secorvo
security consulting

Secorvo Security News

April 2015

Maßlos

Angenommen, wir besäßen ein riesiges Stück Papier mit einer Materialstärke von 0,09 mm. Wie oft müssten wir dieses Papier falten, um den Abstand zwischen Erde und Mond (ca. 384.400 km) zu überbrücken? Den Rechenweg kennen wir aus der Schule:

$$2^n \cdot 0{,}09 \text{ mm} = 384.400 \text{ km},$$
$$\text{also: } n = \log_2 (42{,}71 \cdot 10^{11}) \approx 42.$$

Ein überraschend kleiner Wert, den wir – Douglas-Adams-Fans ausgeschlossen – eher nicht erwartet hätten. Die kleine Rechnung zeigt, wie schwer wir uns exponentielles Wachstum vorstellen können.

Und das hat Folgen. Im Januar 1997 lobte die Firma RSA eine *Crypto Challenge* aus: Eine mit RC5 und einem 56 bit langen Schlüssel verschlüsselte Nachricht sollte durch eine Brute-Force-Attacke entschlüsselt werden. Das gelang einem riesigen Netzwerk von Freiwilligen, die die Leerlaufzeiten ihrer PCs für die Schlüsselsuche zur Verfügung stellten, in 270 Tagen. Einer dieser Freiwilligen war ein Student, den ich betreute. Nachdem der Schlüssel gefunden war, erklärte er mir freudestrahlend, jetzt wolle er mit den Institutsrechnern an der RC5-64 bit-Challenge teilnehmen. Als ich ihn fragte, wer ihm denn ein so langes Studium bezahle, sah er mich mit großen Augen an – und ich musste ihm vorrechnen, dass die Challenge die 2^8-fache Rechenleistung benötigt, seine 4.000 Teams ohne schnellere Rechner fast 190 Jahre suchen müssten.

So verleitet uns unsere mangelnde Vorstellungskraft, es bei Schlüssellängen ständig zu übertreiben. Denn ein 256 bit-AES-Schlüssel ist nicht doppelt, sondern 2^{128}-mal so sicher wie ein 128 bit-Key. Das ist, als wolle man ein Haus mit einer gepanzerten Tür dadurch sicherer machen, dass man nicht eine zweite, sondern gleich $3{,}4 \cdot 10^{38}$ zusätzliche Türen montiert. Die würden übrigens nicht in unser Universum passen – das hat lediglich einen Durchmesser von 93 Milliarden Lichtjahren (etwa $8{,}8 \cdot 10^{26}$ m), wir benötigten also 387 Milliarden weitere Universen gleicher Größe dafür.

Inhalt

Maßlos

Security News

Nächster Persilschein

Car to go

Ende des Passworts?

XP lebt!

Secorvo News

Symposium „No Blackout“

7. Tag der IT-Sicherheit

Mit Brief und Siegel

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Nächster Persilschein

Gerade ein Jahr ist es her, dass Microsoft einen vermeintlichen Persilschein der europäischen Datenschutz-Aufsichtsbehörden (Art.-29-Gruppe) für Microsoft Office 365 erhielt (SSN 04/2014). Nun hat auch Amazon den Datenschutz als Schlüssel zum europäischen Markt entdeckt und am 06.03.2015 ein ähnliches Dokument der luxemburgischen Datenschutzaufsicht (CNPD), stellvertretend für die Art.-29-Gruppe, für seinen Cloud-Service AWS erhalten. Wie zuvor Microsoft verkündet Amazon seitdem vollmundig, AWS sei damit datenschutzkonform einsetzbar. Tatsächlich schreibt die CNPD genau das Gegenteil: Sie habe lediglich gemäß dem Cloud-Leitfaden der Art.-29-Gruppe die Vertragsstruktur geprüft und will das positive Prüfergebnis gerade nicht als Freigabe für AWS verstanden wissen.

