Secorvo Security News
Februar 2005

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 2, 4. Jhrg. 2005
Stand 24. Februar 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: Wer dreimal lügt...

Wieder einmal wird eine (Krypto-)Sau durchs Dorf getrieben. Diesmal haben die Hashfunktionen Jagdsaison. Zum zweiten Mal steht der „Secure Hash Standard“ (SHA) des NIST auf der Abschussliste: Schon 2004 geisterten Gerüchte durch die Gazetten, SHA sei gebrochen. Tatsächlich waren Schwachstellen der ursprünglichen, vom NIST bereits 1995 ersetzten Version SHA-0 gefunden worden. „Hilfe, der Wolf kommt!“ – der erste Fehlalarm.

Jetzt hat es jedoch den SHA-1 erwischt. Bruce Schneier löste am 15.02.2005 mit einem Eintrag in seinem Blog („SHA-1 has been broken“) die zweite Welle der „Hilfe, der Wolf kommt!“-Alarme aus. Vier chinesische Forscher hatten ein kryptographisch bemerkenswertes Ergebnis angekündigt: Mit einem Aufwand von 2^{69} sei es möglich, SHA-1-Kollisionen zu finden. Dies ist allerdings ein Aufwand, der deutlich jenseits eines praktikablen Angriffs liegt – und nur zwei beliebige, keineswegs sinnvolle Zeichenfolgen liefert, die denselben Hash-Wert besitzen. Zweiter Fehlalarm.

Die Erfahrung der vergangenen Jahre hat jedoch gezeigt, dass ein solcherart angeschossener Algorithmus schon bald tatsächlich erlegt sein kann. Fatal wäre allerdings, wenn der SHA das Schicksal des Hashalgorithmus MD5 teilen würde: Auch beim MD5 gab es zwei Fehlalarme; der dritte Alarm Mitte 2004, nach dem Kollisionen mit einem Workstation-Cluster in weniger als einer Stunde konstruiert werden können, wurde überhört: Noch immer verwenden zahlreiche kryptographische Anwendungen und Produkte den MD5 als Hash-Algorithmus.

Sollte ein dritter, berechtigter „Hilfe, der Wolf kommt!“-Alarm beim SHA-1 ungehört verhallen, droht allerdings ein GAU – denn zum SHA-1 gibt es derzeit fast keine standardisierte und vor allem in Anwendungsstandards wie z. B. S/MIME berücksichtigte Alternative.

Der einzige Unterschied zwischen dieser Geschichte und dem Gleichnis mit dem Wolf: Die „Hilfe“-Rufer würden überleben.

1 Security News

1.1 SHA-1 – Gebrochen?

Ausgelöst durch einen Weblog-Eintrag des Krypto-Experten Bruce Schneier verbreitete sich am 15.02.2005 wie ein Lauffeuer die Nachricht, dass es einem renommierten chinesischen Forscherteam um Xiaoyun Wang gelungen ist, die Krypto-Hashfunktion SHA-1 zu brechen. Die Aufregung ist verständlich, wenn man bedenkt, dass SHA-1 ein zentraler Baustein für PKI-Zertifikate und -Anwendungen wie z.B. digitale Signaturen, SSL oder S/MIME ist.

Das Papier von Wang und Kollegen ist noch nicht öffentlich verfügbar. Soweit die Fakten mittlerweile bekannt sind, bedeutet „gebrochen", dass ein theoretischer Durchbruch gelungen ist: Der Aufwand zum Finden zweier verschiedener Klartexte, die denselben 160-Bit SHA-1-Hashwert besitzen, konnte von 2^{80} für eine Brute-Force-Attacke auf 2^{69} Schritte verringert werden. Letzteres erscheint z.B. im Vergleich mit dem mehr als vier Jahre dauernden „Brute-Forcing" von 2^{64} RC-5 Schlüsseln deutlich jenseits des heute praktisch Machbaren.

Zweifel an der Sicherheit des SHA-1 waren bereits aufgekommen, als auf der Expertenkonferenz Crypto 2004 mehrere Forschergruppen neue Angriffe auf Hashfunktionen vorstellten. Als Reaktion hierauf kündigte das NIST, Urheber des SHA-1, bereits am 25.08.2004 an, spätestens 2010 den SHA-1 zugunsten der designierten Nachfolger SHA-224 bis SHA-512 (jüngster SHA-Standard vom 01.08.2002) auslaufen zu lassen.

Das Dilemma für den Anwender ist, dass derzeit praktisch keine Alternativen zur Verfügung stehen: MD4 und MD5 wurden effektiv gebrochen (siehe auch SSN 12-04), RIPEMD-160 ist kaum verbreitet und nach ähnlichen Prinzipien aufgebaut wie SHA-1 (also eventuell auch ähnlich anfällig), und die jüngeren Algorithmen SHA-224/256/384/512 (auch als „SHA-2" bezeichnet) wurden bislang erst in wenige Produkte integriert.

