Anhörung am EuGH über die Vorratsdatenspeicherung

Pressemeldung vom Verein Digitalcourage aka Foebud:
Die heutige Anhörung am EuGH über die Vorratsdatenspeicherung verlief in weiten Teilen desaströs für die Befürworter der umstrittenen EU-Richtlinie. Es ging um eine Klage der irischen Bürgerrechtsorganisation „Digital Rights Ireland“ und Bedenken des Österreichischen Verfassungsgerichtshofes gegen die Vorratsdatenspeicherung.

Die Richter am EuGH verlangten dabei mehrmals Zahlen zur Wirksamkeit oder andere Beweise, dass die Vorratsdatenspeicherung unbedingt notwendig sei. Spanien, Italien und England blieben als Befürworter der Richtlinie, die vor dem Gericht Stellung nahmen, diese Beweise schuldig. Das Gericht zeigte sich teilweise verägert und bezweifelte, dass die Richtlinie die Verhältnismäßigkeit immer wahre.

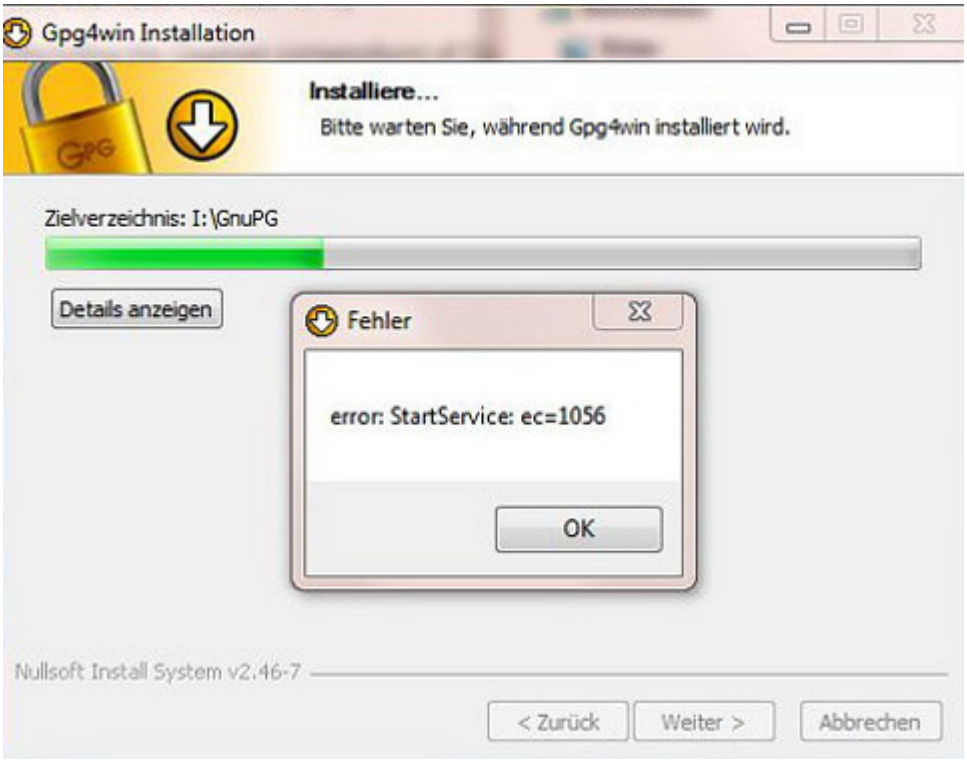
Auf der anderen Seite bemängelte der Vertreter des Europäischen Datenschutzbeauftragten, dass die Grundrechtecharta der EU einen so weitreichenden Eingriff wie die Vorratsdatenspeicherung in einer demokratischen Gesellschaft nicht rechtfertige. Den Prism-Skandal wahrscheinlich im Hinterkopf fragte das Gericht auch nach der Speicherpraxis und Outsourcing der Verbindungsdaten. Beides ist in der Richtlinie nicht verboten und weckt sicherlich auch Begehrlichkeiten von anderer Stelle.

Anmerkung: 1. Man kann auch in Pressemeldungen ~~digitalen Mut zeigen~~ Links setzen; die oben sind alle von mir hinzugefügt. 2. Der vorletzte Satz ist Deutsch des Grauens. 3. Man muss nicht bei jedem verbalen Furz gleichzeitig zu Spenden aufrufen.

Vgl. auch den Artikel bei Telepolis: „Anhörung zur

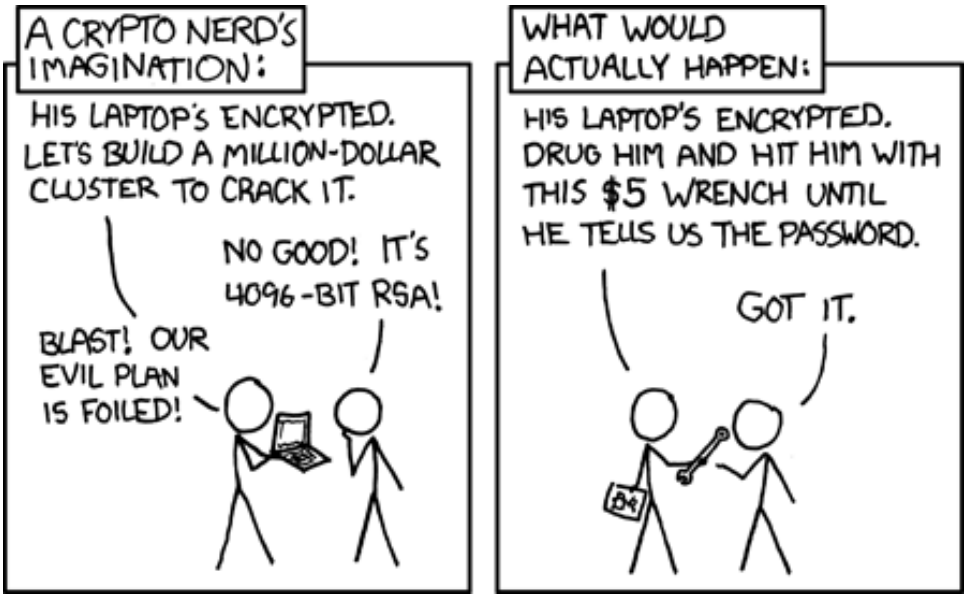
Vorratsdatenspeicherung beim EuGH: Gordischer Argumentationsknoten“.

