Universidad Central del Ecuador

“Omnium Potentior Est Sapientia”

Trabajo Grupal

Criptografía y Seguridad de la Información

Informe Grupo 01

Aplicación Criptográfica Acceso Remoto Seguro

Computación

Ingeniería y Ciencias Aplicadas

Octavo Semestre

¿Qué es el Acceso Remoto Seguro?

El acceso remoto seguro se refiere a aquel conjunto de mecanismos técnicos y criptográficos los cuales permiten a los usuarios autenticados en una determinada plataforma de información conectarse a una red privada, a sistemas remotos a través de las redes públicas como la Internet, manteniendo así su confidencialidad, integridad y autenticación de la información intercambiada.

Según M. Hancock en un estudio realizado en 1994 sobre los problemas y cuestiones en el acceso remoto seguro [1], el acceso remoto plantea múltiples riesgos si no se llega a implementar las políticas de control de acceso y cifrado robustas, en este entorno, el uso de los protocolos como SSH, VPN y los túneles de cifrado no existían para aquella época y a la par se encontraban aún en sus primeras etapas de desarrollo, se usaban otro tipo de protocolos que representabas riesgos significativos para la seguridad como el uso de Telnet, Rlogin o Rsh, FTP, SLIP, entro otros, estos protocolos realmente no eran tan eficientes y no llevaban consigo un mecanismo moderno criptográfico, por lo cual la transmisión de datos y credenciales en texto plano lo hacía altamente vulnerable a ataques de interceptación, suplantación y espionaje, su autenticación era débil, basada en confianza implícita o archivos de configuración inseguros.

Según M. Peyravian y C. Jeffries en un estudio realizado en 2006 sobre el acceso seguro de usuarios remotos a través de redes inseguras [2], este tipo de tecnología “Acceso Remoto Seguro” es ampliamente utilizado en entornos empresariales, industriales, académicos y gubernamentales, ya que facilita algunas tareas relacionadas con la administración remota de servidores, la asistencia técnica desde cualquier parte del mundo, el teletrabajo y el monitoreo de datos en tiempo real, sin comprometer la seguridad de la información en dicho proceso, en este estudio se destaca que un sistema de acceso remoto seguro debe integrar los siguientes componentes: una autenticación fuerte basada en tokens, certificados o la forma clásica de usuario y contraseña, debe existir un mecanismo de cifrado de extremo a extremo como AES, RSA o TLS, también este sistema debe de integrar el control de privilegios y la auditoria de actividades constantes.

¿Qué algoritmos criptográficos están involucrados?

Según lo afirmado en estudios como el de I. Capuñay, A. Guerrero y E. Villegas [3], los protocolos de acceso remoto seguro modernos como el SSH y la VPN se fundamentan con la combinación de algoritmos criptográficos simétricos, asimétricos, de intercambio de claves y funciones hash, algunos algoritmos principalmente utilizados son:

1. RSA, el cual es un algoritmo de cifrado asimétrico que se utiliza para el intercambio seguro de las claves y la autenticación segura, empleando un par de claves basada en la gestión de clave pública y privada, permitiendo así establecer una conexión o acceso seguro a través de canales inseguros que existen en una red pública o privada.

2. SHA-256, es una función hash criptográfica usada para asegurar la integridad de los datos, proviene de la familia SHA-2, esta función permite convertir cualquier tipo de entrada en una cadena de 256 bits, permitiendo detectar si los datos o información ingresada en un texto plano ha sido modificada durante una transmisión, función hash resistente a colisiones y ampliamente implementado en protocolos seguros.
3. AES, es un algoritmo de cifrado simétrico ampliamente adoptado en el entorno empresarial y gubernamental por su eficiencia y robustez, usa una clave de 128 bits comúnmente, existen otros sistemas que incorporan claves de hasta 256 bits para cifrar los datos de la sesión de un usuario, garantizando la confidencialidad de la información transmitida en tiempo real, AES es un estándar oficial de cifrado resistente a taques de fuerza bruta actualmente.
4. ECDH, es una versión mejorada y moderna de los protocolos de intercambio basados en claves de Diffie-Hellman, hace uso de la criptografía basada en curvas elípticas, el ECDH permite que ambas partes involucradas establezcan una clave secreta compartida a través de un canal inseguro, con mayor seguridad y menor tamaño de clave que el Diffie-Hellman tradicional, lo cual lo vuelve ideal para dispositivos con recursos limitados.

¿Qué protocolos criptográficos están involucrados?

