Eine Eins mit 290 Nullen

Man könnte es eine Falschmeldung nennen oder behaupten, der Autor sei sogar zu faul oder zu dumm, bei Wikipedia zu suchen: „Nach allem, was bekannt ist, brauchen auch die Mathematiker der NSA mit ihren Großrechnern für das Knacken asymmetrischer Verschlüsselung viele Jahre“, schreibt Spiegel online.

Falsch. Guckst du hier: „Für den 2048 Bit Schlüssel bräuchte man also ca. (ganz grob) 10^290 (Das ist eine Eins mit 290 Nullen) ‚mal so lange, wie das Universum existiert…“

Das sind natürlich viele Jahre. Sehr viele. Insofern ist es auch keine Falschmeldung. Mein Schlüssel hat übrigens 4096 Bit.

Wir wissen den großen Bruder zu schätzen

Bild.de (vgl. auch Golem.de): „Tatsächlich aber speichern Programme wie PRISM nahezu ALLE Inhalte von elektronischer Kommunikation außerhalb der USA, auch in Deutschland. (…) Nach BILD-Informationen hat zumindest der Bundesnachrichtendienst seit Jahren von der enormen Vorratsdatenspeicherung der US-Dienste Kenntnis – und hat in den vergangenen Jahren aktiv darauf zugegriffen. (…) So ging es bei der Friedrich-Reise nach BILD-Informationen vor allem darum, der US-Regierung zu versichern, dass man die zahlreichen Hinweise von NSA und CIA sehr zu schätzen wisse.“

Ach.

Das Bundesverfassungsgericht kann also das jüngst neu geschaffene „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ wieder in die Tonne treten. Unsere Behörden und den Innenminister interessiert das einen Dreck, und die US-Amerikaner sowieso.

Handel mit Edelsteinen

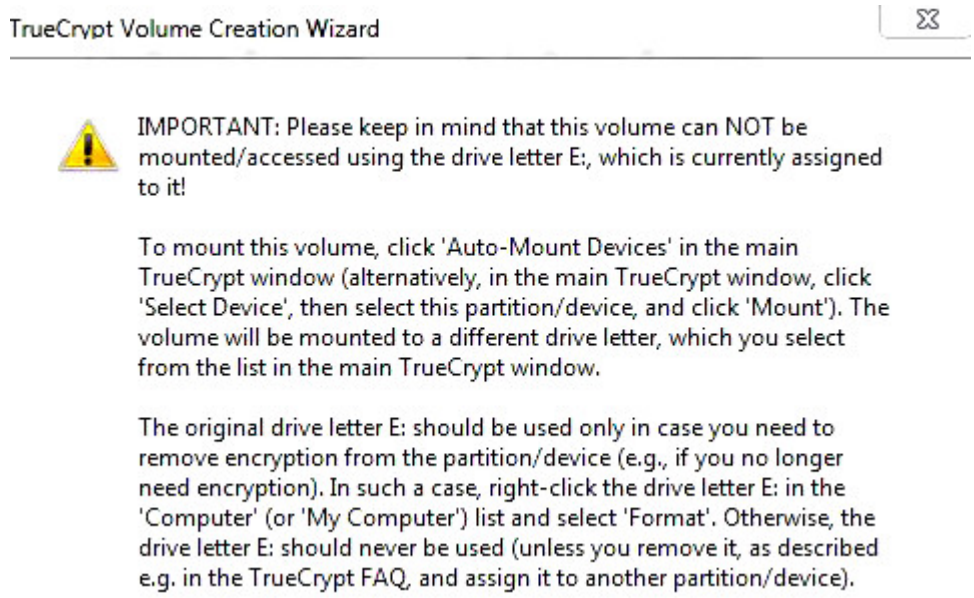
Mein Avatar (links, der mit den zwei Schwertern auf dem Rücken und der Maske) handelt mit Edelsteinen. Das Bankgebäude, in der das Feilschen stattfindet, habe ich auch selbst gebaut, und natürlich auch die „Edelsteine“. Das musste mal gesagt werden. Es ist übrigens meine Bank.

Nur zum virtuellen Chillen, bevor es wieder politisch und/oder ökonomisch wird oder ich die wohlwollenden Leserinnen und geneigten Leser mit technischen Problemen behellige. Ich werde mich gleich in der realen Welt auf eine sonnige Wiese legen, das Laptop mitnehmen und ein wenig arbeiten.

Tutorial Beta

Die Einführung für die beiden Tutorials ist fertig.

