Secorvo Security News
März 2003

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch

Secorvo Security Consulting GmbH

Nr. 3, 2. Jhrg. 2003
Stand 28. März 2003

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

Inhalt

Editorial: Von Keilen und groben Klötzen

Ein Mann, der sich für stark gehalten,
versuchte, einen Klotz zu spalten.

Geheimnisumwölkt und leicht verrucht lockt die Kryptografie Hobbyexperten wie das Lampenlicht die Sommermotten.

Doch schwang vergeblich er sein Beil,
der Klotz war gröber als der Keil.

Unter Kryptologen sind die Geschichten von vermeintlich „unbrechbaren neuen Verfahren“ Legende – ebenso wie ihre desillusionierende Kompromittierung.

Ein zweiter sprach: Ich werd’s schon kriegen! –
umsonst, der grobe Klotz blieb liegen.

Aber auch der umgekehrte Fall ist nicht selten: hoch intelligente und erfahrene Krypto-Experten, die sich an dem Versuch, ein neues Verfahren zu brechen, die Zähne ausbeißen.

Ein dritter kam nach Jahr und Tag,
dem glückt es auf den ersten Schlag.

Und dann gibt es den dritten Fall: Verfahren, die jahrelang genutzt werden, von deren Sicherheit Experten wie Laien überzeugt sind, die Eingang in Standards und Produkte gefunden haben – und eines Tages einem neuen kritischen Blick, der das danach so scheinbar Offensichtliche zu Tage fördert, zum Opfer fallen.

Diese Fälle sind zum Glück selten, auch wenn die jüngsten Erkenntnisse zu SSL, RSA und Kerberos gleich drei sehr prominente Verfahren betreffen.

War der nun wirklich gar so forsch?
Nein – nur der Klotz war seitdem morsch.

Zwar sind die Angriffe in realen Umgebungen nicht durchführbar. Aber sie zeigen: Erfahrung schützt vor Irrtum nicht.

Und sie sind zugleich eine Mahnung an die enthusiastischen Verfechter des Open Source-Paradigmas: Auch die Veröffentlichung des Source-Codes verhindert keine Fehler. Wir werden noch viele davon kennen lernen – sofern wir ein wenig Geduld mitbringen.

1 Security News

1.1 In Memoriam Roger Needham

Einer der Pioniere der Computer-Sicherheit ist tot. Roger Needham, langjähriger Cambridge-Professor und zuletzt Managing Director von Microsoft Research Ltd. verstarb Anfang März im Alter von 68 Jahren.

Seine wohl bekannteste Arbeit ist das 1978 zusammen mit Michael Schroeder veröffentlichte Authentifikationsverfahren, das die wissenschaftliche Grundlage des Kerberos-Protokolls bildet, mit dem sich heute beispielsweise die Benutzer von Windows 2000 am Domänen-Controller anmelden.

http://research.microsoft.com/users/needham/

1.2 Biometrie mit Problemen

In zahlreichen Pilotversuche zum Einsatz biometrischer Verfahren bei der Personenkontrolle steht derzeit die Gesichtserkennung auf dem Prüfstand. Insbesondere die Sie gilt als sehr attraktiv, da ein Foto als biometrisches Merkmal in Ausweisdokumenten im Gegensatz etwa zu Fingerabdrücken allgemein akzeptiert ist.

Allerdings haben die Verfahren im praktischen Einsatz noch einige Probleme. Bei einem Pilotprojekt zur Überprüfung von Flugreisenden am Nürnberger Flughafen war das System dem menschlichen Auge des geschulten Personals weit unterlegen.

http://www.heise.de/newsticker/data/jk-18.03.03-006/

Im Verlauf eines ähnlichen Versuchs am Flughafen von Sydney gelang es zwei japanischen Reisenden sogar, ihre Pässe zu tauschen, ohne dass dies von der automatischen Gesichtskontrolle bemerkt wurde.

http://australianit.news.com.au/articles/0,7204,6048331^15306^^nbv^,00.html

1.3 Sendmail-Bug bei „weitergereichten“ Mails

Sicherheitslücken in Sendmail sind ja an sich nichts Neues. Viele Anwender schützen ihre Sendmail-Installation deshalb durch einen vorgelagerten Sicherheits-Proxy der Firewall, der eine direkte Verbindung vom Internet zu einem Sendmail-basierten Mailserver verhindert.