Derweil kämpfen die amerikanischen Cloud-Anbieter weiter um den europäischen und insbesondere den deutschen Markt und setzen dabei zunehmend auf nationale Niederlassungen, wie den AWS Marketplace in Frankfurt. Doch die augenscheinlich lokal angebotenen Dienste sind weiterhin in die globale Infrastruktur des Anbieters eingebunden. Cloud-Willige sollten daher nicht den Fehler machen, sich ohne eine gründliche (datenschutz-) rechtliche und (sicherheits-)technische Prüfung auf die Marketing-Aussagen der Anbieter zu verlassen.

Car to go

Das Keyless-System PKES entriegelt Fahrzeugtüren automatisch, wenn der Besitzer naht. Oder auch ein geschickter Dieb: Am 06.04.2015 musste der Reporter Nik Bilton zusehen, wie zwei Teenager mit seinem Toyota Prius davonfuhren. Wahrscheinlich nutzten die beiden einen simplen Signalverstärker, der die Reichweite der Kommunikation zwischen Token und Fahrzeug vergrößerte.

Der Fehler liegt nicht im verwendeten kryptografischen Protokoll - denn Kryptografie hilft nicht gegen diese Art von Angriffen. Ein weiteres Beispiel dafür, dass mancher Komfortgewinn nur auf Kosten der Sicherheit erhältlich ist.

Zur Prävention können betroffene Autobesitzer ihr Token mit Schutzhüllen vor Funksignalen abschirmen – oder besser gleich wieder auf herkömmliche Schlüssel mit Knopfdruckentriegelung umsteigen.

Ende des Passworts?

Die unter anderem von Paypal initiierte FIDO-Alliance, der inzwischen weitere Größen wie Alibaba oder die Bank of America beigetreten sind, engagiert sich neben der 2-Faktor-Authentifikation (U2F, siehe SSN 10/2014) verstärkt für biometrische Authentifikationsverfahren (Fingerabdruck-, Herzrhythmus- und Venenerkennung) und hat am 09.12.2014 Version 1.0 ihres Universal Authentication Framework (UAF) veröffentlicht.

Doch Biometrie hat bekannte Schwächen. Jüngst zeigten das der Vortrag von starbug auf dem 31. Chaos Communication Congress am 27.12.2014, der u. a. über Kameras in Mobiltelefonen biometrische Merkmale ausspähte, und der Hack des iPhone-Fingerabdrucksensors von Ben Schlabs, dem es im September 2014 gelang, den Sensor mit einem Holzleim-Fingerimitat zu täuschen.

Ein grundsätzliches Problem ist, dass sich biometrische Merkmale, wenn sie einmal gestohlen wurden, nicht einfach wie ein Passwort ändern lassen – lediglich der Fingerabdruck erlaubt bis zu neun Wechsel. Das wiegt umso schwerer, als dieselben biometrischen Merkmale unvermeidlich für die Authentifikation in zahlreichen unterschiedlichen Anwendungen zum Einsatz kommen werden.

Mit Passwörtern werden wir daher wohl noch eine Weile leben und sollten uns mit Verfahren beschäftigen, die zu sichereren Passwörtern führen. So lassen sich Anwender möglicherweise zu Wahl stärkerer Passwörter bewegen, wenn sie von Passwort-Managern unterstützt werden. Und Anwendungen könnten die Stärke eines gewählten Passworts mit Passwort-Metern bei der Eingabe messen und zu schwache Passwörter zurückweisen.

XP lebt!

Totgesagte leben länger. Dies belegen Anfragen der Grünen und der Piratenpartei zum Einsatz von Windows XP in der Berliner Stadtverwaltung anlässlich des bevorstehenden Ablaufs der teuer bezahlten Supportverlängerung von Microsoft: Ab April 2015 werden keine Aktualisierungen mehr geliefert. Tatsächlich ist Berlin nicht die einzige Stadtverwaltung, bei der ältere Anwendungen die Ablösung von Windows XP bisher verhindert haben. Auch werden noch eine Vielzahl von Geldautomaten unter Windows XP betrieben. Wie groß aber ist die Gefährdung durch Windows XP wirklich?

Werden neu entdeckte Sicherheitslücken von XP nicht mehr behoben, steigt das Risiko, dass Schadsoftware durch Ausnutzung dieser Lücken Systeme befällt. Dagegen hilft eine strikte Entkopplung der produktiven Anwendungen von „Malwarezugängen“ wie dem Internet, den lokalen Datenschnittstellen (vulgo USB-Anschlüsse) und dem Einfallstor E-Mail-Anhang.

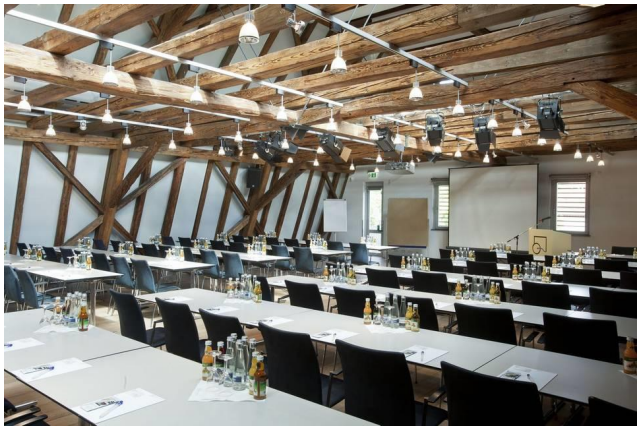
Realisieren lässt sich das, indem man z. B. den Internet- und E-Mail-Zugang über einen Terminalserver bereitstellt oder, noch besser, die alte Software in eine virtuelle Maschine mit XP verfrachtet – und diese auf aktuellen Windows-Clients betreibt.

Dass Abschalten keine Lösung, sondern „friendly fire" ist, dürfte auch dem Berliner Datenschutzbeauftragten Dix klar sein. Mit einer besonnenen und differenzierten Analyse lassen sich Lösungen finden, XP-abhängige Anwendungen mindestens für eine Übergangszeit und mit vertretbaren Komforteinbußen für die Benutzer weiter zu betreiben, ohne damit einen Sicherheits-Gau zu riskieren.

Secorvo News

Symposium „No Blackout"

Anlässlich der bevorstehenden Verabschiedung des IT-Sicherheitsgesetzes und der daraus folgenden Verpflichtungen von Betreibern kritischer Infrastrukturen veranstaltet Secorvo am **12.** und **13.05.2015** das Symposium „No Blackout – IT-Sicherheit für die Energieversorgung" in der Buhlschen Mühle in Ettlingen.



Die Veranstaltung richtet sich nicht nur an Unternehmen und Institutionen aus dem Bereich der kritischen Infrastrukturen – sie bietet wertvolle Erfahrungen für alle Firmen, die den Aufbau eines Information Security Managements (ISMS) planen oder bereits vorbereiten.

Unter anderem werden die Stadtwerke Ettlingen über den „fx-Hack" und die Folgen berichten, und wir werden etwas über die IT-Sicherheit in Kernkraftwerken erfahren. Gelegenheit zur Diskussion bieten das gemeinsame Dinner in der Villa Hartmaier's am 12.05. und die Networking-Pausen.

Wir freuen uns auf Ihre Teilnahme.

7. Tag der IT-Sicherheit

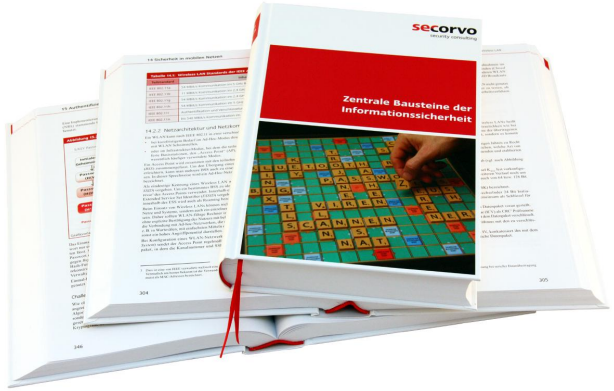
Beim 7. Tag der IT-Sicherheit am **19.05.2015**, einer Kooperationsveranstaltung der KA-IT-Si mit der IHK Karlsruhe, dem CyberForum und KASTEL, informiert das Landesamt für Verfassungsschutz über die aktuelle Bedrohungslage und die Risiken „Mensch" und „Technik". Es folgen Fachvorträge zu den Themen Netzwerksicherheit, Datenschutz und Mobile Computing. Das Programm schließt mit einem Live-Hacking, in dem gezeigt wird, welche Sicherheitsschwächen zahlreiche Webanwendungen aufweisen.

Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern bieten die „Networking-Pausen". Wir freuen uns auf Ihre Anmeldung.

Mit Brief und Siegel

Seit vielen Jahren setzt Secorvo College auf Seminare, bei denen die Teilnehmer ihre Qualifikation durch eine anschließende Prüfung und ein Zertifikat nachweisen können.

Dazu zählt insbesondere der T.I.S.P. (TeleTrusT Information Security Professional), ein inzwischen deutschlandweit anerkanntes Expertenzertifikat für Informationssicherheit. In unseren T.I.S.P.-Schulungen erhalten Sie in fünf Tagen einen kompakten Überblick zu allem, was in der Informationssicherheit zählt – unterstützt vom T.I.S.P.-Buch „Zentrale Bausteine der Informationssicherheit". Auf dem Seminar vom **22.** bis **26.06.2015** gibt es noch wenige Plätze; weitere Gelegenheiten zur Zertifizierung Ihrer Expertise bieten wir im September (**21.–25.09.2015**) und November (**23.–27.11.2015**) in unseren Seminarräumen in Karlsruhe.



Die Zertifikatsschulung T.E.S.S. – Sichere Systeme dank System Security Engineering zeigt Wege auf, wie ganze Systeme mit allen Komponenten, Schnittstellen und Prozessen mit angemessener Sicherheit gestaltet werden können. Der T.E.S.S. (TeleTrusT Engineer for System Security) steht für interdisziplinäre Sicherheitskompetenz. Termine: **14.–19.06.2015** und **10.–13.11.2015** in Karlsruhe.

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/college.

Veranstaltungshinweise

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

Mai 2015	
06.-07.05.	16. Datenschutzkongress (EUROFORUM, Berlin)
12.-13-05.	Symposium „No Blackout“ – IT-Sicherheit für die Energieversorgung (Secorvo, Karlsruhe)
18.-21.05.	OWASP AppSec EU 2015 (OWASP Foundation, Amsterdam/NL)
18.-20.05.	IMF 2015 (Fraunhofer IAO, Magdeburg)
19.-21.05.	14. Deutscher IT-Sicherheitskongress (BSI, Bonn)
19.05.	7. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si; Karlsruhe)
20.-22.05.	Entwicklertag 2015 (VKSI, GI, ObjektForum; Karlsruhe)
26.-28.05.	IFIP SEC 2015 (IFIP, Hamburg)
Juni 2015	
08.-12.06.	Audit Challenge 2015 (Frankfurt School of Finance & Management, Frankfurt)
15.-16.06.	DuD 2015 (COMPUTAS, Berlin)

Fundsache

Am 02.04.2015 wurden vom Open Crypto Audit Project die Ergebnisse des TrueCrypt-Audits (v7.1a) veröffentlicht. Mängelfrei ist die Software nicht, aber Hintertüren oder einfach ausnutzbare Angriffsmöglichkeiten wurden nicht gefunden. Trotz der Einstellung der Weiterentwicklung spricht also derzeit nichts gegen die Nutzung dieser Version – oder auf TrueCrypt aufbauender Lösungen wie VeraCrypt.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Sven Köhler, Christoph Schäfer

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