C A P Í T U L O VIII

VERIFICACIÓN DE LA HIPÓTESIS, CONCLUSIONES Y RECOMENDACIONES

8.1 Verificación de la Hipótesis

8.2 Conclusiones

8.3 Recomendaciones

8.1 VERIFICACIÓN DE LA HIPÓTESIS

HIPÓTESIS:

El estudio y evaluación de los Protocolos Criptográficos y los mecanismos de encriptación permitirá desarrollar sistemas seguros y eficientes para el intercambio de información a través de canales inseguros.

VERIFICACIÓN:

El estudio, análisis y evaluación crítico, profundo y detallado de los diferentes algoritmos de encriptación de información, utilizados actualmente en nuestros sistemas de información tanto para la confidencialidad, no repudio, autentificación de mensajes, firmas digitales, certificación de claves, etc. nos ha permitido conocer y valorar sus diferentes bondades (ventajas) y en especial todas y cada una de sus debilidades (desventajas), que son un aspecto muy importante a tomar en cuenta en el momento de seleccionarlos para implementar sistemas seguros y eficientes, capaces de adaptarse a las necesidades de un determinado servicio o proceso en particular. Tomando en cuenta algunos criterios técnicos de evaluación tales como: la complejidad del algoritmo criptográfico, tamaño de clave utilizado, recursos de máquina requeridos, tiempos de respuesta, niveles de seguridad proporcionados; especialmente en aquellos casos en donde el tratamiento y manipulación de la información es de vital importancia para las entidades sean éstas del sector público o privado.

La mala selección e implementación de un determinado algoritmo criptográfico destinado a proporcionar la seguridad requerida en un determinado servicio o actividad, puede incurrir en costos innecesarios para la

empresa o institución, debido a la sobrecarga y consumo innecesario de recursos de máquina, ancho de banda, etc. Por lo que el servicio solicitado por un determinado proceso o cliente será deficiente, con tiempos de respuestas bastante pobres, lo que significa ser un punto a favor para la competencia de la empresa.

8.2 CONCLUSIONES

1. La explotación comercial de Internet exige disponer de sistemas de comunicación seguros, capaces de adaptarse a las necesidades de los nuevos servicios, como la compra electrónica o la banca a distancia.

2. La Internet constituye un canal de comunicaciones inseguro, debido a que la información que circula a través de esta amplia red es fácilmente accesible en cualquier punto intermedio por un posible atacante. En cualquiera de ellos es posible leer el contenido de los paquetes, destruirlo e incluso modificarlo, posibilitando todo tipo de ataques contra la confidencialidad y la integridad de sus datos.

3. La información es uno de los activos más importantes de las entidades, y de modo especial en algunos sectores de actividad. Es indudable que cada día las entidades dependen en mayor medida de la información y de la tecnología.

4. Los problemas de seguridad de las redes pueden dividirse en términos generales en cuatro áreas interrelacionadas: secreto, validación de identificación, no repudio y control de integridad.

5. Hay dos tipos básicos de Criptosistemas: los simétricos (también conocidos como convencionales o de clave secreta) y los asimétricos (de clave pública).

6. *Los cifrados simétricos* requieren que tanto el emisor como el receptor tengan la misma clave. Esta clave es usada por el emisor para cifrar los datos, y de nuevo por el receptor para descifrar los datos. Entre los algoritmos simétricos más utilizados tenemos: DES (Data Encryption Standard) y el IDEA (International Data Encryption Algorithm).

7. *Los cifrados asimétricos* son mucho más flexibles desde el punto de vista de la administración de claves. Cada usuario tiene un par de claves: una clave pública y una clave privada. Los mensajes cifrados con una clave pública pueden ser descifrados solamente por la clave privada. La clave pública puede ser ampliamente diseminada, mientras que la clave privada se mantiene en secreto. Entre los algoritmos asimétricos más utilizados tenemos: RSA *(Rivest, Shamir, Adleman)*, El Gamal, Criptosistemas basados en Curvas Elípticas CCE, Criptosistemas basados en Logaritmos Discretos.

