Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
National Cyber Security Centre NCSC

Rolf Oppliger

4. August 2010
5. August 2020 (aktualisiert)

Technologiebetrachtung

Kollisionsresistenz und Brechung kryptografischer Hashfunktionen

1 Einleitung

In den Medien wird immer wieder über die Brechung von kryptografischen Hashfunktionen (z.B. MD5, SHA-1, …) berichtet. Dabei ist nicht immer klar, was Gegenstand der Brechung ist bzw. was die Implikationen sind. Im Rahmen dieser Technologiebetrachtung wird kurz aufgezeigt, was eine kryptografische Hashfunktion ist, welche spezifischen Eigenschaften sie aufweist, was unter einer Brechung zu verstehen ist, was die Implikationen sind und was man aus applikatorischer Sicht allenfalls dagegen tun kann.

Die Aktualisierung betrifft vor allem den in Abschnitt 3 erwähnten SHAttered-Angriff bzw. dessen Auswirkung auf SHA-1, sowie das Entfernen des Vorschlages, mehrere Hashfunktionen kombiniert einzusetzen.

2 Kryptografische Hashfunktionen

Kryptografische Hashfunktionen stellen Kompressionsfunktionen dar, die – in Ergänzung zu ihrer Kompressionseigenschaft – noch verschiedene andere Eigenschaften aufweisen müssen. Insbesondere muss eine solche Funktion h kollisionsresistent sein, d.h. es darf für einen Aussenstehenden mit praktikablem Aufwand nicht möglich sein, zwei Nachrichten x und x‘ zu finden, die unter h abgebildet den gleichen Hashwert h(x) = h(x‘) aufweisen. Dabei wird üblicherweise zwischen schwacher und starker Kollisionsresistenz unterschieden.

- Bei der schwachen Kollisionsresistenz darf es mit praktikablem Aufwand nicht möglich sein, zu einem gegebenen Hashwert h(x) eine zweite Nachricht x‘ ≠ x zu finden, die den gleichen Hashwert h(x) aufweist.
- Demgegenüber darf es bei der starken Kollisionsresistenz mit praktikablem Aufwand nicht einmal möglich sein, zwei beliebige Nachrichten x und x‘ zu finden, die unter der Hashfunktion h abgebildet den gleichen Hashwert h(x) = h(x‘) aufweisen.

Man beachte, dass es aufgrund der Kompressionseigenschaft der Hashfunktion zwar immer Kollisionen geben muss, dass es aber mit praktikablem Aufwand nicht möglich sein darf, solche zu finden. Eine Möglichkeit, Kollisionen zu finden, stellt in jedem Fall die vollständige Suche dar, d.h. man erzeugt eine sehr grosse Zahl von zufälligen Nachrichten

und sucht nach Kollisionen unter den entsprechenden Hashwerten. Bei einer Hashfunktion, die Hashwerte der Länge n Bit erzeugt, wird man nach 2^n Versuchen mit hoher Wahrscheinlichkeit eine zweite Nachricht gefunden haben, die den gleichen Hashwert aufweist, wie eine vorgegebene Nachricht. Wenn man nur zwei beliebige Nachrichten sucht, die unter der Hashfunktion abgebildet den gleichen Hashwert aufweisen, wird man – aufgrund des Geburtstag-Paradoxons der Wahrscheinlichkeitstheorie – im Schnitt bereits nach $2^{n/2}$ Versuchen erfolgreich sein. Deshalb verlangt man bei kryptografischen Hashfunktionen meist eine minimale Länge der erzeugten Hashwerte von 160 Bit. Die vollständige Suche nach einer Kollision hat dann einen Aufwand von $2^{160/2} = 2^{80}$.

Obwohl es in der Praxis meist ausreichend wäre, schwach kollisionsresistente Hashfunktionen einzusetzen, verlangt man für solche Funktionen meist starke Kollisionsresistenz. Sobald für eine kryptografische Hashfunktion algorithmisch eine Kollision mit einem kleineren Aufwand als mit der vollständigen Suche gefunden wird, gilt die Funktion als gebrochen. Entsprechende Resultate sind für MD5 und SHA-1 publiziert und haben in der internationalen Forschung eine Suche nach effizienten Kollisionssuchalgorithmen auch für andere Hashfunktionen ausgelöst.

