SEGURIDAD EN EL COMERCIO ELECTRONICO A TRAVES DE VPN

Rita Cabrera Sarmiento[1], Lenin Lemos Ponce[2], Ricardo Moran Vera[3], Jose Escalante

[1]Ingeniero Eléctrico en Electrónica 2006
[2]Ingeniero Eléctrico en Electrónica 2006
[3]Ingeniero Eléctrico en Electrónica 2006
^Director de Tópico, Ingeniero Eléctrico en Electrónica , escuela Superior Politécnica del Litoral, 1996,Diplomado en Administración de Proyectos, Profesor de la ESPOL, 1997.

RESUMEN

En un entorno donde las empresas necesitan ser cada vez mas competitivas, se hace necesario que estas mantengan sus sistemas computacionales lo mas actualizados posible. Esto se logra únicamente interconectándose unas con otras y utilizando aplicaciones de e-commerce.

Lamentablemente en nuestra realidad local estas conexiones pueden resultar demasiado costosas mediante las formas tradicionales. En este trabajo demostramos que las VPN son una herramienta suficientemente segura, y que además es mas manejable, menos costosa y que puede ser utilizada con absoluta confianza por las empresas que quieren empezar o continuar desarrollando sus aplicaciones de e-commerce.

RESUMEN IN ENGLISH

At a environment where the business need to be better every day than rivals. It's necessary that this ones have their Computational Systems in full upgrade and fast state. This is posible only if they binding each one and use E-commerce applications.

Regretfully in our local reality this binding could to be too expensive through traditional ways. At this topic we prove that the VPN bindings are a tool safe enough, and also more adaptable, less expensive and that is full reliable by small and enterprise business that can begin or increase their E-commerce applications.

INTRODUCCION

Hoy en día las personas realizan sus transacciones comerciales a través de Internet lo cual desean que sean privadas y que nadie interrumpa su labor, en nuestra tesis hemos investigado como poder hacerlas mas seguras, hablamos de las redes privadas virtuales en donde usted realiza una transacción comercial o una conversación a través de un túnel virtual, en donde todo lo que usted escriba se en cripta es decir se hace basura.

CONTENIDO

CAPITULO I.
COMERCIO ELECTRÓNICO

1.1 ¿QUE ES EL COMERCIO ELECTRONICO?

Es cualquier forma de transacción comercial basada en la **transmisión de datos sobre redes de comunicación** como Internet en la que las partes interactúan electrónicamente en lugar de por intercambio o contacto físico directo.

El comercio electrónico es el nuevo marco de negocios en el que se desarrollan cada vez más operaciones mercantiles. Cada vez son más numerosas las empresas que realizan todas sus operaciones comerciales utilizando tecnologías de la comunicación, aunque solo lo utilicen para algunas funciones especificas. El comercio electrónico, de carácter mundial por su propia naturaleza, abarca una amplia gama de actividades, algunas de ellas conocidas, la mayoría totalmente nuevas.

1.2 TIPOS DE COMERCIO ELECTRONICO SEGÚN AGENTES QUE INTERVENGAN.

- Comercio entre empresas “business to business” (B2B).
- Venta de productos fiables a un consumidor o “business to consumer” (B2C).
- Consumer to Consumer” (C2C) subastas en la que usuarios particulares venden productos.
- A2B/C/A “administration to business/consumer o administration”.
- “Peer to peer” (P2P), o de amigo a amigo.
- “Business to employee” (B2E), comunicaciones entre empresas y trabajadores.
- “Goverment to Consumer” (G2C).
- “Goverment to Goverment” (G2G).