Handlungsbedarf besteht also, aber Panik ist nicht angezeigt. Selbst wenn die Attacke in Einzelfällen praktisch umsetzbar wäre, erlaubt sie es nicht, einen zweiten Klartext zu finden, der zu einem vorgegebenen Hashwert – z.B. aus einem existierenden CA-Zertifikat – passt, sondern erzeugt „nur" zwei zunächst zufällige Zeichenfolgen so, dass deren Hashwerte (und damit auch die Signaturen) übereinstimmen. Somit sind bereits geleistete Signaturen ohnehin nicht gefährdet.

Am dringlichsten sind die Hersteller von Signaturanwendungen gefordert, alternative Hash-Algorithmen in ihre Produkte aufzunehmen. Als einer der ersten Hersteller hat PGP am 18.02.2005 die Gelegenheit ergriffen, ein Update anzukündigen.

1.2 SigG-Algorithmen

Noch ohne Kenntnis der neuesten Ergebnisse zum SHA-1 gab die RegTP am 02.01.2005 die Übersicht über geeignete Algorithmen nach dem Signaturgesetz bekannt. Wie auch durch das NIST wird darin dem SHA-1 eine (nun möglicherweise zu überdenkende) Lebenszeit bis 2010 gegeben. Zulässige Alternativen als Hashfunktion sind RIPEMD-160 und SHA-2.

1.3 Riskmanagement-Studie

Das Institut für Wirtschafts- und Verwaltungsinformatik von Prof. Dr. Hampe an der Universität Koblenz führt ab dem 24.02. 2005 eine Delphi-Studie zum IT Riskmanagement durch. Ziel dieser Studie ist es, Trends und Entwicklungen im Bereich des IT Risk Managements zu ermitteln. Die Studie richtet sich ausschließlich an Fachexperten, daher ist eine Teilnahme nur mit den folgenden Login-Daten möglich: Kennung: itrm, Passwort: mrti. Für weitere Informationen steht die Projektleiterin, Frau Meletiadou (0261/287-2535) zur Verfügung.

1.4 Neue Schläuche bei RFID

Am 28.01.2005 veröffentlichte ein Forscherteam der Johns Hopkins University

und der RSA Laboratories die – auch praktisch umgesetzte – Analyse eines RFID-Chips von Texas Instruments, der u.a. in Wegfahrsperren häufig eingesetzt wird.

Angesichts der Verwendung eines 40-Bit-Schlüssels, der eine Brute-Force-Suche ermöglicht, ließe sich dies als alter Wein (oder eher Essig) in neuen RFID-Schläuchen abtun. Bemerkenswert daran sind jedoch mehrere Punkte: Die Bereitschaft zur Kooperation des Herstellers (anstelle eines leider häufigen peinlichen Schweigens oder Abstreitens), die von den Autoren beschriebene Black-Box Rekonstruktion des im Chip verwendeten Algorithmus und die Überlegungen, wie man sich als Träger eines RFID-Chips vor unbeabsichtigtem Auslesen der darauf gespeicherten Daten schützen kann. Letzteres könnte eine neue Klasse von Produkten oder Werbe-Giveaways hervorbringen: einfach zu handhabende Faradaysche-RFID-Hüllen – womit sich der Kreis zu den Schläuchen schließt.

1.5 Netfilter IP-Tables 1.3

Das Netfilter-Team um Harald Welte hat am 12.02.2005 die Version 1.3 von iptables freigegeben. Die im Linux Kernel integrierten Funktionen ermöglichen eine stateful Paketfilterung und eine Reihe weiterer (Firewall)-Funktionen. In Version 1.3 wurden Bugs beseitigt und die Performance nochmals verbessert.

1.6 Nessus übernommen

Der verbreitete OpenSource-Scanner Nessus wurde unter die Hoheit von Tenable Network Security als offiziellem Sponsor gestellt. Tenable ist der Hersteller der kostenpflichtigen Windows32-Variante des Security Scanners (NeWT Pro), die kostenfreie Variante NeWT ist auf das lokale Subnetz beschränkt.

Nach einer Benutzerregistrierung kann Nessus weiterhin kostenfrei unter Linux und anderen Unix-Plattformen eingesetzt werden. Allerdings werden aktuelle Plugins von Tenable erst nach einer Wartezeit von sieben Tagen zur Verfügung gestellt. Wer die Plugins sofort einsetzen möchte, muss den „Direct Feed Update Service“ zum Preis von 1.200 $ pro Jahr buchen. Die unter der Gnu Public Licence (GPL) von der Community erstellten Plugins sind auch weiterhin ohne Verzögerung und kostenfrei erhältlich.

