Werner Koch (GnuPG) im Interview

Eine Abschrift des Interviews zwischen Ingo Ebel (RadioTux[1,2]) und Werner Koch[3] (Hauptentwickler von GnuPG[4,5]), welches auf dem Frühjahrsfachgespräch der German Unix User Group[6,7] aufgenommen und in RadioTux Sendung März 2015[8] veröffentlicht wurde. Ich habe div. „äh's" und „ja's" entfernt, sowie sprachliche Holperer korrigiert, ohne allerdings den Inhalt zu verändern. Daher ist dies immer noch ein Sprachtext.

IE: Ich bin jetzt auf dem Frühjahrsfachgespräch der GUUG in Stuttgart. Bei mir ist Werner Koch. Er ist Hauptentwickler von GnuPG und … ja, hallo erst mal.

WK: Hallo.

IE: Ihr hattet in der letzten Zeit ja so ein bisschen Finanzprobleme und nun habt ihr … Ja, es stellte sich die Frage, wie geht es mit dem Projekt überhaupt weiter. Ihr habt Spenden eingesammelt und wie sieht's da jetzt aus?

WK: Zur Zeit sieht's einfach super aus. Das war ein richtiger Erfolg. Der kam auch sehr unerwartet. Seit Jahren kommen keine Aufträge mehr herein und Wartungsverträge sind auch alle gecancelt worden inzwischen. Seit vier Jahren habe ich kaum noch Einnahmen aus den Bereichen Mithilfe für GnuPG und Support und musste zeitweise auch andere Sachen machen. Wir hatten vorletztes Jahr bei GOTEO[9] eine Croudfunding-Kampagne gemacht, da sind letztendlich netto 18.000 bei rum gekommen. Das war auch sehr hilfreich, da konnte ich ein bisschen weiter arbeiten. Kurz bevor Snowden[10] hatte ich wirklich ernsthaft überlegt aufzuhören mit der ganzen Sache und mir irgendeinen bezahlten Codeknecht-Job zu suchen. Ja, wegen Snowden habe ich das sein gelassen … und es gibt auch immer mehr Anfragen dazu, aber wirklich viel kam damals nicht rum. Ja, GOTEO hat mir erst mal etwas geholfen, weiter zu machen. Kurz vor Weihnachten letztes Jahr haben Freunde mich angesprochen ich solle jetzt unbedingt irgendeine Spendenkampagne machen. Dann hat die FSFE[11,12] dazu eine Presseerklärung gemacht, zusammen mit der Wau Holland-Stiftung[13,14]. … Ja, ich hab' da so einen Spendenbalken programmiert … Durch den Congress in Hamburg[15,16] sind auch 37.000 brutto eingegangen bis Ende Januar. Und dann kam ein Artikel in ProPublica[17], das ist

1 http://de.wikipedia.org/wiki/RadioTux
2 http://www.radiotux.de/
3 http://de.wikipedia.org/wiki/Werner_Koch_(Softwareentwickler)
4 http://de.wikipedia.org/wiki/GNU_Privacy_Guard
5 http://www.gnupg.org/
6 http://de.wikipedia.org/wiki/German_Unix_User_Group
7 http://www.guug.de/
8 http://www.radiotux.de/index.php?/archives/7995-RadioTux-Sendung-Maerz-2015.html
9 http://goteo.org/
10 http://de.wikipedia.org/wiki/Edward_Snowden
11 http://de.wikipedia.org/wiki/Free_Software_Foundation_Europe
12 http://fsfe.org/
13 http://de.wikipedia.org/wiki/Wau_Holland_Stiftung
14 http://www.wauland.de
15 http://de.wikipedia.org/wiki/Chaos_Communication_Congress
16 http://events.ccc.de/congress
17 http://www.propublica.org/article/the-worlds-encryption-software-relies-on-one-guy-who-is-

