secorvo
security consulting

Secorvo Security News

September 2010

Laufzeitverlängerung

In Deutschland wurde im vergangen Jahrhundert eine Technologie eingeführt, die man für so sicherheitskritisch hielt, dass ihre Rahmenbedingungen gesetzlich geregelt wurden und der Bund eine Aufsichtsbehörde etablierte, um die Unternehmen zu überwachen, die die kritischen Anlagen zur Nutzung dieser Technologie betreiben. Die Begeisterung der Bürger über diese Technologie hielt sich stark in Grenzen – nun aber wird aus Gründen der Wirtschaftlichkeit diskutiert, ob die Bundesregierung nicht deren Laufzeit verlängern sollte.

Nein, die Rede ist nicht von der Nutzung der Kernenergie – sondern von der „qualifizierten elektronischen Signatur" (QES).

In einem Gutachten zu den Auswirkungen des ELENA-Verfahrens auf Wirtschaft, Bürger und Verwaltung vom 13.09.2010 stellte der Nationale Normenkontrollrat kürzlich fest, dass der mit Abstand größte Kostenfaktor auf Verwaltungsseite die Erstattung für die QES an die Antragsteller ist, die damit ihr Einverständnis zum Abruf ihrer Daten geben müssen – und das, obwohl die Beträge sehr optimistisch geschätzt wurden. Zur Kostensenkung wird nun vorgeschlagen, die Gültigkeit des QES-Zertifikats von fünf auf zehn Jahre zu verdoppeln oder aber gleich einen QES-fähigen Dritten „stellvertretend" schriftlich (sic!) zur Abruf-Autorisierung zu ermächtigen.

Nun ist aus Sicherheitsgründen die Gültigkeit der QES-Zertifikate per Rechtsverordnung auf fünf Jahre begrenzt, und auch die Sicherheit der Kryptoalgorithmen wird derzeit nur für sieben Jahre prognostiziert. Daraus lässt sich nun zweierlei folgern: Entweder wurden die durch ELENA möglichen Einsparungen deutlich zu optimistisch dargestellt. Oder aber die Nutzung der QES wird seit mehr als einem Jahrzehnt mit übertriebenen Sicherheitsrestriktionen gegängelt – und so unnötig verteuert.

Zum Glück ist es nur die qualifizierte Signatur, über deren Nutzung so munter spekuliert wird. Und nicht die Atomkraft.

Inhalt

secorvo
security consulting

Security News

Auslaufmodell Passwort

Seit 2003 ist es dank der von P. Oechslin entwickelten Rainbow-Tables heute für Passwort-Cracker um ein Vielfaches leichter, ein einwegverschlüsseltes Passwort zu rekonstruieren. Besonders betroffen von solchen Angriffen sind die Passwort-Hashes des Windows (LM) und des NT LAN Managers (NTLM), die kein „Salz" beim Hashen verwenden.

Oechslins Unternehmen stellt eine Webseite zur Verfügung, über die sich in Sekundenschnelle praktisch alle bis zu 14-stelligen Windows-Passwörter aus dem LM-Hash rekonstruieren lassen. Und im Projekt RainbowCrack (siehe SSN 8/2010) wurden inzwischen die NTLM-Hashes für fast alle achtstelligen Passwörter aus Großbuchstaben, Kleinbuchstaben und Ziffern tabelliert – auch für alle kürzeren Passwörter mit Sonderzeichen, und für alle neunstelligen aus Kleinbuchstaben und Ziffern.

Wenn irgend möglich sollten Windows XP-Administratoren daher LM-Hashes deaktivieren – bei Windows Vista ist dies ohnehin die Grundeinstellung, und Windows-Passwörter unter neun Zeichen Länge sollten grundsätzlich tabu sein.

Zehnstellige und längere Passwörter, die inzwischen zu fordern sind, sind für Anwender eine Zumutung – es scheint nun endgültig an der Zeit, über Alternativen wie Smartcard Logon nachzudenken.

Smartes Energienetz

Am 22.09.2010 veröffentlichte das amerikanische Marktforschungsunternehmen PikeResearch eine Studie, die für das intelligente Stromnetz (vulgo „Smart Grid") ein Marktwachstum von 75% für die kommenden Jahre vorhersagt – auf einen mehrstelligen Milliardenbetrag in 2015. Kein Wunder, dass sich Unternehmen wie Cisco bereits in Stellung bringen und Miele auf der IFA die ersten Smart-Grid-fähigen Haushaltsgeräte vorgestellt hat. Dass sich aus der Verbindung von Stromnetz, Haushaltsgeräten und Internet neue Schwachstellen ergeben, ist leicht auszumalen: Verhaltensprofile beim Messstellenbetreiber und ferngesteuerte Waschmaschinen bieten viel Stoff für Phantasien.

