secorvo
security consulting

Secorvo Security News

Februar 2012

Trau, schau, wem?

Nicht erst durch die jüngste Entdeckung identischer Primfaktoren in Public Key Zertifkaten durch die Krypto-Forscher der EPFL (siehe „PKI-Feldstudie“) wissen wir, dass es mit der Vertrauenswürdigkeit von „Trust Centern“ möglicherweise nicht immer so weit her ist, wie wir glaubten. Dabei ist schon der Begriff „Trust Center“ semantischer Nonsens – denn natürlich wird dort weder Vertrauen gesammelt noch erzeugt. Im Kontext von Technik ist „Vertrauen“ ohnehin irreführend. Denn der Begriff bezeichnet „die subjektive Überzeugung (auch Glaube) der Richtigkeit, Wahrheit bzw. Redlichkeit von Handlungen, Einsichten und Aussagen eines anderen oder von sich selbst“, so die Definition in Wikipedia. Vertrauen können wir daher einzig und allein Menschen entgegen bringen, denn Richtigkeit, Wahrheit und Redlichkeit sind keine Eigenschaften technischer Systeme. Wenn wir von „Vertrauen in Technik“ sprechen, meinen wir daher eigentlich etwas anderes: nämlich unser Vertrauen darauf, dass diejenigen, die ein technisches System entwarfen, entwickelten, betreiben und warten unser Vertrauen verdienen.

Menschen vertrauen anderen Menschen vor allem dann, wenn sie gute Erfahrungen damit gemacht haben, wenn ihnen keine Hinweise bekannt sind, die Misstrauen nahe legen, und wenn sie den Eindruck gewinnen, dass dem Gegenüber die Bestätigung des Vertrauens wichtig ist. Genau deshalb sind ein positives Markenimage und Prüf-Zertifkate unabhängiger Dritter vertrauensbildend, und Berichte über Vorfälle Gift für eine Vertrauensbeziehung.

Allerdings darf man Vertrauen nicht mit Sicherheit verwechseln. Vertrauen „überbrückt“ Unsicherheit und (Rest-)Risiken: Es greift da, wo Technik nicht weiterhilft. Denn dass RSA-Schlüssel nicht faktorisiert werden können, dass die Identität des Schlüsselinhabers sorgfältig geprüft wurde und dass die zugehörigen Private Keys Dritten unzugänglich sind, lässt sich durch Technik nicht garantieren. Daran müssen wir glauben. Oder auch nicht, wie Aesop schon wusste.

Inhalt

secorvo
security consulting

Security News

PKI-Feldstudie

Krypto-Forscher der EPFL Lausanne haben in einer am 17.02.2012 veröffentlichten Studie mehrere Millionen Public Keys untersucht, die u. a. vom SSL-Observatory der EFF gesammelt worden waren. Dabei traten einige Fakten zutage, die bei Fachleuten nur Kopfschütteln ernten können: U. a. wurden zu ein und demselben RSA-Schlüsselpaar über 16.000 verschiedene X.509-Zertifikate entdeckt – unklar bleibt, für wie viele unterschiedliche Inhaber. Und etwa 0,2 % der untersuchten RSA-Moduli haben einen ihrer beiden Primfaktoren mit anderen Public Keys gemeinsam, d. h. sie können trivial per GGT-Berechnung gebrochen werden. Dazu kommen noch vereinzelte RSA-„Schlüssel", bei denen einer der beiden Primfaktoren 2 ist, oder bei denen als öffentlicher Exponent 1 verwendet wird – in beiden Fällen ist auch ein 2048-Bit-RSA-Key nicht sicherer als Doppel-ROT13. Daneben gibt die Studie Aufschluss auf die Verbreitung verschiedener Algorithmen und Schlüssellängen: Nur einer von über 11 Mio. Public Keys nutzte elliptische Kurven (ECDSA).

Um die Betroffenen zu schützen, wurde nicht veröffentlicht, ob die betreffenden Schlüssel in PGP-Keys, in selbstsignierten Zertifikaten von Billig-Routern oder in durch öffentliche Trustcenter erstellten Zertifikaten gefunden wurden. Letzteres würde ein weiteres Schlaglicht auf die unterentwickelte Qualitäts- und Risikomanagement-Kultur der Branche werfen – genau wie der am 04.02.2012 publik gewordene Fall, dass bewusst ein CA-Zertifikat zum „Aufbrechen" von SSL verkauft wurde. Merke: Die Schlüssellänge allein garantiert keine unknackbaren Schlüssel – und ein Zertifikat offenbar auch nicht.

Grenzen staatlicher Auskunftsrechte

Das Bundesverfassungsgericht hat mit Beschluss vom 24.02.2012 die Auskunftsbefugnisse von Geheimdienst-, Ermittlungs- und Polizeibehörden eingeschränkt. Überprüft wurden die Auskunftsverfahren über Telekommunikationsbestandsdaten nach den §§ 111 ff. Telekommunikationsgesetz (TKG). Die Preisgabe von PIN, PUK und weiteren Zugangscodes zu den Endgeräten und die Zuordnung von dynamischen IP-Adressen über diese Auskunftsansprüche sind danach verfassungswidrig.