eine amerikanische Community-Zeitschrift, die von einer Stiftung bezahlt wird, die investigativen Journalismus machen. Das ist ganz interessant. Mit einer Journalistin davon hatte ich mich getroffen auf dem Congress und sie hat dann eine Story geschrieben … wahrscheinlich kennt ihr die schon. Am Abend, dem 5. Februar schaue ich dann noch mal in meinen Mailfolder rein, und sehe auf einmal 1000 Mails von meinem Donation-Account[18]. Ich denke „Da ist irgendwas schief gelaufen.“, bis ich das dann fest gestellt hatte. Da sind innerhalb von zwei Tagen 150.000€ umgerechnet rein gekommen. Am gleichen Abend hat mich noch ein Gründer von Stripe[19,20] angerufen und gefragt ob ich noch Spenden haben wolle von ihm und Facebook[21,22] … die das jährlichen machen wollen, jeder 50.000$. Ja, das ist super. Die Linux Foundation[23,24] hatte mir kurz vorher gesagt, dass sie mich dieses Jahr auch fördern würden mit 60.000$ einmalig. Zu der Zeit konnte ich das noch nicht veröffentlichen, da … sie mussten dass noch klären wegen der Pressemitteilung und so was. Dieser Artikel kam da ein wenig dazwischen. Ja, jetzt haben wir eigentlich genug Geld. Ich weiß eigentlich gar nicht, wie wir mit dem Geld umgehen. Ich muss mir jetzt erst mal einen Steuerberater suchen, der … wir überlegen, wie wir am günstigsten mit dem Geld umgehen, damit es lange reicht … Konkret habe ich Neal Walfield[25] inzwischen eingestellt. Neal kennen manche vielleicht von der Hurd-Entwick-lung[26,27] und von Debian[28,29]. Er hat eigene Betriebssysteme geschrieben und ist eigentlich ein sehr guter Coder und wohnt zufälligerweise auch in Düsseldorf … (lacht) … ich treffe ihn auch regelmäßig und er suchte, weil er mit seiner Doktorarbeit gerade fertig ist, einen Job. Und bevor er jetzt irgendwo bezahlt zu irgend einer Firma geht und so, dachte ich, er kann auch hier etwas machen. Und er macht halt gerne freie Software[30] und jetzt ist er eingestellt und beginnt sich einzuarbeiten. Und das ist natürlich sehr praktisch, dass ich mal wieder Sachen abgeben kann und nicht alles selber machen muss. Es gibt da noch weitere Pläne, was wir da genau machen müssen, können und wen wir da noch fördern. Genaueres kann ich noch nicht sagen. Aus steuerlichen Gründen müssen wir erst gucken, wie das aussieht, damit man da einen genauen Plan machen kann. Ich freue mich sehr über die ganzen Spenden und diese Aufmerksamkeit, die das ganze erreicht hat. Die ganzen Glückwünsche und „weiter so“, tausende davon. Da macht man doch gerne weiter. Macht auch wieder richtig Spaß!

---

going-broke

18 http://www.gnupg.org/donate
19 http://en.wikipedia.org/wiki/Stripe_(company)
20 http://stripe.com/
21 http://de.wikipedia.org/wiki/Facebook
22 http://www.facebook.com/
23 http://de.wikipedia.org/wiki/Linux_Foundation
24 http://www.linuxfoundation.org/
25 http://walfield.org/
26 http://de.wikipedia.org/wiki/GNU_Hurd
27 http://www.gnu.org/software/hurd
28 http://de.wikipedia.org/wiki/Debian
29 http://www.debian.org/
30 http://de.wikipedia.org/wiki/Freie_Software

IE: Ist doch schön, dass das so funktioniert hat. D.h. du hast eine Firma, die sich vornehmlich mit der Entwicklung GnuPG beschäftigt und dem Support rings rum. Und jetzt ist erst mal für die nächsten paar Jahre so gesichert, dass ihr weiter machen könnt?

WK: Vorläufig, so wie es aussieht, können wir weiter machen zu zweit. Jetzt ist auch der Druck weg, neue Aufträge zu besorgen oder irgendwie an Geld zu kommen oder woanders zu arbeiten. Deswegen ist auch genügend Zeit da, sich um Sachen zu kümmern. Das erste was wir gemacht haben … das hatten wir schon Anfang Januar geplant, das wir ein Treffen machen werden in Frankfurt mit einigen Entwicklern, die Frontends[31] schreiben … und Mailer. Da wollen wir erst mal sehen, wie das so geht. Und das hat so ein Rieseninteresse erweckt, dieser GnuPG summit[32], dass wie jetzt eigentlich alle ablehnen müssten. Wir könnten eine kleine Konferenz machen … wird irgendwann diesen Herbst vielleicht doch noch passieren. Ja, ich denke, dass wenn wir dann zusammen kommen und uns treffen viele Konflikte dann gelöst werden können, oder … ja, man kennt das: jeder arbeitet so vor sich hin. Es war nie so richtig gut koordiniert in den letzten Jahren.

