06.01.2009 13:06

Jürgen Schmidt

Hash mich, die zweite

Konsequenzen der erfolgreichen Angriffe auf MD5

Ende 2008 gelang einem internationalen Forscher-Team ein Aufsehen erregender Angriff auf MD5: Sie missbrauchten die Unterschrift einer Zertifizierungsstelle, um sich selbst ein Zertifikat für eine Zertifizierungsstelle auszustellen. Mit dem hätten sie sich beliebige Zertifikate erstellen können, die jeder Browser als echt akzeptiert hätte. Damit demonstrierten sie eindrucksvoll, wie unsicher der immer noch an vielen Stellen eingesetzte Hash-Algorithmus MD5 ist.

Mit Hilfe eines Clusters von 200 Playstation-3-Systemen konnten die Forscher innerhalb von zwei Tagen zwei gültige Zertifikatsanträge mit vorgegebenen Datenfeldern erstellen, die denselben Hashwert ergaben. Sie variierten dabei lediglich den Inhalt in unwichtigen Feldern, wie den Netscape Kommentarerweiterungen. Dann ließen sie sich den ersten Antrag, der auf eine Domain in ihrem Besitz ausgestellt war, von der Zertifizierungsstelle Rapid-SSL unterschreiben. Die digitale Unterschrift setzten sie anschließend unter das zweite Zertifikat, das die Identität der fiktiven Zertifizierungsstelle "MD5 Collisions Inc. (http://www.phreedom.org/md5)" bestätigte. Da es denselben Hashwert wie das signierte Original hat, kann kein Programm die Fälschung erkennen.

Diese Vorgehensweise entspricht einem sogenannten Kollisionsangriff. Dabei kann der Angreifer sowohl die später präsentierte Fälschung als auch das Original vor der Unterschrift so lange manipulieren, bis er zwei Exemplare hat, die denselben Hashwert ergeben.

Davon zu unterscheiden ist der so genannten Pre-Image-Angriff. Dabei ist ein Original -- also beispielsweise ein bereits digital signiertes Dokument -- fest vorgegeben. Der Angreifer will dann ein zweites Dokument erstellen, das nicht nur den gewünschten Inhalt hat, sondern auch denselben Hashwert ergibt. Derartige Pre-Image-Angriffe sind um viele Größenordnungen aufwendiger; der

Artikel **Hash mich, Konsequenzen der erfolgreichen Angriffe auf SHA-1[1]** erklärt das genauer. Bislang gibt es keine realistischen Szenarien für Pre-Image-Angriffe auf MD5.

Mit Hilfe dieser Fakten kann man schon recht konkret die konkreten Gefahren ableiten, die der aktuelle Angriff aufgezeigt hat. Von dem gefälschten MD5-Collisions-CA-Zertifikat geht keine echte Bedrohung aus. Um es für Angriffe zu missbrauchen, müsste man dessen geheimen Schlüssel haben, und den halten die Forscher unter Verschluss. Außerdem haben sie es freiwillig mit einem Ablaufdatum in der Vergangenheit versehen, sodass man damit keine gültigen Zertifikate erstellen könnte.

Der Angriff lässt sich auch nicht ohne weiteres wiederholen. Die Zertifizierungsstelle RapidSSL verwendet mittlerweile kein MD5 mehr; die anderen werden hoffentlich bald folgen. Außerdem nutzte der Hack bestimmte Eigenschaften des Zertifizierungsvorgangs aus, wie die, dass die Seriennummern der ausgestellten Zertifikate einfach aufsteigend gewählt wurden, also vorhersehbar waren. Das bedeutet, dass ein Nachahmer zunächst einiges an eigener Recherche und Arbeit investieren müsste, um den Angriff zu wiederholen. Vorsichtig geschätzt bräuchte er dazu wenigstens einige Monate.