8. La principal ventaja que ofrecen los Criptosistemas basados en Curvas Elípticas (CCE) en comparación con **RSA**, es la longitud de la clave secreta. Se puede mostrar que mientras en **RSA** se tiene que usar una clave de 1024 bits para ofrecer una considerable seguridad, los **CCE** solo usan 163 bits para ofrecer la misma seguridad.

9. Los **CCE** son idóneos para ser implementados en donde el poder de cómputo y el espacio del circuito sea reducido, donde sea requerida una

alta velocidad de procesamiento o grandes volúmenes de transacciones, donde el espacio de almacenamiento, la memoria o el ancho de banda sea limitado. Lo que permite su uso en smart cards, teléfonos celulares, Fax, PCs, etc. [WWW 004]

10. Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos se recomiendan claves de al menos 1024 bits. En la práctica los métodos asimétricos se emplean únicamente para codificar la clave de sesión de cada mensaje.

11. El *criptoanálisis* es la actividad que se encarga de estudiar las debilidades de un criptosistema y su objetivo es el de encontrar soluciones fáciles al reto implantado en el criptosistema. Consiste en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la llave, o bien obteniendo a partir de uno o más criptogramas la clave que ha sido empleada en su codificación. Un par de métodos de criptoanálisis que han dado interesantes resultados son *el criptoanálisis diferencial y el criptoanálisis lineal.*

12. La validación de identificación *(autentificación)* se encarga del asunto de comprobar si realmente nos estamos comunicando con otro proceso específico, es decir, el proceso *A* está seguro de que está 'hablando' con el proceso *B*, y *B* también está seguro de que está 'hablando' con *A* [LIB 001].

13. Kerberos es un Protocolo de Validación de Identificación usado en muchos sistemas reales, tales como Unix, Linux y Windows 2000. Se podría decir que como servicio de autentificación, cuida las puertas de la red, impidiendo el ingreso a personas indeseadas. Este protocolo usa fuertemente la criptografía simétrica, por tanto un cliente puede demostrar su identidad a un servidor (y viceversa) a través de una conexión de red insegura.

14. Las técnicas de encriptación protegen de las agresiones pasivas, es decir, de las escuchas, pero no protege de las agresiones activas como la falsificación de los datos. La protección contra estas agresiones activas se conoce como autentificación de mensajes y los llevan a cabo los algoritmos de hashing. Los dos aspectos importantes son verificar que el contenido del mensaje no haya sido alterado durante el transcurso y que el origen del mensaje es auténtico. Se ha propuesto una variedad de funciones hash. Las más sobresalientes y de mayor uso son: El MD5 (Message Digest 5) y el SHA (Secure Hash Algorithm).

15. Las firmas digitales son un reemplazo a las firmas manuscritas con tinta y papel, por lo tanto, la firma digital tiene el mismo valor legal que una firma holográfica tradicional (en los países que poseen una ley de firma digital). Básicamente lo que pretende es *"firmar"* el mensaje que se va a enviar a otra parte de modo que:
    1. El receptor pueda verificar la identidad proclamada del transmisor.
    2. El transmisor no pueda repudiar después el contenido del mensaje.
    3. El receptor no haya podido confeccionar el mensaje, él mismo.

Las firmas digitales son generadas utilizando un algoritmo de clave pública. Cualquiera puede verificar la firma de un usuario empleando la llave pública de ese usuario. La generación de la firma sólo puede realizarse por el poseedor de la llave privada del usuario. El DSA (Digital Signature Algorithm) proporciona la capacidad para generar y verificar las firmas digitales.

16. La identificación por medio de Sistemas Biométricos es una de las tecnologías más prometedoras e inquietantes y se perfilan como la futura llave que nos abrirá todas las puertas. Nuestras características físicas, únicas y distintas de las de cualquier otro ser humano, tales como las huellas dactilares, geografía de la mano, reconocimiento facial, del iris, de la voz o del ADN se convertirán en los nuevos passwords de entrada a múltiples sistemas, desde el acceso a cuentas bancarias, vehículos, áreas laborales y archivos informáticos hasta, ¿por qué no?, a nuestro propio domicilio.