Zwar wurde das automatisierte Auskunftsverfahren und die grundsätzliche Speicherpflicht der TK-Provider in weiten Teilen bestätigt. Der Grundrechtseingriff sei vergleichsweise gering und gerechtfertigt. Die Auskunftserteilung über die Zuordnung von dynamischen IP-Adressen sei jedoch ein Eingriff in das Telekommunikationsgeheimnis (Art. 10 GG) und von den Auskunftsnormen nicht umfasst. Zudem stellen die Auskunftspflichten keine Erhebungsgrundlage für die abfragenden Behörden dar. Diese benötigen fachspezifische Befugnisnormen. Im Fall von § 113 Abs. 1 S. 2 TKG, der Auskunft über Zugangscodes, fehle der Regelung zudem eine ausreichende Bindung an die Zwecke der Codeverwendung.

Bemerkenswert sind die Ausführungen zur bevorstehenden Einführung von IPv6 mit flächendeckend statischen IP-Adressen. Sollte es hierdurch zu einer umfassenden Deanonymisierung der Internetnutzung kommen, wird dem Gesetzgeber die Pflicht zur Neubetrachtung der Eingriffsbeschränkung aufgegeben. Damit bleibt das Bundesverfassungsgericht seiner Rolle als Bollwerk gegen ausufernde staatliche Überwachung treu.

Taschendiebstahl 2.0

Mit der zunehmenden Verbreitung von Smartcard-Chips, die neben den Kontaktflächen auch eine RFID-Schnittstelle besitzen, sprießen auch deren Anwendungen: Nach dem nPA hat am 11.01.2012 die Deutsche Kreditwirtschaft angekündigt, dass die GeldKarte bald unter dem Namen „girogo" auch berührungslos nutzbar sein wird.

Das weckt Befürchtungen über einen berührungslosen Taschendiebstahl. Prompt wurde auf der Shmoocon am 29.01.2012 demonstriert, wie einfach sich eine RFID-fähige Kreditkarte „im Vorbeigehen" kopieren lässt. Glücklicherweise muss der Cyber-Taschendieb bei sicheren Verfahren als „Händler" auftreten und riskiert so seine Entdeckung. Und gegen eine Weiterleitung als Man-in-the-Middle an einen realen Händler helfen Protokolle, die mittels Kryptographie und Signallaufzeiten den Radius eines möglichen Missbrauchs beschränken. Eher ist jedoch zu erwarten, dass elektromagnetische Abschirmung für Portemonnaies bald genauso üblich sein wird wie eingewebte Metallfäden in Winterhandschuhen.

Bauen am IT-Grundschutz

Am 19.02.2012 hat das BSI auf den Webseiten zum IT-Grundschutz die Entwürfe für drei neue Bausteine (Webanwendungen, MacOSx und OpenLDAP) zur Kommentierung bereitgestellt. Da die Weiterentwicklung der IT-Grundschutz-Kataloge zur Zeit etwas stagniert – die 11. Ergänzungslieferung aus 2009 ist immer noch die aktuelle zertifizierungsrelevante Version – ist die Fortschreibung von Bausteinen zu begrüßen. Eine Kommentierung der Entwürfe legen wir allen Interessierten ans Herz.

Die Bereitstellung der bereits im Juni 2011 zunächst nur als pdf publizierten 12. Ergänzungslieferung mit anderen wichtigen Bausteinen als Meta-Daten für das Grundschutz-Tool sowie als html-Version wird dennoch sehnlich erwartet.

Multimedialer Overflow

Der Titel "Spiel mir das Lied vom Rootkit" im Heise-Newsticker vom 30.01.2012 gefiel auch uns – die darin vorgestellte Angriffsmethode allerdings weniger: Eine präparierte Midi-Datei auf einer Webseite kann via Internet-Explorer und Windows-Media Player über eine Heap Spray Attacke einen Buffer Overflow in der Bibliothek winmm.dll auslösen. Anschließend kann beliebiger Code ausgeführt und das System übernommen werden. Trojaner, die die Schwachstelle ausnutzen, sind bereits im Umlauf. Mit einem Patch von Microsoft wurde die Schwachstelle, von der zahlreiche Windows-Systeme betroffen sind, im Januar behoben.

Soweit so vertraut: Richtig neu sind Buffer Overflows in Multimediaanwendungen nicht. Im Gegenteil: Darüber sollten Softwareentwickler inzwischen hinaus sein. Zu befürchten ist aber wohl, dass auch weiterhin derartige Schwachstellen aufgedeckt werden. Dagegen helfen nur Ansätze wie das Sandboxing von IE9, dedizierte Lösungen wie Bitbox oder Surf-VMs à la c't Surfix. Oder eine komplette Trennung des Internetzugangs vom Client-PC über eine virtuelle Maschine wie ReCoBS. Btw.: Haben Sie auf den ersten Link des Beitrags geklickt?

