Secorvo Security News
August 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 2, 1. Jhrg. 2002
Stand 09. August 2002

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

Inhalt

Editorial: Lang ist lang genug

Seit 25 Jahren tobt die Diskussion über angemessene Mindestschlüssellängen für kryptografische Verfahren. Sie begann mit dem Data Encryption Standard (DES): Erst nachdem die National Security Agency (NSA) die Schlüssellänge des ursprünglichen IBM-Entwurfs von 128 auf 56 bit verkürzt hatte, wurde der DES 1977 zum amerikanischen NBS-Standard. Im selben Jahr skizzierten die Kryptologen Diffie und Hellman die Konstruktion eines Chips, der in etwa 12 Stunden einen DES-Schlüssel finden sollte.

Tatsächlich wurde erst 22 Jahre später eine funktionierende DES-Entschlüsselungsmaschine konstruiert: Die von der Electronic Frontier Foundation (EFF) finanzierte Entwicklung benötigte mit 1.800 parallelen Spezialchips ("Deep Crack") immer noch knapp 56 Stunden, um einen DES-Schlüssel heraus zu finden.

Das Beispiel zeigt, dass aus theoretischen Betrachtungen abgeleitete Befürchtungen und reale Möglichkeiten weit auseinander klaffen können. Das gilt gelegentlich auch für Empfehlungen einer Mindestlänge für kryptografische Schlüssel. Insbesondere bei asymmetrischen Kryptoverfahren ist für die Bestimmung der Mindestschlüssellänge nicht nur die zukünftige Entwicklung der Rechenleistung zu prognostizieren, sondern es müssen auch mögliche neue mathematische Erkenntnisse berücksichtigt werden. Groß ist die Versuchung, auf „Nummer Sicher“ zu gehen, wie im Entwurf der Algorithmenempfehlung 2002 des BSI zum Signaturgesetz, deren Endfassung von der RegTP für Herbst 2002 angekündigt wurde:

http://www.bsi.bund.de/esig/basics/techbas/krypto/bund02v5.pdf (43 kB)

In einer Stellungnahme hat Secorvo die Entwicklung der Faktorisierungserfolge der vergangenen 25 Jahre ausgewertet – und hält deutlich kürzere RSA-Schlüssellängen für ausreichend sicher:

http://www.secorvo.de/whitepaper

1 Security News

1.1 SPHINX-Einsatzempfehlungen des BSI

Das BSI hat jüngst die Ergebnisse der im ersten Quartal 2001 durchgeführten Interoperabilitätstests mit einer Empfehlung für Sphinx-konforme E-Mail-Verschlüsselungslösungen publiziert. Darin erhielten nur drei Produkte (zwei Plugins für Outlook 98 und eine Lösung für Groupwise 5.5) eine uneingeschränkte Empfehlung:

http://www.bsi.de/aufgaben/projekte/sphinx/interop/empf102.htm

1.2 ISIS-MTT Version 1.0.2

Mit Unterstützung des BMWi wurde im vergangenen Jahr unter der Federführung von TeleTrusT Deutschland der Standard ISIS (Industrial Signature Interoperability Specification) der Trustcenter-Gruppe „T7“ mit dem von Secorvo für TeleTrusT entwickelten PKI- und E-Mail-Sicherheitsstandard MailTrusT zu einem gemeinsamen Standard ISIS-MTT verschmolzen. Die erste Version dieser auf X.509, PKIX und S/MIME aufbauenden Spezifikation wurde am 01.10.2001 veröffentlicht. Inzwischen ist ISIS-MTT obligatorischer Teil von SAGA (Standards und Architekturen für eGovernment Anwendungen). Auf der Grundlage zahlreicher Kommentare wurde am 19.07.2002 die Version 1.0.2 publiziert:

http://www.teletrust.de/teletrust.asp?id=61040

1.3 Bugs in OpenSSL, Trojaner in OpenSSH

Am 30.07.2002 informierten DFN- und RUS-CERT über fatale Fehler in OpenSSL: In allen Versionen bis einschließlich 0.9.6d kann auf unterschiedliche Weise ein Buffer Overflow verursacht werden, der die Ausführung beliebigen Codes auf dem SSL-Server im privilegierten (Root-)Mode ermöglicht. Gegenmaßnahme: Update auf OpenSSL Version 0.9.6e oder Lösungen der Hersteller abwarten:

