trabaja en multimodo habrá muchos rayos de luz diferentes (cada una de ellos viajando con un ángulo de reflexión distintos, pero siempre menores que el ángulo crítico) viajando a lo largo del núcleo[5].

1.5.5.4 Ventajas.

Las principales ventajas de la fibra óptica sobre los sistemas de cableado son la baja atenuación, y el ancho de banda tan grande disponible. Y como la atenuación es baja, pueden ser alcanzadas distancias grandes entre repetidores.

La fibra es el medio más económico para transmisión de varios canales de voz, vídeo y datos de alta calidad a largas distancias, es por ello que la transmisión vía fibra óptica abre un nuevo concepto en los sistemas de comunicación. En la tabla No 1.4 se muestra la comparación de la fibra óptica y el coaxial en cuanto a al seguridad física.

	Fibra óptica	**Coaxial**
RFI	Ninguna	Problema
Fallas a tierra, rayos eléctricos.	Ninguna	Gran Problema
Seguridad	Segura	Gran Problema
Apoyo de multimedios	Si	Cuestionable
Facilidad de identificación de fallas/pruebas de instalación	Simple	Difícil
Duración (tiempo de vida)	10 a 15 años	3 a 5 años

Tabla No 1.4. Tabla comparativa entre cable de fibra **óptica** ***y cable coaxial***

[5] Networking Standars
William Stallings
Addison-Wesley
1994

1.5.5.5 Desventajas.

La desventaja que puede existir es la fragilidad (para el caso de cables de unión). Otro aspecto que cabe mencionar es que este medio (fibra óptica) se estaría desperdiciando en el caso de utilizar muy poco este canal, es decir transportar poca cantidad de información, por lo que puede resultar en ciertos casos caro.

A continuación se apuntan algunas limitantes que se tienen, pero aclarando que utilizando otros medios estos límites se incrementan.

Existen dos factores que limitan la utilidad de la fibra óptica para comunicaciones. La primera es la atenuación, esta es siempre un nivel de transmisión máximo y un nivel mínimo útil recibido. La diferencia entre estos es la perdida total, la cual es debido a la atenuación de la fibra. La atenuación de la fibra es expresada en dB/km, limita la máxima distancia entre el transmisor y el receptor.

El otro factor limitante es el ancho de banda. La fibra óptica tendrá un ancho de banda máximo para señales que son transmitidas mediante la fibra sin distorsión. El ancho de banda limita el valor al cual la señal puede cambiar su intensidad u otros parámetros de la señal, y así el valor para el cual la información puede ser transmitida.

1.6 TCP/IP

Los protocolos de seguridad en redes dependeran de los servicios y aplicaciones que se encuentre en tu ambiente. A nivel de red del modelo de OSI, la arquitectura IPSec brinda soluciones de seguridad.

TCP/IP (Transmission Control Protocol/Internet Protocol) es un compendio de protocolos que se encuentra en el nivel 3 del modelo de OSI. El Departamento de Defensa de EUA (DoD) desarrolló estos protocolos a los que posteriormente les llamó de Internet, los cuales se asocian más con sólo un par de ellos TCP/IP. TCP e IP son los protocolos más populares en el medio. TCP/IP fue diseñado para soportar comunicaciones entre hosts conectados por una red y proporcionan seguridad en la transmisión de datos utilizando arquitecturas de nivel 3 del modelo OSI, como por ejemplo IPSec. Como sabemos las redes pueden estar conectadas por algunos de los siguientes métodos de comunicación en redes privadas o públicas:

- Transmisión por banda base
- Carriers públicos de transporte
- Redes satelitales
- Radiomóvil
- LAN

TCP/IP es una arquitectura que permite la transferencia de datos entre sistemas. Desde mediados de los 80's todas las arquitecturas han sido comparadas al Open Systems Interconnection (OSI) como modelo de referencia. Una examen de este modelo esencialmente para entender la relación del presente y futuro en la arquitectura de redes.

TCP/IP es actualmente un conjunto de protocolos para la transferencia de datos entre sistemas heterogéneos. Las tareas específicas para las cuales los protocolos fueron desarrollados incluyen las siguientes:

- Acceso al mecanismo de transporte
- Trazo de la(s) rutas para datos
- Reporte de errores asociados con el transporte de los datos
- La presentación de datos
- Acceso a los datos una vez que encuentra su destino

Ya tiene establecidas las capas del enlace y física, las cuales dan la seguridad de los datos y las conexiones físicas, backbone de la red está listo para el transporte de datos por medio de TCP/IP.

El protocolo TCP fue diseñado para ofrecer el servicio en la capa de transporte, para asegurar la transferencia de datos entre procesos. El protocolo IP fue diseñado para servir en la capa de red como un distribuidor de datos entre nodos. El Protocolo de Control de Mensajes en Internet (ICMP, Internet Control Message Protocolo) es una implementación

del protocolo IP para reportar errores y controlar los mensajes asociados con la ruta de los datos.

Los protocolos de aplicación fueron diseñados para asignar las funciones de las tres capas superiores, aplicación, presentación, sesión. Las necesidades más comunes se enfocaron a asignar un camino a:

- Conexiones remotas
- Iniciar una sesión remota
- Identificar archivos remotamente
- Controlar la transmisión de archivos remotamente

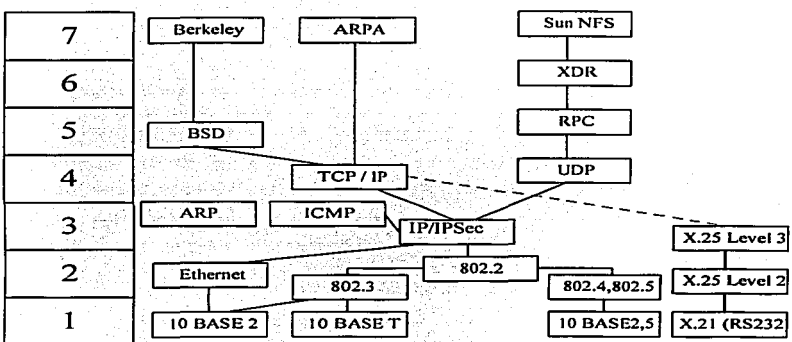


Figura 1.16 Protocolos Internet, según el Departamanto de Defensa (DoD) de EUA

Estos se controlan por medio de protocolos algunos de los cuales se listan en la tabla 1.3:

7 Application	ftp telnet bootp tftp named gated	rcp rlogin rexec rwho ruptime sendmail	NFS NIS VHE	Services
6 Presentation	SMTP		XDR	
5 Session		BSD IPC	RPC	
4 Transport	TCP	TCP	UDP	
3 Network	IP/IPSec	IP/IPSec	IP/IPSec	LAN Link
2 Data Link	Ethernet	Ethernet	Ethernet	
1 Physical	Ethernet/IEEE 802.3	Ethernet/IEEE 802.3	Ethernet/IEEE 802.3	

Tabla 1.3 Pila de protocolos.

Servicios ofrecidos por los protocolos y servicios basados en las especificaciones del DoD

Existen tres principales entidades que liderean los servicios de las capas superiores:

- ARPA, sección del DoD encargada de desarrollar servicios basados en TCP/IP
- BSD (Berkeley Software Develompment), servicios desarrollados por la Universidad de Berkeley en base a TCP/IP.
- NFS (Network File System), servicios que permiten el intercambio de información completa a otras máquinas que es independiente del hardware.

En la capa de transporte se aprecian dos tipos de protocolos, los cuales seran encriptados por IPSec como veremos mas adelante:

- UDP (User Datagram Protocol), que es un protocolo connection less.
- TCP (Transport Control Protocol), que es un protocolo connection oriented.

Como sabemos, un protocolo connection less es aquél que no necesita reconocimiento de transmisión para poder seguir con la secuencia de tramas; es un protocolo mucho muy rápido pero no asegura, en esta capa, la seguridad de los datos.

Un protocolo connection oriented, es aquél que necesita reconocimiento de la transmisión para asegurar la integridad de los datos pero es un protocolo lento.

En la capa de red, observamos a IP junto a un par de protocolos que son el ARP y el ICMP. Como ya se mencionó, IP es un protocolo que permite la distribución de los paquetes para una mejor administración de la(s) red(es). IP se basa en direcciones las cuales se forman de dos partes, una que define el número de Red y otra que define el número de máquina, utilizadas también por IPSec. Estas direcciones son asignadas a través de cuatro octetos; para que su representación sea mucho más sencilla se diseño un método que implica cambiar el valor de los octetos a uno decimal separado cada uno por un punto. Existen varias clasificaciones según el número de redes y nodos que se quieran usar, según se muestra en la figura 1.33.

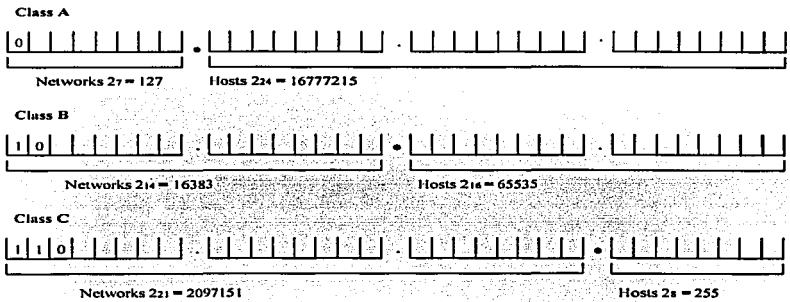


Figura 1.17. Asignación de direcciones IP y sus clases.

ARP (Address Resolution Protocol) El módulo IP finaliza con el datagram, éste pasó al protocolo de acceso a la red el cual está en el nivel de link. Si el protocolo es LAN entonces el mapeo de dirección es requerido. Nosotros sabemos que la dirección IP es de 32 bits, mientras una direccion LAN es de 48 bits. ARP diseño la IP para traer la dirección de la LAN cuando ésta es conocida. ARP envía fuera un broadcast requiriendo la dirección Ethernet para dar una dirección IP.

ICMP (Internet Control Message Protocol) IP fue diseñado para proveer algunos significados de reportes de problemas de comunicación, y que deben ser implementados con IP. Los mensajes ICMP son generalmente enviados a reportes con un error cuando se está procesando un datagrama. Otros puntos que se incluyen cuando envía mensajes son:

- El destino inalcanzable
- Los recursos del gateway tienen insuficiente buffer
- El gateway puede identificar una ruta corta

Lo relevante de estos protocolos es la eficiencia y la interoperabilidad de sistemas de cómputos diversos residiendo en ambientes de red heterogénea. La guía de conexión es el protocolo de internet, el ahora familiar IP. Protocolos de capas superiores proveen servicios orientados a conexión, como es el caso de TCP, y orientados a no conexión.

Estos protocolos están organizados en cuatro capas que en términos del modelo OSI, pueden ser descritos como la capa de aplicación, transporte, red, enlace de datos y física, la descripción de estas capas es :

- Capa de Aplicación. Es la que contiene las aplicaciónes de red; ejemplos de aplicaciones de red incluyen programas para la comunicación interpersonal tales como correo electrónico y bulletin board, emulaciones de terminal virtual (TELNET y Transferencia de Archivo), esta capa contrasta con la del modelo OSI la cual contiene elementos de servicios de aplicación que puede ser combinada con elementos específicos de aplicación para dar forma a un ambiente de aplicación (Aplicaciónes de red).

- Capa de Transporte. La primera función de la capa es asegurar conexiones punto a punto; es en esta capa donde programas o procesos sobre diferentes computadoras se hablan directamente unos con otros. Los dos protocolos internet definidos en esta capa son el TCP (Transmission Control Protocol) y el UDP (User Datagramm Protocol). TCP provee una conexión basado en el modelo de circuitos virtuales para comunicaciones de red; UDP presta un servicio basado en el modelo de no conexión que es el servicio de datagramas que el protocolo IP presta.

- Capa de Red. Habilita a múltiples redes la comunicación a una misma red, el protocolo definido en esta capa es el llamado IP (Internet Protocol). IP proporciona una conexión con servicios de datagramas para protocolos en capas superiores. Es un servicio poco seguro, siguiendo con esta capa, IP provee servicios de ruteo a computadoras y es el encargado de ligar redes y computadoras en la internet.

- Capa de Acceso al Medio. Provee el acceso al medio de comunicación con control de flujo opcional y detección de errores y corrección. Este grupo de protocolos puede hacer uso del protocolo que paquetes X.25 para redes de área amplia y especificaciones IEEE 802 como lo son (802.3 Ethernet y 802.5 Token Ring) para acceso a redes locales.

El direccionamiento usado por el grupo de protocolos TCP/IP son llamados direccionamiento Internet. Estos direccionamientos tienen valores de 32 bits que son divididos en números de red y en números de host. Los diseñadores de este tipo de direccionamiento crearon tres clases de direcciones. El direccionamiento clase A tiene el bit de mayor significancia puesto a cero, con los siguientes 7 bits identificando la red y los restantes 24 bits identificando el host. El direccionamiento clase B tiene los primeros 2 bits

en 10, los siguientes 14 bits identifican la red y los restantes 16 identifican el host y en la clase C los primeros 3 bits son 110, los siguientes 21 bits identifican la red y los ultimos 8 bits identifican el host.

Los diseñadores escogieron estas tres clases de direcciones porque sintieron que las diferentes configuraciones de red pueden ser mejor atendidas con una variedad en la estructura de direccionamiento. Creyeron que podría haber un numero pequeño de redes con una gran cantidad de host, una cantidad razonable de redes con número moderado de host y un gran número de pequeñas redes[6].

1.6.1 Gráfica de direcciones

Una idea del flujo de datos es la siguiente. La aplicación del usuario pasa los datos a TCP a través de un API (Aplication Programm Interface). Es entonces cuando TCP crea una conexión, la conexión al proceso remoto y permite que el IP enrute y transfiera los paquetes de datos hacia la computadora remota. TCP hace esto al pasar los datos, direcciones destino y fuente además de información de control a IP hasta que se reciben los datos en el modo remoto IP le da estos datos a TCP en la computadora remota lugar en el que los datos son almacenados en un bufer. La aplicación remota lee estos datos desde la conexión y es cuando la transferencia está completa.

1.6.2 TCP

Este protocolo asegura la conexión a través de un servicio de circuito virtual para procesos de aplicaciones en comunicaciones de host a host, es la norma para comunicar procesos. Las aplicaciones que requieran una seguridad en la conexión de una aplicación a otra, deberán usar este servicio. Las aplicaciones de red deben interactuar directamente con TCP a través de API's que es una implementación del protocolo, dependiendo del sistema operativo en el host, este API puede crear un componente íntegro del sistema operativo. Las aplicaciones usan llamadas comunes de entrada y salida como open, close, read, write y llamadas que presentan el estado de la conexión.

TCP, que usa un protocolo orientado a conexión requiere que la conexión esté establecida entre los dos procesos.

El punto final de una conexión TCP es llamado socket. Un socket es una combinación de direcciones de red, direcciones físicas y el número de puerto sobre el

[6] Internetworking with TCP/IP
Volume I Principles, Protocols, and Architecture
Second edition
Douglas E. Comer
Prentice Hall
Marzo 1991

servidor local. Puerto es un concepto lógico que habilita a procesos de múltiples aplicaciones para usar el servicio de transporte de TCP sobre la misma máquina. El socket identifica el punto final de la conexión al mandar y recibir los datos anteriores; es por esto que un par de sockets diferentes identifican la conexión.

TCP ocupa tres tipos de handshake para el establecimiento de la conexión, punto importante en el tema de seguridad pues existen diversos tipos de amenazas utilizando este proceso, los paquetes enviados tienen banderas de control que indican el proceso de entrega en particular las banderas de sincronia(synchronize SYN y el acuse de recibo(acknowledgment ACK) son usadas de la siguiente manera en la figura No 1.18

1) Computadora A envía un SYN con un número de secuencia a la computadora B.

2) Computadora B envía un ACK y SYN (Ambos enviados en un solo mensaje) a la computadora A con el número de secuencia.

3) Computadora A envía un ACK con el número de secuencia a la computadora B.

4) La conexión está terminada al intercambiar segmentos con la bandera de control FIN.

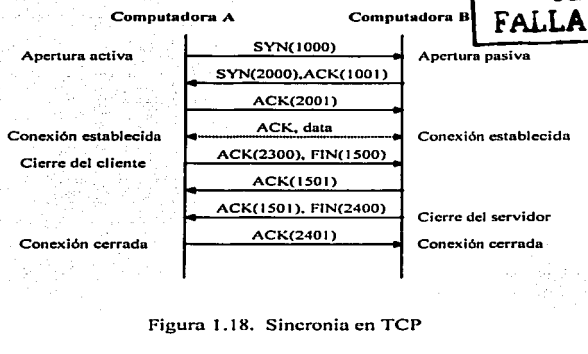


Figura 1.18. Sincronia en TCP

1.6.3 Encabezado TCP

El segmento TCP está implícito en el datagrama de IP para transferencia sobre la red. Porque IP está interesado en obtener el paquete del destinatario en la red, esta dirección está contenida en el encabezado de IP y no en el de TCP. De igual manera ya que el puerto es un concepto de TCP, los puertos fuente y destino son almacenados en el encabezado de TCP, éstos tienen un valor de 16 bits. Estos conceptos de encabezados de IP y de TCP son muy importantes para el correcto funcionamiento de IPSec.

El número de secuencia tiene un valor de 32 bits que contiene la secuencia del primer octeto de datos en el segmento. También tiene el efecto de ACK, todos los datos recibidos arriba del número de secuencia menos uno.

El campo de Data Offset es un delimitador al inicio del header para indicar el inicio de datos. Los siguientes 6 bits están reservados para un uso futuro y su valor debe ser 0.

El campo para las banderas de control tienen una longitud de 6 bits y su significado es el siguiente:

URG (Urgent) Indica que el apuntador de urgente contiene un valor significativo.

ACK Indica que el acuse de recibo contiene el número de secuencia esperado.

PSH (Pushed) Indica que los datos deben ser enviados inmediatamente y no almacenados antes de transferirlos.

RST (Reset) Informa a TCP que la conexión debe ser inicializada

SYN Bandera de control para establecer una conexión y sincronizar los números de secuencia. Concepto imporante dentro del tema de Seguridad en las redes de Telecomunicaciones.

FIN Indica que ya no existen más datos a transmitir y desea terminar la conexion. También importante en la seguridad en redes.

La ventana es un campo de 16 bits que contiene el número de octetos que el receptor puede aceptar, después de un ACK.

1.6.4 UDP (User Datagram Protocol)

El UDP usa IP para proveer los procesos de aplicación con un protocolo de datagramas sin reglas en la capa de transporte, habilitando a las aplicaciones a comunicarse sin la sobrecarga de la conexión y desconexión. Como IP, UDP no garantiza la entrega de paquetes no provee secuencias de paquetes o supresión de duplicación de los paquetes. Aplicaciones que requieran este tipo de servicios debe considerar a TCP.

UDP es útil para aplicaciones que pueden tener sus razones para implementar su propia secuencia de entrega de paquetes y confiabilidad. En estos casos los servicios que provee TCP pueden dejar de usarse esperando una considerable baja en la carga. El formato del header UDP es el siguiente:

1.6.4.1 UDP Header

Source Port an Destination Port. Especifica los puertos de proceso de la aplicación que envía y recibe respectivamente.
Length. La longitud del paquete UD incluyendo el header y los datos.
Checksum. Un cómputo de 16 bits que verifica que los datos fueron transferidos sin daño.

1.6.5 IP (Internet Protocol)

IP provee un servicio de datagramas inseguro orientado a no conexión para la conmutación de datos sobre una red de conmutación de paquetes. También provee facilidades para fragmentar grandes paquetes para la transmisión y el reensamble en las estaciones receptoras. IP no provee control de flujo, secuencia o supresión de duplicación alguna.

IP usa tanto TCP como UDP para rutear y entregar paquetes a través de la red. El segmento de TCP (header y datos) está localizado en la sección de datos del datagrama IP. IP debe ser implementado en cada host que esté conectado a la red y que sea capaz de rutear paquetes sobre la red local.

IP usa una estructura jerárquica de las direcciones internet y rutea cada datagrama independiente del otro.

1.6.5.1 Header del datagrama IP

Versión. Denota el formato del header IHL (Internet Header Length) es el inicio de los datos, el valor de este campo está multiplicado por 32 bits para indicar el valor del delimitador.

Type of Service. Campo de 8 bits que contiene el valor que indica la calidad del servicio a proveer en ciertas redes. Un ejemplo del tipo de servicios es *Precedence*, el cual asigna prioridad para asignar paquetes.

Total Length. Campo de 16 bits que contiene la longitud del header y los datos juntos. Este campo de 16 bits asigna un límite en el tamaño del datagrama de 65 535 octetos por lo general, las implementaciones en IP mantienen este campo en 576 octetos para asegurar que puedan pasar a través de cualquier ruteador en la red.

Identificación. Usada por la máquina que recibe para reensamblar datagramas fragmentados.

Flags. Campo de 3 bits que indica la fragmentación de datagramas.

Bit 0. Está reservado y siempre es 0.

Bit 1. Indica si el datagrama está o no fragmentado.

Bit 2. Indica si el paquete es el último fragmento o si existen más fragmentos.

Fragment Offset. Campo de 13 bits y que muestra la localización del fragmento en el datagrama. El valor de este campo está multiplicado por 8 octectos para determinar el octeto delimitador del fragmento en el datagrama. Un datagrama es fragmentado cuando quiere pasar a través de una red que tiene definido un tamaño de paquete más pequeño que el datagrama. El datagrama no será fragmentado si la bandera de no fragmentar (don't fragment) está indicada, en este caso el datagrama será descartado y un reporte será enviado al fuente a través del ICMP.

Time to live: Campo de 8 bits que especifica el tiempo máximo que un datagrama puede existir en la red antes de que sea atrapado en algún ciclo indefinido dentro de la red y sea destruido. La unidad de tiempo es el segundo; el campo es para intentar prevenir que un datagrama navegue indefinidamente por la red.

Protocol. Campo de 8 bits que especifica el protocolo que creó los datos y que el datagrama debe entregar al host remoto.

Checksum. Un cómputo de 16 bits que verifica que los datos fueron transferidos sin daño. Concepto utilizado para seguridad en la transmisión de datos a traves de redes no confiables.

Source & Destination Address. Campos de 32 bits cada uno que contiene la dirección internet para el host local y remoto respectivamente.

Options. Campo de longitud variable que es opcional en el datagrama. Casi siempre los host y ruteadores que implementan IP deben soportarlo si está presente.

1.6.6 Internet Control Message Protocol (ICMP).

Este protocolo es usado para notificar de errores que ocurrieron en la entrega de datagramas a través de la red. Generalmente el host destino o un ruteador interno es quien origina este mensaje. Este dispositivo puede mencionar que el destino es inalcanzable o que el ruteador no tuvo los suficientes bufers para almacenar y pasar (Store & Forward) el datagrama. El mensaje puede contener información referente al transmisor y la ruta más corta a usar.

Los mensajes de ICMP se distinguen uno de otro por el primer octeto de la porción de datos en el paquete IP y ellos habilitan al modulo ICMP para interpretar y manejar estos mensajes.

Cuando el header de IP está construido, el ruteador o host lo usa como dirección fuente si un error se presenta. El destino es la dirección del mensaje inicio.

Echo replay. Respuesta si cualquier envío presenta el mensaje. El número de secuencia puede ser usado para determinar qué petición de echo se está respondiendo.

Destination Unreachable. Información concerniente a las siguientes condiciones: la red fue inalcanzable, el destino fue inalcanzable, el puerto destino fue inalcanzable o un paquete no se pudo fragmentar. Varios de los mensajes regresan al header de IP y los primeros 64 bits del campo de datos en el datagrama inician el mensaje ICMP.

Source Quench. Envia por un ruteador o el destino indica que los datagramas están llegando tan rápido que no tiene espacio en su memoria o poder de procesamiento para manejarlo. El mensaje a la estación transmisora es para reducir su tasa de paquetes enviados.

Redirect. Enviado por un ruteador cuando descubre una ruta más corta al destino en su propia tabla de ruteo. Este mensaje no es enviado si el datagrama está haciendo uso de la información fuente/ruteo.

Echo. Una petición para que el destino conteste con un mensaje echo replay. Esta respuesta es un acuse de recibo que el datagrama pudo llegar al destino.

Time Exceeded. Enviado por un ruteador si éste notifica que el campo time to live en el datagrama ha expirado. El ruteador usa este mensaje para informar al transmisor que se ha descargado el datagrama. Un host puede mandar este mensaje si es imposible reensamblar los fragmentos de un datagrama.

Parameter Problem. Enviado por un ruteador o host que fue forzado a descartar un datagrama porque encontró algo criticamente mal en el header del datagrama. El mensaje también contiene un apuntador indicando la localización del error en el header.

Timestamp. Informacion reunida acerca del tiempo requerido para alcanzar un destino. El transmisor llena en los 32 bits el tiempo que le toma (medido en milisegundos), usando UTC (Universal Time Coordinate) como referencia.

Timestamp replay. Respuesta a un mensaje timestamp; contiene un timestamp de cuando el datagrama fue recibido por el destino y un timestamp de cuando la respuesta fue enviada. La aplicación del cliente es libre para usar esta información de cualquier manera.