Der jüngst entdeckte Heap-Overflow tritt jedoch bei der Bearbeitung des Mail-Envelope-Headers auf und betrifft somit auch Sendmail-Installationen, die hinter einer Firewall Deckung suchen. Patches sind verfügbar und entfernen auch gleich die gefährlichen Header-Zeilen, so dass selbst eine weitergeleitete Mail keinen Schaden mehr anrichten kann.

http://www.cert.org/advisories/CA-2003-07.html

1.4 „Side-Channel“ Angriffe auf SSL und RSA

Gleich drei aktuelle Angriffe machen sich „Randinformationen“ von SSL- bzw. RSA-Implementierungen zu nutze. Als Testobjekt für die praktische Demonstration diente den Autoren OpenSSL – der Quelle vieler SSL-Lösungen. Daher sind höchstwahrscheinlich auch andere Implementierungen betroffen.

Forscher der Eidgenössischen Technischen Hochschule Lausanne benutzen das Timing von schneller oder langsamer zurückgemeldeten Fehlermeldungen, um Hinweise zur Entschlüsselung von SSL-geschützten Nachrichten zu erhalten. Dieser ausgefeilte Angriff ist glücklicherweise nur unter sehr speziellen Umständen anwendbar und daher wenig praxisrelevant.

http://lasecwww.epfl.ch/memo_ssl.shtml

Zwei Stanford-Forscher messen die benötigte Zeit für die Ausführung der RSA-Operation, um den verwendeten geheimen Exponenten zu ermitteln. Hierüber könnte

beispielsweise der geheime Schlüssel eines SSL-Webservers ermittelt werden.

http://crypto.stanford.edu/~dabo/abstracts/ssl-timing.html

Und tschechische Kryptologen werten die unterschiedlichen Reaktionen auf verschiedene Fehlerfälle, die während eines SSL-Verbindungsaufbaus auftreten können, um einen SSL-Sitzungsschlüssel zu ermitteln oder eine RSA-Signatur im Namen des SSL-Servers zu fälschen. Auch dieser Angriff ist nur von beschränkter Praxisrelevanz: Er erfordert Millionen von fehlgeschlagenen SSL-Verbindungen, die für aufmerksame Systemadministratoren nicht zu übersehen wären.

http://eprint.iacr.org/2003/052/

Für OpenSSL wurden umgehend Patches gegen alle drei Attacken bereit gestellt.

http://www.openssl.org/

1.5 BVerfG urteilt zur TK-Überwachung

Am 12.03.2003 hat das Bundesverfassungsgericht (BVerfG) zwei Verfassungsbeschwerden von Journalisten zurückgewiesen, deren Telefone im Zuge der Verfolgung schwerer Straftaten abgehört wurden. Beschwerdeführer waren das ZDF, zwei seiner journalistischen Mitarbeiter und eine für das Magazin „Stern“ tätige Journalistin, die Informationen zu verschiedenen Kriminalfällen recherchierten.

Da angenommen wurde, dass die Journalisten mit den Beschuldigten in telefonischem Kontakt stehen, ordnete das Amtsgericht Frankfurt a.M. auf Antrag der Staatsanwaltschaft die Auskunft über entsprechende Verbindungsdaten der Telefongespräche an. Die Verfassungsbeschwerden richteten sich gegen diese richterliche Anordnung der TK-Überwachung.