Auf diese Gefahren reagierte das US-amerikanische NIST am 02.09.2010 mit der Publikation der 600 Seiten starken Richtlinie „Guidelines for Smart Grid Cyber Security". Teil 2 des dreibändigen Werks ist dem Thema Datenschutz gewidmet. An ausgewählten Beispielen wird darin deutlich, welche Begehrlichkeiten der Zugriff auf Stromverbrauchsdaten wecken dürfte: So lokalisierte eine amerikanische Regierungsbehörde anhand des Energieverbrauchs pro Wohnfläche eine Marihuanazucht.

Auch in Deutschland werden datenschutzrechtliche Einwände gegen die Datenerhebung der derzeit ausgerollten Smart Metern laut. Denn aus dem Gebot in § 21b Abs. 3a EnWG, Messeinrichtungen bereitzustellen, die „den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegeln", lässt sich kein Erfordernis zur zeitnahen Übermittlung der Messdaten an den Messstellenbetreiber ableiten – zur Abrechnung reicht die Übermittlung der zeitlich aggregierten Daten.

Auch zur Bereitstellung der in § 40 Abs. 3 EnWG geforderten „lastvariable[n] Tarife" ist eine alternative Gestaltung denkbar: die Daten können z. B. so übertragen werden, dass eine Zuordnung einzelner Datensätze zu einem konkreten Zähler nicht möglich ist – und somit auch keine Erstellung haushaltsbezogener Profile.

Die derzeitigen Implementierungen, bei denen die Verbrauchsdaten im 15-Minuten-Intervall an den Energieversorger übermittelt werden, ist zur Vertragserfüllung nicht erforderlich – und mit dem Prinzip der Datensparsamkeit unvereinbar. Eine datensparsame Realisierung käme hingegen ganz ohne Profile außerhalb des Haushaltes aus.

Traurige Nachricht

Am 23.09.2010 ist im Alter von 52 Jahren überraschend Andreas Pfitzmann verstorben. Mitte der 80er Jahre hatte er mit seinen Arbeiten an der Universität Karlsruhe den „technischen Datenschutz" begründet und war seitdem ein einflussreicher Mahner und Mittler zwischen den Welten des Rechts, der Informatik und gesellschaftlicher Fragestellungen. Andreas Pfitzmann hat nicht nur durch seine mehr als 250 Veröffentlichungen und Stellungnahmen wichtige Weichenstellung der Technikgestaltung beeinflusst, auch als Gutachter des Bundesverfassungsgerichts (Vorratsdatenspeicherung, Online-Durchsuchung) und vieler Bundesbehörden, sondern auch als Hochschullehrer hunderte Studenten für das Thema begeistert. Er wird uns fehlen.

Datenschutz-Informationsquelle

Am 17.09.2010 hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) offiziell ein neues Datenschutz-Wiki als Nachschlagewerk für Datenschutz-Laien und Fachleute eröffnet. Das zum Start verständlicherweise noch recht überschaubare Angebot ist nicht amtlich und offen für jeden Interessierten. Auch die im Internetauftritt des BfDI enthaltenen Materialien sollen übernommen werden, vielleicht auch Texte der Luchterhand-Loseblatt-Sammlung.

Hervorgegangen ist das neue Angebot aus dem Datenschutz-Forum, einem Diskussionsforum zu Datenschutzfragen. Es reiht sich ein in weitere Informationsangebote wie das virtuelle Datenschutzbüro des ULD, das Berichtsarchiv ZAfTDa der FH Gießen-Friedberg, das thematisch engere Wiki des AK-Vorratsdatenspeicherung, die Dokumentation von Datenschutzvorfällen des Projekts Datenschutz und das stärker Material orientierte DuD-Wiki.

Für eine faire Bewertung der Qualität ist es noch zu früh, und verschiedene Bereiche wie die Kategorienbildung, bereitgestellte Artikelvorlagen und die Hilfe bedürfen noch der Entwicklung. Grundsätzlich ist die Initiative jedenfalls zu begrüßen. Es ist zu hoffen, dass durch die Beteiligung vieler Experten eine Wissenssammlung entsteht, die auch Hilfestellung in Zweifelsfällen und Auslegungsfragen bietet.

Servergesteuertes NoScript

In sicherheitsbewussten Kreisen sind die Firefox-Erweiterungen NoScript und RequestPolicy, durch die sich Nutzer vor Cross-Site-Scripting (XSS) schützen können, inzwischen fester Bestandteil des Browsers. Die Freude daran wird jedoch dadurch getrübt, dass ein Nutzer ständig entscheiden muss, welche Webseite er für hinreichend vertrauenswürdig hält, um aktive Elemente zuzulassen.

Mit einem Konzept für serverbasierte Vorgaben, "Content Security Policy" (CSP) genannt, gibt Mozilla nun Anbietern die Möglichkeit festzulegen, welchen Dritt-Anbietern von Inhalten mit aktiven Komponenten vertraut werden soll. Damit wird ein Teil der Funktionalität von NoScript und RequestPolicy fest in der kommenden Version 4 des Firefox-Browsers verankert. Die Gefahr eines XSS-Angriffs wird damit signifikant beschränkt, sofern CSP auch von Web-Anbietern genutzt wird. Bis dahin wird es sicher noch etwas dauern – das Interview mit dem Chefentwickler Brandan Sterne mag die Wartezeit ein wenig verkürzen.