Error: StartService: ec=1056



Weiß jemand, was diese lustige und folgenlose Fehlermeldung bedeutet? Ich schreibe gerade an einem Tutorial, wie man E-Mails verschüsselt, und habe Gpg4win-Vanilla 2.1.1 auf einen USB-Stick installiert (unter Windows7), einfach um zu sehen, was so passiert und ob *Thunderbird Portable*, das ebenfalls dort zu Übungszwecken ist, eventuell herumzickt.

Security



Verschlüsselung – nein danke!

Ein Artikel von mir in Telepolis: „Verschlüsselung – nein danke! – Trotz der bitteren Einsicht, dass die gesamte digitale Kommunikation überwacht und belauscht wird, weigert sich die übergroße Mehrheit der deutschen Journalisten, daraus irgendwelche persönliche Konsequenzen zu ziehen. Warum?“

Thunderbird-Usability-Problem für fortgeschrittene

Paranoiker

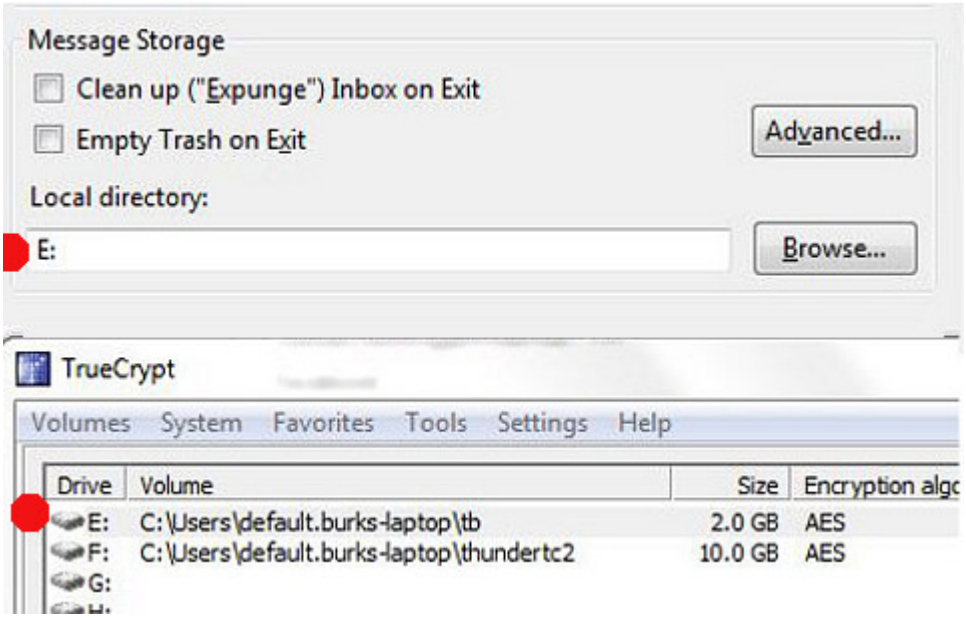
Ich kann gut nachvollziehen, warum viele Leute sich weigern oder schnell entnervt aufgeben, wenn man sie auffordert, ihr Verhalten am Rechner zu ändern. Es begegnen einem so viele Probleme der unerwarteten Art, vor denen die Macher der Software nie warnen. Wenn man aber alle möglichen Tücken der jeweiligen Software gleich in die Anleitung schreiben würde, wäre die unlesbar. Mit Computerprogrammen ist es wie mit komplizierten Haushaltsgeräten: Ich habe keine Lust ein Handbuch zu lesen, das 50 Seiten umfasst, wenn ich mir einen neuen Staubsauger oder einen Nassrasierer gekauft habe. Das Ding soll das tun, wofür ich es angeschafft habe und nicht rumzicken.

Ich habe gegenüber den meisten Menschen, denen ich etwas über Verschlüsseln und dergleichen erzähle, einen Erfahrungsvorsprung von mindestens 15 Jahren, was gleichzeitig bedeutet, dass ich schon alle Fehler gemacht habe, die sie gar nicht mehr machen können. Ich kann mich noch gut daran erinnern, dass ich in den frühen 90-er Jahren mit Windows for Workgroups 3.11 noch unter MSDOS den berühmten Norton Commander zum Absturz gebracht habe, obwohl das eigentlich gar

nicht möglich ist. Ich denke einfach anders als Programmierer: Denen ist Usabilty völlig egal.

Das gilt insbesondere für die kostenlose Software, mit der man E-Mails verschlüsselt. Eigentlich ist das kinderleicht, aber nur eigentlich. Man muss sich nur mal die Website von Gpg4win anschauen:
Gpg4win 2.1.1 contains: GnuPG 2.0.20, Kleopatra 2.1.1 (2013-05-28), GPA 0.9.4, GpgOL 1.1.3, GpgEX 0.9.7, Claws Mail 3.9.1, Kompendium (de) 3.0.0, Compendium (en), 3.0.0-beta1.

Geht's noch? Habt ihr noch alle Tassen im Schrank? Die Hälfte von dem Quatsch braucht kein Mensch. Von Usability (Benutzerfreundlichkeit) keine Spur. Stellt euch doch mal Leute vor, die den Unterschied zwischen Webmail und einem E-Mail-Programm gar nicht kennen, die verlegen zögern, wenn man sie fragt, welches Betriebssystem sie nutzen und die verständnislos mit dem Kopf schütteln, wenn sie nach einem „Texteditor, der *nicht* Word heisst" gefragt werden. Das ist leider die übergroße Mehrheit und *das* ist das Niveau, vom dem man die Leute abholen muss. Ich bin froh, dass ich mit solchen ~~DAUs~~ Menschen oft zu tun habe, die mich auf den Boden der Realität zurückholen.