Information Request & Information Replay. Usada por el host para determinar el número de red a la que está conectada. Estos mensajes son definidos en la especificación del protocolo pero generalmente no son implementados[7].

[7] Enhanced IP Services
Donald C Lee
Cisco System
1999

CAPITULO 2
CRIPTOLOGIA

2 Criptología.

2.1 Criptología

La Criptología es la ciencia interesada en la comunicación en una forma segura y fiable. Comprende dos términos que son: la Criptografía y el Criptoanálisis.

El termino Criptología se deriva del griego Kryptos, oculto y del logos, palabra. La seguridad se obtiene desde Autenticar a los usuarios, el transmisor y el receptor, los cuales podrán transformar la información obteniendo un mensaje codificado (ciphertext) en combinación con una llave secreta, esta llave, será una parte de la información que solo conocerá el transmisor y el receptor. Aunque el mensaje codificado (ciphertext) es inescrutable y frecuentemente sin posibilidad de entenderlo sin que se tenga copia de la llave secreta para decodificarlo (plaintext), solo el receptor autorizado podrá leer la información codificada y recobrar la información oculta y/o verificar que fue enviado por alguien que posee la llave secreta. La Criptografía se deriva del griego Kryptos, oculto y graphein, escribir, es el estudio de los principios y técnicas por la cual la información puede ocultarse en códigos y posteriormente revelada por usuario legítimo empleando la llave secreta, siendo imposible el adivinar el código por usuarios no legítimos. El Criptoanálisis se deriva del griego Krypto, oculto y analyein, soltar, es la ciencia o arte de recobrar la información de los mensajes codificados sin conocimiento de la llave secreta. La Criptología es a menudo considerada como un sinónimo de la Criptografía y del Criptoanálisis, aunque especialistas en el campo han adoptado por años la convención que Criptología es él termino que más comprende a ambos términos Criptografía y el Criptoanálisis.

Los principios de la Criptografía aplican igualmente en la seguridad del flujo de datos entre computadoras, como el lenguaje digitalizado, a los facsímiles codificados y a las señales analógicas empleadas como por ejemplo en la televisión. La mayoría de las comunicaciones por satélite, por ejemplo, encriptan los datos que envían a sus subscriptores garantizando privacidad. A causa de este amplio campo de la criptografía, también se ha ampliado el campo del criptoanálisis incluyendo la recuperación de la información a partir de codificados de cualquier tipo de formato de datos. La criptografía esta preocupada inicialmente en proveer seguridad a los mensajes empleando mecanismos de seguridad, estos mecanismos lo definimos como procesos de encripción. Estos procesos se pueden clasificar en encripción simétrica y encripción asimétrica. Para la encripción simétrica es llamada también como encripción convencional o encripción simétrica y la encripción asimétrica es llamada encripción de llaves públicas.

Las funciones básicas del proceso de encripción contiene varios elementos, para ello vamos auxiliarnos describiendo el proceso de encripción mas sencillo, la encripción simétrica y posteriormente detallaremos la encripción asimétrica. La tabla No 2.11, resume algunos aspectos importantes de los algoritmos convencionales y de llave Pública.

2.2 Definiciones de seguridad

Si bien un término Seguridad tiene más de un significado -aún los profesionales que trabajan en el área de Seguridad no se han puesto de acuerdo en lo que este término significa- por lo que se intentará dar un concepto.

Una versión acerca de un sistema completamente seguro se la atribuye a Gene Spafford, podría juzgarse de cómica pero nos refleja cuán difícil puede ser mantener un sistema confiable y seguro:

"El único sistema que es completamente seguro es aquel que está apagado, desconectado, guarnecido en una caja fuerte de titanio, enterrado en una caja de concreto, rodeado de gas irritante y por unos guardias altamente armados (aún así yo no arriesgaría mi vida en él)".

Otra definición:

"Una computadora es segura si uno puede depender de ésta y su software, y si éstos funcionan como uno esperan que lo haga".

Si uno espera que los datos que hoy dejó en la máquina, en unas semanas sigan ahí sin que alguien más los haya leído, entonces la máquina es segura, a este concepto también se le conoce como "confiabilidad".

Esto nos lleva a identificar a la seguridad como protección, ahora nos falta específicar qué es lo que queremos proteger y de qué. Son tres las áreas de protección que nos interesan: software, hardware y los datos, de qué los queremos proteger es:

- Hardware.- Protección de destrucción de hardware valioso
- Software.- Protección de destrucción de programas valiosos
- Datos.- Protección de destrucción de datos valiosos

Y para las tres áreas (Hardware, Software y Datos):

- Protección a cambios no autorizados
- Protección a uso no autorizado

El siguiente paso es definir los diferentes tipos de seguridad qué puede afectarla, los criterios para evaluar un sistema, así como otros conceptos[8].

[8] N. Derek Arnold
UNIX Security a practical Tutorial
McGrawHill 1993

2.2.1 Seguridad en la Información (INFOSEC).

La protección en el proceso de la información se requiere por que la información puede ser comprometida por ignorancia, inadvertencia, accidentalmente o por malicia.

2.2.2 Seguridad en Cómputo (COMPUSEC).

El sentido general de "seguridad en cómputo" (COMPUSEC), en éste contexto será expuesto como el estado de certeza de que los datos computarizados y los archivos de programas no pueden ser accesados, obtenidos o alterados por personas no autorizadas.

2.2.3 Seguridad en los datos.

Consiste de procedimientos y acciones diseñados para prevenir la revelación no autorizada, transferencia, modificación o destrucción, accidental o intencional de los datos. Hoy en día el término de datos debe ser cambiado por información, simplemente por que cada vez más el tráfico de la red consiste de información en general, más que datos (incluyendo imágenes, FAX, video, etc.).

2.2.4 Seguridad en Comunicaciones (COMSEC).

En los años recientes, el tema ha tomado la dirección de que la información "segura" fluye en redes y líneas de comunicación "seguras". La seguridad en comunicaciones -COMSEC es, por lo tanto, la protección como resultado de la aplicación de "criptoseguridad", seguridad en la transmisión, la emisión de medidas de seguridad a telecomunicaciones y de la aplicación de medidas de seguridad física a la información que se transmite por los distintos medios de comunicación.

Como se puede notar existen algunos conceptos que hacen falta aclarar para completar la explicación:

2.2.5 Seguridad en la transmisión (TRANSEC).

Es el componente de COMSEC que resulta de todas las medidas destinadas a proteger los transmisores de intercepciones y exploraciones no autorizadas.

2.2.6 Emisión de la Seguridad (EMSEC).

El componente de COMSEC que resulta de todas las medidas tomadas para negar el acceso a personas no autorizadas el acceso a información valiosa, que podría ser obtenida de interceptar las emanaciones de equipo de encriptamiento y sistemas de telecomunicaciones.

2.2.7 Seguridad Física.

El componente de COMSEC que resulta de todas las medidas físicas necesarias para salvaguardar equipo clasificado, material y documentos de acceso u observación por personas no autorizadas.

2.2.8 Sistemas de seguridad.

Consisten de la combinación de subsistemas de hardware y software. Seguridad en equipo de comunicaciones. Por ejemplo, equipo diseñado para proveer seguridad a telecomunicaciones, para convertir la información a una forma ininteligible a un interceptor no autorizado, y posteriormente reconvertir ésta información a su forma original para los receptores autorizados; tanto como equipo diseñado específicamente para obtener ayuda o como sólo un elemento en el equipo de conversión.

2.2.9 Seguridad a través de la oscuridad.

El concepto de seguridad, derivado en gran medida de la inteligencia militar, se basa en la "necesidad de saber". La información es particionada y se da a conocer tanto como sea necesario para realizar el trabajo.

En ambientes de trabajo donde puntos específicos de la información son susceptibles, o donde la seguridad inferencial es importante, esta política se vuelve consideradamente importante. Si tres piezas de información juntas pueden tornarse un punto vulnerable del sistema y uno no tiene acceso a más de dos, se puede asegurar la información.

En ambientes de operación de las computadoras, aplicar el mismo concepto, no es usualmente apropiado especialmente si se basa la seguridad en el hecho de que algo es desconocido a los atacantes. Este concepto puede mas que preservar, hacer daño a la seguridad.

Considerar un ambiente donde los administradores deciden mantener lejos de los usuarios los manuales para impedir que aprendan acerca de los comandos y las opciones del sistema es absurdo. Bajo estas circunstancias el administrador podría pensar que esta incrementando el nivel de seguridad en el sistema, pero probablemente no. Para muchos posibles atacantes al sistema puede ser relativamente fácil conseguir este tipo de información en otras partes. Muchos vendedores sacan copias a su documentación sin requerir una licencia de ejecución. Usualmente para lograr esto sólo se requiere visitar una universidad, localizar el material y fotocopiarlo.

Mientras tanto los usuarios locales se vuelven menos eficientes para manipular la máquina, porque no les es permitido aprender sobre los comandos que les permitirían

incrementar su nivel de eficiencia. Este tipo de personas son comúnmente quienes tienen una pobre actitud, porque el mensaje implícito del administrador es: "no estamos completamente seguros de que seas un usuario responsable". Además si un usuario no esta abusando de los comandos y de las características del sistema, esto implica que el administrador no tiene la suficiente capacidad para tratar el problema.

Mantener algoritmos en secreto, tanto como desarrollar algoritmos de cifrамiento, son valores cuestionables. Al menos que sea un experto es poco probable que se analice la consistencia del algoritmo. El resultado puede ser un mecanismo que tiene "un hoyo muy abierto", en cuanto a seguridad se refiere. Un algoritmo que se mantiene en secreto no es estudiado por otros, y de esta forma paradójicamente si alguien descubre el hoyo en el sistema, tiene libre acceso a los datos sin el conocimiento de ello a los administradores o al dueño de la información.

De la misma forma, mantener el código fuente del sistema operativo en secreto no es una garantía de seguridad, quienes están predispuestos a entrar y romper el sistema, encontrará hoyos de seguridad -con o sin el código fuente. Pero sin el código fuente no es posible realizar una examinación sistemática del programa para encontrar y solucionar problemas[9].

2.2.10 Agujeros en la seguridad.

Los "*agujeros*" en la seguridad (puntos vulnerables) se manifiestan de cuatro formas:

1. *Agujeros* de Seguridad en la parte física.

En estos el problema básicamente consiste en dar acceso a la parte física de la máquina a personas no autorizadas. Ejemplos de esto son aquellos centros donde se tienen estaciones de trabajo y para un usuario puede resultar trivial reinicializar una máquina en modo monousuario (single user) y alterar el almacenamiento de archivos, o bien no restringir el acceso a respaldos de cintas confidenciales, que pueden ser leídas por cualquier usuario con acceso al manejador de cintas.

2. *Agujeros* de Seguridad en Software.

Estos son básicamente software mal desarrollado, que debido a esto tiene altos privilegios que permiten acceder información confidencial.

3. *Agujeros* de Seguridad por incompatibilidad de uso.

En ocasiones debido a la falta de experiencia del administrador del sistema, ensambla una combinación de hardware con software que son útiles, pero desde el punto de vista de seguridad presentan un agujero, esto es conectar dos cosas incompatibles que aunque funcionen, son vulnerables en seguridad.

[9] Cooper, James Arlin
Computer & Communications Security
McGraw Hill Publishing N.Y., 1989

4. En no elegir una idónea filosofía de seguridad y mantenerla.

El cuarto tipo es percepción y entendimiento. Un software perfecto, hardware protegido, y compatibilidad de los componentes no trabajan a menos que se seleccione y aplique una política de seguridad adecuada. Tener el mejor mecanismo del mundo para asignar contraseñas (passwords), está por demás si los usuarios asignan el nombre de su clave como contraseña.

La seguridad es relativa a la política o conjunto de políticas y a la función del sistema conforme a ese conjunto de políticas.

2.3 Modelo de Seguridad.

Para evaluar las necesidades de implementar la Seguridad en los sistemas de Información en cualquier organización y poder elegir mas apropiadamente los productos y/o políticas, recae en la responsabilidad del administrador en definir con claridad los requerimientos y características de la organización. Una manera de enfocarlo es considerando tres aspectos de la Seguridad:

1 **Servicios en Seguridad.-** Un servicio que mejora la Seguridad en los Sistemas de procesamiento en Datos y la Información enviada por la Organización. Los Servicios son orientados a oponerse a los Ataques de Seguridad haciendo uso de uno o más mecanismos para garantizar el Servicio.

2 **Mecanismos de Seguridad.-** Un mecanismo diseñado para detectar prevenir los ataques en Seguridad.

3 **Ataques en Seguridad.-** Cualquier acción que compromete la Seguridad en la Información de la Organización.

2.3.1 Servicios en Seguridad

Mucho de la actividad humana se basa en el intercambio de información en forma electrónica y depende de las transacciones confidenciales y en la integridad de estos documentos. Los documentos típicamente tienen información valiosa, así como firmas y fechas, los cuales debe ser necesario protegerlos contra alguna destrucción. Como en los sistemas de información llega a ser más esencial para el manejo de nuestro negocio, la información electrónica toma muchos roles en la organización.

Una clasificación de los Servicios de Seguridad sería la siguiente:

2.3.1.1 Confidencialidad

Asegura que la información recibida sea accesada únicamente por las entidades autorizadas.

2.3.1.2 Autenticación

Asegura al transmisor sea correctamente identificado para que su identidad no sea falsificada por un tercero.

2.3.1.3 Integridad

Asegura que solo las partes puedan modificar la información transmitida. Estas modificaciones incluyen escritura, cambios, borrar, crear, retrasar o reenviar la información. La información recibida es igual a la transmitida por medio de funciones matemáticas y firmas digitales como veremos mas adelante.

2.3.1.4 Norepudiación

Así como los usuarios no autorizados deben ser controlados, los usuarios autorizados también cometen errores y aún más actos maliciosos. En este caso se debe determinar qué fue hecho, por quién y qué fue afectado. La única forma de obtener esta información es por medio de un registro incorruptible que registre todas las actividades del sistema y que sea capaz de identificar el actor y las acciones involucradas, de esta manera se evita que quien(es) esté(n) involucrados en la comunicación nieguen haber participado. Requiere que las partes involucradas no puedan rechazar la transmisión

2.3.1.5 Control de acceso

Requiere que el acceso a los recursos puedan ser controlada por el sistema destino. se deben determinar los siguientes puntos: cómo logro entrar, qué ha hecho y quién, o qué más tiene acceso al sistema. No debe confundirse el controlar el acceso con autenticar ya que se puede autenticar a un usuario para accesar el sistema y mediante el aislamiento se definen los permisos que tiene.

2.3.1.6 Disponibilidad

Requiere que los recursos estén disponibles para entidades autorizadas[10].

[10] Lynch, Daniel C. and Rose, Marshall T
Internet System Handbook
Addison Wesley Publishing Company, INC. , 1993

2.3.2 Mecanismos de Seguridad

No hay un mecanismo que provea funciones tales como Identificación, Autorización, Acceso, Válidación, etc. A lo largo de este capítulo veremos como algunos puntos de desarrollo, uso y de administración son comunes en las técnicas de criptografía. La encripción de información son los primeros puntos para proveer Seguridad, el cual es tema de desarrollo posteriormente.

2.3.3 Los Intrusos.

Este es uno de los puntos más importantes, identificar quiénes pueden ser nuestros "enemigos" y sus causas.

A diferencia de lo que muchos pueden creer el mayor número de atacantes en las diferentes redes han sido personas de la misma empresa: administradores resentidos, vengativos, empleados que buscan algún beneficio propio ($), y los menos -pero no por eso menos peligrosos- son aquéllos que por curiosidad o para probar sus capacidades y la de su objetivo se entrometen en nuestro sistema, éstos últimos son los más famosos y existen diferentes acepciones para ellos, a veces llamados hackers y en otras crackers, aunque difieren las definiciones que podemos hallar a continuación pondremos las más difundidas:

¿Qué es un Hacker?

1.- Una persona que aprende los detalles de los sistemas de cómputo y como extender sus capacidades -opuesto a la mayoría de los usuarios, quienes prefieren aprender el mínimo necesario.
2.- Alguien que programa entusiasmadamente o quien se divierte programando, en lugar de revisar la teoría acerca de programar.

Hacker (según James Arlin Cooper)[11]

"Individuo que persistentemente explora computadoras y redes para aprender como pueden ser utilizadas. Actualmente el término se aplica a aquellos que tratan de burlar las barreras de seguridad de la computadora y de la red, la mayoría de las veces como un desafío."

La diferencia básica que hay entre un hacker y un cracker es la intención para el primero de aprender y para el segundo de dañar, no por esto vamos a justificar al hacker que de cualquier forma está violando nuestra seguridad.

Aunque éstos intrusos son muy peligrosos, no debemos olvidar a los primeramente mencionados y más dañinos por su propia naturaleza. La mayoría de las perdidas ocurridas

[11] Cooper, James Arlin
Computer & Communications Security
McGraw Hill Publishing N.Y., 1989

en empresas u organizaciones cada año, es el resultado de errores humanos, accidentes y omisiones, y de esto se deriva que las veces éstos son ocasionados por personal de la empresa o gente que colabora en la organización, y una minoría de estas pérdidas es ocasionada por personas ajenas al lugar donde suceden las mismas. Una persona que tiene por su labor acceso a nuestro sistema, un usuario, no tiene que evadir las barreras que un hacker ni las lógicas ni las físicas, así que le es más fácil destruir u obtener provecho de la información o del equipo, existen cientos de casos de gentes que han violado la seguridad, realizando fraudes, haciéndose ricos, obteniendo información clasificada o vengándose de alguna actitud tomada hacia él, y estas personas estaban o habían laborado en la empresa.

2.3.4 Ataques en Seguridad

Los ataques en Seguridad de un Sistema Computaciones o en una Red de Computación son los mejores ejemplos donde se caracterizan estos tipos de funciones. En general, hay flujos de información entre fuentes y destinos, tales como entre usuarios o entre Servidor y usuario donde una tercera entidad llamada intruso puede bloquear su información, como se muestra en la figura No 2.1.

En base al esquema detallado en la figura No 2.1, podemos mencionar que tales ataques de seguridad se pueden clasificar en:

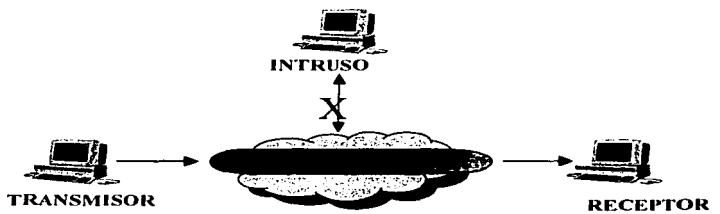


Figura No 2.1 Ataques en seguridad

2.3.4.1 Intercepción

Una entidad sin autorización ganando acceso a los recursos. Este tipo de ataque es sobre la Confidencialidad. La parte no autorizada podría ser una persona, un programa o una computadora. Como ejemplo puede ser la copia ilícita de archivos. Figura No 2.2.

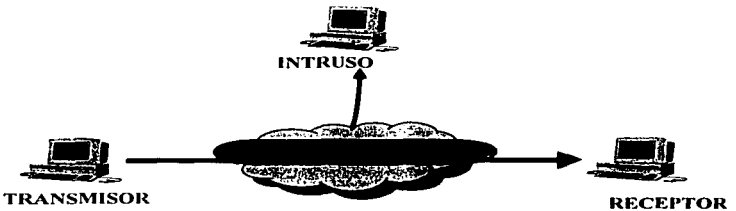


Figura No 2.2 Ataque de tipo intercepción.

2.3.4.2 Interrupción

Este es un tipo de ataque sobre la disponibilidad. Como ejemplos se tendría cuando se destruye un sector de un disco duro o el romper una línea de comunicación. En forma gráfica podemos verlo en la figura No 2.3.

Figura No 2.3 Ataque tipo interrupción.

2.3.4.3 Modificación

Una parte no autorizada no solo ganando el acceso sino también tomando recursos de la organización. Este tipo de ataque recae en la Integridad. Como ejemplo, los valores cambiados en un archivo y luego siendo transmitidos hacia la Red. Figura No 2.4.

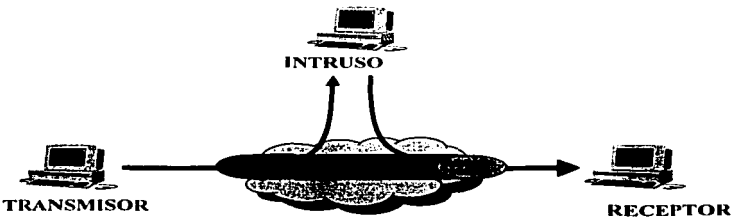


Figura No 2.4 Tipo modificación.

2.3.4.4 Fabricación

En la figura No 2.5 podemos describir este tipo de ataque, la falsificación de objetos en los sistemas por alguien no autorizado. Es un ataque en la Autenticidad. Cuando el intruso inserta mensajes falsos a la red o cuando agrega registros a los archivos.

Una categoría conveniente de estos ataques es en términos de ataques Pasivos y Activos, como veremos posteriormente.

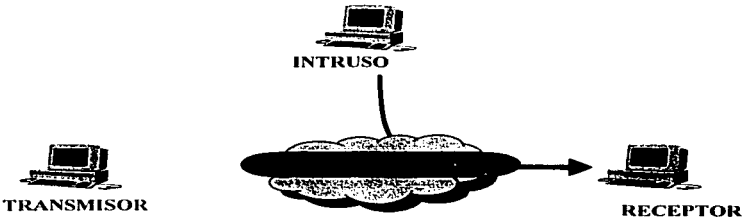


Figura No 2.5 Ataque tipo fabricación.

2.3.5 Ataque Pasivo

Este tipo de ataques es por naturaleza de intromisión sobre las transmisiones o monitoreos a los Sistemas. El objetivo del intruso es el de obtener información sobre el canal de comunicación. Los dos tipos de ataques de ataques Pasivos son: el Análisis de Trafico y al contenido de Información.

El ataque al contenido de información es, por ejemplo en una conversación telefónica, en un mensaje electrónico (E-Mail) o en la transferencia de archivos puede contener información confidencial y nosotros prevenimos que el intruso accese a los contenidos de información confidencial..

El ataque de Análisis de Trafico es más inteligente, suponer que tenemos la manera de disfrazar el contenido de la información utilizando técnicas comunes como son encriptando o codificando el contenido.
El intruso podría determinar la ubicación e identificar las entidades de comunicaron entre usuarios poniendo atención en la frecuencia y longitud de los mensajes en intercambio. Esta información podría ser útil para descifrar esta misma.

Los ataques Pasivos son difíciles de detectar pues atacan a la confidencialidad y no involucran alteración en los archivos de datos. Sin embargo, es posible el prevenir este tipo de ataques mas que su detección. Ver figura No 2.6 (a).

2.3.6 Ataque Activo

Este tipo de ataques involucra la modificación o creación de información falsificada que puede ser clasificada como: información falsificada, REPLAY , modificación de mensajes y rechazo de servicio.

- Un ataque falsificando información se encuentra cuando una entidad trata de introducirse entre una conversación y finge ser una de las dos con el objetivo de obtener privilegios extras.
- El ataque REPLAY involucra una captura pasiva de datos y su subsecuente retransmisión para producir un efecto no autorizado.
- La modificación de mensajes simplemente significa que una parte de un mensaje legitimo es alterado y que este mensaje es retrasado y grabado para producir un efecto no autorizado.
- El rechazo de servicio previene o inhibe el uso normal del canal de comunicación. Este ataque es frecuentemente hacia un destino en especifico.

Los ataques Activos presentan lo opuesto a los Pasivos. Donde los pasivos son difíciles de detectar, las medidas son disponibles para prevenir sus éxitos. De otra manera, es bastante difícil él prevenirlos y se tendría quedar protección física a todas las entidades y caminos todo el tiempo. Siendo mejor él detectarlos para recuperar o retrasar la ruptura causada a los sistemas. Este tipo de ataque se muestra en la figura No 2.6. (b)[12].

Figura No 2.6 (a) Ataques Pasivos.

Figura No 2.6 (b) Ataques Activos.

[12] Cryptography And Network Security
William Stallings
Prentice may
1999

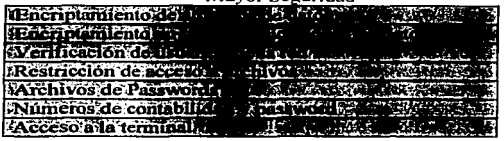
2.3.7 Modelo básico para Seguridad en redes.

A continuación se presenta un primer modelo de seguridad que provee una descripción de los puntos que se deben tratar en cuanto a seguridad en redes e integridad de los datos se refiere.

Davidson y White, sugieren un sistema de seguridad como una serie de círculos concéntricos formando capas alrededor de los datos de la computadora. Fuera de estos círculos se representa el nivel mínimo de seguridad y hacia dentro de los círculos se representa el máximo nivel de seguridad.

El modelo es demasiado simplista a la luz de la nueva tecnología. En vez de círculos se presenta a continuación un modelo integrado por capas, donde la capa superior representa el máximo nivel de seguridad y la más baja el mínimo nivel de seguridad.

Mayor Seguridad



Menor Seguridad

En base a lo anteriormente detallado podemos pasar a dimensionar un modelo de seguridad, en lo que se refiere en términos generales, un mensaje enviado entre dos puntos a través de algún medio de comunicación, como Internet. Estos puntos son la parte principal de esta transacción, pues deben cooperar para este intercambio. Un canal lógico es establecido definiendo la ruta entre fuente y destino además de los protocolos necesarios para ayudar a este intercambio.