http://cert.uni-stuttgart.de/ticker/article.php?prev=905

Ende Juli 2002 wurden die Domainen ftp.openbsd.org und ftp.openssh.org Hackeropfer: Am 01.08. wurden mehrere SSH-Versionen mit integriertem trojanischen Pferd entdeckt (und entfernt):

http://cert.uni-stuttgart.de/ticker/article.php?mid=911

1.4 Win2000 Security Patch

Am 01.08.2002 wurde von Microsoft das lange angekündigte Service Pack 3 (SP3) für Windows 2000 publiziert, das überwiegend Sicherheitslücken behebt:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/w2ksp3.asp

1.5 AES im SSL-Standard

Ende November 2001 wurde nach einem vierjährigen fachöffentlichen Bewertungsprozess der in Belgien entwickelte Verschlüsselungsalgorithmus Rijndael vom amerikanischen National Institute of Standards and Technology (NIST) als Advanced Encryption Standard (AES) ausgewählt und als FIPS 197 veröffentlicht:

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (243 kB)

Nun wird diesem Nachfolger des in die Jahre gekommenen DES der Weg in die Anwendungen geebnet: Mit RFC 3268 hat die Internet Engineering Task Force (IETF) im Juni 2002 die Liste der von SSL (Transport Layer Security Protocol – TLS) unterstützten Verschlüsselungsverfahren um den AES ergänzt:

http://www.ietf.org/rfc/rfc3268.txt

Bisher unterstützte der SSL-Standard (RFC 2246 vom Januar 1999) nur die Algorithmen RC2, RC4, IDEA, DES und 3DES.

1.6 PKI-Umfrage

Die TeleTrusT-Arbeitsgruppe „Public Key Infrastrukturen“ (AG 7) hat eine Web-Umfrage zum Stand von Public Key Infrastrukturen in Deutschland gestartet:

http://www.teletrust.de/glossar.asp?ID=60880,3&HomePG=0&sw=1&Sprache=D

Die Arbeitsgruppe erhofft sich eine repräsentative Erfassung aktueller PKI-Trends. Einen Zwischenstand der Umfrage wird der Leiter der AG 7, Fritz Bauspieß, auf dem diesjährigen PKI-Symposium 2002 in Karlsruhe vorstellen.

1.7 IT-Sicherheitskongress

Der 8. Deutsche IT-Sicherheitskongress des BSI wird vom **13.-15.05.2003** in Bonn stattfinden. Das Programmkomitee des alle zwei Jahre organisierten Kongresses hat am 18.07.2002 den "Call for Papers“ veröffentlicht. Damit werden interessierte Autoren zur Einreichung fachkundiger Beiträge bis 10.10.2002 aufgefordert:

http://www.bsi.bund.de/veranst/bsikongr/cfp.pdf (91 kB)

1.8 EU-Datenschutzrichtline

Die am 12.07.2002 verabschiedete EU-Datenschutzrichtlinie für elektronische Kommunikation ist nun online verfügbar. Sie muss bis 31.10.2003 in nationales Recht umgesetzt werden:

http://europa.eu.int/eur-lex/de/dat/2002/l_201/l_20120020731de00370047.pdf (167 kB)

1.9 „Liberty Alliance“ strikes back

Nachdem die Akzeptanz von Microsofts .NET-Konzept, eines Web-basierten Authentifikationsdienstes, bisher bescheiden ausfällt, haben nun die unter Führung von Sun in der „Liberty Alliance“ zusammengeschlossenen Mitbewerber am 15.07.2002 ihre Architektur-Spezifikation publiziert:

http://www.project-liberty.org/specs/main.html

2 Secorvo News

2.1 ISIS-MTT-Testbed

Im Auftrag von TeleTrusT Deutschland e.V. hat Secorvo auf Basis der Testspezifikation für ISIS-MTT-konforme Produkte einen Testbed Prototyp entwickelt, der am 01.08.2002 fertiggestellt wurde.

