secorvo
security consulting

Secorvo Security News

Januar 2010

O Elena, O mores...

Noch ist die Entscheidung über die verfassungsrechtliche Zulässigkeit einer Vorratsspeicherung von Telekommunikationsdaten nicht gefallen, da tritt das ELENA-Verfahren aus dem Windschatten in die öffentliche Wahrnehmung. Das überrascht etwas – wurde das Verfahren des „Elektronischen Entgeltnachweises" doch bereits am 22.09.2009 vom Bundestag beschlossen. Tatsächlich weist die Entstehungsgeschichte sogar sieben Jahre weit zurück – und ist ein Lehrstück regulativer Technikgestaltung in Deutschland.

Als Projekt „JobCard" erblickte Elena im August 2002 als ein Vorschlag der Hartz-Kommission das Licht der Welt. Signaturkartenverfechter witterten Morgenluft: War das endlich die „Killer-Applikation" der digitalen Signatur? Mit der Behauptung einer Entlastung der Unternehmen um 85,6 Mio. Euro jährlich – im Schnitt beeindruckende 29 Euro je Unternehmen – wurden die verfassungsrechtlichen Zweifel von Datenschützern an der für das Verfahren erforderlichen zentralen Speicherung von Arbeitnehmerdaten erstickt. Tatsächlich macht die Spezifikation der Datensätze vom 19.10.2009 (inzwischen von der Elena-Webseite gelöscht) sprachlos: Neben Entgeltinformationen werden Fehlzeiten mit Datum und Grund, Urlaubstage, Kündigungsgründe und vorausgegangene Abmahnungen inklusive einer Beschreibung des vertragswidrigen Verhaltens (Freitext) erhoben.

Wir erinnern uns: Datenschutz ist Teil des allgemeinen Persönlichkeitsrechts (Art. 2 GG). Eines der Prinzipien ist der Erforderlichkeitsgrundsatz („Datensparsamkeit") – keine Spur davon bei Elenas Vorratsdatenspeicherung. Aber mit dem Datenschutzrecht nimmt man es bei Elena sowieso nicht so genau: „Eine Auskunft ist vor 2012 (...) nicht realisierbar, da der Abruf durch die abrufenden Stellen erst ab 2012 möglich ist„, heißt es lapidar auf der Webseite. Ein klarer Rechtsverstoß, denn das Auskunftsrecht besteht nach § 34 BDSG uneingeschränkt. Wir empfehlen: Fordern Sie es ein (Vorlage). Und falls Sie keine Auskunft erhalten, wenden Sie sich an den Bundesdatenschutzbeauftragten.

Inhalt

secorvo
security consulting

Security News

768 bit faktorisiert

Schon am 12.12.2009 gelang einem internationalen Kryptologen-Team um Bos, Franke, Kleinjung, Lenstra und Montgomery die Lösung der 768-bit-RSA-Challenge – die Zerlegung eines 768-bit-Modulus in seine Primfaktoren. Details der Number Field Sieve-Faktorisierung veröffentlichten die Autoren am 06.01.2010. Danach benötigten sie 2^{37} Operationen (≈ 4,7 Mio. MIPS-Jahre) zur Bestimmung der Primfaktoren – nur ein Zehntel des von Silverman im Jahr 2000 geschätzten Aufwands. Für den aufwändigsten Teil der Berechnung, das „Aussieben", arbeiteten viele hundert Workstations über zwei Jahre – das entspricht etwa 1.500 Rechenjahren eines 2.2 GHz AMD Opteron-Prozessors.

Tatsächlich deckt sich dieser Erfolg fast exakt mit der im Jahr 2002 veröffentlichten Prognose von Secorvo (siehe Abb.): Darin hatten wir die Faktorisierung von 768 bit für Anfang 2010 vorausgesagt.

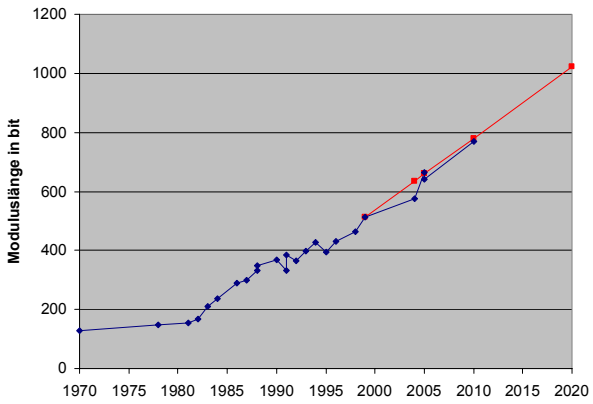

Abb.: Faktorisierungserfolge (blau), Prognose (rot)

Trotz dieses Faktorisierungserfolgs liegt die öffentliche NFS-Faktorisierung eines 1.024-bit-Modulus noch deutlich in der Zukunft – der dafür erforderliche Aufwand ist um den Faktor 1.000 größer. In den kommenden fünf Jahren sei daher auch unter Berücksichtigung des technischen Fortschritts nicht mit einer Faktorisierung zu rechnen. Die Secorvo-Prognose erwartet die Faktorisierung Anfang des Jahres 2020 – spätestens dann sollten 1.024-bit lange RSA-Schlüssel nicht mehr eingesetzt werden.