Heute aber nichts für die, sondern für fortgeschrittene

Paranoiker. Wie schon erwähnt, läuft bei mir das E-Mail-Programm *Thunderbird* in einem Truecrypt-Container. Das bedeutet: Wenn jemand in meinen Rechner schaute, würde diese Person vermuten, ich besäße gar kein E-Mail-Programm oder könnte nicht beweisen, dass ich eins hätte. Ich muss diesen Container, bevor ich nach meinen Mails schaue, immer erst mit zwei Mausklicks und der Eingabe eines langen Passworts öffnen. (Wie unbequem! Das dauert ja zwei Sekunden länger als ich es gewohnt bin! Igitt! Das tu ich mir nicht an!) Ich habe also das E-Mail-Programm auf meinen Windows-Rechnern nicht dort installiert, wo es von ~~dem höheren Wesen Kleinweich~~ Bill Gates vorgesehen ist, sondern die „fortgeschritten"-Option („advanced") gewählt, um das selbst entscheiden zu können – in diesem Fall eben in einen durch Truecrpyt vorher angelegten Container (der, wenn er geöffnet worden ist, vom Dateimanager von Windows mit einem ganz normalen Laufwerksbuchstaben angezeigt wird. Unter Linux ist das viel praktischer, aber das ist heute nicht dran).

Seit einigen Tagen weigerte sich Thunderbird auf meinem Laptop, einen meiner E-Mail-Accounts zu öffnen, ausgerechnet den von burks@burks.de. Auf allen anderen Rechnern, sogar auf meinem Smartphone, rauschten meine E-Mails nur so herein, aber dem Laptop bliebt alles wüst und leer. Nun bin ich kein Laie, sondern versuche immer selbst herauszufinden, was falsch läuft.

Diagnose: Mein Programm versuchte sich mit dem SMTP-Server meines Providers zu verbinden. So weit, so gut. Aber dann hörte es irgendwann nach ein paar Minuten auf, als sei es frustriert, und nix passierte. („Account Settings" | „Server Settings" | „Server name": IMAP- und SMTP-Server noch richtig? Ja. „Connection Security": SSL/TLS oder STARTTLS? Hab ich vergessen, muss ich nachschauen – Mist, schon wieder eine Minute mehr gebraucht – verdammt, wo steht das noch gleich?) Half aber alles nichts.

Irgendwann habe ich die harte Tour gewählt und einfach das

gesamte Thunderbird-Verzeichnis von meinem Hauptrecher auf meinen Laptop gebeamt, also das offenbar Kaputte mit dem überschrieben, was funktionierte. Dummerweise änderte das gar nichts. Ich konnte meine Mails immer noch nicht aufrufen. („Warum hast du denn alles auf Englisch?“ – „Damit ich besser englische Handbücher lesen kann.“) Dann habe ich mir erst einmal Kaffee gemacht, um von der Palme, auf der ich schon saß, herunterzukommen.

Zum Glück hatte ich irgendwann eine Eingebung: Wenn man Thunderbird zwingt, sich woanders zu installieren als es vorgeschlagen wird, muss man nicht nur per Hand den Ort („Pfad“) eingeben, wo das geschehen soll, sondern auch noch in den Einstellungen bei „Message Storage“ (keine Ahnung, wie das auf Deutsch genau heißt) definieren, wo die Nachrichten gespeichert werden. Das hatte ich bei der Installation auch brav gemacht, aber vergessen, dass Truecrypt einem die Wahl lässt, unter welchem „Laufwerkbuchstaben“ man den Container jeweils öffnet. Und wenn der nicht mit dem übereinstimmt, der bei der Installation eingegeben worden war, dann reagiert Thunderbird wie eine beleidigte Leberwurst, macht gar nichts und spuckt noch nicht einmal eine Fehlermeldung aus – ein Benehmen, dass ich auch von Frauen kenne.

Mail Isolation Control and Tracking

Vorratsdatenspeicherung auch bei Snail Mail: Laut der New York Times (via Heise) wird der gesamte Briefverkehr in den USA registriert. „Absender und Empfänger jeder über den staatlichen Postdienst USPS verschickten Sendung werden von Computern abfotografiert“.

Bruce Schneier, a computer security expert and an author, said whether it was a postal worker taking down information or a computer taking images, the program was still an invasion of privacy.

So etwas könnte hierzulande bestimmt *nie* passieren.

Eavesdropping a fax machine

Markus Kuhn auf Light Blue Touchpaper über „US eavesdropping technique ‚DROPMIRE implanted on the Cryptofax at the EU embassy [Washington] D.C.'."

Verschlüsselung verbieten!

Lutz Donnerhacke (1997): „Die Bundesregierung will in aller Eile strikte gesetzliche Regelungen für den Gebrauch sogenannter Verschlüsselungstechnik beschließen."

Ebd.: „Rede von Bundesinnenminister Manfred Kanther anläßlich der Eröffnung des 5. IT-Sicherheitskongresses am 28. April 1997 in Bonn „Mit Sicherheit in die Informationsgesellschaft": *Die legalen Überwachungsmöglichkeiten müssen auch dann gewahrt bleiben, wenn der Fernsprechverkehr künftig mehr und mehr verschlüsselt wird. Die Frage, ob deswegen der Einsatz von Verschlüsselungsverfahren gesetzlich zu regeln ist, wird derzeit leidenschaftlich diskutiert. Wenn in einigen Jahren nicht nur der gesamte Datenverkehr über das Internet und andere Netze verschlüsselt wird, sondern vielleicht sogar das*

ganz normale klassische Telefongespräch, dann hat das ohne eine wirksame Regulierung zur Folge, daß die Befugnisse der Strafverfolgungs- und Sicherheitsbehörden nach dem G 10-Gesetz, der Strafprozeßordnung oder dem Außenwirtschaftsgesetz zum Mithören des Telefon- und Datenverkehrs praktisch ins Leere laufen werden.

