secorvo
security consulting

Secorvo Security News

November 2008

Editorial: Geschichtsvergessen

Das aktuelle Politbarometer der Mannheimer Forschungsgruppe Wahlen vom 21.11. 2008 enthält die erste repräsentative Befragung zur geplanten Ermächtigung des BKA zu Online-Durchsuchungen. Das ernüchternde Ergebnis: 57% der Deutschen halten die Befugnis für grundsätzlich richtig, 39% sprachen sich dagegen aus.

Ist das stereotype „ceterum censeo" des BKA-Präsidenten, eine verbreitete „Ich-hab-nichts-zu-verbergen"-Mentalität oder die mediale Beschwörung der terroristischen Bedrohung (zum Vergleich: 2007 starben in Deutschland 340 Menschen durch Mord, 600 bei Brandkatastrophen und knapp 5.000 bei Verkehrsunfällen – und niemand bei einem Terroranschlag) für dieses Ergebnis verantwortlich?

Vor 40 Jahren, im Sommer 1968, trieben die als „Ermächtigungsgesetz" geziehenen Notstandsgesetze der Großen Koalition Jugendliche und Studenten zu Tausenden auf die Straßen. Die Ermächtigung der Nachrichtendienste im G-10-Gesetz zu Eingriffen in das Post- und Fernmeldegeheimnis – unter strenger parlamentarischer Kontrolle durch die G-10-Kommission – war eines der zentralen politischen Reibungspunkte der Außerparlamentarischen Opposition, aus deren Trümmern zwei Jahre später die RAF hervorging.

Heute bleibt Deutschland angesichts der fortschreitenden Aushöhlung des Fernmeldegeheimnisses gelassen. Während die Liste der Katalogstraftaten in § 100 StPO, die Abhörmaßnahmen rechtfertigen, schrittweise ausgeweitet wurde und die Zahl der Abhöranordnungen von 1985 (1.400) bis 2007 (44.280) auf das 30-fache anstieg (vgl. SSN 06/2006), wirkt selbst die Aufregung über die Auswertung der Verbindungsdaten von Journalisten durch die Deutsche Telekom angestrengt. Bei der verfassungswidrigen Durchsuchung der Redaktionsräume des „Spiegel" im Jahr 1962 hatte es noch zu einer Entscheidung des BVerfG, dem Spiegel-Urteil vom 05.08.1966 gereicht.

Wie formulierte Alexis de Tocqueville 1835 doch so zutreffend: „Die schlimmsten Feinde der Freiheit – sind die glücklichen Sklaven."

Inhalt

Editorial: Geschichtsvergessen

Security News

Kryptographie bleibt schwierig

Neue Schlüssel – gute Schlüssel?

WPA-Erbsünde rächt sich

Sicherere Software

Mühsam nährt sich der Spammer

Social Communities für Eltern

Neuer NIST-Signaturstandard

Secorvo News

Secorvo College aktuell

Über Originale und Fälschungen

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Kryptographie bleibt schwierig

Mitglieder des Google Security Teams meldeten am 11.08.2008 in ihrem Blog eine Lösung für das Problem, wie Anwendungsentwickler Kryptoverfahren einfach und sicher einsetzen können: das bei Google gehostete Open-Source Crypto-Toolkit Keyczar. Zielpublikum für die in Java und Phyton vorliegende Keyczar-Implementierung sind primär Web-Entwickler – und zwar solche, die den Keyczar-Autoren zufolge schlimmstenfalls Schlüssel fest im Quellcode ihrer Anwendung hinterlegen würden.

Für Entwickler der letztgenannten Ignoranzklasse mag das Toolkit tatsächlich eine Hilfe sein. Ansonsten aber zeigt ein Blick in das Designdokument, dass Keyczar keine Konkurrenz für die direkte Nutzung von OpenSSL & Co. ist und hinter den eigenen Ansprüchen zurück bleibt. Denn nicht nur für die Bundesnetzagentur zählen SHA-1 und 1024 Bit DSA schon lange nicht mehr zu den „safe default algorithms and key lengths".

Schlimmer wiegt, dass Keyczar zwar optional geheime Schlüssel auch verschlüsselt ablegt, dafür aber einen unverschlüsselten Masterkey im eigenen Format braucht. Die Gefahr ist groß, dass Web-Entwickler die Schlüssel zwar nicht mehr im Quellcode „verstecken", dafür aber den Masterkey offen als Datei ablegen - und sich dabei sicher wähnen.

Das Zweitschlimmste nach dem Irrtum, Sicherheitsverfahren wären einfach selbst zu entwickeln, sind wohl Systeme, die vorgeben, dem Entwickler die nötigen Kenntnisse zu deren Einsatz zu ersparen.

Neue Schlüssel – gute Schlüssel?

Die am 07.11.2008 veröffentlichte NIST Special Publication 800-108 zum Thema „Key Derivation" zeigt, dass ein erläuternder Standard anstelle eines Black-Box-Toolkits wie Keyczar die Anwendung von Kryptoverfahren vielleicht nachhaltiger erleichtern kann.