1.3 VENTAJAS Y DESVENTAJAS EN COMPARACIÓN CON EL SISTEMA TRADICIONAL.

Los negocios en Internet no son tan diferentes de los negocios clásicos. Erróneamente se piensa que lo importante es la tecnología. Ventajas son el ahorro de tiempo y los costes asociados a la compra.
Además debemos considerar también:

LAS 5 REGLAS DE LA NUEVA ECONOMIA.-

- Los costos de interacción y transformación actualmente no son tan elevados.
- Los activos no desempeñan un papel tan fundamental en la generación de la oferta.
- El tamaño de la empresa no condiciona los beneficios.
- El acceso a la información ha dejado de ser caro y restringido.

- No se necesitan varios años ni grandes capitales para establecer un negocio a escala mundial.

1.4 ASPECTOS CLAVES DEL COMERCIO ELECTRONICO.

- Personalización.
- Medios de pagos en tiempo real.
- Barreras tecnológicas
- Seguridad y confianza

CAPITULO II.

SEGURIDAD EN EL WEB.

2.1.- INTRODUCCIÓN A LA CRIPTOGRAFíA.-

La idea de la criptografía tiene miles de años de antigüedad: los generales griegos y romanos la utilizaban para enviar mensajes en clave a los comandantes que están en el campo de batalla. Estos sistemas primitivos se basaban en 2 técnicas: la sustitución y la transposición.

La sustitución se basa en el principio de reemplazar cada letra del mensaje que se desea encriptar con otra. Algunos códigos de sustitución ocupan el mismo esquema de reemplazo para todas las letras del mensaje que se encripta; otros emplean diferentes esquemas para distintas letras.

La transposición se basa en la revoltura de los caracteres del mensaje. Un sistema de transposición implica escribir un mensaje dentro de una tabla, renglón por renglón, y luego leerlo columna por columna. El cifrado de doble transposición implica repetir la revoltura otra vez.

2.2.- ¿Que es la Criptografía?

La criptografía es un conjunto de técnicas empleadas para conservar segura la información. Con ella es posible trasformar palabras escritas y otros tipos de mensajes de forma que sean incomprensibles para receptores no autorizados. Un receptor autorizado puede después regresar las palabras o mensajes a un mensaje perfectamente comprensible.

Por ejemplo, he aquí un mensaje que tal vez se desee enviar:

SSL is a cryptographic protocol.

Este podría ser el mensaje una vez encriptado:

***---'¡'¡&($%$#*-¡"°#$%&&//][_:;¨*¡?=)%**

Aún mejor, mediante la criptografía es posible volver a convertir este código en el comprensible mensaje original.

I.- Terminología.

Los sistemas de encriptación modernos constan de dos procesos complementarios:

a.- Encriptación.

Proceso mediante el cual el mensaje *llano* se transforma en un mensaje *cifrado* mediante una función compleja y una llave de codificación especial.

b.- Desencriptación.

Proceso inverso, en el cual el texto cifrado se convierte nuevamente en el texto llano original mediante una segunda función compleja y *una llave de desencriptación.*

La figura 2.1 muestra como se acoplan ambos procesos.