IE: Es ist, glaube ich, immer ganz wichtig, dass die Community sich mal trifft und man … sei es auch nur mal ein oder zwei Tage zusammen hackt und so ein bisschen weiter kommt.

WK: Ja, genau!

IE: Jetzt hast du hier auf der Konferenz auch die Neuerungen von GnuPG v2.1[33] vorgestellt. Also die Entwicklung geht voran. Und teilweise lagen die Features schon auf Halde. Was gibt es denn jetzt neues in GnuPG v2.1?

WK: GnuPG v2.1 – eigentlich ist das nur ein kleiner Versionsnummernsprung. Es ist eigentlich nicht viel neues drin, wenn man das mal vergleicht mit dem, was GnuPG v2.0 eigentlich machen sollte. Letztendlich ist das drin, was ich vor 10 Jahren schon alles machen wollte in v2.0. Aber da war keine Zeit für da. Es gab halt die Aufträge, die gingen in eine etwas andere Richtung. So, die Neuerungen – was wir haben: Wir haben diesen secring.gpg nicht mehr. Das hat intern erleichtert, dass viele Sachen … jede Menge Code konnte aus GnuPG raus geschmissen werden dadurch. Das ganze funktioniert jetzt genau so wie der kleine Bruder von GPG, GPGSM[34] für S/MIME[35] … das die Schlüssel durch den GPG-Agent[36] verwaltet werden. Das ist praktisch so was wie SmartCard[37], der GPG-Agent. Das bietet halt eine ganze Menge von interessanten Möglichkeiten. Ist auch eine bessere Modularisierung. Ich habe gestern einen Newscase

31 http://de.wikipedia.org/wiki/Front-End_und_Back-End
32 http://wiki.gnupg.org/GnuPGSummit
33 http://www.gnupg.org/faq/whats-new-in-2.1.html
34 http://www.gnupg.org/documentation/manuals/gnupg/Invoking-GPGSM.html
35 http://de.wikipedia.org/wiki/S/MIME
36 http://wiki.ubuntuusers.de/GPG-Agent
37 http://de.wikipedia.org/wiki/Chipkarte

vorgestellt, was man da machen kann. Es kamen oft Leute auf mich zu und haben mich gefragt: „Ja, wie mache ich denn jetzt? Ich habe eine Riesendatei auf'm Server und ich möchte die gerne signieren.“ Jetzt kann man sich irgendwie einen Hash[38] machen und die Datei mit dem Hash signieren, aber das ist recht umständlich. Man möchte das eigentlich direkt signieren. Aber man möchte auf keinen Fall seinen privaten Schlüssel auf den Server hoch laden, weil der ist da doch leicht kompromittierbar. Oder der private Schlüssel ist auf 'ner SmartCard. … Was wir jetzt machen, ist, durch die Trennung zwischen GPG-Agent und GPG können wir GPG auf dem Server laufen lassen. Und der GPG-Agent, der sich um die privaten Schlüssel nur kümmert und da Operationen darauf durchführt, die halt nur auf kleinen Daten arbeiten, letztendlich auf dem Hash auf 32 Byte. Das können wir trennen und das funktioniert deswegen so gut, weil in OpenSSH v6.7[39] kann man Unix Domain Sockets[40], hier heißen die Local Sockets, auch forwarden, genauso wie wie TCP Sockets. Das ist das gleiche Prinzip wie X-Forwarding[41] … Die Operationen von GPG, die verlangen auf dem privaten Schlüssel – also signieren oder entschlüsseln – werden dann über SSH über einen Kanal an GPG-Agent auf dem Client geleitet, evtl. dort weiter an eine SmartCard und wieder zurück und das passiert da. D.h. der private Schlüssel ist lokal, und das andere ist auf dem Server. Man kann das z.B. auch benutzen um auf dem Server vielleicht mit mutt[42,43,44] seine verschlüsselten Mails zu lesen ohne seinen Schlüssel darauf zu haben. Das ist halt ein wirklich guter Newscase für die Trennung von GPG-Agent und GPG. Ganz abgesehen von der besseren Modularität ist das etwas ganz praktisches.

IE: Dann habe ich gesehen im Vortrag der GPG-Agent kann jetzt auch SSH-Agent[45,46] mitmachen, quasi. Also ich bräuchte jetzt nicht mehr zwei Sachen.