17. Una Autoridad Certificante CA es una institución o empresa comercial que atestigua por la identidad de individuos, organizaciones u otro Certificador de nivel jerárquico inferior. Son entidades públicas o privadas cuya función es ofrecer confianza en los certificados que firman. Es un sistema parecido a la cédula de identidad, donde el estado, como entidad de confianza, genera un documento que los bancos y las empresas consideran fiable. Actualmente la CA más conocida es la empresa privada americana VeriSing (www.verisign.com), además de las empresas de tarjetas de crédito como: Visa, Mastercard y American Express.

18. Los certificados X.509 V3 es un formato estándar para la certificación de claves públicas recomendado por la ISO (International Standards Organization). El certificado es esencialmente una clave pública y un identificador, firmados digitalmente por una Autoridad de Certificación. Su utilidad es demostrar que una clave pública pertenece a un usuario concreto. Los certificados permitirán a sus titulares realizar una gran cantidad de acciones a través de la Internet.

8.3 RECOMENDACIONES

1. Se recomienda a todas las personas relacionadas de una u otra manera con la informática, énfasis en el estudio y análisis de los diferentes mecanismos utilizados para la protección de la información, los mismos que posteriormente sabrán emitir criterios profundos y objetivos en el momento de implementar una correcta seguridad en sus diferentes lugares de trabajo.

2. Es recomendable el uso moderado de los procesos criptográficos, en especial en aquellas áreas en donde se requiere comunicaciones con tiempos de respuestas bastantes óptimos, puesto que no se tendrá excelentes velocidades de transmisión debido al tiempo adicional requerido para el proceso de cifrado y descifrado de información.

3. Cabe indicar que los algoritmos criptográficos existentes en el mercado pueden ser acoplados e implementados a cualquier actividad, situación, empresa o institución, se recomienda seleccionar el algoritmo más acertado para adaptarse a las necesidades de un determinado servicio o proceso en particular, tomando en cuenta los siguientes criterios: la

complejidad del algoritmo, tamaño de clave utilizado, recursos de máquina requeridos, tiempos de respuesta, niveles de seguridad proporcionados.

4. La Criptografía es una ciencia que se encuentra en constante crecimiento y evolución, por lo que se recomienda su estudio en forma periódica. Los nuevos retos, la tecnología de punta, las nuevas técnicas de criptoanálisis que aparecen nos obliga a estar en constante renovación de conocimientos.

5. En la actualidad cuando millones de ciudadanos usan las redes para efectuar sus transacciones bancarias, compras, declaraciones de impuestos, envío de correo electrónico, intercambio de mensajes, etc., la seguridad de las mismas aparece en el horizonte como un problema potencial de grandes proporciones. De esta manera, todo profesional en Informática y Computación, debe poseer sólidos conocimientos en cuanto a los diferentes mecanismos de seguridad empleados actualmente en la protección de la Información, que es uno de los principales activos de las entidades públicas o privadas. Por lo que recomendamos a las Autoridades pertinentes de la Escuela de Ingeniería en Sistemas Computacionales (EISIC), la creación del Pénsum de estudio para la Asignatura de Criptografía, que de preferencia se dictará en el Quinto Semestre, nivel en el cual los estudiantes poseen un alto grado de conocimiento teórico/práctico en las asignaturas de Matemáticas y Lenguajes de Programación, con lo que el análisis, diseño e implementación de los diferentes mecanismos de seguridad será mucho más rápido y provechoso tanto para estudiantes como para docentes.

6. Promover la estandarización e interoperabilidad de los procesos criptográficos con la finalidad de mantener la compatibilidad con los diferentes protocolos criptográficos existentes.

7. Promover la creación e invención de algoritmos criptográficos enfocados hacia el reconocimiento y aceptación mundial de la comunidad informática.

8. Promover y hacer conocer la importancia de la seguridad informática empleados en los medios de comunicación digital a través de talleres y seminarios.

9. Como profesionales informáticos, promover el uso y aprovechamiento de las operaciones que tengan como escenario la Internet, tales como: transferencia de fondos, compras en línea, pago de impuestos, prestación de servicios, publicidad, etc.

10. Las Autoridades pertinentes de la Universidad Técnica del Norte en conjunto con sus colaboradores interesados, promuevan las gestiones necesarias para que éste centro de educación superior se convierta en una Entidad Certificadora y preste los servicios de certificación a las diferentes empresas, instituciones y comunidad en general interesadas en adquirir el servicio.