1.7 Suse mit EAL 4-Zertifikat

Am 15.02.2005 teilte die atsec information security GmbH mit, dass sie für Suse's Linux Enterprise Server 9 (SLES 9) den Prozess der Evaluierung nach Common Criteria (CC) EAL 4+ abgeschlossen habe und ein entsprechendes Zertifikat folgen werde.

EAL 4+ ist ein hohes Evaluationslevel; diese Stufe wird auch für Chipkarten nach dem Signaturgesetz (SigG) verlangt. Eine fundierte Beurteilung einer CC-Evaluierung ist jedoch nur unter Berücksichtigung des der Prüfung zu Grunde liegende Kriterienkatalogs („Protection Profile“) möglich, in dem die Prüfanforderungen definiert sind.

SLES 9 wurde in diesem Fall gegen das Schutzprofil „Controlled Access Protection Profile (CAPP)“ geprüft, welches insbesondere Anforderungen an die Zugriffskontrolle definiert. Auch Windows 2000 wurde bereits gegen CAPP EAL 4 evaluiert – genau diese Evaluierung führte jedoch vor einigen Jahren zu massiver Kritik an dem Schutzprofil: Bei genauerer Betrachtung gilt es nämlich nicht in üblichen Netzwerk-Umgebungen wie dem Internet („*The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers...*“).

1.8 VoIP Security

Am 07.02.2005 wurde unter der Federführung von Tippingpoint die Voice Over IP Security Alliance (VOIPSA) ins Leben gerufen. Die Gruppe hat sich zum Ziel gesetzt, das Thema Security im Bereich VoIP vorwärts zu bringen.

Vom National Institute of Standards and Technology (NIST) ist seit dem 03.01.2005

ein Whitepaper zum Thema "Security Considerations in Voice over IP Systems" verfügbar. Neben technischen Grundlagen werden insbesondere die Sicherheitsfunktionen der Protokolle und auch die Integration mit weiteren Schutzmechanismen wie Firewalls und VPN dargestellt.

2 Secorvo News

2.1 Secorvo College aktuell

Im April stehen zahlreiche Seminarangebote auf der Agenda von Secorvo College:

- drei aktuelle Seminare zur Systemsicherheit: Sichere E-Mail-Kommunikation (05.-07.04.) Lotus Notes Security (12.-13./14.04.) und Inside Windows Security (19.-20.04.2005), sowie
- eine in Zusammenarbeit mit dem Unternehmen Compass Security Network Computing AG (Schweiz) entwickelte „Hands on" Seminarreihe: Live Hacking Lab (26.-28./29.04.2005) und Web-Application Security (02.-04.05. 2005).

Veranstaltungsprogramme, das vollständige Seminarangebot mit weiteren Terminen und ein Anmeldeformular finden Sie auf den Webseiten von Secorvo College.

2.2 Forensik kompakt

In der kommenden Woche findet das erste Computer Forensik Symposium der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) bei Secorvo in Karlsruhe statt (01.-02.03. 2005). Themen sind die Sichtweisen und Erfahrungen von Staatsanwaltschaft, BKA und betroffenen Unternehmen sowie die Vorstellung von Forensik Tools und deren praktischem Einsatz. Die zahlreichen Anmeldungen versprechen spannende Diskussionen. Für Kurzentschlossene gibt es noch einige wenige freie Plätze.

2.3 DuD – das Programm

Das Programm der Fachkonferenz „Datenschutz und Datensicherheit" (DuD, 18.-19. 04.2005) ist jetzt verfügbar.

3 Veranstaltungshinweise

März 2005	
01.-02.03.	Computer Forensik Symposium 2005 (KA-IT-Si, Karlsruhe)
02.-03.03.	DFN-CERT Workshop (DFN-CERT, Hamburg)
15.-16.03.	D-A-CH Security 2005 (GI/OCG/ BITKOM/SI/TTT, TU Darmstadt)
April 2005	
05.-07.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
05.-08.04.	Sicherheit 2005 (GI, Uni Regensburg)
12.-13.04.	Lotus Notes Security (Secorvo College, Karlsruhe)
14.04.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
18.-19.04.	Datenschutz und Datensicherheit – DuD 2005 (COMPUTAS, Berlin)
19.-20.04.	Inside Windows Security (Secorvo College, Karlsruhe)
26.-28.04.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.04.	Live Hacking Spezial (Secorvo College, Karlsruhe)
Mai 2005	
02.-04.05.	Web-Application Security (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de