Una tercera entidad debe ser necesaria para asegurar la comunicación entre A y B, él arbitro. Esta entidad es la responsable de distribuir la información secreta a las entidades principales como por ejemplo, la llave secreta descrita posteriormente.

El intruso puede llegar a ser humano, como un hacker o craker, o bien software, como los virus[13].

[13] Cooper, James Arlin
Computer & Communications Security
McGraw Hill Publishing N.Y., 1989

Finalmente todos los elementos que componente nuestro modelo serian como lo muestra la figura No 2.7.

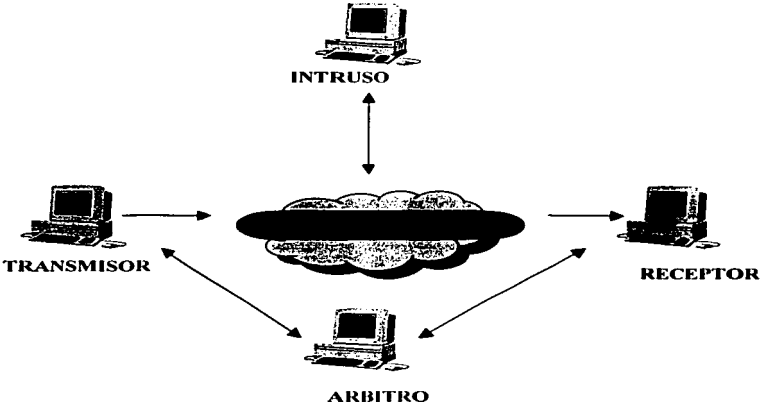


Figura No 2.7 . Modelo de seguridad

2.4 Criptografía simétrica

La Criptografía simétrica o también llamada encripción simétrica utiliza algoritmos comercialmente conocidos como:

- Data Encryption Standard (DES)
- 3DES (triple DES)
- Rivest Cipher 4 (RC4)
- International Data Encryption Algorithm (IDEA)

La Criptografía simétrica es ampliamente utilizada para brindar servicios de confidencialidad debido a que estos algoritmos fueron disenados para ser implementados en hardware principalmente y han sido optimizados para encriptar grandes cantidades de datos.

El reto de la encripción simétrica es:

- Cambiar las llaves secretas frecuentemente para evitar el riesgo de comprometer las llaves.
- Generarar con alta seguridad las llaves secretas
- Distribuir con alta seguridad las llaves secretas

Un mecanismo comúnmente utilizado para intercambiar las llaves secretas con alta seguridad es utilizando el algoritmo Diffie-Hellman, descrito posteriormente.Los componentes básicos del proceso de encripción simétrica, se detallada en la figura No 2.8.

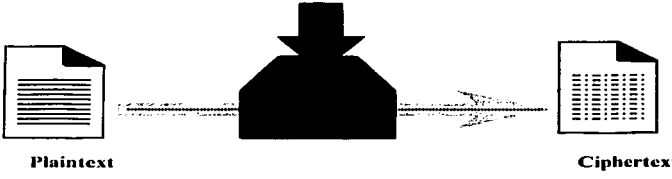


Figura No 2.8 . Elementos de la encripción.

Aplicando estos elementos de encripción a nuestro anterior modelo de seguridad en la sección 2.2.7., podemos decir, una entidad que desea transmitir información a través de medio seguro producirá un mensaje lo llamaremos "plaintext", de la forma $X = [X_1, X_2, \ldots, X_S]$. Los elementos S de X son letras dentro un alfabeto finito. Tradicionalmente, el alfabeto contiene 26 letras. Hoy en día, el alfabeto binario [0,1] es usado. Para encripción, la llave secreta de la forma $K = [K_1, K_2, \ldots, K_J]$ es generada. Si la llave secreta es generada en la entidad transmisora, luego entonces el destino deberá tener o compartir esta misma llave secreta, para proveer un canal de comunicaciones seguro. Alternativamente una tercera entidad podría generar esta llave secreta y luego distribuirla a ambas entidades.

Con el mensaje X y la llave secreta K como entrada, el algoritmo de encripción formara el mensaje encriptado llamado "Ciphertext" $Y = [Y_1, Y_2, \ldots, Y_R]$. Luego nosotros podemos deducir:

$$Y = E_K (X)$$

Donde esta notación indica que Y es producido usando un algoritmo de encripción E como función del plaintext X, con la función especifica determinada por el valor de K.

El receptor, en posesión de la misma llave secreta K podrá invertir la función Y de transformación:

$$X = D_K (Y)$$

El intruso, observando el valor Y sin tener acceso a los valores de K y de X, su reto será el intentar recobrar X o K o aun ambos valores. Asumiendo que el intruso conoce los algoritmos de encripción E y de desencripción D, el intruso estará interesado en un mensaje en particular, luego se enfocara en recuperar el valor X por medio de la generación de un plaintext estimado X' . Sin embargo, el intruso estará interesado en poder leer los mensajes a futuro, en dicho caso intentara recuperar el valor de K, generando un valor estimado K'.

Finalmente nuestra figura No 2.8 se vería como la figura No. 2.9

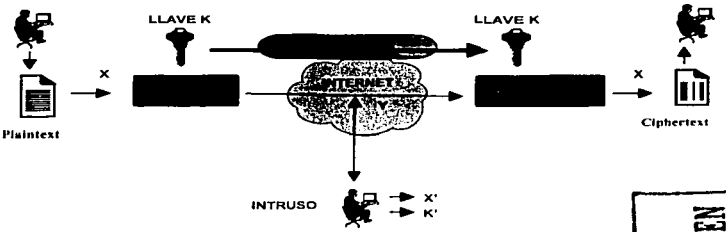


Figura No 2.9 . Modelo de Encripción.

2.4.1 Elementos de encripción simétrica.

Los sistemas Criptográficos son generalmente clasificados depediendo de:

2.4.1.1 El tipo de operación del mensaje plaintext a un ciphertext.

El tipo de operaciones utilizadas para transformar el texto a un mensaje codificado (ciphertext). Todos los algoritmos son basados en dos principios: el de sustitución, en el cual cada elemento del texto es mapeado a otro elemento y de la transposición en el cual los elementos en el texto son reacomodados. Los principales sistemas son referidos como productos de sistemas comprendiendo múltiples fases de sustituciones y transposiciones.

2.4.1.2 Llaves.

El numero de llaves utilizadas. Ambos el transmisor y el receptor usan la misma llave, el sistema es llamado como simétrico, llave simple, llave secreta o simplemente encripción privada. Si ambos usuarios utilizan diferentes llaves el sistema se llama asimétrico o encripción pública.

2.4.1.3 *El proceso del plaintext.*

La forma en la cual el plaintext es procesado. Una forma es empleando el proceso de bloques a codificar (plaintext), entra un bloque de datos y se obtiene un bloque codificado (ciphertext) del mismo tamaño. El proceso de codificado (ciphertext) por frase, en el cual entra una frase de longitud variable y se produce una frase codificada de la misma longitud que la original.

2.4.2 El criptoanálisis

El Criptoanálisis es el proceso de intentar descubrir los mensajes codificados por el intruso. La estrategia a seguir depende de la naturaleza del algoritmo de encripción y de la información disponible. En la tabla No 2.1. se muestran algunos de estos ataques.

TIPO DE ATAQUE	DEL CRIPTOANÁLISIS (INTRUSO)
Mensaje codificado (ciphertext) (ciphertext)	• Algoritmo de Encripción • El mensaje a ser decodificado (ciphertext)
Mensaje a codificar (plaintext) (plaintext)	• Algoritmo de Encripción • El mensaje a ser decodificado (ciphertext) • Uno o pares de mensajes codificados con la llave secreta

Tabla No 2.1. Tipos de Ataques.

Se resumen varios tipos de ataques de Criptoanalísis(intruso) basados en la cantidad de información conocida[14].

[14] Cryptography And Network Security
William Stallings
Prentice may
1999

Un posible ataque es el llamado BRUTE-FORCE que tratara de adivinar la llave buscando todas los posibles valores. Nosotros podemos considerar que el tiempo requerido cuando se utiliza este tipo de ataque es el mostrado en la tabla No 2.2.

TAMAÑO DE LLAVE (bits)	NUMERO DE LLAVES ALTERNAS	TIEMPO REQUERIDO EL ENCRIPCION/us	TIEMPO REQUERIDO 10⁶ ENCRIPCION/us
32	2^{32}	2^{31} µs= 35.8 minutos	2.15 milisegundos
56	2^{56}	255 µs = 1142 años	10.01 horas
128	2^{128}	2^{127} µs = $5.4*10^{24}$ años	$5.4*10^{18}$ años
26 permutaciones de caracteres	$26! = 4 * 10^{26}$	$2*10^{26}$ µs = $6.4*10^{12}$ años	$6.4*10^{6}$ años

Tabla No 2.2. Tiempos promedios.

Se muestra el tiempo que es tomado en encontrar el resultado correcto dependiendo de la longitud de la llave. Los resultados también son mostrados para aquellos llamados códigos por sustitución que usan llaves de 26 caracteres, detallados a continuación[15].

2.4.3 Técnicas de encripción

2.4.3.1 Técnicas de sustitución.

Una técnica de sustitución es en la cual las letras del texto es reemplazado por otra letra, números o símbolos. Si el texto es observado como un a secuencia de bits, luego la sustitución reemplaza este patrón de bits con un patrón de bits codificados.

El codificador Caesar fue de los iniciados y es el mas simple. Este codificador reemplaza cada letra del alfabeto con una letra desfasada tres localidades hacia abajo del alfabeto. Por ejemplo:

Mensaje plaintext = h o l a
Mensaje ciphertext= KROD

Observar que el alfabeto es secuencial, así que la letra Z sigue la A. Nosotros podemos definir la transformación completando el ciclo como sigue:

No codificado (plaintext)= a b c d e f g h i j k l m n o p q r s t u v wx y z

Codificado (ciphertext)= D E F G I H J K L M N O P Q R S T U V W X Y Z A B C

[15] Designing Network Security
Merike Kaeo
Cisco System
1999

Si nosotros asignamos un numero equivalente a cada letra (a=1, b=2, etc)entonces el algoritmo se puede expresar como sigue. Para cada mensaje a codificar (plaintext) seria "m", es sustituido por una letra codificada "c", luego entonces:

$$C = E(m) = (m + 3) \bmod(26).$$

Donde,
E= Algoritmo de encripción.

Desplazando aleatoriamente finalmente nos queda:

$$C = E(m) = (m + k) \bmod(26)$$

Donde K tomara los valores del rango de 1 a 25.

Para el algoritmo de decodificar (plaintext) es simplemente:

$$m = D(C) = (C - k) \bmod(26)$$

Si se conoce que el mensaje decofícado fue realizado con el algoritmo anterior, entonces el ataque BRUTE-FORCE será bastante fácil, solo seria el tratar con las 25 posibilidades de las llaves. En la tabla No 2.3., se muestran las 25 posibles llaves.

	KROD
1	j q n c
2	i p m b
3	h o l a
4	g n k z
5	f m j y
6	e l i x
7	d k h w
8	c j g v
9	b i f u
10	a h e t
11	z g d s
12	y f c r
13	x e b q
14	w d a p
15	v c z o
16	u b y n
17	t a x m
18	s z w l
19	r y v k
20	q x u j
21	p w t i
22	o v s h
23	u n r g
24	m t q f
25	l s p e

Tabla No 2.3. Criptoanálisis Brute-Force.

Tres importantes características resulta del problema anterior:

1.- La encripción y la desencripción de algoritmos son conocidos.
2.- Existen solo 25 llaves o posibilidades.
3.- El lenguaje del plaintext es común y fácilmente reconocible.

El uso del BRUTE-FORCE llega a hacer impractico cuando el algoritmo utiliza llaves de mayor longitud en el algoritmo de encripción.

La tercer característica es también importante. Si el lenguaje del mensaje plaintext esta en un lenguaje no común entonces llega a ser difícil, como por ejemplo un archivo comprimido con utilerias tipo ZIP.

2.4.3.2 Técnicas de transposición.

Una gran variedad de mapeos es realizada con alguna clase de permutación sobre las letras del mensaje a codificar (plaintext). Esta técnica es llamada codificación de transposición.

Esta técnica funciona de la forma en que el mensaje es escrito en secuencia pero hacia abajo en forma de diagonales y luego leído en secuencia lineal o en filas. Por ejemplo, el mensaje " prueba numero uno" con una profundidad de dos 2 líneas podremos formar el siguiente mensaje:

```
P u b n m r u o
  r e a u e o n
```

El mensaje encriptado seria:

PUBNMRUOREAUEON

Este ordenamiento llegaría a ser trivial para un intruso. Un esquema más complejo seria escribir el mensaje en un rectángulo, fila por fila, y leer el mensaje, columna por columna, pero realizando la permutación del orden de las columnas. El orden de las columnas se convertirá en la llave del algoritmo.
Ejemplo:

Llave:	4 3 1 2 5 6 7
Mensaje plaintext:	h o l a b u e
	n o s d i a s
Mensaje ciphertext:	LSADOOHNBIUAES

Una codificación pura por transposición es fácil de reconocer por que tiene la misma frecuencia que el mensaje sin codificar (plaintext). Para el tipo de transposición de columnas el criptoanálisis es muy lineal y se complica poniendo el mensaje codificado (ciphertext) en una matriz y jugando con las posiciones de las columnas.

La transposición podría significativamente llegar a ser más segura por la ejecución de mas de un estado de transposición. El resultado es una permutación compleja pues no es tan fácil la reconstrucción. Vea el mensaje si lo recodificamos por segunda vez.

Llave: 4 3 1 2 5 6 7
Mensaje plaintext: L S A D O O H
N B I U A E S

Mensaje ciphertext: AIDUSBLNOAOEHS

2.4.3.3 Técnicas de rotación.

Cuando hablamos de múltiples fases de codificaciones producen algoritmos significativamente más potentes y difíciles de criptoanalizar, esto es realmente cierto para las técnicas antes mencionados. Antes de la introducción de DES las principales aplicaciones utilizaron algoritmos conocidos como técnicas de rotación.

El principio básico de esta técnica se muestra en la figura No 2.10.

La maquina consiste en un conjunto de cilindros rotando independientemente a través de los cuales los pulsos eléctricos pueden fluir. Cada cilindro tiene 26 entradas y 26 salidas con conexiones internas que enlazan cada entrada con cada salida. Si nosotros asociamos cada entrada con cada salida con una letra del alfabeto entonces el primer cilindro define una técnica de sustitución.

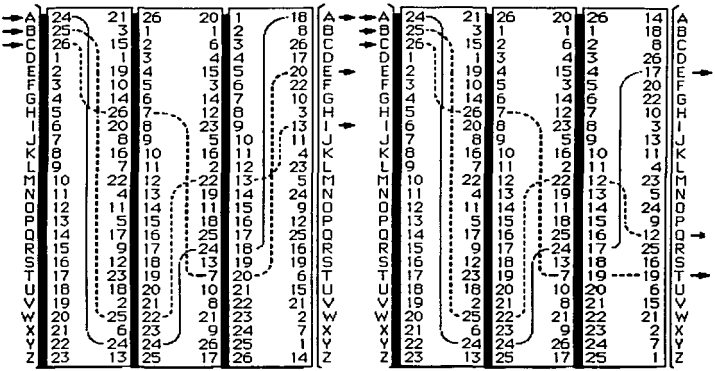


Figura No 2.10. Maquina de rotación

Si un operador oprime la tecla de la letra A un pulso eléctrico es aplicado a la primer entrada y sale por su correspondiente salida. Pensemos en una maquina con un solo cilindro, después de cada entrada, el cilindro realiza un movimiento de rotación, así que las conexiones internas para este momento han sido desfasadas. De este modo se ha definido una diferencia en cuanto a los algoritmos de sustitución. Después de 26 letras del mensaje a encriptar pasaran por el cilindro estaría en su posición original. De esta manera, nosotros tenemos un algoritmo de sustitución mas aleatorio con periodos de 26 letras.

Un sistema de un simple cilindro es trivial y no presenta una tarea el criptoanalizarlo. La fuerza de la técnica de rotación esta en el uso de varios cilindros, en el cual la salida de uno de los cilindros esta conectado a la entrada del próximo. En la parte de la izquierda de la figura No 2.10.

Muestra la entrada para la letra A la cual enrutada a través de los tres cilindros para salir en la segunda salida, la letra B. Este es simple el funcionamiento rotación y apunta como funcionan los algoritmos más recientes como: DES.

2.4.4 Encripción Moderna.

2.4.4.1 *Principios de los codificadores*

Existen dos tipos de codificadores. El primero seria el codificador por **Stream** funciona encriptando un stream de datos digitales que puede ser un bit o un byte. Ejemplos clásicos son el Codificador Vigenere y el Vernam. Un codificador por **bloque**, es cuando existe un bloque de texto para ser convertido en un bloque codificado (ciphertext) de igual longitud. Generalmente son bloques de 64 bits. Como ejemplo es el codificador por bloques Feistel.

Todos los algoritmos de encripción simétricos por bloques están basados en una estructura del Codificador Feistel.

2.4.4.2 *Codificador Feistel.*

Un codificador por bloques trabaja sobre un mensaje a codificar (plaintext) de N bits (un bloque) para producir un bloque codificado (ciphertext) de N bits. Hay 2^n posibles bloques diferentes para que la encripción sea reversible, es decir, que sea posible desencriptar, cada uno debe producir un único bloque codificado (ciphertext). Esta transformación es llamada reversible. Por ejemplo, cuando se produce bloque para n = 2 la siguiente tabla No 2.6 (a) nos muestra el caso en que se produce un mapeo único, mientras que en la en la tabla No 2.6 (b), nos muestra cuando no se cumple el mapeo único.

BLOQUE REVERSIBLE	BLOQUE ENCRIPTADO
00	11
01	10
10	00
11	01

Tabla No 2.6 (a)

BLOQUE TEXTO REVERSIBLE	BLOQUE ENCRIPTADO
00	11
01	10
10	01
11	01

Tabla No 2.6 (b)

Ahora, para ejemplos donde n=4 existe una entrada de 4 bits producirá 16 posibles salidas. Los mapeos de encripción y desencripción pueden ser definidos por una tabulación como en la tabla No 2.7. Esta es la forma más general de un codificador por bloques que puede ser usado para definir cualquier mapeo con características reversibles entre el mensaje a codificar (plaintext) y el mensaje codificado (ciphertext).

Sin codificar (plaintext)	Codificado (ciphertext)
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Tabla No. 2.7 (a)

(plaintext)	(ciphertext)
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Tabla No. 2.7 (b)

Pero hay un problema practico, si el tamaño del bloque es demasiado pequeño, como n=4 entonces el sistema es equivalente a un codificador normal de substitución anteriormente mencionado. Estos sistemas como hemos visto son vulnerables a los análisis del mensaje. Esta debilidad no esta inherente en el uso de un codificador por substitución sino en el uso de pequeños bloques.

Feistel propuso que se puede utilizar el concepto de producto codificado (ciphertext), el cual se lleva a cabo con dos o más bloques ya codificados colocándolos en forma secuencial, de tal manera que el resultado final o el producto es criptográficamente mucho mas fuerte contra los ataques. Feistel propuso el uso de alternar las operaciones de substitución y permutaciones anteriormente detalladas.

2.4.4.2.1 Estructura del Codificador Feistel.

En la figura No 2.11, muestra la estructura propuesta por Feistel. La entrada del mensaje a codificar (plaintext) es de longitud 2w (w = 8 bits) y la llave secreta K. El bloque de entrada es divido a la mitad. L_0 y R_0 , estas dos partes pasan a través de N ciclos de proceso y son combinados para producir un bloque codificado (ciphertext). Cada ciclo i tiene una entrada L_{i-1} y R_{i-1}, derivado del anterior ciclo también como la subllave K_i, derivada de K . En general las llaves K son diferentes de la subllaves K_i. Todos los ciclos tienen la misma estructura.

La exacta realización depende de la elección de los parámetros y diseños:

Tamaño del bloque.- tamaños largos significan mayor seguridad pero reduce la velocidad de codificación/decodificación. Un bloque de 64 bits es un tamaño razonable y muy cercano al diseño universal de los codificadores por bloques.

Tamaño de la llave secreta.- una llave larga también significa mayor seguridad pero alenta el proceso de codificación/decodificación. Los tamaños de 128 bits han llegado a ser comunes.

Numero de ciclos.- la esencia del codificador Feistel es que un simple ciclo ofrece una insuficiente seguridad. El valor típico es de 16 ciclos.

Subllave.- mayor complejidad para mayor dificultad de un Criptoanálisis.

Función de ciclo.- mayor complejidad para mayor dificultad de un Criptoanálisis.

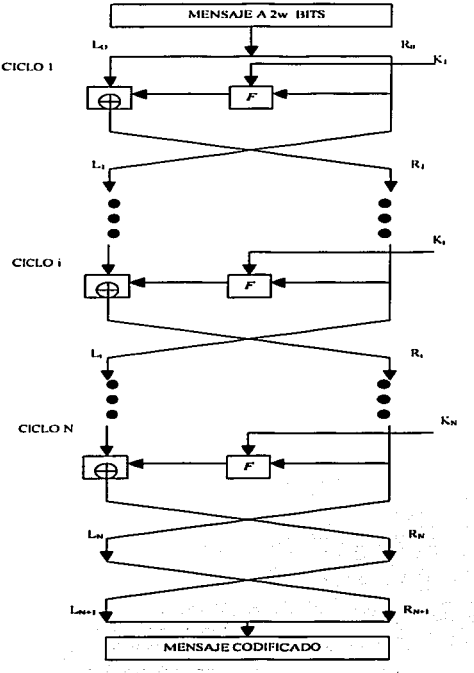


Figura No 2.11 Función de Feistel

Donde la función F realiza operaciones de expansión y permutación alterando unicamente los 4 bits a la izquierda y en un segundo proceso opera en los 4 bits restantes.

2.4.5 Data Encryption Standard. (DES)

Dentro de los algoritmos más importantes de los Codificadores por Bloques Simétricos son el Data Encryption Standard (DES) el Triple DES, IDEA, Blowfish, RC5, CAST y RC2. La selección fue basada en algunos criterios:

- Ellos son populares en aplicaciones sobre Internet.
- Ellos ilustran técnicas modernas de Codificadores de Bloques Simétricos que han sido desarrollados a partir de DES.

A continuación solo describiremos a detalle los algoritmos de DES y Triple DES, el resto solo serán mencionadas algunas características importantes.

El esquema de encripción mas ampliamente utilizado es el Data Encryption Standard adoptado en 1977 por National of Standard and Technology (NIST). Para DES, la encripción es utilizando bloques de 64 bits y una llave de 56 bits. El algoritmo transforma 64 bits de entrada después de una serie de pasos a un bloque de 64 bits. Con los mismos pasos y con la misma llave se hace el proceso inverso para su decodificación.

En forma genenral se presenta la figura No 2.12

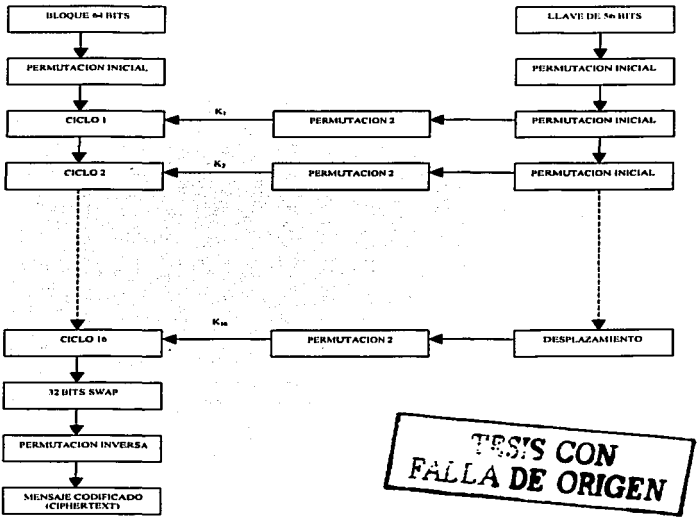


Figura No 2.12. Diagrama a bloques de DES

Como en cualquier esquema existen dos datos de entrada que son el mensaje a codificar (plaintext) de 64 bits de longitud y la llave de 56 bits de longitud. En la parte izquierda se observa tres pasos de este esquema. Primero, el mensaje pasa a través de una permutación (IP) que reestructura los bits para producir una entrada permutada. Esto es seguido por 16 ciclos de la misma función, la cual involucra permutaciones y substituciones. La salida de la función 16 ava se entrega al penúltimo paso de intercambio para producir un resultado. Finalmente este preresultado es pasado a una permutación inversa (IP^{-1}) que es la inversa de la primer permutación y su salida dará un bloque

codificado (ciphertext) de 64 bits en longitud. Con la excepción de la funciones de permutación, DES tiene la misma estructura que el codificador Feistel.

En la parte derecha se observa que la llave de 56 bits es pasada a través de una función de permutación y luego para cada uno de los 16 ciclos una subllave K_j es producida por la combinación de un desplazamiento circular y una permutación. La función de la permutación es la misma en cada ciclo, pero una subllave diferente es producida en cada ciclo a causa de la iteración repetitiva.