WK: Ja, ich glaube, Moritz hat das schon vor 9 oder 10 Jahren implementiert gehabt. Ich benutze das auch so lange schon. Und es gibt eine ganze Reihe, die das benutzen. Aber das ist ein Feature, das nicht ganz so bekannt ist. Der GPG-Agent kann halt den SSH-Agent ersetzen. SSH-Agent spricht ein Protokoll mit SSH. Das ist festgelegt und definiert. Und genau das implementiert GPG-Agent auch und kann sich die Schlüssel selber halten. Das ist halt ganz praktisch, das ist persistent. Man muss kein 'ssh-add'[47] mehr benutzen. Es funktioniert einfach ganz automatisch und viel bequemer als SSH-Agent vorher zu starten, der halt keine persistenten Keys hat. Und man kann ganz einfach mit den SmartCards dran arbeiten.

---

38 http://de.wikipedia.org/wiki/Prüfsumme
39 http://www.openssh.com/txt/release-6.7
40 http://de.wikipedia.org/wiki/POSIX_local_inter-process_communication_socket
41 http://wiki.ubuntuusers.de/SSH#X-Forwarding
42 http://de.wikipedia.org/wiki/Mutt
43 http://wiki.ubuntuusers.de/Mutt
44 http://www.mutt.org/
45 http://en.wikipedia.org/wiki/Ssh-agent
46 http://wiki.ubuntuusers.de/SSH#Der-SSH-Agent
47 http://wiki.archlinux.de/title/SSH-Authentifizierung_mit_Schlüsselpaaren#SSH-Agent_nutzen

IE: Und ihr habt aber auch allgemein noch an der Verschlüsselung gearbeitet. D.h. ich kann jetzt nicht nur RSA-Keys[48] und so was benutzen, sondern auch Keys, die auf elliptischen Kurven[49] beruhen.

WK: Es gibt den RFC 6637[50], der spezifiziert, wie elliptische Kurven um PGP angebracht werden. Es gab die erste Implementierung von dem Autor des RFCs vor drei Jahren oder so. Wir haben da noch einiges dran gemacht. Das geht mit GnuPG v2.1 jetzt. Man kann elliptische Kurven machen … Jetzt gibt's das kleine Problem, das diese amerikanischen Kurven … wenn ich von Kurven rede, kann man das auch Domain Parameter nennen. Und die beschreiben genau, wie die Kurve ist. Die legt man einmalig fest und das entspricht in etwa so was wie den Schlüssellängen. Viele Leute mögen diese Kurven nicht, weil keiner genau weiß, wie die entwickelt wurden, ob da nicht was nicht ganz koscher ist mit diesen Kurven. Und auch diese europäischen Brainpoolkurven[51], die dann viele anbieten, sind A) langsamer, wenn man die benutzt und nun ja, ich weiß nicht, ob man in Europa den Geheimdiensten, die da mitgewirkt haben, so vertrauen sollte. Warum soll man das machen und sollte nicht Bernstein's und Lange's Entwicklung benutzen, also Curve25519[52] bzw. den dazu gehörigen Signatur-algorithmus. Und genau das machen wir so. Wir haben für den Signatur-algorithmus … die Kurve heisst dann Ed25519 … das ist implementiert. Ich hab dann einen Draft für 'nen RFC geschrieben und dann war's implementiert. Google hat gesagt, ihre End-to-End-Implementierung in der Gruppe … sie werden das auch so in CC umsetzen dafür. Womit wir eine gute Basis haben werden dafür für Schlüssel … Meine Git[53] commit messages werden inzwischen damit signiert. Es können halt noch nicht viele damit umgehen. Das ist das, was in Zukunft der Default-Schlüssel sein soll und nicht die NIST-Kurven[54]. Aktuell ist Verschlüsselung mit dieser Curve25519 noch nicht drin, weil wir uns noch auf kleine Details einigen müssen. Das bezieht sich auf Point Compression oder Darstellung der Punkte im Protokoll. Das ist eigentlich eine Kleinigkeit … ist aber nicht so wichtig, weil Verschlüsselungs-Key das ist ein Sub-Key, den kann man jederzeit später an den Haupt-Key dran machen und deswegen kann das ruhig in einer nächsten Version erst passieren.

IE: Das heisst, ihr unterstützt diese NIST-elliptischen Kurven gar nicht oder die auch?