Oder auch Lawww.de (1997):

Süddeutsche Zeitung v. 5.3.1996; Der Spiegel 13/1996, 132, 142; Antwort des Parl. Staatssekretärs beim Bundesinnenministerium Eduard Lintner auf die Zusatzfrage des MdB Jörg Taus in der Fragestunde des Bundestages v. 19.4.1996: „… Sie wissen wie ich, daß es ein legitimes Interesse gibt, die eigenen Daten zu schützen, daß aber auch Vorkehrungen getroffen werden müssen, um beispielsweise zu verhindern, daß Kriminelle diese Verschlüsselungsmöglichkeiten offensiv gegen die Gesellschaft und gegen den Bürger nutzen"; BT-Drs. 13/4403, Frage 22

Antwort der Bundesregierung auf eine Kleine Anfrage der Fraktion Bündnis 90 / Die Grünen (BT-Drs. 13/1889)(…). Nach einer Meldung in Der Spiegel 52/1996, 16 plant die Bundesregierung nun ein solches Gesetz in „aller Eile" beschließen zu lassen.

Im Beschluß des Ministerkomitees an die Regierungen vom 11.9.1995 (Recommendation No. R [95] 13) heißt es dazu: „Use of Encryption: Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary"; (…) Nach einem Bericht der c't soll die Empfehlung bei der EG-Kommission auf „Überraschung" gestoßen sein: c't 11/1995, 32.

ZDNet: „US-Politiker fordern Verbot von Verschlüsselungstechnik" (2001).

BBC (2011): „The legal challenge has been brought by The

French Association of Internet Community Services (ASIC) and relates to government plans to keep web users‘ personal data for a year.“

Piraten Neu-Ulm: „Freund liest mit – Verbot von Verschlüsselungssoftware wird vorbereitet“ (2013).

Erklärvideo: Mails verschlüsseln leicht gemacht

Erklärvideo: Mails verschlüsseln leicht gemacht von Boris Kartheuser. Ich werde, so bald ich die Zeit dazu finde, auch so etwas machen, weil ich diese Anleitung noch zu wenig volkstümlich finde. Einige – irrelevante – Kleinigkeiten sind auch schlicht falsch.

Passwörter

Heise: „Neuregelung zur Datenweitergabe an Ermittler tritt in Kraft“.

Die Gesetzesänderung betrifft sogenannte Bestandsdaten. Das sind feste Daten zu einem Telefon- oder Internetanschluss (wie der Name und die Adresse des Anschlussinhabers), aber auch persönliche Kennzahlen (PINs) und Passwörter.

Alles klar soweit? Die Passwörter für den Zugang zu Eurem E-Mail Konto sind unter anderem gemeint. Auch bei Ordnungswidrigkeiten.

Verschlüsseln JETZT!

Aha. Man muss die Leute anbrüllen, dann bewegt sich was. Feynsinn kann jetzt auch verschlüsseln und liefert gleich noch Links zu zwei benutzerfreundlichen Anleitungen, wie das geht, von Todamax und Verbraucher sicher online.

Update:
Demnach erhält PRISM sofort eine Nachricht, wenn sich ein überwachter User zum Beispiel in einen der ausspionierten Dienste einloggt, einen Chat startet, eine E-Mail versendet oder sich abmeldet. (Heise)

Publikumsbeschimpfung

The Dissenter (via Fefe) lässt Gleen Greenwald ausführlich zu Wort kommen:
Another document that I probably shouldn't share since it's not published but I am going to share it with you anyway—and this one's coming soon but you're getting a little preview—It talks about how a brand new technology enables the National Security Agency to redirect into its repositories one billion cell phone calls every single day, one billion cell phone calls every single day.

What we are really talking about here is a globalized system that prevents any form of electronic communication from taking place without its being stored and monitored by the National Security Agency.

Jetzt vergleichen wir die Krokodilstränen unserer politischen Kaste, von den US-Amerikanern ausgespäht zu werden, mit dem, was sie seit 2006 zum Thema „Online-Durchsuchung" von sich gegeben haben. Was für eine heuchlerische, verlogene Bande! Das gilt auch für viele Journalisten. Mein hanebüchenstes Lieblingszitat (weil es Unfug ist) von Annette Ramelsberger (Süddeutsche, 07.12.2006):
Den meisten Computernutzern ist es nicht klar: Aber wenn sie im Internet surfen, können Verfassungsschützer oder Polizei

online bei ihnen zu Hause auf die Festplatte zugreifen und nachschauen, ob sie strafbare Inhalte dort lagern – zum Beispiel Kinderpornographie oder auch Anleitungen zum Bombenbau.