Man kann auch eine SSL-gesicherte Übertragung nicht automatisch direkt belauschen, nur weil einer der Partner ein MD5-signiertes Zertifikat einsetzt. Ein typisches Angriffsszenario kann man sich eher so vorstellen: Um beispielsweise Kreditkartendaten aus einer Übertragung an eine SSL-gesicherte Seite eines Webshops auszuspionieren, müsste der Angreifer einen Server aufsetzen, der sich als der Shop ausgibt und sich dabei mit einem gefälschten Zertifikat ausweist. Dafür gibt es bereits fertige Tools. In einem zweiten Schritt leitet der Angreifer die Verbindung des Opfers zum Webshop auf seinen Proxy-Server um. Dies kann beispielsweise in einem lokalen oder drahtlosen Netz via ARP-Spoofing passieren. In größerem Maßstab kämen wohl eher DNS-Spoofing oder Pharming zum Einsatz, was allerdings **verwundbare DNS-Server[2]** erfordert.

Konsequenzen

Da keine akute Gefahr besteht, gibt es keinen Grund zur Panik. Leider gibt es allerdings auch keinen Weg, das Problem einfach und nachhaltig aus der Welt zu schaffen. Man kann nur diesen Angriff zum Anlass nehmen, um MD5 endgültig das Vertrauen zu entziehen und so schnell wie möglich auszumustern. Als allererstes sind da die Zertifizierungsstellen gefragt, die ab

sofort keine Zertifikate mehr mit MD5 unterschreiben sollten. Des weiteren wäre es sehr wünschenswert, wenn sie von sich aus die Eigentümer MD5-signierter Zertifikate ansprechen und zu einem kostenlosen Umstieg auf SHA-1 animieren würden. Auf SHA-1 gibt es zwar ebenfalls **erste Angriffe[3]**, die sind allerdings noch nicht wirklich praxisrelevant. Der designierte Nachfolger SHA-2 ist noch nicht reif für den Einsatz in der Praxis und **SHA-3[4]** muss erst noch gekürt werden.

Als Besitzer eines MD5-Zertifikats sollte man – auch wenn kein akuter Grund zur Sorge besteht – möglichst bald ein neues Zertifikat beantragen. Jedes MD5-Zertifikat weniger ist ein Schritt näher zum kompletten Verzicht auf MD5. Und als Anwender kann man eigentlich nur hoffen, dass die Hürden für einen erfolgreichen Angriff hoch genug sind. Denn eine wirklich endanwendertaugliche Möglichkeit, sich vor derartigen Angriffen auf die Verschlüsselung zu schützen gibt es derzeit nicht. Die FAQs auf der nächsten Seite geben immerhin ein paar Tipps für Experimente.

FAQs

- *Wie finde ich heraus, ob ein Zertifikat gefälscht wurde?*

Es gibt leider keine allgemein gültige Methode, ein derart gefälschtes Zertifikat von einem echten zu unterscheiden. Sie alle haben gemeinsam, dass sie von einer CA ausgestellt wurden, die MD5 verwendet. Leider haben sie das auch mit etwa 30 Prozent der echten Zertifikate gemein, sodass man daraus allein keinen Angriff ableiten kann.