3 Implikationen

Die Brechung einer kryptografischen Hashfunktion bedeutet, dass die zur Diskussion stehende Hashfunktion nicht mehr als stark kollisionsresistent angenommen werden kann. Dabei ist es unerheblich, ob der gefundene Kollisionssuchalgorithmus praktikabel ist. Im Falle von SHA-1 hat der derzeit effizienteste Algorithmus z.B. einen Aufwand von 2^{63} (statt 2^{80}) und liegt damit immer noch deutlich über dem Aufwand einer vollständigen Schlüsselsuche für DES.

Die Tatsache, dass eine kryptografische Hashfunktion nicht mehr als stark kollisionsresistent angenommen werden kann, bedeutet, dass ein Angreifer mit einem Aufwand, der kleiner ist als die vollständige Suche, zwei Nachrichten finden kann, die den gleichen Hashwert aufweisen. Er könnte dann eine Nachricht digital signieren lassen und mit der Signatur und einer zweiten Nachricht vor den Richter treten, um Gültigkeit dieser Signatur für die zweite Nachricht einzufordern. Mit Hilfe der heute bekannten Kollisionssuchalgorithmen kann der Angreifer meist nur zwei zufällige Nachrichten finden. Damit lässt sich der skizzierte Angriff nicht durchführen. Um diesen Angriff wirklich durchzuführen, muss der Angreifer zwei Nachrichten erzeugen, die beide sinnvoll sind und von denen wenigstens eine harmlos wirkt. Ein entsprechender Angriff (SHAttered[1]) ist 2017 für SHA-1 und zwei PDF-Dokumente demonstriert worden. Er hat das faktische Ende von SHA-1 eingeleitet.

Letztlich hängt die Frage, ob ein Angriff möglich und realistisch ist, auch vom applikatorischen Umfeld ab. So werden kryptografische Hashfunktionen oft in Konstruktionen eingesetzt, die solche Angriffe a priori ausschliessen. Wird z.B. eine kryptografische Hashfunktion zur Abbildung von Passwörtern und deren „sicheren“ Speicherung in Passwortdateien eingesetzt, dann stellen Kollisionen kein grosses Problem dar (genutzt wird dann primär die Einweg-Eigenschaft der Hashfunktion). Auch die HMAC-Konstruktion, die in vielen kryptografischen Sicherheitsprotokollen im Internet (z.B. IPsec, SSL/TLS, …) eingesetzt wird, um Nachrichten zu authentifizieren, gilt als resistent gegenüber Kollisionsangriffen auf die eingesetzte Hashfunktion.

[1] https://shattered.io

4 Schlussfolgerungen und Ausblick

Aufgrund des Gesagten muss vom Einsatz von als gebrochen geltenden kryptografischen Hashfunktionen (insbesondere MD5 und SHA-1) grundsätzlich abgeraten werden. Wie kritisch der Einsatz einer solchen Hashfunktion aber wirklich ist, hängt im Einzelfall auch von der Applikation ab. In jedem Fall ist der Einsatz alternativer Hashfunktionen angebracht. Als Alternativen zu MD5 und SHA-1 bieten sich insbesondere die Hashfunktionen aus der SHA-2-Familie (insbesondere SHA-224, SHA-256, SHA-384 und SHA-512[2], wobei sich die Zahl hinter der Abkürzung SHA auf die jeweilige Länge des erzeugten Hashwertes bezieht) oder SHA-3/Keccak an. Weil diese Funktionen längere Hashwerte erzeugen, sind sie auch resistenter gegenüber Kollisionsangriffen. Der gleichzeitige Einsatz verschiedener Hashfunktionen ist zwar in vielen Applikationen und Standards vorgesehen, bietet aber unter Umständen nur einen marginalen Sicherheitsgewinn. Vor solchen Konstruktionen ist deshalb eher abzuraten.

Abkürzungen

DES	Data Encryption Standard
HAMC	Hashed MAC
IPsec	IP Security
MAC	Message Authentication Code
MD5	Message Digest Algorithm 5
NCSC	National Cyber Security Centre
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security

[2] SHA-512 gibt es noch als SHA-512/224 und SHA-512/256, wobei die zweite Zahl die Bitlänge des gekürzten SHA-512-Hashwertes angibt.