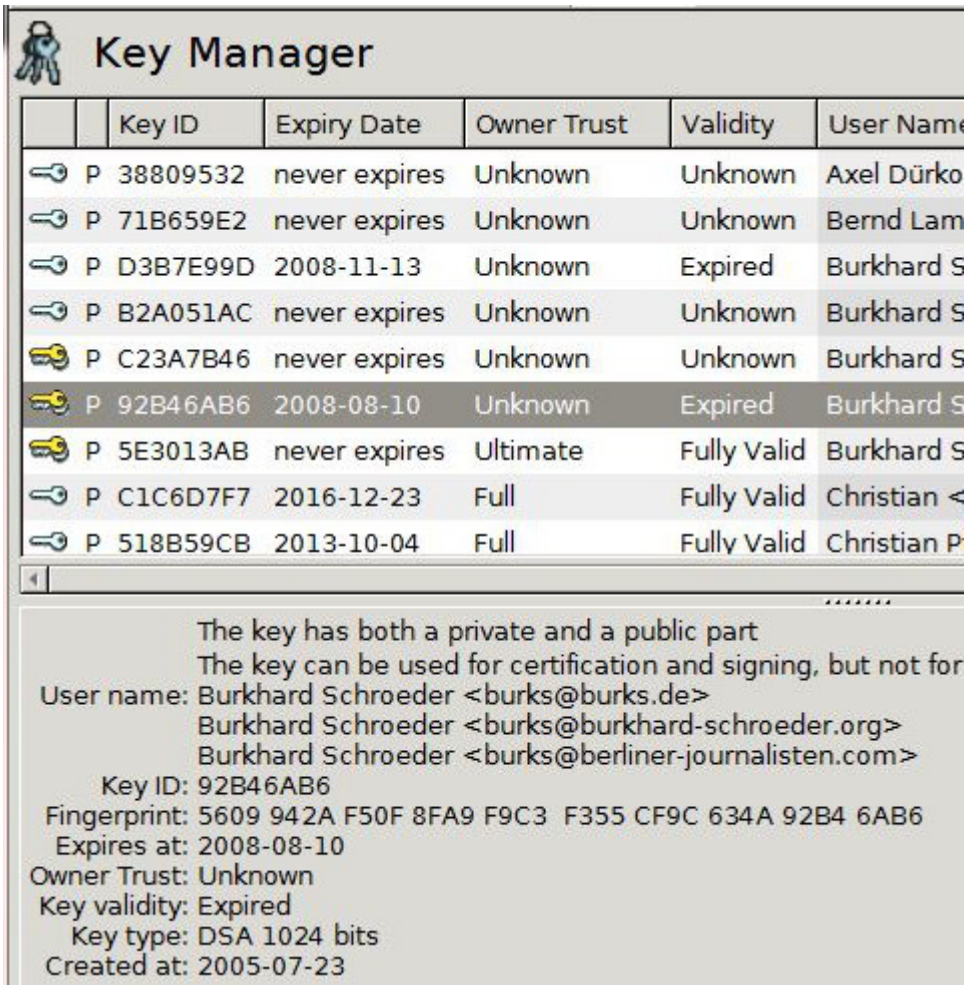
Wenn die NSA und der englische Geheimdienst die elektronische Kommunikation in Deutschland komplett belauschen, welche Konsequenzen ziehen wir daraus? Keine? Wie viele Journalisten in Deutschland verschlüsseln ihre E-Mails? Mehr als hundert? Weniger? Was muss noch passieren, dass die sich vernünftig verhalten? Ich habe bei zahlreichen Redaktionen angefragt, was die zum Thema zu tun gedenken, von den meisten bekam ich gar keine Antwort.

Und wenn hier einer der wohlwollenden Leserinnen und geneigten Leser meint, mir in Zukunft eine unverschlüsselte E-Mail zu schicken – VERGESST ES! Bringt Euch das gefälligst SOFORT bei und verhaltet Euch wie rational denkende Menschen, sonst beschimpfe ich Euch als Pappnasen oder belege Euch mit noch schlimmeren Ausdrücken oder schicke Euch zum Psychologen oder Völkerkundler, um mir erklären zu lassen, warum erwachsene Menschen sich dermaßen bescheuert verhalten.

Ich werde jeden, der mir in Zukunft eine unverschlüsselte E-Mail schickt, als Wähler Angela Merkels oder Bosbach-Groupie abheften. Irgendwo müssen die doch sein. In meinem so genannten sozialen Umfeld gibt es niemanden, der CDU oder FDP wählt. Irgendwo müssen diese Ignoranten ja frei herumlaufen.

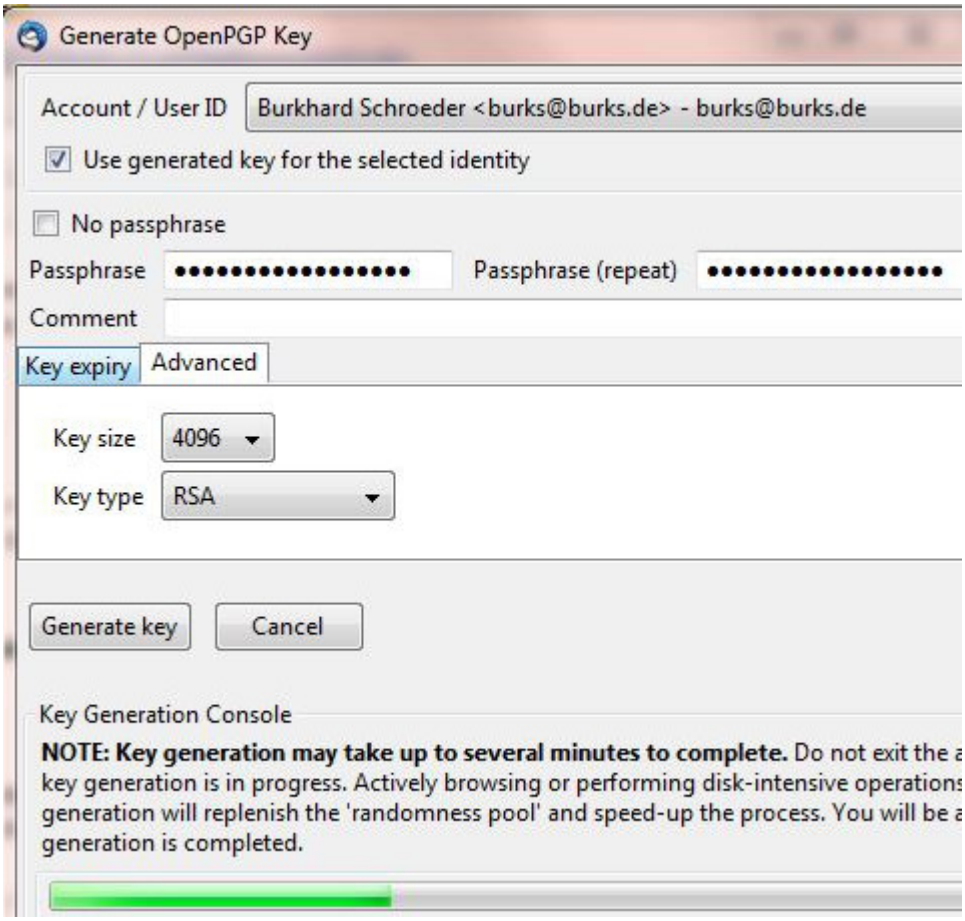
Update: Aufruf zur Datenspende!