Auf 20 Seiten wird dargestellt, wie sich aus einem vorhandenen Schlüssel viele (z. B. für automatisierte Schlüsselwechsel) ableiten lassen, wird hingewiesen, worauf beim Einsatz dieser Verfahren zu achten ist, und wird motiviert, warum manch scheinbar unnützer „Schnörkel" dabei hilfreich ist.

Das Dokument legen wir jedem Entwickler dringend ans Herz, der eine sichere Schlüsselverwaltung entwerfen will.

WPA-Erbsünde rächt sich

Als im Jahr 2001 nach erfolgreichen Angriffen auf das Wired Equivalent Privacy (WEP) Protokoll dringend Abhilfe für die Sicherung von WLANs gesucht wurde, war der erste Wurf für das neue Wifi Protected Access (WPA) Verfahren gar nicht so neu: Das Temporal Key Integrity Protocol (TKIP) des Standards IEEE 802.11i setzt auf der WEP-Verschlüsselung auf, ergänzt um weitere Sicherheitsmechanismen und regelmäßige Schlüsselwechsel. Durch diesen Trick wurde es möglich, allein per Firmware-Update aus vorhandenen, unsicheren WEP-Produkten neue WPA-Produkte zu machen.

Am 08.11.2008 veröffentlichten Martin Beck und Erik Tews, Forscher der Unis Dresden und Darmstadt (woher 2007 schon die bis heute schnellste WEP-Attacke stammt, vgl. SSN 04/07), einen Weg, um trotz der zusätzlichen Vorkehrungen in TKIP über eine ererbte WEP-Schwachstelle einen Teil des RC4-Schlüsselstroms von WEP bzw. TKIP zu ermitteln. Diese Information erlaubt es, einige wenige Datenpakete vom Access Point an WLAN-Clients zu fälschen, beispielsweise zum gezielten Umleiten von Verbindungen.

Wie vor zehn Jahren bei Daniel Bleichenbachers Angriff auf SSL mit RSA hilft hier wieder das Entgegenkommen der Protokolldesigner: Erst die Rückmeldung, die verrät, an welcher Stelle Entschlüsseln und Prüfen eingeschleuster Daten fehlschlagen, zeigt dem Angreifer, wie weit er vorgedrungen ist. Der neue alte Angriff ist nicht so fatal wie die WEP-Attacken und eröffnet keine völlig neuen Angriffswege gegen WPA oder den Nachfolger WPA2. Dennoch sollte man der AES-CCMP Verschlüsselung von WPA2 den Vorzug vor TKIP geben – oder zumindest die TKIP-Schlüsselwechsel auf unter 120 s beschleunigen.

Sicherere Software

Die Entwicklung sicherer Software liegt im Trend: Endlich wird das Problem „unsichere Software" an der Wurzel gepackt. Am 08.10.2008 hat das Software Assurance Forum for Excellence in Code (kurz SAFECode) den Leitfaden Fundamental Practices for Secure Software Development veröffentlicht. Die Organisation, der u. a. Microsoft, EMC und SAP angehören, hat sich zum Ziel gesetzt, zur Verbesserung von Methoden der Softwareentwicklung beizutragen – mit dem besonderen Schwerpunkt Sicherheit.

Das 22-seitige Dokument fasst nach Einschätzung der Autoren die zur Zeit effektivsten Methoden zur sicheren Entwicklung von Software zusammen. Die Darstellung praxiserprobter Vorgehensweisen wird ergänzt durch Verweise auf weiterführende Informationen. Daher kann der Leitfaden gut als Einstieg in die sichere Softwareentwicklung genutzt

werden. Er ergänzt die Übersicht über Fallstudien zum Thema sichere Softwareentwicklung, Software Assurance: An Overview of Current Industry Best Practices, die im Februar 2008 von SAFECode publiziert wurde.

Mühsam nährt sich der Spammer

Nicht nur Stammzellenforschung bringt Ethikkonflikte mit sich – bisweilen auch die IT-Sicherheit: Dürfen Forscher Spam-Mails verschicken, um deren Erfolg oder Misserfolg zu bestimmen? Ein Team aus Berkeley und San Diego (UCSD) stellt in einem Konferenzbeitrag vom 28.10.2008 dar, wie es einen Teil eines Bot-Netzes „zurückkaperte", um die ohnehin darüber versandten Spam-Mails zur statistischen Auswertung zu markieren. Neben dem Wirkungsgrad verschiedener Spam-Filter zeigte sich: Nur knapp eine von zehn Millionen Mails führt zum Kauf der beworbenen blauen Pillen.

Wie die Forscher aus der Strichprobe hochrechnen, dürfte die Marge bei diesem Aufwand-Ertrags-Verhältnis so gering sein, dass weiter verbesserte Anti-Spam-Techniken das Geschäftsmodell empfindlich treffen könnten. Das gibt Hoffnung auf ein mögliches Ende der Plage.