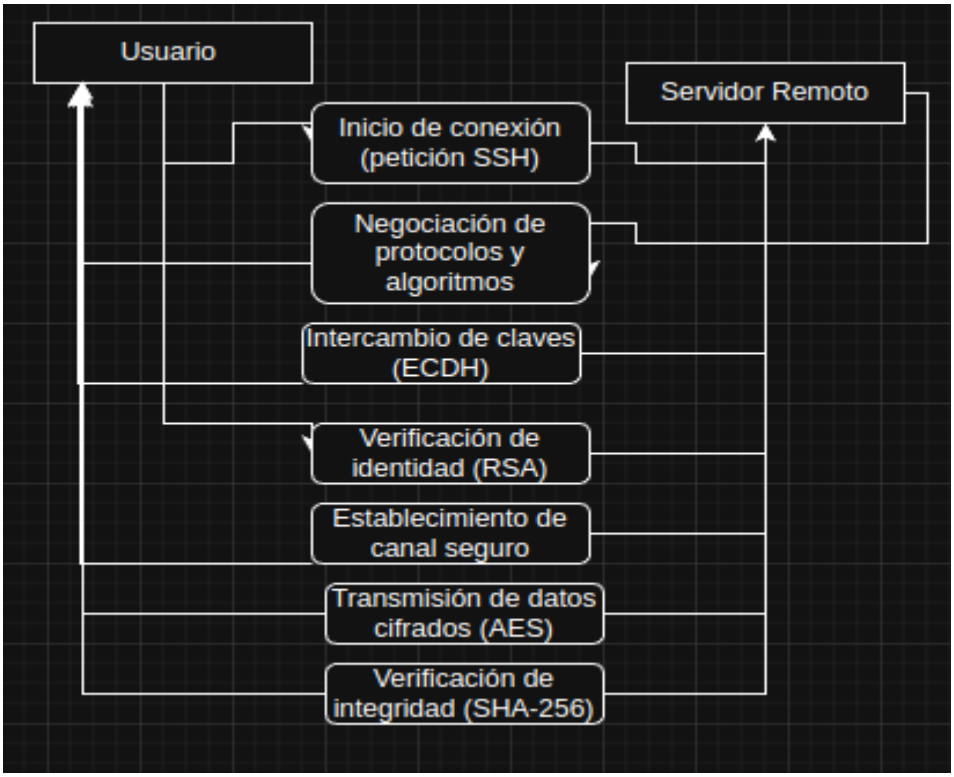
Según lo afirmado en estudios como el de A. Figueroa, F. Andrade, C. Bone y J. Saltos [4], los protocolos criptográficos constituyen una base sobre la cual se van a desarrollar las aplicaciones de acceso remoto, estos protocolos buscan definir el modo en que se va a negociar la seguridad de la información, y el cómo se van a gestionar, donde se establecerán algunos cifrados y se busca garantizar la integridad y la autenticación entra las comunicaciones del cliente y el servidor remoto, algunos protocolos criptográficos involucrados en el acceso remoto son:

1. IPSec, es un conjunto de protocolos que actúan y trabajan dentro del modelo OSI específicamente en la capa de red, la cual se utiliza principalmente para proteger el tráfico de IP mediante el cifrado, autenticación y la verificación de integridad, este protocolo es ampliamente implementado en las redes privadas empresariales y redes virtuales VPN la cual opera en modo de transporte o túnel de información, permitiendo la protección de los datos de extremo a extremo o de red en red.
2. SSH, es un protocolo de red criptográfico el cual permite el acceso remoto seguro a sistemas a través de canales cifrados, el SSH reemplaza los protocolos inseguros como Telnet y Rlogin los cuales eran muy ineficiente, ahora incorporan la autenticación mediante la clave pública, intercambio de claves seguro basados en ECDH y cifrado asimétrico como AES, el SSH es usado para la administración remota de servidores en sistemas Unix o Linux, e incluso en la transferencia segura de archivos en la red por SFTP o SCP.

3. SSL/TLS, ambos protocolos criptográficos proporcionan un nivel de seguridad en las capas de transporte de redes de información o modelo OSI, busca asegurar la comunicación mediante el cifrado simétrico, el intercambio de claves normalmente usado con RSA o ECDH y ciertas funciones hash como SHA-256 la cual es ampliamente usada para proteger el tráfico de información en la web con HTTPS, en otras palabras, SSL y TLS son una base de seguridad en protocolos modernos como SMTPS, FTPS enfocados para la transferencia de datos y archivos por la web.

Diseño esquemático de su funcionamiento

El siguiente diseño esquemático representa un proceso básico o elemental de una conexión mediante un protocolo de acceso remoto seguro, este esquema refleja mejores prácticas descritas en entornos empresariales como Windows Server 2012 de la cual se basa este esquema, donde se enfatiza la importancia de establecer las comunicaciones remotas seguras dado la gran cantidad de datos confidenciales gestionados y soportados por los sistemas modernos [5].



Este esquema parte de la base que al no contar siempre con un acceso físico a los servidores, es fundamental implementar mecanismos de conexión remota cifrada y autenticada, permitiendo garantizar tanto la confidencialidad como la mera integridad de los datos intercambiados.