Hidden Volume – Expertinnen gefragt



Eine Frage an die Truecrypt-ExpertInnen – das Setting ist wie folgt: Ein Hidden Container auf einem USB-Stick, darin Thunderbird Portable samt Enigmail und GPG für Thunderbird Portable. So weit, so gut.

Das Problem ist: Wenn ich an einem fremden Rechner säße, auf dem Truecrpyt *nicht* installiert ist, kann ich das Hidden Volume gar nicht öffnen. Deswegen frage ich mich, wie ich Truecrypt Portable auf den Stick kriege, also sozusagen am

Hidden Volume „vorbei“. Es sehe keine Möglichkeit.

Oder hätte ich erst den ganzen Stick in einen Truecrypt-Container verwandeln müssen, um dann *darin* noch einen Hidden Volume anzulegen? Die Option habe ich gar nicht gesehen…

Schreibender Gringo mit frischem Hemd

Das muss man erklären: Ich sitze hier (1984) auf dem „Dachgarten“ einer einfachen Pension in Cusco, Perú, ungefähr hier, wo die Straßen Huaynapata und Teesecocha aufeinanderstoßen – an der südlichen Ecke war die Persion. (Die kostete damals umgerechnet einen Euro pro Nacht – heute wäre sie vermutlich unbezahlbar.)

Wir waren vorher acht Wochen im bolivianischen Urwald gewesen und hatten per Boot den Rio Madre de Dios von Riberalta bis zur peruanischen Grenze im Westen des Pando bereist (vgl. 04.04.2011: „Der Kautschuksammler, revisited“), und sind dann

von Puerto Maldonado per LKW bis hinauf in die Anden gefahren – über eine der gefährlichsten Straßen der Welt.

Will sagen: Ich war froh, dass an mir noch alles heil war. In Cusco sah ich die erste – wenn auch primitive und eiskalte – Dusche seit rund zwei Monaten, und wir konnten auch zum ersten Mal unsere Sachen mit normalem Wasser waschen und nicht mit Flusswasser. Ich fühle mich relaxed und wie im Luxushotel und trug zur Feier des Tages ein fast weißes Hemd.

Big Brother Watch Online Privacy Survey

Umfrage „Big Brother Watch Online Privacy Survey“ (März 2013). IVPN fragt:
But perhaps the most interesting statistic comes from Germany. According to the survey, Germany was the only country where a majority of respondents (56%) said they were not concerned about their privacy online. How should we read this finding?

Griechenland besänftigt europäische Gläubiger mit riesigem Holzpferd

Der Postillion (seit 1845): „Der stark verschuldete EU-Mitgliedsstaat Griechenland hat seine europäischen Gläubiger

mit der Schenkung eines riesigen Holzpferdes vorübergehend besänftigt. Das mehrere Tonnen schwere Präsent wurde in einer Nacht- und Nebelaktion vor der Europäischen Zentralbank in Frankfurt abgestellt…“

Geniale Lösung für Web-basisertes Verschlüsseln

Etwas unfassbar Praktisches – ich staune immer noch: In einem Artikel über Edgar Snowden wird auf Business Insider erklärt, wie PGP bzw. OpenPGP funktionieren. Dort empfiehlt man PGP Encryption Rool (iGolder), eine Web-Maske, in die man den öffentlichen Schlüssel des Empfängers postet, dann den Klartext der Nachricht. Man erhält dann einen verschlüsselten Text, den man per copy paste nur noch mit einem beliebigen E-Mail-Programm oder per Webmail verschicken kann.

Ich habe es ausprobiert – es funktioniert. Da der Betreiber der Website den geheimen Schlüssel des Empfängers nicht besitzt, hat die Sache keinen Haken. Ich finde das genial. (Allerdings würde ich mir von denen kein Schlüsselpaar erzeugen lassen.)

[Update] Das ist missverständlich ausgedrückt: Ich meinte natürlich, wenn man den Source Code hätte – es ware ein optimaler Ersatz für die PrivacyBox, die es leider nicht mehr gibt.

Tor and HTTPS

Electronic Frontier Foundation (EFF): Tor and HTTPS – „We prepared a graphic last year ago to try to help people visualize which data is concealed by the use of Tor.“ (Javascript erforderlich)

Nackter Mann

Caracas, sozusagen „backstage“: ein Mann ohne Hosen lief mitten über die Straße (1998). Ich habe nicht herausgefunden, was ihm geschehen war – ob er ausgeraubt worden war, ob er schlicht verrückt war oder ob er die falschen psychotrophen Substanzen geraucht hatte. Die Passanten lachten nur.

