SECURITY INSIDER

Definition Message-Digest Algorithm 5 (MD5)

Was ist MD5?

27.03.2019 | Autor / Redakteur: Dipl.-Ing. (FH) Stefan Luber / Peter Schmitz

Beim Message-Digest Algorithm 5 (MD5) handelt es sich um eine Hashfunktion, die aus einer bestimmten Zeichenkette oder Nachricht einen immer gleichen Hashwert erzeugt. MD5 ist für verschiedene Anwendungen wie die Überprüfung von Download-Dateien oder das Speichern von Passwörtern einsetzbar.

<https://cdn1.vogel.de/unsafe/fit-in/1000x0/images.vogel.de/vogelonline/bdb/1535800/1535838/original.jpg>

MD5 ist eine Hashfunktion zur Generierung eines Hashwerts aus beliebigen Zeichenketten.

(Bild: gemeinfrei)

Die Abkürzung MD5 steht für den englischen Begriff Message-Digest Algorithm 5. Es handelt sich um eine Funktion aus dem kryptographischen Umfeld, die aus beliebigen Nachrichten oder Zeichenketten einen Hashwert <https://www.security-insider.de/was-ist-ein-hash-a-635712/> erzeugt. Die Funktion ist im Gegensatz zur Verschlüsselung <https://www.security-insider.de/was-ist-verschluesselung-a-618734/> nicht umkehrbar und verhindert, dass sich aus dem Hashwert die ursprüngliche Zeichenkette ermitteln lässt.

Entwickelt wurde MD5 von Ronald L. Rivest als Nachfolgefunktion des als unsicher geltenden MD4 am Massachusetts Institute of Technology im Jahr 1991. Typische Einsatzbereiche des Message-Digest Algorithm 5 sind das Prüfen von Download-Dateien oder das Speichern von Passwörtern. Heute gilt MD5 als nicht mehr ausreichend sicher <https://isc.sans.edu/diary/MD5 Considered harmful today - Creating a rogue CA certificate/5587> . Es sind verschiedene Angriffsmethoden wie

Kollisionsangriffe bekannt, die es mit vertretbarem Aufwand erlauben, zu einem bestimmten Hashwert passende Ausgangszeichenketten zu erzeugen.

Grundsätzliche Anforderungen an die MD5-Hashfunktion

An die MD5-Hashfunktion <https://www.security-insider.de/was-ist-ein-hash-a-635712/> bestehen wie bei allen Hashfunktionen mehrere Anforderungen. So muss die identische Zeichenkette immer den selben Hashwert generieren. Zudem ist zu verhindern, dass aus einem Hashwert die ursprüngliche Zeichenkette zu ermitteln ist. Unterschiedliche Zeichenfolgen dürfen nicht den gleichen Hashwert erzeugen. Nicht alle Anforderungen lassen sich zu 100 Prozent von MD5 erfüllen. Beispielsweise ist bekannt, dass unterschiedliche Zeichenfolgen durchaus den gleichen Hashwert liefern können. Man spricht in diesem Fall von einer Kollision. Die Sicherheit der MD5-Anwendungen wie die Verschlüsselung oder die Authentisierung <https://www.security-insider.de/was-ist-authentifizierung-a-617991/> sind direkt von der Einhaltung der Anforderungen abhängig.

Der zugrundeliegende Algorithmus der MD5-Hashfunktion

Dem Message-Digest Algorithm 5 liegt die sogenannte Merkle-Damgård-Konstruktion als Algorithmus zugrunde. Er füllt die Ausgangszeichenfolge zu einer bestimmten Länge mit Einsen und Nullen auf und wendet blockweise Komprimierungsfunktionen an. Es werden mehrere Runden mit mathematischen Funktionen wie modularen Additionen durchlaufen, bis das Ergebnis als 128-Bit-Wert feststeht.

Anwendung des MD5

MD5-Hashwerte kommen für verschiedene Anwendungen zum Einsatz. Eine häufige Anwendung ist die Überprüfung einer heruntergeladenen Datei auf Vollständigkeit. Die Überprüfung soll Übertragungsfehler des Netzwerks ausschließen. Zu diesem Zweck wird auf Basis der Quelldatei eine MD5-Prüfsumme berechnet und übertragen. Der Empfänger berechnet eine Prüfsumme auf Basis der empfangenen Download-Datei und vergleicht sie mit der mitgesendeten Prüfsumme. Sind beide MD5-Hashwerte gleich, war die Übertragung erfolgreich und die Integrität der Datei ist sichergestellt. Man-in-the-Middle-Angriffe lassen sich durch diese Prüfmethode nicht ausschließen, da der Angreifer den Hashwert nach Veränderung der Datei selbst neu erzeugen kann.

Ein weiterer Anwendungsbereich ist das sichere Speichern von Passwörtern. Sie werden nicht im Klartext, sondern als MD5-Hashwerte gespeichert. Dadurch kennt niemand, der

Zugriff auf den Datenspeicher hat, die abgelegten Passwörter. Da das Zurückrechnen des Hashwerts unmöglich ist, ist das ursprüngliche Passwort <https://www.security-insider.de/was-ist-ein-sicheres-passwort-a-572229/> nicht rekonstruierbar. Ob ein Passwort korrekt ist, lässt sich aus dem einfachen Vergleich zwischen dem aus dem Passwort berechneten Hashwert und dem auf dem System, auf das zugegriffen werden soll, gespeicherten Hashwert bestimmen. Weitere Anwendungen des Message-Digest Algorithm 5 sind:

- Generierung von Zufallszahlen
- Generierung von Passwörtern
- Ableiten von Schlüsseln
- digitales Signieren

Sicherheitsaspekte des Message-Digest Algorithm 5

MD5 gilt heute als nicht mehr ausreichend sicher. Es sind bereits seit 1994 Schwächen bekannt wie das gezielte Berechnen von Kollisionen. Schon mit einem normalen PC lässt sich binnen kurzer Zeit eine zu einem Hashwert passende Zeichenkette finden. Für alle kryptographischen Anwendungen sollte MD5 daher nicht mehr eingesetzt werden.

Eine weitere Angriffsmethode auf den Message-Digest Algorithm 5 sind sogenannte Regenbogentabellen. Sie beinhalten Zeichenketten und zugehörige MD5-Hashwerte. Durch einfaches Vergleichen eines zu knackenden Hashwerts mit den in der Tabelle gespeicherten Hashwerten lässt sich unter Umständen eine passende Zeichenkette finden. Im Internet kursieren sehr große Regenbogentabellen, die für Angriffe genutzt werden können.

Nachdem Anfang 2017 eine erfolgreiche Kollisionsattacke auf SHA-1 <https://www.security-insider.de/erfolgreiche-kollisionsattacke-auf-sha-1-hashfunktion-a-587296/> durchgeführt wurde, gelten heute (Stand März 2019) noch SHA <https://www.security-insider.de/was-ist-sha-secure-hash-algorithm-a-851098/> -256 oder SHA-3 <https://www.security-insider.de/was-ist-sha-secure-hash-algorithm-a-851098/> als sichere Alternativen zu MD5.

(ID:45811581)

ÜBER DEN AUTOR

Dipl.-Ing. (FH) Stefan Luber

<https://www.xing.com/profile/Stefan_Luber2/>

WEITERE ARTIKEL DES AUTORS

Definition Sender Policy Framework (SPF)

Was ist SPF?

Definition Stateful Packet Inspection (SPI)

Was ist Stateful Packet Inspection?

Definition BDSG (Bundesdatenschutzgesetz)

Was ist das Bundesdatenschutzgesetz?

KOMMENTARE

Sie sind nicht angemeldet