UNIVERSIDAD DEL ISTMO

Campus Tehuantepec

Ingeniería en Computación

Tema: Investigación de seguridad en redes.

Materia: Interacción Humano Computadora.

Alumno: Osorio Ramos Jeremy.

Docente: Ing. Carlos Mijangos Jiménez.

Semestre: Séptimo.

Grupo: 704.

Tehuantepec Oaxaca a 16 de Octubre de 2025.

Introducción

En el campo de la seguridad informática, existen diversos mecanismos y herramientas que garantizan la protección, integridad y confidencialidad de la información. Entre ellos se encuentran los firewalls, los algoritmos de cifrado y firma digital como RSA y MD5, y los métodos de codificación como Base64 (B64). Este documento presenta una descripción general de cada uno, su funcionamiento y su aplicación dentro del entorno digital.

1. Firewall

Definición:
Un firewall es un sistema de seguridad de red que supervisa y controla el tráfico de red entrante y saliente, según un conjunto de reglas de seguridad previamente definidas. Su función principal es actuar como una barrera entre una red interna confiable y otra no confiable, como Internet.

Aplicación:
Los firewalls se utilizan para proteger redes corporativas, servidores y computadoras personales de accesos no autorizados o ataques externos. Por ejemplo:

Bloquear el acceso desde direcciones IP sospechosas.

Permitir solo el tráfico HTTP (puerto 80) y HTTPS (puerto 443).

Evitar la fuga de información o el ingreso de malware.

Los firewalls pueden operar en distintas capas del modelo OSI, desde la capa de red hasta la capa de aplicación, dependiendo de su tipo (por ejemplo, firewall de paquetes, de estado o de próxima generación).

2. RSA (Rivest–Shamir–Adleman)

Definición:
El RSA es un algoritmo de cifrado asimétrico utilizado ampliamente en la seguridad de datos. Utiliza un par de claves: una pública (para cifrar) y una privada (para descifrar). Fue creado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman.

Aplicación:
RSA se usa en:

Firma digital: permite verificar la identidad del remitente.

Cifrado de datos: asegura la confidencialidad de la información transmitida.

Protocolo HTTPS: en la negociación de claves para establecer una conexión segura entre el cliente y el servidor.

Ejemplo: Cuando accedemos a una página web con HTTPS, el navegador y el servidor intercambian claves RSA para establecer una sesión segura cifrada.

3. MD5 (Message Digest 5)

Definición:
El MD5 es un algoritmo de hash criptográfico que toma una entrada (mensaje o archivo) y produce un valor hash de 128 bits (32 caracteres hexadecimales). Fue diseñado por Ronald Rivest en 1991.

Aplicación:
Se utiliza para:

Verificar la integridad de archivos: al comparar el hash original con el generado tras la descarga.

Almacenamiento de contraseñas: aunque hoy en día ha sido reemplazado por algoritmos más seguros como SHA-256.

Comprobación de datos en sistemas y bases de datos.

Ejemplo: si un archivo tiene un hash MD5 conocido y el hash del archivo descargado es distinto, significa que el archivo fue alterado o corrompido.

4. Base64 (B64)

Definición:
Base64 es un método de codificación binario a texto que permite representar datos binarios (como imágenes o archivos) en caracteres ASCII. No es un algoritmo de cifrado, sino una forma de transformar los datos para que puedan transmitirse por medios que solo admiten texto.

Aplicación:

Transmisión de correos electrónicos: codifica archivos adjuntos en formato texto.

Desarrollo web: se utiliza para incrustar imágenes o archivos dentro de código HTML o CSS.

API y autenticación: se usa para codificar credenciales o datos en tokens.

Ejemplo: una imagen convertida a Base64 se puede insertar directamente en una página web sin necesidad de un archivo externo.

Conclusión

Los mecanismos y herramientas de seguridad como firewalls, RSA, MD5 y Base64 cumplen funciones complementarias dentro del ecosistema digital. Mientras que los firewalls protegen el acceso a la red, RSA y MD5 garantizan la confidencialidad e integridad de la información, y Base64 facilita la transmisión segura y estandarizada de datos. Comprender su funcionamiento y aplicación permite fortalecer la seguridad informática en entornos personales y empresariales.

Referencias:

Tanenbaum, A. S., & Wetherall, D. J. (2012). Redes de Computadoras (5ª ed.). Pearson Educación.

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.

RFC 1321: The MD5 Message-Digest Algorithm. (1992). Internet Engineering Task Force (IETF).

RSA Laboratories. (2000). PKCS #1: RSA Cryptography Standard.

Mozilla Developer Network (MDN). (2024). Base64 encoding and decoding. https://developer.mozilla.org/

CISCO. (2023). Firewall Technologies Overview. Cisco Documentation.