Newsletter German Privacy Fund Nr. 12

Der Newsletter German Privacy Fund Nr. 12 (02.07.2013) ist jetzt online. Der Newsletter erscheint alle zwei Wochen. Die Ausgabe Nr. 13 erscheint am 15.07.2013 (Montag). (Abonnement hier.)

Elektronische Post (Mail) ist grundsätzlich ein unsicheres Übertragungsmedium

Humboldt-Universität Berlin: *Auf ihrer Sitzung am 06.06.2013 hat das Präsidium seine Absicht beschlossen, bei der elektronischen Kommunikation an der HU Mails zu verschlüsseln, wenn diese besonders schützenswerte Daten, d.h. Daten vertraulichen Charakters, wie insbesondere Personalinformationen,*
enthalten. In einer ersten Erprobungsphase empfiehlt die Universitätsleitung die Anwendung von Verschlüsselungen, insbesondere im Mailverkehr zwischen den Verwaltungsbereichen der Universität.
Begründung: Elektronische Post (Mail) ist grundsätzlich ein unsicheres Übertragungsmedium.

Die nutzen natürlich S/MIME. Um den Popcorn-Effekt zu erhöhen, bitte die Anleitung Seite 11 lesen (verfasst vom Computer- und Medienservice der HU). Bin mal gespannt, wie populär das wird an der HU….

Friedrich redet Tacheles

„Ich bin der Herr Friedrich aus Deutschland, jetzt reden wir mal Tacheles.“

Religious websites contain more malware than porn sites

Sorry, diese Meldung von Symantec (via The Raw Story) ist schon mehr als ein Jahr alt, aber zu schön, als dass sie den wohlwollenden Leserinnen und geneigten Lesern vorenthalten werden sollte.

Also, liebe Kinder: geht *nicht* auf Websites, die propagieren, man solle höhere Wesen verehren oder die anderen Formen des Aberglaubens huldigen – etwa Esoterik. Das ~~hemmt eure geistige und psychische Entwicklung~~ ist gefährlich!

Statement by Edward Snowden

Wikileaks: „Statement by Edward Snowden to human rights groups at Moscow’s Sheremetyevo airport“.

Warum die Leute keine E-Mails verschlüsseln, revisited

Hinzufügen von GPG und Enigmail

Die portable Version von Mozilla Thunderbird ist mit Unterstützung für GPG und Enigmail erstellt worden, um EMails signieren und verschlüsseln zu können. Um GPG zu Thunderbird hinzuzufügen, laden Sie einfach GPG für Thunderbird Portable 1.4.13 (MD5: 627291d689f08577d0bb9dc2d2da1908) herunter und installieren Sie es einfach über Ihre bisherige Installation. Danach laden Sie die Enigmail-Erweiterung herunter und installieren es in Thunderbird. Wenn Sie Thunderbird Portable neu starten, haben Sie vollen Zugriff auf Enigmail und GPG, beides in portabler version.

Ich werde noch zum rasenden Elch. Aber falsch geraten. Ich will nicht auf faule NutzerInnen einprügeln, die sich weigern, E-Mails zu verschlüsseln, sondern auf die Pappnasen, die auch mit daran schuld sind, dass das kaum jemand macht und Anfänger das als schwierig empfinden.

Ich sitze jetzt seit geschlagenen neunzig Minuten hier und versuche das E-Mail-Programm *Thunderbird Portable* auf einen USB-Stick zu installieren, und zwar *inklusive* Verschlüsselungsprogramm und Enigmail. Es ist mir bisher nicht wirklich gelungen. Wenn ich nicht ein verdammtes benutzerfreundliches Tutorial schreiben müsste, hätte ich schon vor Wut fast aufgegeben.