2.4.5.1 Permutación Inicial.

La permutación de inicio y la inversa son definidas por las tablas No 2.8.

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 No 2.8 (a) Permutación IP

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 No 2.8 (b) Permutación IP^{-1}

Para ver que estas dos funciones son realmente inversa de una de otra, consideremos la siguiente entrada de 64 bits:

M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}
M_{17}	M_{18}	M_{19}	M_{20}	M_{21}	M_{22}	M_{23}	M_{24}
M_{25}	M_{26}	M_{27}	M_{28}	M_{29}	M_{30}	M_{31}	M_{32}
M_{33}	M_{34}	M_{35}	M_{36}	M_{37}	M_{38}	M_{39}	M_{40}
M_{41}	M_{42}	M_{43}	M_{44}	M_{45}	M_{46}	M_{47}	M_{48}
M_{49}	M_{50}	M_{51}	M_{52}	M_{53}	M_{54}	M_{55}	M_{56}
M_{57}	M_{58}	M_{59}	M_{60}	M_{61}	M_{62}	M_{63}	M_{64}

Donde M_i es un dígito binario. Luego la permutación X = IP (M) el resultado sería:

M_{58}	M_{50}	M_{42}	M_{34}	M_{26}	M_{18}	M_{10}	M_2
M_{60}	M_{52}	M_{44}	M_{36}	M_{28}	M_{20}	M_{12}	M_4
M_{62}	M_{54}	M_{46}	M_{38}	M_{30}	M_{22}	M_{14}	M_6
M_{64}	M_{56}	M_{48}	M_{40}	M_{32}	M_{24}	M_{16}	M_8
M_{57}	M_{49}	M_{41}	M_{33}	M_{25}	M_{17}	M_9	M_1
M_{59}	M_{51}	M_{43}	M_{35}	M_{27}	M_{19}	M_{11}	M_3
M_{61}	M_{53}	M_{45}	M_{37}	M_{29}	M_{21}	M_{13}	M_5
M_{63}	M_{55}	M_{47}	M_{39}	M_{31}	M_{23}	M_{15}	M_7

Si nosotros tomamos el inverso de $Y = IP^{-1}(X) = IP^{-1}(IP(M))$, podríamos ver el orden original es restaurado.

2.4.5.2 Detalle de una función dentro de DES

En la figura No 2.13 se muestra a detalle la estructura de un unico ciclo. Otra vez, empezando el enfoque sobre la izquierda del diagrama, se tratan dos bloques de 32 bits, etiquetados con L y R.

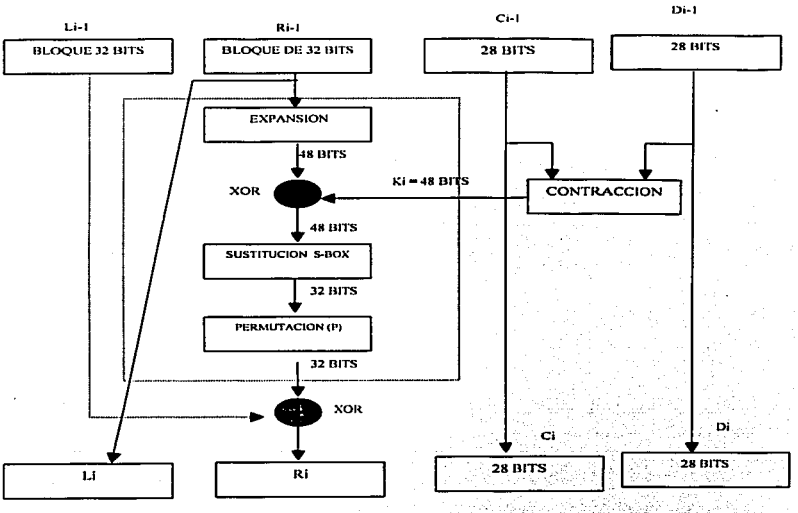


Figura No 2.13 Diagrama de DES para un ciclo.

El ciclo de la llave K_i de 48 bits. La entrada de R es de 32 bits. Esta entrada R primero se expande a 48bits usando tablas que define una permutación más una expansión. El resultado de 48 bits son Xor con K_i. El resultado de 48 bits es pasado ahora a una tablas de sustitución que produce 32 bits de salida. El rol de las cajas S, las cuales consisten en sustituciones, cada un acepta 6 bits de entrada y da una salida de 4 bits

2.4.6 Codificadores por bloques.

El algoritmo DES básicamente esta construido en bloques para proveer seguridad en datos. Para aplicar DES en una variedad de aplicaciones, existen cuatro modos de operación que son proyectados para cubrir todas las posibles aplicaciones de encripción en donde se podría aplicar DES. En la tabla No 2.9 son resumidos.

MODO	DESCRIPCION	TIPO DE APLICACION
Electronic Codebook (ECB)	Cada bloque es encriptado independientemente usando la misma llave.	Transmisión segura, La encripción de una llave.
Cipher Block Changing (CBC)	La entrada de un algoritmo es el XOR de los próximos 64 bits.	Autenticación.
Cipher Feedback (CFB)	La entrada es procesada en un tiempo.	Transmisión orientada en STREAM. Autenticación.
Output Feedback (OFB)	Similar a CFB.	Canales de comunicación por Satélite.

Tabla No 2.9 Resumen de los modos empleados en DES.

2.4.6.1 Electronic Codebook Mode

Este el modo mas simple, en el cual el mensaje a codificar (plaintext) es tomado en 64 bits al tiempo en que el bloque del mensaje es codificado (ciphertext) usando la misma Llave. El termino de Codebook es empleado porque para una llave dada hay único bloque codificado (ciphertext) de 64 bits. Para los mensajes mayores de 64 bits, el procedimiento es simple en romper el mensaje en bloques de 64 bits rellenando el último bloque si es necesario. Para la decodificación es realizada con la misma llave. En la figura No 2.2.14 se muestra el diagrama a bloques del modo ECB.

El modo ECB es ideal para cantidades de datos pequeñas.

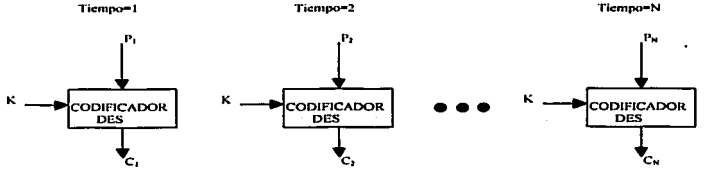


Figura No 2.14. Diagrama del Modo ECB

2.4.6.1.1 Modo Cipher Block Chaining

En la figura No 2.15. se muestra el esquema de cómo funciona el Modo CBC, donde la entrada se empieza con una XOR y luego se procede con la codificación. La misma llave es usada. Este Modo es util para bloques mayores de 64 bits, a demás de utilizarse en la Confidencialidad y la Autenticación.

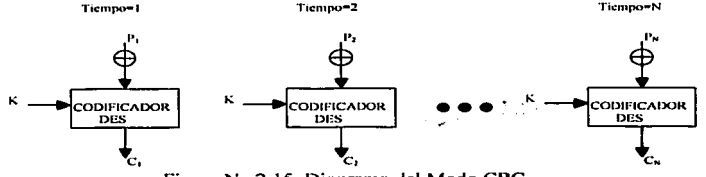


Figura No 2.15. Diagrama del Modo CBC

2.4.6.2 Modo Cipher Feedback.

En este Modo el bloque es convertido en un Codificador por Stream (CARACTER). Los codificadores por Stream eliminan la necesidad rellenar el mensaje para trabajar sobre bloques completos. También trabaja en tiempo real, es decir, si un Stream de caracteres esta siendo transmitido cada carácter será codificado (ciphertext) y transmitido usando un codificador por Stream orientado a carácter.

Una propiedad de estos codificadores es que la misma longitud de entrada será de salida. Si caracteres de 8 bits están siendo transmitidos, cada carácter deberá ser codificado (ciphertext) usando 8 bits. Si mas de 8 bits son usados la capacidad de transmisión será degradada.

2.4.6.3 Modo Output Feedback.

Este modo es similar al CFB. Una ventaja del Modo OFB es en la transmisión de bits con error no son transmitidos. Por ejemplo, si un error de bits ocurre en un C_1 solo el valor recuperado de P_1 es afectado, subsecuentemente las unidades del mensaje no son alteradas.

La desventaja de Modo OFB es que es mas vulnerable a las modificaciones de mensajes Stream que el Modo CFB[16].

[16] Cryptography And Network Security
William Stallings
Prentice may
1999

2.4.7 Triple DES

Dada la potencial vulnerabilidad de DES para los ataques BRUTE-FORCE con los avances de la tecnología, ha sido de interés el buscar una alternativa. Un acercamiento a esto es diseñar un nuevo algoritmo como mencionaremos mas adelante. Otra alternativa es usar múltiples DES con múltiples llaves[17].

La forma más simple de múltiples codificaciones es realizando al doble con dos llaves, como se muestra en la figura No 2.16(a) y 2.16(b). Dado un mensaje P y dos llaves K_1 y K_2, el mensaje codificado (ciphertext) queda:

$$C = E_{K2}(E_{K1}(P))$$

Donde la Decodificación se requiere que las llaves se han aplicadas en orden inverso:

$$P = D_{k1}(D_{k2}(C))$$

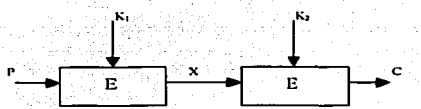


Figura No 2.16.(a) Diagrama del proceso de Doble Codificación.

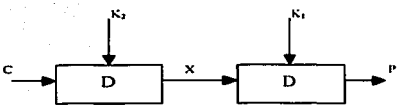


Figura No 2.16 (b) . Diagrama del proceso de Doble Decodificación.

[17]Cooper, James Arlin
Computer & Communications Security
McGraw Hill Publishing N.Y., 1989

Para el esquema se involucra una longitud de llave de 56 X 2 = 112 bits, resultando en un incremento drástico en la longitud de la Criptografía.

Muchas de las investigaciones sobre el Triple llave y el Triple DES muestran una alternativa preferente. Triple DES tiene una longitud de llave eficaz de 168 bits y se define:

$$C = E_{K3} (D_{K2} (E_{K1} (P)))$$

En compatibilidad con DES las llaves son $K_3 = K_2$ o $K_1 = K_2$. El diagrama se observa en la figura No 2.17 a y b.

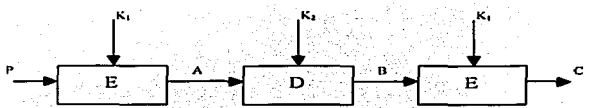


Figura No 2.17.(a) Diagrama de Encripción para Triple DES.

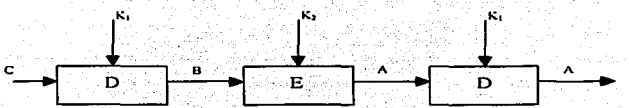


Figura No 2.17.(b) Diagrama de Desencripción para Triple DES.

2.4.8 International Data Encryption Algorithm (IDEA)

El algoritmo IDEA significa International Data Encryption Algorithm y es un codificador por Bloques Simétrico desarrolado por Xuejia Lai y James Massey del Intituto Federal de Tecnología de Suiza.

IDEA es uno de los algoritmos que han sido propuestos recientemente para sustituir a DES.

IDEA es un codificador por bloques que usa 128 bits de llave la encripción de bloques de 64 bits. En contraste con DES que solo usa 64 bits por bloque y 56 de llave, por lo tanto:

- Longitud de bloque.- 64 bits por bloque lo que fundamenta una gran fuerza contra los ataques estadísticos.
- Longitud de llave.- Con la longitud de 128 bits previene exhaustivas búsquedas de llave.

2.4.9 BLOWFISH

Blowfish un codificador por bloques simétricos desarrollado por Bruce Schneiser, con las siguientes características:

- Rápido.- Blowfish encripta datos sobre procesadores a velocidades de 18 ciclos de reloj por byte.
- Compacto.- Blowfish puede correr en menos de 5K en memoria.
- Simple.- Su estructura es fácil de implementar.
- Seguridad variable.- La longitud de la llave es variable y puede ser hasta de 448 bits. Esto permite una ventaja entre alta velocidad y alta seguridad, además de ser invulnerable al ataque de BRUTE-FORCE.
- Longitud de bloque.- Blowfish encripta bloques de 64 bits.

En la tabla No 2.10, se comparan las velocidades de los Codificador por Bloques.

ALGORITMO	CICLOS DE RELOJ	NUMERO DE CICLOS	NUMERO DE CICLOS DE RELOJ POR BYTE ENCRIPTADO
Blowfish	9	16	18
RC5	12	16	23
DES	18	16	45
IDEA	50	8	50
Triple-DES	18	48	108

Tabla No 2.10 Velocidades de codificadores por bloques.

2.4.10 RC5

RC5 es un algoritmo de encripción simétrico desarrollado por Ron Rivest y designado para tener las siguientes características:

- Apropiado.- RC5 utiliza operaciones comúnmente encontradas en cualquier procesador.
- Velocidad.- Es un algoritmo orientado a la palabra.
- Adaptabilidad.- RC5 es adaptable a diferentes longitudes de palabra de los procesadores.
- Ciclos.- Variabilidad en el numero de ciclos.
- Llave.- Longitud de llave variable permitiendo una ventaja en la velocidad y en la Seguridad.
- Simpleza.- RC5 tiene una estructura fácil de implementar.
- Memoria.- Bajas cantidades de memoria requiere RC5.

2.4.11 CAST-128

Este algoritmo fue desarrollado por Carlisle Adams y Stafford Tavares. CAST hace uso de llaves variables de 40 a 128 bits. CAST tiene una estructura como la de Feistel con 16 ciclos y con bloques de 64 bits para producir bloques codificados de 64 bits.

2.4.12 RC2.

RC2 es un algoritmo desarrollado por Ron Rivest y trabaja con bloques de 64 bits y tamaño de llaves variable de 8 a 1024 bits. El algoritmo es de fácil implementación en microprocesadores de 16 bits[18].

[18] Cryptography And Network Security
William Stallings
Prentice may
1999

2.4.13 Administración de Llaves

La administración de llaves es un problema difícil en la seguridad de comunicaciones, principalmente a causa de la sociedad mas que en los factores técnicos. Las maneras de crear y distribuir criptográficamente las llaves han sido desarrolladas y son justamente robustas. Sin embargo, los enlaces débiles en cualquier sistema de comunicaciones es que los humanos son los responsables de mantener la información y las llaves secretas confidencialmente.

Para empresas pequeñas, seria razonable crear llaves secretas y entregarlas manualmente, sin embrago, para empresas con cientos de usuarios usando aplicaciones requiriendo confidencialidad resultaría lento este proceso. En este caso, seria razonable tener una llave secreta por sesión, una sesión seria cualquier comunicación de transferencia de información entre dos entidades. Para estos casos la distribución de llaves se llevaria a cabo a través de centros de distribución con las llaves secretas o a través de algoritmos públicos que establezcan la distribución de estas llaves de manera segura.

El modelo de centro de distribución confiaría en una tercera entidad llamada Centro de Distribución de llaves , este modelo requiere que todos los participantes tenga una llave secreta con la cual estableceran confidencialidad hacia el Centro de Distribución de llaves, donde manualmente se almacenan las llaves secretas y cada entidad tiene su correspondiente llave secreta.

Un método para crear una sesión privada es utilizando el algoritmo de Diffie-Helman, este algoritmo proporciona una manera para que dos entidades establezcan y distribuyan las llaves secretas aunque estén por medios de comunicación no confiables.

En la figura No 2.18 se muestran los pasos que se llevan a cabo para un intercambio de llaves secretas[19]:

- El transmisor inicia el intercambio de dos números P y Q.
- El transmisor elige un numero entero Xa y realiza la ecuación $Ya = (Q^{XA}) \bmod P$.
- El receptor elige un numero aleatorio Xb y calcula $Yb = (Q^{XB}) \bmod P$.
- El transmisor envía Ya y el receptor envía Yb.
- El transmisor calcula la ecuación $Z = (Yb)^{XA} \bmod P$.
- El receptor calcula la ecuación $Z = (Ya)^{XB} \bmod P$.

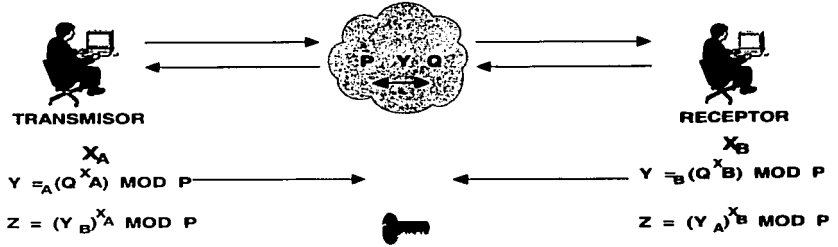


Figura No 2.18 Algoritmo Público de Diffie-Helman.

2.5 *Criptografía Asimétrica*

El desarrollo de la Criptografía Asimétrica o también llamada Encripción de llaves Públicas es el más grande y quizás la verdadera revolución en la Historia de la Criptografía. Todos los sistemas han sido basados en herramientas elementarias de sustitución y permutación. . Un principal avance en la Criptografía simétrica ocurrió con el desarrollo de la maquina de rotor para encriptar y desencriptar. Con la disponibilidad de las computadoras con sistemas aun más complejos el principal desarrollo fue Lucifer por IBM y finalizando en Data Encryption Standard (DES). Pero ambas Maquinas de Rotor y DES, aunque representan avances significativos, aun cuentan con herramientas de sustitución y permutación.

Los sistemas Criptográficos de llaves Públicas proporcionan una radical desviación de lo antes mencionado. Los algoritmos Criptográficos de llaves Públicas están basados en funciones matemáticas mas que en sustituciones y permutaciones. Lo más importante es,

[19] Big Book of IPSec
Pete Loshin
Morgan Kaufmann
Enero 2000

que los algoritmos Criptográficos de llaves Públicas también llamados algoritmos asimétricos incluyen el uso de dos llaves, encontraste con los algoritmos simétricos, los cuales usan solo una llave. El uso de estas dos llaves tiene profundas consecuencias en las áreas de Confidencialidad , Distribución de Llaves y un nuevo elemento, la Autenticación.

La encripción de llaves Públicas no son mas seguros que la encripción simétrica, pues, la seguridad de cualquier sistema de seguridad depende de la longitud de la llave y de que tan fácil es realizar él calculo computacional para descifrar o romper el codificador. No hay un principio que sea superior uno del otro desde el punto de vista del Criptoanálisis.

El concepto de la Criptografía de llave pública desarrollado es el intento de atacar las principales dificultades asociadas con la encripción simétrica, como la Distribución de las llaves.

La Distribución de estas las llaves requiere que dos entidades, ya sea que compartan una llave privada, la cual ha sido de alguna manera distribuida hacia ellos a través de un Centro de Distribución de llaves.

2.5.1.1 Criptosistemas Públicos

La encripción de llaves Públicas confían sobre una llave para encriptar y una llave diferente para desencriptar. Estos algoritmos tienen las siguientes características:

- Computacionalmente es impractico determinar la llave de desencripción teniendo conocimiento el algoritmo de encripción con su llave.
- Cualquiera de las dos llaves pueden ser usadas para encripción y la otra para desencripción.
- Pueden realizar la Autenticación de las entidades involucradas en el envío de información.

Se muestra el proceso de encripción para un algoritmo de llave pública, en la figura No 2.19. Los pasos son:

1.- Cada sistema en la red genera un par de llaves para encriptar/desencriptar el mensaje.
2.- Cada sistema publica su llave para encripción colocándola en un registro público.Esta es llamada llave Pública. La otra llave compañera es seguramente guardada llamada llave privada.
3.- Si el transmisor desea mandar un mensaje al receptor, lo hará encriptando el mensaje usando la llave Pública del receptor.

4.- Cuando el receptor recibe el mensaje, este lo desencripta usando su llave privada. Ningún otro punto puede desencriptar el mensaje por que solo el receptor conoce la llave privada.

Figura No 2.19 Encripción con llaves públicas.

Figura No 2.20 Desencripción con llaves privadas.

En la figura No 2.21 y 2.22 se muestra el proceso de Autenticación para la encripción de llaves Públicas.

Figura No 2.21 Proceso de Autenticación del transmisor hacia el receptor

Figura No 2.22 Proceso de Autenticación del receptor hacia el transmisor

Todos los participantes tendrá acceso a las llaves Públicas, mientras que las llaves privadas son generadas localmente por cada participante y por lo tanto nunca necesitan emplear métodos para su distribución. Cada sistema controla sus llaves privadas, al mismo tiempo cada sistema cambiar su Llave privada y su llave Pública por razones de reemplazar las anteriores llaves para mayor seguridad[20].

[20] Designing Network Security
Merike Kaeo
Cisco System
1999

1. El mismo algoritmo con la misma llave es usado para la encripción y la desencripción	1. Un algoritmo usado para encripción/desencripción con un par de llaves, una para encriptar y otra para desencriptar
2. El transmisor y el receptor deben compartir las llaves Secretas y el algoritmo	2. El transmisor y el receptor deben tener una del par de llaves, la llave Pública.
NECESARIO PARA SEGURIDAD:	*NECESARIO PARA SEGURIDAD:*
1. La llave debe ser guardada secretamente	1. Una de las llaves debe ser guardada secretamente
2. Debe ser impractico desencriptar un mensaje si no se tiene parte de la información intercambiada	2. Debe ser impractico desencriptar un mensaje si no se tiene parte de la información intercambiada
3. Con el conocimiento del algoritmo de encripción mas un mensaje codificado (ciphertext) debe ser insuficiente el determinar la llave.	3. Con el conocimiento del algoritmo de encripción mas un mensaje codificado (ciphertext) mas una de las llaves debe ser insuficiente el determinar la otra llave.

Tabla No 2.11 Encripción simétrica y asimétrica.

La tabla No 2.11, resume algunos aspectos importantes de encripción simétrica contra la asimétrica. Para diferenciar, generalmente nos referimos a Llave Secreta para la encripción simétrica y la encripción asimétrica, hacemos referencia como llave Pública y llave Privada. Invariablemente, la llave secreta o privada es guardada en alta seguridad.

Vamos a revisar los elementos básicos que componente el esquema de la encripción de llaves Públicas. Siendo la figura No 2.23 hay una fuente A o un transmisor que produce un mensaje como PLAINTEXT , $X = [X_1, X_2, ..., X_M]$. La M son los elementos de X y son caracteres del alfabeto finito.

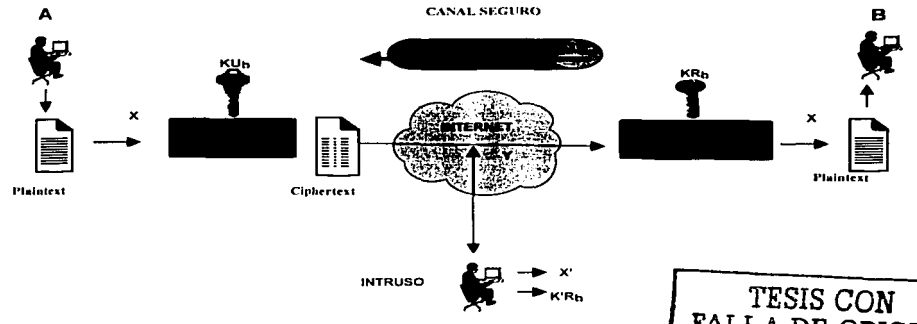


Figura No 2.23 Modelo encripción de llaves Públicas

El mensaje tiene el destino B. B generara un par de llaves: una llave Publica (KU_b), y una llave privada (KR_b). KR_b es solo conocida por B, donde KU_b es conocida públicamente para poder ser accesible por A.

Con el mensaje X y la llave de encripción KU_b como entrada, A formara el mensaje Ciphertext $Y = [Y_1, Y_2, ..., Y_N]$:

$$Y = E_{KUb} (X)$$

El receptor intentara, en posesión de la llave privada, poder invertir el proceso de la transformación:

$$X = D_{KRb} (Y)$$

Un intruso, observando Y y teniendo acceso a KU_b pero sin acceso a KR_b o X, deberá intentar recobrar a X y/o KR_b. Esto implica que el intruso no tiene conocimiento de los algoritmos de encripción/desencripción o E y D como se indico anteriormente. Si el

intruso esta interesado únicamente en este mensaje en particular, luego el objetivo para esforzarse es para recuperar X, por la generación de un mensaje (Plaintext) estimado llamado X'. Frecuentemente, el intruso esta interesado en poder leer los mensajes X posteriores, en cual caso un intento es realizado para recuperar KR_b por la generación parcial un seudo $K'R_b$

Para el caso anterior es un esquema que genera Confidencialidad. Como mencionamos anteriormente, también la encripción de llaves Públicas proporcionan Autenticación. Para este caso, A se prepara con un mensaje hacia B y lo encripta usando una llave Pública perteneciente a A. A causa de que el mensaje fue encriptado usando la llave privada de A, únicamente A podrá prepara el mensaje. Por lo tanto, el mensaje encriptado sirve como una firma digital. Además, es imposible alterar el mensaje sin acceso a la llave privada de A. Por lo que el mensaje es autentificado en ambos términos del transmisor y términos de integridad de datos. El esquema quedaría como en la figura No 2.24

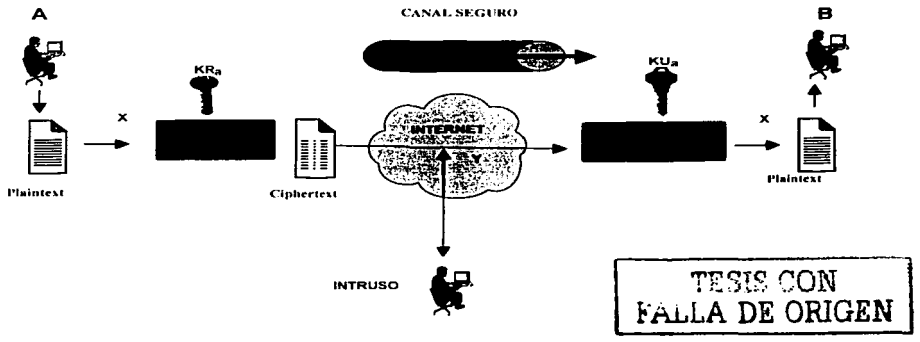


Figura No 2.24 Modelo de autenticación.