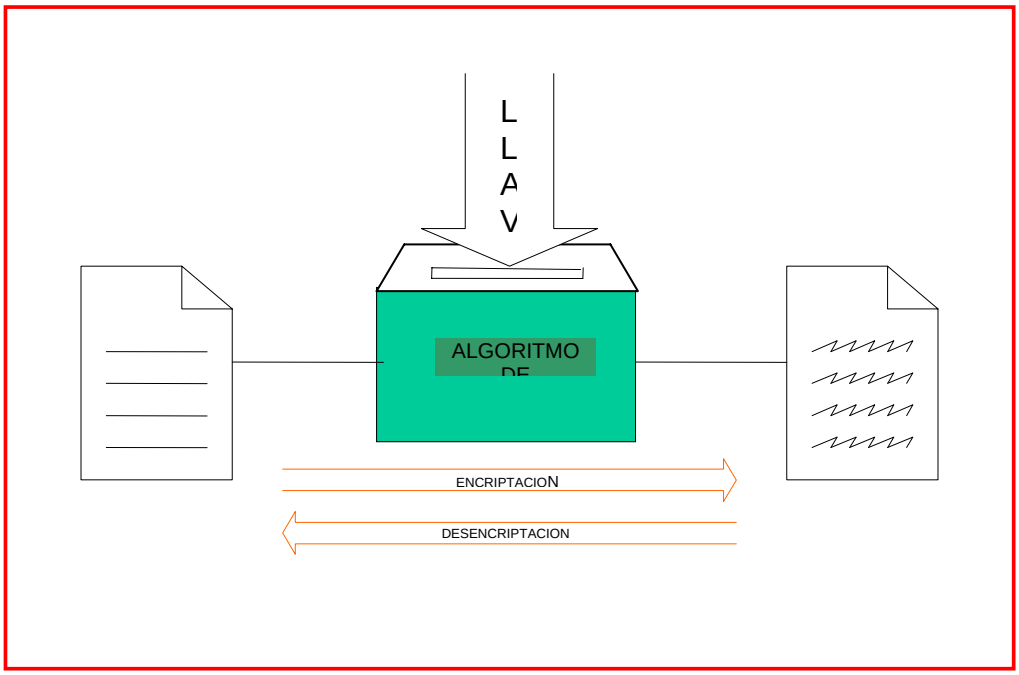

FIG.2.1 ENCRIPTACION DESENCRIPTACION

La meta de la criptografía es hacer imposible tomar el texto cifrado y reproducirlo en su forma original sin la llave correspondiente, y elevar el costo de adivinar la llave más allá de lo práctico.

CAPITULO III.

REDES PRIVADAS VIRTUALES (VPNs).

3.1. INTRODUCCIÓN A LA TECNOLOGÍA RPV.

3.1.1 ¿Qué es una RPV?

Para explicar las RPV, es necesario describir un par de conceptos: cifrado y virtual. El cifrado no es nada más

que tomar un mensaje, por ejemplo, (llegaré tarde), y convertirlo en basura, algo como “2der56gt2345r”. El otro extremo de este proceso se llama descifrado y es el reverso del cifrado. El núcleo dela seguridad de las redes privadas virtuales es que nadie, a excepción del receptor, es capaz de completar la parte de descifrado del proceso.

Las RPV también pueden utilizarse en las líneas rentadas, enlaces ATM/Frame Relay (retransmisión de tramas) o servicios de red telefónica simple (POTN), como las redes digitales de servicios integrados (ISDN) y las líneas de suscrición digital (XDSL).

La figura 3.1 muestra una red corporativa conectada a una red publica de VPN actuales.