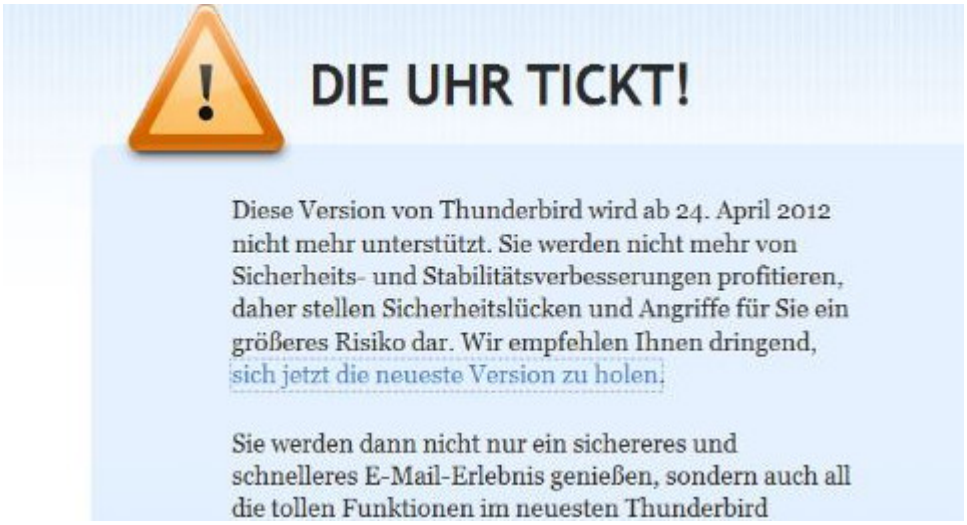
Niemand sagt einem im voraus, dass man beim „normalem“ Thunderbird Portable eben *nicht* verschlüsseln kann, auch gibt es gar keine Möglichkeit, Add-ons wie Enigmail zu installieren, außer man versucht es „per Hand“, was man niemandem empfehlen solle, schon gar keinem Anfänger. Die *Thunderbird Portable*-Version von PortableApps.com ist also Schrott. Was soll ich mit einem Programm, das nur Postkarten erlaubt?

Was lesen wir jetzt? *…laden Sie einfach GPG für Thunderbird Portable 1.4.13 (MD5: 627291d689f08577d0bb9dc2d2da1908) herunter* [Link führt zu Sourcefource]. „Einfach“ bedeutet meistens: Der Schreiber will darüber hinwegtäuschen, dass es Tücken und Fallstricke gibt.

Das war übrigens das erste und einzige Mal, dass mir jemand verkündet, dass das „normale“ *Gnu4win*, das überall empfohlen wird, eben *nicht* für *Thunderbird Portable* geeignet ist. (Hey, das kam hier schon mal vor – wieso hat mich niemand gewarnt?)

Und jetzt: *Danach laden Sie die Enigmail-Erweiterung herunter*. Hurra, alles auf Englisch! Superpraktisch für Anfänger, damit auch niemand etwas versteht. Zu allem Überfluss: „Announcements – Enigmail has a new home“ – und auf der neuen Website finde ich keine Version für *Enigmail* für die portable Thunderbird-Version.. Grmpf.

Aber wir tun ja, was man uns sagt und fummeln stundenlang herum. Was geschieht eigentlich, wenn man die oben empfohlene *Thunderbird Portable* installiert? Man sieht diese hübsche Warnung:



Das macht Mut, um weiterzumachen! April 2012 – ganz entzückend. Der Link führt dann zum „normalen“ Thunderbird und *nicht* zur portablen Version. Ich komme mir vor wie das HB-Männchen. So verarscht man Leute, die guten Willens sind, sich

um Sicherheit zu kümmern.

Das ist auch hübsch: *Laden Sie das passende XPI für die gewünsche Sprache herunter und installieren Sie es im Erweiterungsmanager (Extensionmanager). Dies wird nicht unterstützt und funktioniert oder funktioniert nicht. Volle Unterstützung für komplette Lokalisierung wird es in Zukunft geben.* Äh – wie meinen? XPI? Ist das Klingonisch? Es funktioniert oder auch nicht? Wer hätte das gedacht.

Das deutsche Thunderbird-Wiki kommt schon wieder mit etwas Anderem:
Wenn Sie Thunderbird portable verwenden, bietet sich eine spezielle Version an, die neben dem portablen Thunderbird bereits die passende Enigmail-Version vorinstalliert hat. Außerdem beinhaltet sie auch GnuPG. Sie müssen dann nur noch Ihre Schlüsseldateien hinzufügen. Mehr dazu unter: http://thunderbird.gnupt.de.

Dort lesen wir die volkstümlichen Worte:
Da diverse Erweiterungen noch nicht zu der Version 17.x kompatibel sind, wird das Upgrade bis auf Weiteres nicht automatisch durchgeführt, sondern lediglich ein Hinweis auf die Version 17.x ausgegeben. Soll das Upgrade durchgeführt werden, ist die Thunderbird-Portable.ini zu öffnen und der Parameter Thunderbirdversion auf 17x zu ändern (Thunderbirdversion=17x)

Sorry, aber ihr habt einen Knall. Hier habe selbst ich nicht mehr weitergelesen.