Sin embargo, es posible proporcionar ambas funciones de autenticación y confidencialidad usando un doble uso de la encripción de llaves Públicas. Como se muestra en la figura No 2.25, en este caso, nosotros empezamos como anteriormente encriptando el mensaje (Plaintext) , usando las llaves privadas. Esto proporciona la Firma Digital. Luego, nosotros encriptamos otra vez, usando las llaves Públicas del receptor. El mensaje final codificado (ciphertext) puede ser desencriptado solo por el receptor válido. Esto proporciona confidencialidad.

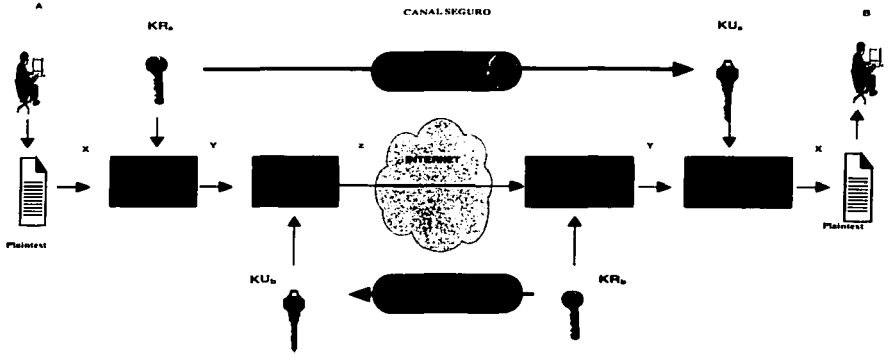


Figura No 2.25 Modelo de encripción y autenticación asimétrica.

2.5.2 Aplicaciones para los sistemas Criptográficos de llaves Públicas

Antes de comenzar, necesitamos aclarar un aspecto de la encripción de llaves Públicas Estos sistemas están caracterizados por el uso de un algoritmo con dos llaves, una llamada Privada y otra llamada Pública. Dependiendo de la aplicación, el transmisor utiliza ya sea la llave privada o la llave Pública, o ambas, para realizar algún tipo de función. En términos generales podemos clasificar el uso de los sistemas de llaves Públicas en tres categorías:

- **Encripción/desencripción:** El transmisor encripta un mensaje con la llave Pública del receptor.
- **Firmas Digitales:** El transmisor firma un mensaje con su llave secreta.
- **Intercambio de llaves:** Los dos puntos cooperan en la sesión de intercambio de llaves.

Algunos algoritmos son convenientes para las tres aplicaciones, donde otros puede solo usar una o dos de estas aplicaciones. La siguiente tabla No 2.12

Algoritmo	*Encripción/desencripción*	*Firma Digital*	*Intercambio de llaves*
RSA	SI	SI	SI
Diffie-Hellman	No	No	SI
DSS	No	SI	No

Tabla No 2.12 Aplicaciones de la encrición de llaves públicas.

2.5.3 Algoritmo RSA

Uno de los primeros en el desarrollo fue en 1977 por Ron Rivest, Adi Shamir y Len Adleman (RSA). El esquema RSA ha sido ampliamente aceptado e implementado como propósito general para la encripción de llaves Públicas.

RSA es un esquema de codificación por bloques en el cual el mensaje a codificar (plaintext) y el mensaje codificado (ciphertext) son enteros entre 0 y N-1 para un N. A continuación mencionaremos el algoritmo de RSA.

2.5.3.1 Desencripcion del Algoritmo de RSA

El esquema desarrollado por Rivest, Shamiry Adleman hace uso de expresiones exponenciales. El Plaintext es encriptado en bloques, donde cada bloque tiene un valor binario menor a N. Esto es, el tamaño del bloque debe ser menor o igual al $\log_2$ (n); en la practica, el tamaño del bloque es 2^K bits, donde $2^k < n < (\text{o igual}) \ 2^{k+1}$. La encripción y la desencripción son de la siguiente forma, para algún bloque plaintext M y un bloque Ciphertext C:

$$C = M^e \mod n$$

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

Ambos , tanto el receptor como el transmisor deben conocer n. El transmisor conoce el valor e, y solo el receptor conoce el valor de d. Este es un sistema de llave pública con una llave pública KU = { e, n } y una llave secreta KR = { d, n }. Para que este algoritmo sea satisfactorio para encripción de llave pública, los siguientes requerimientos deben ser conocidos:

1. Es posible encontrar valores de e, d, n tales que $M^{ed} = M \mod n$ para todo $M < n$.
2. Es relativamente fácil calcular M^e y C^d para todos los valores $M < n$.
3. Es impractico determinar d dado un valor de e y n.

2.5.4 Administración de llaves.

Uno de los principales roles de la encripción de llaves públicas ha sido el problema de la distribución de las llaves. Hay actualmente dos aspectos distintos para el uso de estos algoritmos:

- La distribución de las llaves.
- El uso de encripción de llaves públicas para distribuir las llaves privadas.

2.5.4.1 Distribución de llaves públicas

Algunas técnicas han sido propuestas para la distribución de las llaves públicas. Todas estas propuestas pueden ser agrupadas dentro de los siguientes esquemas:

1. Anuncio publico.
2. Directorios públicos.
3. Autoridad de llaves públicas.
4. Certificado de llaves públicas.

2.5.4.1.1 Anuncio publico

El punto de la encripción de llaves públicas es que la llave pública es realmente pública. Así, hay un extenso aceptación de los algoritmos de llaves públicas, tales RSA, cualquier participante puede enviar sus llaves públicas al otro participante, como se muestra en la figura No 2.26.

Por ejemplo, cuando un usuario envía sus mensajes de correo electrónico a forums públicos tales como USENET o a las listas de email en Internet son agregadas sus llaves públicas.

Aunque este método es muy cómodo, tiene sus debilidades: alguien que pueda falsificar tales anuncios públicos. Esto es, algún usuario que finga ser el usuario A y envíe una llave pública al otro participante o realice una emisión a cualquiera (broadcast) de tal llave pública y poder realizar la autenticación como se menciono anteriormente.

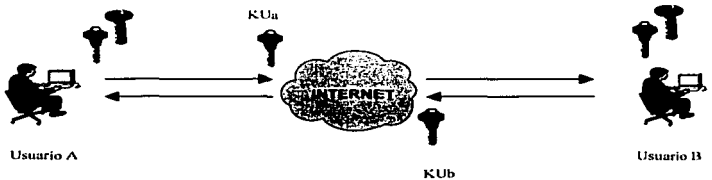


Figura No 2.26 Anuncio publico.

2.5.4.1.2 Directorios públicos

Un mayor grado de seguridad puede lograrse por el uso de un directorio público para llaves públicas. El mantenimiento y la distribución del directorio público tendría que ser responsabilidad de una entidad u organización de tipo arbitro. Tal esquema involucra lo siguiente:

1. La entidad u organización guarda el directorio con registros con {nombre, llave pública} para cada participante.
2. Cada participante registra una llave pública con la entidad. Este registro tendría que ser físicamente en persona o por algún medio de comunicación seguro en autenticación.
3. Un participante puede reemplazar las llaves existentes por determinado tiempo para brindar mayor seguridad.

Este esquema se muestra en la figura No 2.27 y es claramente más seguro que el anterior esquema pero aun tienen sus vulnerabilidades. Si un intruso exitosamente obtiene o calcula las llaves secretas del directorio, el intruso podría permitirse el acceso y falsificar las llaves públicas y poder personificar a cualquier participante.

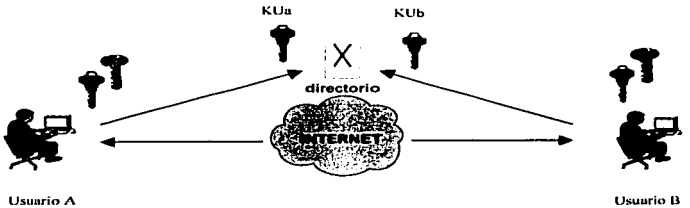


Figura No 2.27 Directorio publico.

2.5.4.1.3 Autoridad de llaves públicas

Para una fuerte seguridad en la distribución de las llaves públicas es utilizan un control hermético sobre la distribución de llaves desde un directorio. Un escenario típico se muestra en la figura No 2.28.

Como antes, el escenario asume que la Autoridad mantiene un directorio dinámico de llaves públicas de todos los participantes. Además, cada participante conoce una llave pública por la Autoridad, donde solo la Autoridad conoce la llave secreta. Los siguientes pasos suceden en la figura posterior.

1. El usuario A envía un mensaje a la Autoridad solicitando la llave pública del usuario B.
2. La autoridad responde con un mensaje que es encriptado usando la llave secreta de la Autoridad. El usuario A podrá desencriptar el mensaje utilizando la llave pública de la Autoridad, por lo tanto el usuario A certifica el mensaje recibido de la Autoridad. Este mensaje contiene lo siguiente:

   - La llave pública del usuario B, conque el usuario A podrá encriptar mensajes y ser enviados al usuario B
   - La respuesta al mensaje de solicitud descrito en el punto 1, con esto el usuario A hará una comparación con su correspondiente mensaje de solicitud.
   - Un mensaje con tiempo de vida, por lo que el usuario A podrá determinar si la llave pública del usuario B aun esta vigente.

3. El usuario A almacena la llave pública del usuario B. El usuario A envía un mensaje con un identificador de sí mismo (ID_A) .

4, 5. El usuario B obtiene de la misma manera la llave pública del usuario A con la Autoridad.

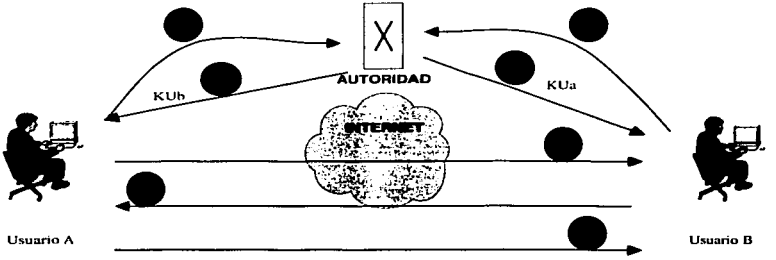


Figura No 2.28 Autoridad de llaves públicas.

En este punto, las llaves públicas de ambos usuarios han sido seguramente entregadas. Para los pasos 6 y 7 se lleva a cabo lo siguiente:

6. El usuario B envía un mensaje al usuario A, el cual es encriptado con la llave pública de A, el contenido son los ID's (ID_A y el ID_B). A consecuencia de que solo el usuario B podría haber desencriptado el mensaje en el paso numero 3, la presencia del ID_A asegura al usuario A la respuesta es del usuario B.

7. El usuario A regresa su ID_B, encriptándolo con la llave pública del usuario B, para asegurar al usuario B que esta respondiendo el usuario A.

Un total de siete pasos son requeridos. Sin embargo, los cuatro primeros pasos podrían ser solo aplicados no tan frecuentemente a causa de que el usuario A y B pueden salvar la información de las llaves públicas para un uso futuro, esta técnica es conocida como caching (segmentos de memoria). Periódicamente un usuario debería actualizar su información de llaves públicas para asegurar que se tiene la información actual.

2.5.4.1.4 Certificado de llaves públicas

Es atractivo pero aun tiene algunos inconvenientes. La Autoridad Pública podría ser un cuello de botella en un sistema, para un usuario que solicite a la autoridad una llave pública para cada usuario que desee contactar. Como antes, el Directorio de nombres y llaves públicas guardado por la autoridad es aun vulnerable.

Como una alternativa, es utilizando los Certificados que pueden ser utilizados por los participantes para el intercambio de llaves sin contactar a la Autoridad de llaves públicas, de esta manera es tan confiable como si las llaves fueran obtenidas directamente de la Autoridad de llaves públicas. Cada certificado contiene una llave pública y él ID del usuario; y es creado por una Autoridad Certificada, el cual es conocido por el participante que contienen una llave secreta autorizada. Los siguientes son los requerimientos de este esquema:

- Cualquier participante puede leer un certificado para determinar el nombre y la llave pública del propietario del certificado.
- Cualquier participante puede verificar que el certificado originado desde la Autoridad Certificada y que no sea falsificado.
- Solo la Autoridad Certificada puede crear y actualizar un certificado.
- Cualquier participante puede verificar los certificados actuales.

Un esquema de certificado se muestra en la figura No 2.29. Donde se llevan a cabo los siguientes eventos:

1. El usuario A proporciona la llave pública de A y realiza una solicitud de un certificado.
2. La autoridad certificada envía un mensaje en respuesta a su solicitud, este mensaje es encriptado con la llave secreta de la Autoridad Certificada. Este mensaje es llamado Certificado, siendo un mensaje encriptado con la llave secreta de la Autoridad y con contenido de la llave pública del usuario A, el tiempo de vida y su ID (ID_A).
3. El usuario solicita un certificado de la llave pública del usuario A y envía su llave pública para almacenarla en la base de datos y poder crear un certificado perteneciente al usuario B.
4. La autoridad envía un certificado conteniendo la llave pública del usuario B, el tiempo de vida y su ID (ID_B).
5. El usuario A envía su certificado con los datos de su llave pública.
6. El usuario B envía su certificado para que el usuario A pueda obtener la llave pública de B.

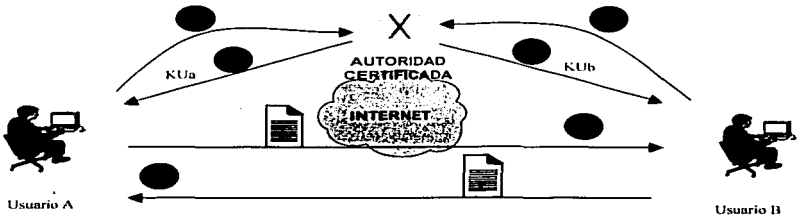


Figura No 2.29 Certificados.

Cada participante aplica a la Autoridad Certificada, proporcionando una llave pública y solicitando un certificado. La aplicación debe ser en persona o por algún medio seguro de comunicación autentificada.

2.5.4.2 X.509 Servicio de Autenticación

Las recomendaciones X.509 de la ITU-T son parte de las series de recomendaciones de la X.500 que define un Servicio de Directorio. El directorio es un servidor o un conjunto de servidores distribuidos que mantienen la base de datos de información a cerca de los usuarios. La información incluye un mapeo desde los nombres de los usuarios hacia sus direcciones de red, así como también los atributos y la información de los mismos.

El X.509 es un estándar importante por que la estructura de los certificados y los protocolos de autenticación definidos en el X.509 son usados en varios contextos. Por ejemplo, el formato de los certificados para IPSec, los certificados de SSL/TLS, etc.

El X.509 esta basado sobre el uso de la Criptografía de llave pública y firmas digitales.

2.5.4.2.1 Certificados

El Corazón del esquema X.509 es el certificado de llave pública asociado a cada usuario. Aquellos usuarios son asumidos para ser creados por alguna Autoridad Certificada (CA en ingles Certification Authority) y colocado en el directorio por un CA o por un usuario. El servidor de Directorio si mismo no es responsable por la creación de las llaves públicas, meramente proporciona un acceso fácil para que los usuarios obtengan sus Certificados.

La figura No 2.30 muestra el formato general de un certificado, el cual incluye los siguientes elementos:

Muestra el formato de un certificado el cual incluyen los siguiente:

- Versión: La versión de inicio es versión 1.
- Numero de serie: Un valor entero, único dentro de un CA.
- Identificador del algoritmo de firma: El algoritmo usado para firmar el certificado.
- Nombre del emisor: El nombre de X.500 de un certificado que firmo y creo este certificado.
- Periodo de Válidación: Consiste de dos componentes: inicio y fin en la cual el certificado es valido.
- Nombre del asunto: El nombre del usuario a quien se refiere este certificado.
- Información de llaves públicas: Las llave pública mas, un identificador del algoritmo por el cual esta llave será empleada.
- Identificador único del emisor: Un bit opcional usado para identificar el emisor CA cuando fue rehusado por diferentes entidades.
- Identificador único del asunto: Un bit opcional para identificar el asunto cuando ha sido rehusado por diferentes entidades.
- Extensiones: Un conjunto de extensiones usadas por certificados versión 3.
- Firma: Cubre todos los campos del certificado, contiene código de una función HASH, encriptado con la llave secreta del CA.

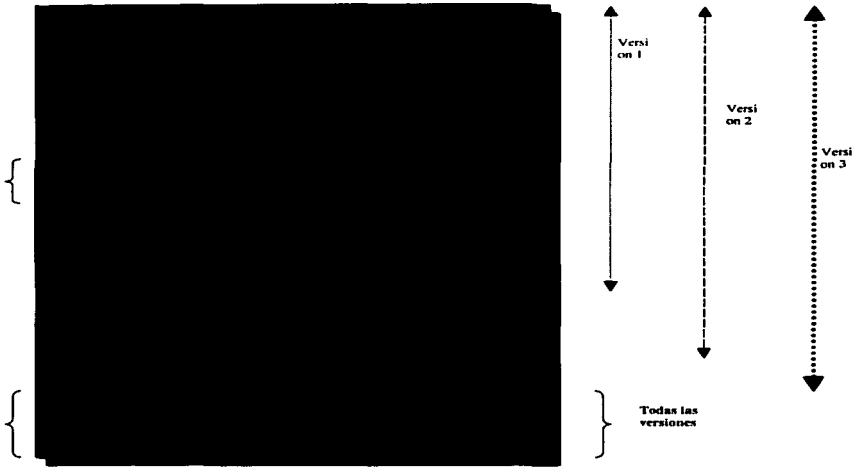


Figura No 2.30 Formato X.509.

2.6 *Autenticación*

Quizás una de las áreas de mayor confusión en la seguridad de redes son los mensajes de autenticación. Seria imposible describir las características completas de estas funciones criptográficas y de los protocolos propuestos o implementados para los mensajes de autenticación.

En resumen, los mensajes autentificados son procedimientos que verifican que el mensaje fue recibido de una fuente válidada y los datos no han sido alterados.

2.6.1 Funciones de autenticación

Cualquier mensaje autenticado puede ser visto con dos niveles. En un nivel inferior, hay funciones que producen un autentificador: un valor para ser usado para Autenticar la información. Este nivel es luego usado de manera primitiva en el nivel alto de autenticación el cual permite al receptor verificar la autenticidad del mensaje.

Los tipos de funciones que puede ser empleadas para producir un autentificador, se pueden agrupar en tres grupos y son:

- **Encripción del mensaje plaintext:** El mensaje encriptado sirve como autentificador.
- **Código de autenticación del mensaje (MAC, en sus siglas en ingles):** Una función pública del mensaje y una llave privada que produce un valor de longitud fija utilizado como autenticador.
- **Funciones HASH:** Una función pública que mapea el mensaje de cualquier longitud a un valor proviene de la Función Hash pero de longitud fija, la cual sirve como autentificador.

Ahora examinaremos cada uno de estas funciones.

2.6.1.1 *Encripción del mensaje plaintext*

Considerar el uso de la encripción simétrica, donde un mensaje es transmitido de la fuente A al destino B encriptando con una llave secreta K, compartida entre A y B. Como se muestra en la figura No 2.31.

Si ninguna otra entidad conoce la llave, luego entonces la confidencialidad es lograda: Ninguna otra parte puede recuperar el mensaje.

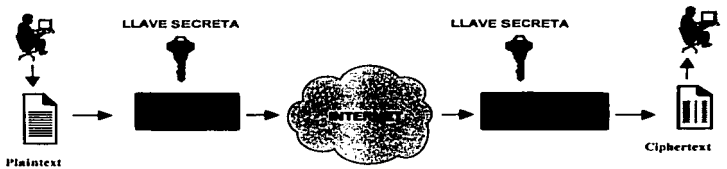


Figura No 2.31 Confidencialidad y autenticación.

2.6.1.2 *Código de autenticación del mensaje*

Una técnica alternativa que comprende el uso de llaves secretas para generar bloques de datos pequeños y de tamaño fijo, es conocido como checksum criptográfico o MAC, que es agregando una parte al mensaje. Esta técnica asume que dos entidades, A y B, comparte una llave secreta K. Cuando A tiene un mensaje a enviar a B, calcula la función MAC en función del mensaje y la llave:

$$MAC = C_K(M)$$

El mensaje mas el resultado de la función MAC (llamado digesto) es enviado al punto destino. El receptor realiza el mismo calculo sobre el mensaje recibido, usando una llave secreta para generar un nuevo valor proveniente de la función MAC.

El valor MAC recibido es luego comparado con este nuevo valor calculado por la entidad B, en otras palabras se compran los digestos. Observar la figura No 2.32.

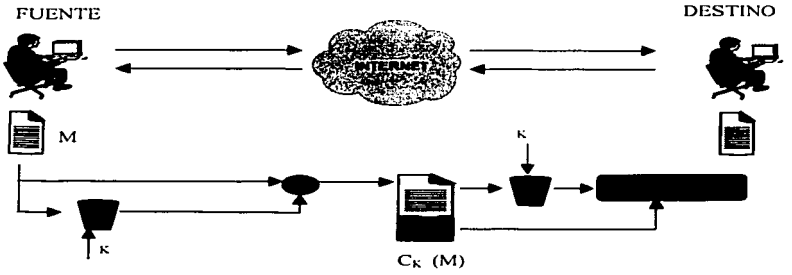


Figura No 2.32 Función básica de un código de autenticación.

Si nosotros asumimos que únicamente que A y B conocen la identidad de la llave secreta K, y si el receptor válida el digesto, luego:

1. El receptor esta asegurando que el mensaje no ha sido alterado. Si el intruso altera el mensaje pero no altera el digesto, cuando se realice él calculo por la entidad receptora habrá diferencia.
2. El receptor esta asegurando que el mensaje proviene de una entidad válida. A causa que nadie conoce la llave secreta y nadie podría calcular el digesto igual al original.
3. Si el mensaje incluye números de secuencia (tales como en TCP), entonces el receptor puede estar seguro de un apropiado numero de secuencia.

Una función MAC es similar a encriptar un mensaje. Una diferencia al respecto es que las funciones MAC no necesitan ser reversibles como los protocolos de encripción simétrica y son menos vulnerables[21].

[21] Cryptography And Network Security
William Stallings Prentice may
1999

2.6.1.3 Funciones HASH

Una variación sobre los códigos de autenticación (MAC) son las funciones HASH. Como las MAC una función HASH acepta mensajes plaintext de tamaño variable y produce un código HASH de tamaño fijo H (M), llamado digesto. Los códigos HASH es una función donde todos los bits del mensaje, y proporciona una capacidad de detección de errores: Un cambio en cualquier bit o bits del mensaje plaintext resultaría en un cambio del código HASH[22].

La figura No 2.33 muestra la función HASH proporcionando la autenticación y confidencialidad de un mensaje.

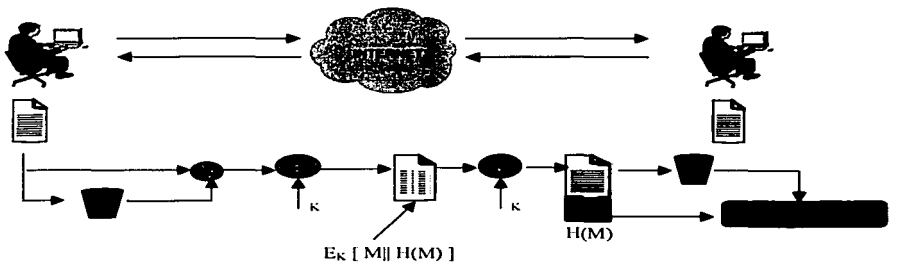


Figura No 2.33 Función HASH como autenticación y confidencialidad.

Este proceso se lleva a cabo como sigue:

1. El mensaje mas el código concatenado es encriptado usando encripción simétrica. A causa de que solo A y B conocen la llave secreta, el mensaje proviene de A sin ser alterado. Las funciones HASH proporciona una estructura o redundancia requerida para lograr la autenticación. A causa de que la encripción es aplicada al mensaje completo mas el digesto, la confidencialidad es también llevada a cabo.