Diese weit gehend automatisierte, auf angepasster Open-Source-Software und eigenen Tools basierende Testumgebung wird im Herbst verfügbar sein. Den Prototyp wird Projektleiter Hans-Joachim Knobloch auf dem diesjährigen PKI-Symposium 2002 in Karlsruhe präsentieren.

2.2 IT-Grundschutz-Audit

Mit dem IT-Grundschutz-Zertifikat hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Februar 2002 ein amtliches Prüfsiegel geschaffen, mit dem die wirkungsvolle Umsetzung von IT-Grundschutzmaßnahmen in einem Unternehmen bzw. einer Behörde dokumentiert werden kann. Voraussetzung für die Erteilung eines solchen Zertifikats durch das BSI ist die Durchführung eines Grundschutz-Audits nach einem festgelegten Prüfschema durch einen vom BSI lizenzierten Auditor:

http://www.bsi.bund.de/gshb/zert/pruef.pdf (105 kB)

Seit dem 10.07.2002 zählt Claus Stark, Security Consultant bei Secorvo, zu den bisher vierzig vom BSI lizenzierten IT-Grundschutz-Auditoren. Damit kann Secorvo zukünftig Grundschutz-Audits durchführen und, bei Erfüllung der Anforderungen des Prüfschemas, dem BSI die Ausstellung eines IT-Grundschutz-Zertifikats empfehlen.

2.3 Anwendungsintegration statt „One Size Fits All“

Das Image der sicherheitstechnischen „Eier legenden Wollmilchsau“, das Public Key Infrastrukturen lange anhaftete, hat Risse bekommen – und gibt den Blick frei auf den wahren Kern einer PKI: Sie ist eine notwendige Infrastruktur für ausgewählte Mechanismen der IT-Sicherheit. Der Hype ist der ernsthaften Hinwendung zu sinnvollen Anwendungen gewichen.

Diese Entwicklung spiegelt das Programm des diesjährigen PKI-Symposiums 2002 (**08.-09.10.2002**): Mit PKI-Praxisberichten wie den „Lessons Learned“ der UBS AG, der Vorstellung spezieller PKI-basierter Anwendungen wie dem digitalen Fahrtenschreiber und einem Microsoft-Blick in die Zukunft der Webservices wird die Diskussion aktueller Entwicklungen und realistischer Perspektiven von PKIs eröffnet. Workshops und das Begleitprogramm werden auch in diesem Jahr reichlich Gelegenheit zu Erfahrungsaustausch und Diskussion geben:

http://www.pki-symposium.de

Kostenbeitrag: 390 € zzgl. MwSt.
(Aus der Erfahrung der Vorjahre empfehlen wir eine möglichst frühzeitige Anmeldung.)

2.4 „PKI-Woche 2002“

Die 41. Kalenderwoche haben wir in Karlsruhe dem Thema Public Key Infrastrukturen gewidmet: Um Ihren Reiseaufwand zu minimieren, haben wir unser PKI-Seminar, das PKI-Symposium 2002 und ein PKI-Vertiefungsseminar in derselben Woche konzentriert. So können Sie an vier aufeinanderfolgenden Tagen, vom **07.-10.10.2002**, in das Thema PKI eintauchen:

http://www.secorvo.de/college/pki-woche

Teilnehmern des PKI-Symposiums bieten wir die Seminarteilnahme zu einem Sonderpreis an (siehe Anmeldung). Natürlich können die Seminare und das PKI-Symposium auch unabhängig von einander gebucht werden.

3 Veranstaltungshinweise

September 2002	
23.-24.09.	IT Risk Management 2002 (Computas)
24.-25.09.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
Oktober 2002	
02.-04.10.	Information Security Solutions Europe – ISSE 2002 (EEMA)
	„PKI-Woche“
07.-08.10.	Public Key Infrastrukturen (Secorvo College)
08.-09.10.	PKI-Symposium 2002 (Secorvo)
10.10.	PKI für Fortgeschrittene (Secorvo College)
14.-16.10.	7th European Symposium on Research in Computer Security – ESORICS 2002 (ETH/IBM Zürich)
22.-23.10.	Virtual Private Networks im praktischen Einsatz (Secorvo College)
29.-30.10.	SAP-Sicherheit im Betrieb (Secorvo College)

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 Feedback an
redaktion-security-news@secorvo.de