Hier wird alles vernünftig erklärt, leider wieder nur auf Englisch. Also ist mein deutsches Tutorial eine Marktlücke. Ich brauche noch bis Sonntag dafür.

Mining PGP Key Servers

Cryptome: „Statements in the Bradley Manning trial describe forensics to establish his online behavior and correspondents. Edward Snowden is reported to have advised his correspondents to use PGP for security. The Bradley forensics and Snowden advice suggests PGP key servers could be used to establish connections among parties, the so-called metadata official, commercial and NGO spies siphon, store and mine. The long-running MIT PGP key server is bountiful for this method but so are other PGP and GPG global servers.“

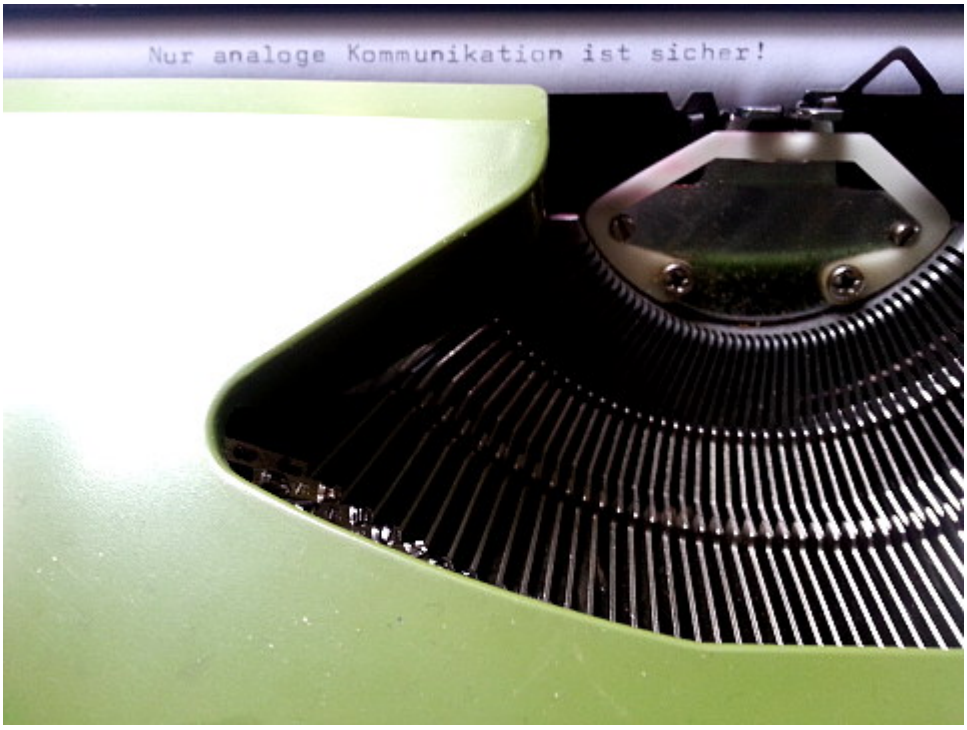
How Microsoft handed the NSA access to encrypted messages

„Die National Security Agency (NSA) habe etwa die Sorge geäußert, Web-Chats auf dem neuen Outlook.com-Portal nicht mitlesen zu können. Microsoft habe daraufhin der NSA geholfen, die konzerneigene Verschlüsselungstechnik zu umgehen. Dieses Vorgehen soll sich dem Bericht zufolge nicht auf die Web-Chats beschränkt haben: Die NSA soll auch Zugang zu E-Mails auf Outlook.com und Hotmail vor der Verschlüsselung gehabt haben.“ (The Guardian via Spiegel online)

The agency already had pre-encryption stage access to email on Outlook.com, including Hotmail.

Noch mal zum Klarstellen: „encrypted“ ist *nicht* ein *public key*-Verfahren, sondern der Schrott, den Microsoft als „verschlüsselt“ definiert, also so was wie De-Mail, das trotz unsicherer Verschlüsselung per Gesetz als „sicher“ deklariert wurde.

Sicher ist sicher [Update]



„Nur analoge Kommunikation kann halbwegs gesichert werden.“ (Stefan Plöchinger, Chefredakteur Sueddeutsche.de)

[Update] Das sagt auch der Russische Geheimdienst. Dann muss es ja stimmen.