[22] Designing Network Security
Merike Kaeo
Cisco System
1999

2. Unicamente el digesto es encriptado usando encripción. Esto reduce el proceso para aquellas aplicaciones que no requieran de la confidencialidad. Observar que la combinación de funciones HASH y encripción, esto es:

$$E_K\ [\ H(M)\ ]$$

en función de un mensaje de longitud variable y una llave secreta K para producir una salida de longitud fija como se muestra en la figura No 2.33

3. Unicamente las funciones HASH son encriptadas, usando una encripción de llaves públicas y utilizando la llave secreta del Transmisor, como en el punto numero 2, esto proporciona autenticación. También proporciona una firma digital, por que solo el transmisor ha producido un código HASH encriptado. De hecho, esto es la esencia de las técnicas para firmas digitales. Este paso sé detallada en la figura No 2.34

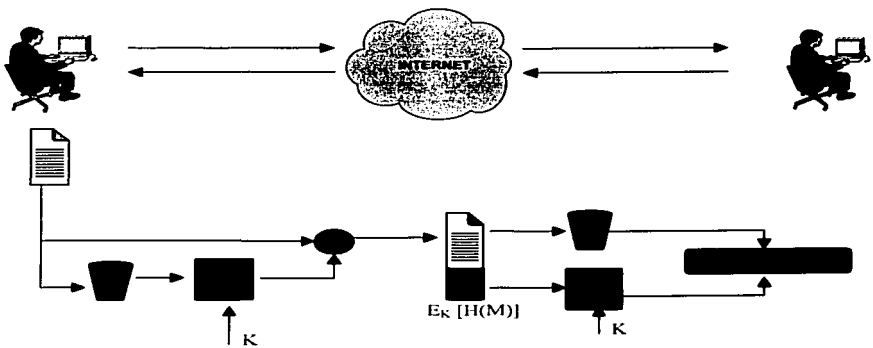


Figura No 2.34 Función HASH como autenticación.

Cuando la confidencialidad no se requiere, el método anterior tienen una ventaja sobre aquellos que encriptan el mensaje completo y es que se requiere menos recursos para su procesamiento. Sin embargo, ha sido de gran interés el eliminar la encripción dentro de cualquier técnica. Algunas razones para ello son:

- La encripción por software es muy lenta.
- La encripción por hardware es de costo elevado.
- La encripción por hardware es optimizada pero únicamente para manejo de información en volúmenes considerables.
- Los algoritmos de encripción deber cubiertos por patentes, elevando mas el costo.
- Los algoritmos de encripción son tema de control para su venta al extranjero.

El valor de la función HASH es generado por la función H de la forma:

$$h = H(M)$$

Donde M es el mensaje de longitud variable y H(M) es el valor de longitud fija, llamado digesto anteriormente mencionado.

Para los requerimientos de las funciones HASH para ser empleadas en la autenticación de mensajes, típicamente es complejo, mencionaremos algunos.

2.6.2 Algoritmo MD4

El algoritmo MD4 es el precursor del algoritmo MD5 desarrollado por el mismo autor, Ron Rivest. Fue originalmente públicado en octubre de 1990. Revisiones ligeras fueron públicadas en abril de 1992. Procesa longitudes de mensajes variables y produce un digesto de 128 bits. Algunas otras características son:

- En seguridad hay un requerimiento el cual menciona, que será impractico encontrar dos valores que tengan el mismo digesto.

- En velocidad, este algoritmo es muy factible que sea implementado en software pues trabaja sobre arquitecturas de 32-bits. Este algoritmo esta basado sobre operaciones simples de 32-bits por palabra.

- Simplicidad y compacto, el algoritmo debería ser simple para describir, sin requerir programas largos o tablas de sustitución.

2.6.3 Algoritmo MD5

El algoritmo MD5 (messages digest algorithm) fue desarrollado por Ron Rivest con el RFC 1321. El algoritmo toma una entrada de mensaje de longitud arbitraria y produce como salida un digesto de 128 bits. La entrada es procesada en bloques de 512 bits. Algunas diferencias con respecto al algoritmo MD4 son:

1. MD4 usa tres ciclos con 16 pasos cada uno, donde MD5 utiliza 4 ciclos con 16 pasos cada uno.
2. MD5 utiliza cuatro funciones primitivas en cada ciclo contra MD4 que trabaja contra tres funciones por ciclo.
3. La fuerza de MD5 de no encontrar dos digestos iguales de dos mensajes, donde la dificultad de encontrarlos seria del orden de 2^{128} operaciones.

Desde el punto de vista del Criptoanálisis, MD5 es considerado vulnerable en la actualidad, desde el punto de vista de un ataque de tipo BRUTE-FORCE. Como resultado, hubo la necesidad de reemplazarlo con funciones más resistentes a los métodos criptoanalíticos. Surgiendo SHA, el cual examinaremos posteriormente.

2.6.4 Algoritmo Secure HASH (SHA)

El algoritmo con sus siglas en ingles SHA fue desarrollado por el Instituto Nacional de Standares (siglas en ingles NIST) y fue públicado en 1993. SHA esta basado en MD4 y su diseño también esta cercano al de MD4. El algoritmo SHA fue en primera instancia referenciado como SHA-1.

SHA-1 toma mensajes de entrada con un máximo de longitud no menor a 2^{64} bits y produce un digesto de 160 bits.

2.7 *Firmas Digitales*

El desarrollo más importante para la Criptografía de llaves públicas son las firmas digitales. Las firmas digitales proporcionan un conjunto de aptitudes de seguridad.

2.7.1 Requerimientos

La protección de mensajes autentificados por dos entidades quienes intercambian estos mensajes, por ejemplo, suponer que tenemos a A enviando un mensaje autentificado hacia B, sucediendo lo siguiente:

1. El punto A podría falsificar un mensaje diferente y reclamar que proviene de B. A simplemente tendría que crear un mensaje y agregarlo al código de autenticación usando una llave compartida.
2. B podría negar el envío de mensajes, por que es posible que A falsifique un mensaje, no hay manera de probar que B de hecho envío el mensaje.

En situaciones donde no esta completa la confianza entre A y B, algo mas que simplemente autenticación. La solución a este problema son las firmas digitales. Las firmas digitales son análogas a las firmas por hardware. Deben tener las siguientes propiedades:

- Deben poder verificar al autor y los datos de elaboración, como fecha y hora de la firma.
- Debe poder Autenticar el contenido de la hora de la firma.
- La firma debe verificarse por medio de una tercera persona, para resolver la disputa.

Sobre las propiedades básicas, podemos formular los siguientes requerimientos para las firmas digitales:

- La firma debe ser un patrón de bits que dependan del mensaje a ser firmado.
- La firma debe usar información única del transmisor.
- Debe ser relativamente fácil producir la firma digital.
- Debe ser fácil reconocer y verificar la firma digital.
- Debe ser impractico falsificar una firma digital.
- Deberá ser imposible guardar una copia de la firma digital.

El Instituto Nacional de Estandares (NIST) publicó el conocido Estándar de firma digital (siglas en ingles DSS). Donde DSS hace uso de las características de la función SHA. El DSS usa un algoritmo que proporciona solamente firmas digitales. A diferencia de RSA, no puede ser usado para encriptar o intercambiar llaves. Sin embargo, es una técnica de llaves públicas.

El DSS también hace uso de las funciones HASH. El código HASH es proporcionado como datos de entrada a las funciones de firma a lo largo de un numero aleatorio K. La firma digital también depende del valor que envía el transmisor (KR_a) y un conjunto de parámetros globales (KU_g) . El resultado es una firma que consiste de dos componentes, etiquetados como s y r.

En el punto de recepción, se genera un código HASH, este mas la firma es la entrada para verificar la función. Esta verificación también depende de la llave pública así como la llave del transmisor (KU_a) la cual es par de la llave secreta. La salida de la función es un valor que es igual a al componente de la firma r si la firma es válida. La función de firma es tal que solamente el transmisor, con conocimiento de la llave secreta podría haber producido una firma válida[21].

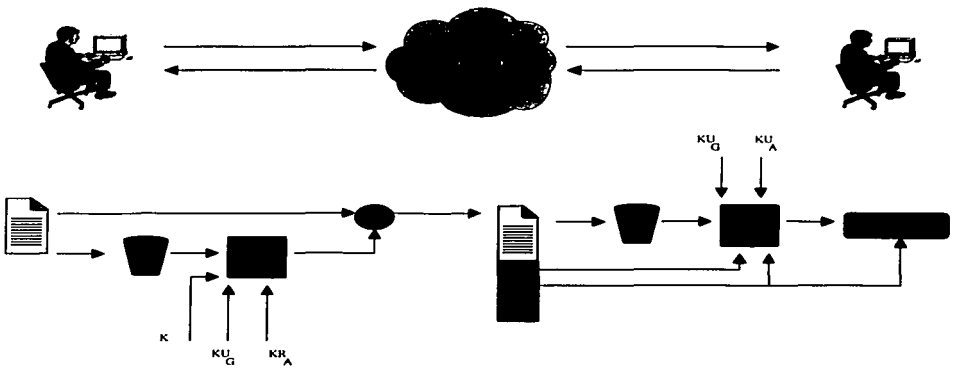


Figura No 2.35 Firmas digitales

[21] Cryptography And Network Security
William Stallings
Prentice may
1999

CAPITULO 3
IPSec

3 IPSec

La Internet ha desarrollado mecanismos de Seguridad para aplicaciones específicas, como el correo electrónico (S/MIME, PGP), Cliente-Servidor (Kerberos), Web (SSL). Hay mucha inquietud sobre la Seguridad a nivel de protocolos de comunicación, las redes Corporativas corren protocolos tales como TCP/IP para encriptar paquetes de datos utilizando protocolos como IPSec.

La Seguridad en nivel IP abarca tres funcionalidades: Autenticación, Confidencialidad y administración de Llaves. Los mecanismos de Autenticación aseguran que el paquete fue recibido, transmitido por la entidad identificado como la fuente dentro del encabezado de IP. A demás este mecanismo asegura que el paquete no ha sido alterado de camino a su destino. La Confidencialidad habilita la comunicación entre nodos para encriptar los mensajes para prevenir el robo de información. La administración de las llaves abarca el problema del intercambio de las mismas[24].

3.1 Antecedentes

En 1994, la Internet Architecture Board (IAB) publico un reporte acerca de la Seguridad en la Arquitectura de Internet. El reporte expresa un acuerdo en general de la necesidad de mejorar la Seguridad en Internet identificando las áreas para los mecanismos de seguridad. Entre otros el asegurar la infraestructura de monitoreos no autorizados o el control del tráfico de la red de usuarios usando mecanismos de encripción y de autenticación.

En respuesta a estos temas, la IAB incluye la encripción y la autenticación como necesarias para la seguridad en la nueva generación de TCP/IP, el cual a sido identificado como IPv6. Afortunadamente, estas capacidades fueron designadas para ser usadas en versiones anteriores como IPv4. Esto significa que vendedores podrán ofrecer estas facilidades en este momento con facilidades de IPSec. Durante este capitulo solo se desarrollara conceptos relacionados a IP versión 4.

[24] Big Book of IPSec
Pete Loshin
Morgan Kaufmann
Enero 2000

3.1.1 Aplicaciones

IPSec proporciona la capacidad de comunicación segura a través de un LAN, a través de redes WAN privadas o publicas y a través de Internet. Ejemplos del uso son:

- Conectividad entre oficinas remotas sobre Internet.
- Accesos remotos sobre Internet.
- Conectividad entre socios por Internet.
- Seguridad en el Comercio Electrónico.

El principal uso de IPSec es que permite el uso de variedad de Aplicaciones que puedan encriptarse y/o autenticarse todo el tráfico en un nivel IP del modelo OSI. Además, todas las aplicaciones distribuidas, incluyendo login remoto, cliente/servidor, E-mail, FTP, WWW, podrán ser seguros.

En la figura 3.1. esta un escenario real del uso de IPSec a través de Internet.

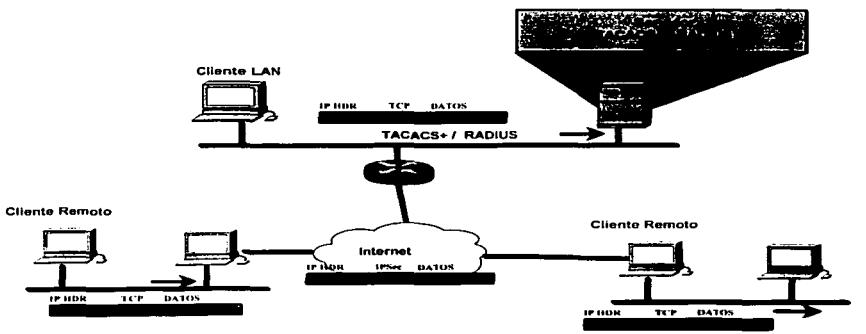


Figura 3.1. IPSec a través de una red pública.

Una organización mantiene localidades remotas dispersas, el tráfico entre redes locales es mantenido sin seguridad de IP y solo para el tráfico entre redes WAN es usado el protocolo IPSec. Este protocolo opera con los dispositivos de red, tales como enrutador o Firewall que son conectados por medio de una LAN hacia el mundo de Internet. IPSec encripta todo el tráfico hacia la Internet y realiza el proceso inverso para el tráfico que se recibe de la Internet, descripta; estas operaciones son transparentes para el usuario y los Servidores[25].

3.1.2 Beneficios de IPSec

Algunos de los beneficios son:

- Cuando IPSec es implementado en un enrutador o Firewall, proporciona fuerza en seguridad que puede ser aplicada a todo el tráfico que cruza el perímetro de la Red Corporativa.
- IPSec esta por debajo del nivel de transporte (TCP y UDP) como se muestra en la figura No 3.2; y es transparente a las aplicaciones. No hay necesidad de cambiar software sobre algún sistema cuando IPSec es implementado en cualquier dispositivo de comunicaciones.
- IPSec puede ser transparente para los usuarios finales
- IPSec puede proporcionar seguridad para usuarios individuales. Esto es util usuarios fuera del Corporativo, usuarios mobiles.

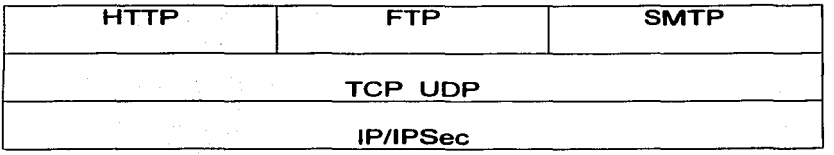


Figura 3.2. Nivel red.

[25] Cryptography And Network Security
William Stallings
Prentice may
1999

3.1.3 Aplicaciones de enrutamiento

Además de soportar a usuarios finales y proteger a sistemas de redes, IPSec también, se encuentra en los protocolos de enrutamiento requeridos para la interoperatividad. Como ejemplo:

- La petición de un enrutador (un nuevo equipo dentro de la red) es un dispositivo autorizado.
- La solicitud de adyacencia (un equipo intenta mantener una relación dentro de un dominio existente) proviene de un dispositivo autorizado.
- El mensaje de REDIRECT del protocolo de ICMP proviene de un equipo que originalmente fue enviado.
- Una solicitud de actualización de rutas falsificado.

Sin estas medidas de seguridad, un intruso puede dividir la comunicación o desviar el tráfico. Los protocolos de enrutamiento tales como OSPF deben correr con seguridad ayudados de IPSec[26].

[26] Designing Network Security
Merike Kaeo
Cisco System
1999

3.2 Arquitectura

Las especificaciones de IPSec han llegado a ser bastante complejas. Empecemos con algunos documentos que definen IPSec.

En agosto de 1995, la IETF publico 5 estándares en seguridad del nivel de Internet:

- RFC 2104—HMAC: Keyed-Hashing for Message Authentication
- RFC 2085—HMAC-MD5 IP Authentication with Replay Prevention
- RFC 2401—Security Architecture for the Internet Protocol
- RFC 2402—IP Authentication Header
- RFC 2403—The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404—The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405—The ESP DES-CBC Cipher Algorithm with Explicit IV
- RFC 2406—IP Encapsulating Security Payload (ESP)
- RFC 2407—The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408—Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409—The Internet Key Exchange (IKE)
- RFC 2410—The NULL Encryption Algorithm and Its Use with IPSec
- RFC 2411—IP Security Document Roadmap
- RFC 2412—The OAKLEY Key Determination Protocol
- RFC 2451—The ESP CBC-Mode Cipher Algorithms

El soportarlos es requisito para IPv6 pero opcional para IPv4. En ambos casos, las facilidades de seguridad son implementadas como extensiones del encabezado que es agregado al encabezado original de IP. Estas extensiones del encabezado son conocidas como encabezado de autenticación; para la parte de encripción es llamado como Encapsulating Security Payload (ESP), los cuales decribiremos mas adelante[27].

Los documentos son divididos en seis grupos, como siguen:

- Arquitectura. Cubre los aspectos generales, conceptos, requerimientos de seguridad, definiciones y mecanismos de la tecnología de IPSec.

[27] Big Book of IPSec
Pete Loshin
Morgan Kaufmann
Enero 2000

- ESP. Cubre el formato del encabezado relacionado al uso de ESP en encripción de paquetes, optionalmente autenticación.
- AH. Informa del formato del encabezado de los paquetes relacionados con AH.
- Algoritmo de encripción. Un conjunto de documentos que describen como varios algoritmos de encripción son usados por ESP.
- Algoritmos de Autenticación.
- Administracion de las Llaves.

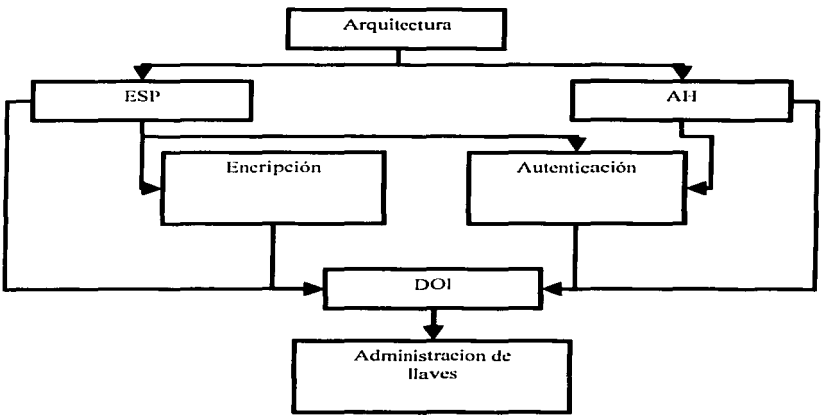


Figura 3.3. Arquitectura en IPSec.

3.2.1 Servicios de IPSec

IPSec proporciona servicios de seguridad en un nivel de red IP habilitando al sistema para seleccionar el protocolo requerido, determina los algoritmos para uso de los servicios. Los algoritmos son dos que proporcionan seguridad: el protocolo de autenticación indicado por el encabezado del protocolo (AH); y una combinación de encripción y autenticación (ESP). Los servicios son los siguientes:

- Control de acceso
- Integridad en conexiones
- Autenticación del transmisor
- Confidencialidad usando encripción

En la tabla 3.1. La cual muestra los servicios que proporcionan los protocolos AH y ESP. Para ESP existen dos casos: con autenticación y no autenticación. Ambos AH y ESP son vehículos para el control de acceso, basados en la distribución de llaves y en la administración del flujo de tráfico[28].

	AH	ESP (no encripción)	ESP (encripción)
Control de acceso	✓	✓	✓
Integridad en conexión	✓		✓
Autenticar al transmisor	✓		✓
Confidencialidad		✓	✓

Tabla 3.1. Servicios en IPSec

[28] Cryptography And Network Security
William Stallings
Prentice may 1999

3.2.2 Asociación de seguridad

Un concepto clave que aparece en ambos mecanismos de autenticación y confidencialidad para IP es la asociación de seguridad (SA). Una asociación es una relación unidirecciónal entre los extremos que envian datos ofreciendo servicios en seguridad. Si es necesario una relación bidirecciónal entre el transmisor y el receptor es necesario tener dos Asociaciones de Seguridad aunque existe una excepción cuando utilizamos el protocolo IKE como veremos posteriormente. Los Servicios de Seguridad son ofrecidos por medio de AH y ESP, pero no ambos.

Los parámetros que identifican una SA son:

- Indice para los Parámetros de Seguridad (SPI): 32 bits asignados a esta Asociacion de Seguridad con significado local. SPI es transportado dentro del encabezado de AH y ESP para indicar al sistema receptor a seleccionar una SA bajo la cual seran procesados los paquetes.
- Dirección IP destino: solo es soportado direcciones unicast dentro de la SA.
- Identificador del Protocolo de Seguridad: indicando si es una SA de AH o de ESP.

La SA es identificada por la dirección IP destino y su SPI[29].

3.2.2.1 *Parámetros de una SA*

Cada instrumentación de IPSec, existe una base de datos para definir a cada SA. Normalmente cada SA se define como sigue:

- Numero de Secuencia: un valor de 32 bits generado para los números de secuencia dentro del encabezado de AH y ESP, requerido en todas las implementaciones.
- Un contador de desborde de secuencia: Una bandera que indique el desbordamiento del Numero de Secuencia para auditar los eventos y prevenir el envío de mas datos, requeridos en todas las implementaciones.
- Información de AH: Algoritmo de autenticación, llaves, tiempo de vida de llaves, valores iniciales de AH (requerido en todas las implementaciones).
- Información de ESP: Algoritmo de encripción y autenticación, llaves, tiempos de vida de llaves, requerido en todas las implementaciones.
- Tiempo de vida de una SA: Un intervalo o un contador para indicar cuando se debe iniciar una nueva SA (requerido en todas las implementaciones).

[29] Big Book of IPSec
Pete Loshin
Morgan Kaufmann
Enero 2000

- Modo del protocolo IPSec: Si es Túnel o Transporte, estos modos son discutidos mas adelante (requerido por todas las implementaciones).
- Máximo tamaño de paquete: Máximo tamaño de paquete que puede ser enviado sin ser fragmentado. (requerido por todas las implementaciones).

3.2.2.2 Selectores de SA

IPSec proporciona una flexibilidad al usuario en la manera en la cual los Servicios de IPSec son aplicados al tráfico de IP. En IPSec se puede indicar y seleccionar el tráfico a ser encriptado por IPSec. Lo que significa que el tráfico de IP especifico se puede relacionar a una SA en particular, llamada Security Policy Database (SPD). En su forma simple, la SPD contienen varias entradas donde cada una define un subconjunto de tráfico de IP apuntando a una especifica SA. En ambientes complejos existen múltiples entradas relacionadas a un simple SA o múltiples SA asociadas a una sola entrada de SPD[30].

Cada SPD esta definida por un conjunto de IP y de valores, llamados Selectores. En efecto, estos selectores son usados para filtrar tráfico mapeado dentro de una particular SA. Este proceso obedece a una secuencia general para cada paquete de IP:

1.- Compara los valores de los campos apropiados en el paquete (el campo del selector) contra el SPD para encontrar una entrada valida, la cual apuntara a cero o algunas SA:
2.- Determina la SA si alguno de estos paquetes y su asociación SPI.
3.- Realizara el procesamiento necesario de IPSec (el proceso de AH o ESP).

Los siguientes selectores determinan una entrada SPD:

- Dirección IP destino: Una unica dirección IP o un rango.
- Dirección IP fuente: Una unica dirección IP o un rango.
- Identificardor de usuario: El ID de un usuario.
- Protocolo de nivel transporte: Obtenido de encabezado de IPv4.
- Protocolo IPSec (AH o ESP o AH/ESP).
- Puertos fuente y destino: Utilizados por TCP o UDP.
- Tipo de Servicio de IPv4: Obtenido del encabezado de IPv4.

[30] Cryptography And Network Security
William Stallings
Prentice may
1999

3.2.3 Modos Túnel y Transporte

Ambos AH y ESP soportan dos modos de uso: Modo Transporte y Túnel. La operación de estos modos tienen las siguientes características:

3.2.3.1 Modo Transporte

Este modo proporciona protección para los niveles superiores. Esto es, que el modo transporte extiende la protección al campo de datos de usuario. Ejemplos incluyen TCP, UDP e ICMP, todos estos operan por encima de IP. Típicamente, el modo transporte es usado para comunicación entre Servidores. Cuando un Servidor corre AH o ESP sobre IPv4 el campo de datos de usuario normalmente va seguido del encabezado de IP.

ESP en modo transporte encripta y opcionalmente autentifica el campo de datos de usuario pero no el encabezado de IP. AH en modo transporte autentifica el campo de datos de usuario y algunos campos del encabezado de IP.

3.2.3.2 Modo Túnel

Este modo proporciona protección completa al paquete de IP. Para lograr esto, después de los campos de AH o ESP son agregados al paquete de IP, el paquete completo mas los campos de seguridad son tratados como el campo de datos de un nuevo paquete de IP. El paquete completo viaja a través del "túnel" de extremo a extremo de la Red. Ningún enrutador en el camino podrá examinar el paquete de entrada. Por que el paquete original fue encapsulado, el nuevo, paquete puede tener una nueva IP fuente y destino, adicionando seguridad. El modo Túnel es usado cuando una o ambas puntas de una SA es una compuerta de seguridad, tal como un Firewall implementado IPSec. Con el modo túnel, un numero de servidores sobre la red detrás del Firewall puede obligarse en una comunicación sin implementar IPSec. Los paquetes no protegidos generados por tales Servidores son pasados a través de redes externas en SA's de modo túnel y con IPSec.

