ALGORITMO MD5 (MESSAGE DIGEST ALGORITHM 5)

AUTOR: RICARDO CASTILLO B.

NOVIEMBRE: 2020

San Marcos

Introducción

MD5 es uno de los algoritmos de reducción criptográficos diseñados por el profesor Ronald Rivest del MIT (Massachusetts Institute of Technology, Instituto Tecnológico de Massachusetts). Fue desarrollado en 1991 como reemplazo del algoritmo MD4 después de que Hans Dobbertin descubriese su debilidad.

A pesar de su amplia difusión actual, la sucesión de problemas de seguridad detectados desde que, en 1996, Hans Dobbertin anunciase una colisión de hash, plantea una serie de dudas acerca de su uso futuro. Es por ello que a continuación se hará refencia al algoritmo MD5, su uso, concepto y su marcha hacia el reemplazo.

Contenido

Algoritmo MD5 – ¿Para qué se puede utilizar?

Usos del cifrado MD5

Además de que contribuye a asegurarse de descargar e instalar un sofware fiable y no uno malicioso, el cifrado MD5 tiene otros usos quese detallarán a continuación:

- Por medio de un programa se puede crear un código MD5 para algún archivo, y de esta manera hacer que únicamente el ususrio que lo creó pueda hacer uso de el.
- Una vez que se haya realizado una descarga y se disponga del archivo completo, puede ser utilizarlo en una instalación de firmware, como en un router.
- Comprobar que un texto no ha sido modificado a la hora de enviárlo a otra persona para evitar que pueda llegar de forma distinta a como era el original. Existen páginas webs en donde se introduce el texto que se a enviar, esta web nos devuelve el hash, y es este el que se envia al destinatario para que compruebe que el texto es el correcto.

MD5 (Message Digest Algorithm 5)

Es un algoritmo que se utiliza como una función de codificación o huella digital de un archivo. De esta forma, a la hora de descargar un determinado archivo como puede ser un instalador, el código generado por el algoritmo, también llamado hash, viene “unido” al archivo. Un hash MD5 está compuesto por 32 caracteres hexadecimales y una codificación de 128 bits.

¿Puede dar errores el MD5?

Como todos los programas, en ocasiónes pueden dar errores con los que no se contaban, no obstante, en el caso de la tecnología MD5 cuenta con años de experiencia, por lo que es bastante fiable.

Esta tecnología es tan utilizada que existen diccionarios para ‘descifrar’ cualquier hash MD5. Esto quiere decir que, aunque no se logre descifrar el código, sí es posible buscarlo en listas que hay en Internet.

Una práctica extendida entre los hackers es ir almacenando palabras y guardándolas en una base de datos, para que a la hora de extraer las contraseñas de cualquier programa puedan acceder a esta base de datos y extraer las contraseñas en MD5, para luego buscarlas en la tabla de equivalencia que han creado.

El algoritmo MD5 tiene las horas contadas

La larga marcha hacia la obsolescencia del algoritmo de cifrado MD5 puede que se demorara un poco, pero es inevitable.

Oracle ha anunciado recientemente que cualquier archivo JAR (la extensión de los archivos Java) que esté firmado con un cifrado MD5 será tratado como no cifrado, y por lo tanto como no seguro y será bloqueado por la nueva actualización de Java que incluía 270 parches.

Al ejecutar un valor (como una URL) o un archivo a través del algoritmo MD5, la función dará una única cadena de 16 bytes, normalmente representada por un número hexadecimal de 32 dígitos. Puede que observaras un fichero MD5 cuando descargas un ejecutable de Internet, normalmente se incluye para que puedas comprobar la integridad del archivo.

Si ejecutas localmente el archivo descargado a través del algoritmo MD5 y tienes el mismo valor que el original, teóricamente los dos archivos deberían ser idénticos.

Desafortunadamente, a mediados de los 90, los expertos en seguridad descubrieron que el MD5 tenía múltiples vulnerabilidades, incluidas algunas que permitían ataques de fuerza bruta. Por supuesto, los estándares comenzaron a cambiar, por eso el uso de MD5 comenzó lentamente a declinar. En 2008, el CERT y el Departamento de Seguridad Nacional de EEUU lo consideraron como no seguro.

Por lo tanto, el uso de MD5 cada vez era menor, y muchas organizaciones buscaron alternativas. Uno de los primeros sucesores de MD5 fue SHA-1, pero también cayó en desgracia al descubrirse varios fallos de seguridad.

El sucesor más aceptado de estos algoritmos es la familia SHA-2 de hash criptográfico, que incluye el SHA-256 y el SHA-512. Los SHA-2 están considerados como mucho más seguros que sus predecesores y muchas empresas punteras los están empleándo.

Dado que las vulnerabilidades de MH5 son conocidas desde hace mucho tiempo, es extraño que Oracle siguiera dándole soporte durante estos últimos años. Se espera que no queden muchos desarrolladores que todavía empleen el MD5 ya que tiene sus horas contadas.

Todo esto tiene un importante impacto en la usabilidad. Especialmente, cuando se trata de verificación, autenticación y manejo de integridad de datos. Lo mejor de todo, es que la mayoría de estas funciones son de dominio público y sus implementaciones son software libre.

Conclusiones y recomendaciones

En general una de las precauciones comunes de la mayoria de las personas que utilizan internet, se evidencia al momento de descargar cualquier archivo de la red, ya sea un programa, contenido audiovisual, etc. El peligro de descargar estos archivos de sitios desconocidos es enorme, no obstante, en dichos casos es muy importante asegurarse que el programa que nos vamos a instalar este limpio de cualquier malware que cualquier usuario con malas intenciones haya podido introducir. Para lograrlo se requieren métodos para comprobar que el software que se ha descargado es el oficial y no resulta peligrosa su instalación es el algoritmo MD5, que además de tener otros usos, verificar los software que se descargan es una de las funciones para la que más se utiliza el MD5.

Referencias bibliográficas

- Sophos Iberia (2017). El algoritmo MD5 tiene las horas contadas. Recuperado de https://news.sophos.com/es-es/2017/01/27/algoritmo-md5-las-horas-contadas/

- Melús D. (2020). Algoritmo MD5 – ¿Para qué se puede utilizar? Recuperado de https://www.nerion.es/blog/cifrado-md5/

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica