Dirk Fox

Secure Hash Algorithm SHA-3

Hintergrund

Hashfunktionen zählen zu den wichtigsten kryptographischen Basisfunktionen. Sie bilden eine Nachricht (oder einen Schlüssel) so auf einen Hashwert fester maximaler Länge ab, dass daraus mit vernünftigem Aufwand weder die originale Nachricht (resp. der Schlüssel) zurück gewonnen noch eine „Kollision" – zwei unterschiedliche Nachrichten mit demselben Hashwert – konstruiert werden können. Diese Eigenschaft wird auch „Kollisionsresistenz" genannt [1].

Hashfunktionen spielen in der Praxis vor allem bei digitalen Signaturen und Schlüsselzertifikaten eine entscheidende Rolle: Um eine Signatur (oder ein Zertifikat) zu erzeugen, muss die Nachricht (resp. der Schlüssel) zunächst auf einen Wert fester Länge „gehashed" werden. Die Signatur wird anschließend zum Hashwert gebildet.

Die Güte einer Hashfunktion ist daher ein wichtiges Element bei der Bewertung der Sicherheit (Unfälschbarkeit) einer digitalen Signatur: Wenn zu einem gegebenen Hashwert eine zweite Nachricht mit demselben Hashwert konstruiert werden kann, lässt sich eine Signatur ganz ohne Angriff auf das Signierverfahren fälschen.

Im Mai 1993 veröffentlichte das US-amerikanische NIST erstmals einen Hashfunktionen-Standard: den Secure Hash Algorithm (SHA) [2]. Die Nachfolger SHA-1 (1995) und die Algorithmengruppe SHA-2 (2002, zuletzt aktualisiert im März 2012 [5]) beseitigten eine Schwäche des ersten SHA und ergänzten den SHA-1 um (vermutlich) sicherere Varianten (SHA-224 bis SHA-512). Daneben verbreitete sich der von Ron Rivest – einem der Väter des RSA-Verfahrens – entwickelte und 1992 als RFC publizierte Hashalgorithmus MD5.

Beide Verfahren beruhen auf dem 1989 publizierten Damgård-Merkle-Prinzip [2]. Die Kollisionsangriffe auf den MD5 2005/2006, der seit 2009 als gebrochen gilt, sorgten daher auch beim NIST für Unruhe: Sollte es gelingen, die Hashverfahren des SHA-1 oder SHA-2 zu brechen, wären Schlüsselzertifikate und digitale Signaturen nicht zu retten – denn es stand kein auf einem anderen Prinzip beruhendes Hashverfahren zur Verfügung, mit denen die Signaturen hätten erneuert werden können.

Daher startete das NIST 2007 eine neue Standardisierungsinitiative für einen SHA-3.

Der Wettbewerb

Am 02.11.2007 lobte das NIST einen Standardisierungswettbewerb für einen neuen Hash-Standard als Nachfolger des SHA-2 aus, der nicht auf dem Damgård-Merkle-Prinzip beruhen sollte. Der Ablauf des Wettbewerbs orientierte sich an dem Advanced Encryption Standard (AES) [3]: Ein mehrstufiges Auswahlverfahren, bei dem Algorithmenvorschläge eingereicht, fachöffentlich begutachtet und ausgewählt werden sollten.

Bis zum 31.10.2008 wurden von Kryptographen aus der ganzen Welt 64 Vorschläge eingereicht – drei Mal so viele wie beim AES-Wettbewerb. 51 Algorithmen wurden für die erste Bewertungsrunde zugelassen, die am 10.12.2008 begann und bis Juli 2009 dauerte. In die zweite Bewertungsrunde schafften es ganze 14 Kandidaten; eineinhalb Jahre später, am 09.12.2010, wurden die fünf Finalisten – BLAKE, Grostel, JH, Keccak und Skein – vom NIST bekannt gegeben.

Nach einer intensiven, knapp zweijährigen Prüfung und Analyse der verbleibenden Verfahren fiel die Wahl des NIST am 02.10.2012 auf den Algorithmus Keccak [4], entwickelt von den vier Kryptologen Guido Bertoni, Joan Daemen, Michaël Peeters und Gilles Van Assche. Joan Daemen hatte bereits Erfahrung mit dieser Ehrung: Er ist einer der Entwickler des Verschlüsselungsstandards AES (ursprünglich unter dem Namen *Rijndael* bekannt), der im Oktober 2000 vom NIST zum DES-Nachfolger gekürt wurde [3].

Keccak wird nun vom NIST als neuer SHA-3 standardisiert.

Fazit

Das neue Verfahren schafft nicht nur einen „Sicherheitspuffer", falls es in naher Zukunft gelingen sollte, SHA-1 oder SHA-2 zu brechen, sondern hat auch durch den intensiven fachöffentlichen Auswahlprozess die Kenntnisse über angriffsresistente Prinzipien in Hashalgorithmen erheblich vertieft.

Beunruhigend ist allein, dass bis heute die meisten Produkte den SHA-1 verwenden, und nur sehr wenige den SHA-2 zumindest als Rückfalloption enthalten. Einige Lösungen setzen sogar immer noch den bereits seit den späten 90er Jahren „angeschlagenen" und inzwischen komplett gebrochenen MD5 ein.

Ein sicherer Standard hilft allerdings nur, wenn Hersteller ihn auch in ihren Produkten implementieren. Immerhin gibt die Tatsache, dass sich der SHA-3 besonders effizient in Hardware realisierten lässt, Anlass zur Hoffnung. Dabei lohnt bereits der Wechsel von SHA-1 zu SHA-2: der Sicherheitsgewinn ist erheblich. Denn ab einer RSA-Schlüssellänge von ca. 1.500 bit bzw. einer DSS-Schlüssellänge von 168 bit ist der SHA-1 bereits kryptographisch das schwächste Glied.

Literatur

[1] Dobbertin, Hans: *Digitale Fingerabdrücke*, DuD 2/1997, S. 82-87.

[2] Fox, Dirk: *Secure Hash Algorithm (SHA)*. Gateway, DuD 4/2005, S. 226.

[3] Fox, Dirk: *Advanced Encryption Standard (AES)*. Gateway, DuD 10/1999, S. 598.

[4] Bertoni, Guido; Daemen, Joan; Peeters, Michaël; Van Assche, Gilles: *The Keccak sponge function family*, 2011. http://keccak.noekeon.org/specs_summary.html

[5] NIST: *Secure Hash Standard (SHS)*. FIPS PUB 180-4, März 2012. http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf