Zur Sicherheit kryptographischer Hashfunktionen und digitaler Signaturen

Stefan Lucks, Universität Mannheim & Rüdiger Weis, cryptolabs Amsterdam, 16. Märtz 2005

In den letzten Monaten wurden bedeutende Fortschritte bei der Analyse von kryptographischen Hashfunktionen gemacht. Hierbei wurden die immer noch in vielen Anwendungen genutzten Hashfunktionen MD4 und MD5 praxisrelevant gebrochen. Besonders beunruhigend sind aber die aktuellen Ergebnisse bezüglich SHA-1 – auch und gerade mit Bezug auf die Fälschungssicherheit digitaler Signaturen. Wir möchten daher die folgenden Konsequenzen anregen:

Beschränkung des Verwendungszeitraums
Im Zusammenhang mit dem deutschen Signaturgesetz werden kryptographische Algorithmen üblicherweise für einen Zeithorizont von sechs Jahren „als geeignet angesehen". Da die Analyse und Entwicklung kryptographischer Hashfunktionen zur Zeit extrem im Fluss sind und fast täglich neue Ergebnisse gemeldet werden, ist dies zu lang. Kryptographische Hashfunktionen sollten für nicht mehr als drei Jahre „als geeignet" gelten und entsprechend regelmässig re-evaluiert werden.

MD4 und MD5 nicht mehr verwenden!
Im Bereich digitaler Signaturen ist die Verwendung von MD5 (oder gar MD4) auf keinen Fall mehr zu rechtfertigen, wobei im Kontext des deutschen Signaturgesetzes MD4 und MD5 ohnehin nicht als „geeignet" gelten . William Burr vom US-amerikanischen National Institute of Standards and Technology (NIST) mahnte bereits im Februar 2005: „*If by some chance you are still using MD5 in certificates or for digital signatures, you should stop.*" [Ol05]

Gültigkeit bereits geleisteter Signaturen prüfen!
Sogar die Gültigkeit bereits geleisteter digitaler MD5-basierter Signaturen sollte als fraglich betrachtet werden, falls nicht bereits unter Einsatz einer anderen Hashfunktion nachsigniert wurde.

Auf die Verwendung von SHA-1 möglichst verzichten!
Ein im Februar 2005 von einem chinesischen Autorenteam [WYY05] angegebener Kollisionsangriff auf SHA-1 ist mit 2^{69} Rechenoperationen zunächst nur für extrem gut ausgestattete und hoch motivierte Angreifer machbar. Trotzdem sei auch hier aus einer ganzen Reihe von Gründen zur geordneten Migration aufgefordert.

So betreffen die aktuellen Fortschritte bei der Analyse von Hashfunktionen gerade die Gruppe der auf MD4 basierenden Hashfunktionen, zu der leider auch SHA-1 gehört. Weiterhin hat sich auch das Merkle-Damgård Design für Hashfunktionen ebenfalls als fragil erwiesen [Jo04]. Wegen der weiteren Verbesserung der Effizienz von Rechnern („Gesetz von Moore") werden 160-bit Hashfunktionen in wenigen Jahren ohnehin obsolet sein. Soweit möglich (weil eine Signatur-Applikation die Verwendung alternativer Hashfunktionen erlaubt), sollte SHA-1 nicht mehr zum Signieren neuer Dokumente verwendet werden, sondern RIPEMD-160 oder die Familie der SHA-2 Funktionen (siehe unten).

Die Sicherheit bereits geleisteter Unterschriften wird durch die aktuellen Angriffe auf SHA-1 nicht in Frage gestellt, es sei denn Angreifer kannten diese Techniken schon länger und haben sie in der Vergangenheit bereits benutzt.

Es gibt Alternativen zu SHA-1 (siehe unten), die zum Glück für digitale Signaturen in Deutschland auch von den zuständigen Stellen als „vertrauenswürdig" eingestuft wurden.

Die Trusted Computing Group (TCG) hat, trotz jahrelanger Warnungen, bei der Spezifikation ihrer „trusted“ Plattform eine derartige Weitsicht leider vermissen lassen und setzte ausschließlich auf SHA-1.