Social Communities für Eltern

Am 04.09.2008 veröffentlichte die Medienkompetenz-Initiative Klicksafe, ein Projekt der Landeszentrale für Medien und Kommunikation Rheinland-Pfalz (LMK), der Landesanstalt für Medien Nordrhein-Westfalen (LfM) und des Europäischen Zentrums für Medienkompetenz (ecmc) eine Handreichung für Eltern zum Thema Social Communities.

Der Kurzratgeber erklärt auf 12 Seiten kompakt und gut verständlich, welche Risiken auf Kinder und Jugendliche bei der Nutzung von Communities wie SchülerVZ & Co. sowie in den beliebten Chatrooms lauern. Die wichtigsten Punkte, die man mit seinen Kindern besprechen sollte, werden erläutert und durch Links auf weiterführende Informationen und Kontaktadressen ergänzt.

Unserer Ansicht nach eine empfehlenswerte Lektüre und ein gutes Hilfsmittel für Eltern – im übrigen nicht das einzige, das sich in der umfangreichen Materialsammlung der Initiative findet.

Neuer NIST-Signaturstandard

Das US-amerikanische National Institute of Standards and Technology (NIST) hat am 12.11.2008 die Entwurfsfassung eines neuen Standards für Digitale Signaturen (FIPS-186-3) veröffentlicht. Der Nachfolger des angejährten FIPS 186-2 vom Januar 2000 unterscheidet sich schon im Umfang erheblich: Aus 76 Seiten wurden 125, allein der „Kern" des Standards (ohne Anhänge) wuchs von vier auf 19 Seiten. Neben den auf dem Diskreten Logarithmusproblem basierenden Signaturverfahren DSA und ECDSA sind nun auch RSA-Signaturen Teil des Standards – nicht mehr nur als kurzer Verweis auf ANSI X.9.31, sondern mit einer mehrseitigen Darstellung der Anforderungen z. B. an die Schlüsselgenerierung. Deutlich erweitert wurden die Anhänge zur Primzahl- und Parameterberechnung.

Die Neufassung des Standards geht deutlich über den eigentlichen Zweck hinaus: Er wurde zu einem ausgewachsenen Leitfaden für Einsteiger und Programmierer erweitert. Der Qualität zukünftiger Implementierungen könnte das zuträglich sein.

Secorvo News

Secorvo College aktuell

Für die rechtzeitige Planung der Weiterbildung 2009 lohnt ein Blick in den Seminarkalender 2009. Neben vier Terminen zum Abschluss der TISP-Zertifizierung bietet Secorvo College 2009 erstmals – im Februar und im Oktober – die Zertifizierung zum CPSSE an: dem Certified Professional for Secure Software Engineering. Das Zertifikat wurde von ISSECO, dem International Secure Software Engineering Council, unter Beteiligung von u. a. der SAP AG entwickelt.

Detaillierte Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Über Originale und Fälschungen

Mit Dongles fing alles an – zwanzig Jahre später spricht man vom „Digital Rights Management", wenn es um den Schutz digitaler Güter geht. War es zunächst nur Software, die vor lizenzwidriger Verbreitung geschützt werden musste, zählen heute auch Daten zu den Schutzgütern – Musikaufnahmen, (Hör-) Bücher, Filme.

Auf dem letzten diesjährigen Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) wird Rüdiger Kügler von Wibu Systems, einem der Pioniere auf diesem Gebiet, am 04.12.2008 (Schlosshotel Karlsruhe, Beginn: 18 Uhr) spannende Rück-, Ein- und Ausblicke in die rasante Entwicklung des Lizenzmanagements geben. Im Anschluss gibt es wie gewohnt Gelegenheit zum „Buffet-Networking". Um Anmeldung wird gebeten.

Veranstaltungshinweise

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

November 2008	
25.11.	OWASP Germany 2008 Conference (www.owasp.org, Frankfurt)
Dezember 2008	
02.-04.12.	Sichere Softwareentwicklung (Secorvo, Karlsruhe)
04.12.	Das Original ist die beste Kopie (KA-IT-Si, Karlsruhe)
27.-30.12.	25th Chaos Communication Congress (CCC, Berlin)
Januar 2009	
20.-22.01.	Omnicard 2009 (inTIME, Berlin)
Februar 2009	
03.-04.02.	19. SmartCard-Workshop (Fraunhofer, Darmstadt)
10.-12.02.	Certified Professional for Secure Software Engineering (CPSSE) (Secorvo College, Karlsruhe)
22.-25.02.	16th Int. Workshop on Fast Software Encryption (IACR, Leuven/BE)
23.-26.02.	13th Financial Cryptography and Data Security 2009 (Int. Financial Cryptography Association, Barbados)

Fundsache

Der lesenswerte Leitfaden zur Nutzung von E-Mail und Internet im Unternehmen des BITKOM erschien im Januar 2008 in der aktualisierten Version 1.5. Das Dokument gibt einen Überblick über die Rechtslage, leitet daraus Empfehlungen für die rechtskonforme Gestaltung der E-Mail- und Internetnutzung ab und schließt mit Formulierungsvorschlägen für eine Betriebsvereinbarung.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch

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