Secorvo Security News
November/Dezember 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 5, 1. Jhrg. 2002
Stand 29. November 2002

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

Inhalt

Editorial: Das Dorf, die Sau und die Kryptologie

Nachdem die Veröffentlichung einer neuen, vermeintlich wesentlich effizienteren Methode zur Kryptoanalyse von RSA-Schlüsseln durch Daniel Bernstein im vergangenen Jahr große Verunsicherung ausgelöst hatte, wird derzeit eine neue „Krypto-Sau“ durch‘s Dorf gejagt. Diesmal hat es die symmetrischen Verfahren erwischt.

Schon 2001 war es Ferguson, Schroeppel und Whiting gelungen, den AES als überraschend einfache geschlossene Formel auszudrücken. Dies ist eine beunruhigende Erkenntnis, wenn daraus auch nicht unmittelbar ein Angriff abgeleitet werden konnte. Auf der diesjährigen Welt-Kryptologie-Konferenz „Crypto“ versetzte jedoch ein neuartiger Angriff auf den AES, die „eXtended Sparse Linearization“ (XSL), die Kryptologen-Elite in Aufregung. Als elektronische Vorab-Veröffentlichung kursierte eine diesbezügliche Arbeit von Courtois und Pieprzyk, die die Autoren auf der Konferenz „AsiaCrypt 2002“ Anfang Dezember präsentieren werden.

http://eprint.iacr.org/2002/044

Nachdenklich stimmt weniger der Angriff selbst: Er ist bislang „nur“ ein theoretisches Konzept, und der tatsächliche Aufwand ist mit 2^{200} Operationen so groß, dass er sich zumindest zu Lebzeiten der Autoren nicht testen lassen wird. Der AES könnte gut damit leben – ein Sicherheitsniveau von 2^{200} liegt jenseits des heute Angreifbaren, und das gilt nach Kryptografenschätzungen sicher noch bis weit in das 22. Jahrhundert. Der Ansatz des Angriffs ist jedoch bedenklicher, denn er wirkt auch beim AES-Kandidaten „Serpent“, den alle Experten für den sichersten Algorihmus im Auswahlverfahren hielten.

Wieder ein Beleg, dass die Kryptografie immer für Überraschungen gut ist. Und dass sich die Krypto-Forschung daher nicht auf ihren Erfolgen ausruhen darf. Und – dass auch bei den besten Kryptologen Irren eine menschliche Eigenschaft ist.

1 Security News

1.1 Big Brother Awards

Die 1990 gegründete internationale Menschenrechtsgruppe „Privacy International“ (PI) initiierte im Jahr 1988 die „Big Brother Awards“ als „Oskar für Datenkraken“. Inzwischen wird diese Auszeichnung für besondere Leistungen beim Missbrauch personenbezogener Daten jährlich in 12 Ländern vergeben.

http://www.privacyinternational.org/bigbrother/

In Deutschland organisiert der Bielefelder „Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs“ (FoeBuD e.V.) seit dem Jahr 2000 die Auswahl der Preisträger und die Preisverleihung. Die diesjährigen deutschen Awards wurden am 25.10.2002 in acht Kategorien verliehen. Die Preisträger finden sich unter

http://www.bigbrotherawards.de/

1.2 TCPA

Ziel der im Frühjahr 1999 von Intel initiierten Trusted Computing Platform Alliance (TCPA) ist die Schaffung einer Betriebssystemumgebung, in der durch einheitliche Mechanismen Integrität und Identität überprüfbar sichergestellt werden. Zu den Gründungsmitgliedern gehören IBM, HP, Compaq und Microsoft. Inzwischen haben sich der Initiative mehr als 160 Unternehmen angeschlossen.

http://www.trustedcomputing.org

Die aktuelle Version 1.1b der „Main Specification“ vom 22.02.2002 (frei gegeben im Mai 2002) findet sich unter:

http://www.trustedcomputing.org/docs/main%20v1_1b.pdf (pdf, 1,7 MB)