Legic gebrochen

Fast auf den Tag genau zwei Jahre nach dem spektakulären Brechen der Mifare-Classic-Chipkarten (siehe SSN 03/2008) haben Karsten Nohl und Henryk Plötz am 29.12.2009 auf dem 26. Chaos Computer Congress das Clonen von Legic Prime Chipkarten präsentiert. Da der Hersteller, wie sie feststellen mussten, komplett auf Kryptoverfahren verzichtet und lediglich ein simples 7-bit-Schieberegister für den „Schlüsselstrom" verwendet hatte, konnten sie sich eine aufwändige Chip-Analyse sparen – „Security by Obscurity" bricht man eleganter mit „Trial and Error".

Unternehmen, die vor zwei Jahren schadenfroh mit dem Finger auf die vom Mifare-Hack betroffenen Firmen gezeigt, sich aber bis heute auf ihre Legic Prime Chips verlassen haben, ohne auf das „Legic Advant"-Verfahren zu migrieren, droht nun ein böses Erwachen – den Passepartout in ihr Unternehmen gibt es jetzt zum Preis einer Taxifahrt.

WASC Threat Classification

Zum Jahresbeginn wurde am 01.01.2010 vom Web Application Security Consortium (WASC) die Version v2.0 der „WASC Threat Classification" veröffentlicht. Die Darstellung von 34 verschiedenen Angriffen (z. B. Buffer Overflow, XSS, SQL Injection) auf Web-Anwendungen und 15 Schwachstellen (z. B. Directory Indexing, Insufficient Authorization, Server Misconfiguration) ist sowohl online als auch als 171 Seiten starkes PDF-Dokument verfügbar. Sie gibt einen guten Überblick über aktuelle mögliche Probleme von Web-Anwendungen.

Jeremiah Grossman nimmt in seinem Blog eine Zuordnung zwischen der WASC Threat Classification und den OWASP Top Ten 2010 RC1 (siehe SSN 11/2009) vor – wobei sich der Eindruck aufdrängt, dass durch eine engere Zusammenarbeit und Abstimmung zwischen WASC und OWASP doppelte Arbeit vermieden werden könnte.

Empfohlene Kryptoverfahren

Das US-amerikanische National Institute of Standards and Technology (NIST) veröffentlichte am 14.01.2010 die jüngsten Empfehlung zu Krypto-Algorithmen und Schlüssellängen als Draft Special Publication 800-131. Danach steigt das vorgeschriebene Sicherheitsniveau ab 2011 auf mindestens 112 bit – nur noch Triple-DES mit drei Schlüsseln und AES-128, -192 und -256 dürfen dann noch von Bundesbehörden eingesetzt werden. Auch der SHA-1 darf ab 2011 nicht mehr für die Signaturerzeugung genutzt werden, DSA und RSA müssen Moduluslängen von mindestens 2.048 bit verwenden und Verfahren auf Elliptischen Kurven wie ECDSA Endliche Körper der Ordnung 224. Ab dem Jahr 2031 soll das Sicherheitsniveau auf mindestens 128 bit steigen – eine Anforderung, die die NSA bereits heute an „secret" klassifizierte Daten stellt.

Dem Entwurf des BSI zu Folge wird sich auch die Empfehlung geeigneter Algorithmen der BNetzA, die in Kürze im Bundesanzeiger publiziert werden wird, an die NIST-Empfehlung annähern: RIPEMD-

160 und SHA-1 dürfen danach nur noch bis Ende 2010 zur Signaturerzeugung eingesetzt werden, die Mindestlänge von RSA-Moduli steigt auf 1.976 bit.

DNSSEC livehaftig

Seit dem 05.01.2010 stellt die DENIC eG im DNSSEC Testbed für Deutschland auf zwei speziell eingerichteten Nameserverclustern einen Name Service für die Top Level Domain .de bereit, bei dem die autoritativen Auskünfte per DNSSEC signiert sind. Dies ist zwar noch kein regulärer DNSSEC Betrieb für .de, aber doch genau wie im richtigen Leben: Die DNS-Auskünfte des Testbeds sind ebenso vollständig und aktuell wie die der offiziellen Nameserver von a.nic.de bis z.nic.de.

Wer selbst schon DNSSEC für seine .de-domain einsetzt, muss sich noch bis zum März 2010 gedulden - ab dann wird die DENIC auch Key Signing Keys untergeordneter Domains registrieren und per DNSSEC zertifizieren.