Wer zweimal klaut...

Zum Schutz gegen Urheberrechtsverletzungen im Internet werden derzeit Warnhinweismodelle diskutiert. Danach sollen Zugangsprovider auf Veranlassung von Rechteinhabern Anschlussinhabern, die eine Urheberrechtsverletzung begehen, eine Warnung zusenden sowie eine Liste der gewarnten Anschlussinhaber führen. Nach einer festzulegenden Zahl von Verstößen sollen die Rechteinhaber informiert werden; sie können dann entscheiden, ob sie eine Auskunft über den Anschlussinhaber zur Rechtsverfolgung einholen möchten.

Das Bundeswirtschaftsministerium (BMWi) hat nun am 01.02.2012 eine 2011 in Auftrag gegebene vergleichende Studie über Warnhinweismodelle und die Umsetzbarkeit eines solchen Modells in Deutschland veröffentlicht. Die knapp 350seitige Studie (zzgl. 50 Seiten Anhang) bewertet die Modelle grundsätzlich positiv, unter der Voraussetzung, dass bei Missachtung der Warnungen eine konsequente Rechtsverfolgung erfolgt.

Voraussetzung für das Modell ist jedoch eine Vorratsdatenspeicherung der Zugangsanbieter. Die Studie geht von der grundsätzlichen Zulässigkeit der Verwendung dieser Daten aus. Das Datenschutzrecht wird jedoch nur oberflächlich und fehlerhaft berücksichtigt: So verwechseln die Autoren bezüglich der zu führenden Liste Anonymität und Pseudonymität; auch wird die Erforderlichkeit außer Acht gelassen, bei der Übermittlung von Mehrfachverstößen nach Rechteinhabern zu differenzieren.

Nebenbei liefert die Studie außer dem Vergleich der verschiedenen europäischen Ansätze einen Einblick in die derzeitigen Planspiele der Bundesregierung.

Secorvo News

Bildungszeit

Vom 13.-15.03.2012 haben Sie die Möglichkeit, Ihre IT-Security-Grundlagenkenntnisse beim Seminar IT-Sicherheit heute aufzufrischen. Sichern Sie sich kurzfristig noch einen der freien Plätze. Wir freuen uns auf Ihre Teilnahme!

Die nächste Schulung mit anschließender Zertifikatsprüfung zum TeleTrusT Information Security Professional (T.I.S.P.) findet vom 07.-11.05.2012 statt. Bei frühzeitiger Anmeldung bekommen Sie Ihr Exemplar des T.I.S.P.-Buchs rechtzeitig vorab zugesandt.

Ebenfalls im Mai, vom 23.-24.05.2012, können Sie sich beim Seminar Aktuelle Herausforderungen der Informationssicherheit einen Überblick über neue Angriffsszenarien und Risiken sowie wirksame Schutzstrategien und Sicherheitstechnologien verschaffen.

Die Programme aller Seminare sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Rolltor für den Online-Shop

Die Entwicklung sicherer Online-Plattformen, die potentiell jedem Angreifer ausgesetzt sind, stellt aus Sicherheitssicht eine ganz besondere Herausforderung dar. Sie stellen gänzlich neue Anforderungen an die Qualifikation der Entwickler, die Sicherheitskultur des Unternehmens und die Qualität und Verfügbarkeit von Sicherheitswerkzeugen.

Matthias Honka (asknet AG) beleuchtet in seinem Vortrag auf dem kommenden KA-IT-Si-Event am **01.03.2012** die Gratwanderung zwischen agiler Softwareentwicklung und schneller Reaktion auf Kundenwünsche einerseits und Kontrollmaßnahmen zum Schutz digitaler Güter andererseits. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

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

März 2012	
01.03.	Rolltor für den Online-Shop (KA-IT-Si, Karlsruhe)
13.-15.03.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-16.03.	Black Hat Europe 2012 (Blackhat, Amsterdam/NL)
21.-22.03.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
26.-30.03.	CPSSE (Secorvo College, Karlsruhe)
April 2012	
15.-19.04.	Eurocrypt 2012 (IACR, Cambridge/UK)
16.-17.04.	a-i3/BSI-Symposium 2012 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
Mai 2012	
07.-12.05.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
23.-24.05.	Aktuelle Herausforderungen der Informations-sicherheit (Secorvo College, Karlsruhe)

Fundsache

Der Branchenverband BITKOM hat am 03.02.2012 die digitale Fassung einer Broschüre mit Sicherheitstipps für Smartphone-Nutzer publiziert, die für den IT-Gipfel 2011 erstellt worden war. Ein hilfreiches Handout auch für Unternehmen – wenn die wesentliche Nachricht auch ist: Wenn Ihr Sicherheit wollt, müsst Ihr Zeit investieren.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

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