Durch eine in mehreren Sprachen verfügbare „FAQ“-Liste von Ross Anderson kommt jetzt allerdings Wirbel in das Thema: Er vermutet hinter der Initiative den Versuch, mit in Hardware realisierten kryptografischen Mechanismen zum Digital Rights Management (DRM) die Nutzung manipulierter oder nicht lizenzierter Software und unerwünschter Daten (z.B. MP3-Files) zu kontrollieren sowie Nutzer-Informationen zentral zu registrieren – eine Breitseite auf den Datenschutz mit Zensurpotential.

http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

1.3 Windows 2000 zertifiziert

Im Oktober 2002 hat Microsoft für Windows 2000 die Sicherheitszertifizierung nach den Common Criteria bezüglich des Controlled Access Protection Profile und für Evaluation Assurance Level EAL-4 bestanden.

Hinweise für die erforderliche Konfiguration für einen mit dieser Zertifizierung konformen Betrieb von Windows 2000 gibt:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/w2kccwp.asp

1.4 „Backdoor“ im EFS

Unter Windows 2000 enthält das Encrypted File System (EFS) eine hässliche ungeplante Hintertür, wie die Fachzeitschrift c’t (23/2002, S. 33) berichtet: Bootet man beispielsweise einen mit EFS gesicherten Laptop mit der Startdiskette, kann man hinter dem Rücken des Rechnerinhabers das Zugriffspasswort ändern. Anschließend kann auf EFS-verschlüsselte Dateien frei zugegriffen werden.

Microsoft empfiehlt, diese Aushebelung der integrierten Dateiverschlüsselung in Windows 2000 durch die Verwendung eines höheren Syskey-Modus (2 oder 3) zu verhindern: Dann ist ein zusätzliches Passwort bzw. sogar eine Schlüsseldiskette beim Systemstart erforderlich.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/efs.asp

1.5 Sammelpatch IE 5.x-6.0

Microsoft hat mit dem Siegeszug des Internet Explorers die Browser-Schlacht für sich entschieden: In den meisten Unternehmen genießt der IE heute den Status des Standard-Browsers. Der große Funktionsumfang des IE gibt aus Sicht der IT-Sicherheit allerdings wenig Anlass zur Freude: ActiveX, JScript, VBScript und ActiveScripting eröffnen auch Angreifern großartige Möglichkeiten. Immer wieder werden zudem sicherheitsrelevante Programmierfehler entdeckt und „Exploits" – Programme, die die Nutzung dieser Schwächen exemplarisch vorführen – im Internet veröffentlicht.

Zuletzt gab Microsoft am 20.11.2002 einen aktuellen Sammelpatch für den Internet Explorer heraus, der zahlreiche, z.T. schwere Fehler der Versionen 5.x-6.0 (SP 1) korrigiert:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-066.asp

Software-Updates „hinken" den Entdeckungen findiger Programmierer zwangsläufig hinterher. Dass einige Fehler allerdings auch von dem aktuellen Patch nicht behoben sind, zeigt die von Thor Larholm gepflegte „unpatched"-Liste ungelöster Fehlerreports zum Internet Explorer:

http://www.pivx.com/larholm/unpatched

Eine Online-Prüfung auf von Angreifern nutzbare Konfigurations- und Programmierfehler für den Internet-Explorer findet sich auf den Webseiten der Zeitschrift c't:

http://www.heise.de/ct/browsercheck/e5demo.shtml

Sensibilisierung für die sichere Nutzung des Internet Explorers und Hinweise zur geeigneten Konfiguration bietet auch das von Secorvo erstellte Video „Safer Surfen mit dem Internet Explorer", das seit kurzem verfügbar ist:

http://www.secorvo.de/video

1.6 Mcert gegründet

Am 15.10.2002 wurde vom Präsidium des Branchenverbands Bitkom der Aufbau eines Computer-Notfall-Teams (CERT) beschlossen. Die Finanzierung dieses „Mittelstand-CERTs" übernehmen in den ersten drei Jahren BMWi, BMI, Bitkom sowie sieben Unterstützer aus der Industrie. Mit speziell aufbereiteten Warn- und Schwachstellenmeldungen sowie einer koordinierten Behandlung von Sicherheitsvorfällen und -problemen soll speziell der Mittelstand beim Thema IT-Sicherheit unterstützt werden.