Obwohl das BVerfG sowohl den Eingriff in das Fernmeldegeheimnis als auch den Eingriff in die Presse- und Rundfunkfreiheit der Beschwerdeführer anerkannte, hatten die Verfassungsbeschwerden keinen Erfolg. Zur Begründung gab das Gericht an, dass auch schwer wiegende Grundrechtseingriffe als verhältnismäßig anzusehen sind. Denn „angesichts der Schwere der in Rede stehenden Straftaten“ hätten die Gerichte „dem Gebot der wirksamen Strafverfolgung zu Recht den Vorrang eingeräumt“.

http://www.bverfg.de/bverfg_cgi/pressemitteilungen/frames/bvg20-03

1.6 Eindringen per Intrusion Detection System

Ein Buffer Overflow bei der Analyse des mitgeschnittenen Datenverkehrs durch das Open-Source Intrusion Detection System (IDS) „snort“ ermöglichte es Angreifern, mittels einer vorgeblichen Attacke auf RPC-Dienste in Wirklichkeit den IDS Server anzugreifen. Entdeckt wurde die Sicherheitslücke vom kommerziellen IDS-Hersteller ISS Inc.

http://www.snort.org/

1.7 Krypto-Schwäche in Kerberos v4

Eine neu entdeckte Schwäche im altbekannten Kerberos v4 Protokoll ermöglicht verschiedene Angriffe durch Kerberos-Benutzer und durch Administratoren fremder Verwaltungsbereiche („Realms“). Wer noch Kerberos v4 einsetzt, sollte den empfohlenen Patch installieren – oder gleich zu Kerberos v5 wechseln.

http://web.mit.edu/kerberos/www/advisories

1.8 Unendliche Geschichte: Windows-Patches

Immer wieder einen Blick wert ist die Security Bulletin Liste von Microsoft. Neu hinzu gekommen sind kritische Sicherheitslücken in der Windows Script Engine und in der DOS/NT Namenskonvertierung sowie Denial-of-Service gegen ISA Server und RPC.

http://www.microsoft.com/technet/security/current.asp

2 Secorvo News

2.1 Secorvo College aktuell

Über fünf Jahre Erfahrung mit der Konzeption, dem Aufbau und dem erfolgreichen Betrieb von Public Key Infrastrukturen bündelt Secorvo in dem Seminar-Paket „PKI“ und „PKI für Fortgeschrittene“:

- PKI – Public Key Infrastrukturen, 06.-07.05.2003.
- PKI für Fortgeschrittene, 08.05.2003.

Einsteigern in das Thema IT-Sicherheit bietet Secorvo außerdem jetzt einen einwöchigen Intensivkurs:

- IT-Sicherheitsmanagement von A (wie Audit) bis Z (wie Zertifizierung), 12.-16.05.2003

Für Teilnehmer dieses Seminars ist der Eintritt zur Veranstaltung der Karlsruher IT-Sicherheitsinitiative am 15.05.2003 kostenfrei.

2.2 Evaluierung der EU-Signaturrichtlinie

Im Oktober 2002 hatte die Europäische Kommission eine Evaluationsstudie über „rechtliche und marktbezogene Aspekte der Anwendung der Richtlinie“ (zu elektronischen Signaturen) ausgeschrieben. Ziel der Studie ist es, den aktuellen Stand der praktischen Umsetzung der Signaturrichtlinie in den einzelnen Mitgliedsstaaten zu dokumentieren.

Ein internationales Konsortium unter der Leitung von Professor Jos Dumortier (KU Leuven, ICRI, Belgien) hat diese Ausschreibung gewonnen. Das Team aus Jos Dumortier, Patrick an Eecke (Belgien), Georgia Skouma (Belgien), Hans Nilsson (Schweden) und Stefan Kelm von Secorvo wird die Studie voraussichtlich im Juli 2003 vorlegen.

3 Veranstaltungshinweise

April 2003	
09.04.	Lampertz-Sicherheitstag (Lampertz, Speyer)
13.-17.04.	RSA Conference 2003 (RSA, San Francisco)
Mai 2003	
05.-06.05.	DuD 2003 (Computas, Berlin)
06.-07.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
08.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
13.-15.05.	BSI-Kongress 2003 (BSI, Bonn)
15.05.	Karlsruher IT-Sicherheitsinitiative (KA-IT-Si, Karlsruhe)
12.-16.05.	IT-Sicherheitsmanagement von Audit bis Zertifizierung (Secorvo College, Karlsruhe)
19.-20.05.	IT Risk Management (ITRM 2003) (Computas, Karlsruhe)
20.-21.05.	Lotus Notes Security (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 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 Feedback an
redaktion-security-news@secorvo.de