Standardisierte Kurzfrist-Alternativen: SHA-2 und RIPEMD-160

Der neue NIST-Standard SHA-2 [NI02] definiert eine ganze Reihe von Funktionen mit längerer Hashwertlänge: zwischen 224 bit (SHA-224) und 512 bit (SHA-512). Leider gibt es bisher kaum Analysen der Sicherheit dieser Hashfunktionen. Analog zum Verfahren bei SHA-0 und SHA-1, stammt das Design von der NSA und wurde nicht ausreichend dokumentiert. Gilbert und Handschuh [GH03] zeigten, dass die SHA-2 Hashfunktionen eine Reihe von bei SHA-1 und MD4 möglichen Angriffstechniken zwar sehr widerstandsfähig sind – aber auch, dass die SHA-2 Hashfunktionen unangenehm fragil sind. Dies bedeutet konkret, dass bereits kleinste Änderungen der Hashfunktionen dramatische Auswirkungen die Sicherheit des Verfahrens haben. Es erscheint kryptographisch höchst wünschenswert, dass kleine Änderungen nur moderate Auswirkungen auf die Sicherheit der Hashfunktion haben. Dennoch sind die Hashfunktionen des SHA-2 Standards eine mögliche kurzfristig Alternativen zu SHA-1, da bisher noch keinen Angriff gegen diese Funktionen veröffentlicht wurden. Eine weitere Alternative ist RIPEMD-160 [DBP96], eine europäische Hashfunktion gegen die bisher auch noch kein Angriff bekannt wurde. Wenn verfügbar, sollten deshalb ab sofort zum Signieren digitaler Dokumente RIPEMD-160 oder SHA-256 verwendet werden, statt SHA-1 (oder gar MD4 oder MD5).

Mittelfristige Alternativen

Auch die Funktionen der SHA-2 Familie sowie RIPEMD-160 basieren letztlich auf MD4. Der Vorgänger RIPEMD von RIPEMD-160 wurde in jüngerer Zeit ebenfalls gebrochen. Das lässt auch für die Sicherheit von SHA-2 und RIPEMD-160 Schlimmes befürchten. Mittel- und langfristig werden neue, auf anderen Designprinzipien basierende Hashfunktionen gebraucht (s.a. [W00], [We05]), die das Design von MD4 und sogar das Designprinzip von Merkle und Damgård vermeiden [Lu04]. Interessante Ansätze sind beispiesweise Tiger [AB96] und vor allem der aus dem europäischen NESSI-Projekt stammede Whirlpool [BR00]. Wegen der bisher nicht ausreichend durchgeführten kryptographischen Analysen möchten wir jedoch einen kurzfristigen Einsatz dieser Funktionen nicht uneingeschränkt empfehlen.

Die Suche nach einer langfristigen Lösung

Um in einigen Jahren zu neuen, gut untersuchten und öffentlich dokumentierte Hashfunktionen zu kommen, bietet sich ein Wettbewerb um die Findung geeigneter Standard-Hashfunktionen an, analog zu dem sehr erfolgreichen AES-Prozess für eine Standard-Blockchiffre. Bis zu einem Abschluss dieses Projektes sollte man sich mit den angeregten Zwischenlösungen behelfen.

Literatur

[AB96] Anderson, R., Biham, E., Tiger: A Fast New Hash Function, Fast Software Encryption – FSE'96, LNCS 1039, Springer-Verlag, 1996.
[BR00] Barreto, P., Rijmen, V., The Whirlpool Hashing Function, First open NESSIE Workshop, Leuven, Belgium, 13-14 November 2000.
[DBP96] Dobbertin, H., Bosselaers, A., Preneel, B., ``RIPEMD-160, a strengthened version of RIPEMD,'' Fast Software Encryption 1996, LNCS 1039, D. Gollmann, Ed., Springer-Verlag, 1996, pp. 71-82.
[Jo04] Joux, A., Multicollisions in iterated hash functions, application to cascaded constructions. Crypto 04, LNCS 3152, pp. 306-316.
[Lu04] Lucks, S., Design Principles for Iterated Hash Functions, Cryptology ePrint Archive: Report 2004/253.
[NI93] National Institute of Standards and Technology (NIST), FIPS180-1, SECURE HASH STANDARD,
[NI02] NIST, "FIPS 180-2: Secure Hash Standard (SHS)", August 2002 (change notice: February 2004).
[Ol05] Olsen, F., NIST moves to stronger hashing, Federal Computer Week, Feb. 7, 2005.
[We00] Weis, R., “Cryptographic Protocols and Algorithms for Distributed Multimedia Systems” ,PhD Thesis, 2000.
[We05] Weis, R., Hash Problems, CCC Datenschleuder, 2005.
[WL05] Weis, R., Lucks, S., “Hash Funktionen gebrochen”, Datenschutz und Datensicherheit, Dud 2005.
[WYY05] Wang, X., Yin, Y., Yu, X., Collision Search Attacks on SHA-1. http://theory.csail.mit.edu/~yiqun/shanote.pdf