Neuer Schlüssel



Ich habe mit Schrecken gesehen, dass mein Schlüssel schon fast fünf Jahre alt war, ein anderer sogar noch älter (vgl. oben). Zeit, um ihn zu erneuern. Bitte benutzt, um mir eine verschlüsselte E-mail zu schreiben, in Zukunft nur noch diesen:

burks@burks.de(0xC23A7B46)pub.asc – | ID 0x2E47F7D2 | Fingerprint: 6EAA 48C5 C7FB FBCB DA5F 0391 37D5 33B1 2E47 F7D2



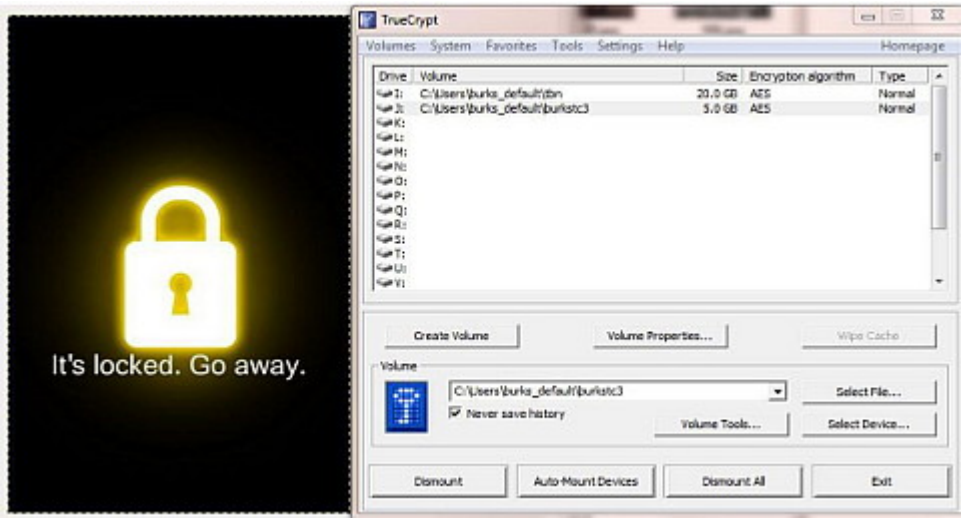
Ich musste mich unter Windows wieder ärgern. Nur Enigmail für Thunderbird bietet die Option („advanced“) an, 4096-Bit-Schlüssel zu erzeugen. Kleopatra und der GNU-Privacy-Assistent von GPA btw. Gpg4Win fragen nicht nach oder generieren automatisch schwächere Schlüssel. Wieder ein Argument, dass Programmierer manchmal abschrecken oder verwirren wollen anstatt den Nutzern zu erleichtern, Programme zu benutzen.

Slashdot: „The catch is that the private key needs to be fairly large to be secure: a 4,096-bit RSA key should suffice for some years.“

Internet Censorship and Control

Hal Roberts | Internet Censorship and Control (via Light Blue Touchpaper, University of Cambridge): „In the following collection, published as an open access collection here and as well in a special issue of IEEE Internet Computing, we present five peer reviewed papers on the topic of Internet censorship and control. The topics of the papers include a broad look at information controls, censorship of microblogs in China, new modes of online censorship, the balance of power in Internet governance, and control in the certificate authority model.“

Sichere Daten



Das Modul 8: „Sichere Daten“ (pdf) meiner Seminarreihe „Sicher Surfen im Internet“ steht jetzt – leicht gekürzt – öffentlich zur Verfügung.

How can we invest our trust in a government that spies on us?

„How can we invest our trust in a government that spies on us?“, fragt George Monbiot vom Guardian. Die Antwort, warum die Deutschen ihre Regierung lieben, findet man hier.

Sollen die Idioten doch in ihr Unglück rennen

Aus einem Posting im Heise-Forum:
„Das Ausmaß und die Tatsache der Schnüffelei ist schon recht heftig – was mich aber an der ganzen Sache am meisten ankotzt, ist die Tatsache, wievielen Menschen das absolut egal ist oder sogar von ihnen befürwortet wird. Man hat ja nichts zu verbergen und so.

Das nervte mich schon immer, aber ich dachte: hey, wenn irgendwann rauskommt wie sehr wir überwacht werden, wachen die Leute auf. Falsch gedacht. Viele befürworten ja die Überwachung und freuen sich, daß dadurch total viele Terroranschläge auf ihre Nachbarschaft verhindert werden. Ja ne ist klar.

Ich habe keine Lust mehr. (…) Ich habe keinen Bock mehr den Leuten zu erklären, daß Zensur und Überwachung niemals gut

ist. Sollen doch die Millionen Facebook-Idioten und Stasi-Befürworter in ihr Unglück rennen.“

Not Trusting Google is Good Idea

Herbert Snorrason (anarchism.is) (via Fefe):

I. Information to be disclosed by Google, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., Google, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, deleted e-mails, emails preserved pursuant to a request made under 18 U.S.C. § 2703(f), the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

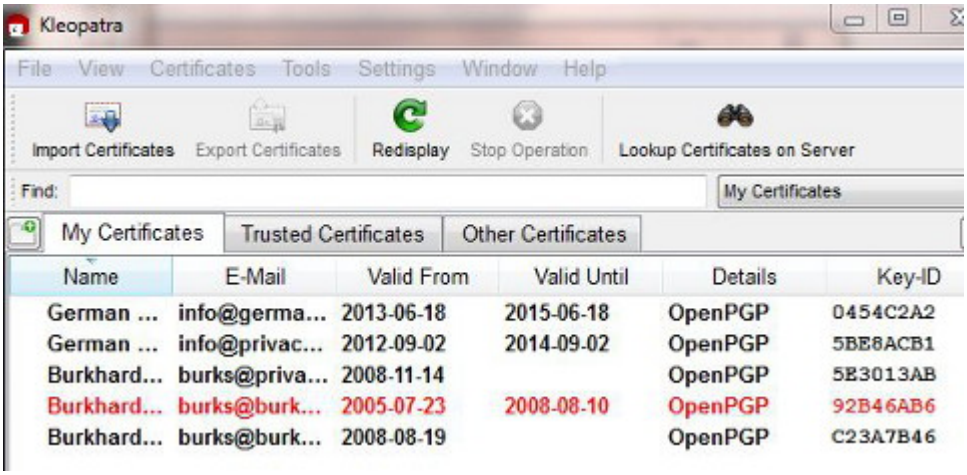
All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and

source of payment (including any credit or bank account number);