Audit-Wundertüte runderneuert

Die am 11.01.2010 erschiene Auditing-Distribution Backtrack 4 Final wurde gegenüber Version 3 auf Ubuntu umgestellt, um ein zeitnahes Patchmanagement zu ermöglichen. Der revisionssicher nachvollziehbare Change der ca. 500 Prüfwerkzeuge – sowie zukünftiger Ergänzungen – kann anhand der Loginformationen der Installationsumgebung nachgewiesen werden. Wichtige Ergänzungen – neben der deutlich erweiterten Treiberunterstützung für Hardware – sind bekannte Programmpakete, wie OpenVAS 3.0, Nmap 5.2 und Metasploit 3.3.3. Die Sniffersuite lässt nun auch bei Bluetooth, RFID und Voice over IP kaum noch einen Wunsch offen.

Der Scanner OpenVAS wurde als freier Nessusersatz integriert und läuft stabil mit ca. 15.500 Prüfungen. Zeitsparend ist die integrierte Versionierung von bisherigen Scans und Scanergebnissen für deren Wiederholbarkeit. Für Prüfungen, die einen Proof-of-Concept erfordern, ist die Weiterführung von milw0rm in der exploit-db (mehr als 10.000 technische Schwachstellen) eine erfreuliche Ergänzung. Spannend wird es – die richtige Grafikkarte(n) vorausgesetzt – bei der Nutzung von Werkzeugen, die auf CUDA basieren. Hier sind u. a. Multiforcer (Passwort-Bruteforcer für MD5, FASTMD5, MD4, FASTMD4, NTLM, FASTNTLM, SHA1, FASTSHA1), der RAR-Archivbrecher cRARk und Pyrit (für WPA2-PSK) treue Helfer.

Insgesamt also ein unverzichtbares Werkzeug für den (technischen) Auditor mit zahlreichen sinnvollen „Aufrüstungen".

SOA-Kompendium

Am 05.01.2010 hat das BSI Version 2.0 des in erster Fassung vor zwei Jahren veröffentlichten „SOA-Security-Kompendium Sicherheit in Service-orientierten Architekturen" herausgegeben. In dem 371seitigen PDF-Dokument werden verschiedene Sicherheitsaspekte von SOA-Umgebungen ausführlich dargestellt. Aufgrund der Komplexität des Themas ist die Verfügbarkeit eines umfassenden Referenzwerks, das neben einer Einführung besonders die Themen Technologien (96 Seiten), Security Management (46 Seiten) und spezielle Sicherheitskonzepte (72 Seiten) behandelt, eine echte Arbeitshilfe.

Secorvo News

Secorvo College aktuell

Die Nachfrage nach einer TISP-Zertifizierung ist ungebrochen - seit 2004 haben 350 Sicherheitsexperten das Zertifikat erworben. Lassen auch Sie Ihre Qualifikation bei der nächsten TISP-Schulung mit anschließender Prüfung vom **22.–27.02.2010** zertifizieren. Dass Sicherheit auch in der Software Entwicklung eine immer wichtigere Rolle spielt, zeigt das wachsende Interesse am Certified Professional for Secure Software Engineering (CPSSE). Das Zertifikat können Sie vom **16.–19.03.2010** erwerben. Im März steht außerdem erstmals das neue Seminar „Sicherheitsmanagement heute" auf dem Programm. Verschaffen Sie sich vom **23.–25.03.2010** einen Überblick über die Grundlagen des Information Security Managements. Das gesamte Seminarangebot 2010 sowie die Möglichkeit zur Online-Anmeldung finden Sie hier.

SecurityCup 2009

Die Karlsruher IT-Sicherheitsinitiative beginnt ihre diesjährige Veranstaltungsreihe mit einem spannenden Thema: Die FIDUCIA IT AG führte 2009 ihre dritte Security-Awareness-Kampagne durch – auf höchstem konzeptionellen Niveau und mit einer aktiven Mitarbeiterbeteiligung von über 50 Prozent. Am 18.02.2010 stellen Lutz Bleyer, Leiter der Zentrale Security bei der FIDUCIA IT AG Karlsruhe, und Sven Kaun, Geschäftsführer der Dauth.Kaun Communication Group GmbH sowohl die Highlights des „SecurityCup 2009" als auch ihre „Lessons Learned" und „Do's and Dont's" vor. Anschließend gibt es Gelegenheit zum Networking am Buffet. Um Anmeldung wird gebeten.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2010	
02.-03.02.	20. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
03.-04.02.	ESSoS (DistriNet Research Group, Pisa/I)
04.-05.02.	COSADE 2010 (CASED, Darmstadt)
05.-07.02.	ShmooCon 2010 (Shmoo Group, Washington/USA)
09.-10.02.	17. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
11.02.	Infoveranstaltung Datenschutz (CyberForum/ORGA GmbH, Karlsruhe)
15.-18.02.	SecSE 2010: Fourth International Workshop on Secure Software Engineering (SINTEF, Krakau/PL)
18.02.	Wege zum Ruhm – „SecurityCup 2009“ (KA-IT-Si, Karlsruhe)
22.-26.02.	TISP-Schulung (Secorvo College)
23.02.	CASED-Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
März 2010	
16.-19.03.	ISSECO Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)
April 2010	
13.-16.04.	PKI (Secorvo College)
20.-21.04.	Security News Symposium 2010 (Secorvo, Ettlingen)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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