Como ejemplo de cómo pasa un paquete en IPSec sobre un modo túnel. Servidor A genera un paquete con una IP destino del servidor B. Este paquete es enrutado desde el servidor original hacia el Firewall en los limites de la red de A. El firewall filtra todos los paquetes para determinar la necesidad para el procesamiento de IPSec. Si este paquete de A hacia B requiere IPSec, el Firewall realiza el procesamiento de IPSec y encapsula el paquete con un nuevo encabezado. La dirección IP fuente de este paquete seria la del Firewall, y la dirección destino podría ser la de un Firewall de la periferia de la red de B. Este paquete enrutado hacia el Firewall B, donde se elemina el encabezado agregado por el Firewall de A para luego ser entregado el paquete hacia B.

ESP en modo Túnel encripta y opcionalmente autentifica el paquete completo incluyendo el encabezado de IP. AH en modo Túnel autentifica el paquete completo[22].

3.3 Protocolo AH

El protocolo o encabezado AH proporciona integridad y autenticación de los paquetes. La facilidad de integridad asegura que las modificaciones de un paquete en tránsito no es posible. Esta facilidad permite al sistema o al dispositivo el autenticar a usuarios o aplicaciones y filtra el tráfico en consecuencia; también previene de ataques engañosos (ataque spoofing) muy comunes hoy en día. AH también se protege de los ataques de robo de información (ataque Reply). La autenticación consiste de los siguientes campos:

- Indice de Parámetro de Seguridad (32 bits): Identifica a la SA.
- Numero de secuencia (32bits): un contador de ventana.
- Datos de Autenticación (variable): Longitud variable.

Figura 3.4. Encabezado de AH.

[22] Big Book of IPSec
Pete Loshin
Morgan Kaufmann
Enero 2000

3.3.1 Integridad

Los datos autenticados mantiene un valor referido como Valor de Integridad. El Valor de Integridad es un mensaje autentificado o una versión truncada de código producido por una función MAC. La presente especificación dicta que la implementación debe soportar:

HMAC-MD5-96
HMAC-SHA-1-96

Ambos usan algoritmos HMAC, el primero con una Función Hash MD5 y el segundo con una Función Hash SHA. En ambos casos, el completo valor HMAC es calculado pero luego truncado usando los primeros 96 bits, la cual es el default del campo de Datos Autenticados.

El MAC es calculado sobre lo que sigue:

El encabezado de IP que no cambia en tránsito. Los campos que pueden cambiar en transito son aquellos que son impredecibles son configurados a cero para propositos de calculo de ambos fuente y destino.

El campo de Datos Autenticados son puestos a cero para propósitos de calculo de ambos fuente y destino. El protocolo de datos de nivel superior, el cual se asume a ser inmutable en transito(ej, TCP o un paquete interno al Modo Túnel).

Para IPv4, los ejemplos de campos inmutables son la longitud del encabezado de IP y la dirección IP fuente. Un ejemplo de campos mutables pero predecibles es la dirección IP destino. Ejemplos de campos mutables que son configurados antes del calculo del valor Integridad sin el Time to Live y el campo del Checksum. Observando que ambos campos de direcciónes IP fuente y destino son protegidas, previniendo los ataques Spoofing.

3.3.2 Los modos Transporte y Túnel

La figura No 3.5. muestra dos caminos con el servicio de autenticación de IPSec. En un caso, la Autenticación es proporcionada directamente entre Servidores y Clientes, donde estos pueden ser de la misma red o pueden estar en redes externas.

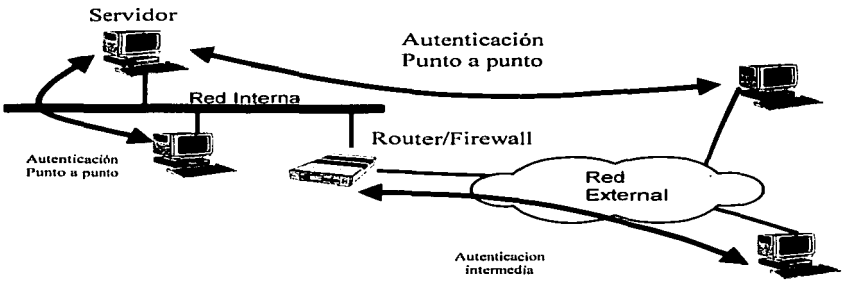


Figura 3.5. Autenticación con IPSec.

A lo largo de las estaciones y de los Servidores compartidos una llave Secreta los protege el proceso de Autenticación. Este caso usa modo transporte de una SA. En el otro caso, una estacion Autenticar al Firewall, ya sea para acceso hacia la red interna o porque el Servidor no solicito soporte de Autenticación. Este seria el caso del modo Túnel. Acontinuacion detallaremos el alcance que AH proporciona para la Autenticación y donde se ubica el encabezado de dichos modos.

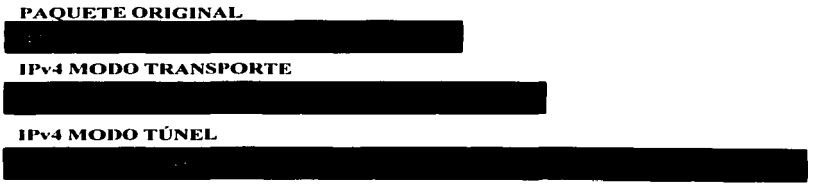


Figura 3.6. Autenticación AH.

Para el caso de datos en TCP, aunque podria ser también una unidad de datos para cualquier protocolo de ICMP o UDP.

Para el modo AH Transporte, el encabezado de AH es insertado después de encabezado original de IP y antes de los datos; esto es mostrado en la primero parte de la figura 3.4.

La autenticación cubre el paquete completo, eliminando los campos mutables del encabezado de IP que son configurados a cero para el calculo de MAC.

Para el modo AH Túnel, el completo paquete de IP es autenticado y el AH es insertado entre el encabezado IP y un nuevo encabezado de IP. El encabezado interno de IP transporta las direcciones fuente y destino finales, mientras que el encabezado externo transporta direcciones diferentes de IP (ej. La dirección del Firewall)
Con el modo túnel, el paquete completo interno es protegido por AH. Para el encabezado del paquete externo es protegido excepto para los campos mutables o predecibles.

3.4 El protocolo ESP

El protocolo ESP proporciona servicios de Confidencialidad, incluyendo la confidencialidad de el contenido del mensaje. Como una opción , ESP puede también proporcionar facilidades de Autenticación.

3.4.1 Formato de ESP

El formato de un paquete ESP contiene lo siguiente:

SPI (32bits): Identifica a la SA.
Numero de Secuencia (32bits): Un contador que lleva el control de la secuencia.
Payload de Datos(variable): Este es un segmento de nivel de transporte para el paquete de IP que es protegido por encripción.
Datos Autenticados(variable): Campo de longitud variable (debe ser entero de 32 bits) que contenga el calculo del valor de Integridad sobre el paquete ESP menos el campo de Datos Autenticados.

3.4.2 Algoritmos de Encripción y Autenticación

El campo de datos son encriptados usando los servicios de ESP. Si el algoritmo usado para encriptar los datos requiere sincronización de datos, tal como un vector de inicio, luego estos datos pueden ser pueden ser transportados. Si se incluye, un IV es usualmente no encriptado, aunque es referido para ser parte del texto codificado.
Las actuales especificaciones dictan que una implementación debe soportar DES en modo CBC, descrito en el capitulo anterior.

Un número de otros algoritmos han sido asignados y podría ser fácilmente empleados para encriptar. Estos son los siguientes: **3DES, RC5, IDEA, CAST** y **Blowfish.**

Estos algoritmos fueron descritos en el capitulo anterior.

Como AH, ESP soporta el uso de MAC con longitud de default de 96 bits. También como AH, debe soportar HMAC-MD5-96 y HMAC-SHA-1-96.

3.4.3 Modos Túnel y Transporte

En la figura 3.7. muestra dos caminos IPSec con el servicio de ESP empleado. Se observa encriptando (autenticando en forma opcional) aplicada entre dos diferentes Servidores.

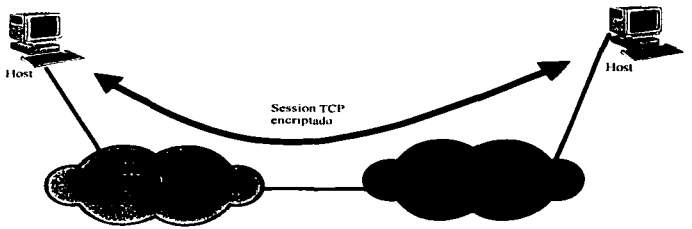


Figura 3.7. Nivel transporte

Se muestra la operación del modo Túnel puede ser usada para configurar una Red Vitual Privada. En este ejemplo, una organización tiene cuatro redes privadas a través de Internet. Los Servidores sobre la red Interna utiliza a Internet para transportar Datos pero no interactúan con los dispositivos de Internet. Ver la figura No 3.8.

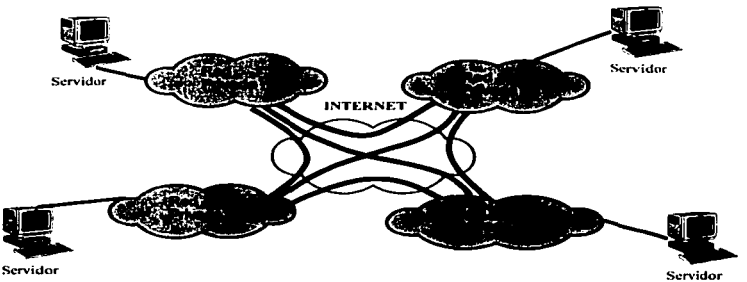


Figura 3.8. Red Virtual en modo Túnel.

Vamos a revizar el alcance de ESP en sus dos modos.

3.4.3.1 ESP en el modo de Transporte.

ESP es usado para encriptar y opcionalmente para autenticar los datos que transporta IP como se observa en la figura 3.9.

Para este modo, el encabezado de ESP es insertado dentro del paquete de IP antes del encabezado del nivel de Transporte y el ESP trailer es colocado después de los datos de IP; si la Autenticación es seleccionada, el campo de ESP de Autenticación de Datos es agregado después del ESP trailer. El completo segmento del nivel de transporte mas el ESP trailer son encriptados. La Autenticación cubre todo el paquete encriptado mas el encabezado de ESP.

El modo de Transporte puede ser sumarizado como sigue:

1.- En el lado del transmisor, el bloque de datos consistente del ESP Trailer mas el segmento son encriptados y el mensaje a encriptar de este bloque es reemplazado con su

mensaje codificado para formar el paquete de salida. La Autenticación es agregada si la opción fue seleccionada.

2.- El paquete es luego enrutado a su destino. Cada enrutador intermedio necesita examinar y procesar el encabezado de IP mas el encabezado no encriptado de las extensiones, pero no necesita examinar el mensaje codificado.

3.- El Nodo receptor examina y procesa el encabezado de IP mas los encabezados de las extensiones de IP. Luego, en base a su SPI dentro del encabezado de ESP, el nodo destino desencripta el resto del paquete para recuperar la información en texto normal.

El Modo de Transporte proporciona confidencialidad para cualquier aplicación que lo use, evitando la necesidad de implementar Confidencialidad en cada aplicación. Este modo de operación es razonablemente eficiente. Una desventaja de este modo es que es posible hacer análisis de tráfico sobre los paquetes transmitidos.

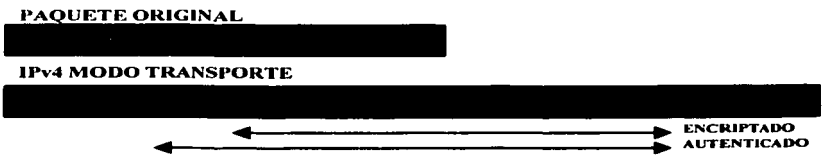


Figura 3.9. Red Virtual en modo transporte.

3.4.3.2 Modo Tunel ESP

Este Modo Túnel ESP es empleado para encriptar el paquete completo de IP, ver figura 3.10. Para este modo, el encabezado de ESP es antepuesto al paquete y luego el ESP Trailer es encriptado. Este método es empleado para prevenir los ataques de análisis de tráfico.

El Modo de Transporte es conveniente para proteger las conexiones entre Servidores que soporten los servicios de ESP, el Modo Túnel es útil en una configuración que incluye el Firewall o enrutador. En este caso, la encripción ocurre solo entre Servidores externos o entre dos equipos Firewalls.

Considerar un caso en el cual un Servidor Externo requiere comunicarse con un Servidor de una Red Interna protegida por un Firewall, en el cual ESP es implementado en el Servidor Externo y en Firewall. Los siguientes pasos ocurren para transferir información:

1.- El Transmisor prepara un paquete interno de IP con un dirección IP destino. Este paquete es antepuesto por un encabezado de ESP; luego el paquete y el ESP Trailer pueden ser encriptados y la Autenticación puede ser agregada. El resultante bloque es encapsulado con un nuevo encabezado IP.

2.- El paquete externo es enrutado al Firewall examinando el encabezado externo de IP pero no necesita examinar el contenido del paquete encriptado.

3.- El Firewall examina y procesa el paquete y luego en base a algún SPI dentro del encabezado de ESP, el nodo destino descripta el resto del paquete para recobrar el paquete interno de IP, para luego ser transmitido al Servidor de la red Interna.

4.- El paquete es enrutado hasta el Servidor final[23].

Figura 3.10. Red Virtual en modo Túnel.

[23] Cryptography And Network Security
William Stallings
Prentice may
1999

3.5 *Administración de llaves (IKE)*

La parte de administración de llaves para IPSec involucra la determinación y distribución de llaves usando el protocolo IKE (Internet Key Exchange) el RFC 2409. La arquitectura de IPSec maneja dos tipos de administración de llaves manual y automático.

El protocolo de IKE provee a IPSec con los siguientes servicios:

- Establecer SA's dinámicamente, sin IKE el operador deberá configurar las SA's manualmente entre todos los puntos remotos.
- Con IKE las llaves tienen tiempo de expiración y la renegociación sera establecida automáticamente. Con esto da mejoras para IPSec limitando la cantidad de tráfico protegido por una llave e incrementando el número de llaves que un atacante tendrá que calcular. Algunos aspectos adicionales son mencionados en el RFC 2405.
- Sin IKE no hay forma de soportar los certificados digitales[33].

Por esto y mas razones IKE es recomendable. IKE agrega seguridad, escalabilidad y simplifica la configuración. Existen varios metodos de autenticación, Llaves compartidas, encripción con RSA y certificados digital con RSA.

- **Llaves compartidas.**- 2 dispositivos son configurados con llaves predeterminadas, estos dispositivos son autenticados si tienenla misma llave. Este metodo no emplea llaves públicas o ceritificados digitales.

- **Encripción con RSA.**- Este metodo emplea llaves públicas pero no usa certificados digitales.

- **Certificado Digital.**- Utilizando certificados digitales provee escalabilidad para redes de gran covertura.

[33] Big Book of IPSec
Pete Loshin
Morgan Kaufmann
Enero 2000

Para que 2 dispositivos se comuniquen con IPSec, ellos primero se autentican usando IKE y luego establecen una SA entre ellos. La SA da seguridad y actúan como control del canal para intercambio y administración de llaves. A diferencia de IPSec SA la cual es unidireccional, en IKE la SA es bidireccional . Solo una SA en IKE es necesaria entre 2 conexiones remotas, ver figura 3.11

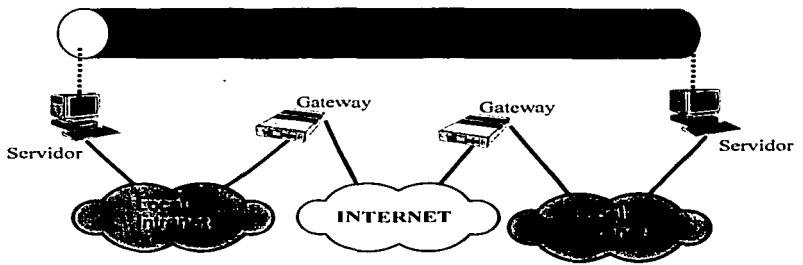


Figura 3.11. SA IKE.

CAPITULO 4
Implementación

4 Implementación

Se analizará los requerimientos de una empresa "X" y disenar una solución integral de con tecnología en Seguridad. En este capitulo describiremos la solución que se propone desde sus aplicaciones con alta prioridad asi como su política de Seguridad, posteriormente llegaremos a su implementación en cada uno de los equipos de comunicaciones conocidos como enrutadores.

4.1 Equipo

La empresa "X" cuenta con aplicaciones de escritorio de FTP y correo electrónico dentro de 2 sitios remotos y en el Corporativo con 2 servidores para cada aplicación. En la parte de comunicaciones cuenta con equipo marca Cisco modelo 3600 en cada nodo, en cada punto existe un enlace hacia Internet y otro puerto hacia la LAN local, por lo que solo se requiere implementar el software para habilitar la plataforma de IPSec la cual proporcionará seguridad al envió de la información entre el corporativo localizado en México y los 2 sitios remotos ubicados en Guadalajara y Monterrey.

4.2 Caracteristicas de red en los Sitios México, Guadalajara y Monterrey

Topología : BUS (LAN)
Medio de transmisión: UTP
Protocolos de Red: TCP/IP, Servidor de FTP, correo electrónico y servidor WEB.
Hardware de red: Tarjeta 3com.
Protocolo de red: eigrp 100

4.3 Topología

La topología actual de la empresa "X" esta comprendida en 3 sitios remotos. Comprende un corporativo y 2 sitios remotos. El corporativo cuenta con una amplia gama de altamente confidencial y esta localizado en la ciudad de México. Los sitios remotos Guadalajara y Monterrey requieren transferir información de aplicaciones tipo FTP y correo electrónico hacia el corporativo, en forma segura a través de Internet.

La distribución física la conforma una topología en estrella con un punto central como el corporativo.

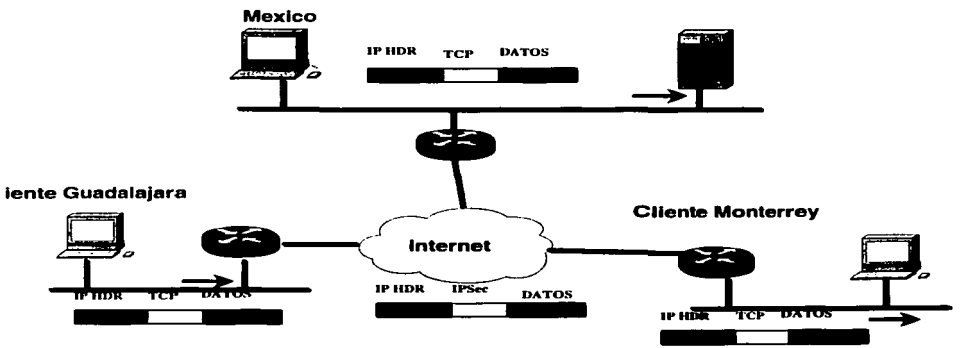


Figura 3.1. IPSec a través de Internet.

4.4 Direccionamiento TCP/IP

Los protocolos utilizados son TCP/IP en todos los equipos servidores y con OSPF como protocolo dinámico de enrutamiento. Debido a que la empresa "X" su premisa es dar seguridad solo al trafico de aplicación no se dará autentificación a los paquetes de enrutamiento eigrp.

En la siguiente tabla se muestra el esquema de direccionamiento:

Dirección	Puerto	Nodo	Ubicación
10.213.55.2	Serial 0	Nodo_Corporativo	Corporativo Mexico
10.16.157.2	Serial 0	Nodo_GDL	Guadalajara
10.16.158.2	Serial 0	Nodo_MTY	Monterrey

4.5 Aplicaciones

Dentro de las aplicaciones hay servidores de FTP y correo, estas aplicaciones ya cuenta con equipo de Autenticación de usuarios, en este caso con un servidor Kerberos, por lo que solo nos enfocaremos en la seguridad a nivel red.

4.6 Política de Seguridad

La empresa X desea implantar la siguiente política de seguridad.

- Utilizar direccionamiento público para cualquiera de los 3 puntos.
- La información de FTP y sesiones Telnet utilizada entre cualquiera de los 3 puntos será encriptada mientras que resto de las aplicaciones se enviaran sin encriptar.

4.7 Desarrollo

La política de Seguridad se implementará con los siguientes comandos:

4.7.1 IKE

IPSec ofrece standares de encripción y autenticación para paquetes unicast. IKE es el protocolo que administra las llaves en IPSec. Aunque IPSec tiene la opción de ser configurado sin IKE, hace más compleja la configuración y su administración, a demás que IKE ofrece a IPSec ser escalable utilizando certificados digitales.

IKE negocia las políticas de IPSec SA's las cuales deben ser idénticas sino la negociación fallará. Estos parámetros deberán ser idénticos: el algoritmo de encripción, autenticación, hash y el grupo Diffie-Hellman. Se tomará el tiempo de vida más corto de cada SA. El comando para realizar lo anterior es:

crypto isakmp policy <priority>

Donde puedes configurar más de una crypto, lo importante es que al menos una política debe ser idéntica al otro extremo. El parámetro de priority es del rango de 1 a 10,000, donde la número 1 es de mayor prioridad.

Parámetro	Valor
Algoritmo de encripción	DES
Algoritmo HASH	SHA-1
Autenticación	RSA
Diffie-Hellman	Grupo 1 (768 bits)
SA tiempo de duración	86400 segundos

4.7.2 IPSec

IPSec debe incorporar:

- Flexibilidad en seleccionar diferentes tipos de tráfico.
- Combinar los servicios de seguridad.

IPSec utiliza filtros donde se define el tipo de tráfico que será aplicada en la política de seguridad. Estas definiciones son por medio del comando ***set transform-set*** que son contenidos dentro de ***crypto maps*** los cuales son aplicados a las interfaces físicas del equipo.

crypto map combined 30 ipsec-isakmp
set peer 10.213.55.2
set transform-set auth-md5
match address 105

crypto isakmp policy 4
hash md5
authentication pre-share
crypto isakmp key iketest address 10.213.55.2

Los enrutadores que se encargan de encriptar y desencriptar trafico, son llamados "***pareja***" y son definidos por un administrador de red. Por ejemplo la aplicación FTP en el Servidor A está haciendo una conexión ***pareja*** hasta la aplicación FTP en el Servidor B. Ahora el comportamiento del tráfico sería, el Servidor A en México enviará trafico hacia el Servidor B en Guadalajara, por lo que cuando el paquete IP sale del Servidor no se encuentra sin encriptar (cleartext), para cuando llega al enrutador A' se evalúa si el paquete es encriptado de acuerdo a que política de Seguridad. Estos filtros de clasificación de tráfico son de especial cuidado, para los protocolos IKE, IPSec y algunos mas utilizan UDP con el puerto número 500 y para IPSec AH y ESP utilizan el número 50 y 51 respectivamente, por lo tanto, se tendrán que evitar filtrar estos puertos en las puertas entrada / salida (Firewall) hacia Internet.

4.7.3 Transform

Durante la negociación de IKE el transmisor ofrece diferentes algoritmos, los llamaremos TRANSFORM. Actualmente dentro de cada ***Transforms*** hay los siguientes algoritmos:

- HMAC- MD5
- HMAC- SHA
- DES-CBC con Explicit IV
- 3DES-CBC con Explicit IV

La sintaxis para declararla es de la siguiente forma:

crypto ipsec transform-set name trans1 [trans2]

ah-md5-hmac AH-HMAC-MD5
ah-sha-hmac AH-HMAC-SHA
esp-3des ESP con DES (168 bits)
esp-des ESP con DES (56 bits)
esp-md5-hmac ESP con HMAC-MD5 auth
esp-sha-hmac ESP con HMAC-SHA auth

Cada ***Transform*** puede ser especificada para AH o ESP o ambos. Algunos ejemplos se listan.

Para autenticar solo con MD5 hash:

crypto ipsec transform-set auth-md5 ah-md5-hmac

Para autenticar solo con SHA hash:

crypto ipsec transform-set auth-sha ah-sha-hmac

Para confidencialidad:

crypto ipsec transform-set encrypt esp-des

Para confidencialidad y autenticar con MD5:

crypto ipsec transform-set encrypt-md5 esp-des esp-md5-hmac

Hasta 5 Transform pueden ser especificadas, en prioridad.secuencial, pero solo una será elegida por cada sesión de IPSec.

4.7.4 Modos

Los modos aplican a todos las ***Transforms***. No se podrá aplicar AH en modo transporte mientras que ESP en modo túnel dentro de la misma ***Transform***. Si el modo túnel es especificado (default) entonces todos los paquetes IP estarán en modo túnel. El enrutador negociara estos parámetros.