All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files, and including any deleted information and any information preserved pursuant to a request made under 18 U.S.C. § 2703(f);

Noch Fragen? Will mir noch jemand eine unverschlüsselte E-Mail per GMail senden? Echt?

Kleopatra sei Dank!



Hurra, nach stundenlangem Dröseln und Rätseln habe ich mein APG-Problem gelöst und kann jetzt auch E-Mails auf meinem Android-Smartphone verschlüsseln. Es gab zwei Probleme:

Erstens: Wie einige kundige Leser schon vermuteten, ist das Format, das Enigmail (das OpenPGP-Add-on für Thunderbird) zum Export der Schlüssel benutzt, offenbar nicht kompatibel mit der Dateiverwaltung von Android, obwohl der Schlüssel korrekt im ASCII-Format erscheint. Da muss man erst mal drauf kommen.

Also genau das, was hier ~~in Klingonisch~~ erwähnt wird:
APG cannot import keys in .asc files terminated with CR/LF (PC-style): it requires LF only (UNIX style). If your PC editor offers you a choice (e.g., TextPad does) save the file as UNIX text.

Ich habe es also mit Kleopatra versucht und damit die öffentlichen und meine geheimen Schlüssel exportiert und auf das Smartphone gebeamt.

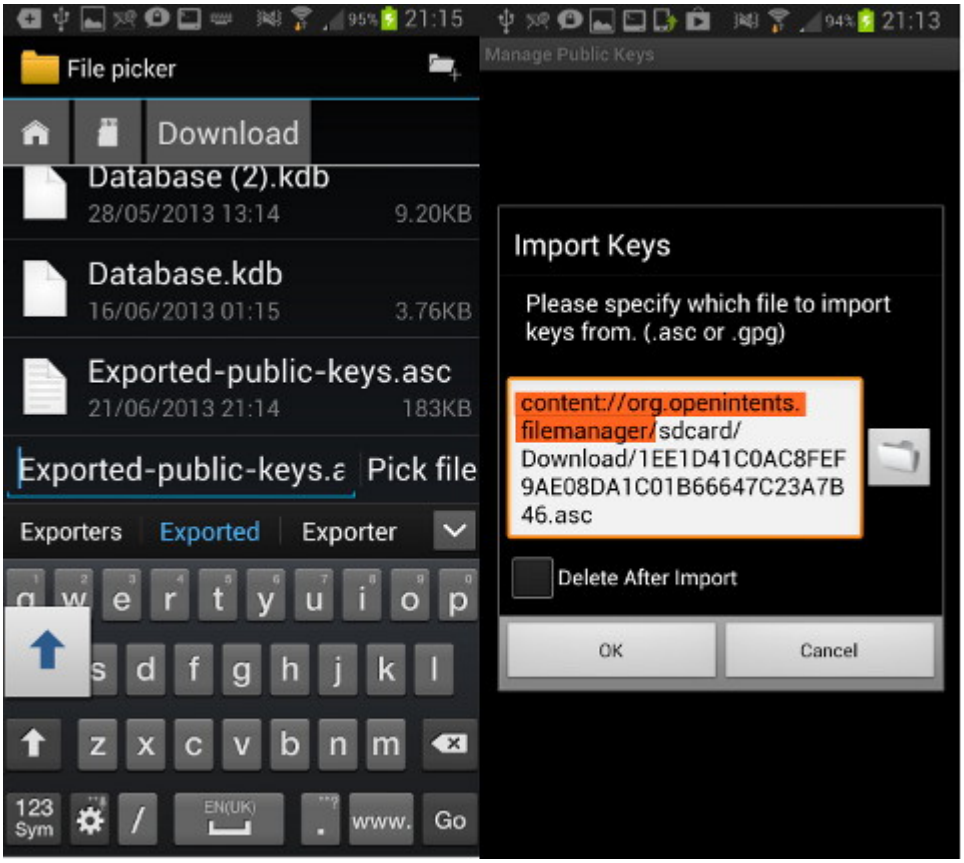
Nun zu uns, Programmierer! Wir sind ja alle dankbar, dass ihr uns das Schöne, Gute und Wahre Open Source und gratis usw. zusammendröselt und zum Downlad anbietet. Ihr habt aber trotzdem einen Knall: Welche Pappnase denkt sich für jeden Softwareschnipsel einen anderen Namen aus? Kleopatra, „ist der bevorzugte Zertifikatsmanager in Gpg4win“. Geht’s noch? Sind wir hier im Gallischen Krieg oder beim großen Latinum? Und das nur, weil ihr Leute abschrecken wollt, das auch zu nutzen?

Was kriegt der Laie in den ersten fünf Minuten alles zu sehen: PGP, OpenPGP, GnuPG, Gpg4Win, GPG, OpenPGP & S/MIME, Algorithmenstärken, öffentliche und private Schlüssel, und jetzt auch noch Kleopatra – glaubt ihr denn, auch nur ein wohlwollender Nutzer und eine geneigte Nutzerin hat da noch Lust, überhaupt anzufangen? Und welche Knalltüte nennt die Schlüssel bei Kleopatra „Zertifikate“? Sogar ich musste erst überlegen und probieren, und ich verschlüssele meine E-Mails seit 1995.

Ich glaube, ich sollte mich mal selbst hinsetzen, der breiten Masse aufs Maul schauen und die Angelegenheit volkstümlich formulieren. So wird das nix.