Escenarios donde se usa con frecuencia

El acceso remoto seguro tiene una gran relevancia en distintos sectores productivos, científicos y tecnológicos, particularmente a raíz de los eventos globales que exigieron alternativas al trabajo

presencial, como la pandemia presentada del COVID-19, algunos de los escenarios más representativos donde su aplicación es fundamental son:

1. Según M. Cuchillac [6], el teletrabajo en PYMEs durante el confinamiento de los años 2020, muchas micro y pequeñas empresas se enfrentaron a una necesidad urgente la cual fue implementar esquemas de acceso remoto para continuar operando, entonces, se identificaron tecnologías como las VPNs, escritorios remotos y los túneles SSH se proponen como soluciones prácticas y relativamente accesibles, este tipo de organizaciones, que suelen contar con presupuestos limitados y personal técnico escaso, recurrieron al acceso remoto seguro como una estrategia clave para facilitar y agilizar el teletrabajo sin comprometer la seguridad de los datos.
2. Según E. López y A. Fonseca [7], la telemedicina y el tratamiento de señales biomédicas en el área de la salud, el acceso remoto seguro ha sido clave en el desarrollo de sistemas de teleconsulta y telemonitoreo, dentro del estudio señalado por estos autores se ha diseñado un tipo de plataforma para la recolección, almacenamiento y visualización remota de señales médicas como ECG y temperaturas corporales, este sistema incluye autenticación segura y protocolos cifrados para proteger la información sensible de los pacientes, garantizando la confidencialidad, integridad y disponibilidad en el entorno médico remoto.
3. Según A. Figueroa, F. Andrade, C. Bone y J. Saltos [4], dentro de la seguridad de la información y control de infraestructura de TI el acceso remoto seguro no solo forma parte de la misma seguridad informática, sino que es un componente esencial de la seguridad de la información, su implementación permite que los administradores de la red puedan gestionar servidores, respaldos y configuraciones desde ubicaciones externas sin exponer los sistemas a un ataque, también incorpora una correcta autenticación, el cifrado de datos y el registro de accesos son elementos cruciales que distinguen el acceso remoto seguro como una herramienta imprescindible para gobernanza de los activos digitales de las empresas.

Bibliografías

[1] W. M. Hancock, “Issues and problems in secure remote access”, *Netw. Secur.*, vol. 1994, n.º 6, pp. 14–18, junio de 1994. Accedido el 23 de mayo de 2025. [En línea]. Disponible: https://doi.org/10.1016/1353-4858(94)90048-5

[2] M. Peyravian y C. Jeffries, “Secure remote user access over insecure networks”, *Comput. Commun.*, vol. 29, n.º 5, pp. 660–667, marzo de 2006. Accedido el 23 de mayo de 2025. [En línea]. Disponible: https://doi.org/10.1016/j.comcom.2005.07.025

[3] D. I. Capuñay Puican, A. M. Guerrero Millones y J. E. Villegas Vega, “ANÁLISIS COMPARATIVO DE ALGORITMOS CRIPTOGRÁFICOS PARA REDES PRIVADAS VIRTUALES”, *INGENIERIA*, vol. 3, n.º 2, pp. 121–133, septiembre de 2016. Accedido el 24 de mayo de 2025. [En línea]. Disponible: https://doi.org/10.26495/icti.v3i2.440

[4] J. A. Figueroa-Suárez, R. F. Rodríguez-Andrade, C. C. Bone-Obando y J. A. Saltos-Gómez, “La seguridad informática y la seguridad de la información”, *Polo Del Conoc.*, vol. 2, n.º 12, p. 145, marzo de 2018. Accedido el 23 de mayo de 2025. [En línea]. Disponible: https://doi.org/10.23857/pc.v2i12.420

[5] D. Rountree, “Secure Remote Access”, en *Windows 2012 Server Network Security*. Elsevier, 2013, pp. 89–121. Accedido el 23 de mayo de 2025. [En línea]. Disponible: https://doi.org/10.1016/b978-1-59749-958-3.00004-2

[6] V. M. Cuchillac, “Clasificación de las tecnologías de acceso remoto para el teletrabajo en PYME”, *Real. Reflex.*, vol. 1, n.º 55, pp. 28–58, junio de 2022. Accedido el 23 de mayo de 2025. [En línea]. Disponible: https://doi.org/10.5377/ryr.v1i55.14411

[7] N. E. Olarte López y A. Rubiano Fonseca, “Sistema de almacenamiento de señales biológicas, con acceso remoto y parámetros de seguridad”, *Rev. Tecnura*, vol. 17, n.º 37, p. 74, septiembre de 2013. Accedido el 23 de mayo de 2025. [En línea]. Disponible: https://doi.org/10.14483/udistrital.jour.tecnura.2013.3.a07