4.7.5 Mapas Crypto

Después de que los filtros y la política han sido definidos es necesario construir un ***mapa crypto*** para vincular todos los elementos. El ***mapa crypto*** contiene el filtro para trafico que será aplicada a la política de seguridad y los algoritmos empleados. Cuando se define los crypto maps hay 2 modos:

- ipsec-manual—IPSec usando un método manual (no usa IKE)
- ipsec-isakmp—IPSec usando IKE

Por ejemplo:

crypto map Peer-remoto 10 ipsec-isakmp

Después se tendrá que aplicar a la interface fisica como:

interface Serial0
ip address 192.168.1.1
crypto map Peer-remoto

Con esto se aplica el crypto map a una interface tipo WAN serial 0 con dirección IP 192.168.1.1

4.7.6 PEER's (pareja)

En IPSec se identifica a un extremo como PEER donde se define la dirección IP que va a formar el la relación de pareja.

set peer host_name_or_IP_address

4.7.7 Match Address

Este comando identifica a que filtro se relaciona.

match address ACL_list_identifier

4.7.8 Time out SA.

Cada SA creada tendrá un tiempo de vida, con ayuda de este comando se puede variar su tamaño, para el criptoanálisis entre mayor tiempo se utilice la misma llave tendrá mayor oportunidad de encontrar la llave. El comando es:

ipsec session-key 60–86400 segundos

4.8 Configuración

La autentificación se realizará empleando IKE con el método de llaves compartidas. Los 3 equipos son configurados manualmente con las mismas llaves. El diagrama final se muestra en la figura No 3.2

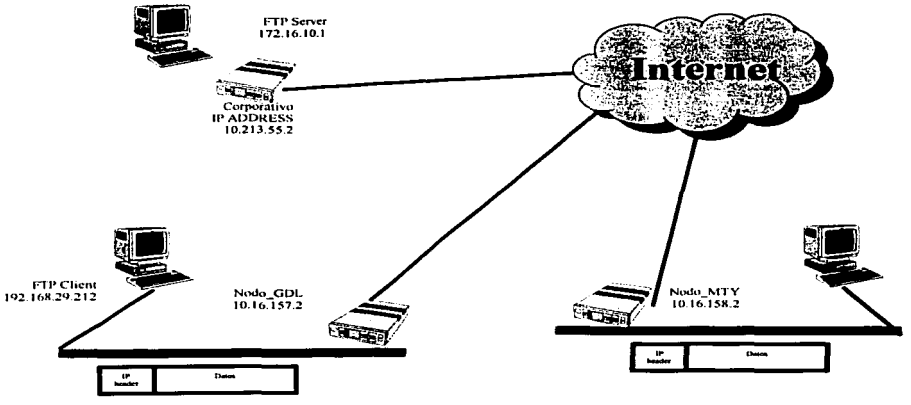


Figura 3.2. Diagrama de conexión.

Equipo nodo_GDL:

```
!
ip multicast rpf-check-interval 0
!
crypto isakmp policy 4
hash md5
authentication pre-share
crypto isakmp key iketest address 10.213.55.2
!
!
crypto ipsec transform-set auth-sha ah-sha-hmac
crypto ipsec transform-set encrypt-des esp-des
crypto ipsec transform-set auth-md5 ah-md5-hmac
!
crypto map mixto 30 ipsec-isakmp
set peer 10.213.55.2
set transform-set auth-md5
match address 105
crypto map mixto 40 ipsec-isakmp
set peer 10.213.55.2
set transform-set encrypt-des
match address 102
!
!
!
interface Ethernet0
ip address 192.168.29.1 255.255.255.0
!
interface loopback0
ip address 192.168.45.1 255.255.255.0
!
interface Serial0
ip address 10.16.157.2 255.255.255.0
crypto map mixto
!
!
router eigrp 100
network 10.0.0.0
network 192.168.29.0
network 192.168.45.0
!
```

```
no ip classless
access-list 102 permit tcp 192.168.0.0 0.0.255.255 172.16.24.0 0.0.0.255 eq telnet
access-list 105 permit tcp host 192.168.29.212 host 172.16.10.19 eq ftp
!
line con 0
line vty 0 4
password cisco
login
!
end
```

Equipo nodo_MTY:

```
!
ip multicast rpf-check-interval 0
!
crypto isakmp policy 4
hash md5
authentication pre-share
crypto isakmp key iketest address 10.213.55.2
!
!
crypto ipsec transform-set auth-sha ah-sha-hmac
crypto ipsec transform-set encrypt-des esp-des
crypto ipsec transform-set auth-md5 ah-md5-hmac
!
crypto map mixto 30 ipsec-isakmp
set peer 10.213.55.2
set transform-set auth-md5
match address 105
crypto map mixto 40 ipsec-isakmp
set peer 10.213.55.2
set transform-set encrypt-des
match address 102
!
!
!
interface Ethernet0
ip address 192.168.30.1 255.255.255.0
!
interface loopback0
ip address 192.168.46.1 255.255.255.0
!
interface Serial0
ip address 10.16.158.2 255.255.255.0
crypto map mixto
!
!
router eigrp 100
network 10.0.0.0
network 192.168.30.0
network 192.168.46.0
!

no ip classless
```

```
access-list 102 permit tcp 192.168.0.0 0.0.255.255 172.16.24.0 0.0.0.255 eq telnet
access-list 105 permit tcp host 192.168.29.213 host 172.16.10.19 eq ftp
!
line con 0
line vty 0 4
password cisco
login
!
end
```

Equipo **Nodo_Corporativo:**

```
!
ip multicast rpf-check-interval 0
!
crypto isakmp policy 4
hash md5
authentication pre-share
crypto isakmp key iketest address 10.16.157.2

crypto isakmp policy 5
hash md5
authentication pre-share
crypto isakmp key iketest address 10.16.158.2

!
!
crypto ipsec transform-set auth-sha ah-sha-hmac
crypto ipsec transform-set auth-md5 ah-md5-hmac
crypto ipsec transform-set encrypt-des esp-des
!
!
crypto map mixto 7 ipsec-isakmp
set peer 10.16.157.2
set transform-set encrypt-des
match address 103
crypto map mixto 8 ipsec-isakmp
set peer 10.16.157.2
set transform-set auth-md5
match address 105
crypto map mixto 9 ipsec-isakmp
set peer 10.16.158.2
set transform-set encrypt-des
match address 103
crypto map mixto 10 ipsec-isakmp
set peer 10.16.158.2
set transform-set auth-md5
match address 106

!
interface Ethernet0
ip address 172.16.10.1 255.255.255.0
!
interface loopback0
```

```
ip address 172.16.24.1 255.255.255.0
!
interface Serial0
ip address 10.213.55.2 255.255.255.0
crypto map mixto
!
interface BRI0
no ip address
encapsulation ppp
no ip route-cache
no ip mroute-cache
shutdown
!
router eigrp 100
network 10.0.0.0
network 172.16.0.0
!
no ip classless
access-list 103 permit tcp 172.16.0.0 0.0.255.255 eq telnet 192.168.0.0 0.0.255.255
access-list 105 permit tcp host 172.16.10.19 eq ftp host 192.168.29.212
access-list 106 permit tcp host 172.16.10.19 eq ftp host 192.168.29.213
!
line con 0
exec-timeout 0 0
line vty 0 4
password cisco
login
!
end
```

En esta sección describiremos paso a paso la configuración de una SA utilizando IKE, cuando una máquina empieza a realizar el FTP del nodo_GDL hacia el Nodo_Corporativo

Monitoreo de inicio de información para el equipo **nodo_GDL:**

ISAKMP (113): beginning **Main Mode** exchange
ISAKMP (113): Checking ISAKMP transform 1
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 1
ISAKMP: auth pre-share
ISAKMP (113): atts are acceptable. Next payload is 0
ISAKMP (113): **SA is doing pre-shared key authentication**
ISAKMP (113): SKEYID state generated
ISAKMP (113): SA has been authenticated
ISAKMP (113): beginning **Quick Mode exchange**, M-ID of 759865900
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): **getting spi 275192711 for SA from 10.213.55.2 to 10.16.157.2**
ISAKMP (113): Checking IPSec proposal 1
ISAKMP: transform 1, **AH_MD5_HMAC**
ISAKMP: attributes in transform:
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 3600
ISAKMP: SA life type in kilobytes
ISAKMP (113): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(kei) dest= 10.213.55.2, src= 10.16.157.2,
dest_proxy= 172.16.10.19/255.255.255.255/6/21,
src_proxy= 192.168.29.212/255.255.255.255/6/0,
protocol= 2, transform= 2, hmac_alg= 0,
lifedur= 0x0s and 0x0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (113): Creating IPSec SAs
inbound SA from 10.213.55.2 to 10.16.157.2 (proxy 172.16.10.19 to 192.168.29.212)
has **spi 275192711** and **conn_id 114** and flags 4
lifetime of 3600 seconds
lifetime of 4608000 kilobytes
outbound SA from 10.16.157.2 to 10.213.55.2 (proxy 192.168.29.212 to 172.16.10.19)
has **spi 197333476** and **conn_id 115** and flags 4
lifetime of 3600 seconds
lifetime of 4608000 kilobytes
IPSEC(key_engine): got a queue event...

```
IPSEC(initialize_sas): processing an sa request of size 148
IPSEC(initialize_sas): ,
(kei) dest= 10.16.157.2, src= 10.213.55.2,
dest_proxy= 192.168.29.212/255.255.255.255/6/0,
src_proxy= 172.16.10.19/255.255.255.255/6/21,
protocol= 2, transform= 2, hmac_alg= 0,
lifedur= 0xE10s and 0x465000kb,
spi= 0x10671B87(275192711), conn_id= 114, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(kei) src= 10.16.157.2, dest= 10.213.55.2,
src_proxy= 192.168.29.212/255.255.255.255/6/0,
dest_proxy= 172.16.10.19/255.255.255.255/6/21,
protocol= 2, transform= 2, hmac_alg= 0,
lifedur= 0xE10s and 0x465000kb,
spi= 0xBC311E4(197333476), conn_id= 115, keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
(sa) sa_dest= 10.16.157.2, sa_prot= 51,
sa_spi= 0x10671B87(275192711),
sa_trans= ah-md5-hmac , sa_conn_id= 114,
IPSEC(create_sa): sa created,
(sa) sa_dest= 10.213.55.2, sa_prot= 51,
sa_spi= 0xBC311E4(197333476),
sa_trans= ah-md5-hmac , sa_conn_id= 115,
```

Verificar la nueva SA en la base de datos del **nodo_GDL**:

nodo_GDL #sh crypto ipsec sa
interface: Serial0
Crypto map tag: mixto, local addr. 10.16.157.2
local ident (addr/mask/prot/port): (192.168.29.212/255.255.255.255/6/0)
remote ident (addr/mask/prot/port): (172.16.10.19/255.255.255.255/6/21)
current_peer: 10.213.55.2
PERMIT, flags={origin_is_acl,ident_is_ipsec,}
#pkts encaps: **17**, #pkts encrypt: 0, #pkts digest **17**
#pkts decaps: **15**, #pkts decrypt: 0, #pkts verify **15**
#send errors 0, #recv errors **0**
local crypto endpt.: 10.16.157.2, remote crypto endpt.: 10.213.55.2
path mtu 1500, media mtu 1500
current outbound spi: BC311E4
inbound esp sas:
inbound ah sas:
spi: 0x10671B87(**275192711**)
transform: **ah-md5-hmac** ,
in use settings ={**Tunnel**, }
slot: 0, **conn id: 114, crypto map: mixto**
sa timing: remaining key lifetime (k/sec): (413694/3394)
replay detection support: Y
outbound esp sas:
outbound ah sas:
spi: 0xBC311E4(**197333476**)
transform: **ah-md5-hmac** ,
in use settings ={**Tunnel**, }
slot: 0, **conn id: 115, crypto map: mixto**
sa timing: remaining key lifetime (k/sec): (413694/3394)
replay detection support: Y
local ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/6/0)
remote ident (addr/mask/prot/port): (172.16.24.0/255.255.255.0/6/23)
current_peer: 10.213.55.2

Verificación el estado de conexión de la SA[34]:

```
nodo_GDL #sh crypto isakmp sa
        dst             src             state          conn-id      slot
     10.213.55.2     10.16.157.2     QM_IDLE          113          0
```

[34] Designing Network Security
Merike Kaeo
Cisco System
1999

5 Conclusión

Esta tesis sobre "Seguridad con IPSec" proporciona información fácilmente entendible, de la teoría a la practica, pensando siempre en los temas de mayor interés. Concluyendo en varios puntos.

Se explico como IPSec opera en el nivel de red IP dando seguridad en todas las aplicaciones de nivel superior entre dos sitios remotos, como por ejemplo: Correo Electrónico, WEB (HTTP), Aplicaciones cliente-servidor, base de datos, entre otros, . Los usuarios remotos tienen acceso seguro a todos los recursos del corporativo como si estuvieran físicamente conectados a la red local, empleando IPSec para brindar seguridad a través de Internet, mientras que los servicios o aplicaciones que este caso fueron File Transfer Protocol y una emulación de terminal (Telnet) dentro de los servidores, no fueron modificados debido a que el software de IPSec se encontraba sobre los enrutadores brindando flexibilidad, independencia y modularidad, concluyendo que IPSec cumple con estas características.

En cuanto a los servicios que ofrece IPSec para confidencialidad, integridad y Control de Acceso cubre estos requerimientos. En confidencialidad soporta 56-bit DES y 112 – 168 bit con triple DES. En el control de acceso utiliza el protocolo AH o ESP para crear el canal de conexión.

Al utilizar IKE hay flexibilidad de aceptar políticas de seguridad a través del concepto de Asociaciones de Seguridad ya que al momento de realizarse la conexión se lleva a cabo la negociación de estos parámetros en forma automática. El protocolo IKE resuelve los problemas de escalabilidad automatizando las sesiones SA's y simplificando la configuración debido a que el mantenimiento de las sesiones es mas transparente, el intercambio de llaves para nuevas sesiones. En conclusión, se recomienda utilizar IKE para cumplir con flexibilidad y escalabilidad.

Existen varias limitaciones de IPSec dentro del funcionamiento de TCP/IP. La fragmentación se tendrá que realizar después de aplicar IPSec, otra forma es definiendo el PMTU para evitar la fragmentación eliminando la latencia y el bajo rendimiento por parte del receptor. En cuanto a la clase de paquetes hasta el momento soportado por IPSec son paquetes unicast. También se concluye que IPSec no entrega funciones de QoS/CoS en los servicios de red.

Un punto malo en IPSec es la compleja gestión del mismo, requiere de una configuración compleja, parámetros, políticas de seguridad para crear el canal de comunicación. Lo podemos observar en la gran cantidad de comandos necesarios para crear el canal de comunicación en tan solo 2 puntos fueron necesarios entre 10 a 15 lineas de comandos.

Se concluye que se cubrió los conceptos básicos de seguridad y de criptografía más importantes, necesarios para comprender e implementar cualquier seguridad de datos en la red con el protocolo IPSec. Sabiendo que IPSec es una arquitectura que utiliza tecnologías para asegurar que el tráfico de IPSec será seguro a través de un medio público. El más popular uso de IPSec es a través de Internet pero puede ser empleado en cualquier tipo de conexión entre 2 puntos remotos o locales.

Finalmente, se creo un diseño conceptual de una red "X", donde se emplean los conceptos analizados en capitulos anteriores para emplearlos en forma práctica, a partir de una política de seguridad de la red "X" se cubren las premisas y por lo tanto se desarrollo la configuración básica mostrada en la sección 3.8. Por otra parte, al utilizar un protocolo dentro de los estándares como fue el caso de IPSec, podemos indicar que habrá total interoperabilidad al momento de agregar quizás algún nodo mas dentro de la red "X" sin ser necesariamente equipo marca Cisco.

Bibliografía

Networking Standars
William Stallings
Addison-Wesley
1994

Intenetworking with TCP/IP
Volume I Principles, Protocols, and Architecture
Second edition
Douglas E. Comer
Prentice Hall
Marzo 1991

Big Book of IPSec
Pete Loshin
Morgan Kaufmann
Enero 2000

Designing Network Security
Merike Kaeo
Cisco System
1999

Enhanced IP Services
Donald C Lee
Cisco System
1999

Cryptography And Network Security
William Stallings
Prentice may
1999

N. Derek Arnold
UNIX Security a practical Tutorial
McGrawHill 1993

Lynch, Daniel C. and Rose, Marshall T
Internet System Handbook
Addison Wesley Publishing Company, INC. , 1993

Glosario

Ack Abreviatura de acknowledgment (acuse de recibo). Normalmente se envían ACKs de un dispositivo a otro de la red para indicar que ocurrió algún suceso

Address mask Carátula o máscara de la dirección.

Adyacencia Relación formada entre enrutadores cercanos seleccionados y nodos terminales con el propósito de intercambiar información de enrutamiento.

Algoritmo Reglas o procesos bien definidos para alcanzar la solución de un problema.

API Application Programming Interface: Interface para programas de aplicacion. Especificación de convenciones de llamadas a funciones para definir la interface con un servicio.

ARPANET Red pionera de conmutación de paquetes (packet switching) desarrollada al inicio de los años 70 por la empresa BBN y financiada por la agencia ARPA (luego DARPA

ASCII American Standard Code for Information Interchange: Código estándar nortamericano para intercambio de información. Código de ocho bits para representar caracteres que emplea siete bits más paridad.

AUI Attachment Unit Interface: Interface de unidad de vinculación. Cable IEEE 802.3 que conecta la unidad de acceso al medio (MAU: Media Access Unit al dispositivo en red. El término AUI también se puede usar para referirse al conector del panel trasero principal al que se puede fijar el cable AUI.

Autenticación proceso para verificar la identidad del transmisor

Block cipher Algoritmo de encripción simétrica

byte Término genérico que se refiere a una serie de digitos binarios consecutivos con los que se trabaja como si fueran una unidad; un ejemplo son los bytes de 8 bits.

Cable coaxial Cable consistente en un conductor cilindrico externo hueco que cubre a un alambre conductor único. Suelen emplearse dos tipos de cable coaxial para las redes locales: cable de 50 Ohms, para señales digitales, y cable de 75 Ohms, para señales analógicas y para señales digitales de alta velocidad.

CCITT Comité Consultivo Internacional de Telegrafía y Telefonía (siglas en francés). Organización internacional que desarrolla estándare de comunicaciones, como la recomendación X.25 .

checksum Suma de control. Método para verificar la integridad de los datos transmitidos. Es un número entero calculado a partir de una secuencia de octetos por medio de una serie de operaciones aritméticas. El valor se recalcula en el lado del receptor y se compara para verificarlo.

Cipher Algoritmo para encriptar y desencriptar por medio de una llave secreta

Ciphertext La información de salida de un algoritmo de encripcion

Clase de servicio En forma general se refiere a cómo manejar un paquete. El tipo de servicio (TOS) IP es una clase de servicio. La clase de servicio es la designación de las características de control de trayectoria de la red, incluyendo la seguridad de la trayectoria, el ancho de banda y las prioridades de transmisión que se aplican a alguna sesión en particular. En telefonía existen varias clases de servicio para los abonados dependiendo del servicio requerido.

Cliente Nodo o programa de software que requiere servicios de un servidor.

Connectionless Sin conexiones. Término empleado para describir transferencias de datos sin la existencia de un circuito virtual.

connection-oriented Por conexión.Término empleado para describir transferencias de datos posteriores al establecimiento de un circuito virtual.

Dirección Estructura de datos empleada para identificar una entidad única, como algún proceso o la localización de una red.

DoD Department o defense: Departamento (o ministerio) de la Defensa de los Estados Unidos. Organización de gobierno responsable de la defensa del país. El DoD frecuentemente ha financiado desarrollos de protocolos de comunicaciones.

Encripción La conversión del Plaintext basado en una tabla de conversión

Ethernet Especificación de red LAN de banda base inventada por la corporación Xerox y desarrollada en forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet operan a 10 megabits por segundo utilizando CSMAICI) sobre cable coaxial. Es similar a una serie de estándares producidos por IEEE y conocidos como IEEE 802.3.

ICMP Protocolo Internet de control de mensajes. Protocolo de la capa de red que permite que los paquetes de mensajes reporten errores e información relevante al procesamiento de paquetes IP. Está documentado en RFC 792.

IEEE Institute of Electrical and Electronic Engineers: Instituto de ingenieros eléctricos y electrónicos. Organización profesional que define estándares de redes. Los estándares LAN de IEEE son los predominantes en la actualidad, e incluyen protocolos similares o virtualmente equivalentes a Ethernet y Token Ring

IEEE 802.2 Protocolo LAN de IEEE que especifica la implantación de la subcapa de control de enlace lógico de la capa de enlace. Se encarga del manejo de errores, creación de marcos y flujo de control; es interface de servicio con la capa 3. Se emplea en redes LAN tales como IEEE 802.3 e IEEE 802.5

IEEE 802.3 Protocolo LAN de IEEE que especifica la implantación de la capa física y de la subcapa MAC de la capa de enlace. Utiliza accesos CSMA/CD en varias velocidades usando varios medios físicos. Una variante física de IEEE 802.3 (10BASE5) es muy similar a Ethernet.

IEEE 802.4 Protocolo LAN de IEEE que especifica la implantación de la capa física y de la subcapa MAC de la capa de enlace. Utiliza acceso token passing sobre una topología de bus.

IEEE 802.5 Protocolo LAN de IEEE que especifica la implantación de la capa física y de la subcapa MAC de la capa de enlace. Utiliza acceso token passing a 4 ó 16 Mbps sobre cable de par trenzado blindado y es muy similar a Token Ring de IBM.

IEEE 802.6 Especificación IEEE de red de área metropolitana (Metropolitan Area Network: MAN) basada en tecnología DQDB.

IETF Internet Engineering Task Force: Fuerza de trabajo de ingeniería Internet. Equipo de trabajo IAB que consiste en más de 40 grupos responsables de asuntos ingenieriles Internet solubles a corto plazo.

Interface Conexión entre dos sistemas o dispositivos. En la terminología de enrutadores, es una conexión de la red. También se refiere a la frontera entre capas adyacentes del modelo OSI. En telefonía, es una frontera compartida que está definida por características de interconexión física comunes, características de la señal y significados de las señales intercambiadas.

Internet Término empleado para referirse al sistema de interconexión de redes más grande del mundo, que conecta miles de redes en todo el planeta, y que desarrolló una "cultura" basada en simplicidad, investigación y estandarización fundamentada en el uso real. Buena parte de la tecnología de punta en redes vino de esta comunidad. Internet evolucionó a partir de ARPANET.

Internet address Dirección Internet. También llamada "dirección IP", es una dirección de 32 bits asignada a máquinas anfitrionas que emplean puntos (formato decimal con punto), formados por la sección de la red, una sección opcional de subred y una sección del anfitrión.

internetwork Redes interconectadas. Conjunto de redes interconectadas por enrutadores y que en forma genérica funciona como una sola. A veces se le llama internet, lo cual no debe confundirse con la palabra Internet.

internetworking Interconexión de redes. Término genérico usado para referirse a la industria que surgió alrededor del problema de conectar redes. El término se puede referir tanto a productos como a procedimientos y tecnologías.

interoperability Interoperabilidad. Capacidad para comunicar equipos de computación de diversos fabricantes mediante una red.

Intruso Un individuo que intenta ganar un acceso no autorizado

Llave Una cadena de caracteres alfanumericos usado como identificador

Llave Privada Llaves usadas dentro de un sistema simétrico

Llave Pública Llaves utilizadas dentro de un sistema asimétrica

Llave secreta Es la llave usada en la encripcion simétrica, ambas entidades deben compartir la llave

Plaintext La información de entrada o salida de un algoritmo de encripcion o desencripcion

network Red. Conjunto de computadoras y otros dispositivos que son capaces de comunicarse entre sí empleando un medio reticular.

network address Dirección de la red. También llamada protocolo de la red (network protocol), es una dirección de la capa de red (network layer) que se refiere a un dispositivo lógico, no físico, de la red.

network administrator Administrador de la red. Persona que ayuda a mantener la red.network analyzer Analizador de la red. Dispositivo de hardware/ software que ofrece algunas características de solución de problemas de la red, incluidos decodificadores de paquetes de protocolos específicos, pruebas de errores preprogramadas, filtrado y transmisión de paquetes.

OSI Reference Model Modelo de referencia OSI. Modelo de arquitectura de redes desarrollado por ISO y CCITT. Consiste en siete capas, cada una de las cuales especifica funciones particulares de la red, tales como direccionamiento, control de flujo, control de errores, encapsulamiento, transferencia confiable de mensajes y muchas otras. La capa más alta (application layer: capa de aplicación) es la más cercana al usuario. La capa más baja (physical layer: capa física) es la más cercana a la tecnología del medio físico. El modelo de referencia OSI es universalmente usado como método de enseñar y entender la funcionalidad de las redes.

ping Aviso de paquete Internet. Se refiere al mensaje de eco ICMP y a su contestación. Suele usarse para probar el grado de alcance de un dispositivo de la red.

TCP/IP Transmission Control Protoco/Internet Protocol: Protocolo de control de transmisiones/Protocolo Internet. Los dos protocolos Internet mas conocidos, que erróneamente suelen confundirse con uno solo. TCP corresponde a la capa 4 (capa de transporte) del modelo de referencia OSI y ofrece transmisión confiable de datos. IP corresponde a la capa 3 (capa de red) del modelo de referencia OSI, y ofrece servicios de datagramas sin conexión. TCP/IP fue desarrollado por el Departamento de la Defensa de los Estados Unidos en los años 70 como apoyo a la construcción de interconexión de redes a escala mundial.

Topología de bus Arquitectura LAN lineal en la cual las transmisiones de las estaciones de la red se propagan a lo largo de todo el medio de comunicación y son recibidas por todas las demás estaciones.