Wie sagte Paulus über das erfolgreiche Missionieren ganz richtig: „Den Juden bin ich geworden wie ein Jude, auf daß ich die Juden gewinne. Denen, die unter dem Gesetz sind, bin ich geworden wie unter dem Gesetz, auf daß ich die, so unter dem Gesetz sind, gewinne. Denen, die ohne Gesetz sind, bin ich wie

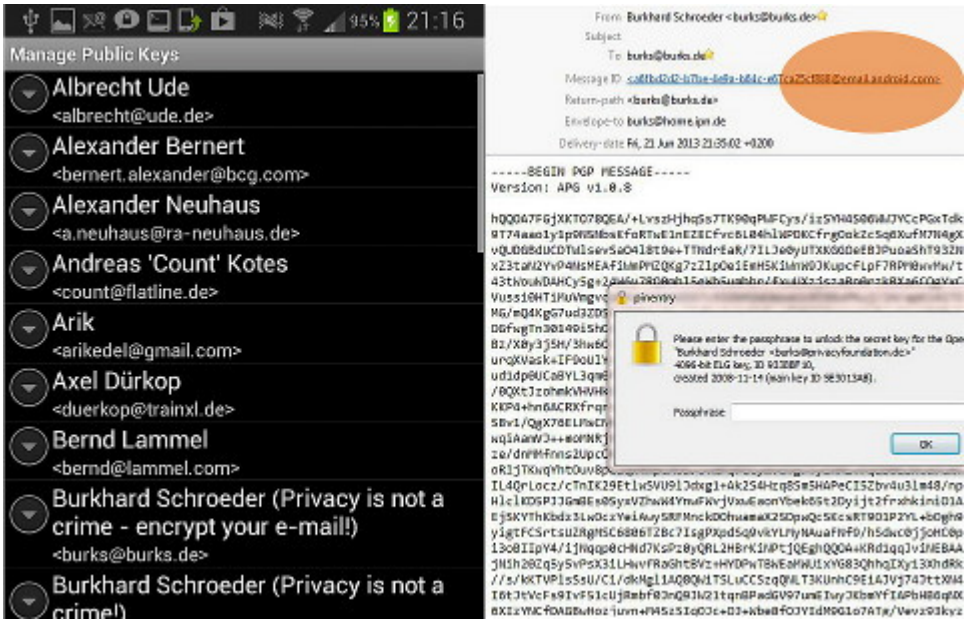
ohne Gesetz geworden , auf daß ich die, so ohne Gesetz sind, gewinne. Den Schwachen bin ich geworden wie ein Schwacher, auf daß ich die Schwachen gewinne. Ich bin jedermann allerlei geworden, auf daß ich allenthalben ja etliche selig mache. Den DAUS bin ich geworden ein Dau, auf daß sie ihre E-Mails verschlüsseln lernen und ich sie selig mache.“



Zweitens: Auch der Dateimanager (ich nutze den OI File Manager) zickt herum.

Auf der linken Seite des oberen Screenshots sind die verschiedenen Dateien im Download-Verzeichnis zur Auswahl zu sehen. Wenn man eine ausgesucht hat und auf „pick file“ drückt, erscheint eben dieselbe, was auf der rechten Seite deutlich wird – hier will ich eine .asc-Datei (so hat Kleopatra meinen öffentlichen Schlüssel genannt) importieren. Niemand sagte mir aber, dass man per Hand (!) zunächst den vorderen Teil des Pfades (alles, was rot markiert ist), eliminieren muss, ansonsten kommt wieder die Meldung „file not found“.

Ich hatte nur so eine vage Ahnung, nachdem ich praktisch alle Forenbeiträge zum Thema der letzten drei Jahre gelesen habe. Das sind gar nicht so viele, und alle natürlich in Englisch. Ich habe einfach herumprobiert. Das kann man niemandem, der das lernen will, zumuten.



Der Verschlüsseln ist auch nicht einfach, und APG stürzt manchmal ab, warum, werde ich herausfinden. Aber immerhin habe ich alle öffentlichen Schlüssel importiert und es geschafft, mir selbst eine verschlüsselte E-Mail zu schicken, die ich mit einem meiner Rechner dann lesen konnte (MessageID email.android.com, oben rechts rot markiert)

Die nächste Aufgabe ist herauszufinden, wo APG die Schlüssel speichert. Ich habe mir für den Fall der Fälle, dass ich sie verstecken will, EDS installiert.

Netzpolitik.org im #Neuland

Netzpolitik.org: „Dan Goodin betont diesen Punkt auf Ars Technica nochmal: Wer Anonymisierung wie Tor verwendet, wird

gespeichert, egal ob US-Bürger oder nicht, weil man damit nicht nachweist, wo man ist. Und wer seine Kommunikation verschlüsselt wie mit OTR oder OpenPGP, dessen Kommunikation ist verdächtig und wird so lange gespeichert, bis die NSA sie entschlüsseln kann."

Ach ja? Die NSA kann OpenPGP entschlüsseln? Was für ein gequirlter Quatsch ist das denn? Und wie will man speichern, wer Tor benutzt? Selten so eine dämliche Verschwörungstheorie gelesen.

Der Autor Andre Meister „begleitet diverse netzpolitische Zusammenhänge". Dann kann ja nichts mehr schief gehen. Wieder jemand, der mich von nun an ignorieren wird. In der Attitude der beleidigten Leberwurst braucht man keine Argumente mehr. Das kenn ich aus dem DJV.

[Update] An den Kommentaren bei netzpolitik.org kann man das Niveau der „Argumentation" wunderbar verfolgen. Ich habe übrigens *nie* behauptet, dass es keinen „Staatstrojaner" gebe, sondern dass der so, wie die Medien sich das vorstellten, nicht funktioniert, nur, wenn das „Opfer" denkbar bescheuert ist. Und „Abfallprodukte" von Skype sind ja wohl etwas anderes. Aber ich füttere auch keine Trolle.