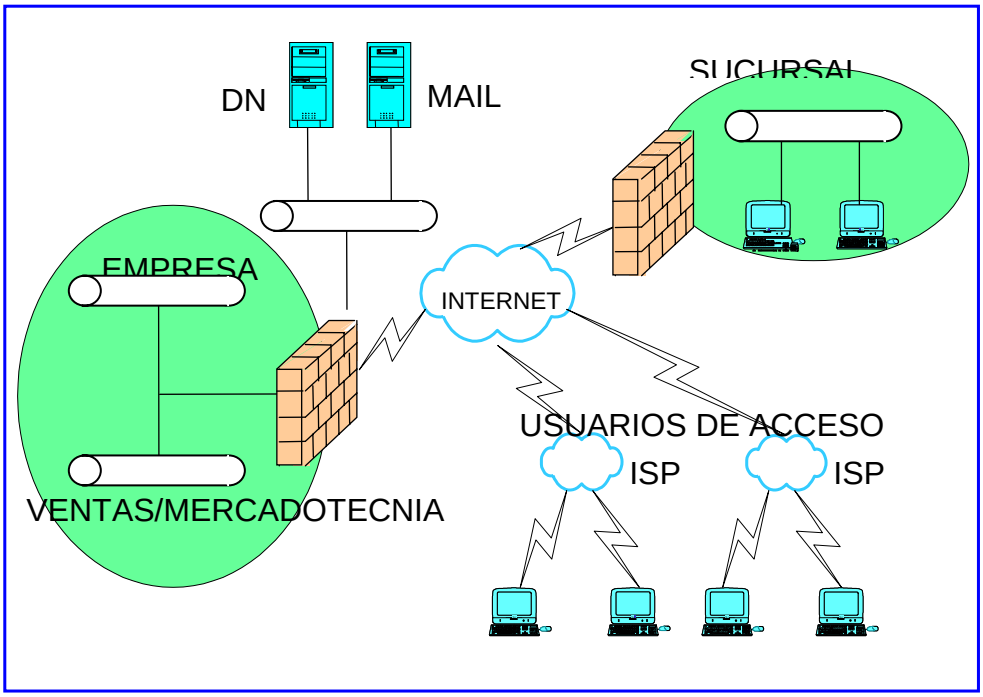

FIG. 3.1 Una VPN Corporativa.

CAPITULO IV.

SITUACIÓN ACTUAL DEL E-COMMERCE EN EL ECUADOR.

4.1. INTRODUCCIÓN.

Todos estamos seguros cada vez más de lo que se puede hacer a través del Internet, y la diferencia a otros tiempos es la rapidez con que se trabaja.
Cuando hubo el Boon de Internet, no pensamos que todo se iba a manejar mediante él y así darle una facilidad a las personas, esto nos hizo hacer un enfoque hacia el consumidor.

El Internet es comercialización hacia el exterior, y, por eso, era necesaria la concentración de la ley de comercio electrónico.

Ecuador era uno de los pocos países de América que no contaba con esa ley esencial y ahora más que cualquier otro, necesita los mercados exteriores para llegar a una economía de gran escala con sus industrias. Esa es la gran oportunidad de Internet.

4.2. NUESTRA LEY DE REGULACIÓN DE COMERCIO ELECTRÓNICO.

El Consejo Nacional de Telecomunicaciones (CONATEL) ha promovido en su página web un texto concerniente a la propuesta de ley sobre regulación del comercio electrónico, la cual puede ser leida por cualquier persona natural o juridica que ayude a mejorar el tema

CONCLUCIONES Y RECOMENDACIONES

Como pudo ver en este trabajo, toda la información que hemos aquí proporcionado permite elaborar una solución potencial en cuanto a la seguridad, la autorización y el acceso de los usuarios, la interoperabilidad con la infraestructura de red interna y con los clientes y proveedores externos de cualquier empresa.

Las RPV continuarán creciendo. Con el comercio electrónico y cada vez más negocios dirigidos a través de Internet, es necesario establecer un ambiente seguro. Cada encuesta que usted lea le indicará el crecimiento de Internet y la dirección del crecimiento futuro.
Las RPV satisfacen las más estrictas necesidades de seguridad; son rápidas y sencillas. Las personas se acostumbrarán tanto a Internet que ni siquiera se preocuparán porque sus paquetes lleguen cifrados, se supondrán para ese momento la seguridad de la red es optima.

Esta es una de las principales razones por las que debemos usar tecnologías como la RPV para proporcionar este nivel óptimo de seguridad necesario en las transacciones de comercio electrónico muestra cada vez más pequeña la “Aldea Global”.

BIBLIOGRAFÍA

- http://www.verising.com
- http://www.rsa.com
- http://www.doc.gov/bureaus
- http://www.darpa.com
- http://www.nist.com
- http://www.compueterprivacy.com
- http://ipsec-wit.antd.nist.gov
- RFC 1702 Generic Routing Encapsulation over Ipv4 networks.
- RFC 2410 The NULL Enriptation Algorithm and its use with IPSec.
- RFC 2411 IP Security Document Roadmap.
- Private Network Virtual Implementatión. Steven Brown.
- Cryptography adn Data Security. Denning Dorothy E.
- Criptography Policy. Hoffman Lance J.

-Protocols for Public Key Cryptosystems. G. J. Simmons