Schweigendes Orakel

Eine spezielle Klasse von kryptologischen Angriffen nutzt das angegriffene System als „Orakel", indem diese aus unterschiedlichen Reaktionen (sprich: differenzierten Fehlermeldungen) ableiten, bis zu welchem Punkt der Angriff erfolgreich verlaufen ist.

Nach SSL und WPA (vgl. SSN 11/2008) hat ein solcher Orakel-Angriff nun die Cookies und Sitzungsdaten von ASP.NET-Webservern getroffen, wie Microsoft am 17.09.2010 einräumte: Mit einer auf das Jahr 2002 zurückgehenden Technik können diese Daten ohne Kenntnis des Schlüssels Bit für Bit entschlüsselt werden, solange der Server jedes Mal zurückmeldet, ob bei seinem Entschlüsselungsversuch korrekte Padding-Bits entstanden oder nicht.

Der zunächst von Microsoft empfohlene Workaround entbehrte nicht einer gewissen Ironie: Man nutze die „customErrors" Funktionalität, um die Fehlermeldungen unspezifisch umzugestalten...

OWASP lebt

Am 09. und 10.09.2010 fand die diesjährige weltweite OWASP Konferenz „AppSec 2010" im kalifornischen Irvine statt. Die von etwa 300 internationalen Experten besuchte und mit herausragenden Referenten besetzte Veranstaltung zeichnete sich durch spannende Fachdiskussionen über den Status und die Entwicklung der Web-Sicherheit aus. Zu den Highlights zählte die Keynote von David Rice, der Parallelen zwischen der Regulierung im Umweltschutz und der Web-Sicherheit aufzeigte. Alle Vorträge sollen in Kürze online verfügbar sein.

Interessierte sollten sich den 20.10.2010 vormerkten – an diesem Tag findet in Nürnberg die OWASP AppSec Germany 2010 mit einem ähnlich spannenden Programm statt.

Secorvo News

Secorvo College aktuell

Experten unter sich: Die kommenden Seminare von Secorvo College bieten dank der sehr guten Nachfrage eine ganz besondere Gelegenheit für einen intensiven fachlichen Erfahrungsaustausch, sei es über das Thema PKI, Audit, ISM oder Datenschutz.

Wissensvermittlung durch Secorvo gepaart mit fruchtbaren Diskussionen und viel Praxiserfahrung – noch gibt es freie Plätze bei den Oktober- und Novemberveranstaltungen.

Teamverstärkung

Mit Klaus J. Müller hat das Secorvo-Team am 01.09.2010 erneut Zuwachs bekommen – und damit unsere gesammelte Erfahrung im Gebiet Informationssicherheit und Datenschutz um 10 auf exakt 200 Jahre angehoben. Neben „klassischen" Themen der IT-Sicherheit hat sich Klaus Müller intensiv mit Smart Metern beschäftigt, nachzulesen unter anderem in der Fachzeitschrift DuD („Gewinnung von Verhaltensprofilen am intelligenten Stromzähler", DuD 6/2010).

Veranstaltungshinweise

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

Oktober 2010	
04.-07.10.	ISSE 2010 (Teletrust, Berlin)
04.-07.10.	Sicherheitsmanagement heute (Secorvo College)
09.-15.10.	Hacker Halted 2010 (Hacker Halted USA, Miami/US)
19.-21.10.	it-sa (SecuMedia Verlag, Nürnberg)
21.10.	it-sa Datenschutztag 2010 (Computas, Nürnberg)
26.-28.10.	IT-Sicherheit heute (Secorvo College)
November 2010	
03.-04.11.	#days Workshops: Exploit Laboratory / Protecting from GSM attacks (DEFCON, Luzern/CH)
05.-06.11.	#days Conference (DEFCON, Luzern/CH)
09.-12.11.	PKI (Secorvo College)
15.-17.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
18.-19.11.	34. DAFTA (GDD e.V., Köln)
22.-26.11.	T.I.S.P.-Schulung (Secorvo College)
Dezember 2010	
06.-07.12.	IsSec/ZertiFA 2010 (Computas, Berlin)

Fundsache

Am 20.09.2010 veröffentlichte Chintan Shah in seinem Blog bei McAfee eine lesenswerte Analyse eines der derzeit leistungsfähigsten (und damit gefährlichsten) „Crimeware"-Werkzeuge: Zeus. Über Konfigurationseinträge lässt sich Zeus zu einem individualisierten Banking-Trojaner umgestalten – der inzwischen sogar Angriffsmuster gegen das mTAN-Verfahren beherrscht.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

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