Diese Entscheidung basiert unter anderem auf einer im Auftrag des BMWi erstellten Studie zu „CERT-Dienstleistungen für kleine und Mittlere Unternehmen (KMU)" vom 08.07.2001 (pdf, 479 kB):

http://www.bitkom.org/gbgateinvoker.cfm/Studie_CERT_KMU.pdf?gbAction=gbFileDownload&ObjectID=F93098A0-2DB0-4818-8334CEA5E3FFFB61&DownloadObject=documents&index=1&cacheLevel=0

Die konstituierende Sitzung zum offiziellen Projektstart und der Gründung einer Mcert-Betreiber-GmbH sowie der Berufung eines Mcert-Beirats ist am 03.12.2002 in Berlin geplant.

2 Secorvo News

2.1 Secorvo College aktuell

Alles wird teurer – jedenfalls fast alles. Ein kleines Unternehmen aus Karlsruhe schwimmt gegen den Strom: Wir senken die Teilnahmegebühren für Seminare von Secorvo College durchgängig um ca. 7 %. Denn es ist uns gelungen, Kosten für Druck und Versand unserer Prospekte durch verschiedene Maßnahmen deutlich zu senken. Diese Einsparungen geben wir an Sie weiter: Sie erhalten „schlankere" Post von uns – und sparen bei den Seminargebühren bis zu 140 €.

http://www.secorvo.de/college

2.2 Förderpreis Baden-Württemberg für Secorvo

Am 13.11.2002 wurde Secorvo von Ministerpräsident Erwin Teufel als zweiter Sieger des „Förderpreises des Landes Baden-Württemberg für junge Unternehmen 2002“ für vorbildliche unternehmerische Leistungen ausgezeichnet. Um diesen renommierten Preis hatten sich mehr als 630 Unternehmen aus Baden-Württemberg beworben.

http://www.secorvo.de/presse/pm21-foerderpreis-bw-2002.html

2.3 In neuem Gewand

Seit Ende November hat Secorvo ein neues „Outfit“: Unserem Internetauftritt haben wir eine gründliche Überarbeitung angedeihen lassen. Nicht nur Farbe, Form und Design sind frisch, sondern auch Struktur und Navigation der Seiten wurden neu gestaltet – wir hoffen, zu Ihrem Gefallen und Nutzen. Aber urteilen Sie selbst – wir freuen uns über Ihre Kommentare:

http://www.secorvo.de

2.4 IT-Grundschutz-Auditor

Mitte November 2002 erhielt Stefan Gora, Consultant bei Secorvo, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) seine Lizenz als IT-Grundschutz-Auditor. Herr Gora ist damit berechtigt, IT-Grundschutz-Audits für die Erlangung von IT-Grundschutz-Zertifikaten des BSI durchzuführen sowie IT-Grundschutz-Selbsterklärungen durch ein Testat zu bestätigen.

http://www.secorvo.de/leistungen/grundschutz-audit.html

3 Veranstaltungshinweise

Dezember 2002	
01.-05.12.	AsiaCrypt 2002 (IACR, Otago/NZ)
02.-03.12.	IsSec 2002 (Computas, Berlin)
03.-04.12.	Defense Lab (Live Hacking) (Secorvo College, Karlsruhe)
04.-05.12.	TrustD@y – IT-Sicherheit ist Chefsache (TimeContor, Berlin)
09.-13.12.	ACSAC 2002 (ACSA, Las Vegas)
13.12.	Trust in Electronic Signatures (ETSI, London)
Januar 2003	
15.-17.01.	Omnicard 2003 (inTIME, Berlin)
22.-23.01.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
22.-24.01.	IT-Defense (Cirosec, Leverkusen)
28.-29.01.	PKI – Public Key Infrastrukturen (Secorvo College, Karlsruhe)
30.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)

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

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine automatische Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feed-Back an
redaktion-security-news@secorvo.de