- *Kann ich erkennen, ob ein Zertifikat MD5 einsetzt?*

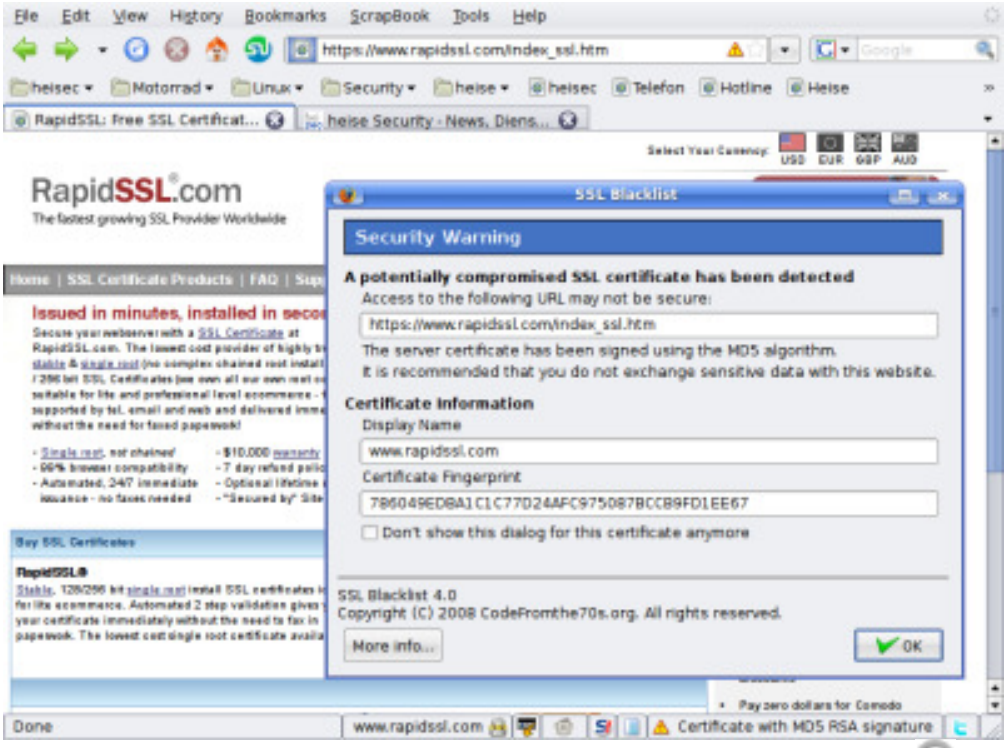
Ja, das steht unter "Certificate Signature Algorithm" in den Eigenschaften des Zertifikats. Beachten Sie jedoch, dass das Zertifikat selbst gar kein MD5 einsetzen muss. Es genügt, wenn eine der Zertifizierungsstellen MD5 verwendet hat und damit kompromittierbar wäre. Mit einer gefälschten Zwischen-CA könnte man dann durchaus ein SHA-1-Zertifikat beglaubigen.

Eine Möglichkeit, das automatisch zu erledigen, bietet das Firefox-Plugin **SSL Blacklist[5]**. Es gibt eine Warnung aus, wann immer ein Zertifikat durch das MD5-Problem gefälscht sein

Erst in den Eigenschaften des Zertifikats findet sich der verwendete Hash-Algorithmus

Angriff zurückzuführen sind.

könnte. Dumm dabei ist, dass man eine Menge Warnungen erhält, die in fast allen Fällen nicht auf einen



Die Firefox-Erweiterung SSL-Blacklist warnt vor MD5-Signaturen.

- *Kann ich mich denn gegen Angriffe mit gefälschten Zertifikaten überhaupt irgendwie schützen?*

Gute Chancen dazu bietet derzeit die Firefox-Erweiterung **Perspectives[6]**. Sie setzt darauf, dass ein Angriff auf eine https-verschlüsselte Übertragung in der Regel lokal begrenzt ist. Das Perspectives-Plugin befragt mehrere sogenannte "Notare", welches Zertifikat sie denn sehen. Wenn die für denselben Server ein anderes Zertifikat sehen, ist die Wahrscheinlichkeit hoch, dass da irgendwas faul ist -- also beispielsweise die eigene Verbindung auf einen gefälschten Server umgeleitet wurde. Näheres beschreibt die heise-Security-Meldung **"Ehrenamtliche Notare" als Konkurrenz zu VeriSign[7]**.

Wer experimentierfreudig ist, kann die Zertifizierungsstellen Browser, denen der Browser vertraut, entfernen und anfangen, jedes wichtige Zertifikat einmal von Hand zu überprüfen und eine passende Ausnahme dazu zu erstellen. Die praktischen Konsequenzen sind jedoch bislang nicht bekannt – da sind Sie auf sich selber gestellt.

- *Besteht nicht die Gefahr, dass kriminelle Banden oder Geheimdienste sich auf diesem Weg bereits ein gefälschtes CA-Zertifikat besorgt haben?*

Das lässt sich leider nicht ausschließen. Allerdings muss man davon ausgehen, dass zumindest Geheimdiensten auch andere Optionen zur Verfügung stehen, um an ein Zertifikat einer Zwischenzertifizierungsstelle heran zu kommen.

- *Ich habe ein Web-Server-Zertifikat, das MD5 als Hashverfahren verwendet. Sind meine Kunden deshalb gefährdet?*

Nicht mehr als bei anderen Zertifikaten auch. Trotzdem sollten Sie bei Ihrer CA nach einem kostenlosen Upgrade auf eine SHA-1-Signatur fragen, um aufmerksame Kunden nicht unnötig zu verunsichern und die Abschaffung von MD5 zu beschleunigen.

- *Welche CAs außer RapidSSL nutzen noch MD5?*

Die Veröffentlichung der Forscher listet folgende CAs auf:

1. RapidSSL C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1
2. FreeSSL C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Network Applications
3. TC TrustCenter AG C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in Data Networks GmbH, OU=TC TrustCenter Class 3 CA/emailAddress=certificate@trustcenter.de
4. RSA Data Security C=US, O=RSA Data Security, Inc., OU=Secure Server Certification Authority
5. Thawte C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA/emailAddress=premium-server@thawte.com
6. verisign.co.jp O=VeriSign Trust Network, OU=VeriSign, Inc., OU=VeriSign International Server CA - Class 3, OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign

Es ist uns nicht bekannt, ob diese Liste zutreffend und vollständig ist.

- *Sind die Extended Validation Zertifikate, die die Browser mit einem grünen Symbol kennzeichnen, auch betroffen?*

Nein. Gemäß der **Spezifikation für EV-SSL[8]** dürfen die CAs keine Zertifikate mit dem Hashverfahren MD5 ausstellen. Außerdem können nur anerkannte EV-CAs EV-Zertifkate unterschreiben. Allerdings gestattet es ihnen die EV-Spezifikation, noch bis Ende 2010 neue Root-CA-Zertifikate mit MD5 zu erstellen. Angesichts der Tatsache, dass die dann oft 20 Jahre gültig sind, ist das eine sehr optimistische Herangehensweise.

Siehe dazu auch:

- **MD5 considered harmful today, Creating a rogue CA certificate[9]**,

Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger

- **Hash mich, Konsequenzen der erfolgreichen Angriffe auf SHA-1[10]**, Artikel auf heise Security

---

URL dieses Artikels:
http://www.heise.de/security/artikel/121148

Links in diesem Artikel:
[1] http://www.heise.de/security/Konsequenzen-der-erfolgreichen-Angriffe-auf-SHA-1--/artikel/56555
[2] http://www.heise.de/security/Erste-Angriffe-auf-Nameserver-beobachtet-Update--/news/meldung/113366
[3] http://www.heise.de/security/Konsequenzen-der-erfolgreichen-Angriffe-auf-SHA-1--/artikel/56555
[4] http://www.heise.de/security/Neue-Hashes-braucht-das-Land--/news/meldung/118352
[5] http://codefromthe70s.org/sslblacklist.aspx
[6] http://www.cs.cmu.edu/~perspectives/
[7] http://www.heise.de/security/Ehrenamtliche-Notare-als-Konkurrenz-zu-VeriSign--/news/meldung/114929
[8] http://www.cabforum.org/documents.html
[9] http://www.win.tue.nl/hashclash/rogue-ca/
[10] http://www.heise.de/security/Konsequenzen-der-erfolgreichen-Angriffe-auf-SHA-1--/artikel/56555