WK: Doch, die sind voll unterstützt. Im RFC steht ... ich glaube, es steht drin „must be supported“. Die werden schon unterstützt, aber keiner muss die anwenden. Und wenn man auswählt, ist auch die erste Kurve, die aufgelistet wird, ist Curve25519. Was aussagen soll, dass das in Zukunft der Default sein

48 http://de.wikipedia.org/wiki/RSA-Kryptosystem
49 http://de.wikipedia.org/wiki/Elliptische_Kurve
50 http://www.rfc-base.org/rfc-6637.html
51 http://www.security-insider.de/themenbereiche/netzwerksicherheit/protokolle-und-standards/articles/450828
52 http://de.wikipedia.org/wiki/Curve25519
53 http://de.wikipedia.org/wiki/Git
54 http://de.wikipedia.org/wiki/Elliptic_Curve_Cryptography

soll.

IE: Auch SSH benutzt die elliptischen Kurven ja schon eine Weile und man kann das …

WK: TLS auch … und auch gerade die Bernstein-Kurven. Es gibt seit über einem halben Jahr in der IETF[55,56] … seit über einem Jahr sind sie schon am diskutieren … das geht hin und her … so eine Art Denial of Service[57] … es kommt nichts wirklich bei raus … alle warten darauf, dass irgendwann mal was passiert. Es passiert irgendwie nichts, man einigt sich auf nichts. Obwohl eigentlich alles klar ist. Ich weiß nicht, woher das kommt.

IE: Ja gut, es gibt manchmal so Arbeitsgruppen, da wird es einfach nichts. Gut, dann eine andere Sache: GPG wird ja ganz oft zur Mail-Verschlüsselung verwendet. Du hast ja auch gesagt, Edward Snowden hat das verwendet. Jetzt ist einer der Punkte, wie man Schlüssel findet und wie man sich gegenseitig vertraut, dieses Web of Trust[58] … ja, man lädt seinen Schlüssel zum Keyserver hoch und kann die irgendwie gegenseitig signieren. Aber so richtig kann man auch nicht verifizieren, kommt der Key jetzt auch wirklich von demjenigen. Weil, ich kann auch – was weiß ich – 'nen Key für angelamerkel@bundestag anlegen, wenn ich das will und ihn irgendwo hoch laden. Und dann könnte mir jemand damit verschlüsselte Mails schicken. … Weiß ich nicht, ob das wirklich Sinn macht. Aber so richtig kann ich nicht verifizieren, ist der Key, den ich jetzt benutzen will, demjenigen, dem ich eine Mail schreiben will, ist das wirklich der Key, den der benutzt. Gibt's da irgendwie 'nen Ansatz, dass besser zu machen oder anders zu machen?

WK: Ja, wenn man das Web of Trust benutzt, dann würde so etwas nicht passieren. Dann würde man ja feststellen, dass der Schlüssel nicht authentisch ist. Und er wäre authentisch weil halt andere das letztendlich unterschrieben haben, dass er das ist. Aber in der Praxis ist das Web of Trust eher ein Game for Geeks und man macht da irgendwie Party und es ist einfach nur cool, Schlüssel zu unterzeichnen. Aber in der Praxis wird sich das nicht durchsetzen. Der Plan ist … Mit Markus Brinkmann hab ich vor Jahren mal ein Paper geschrieben, wie wir das vereinfachen wollen. Und da gibt's halt einen wesentlichen Punkt. Wir müssen einfach davon abkommen von diesem „Kryptografie, es muss alles 100%ig sicher sein, oder 150 oder 200% sicher. Es müssen alle Eventualitäten berücksichtigt werden. Wir müssen ganz, ganz sicher sein, dass das der Schlüssel ist.“ Das geht aber ganz einfach an der Realität vorbei. Da sollten wir einfach ein paar Abstriche von diesen Paranoia machen und uns einfach mal ansehen, wie wir kommunizieren. Und da ist es zunächst einmal wichtig festzustellen, ich habe eine Mail-Adresse, an den schicke ich irgend etwas und dazu muss ich wissen, welcher Schlüssel dazu passt. Das kann man mit dem

55 http://de.wikipedia.org/wiki/Internet_Engineering_Task_Force
56 http://www.ietf.org/
57 http://de.wikipedia.org/wiki/Denial_of_Service
58 http://de.wikipedia.org/wiki/Web_of_Trust

Fingerprint[59] feststellen. Und deswegen muss es irgendwo eine Datenbank geben, dass der Fingerprint zur Mailadresse gehört. Das meine Mailadresse auf den Fingerprint mappen kann und mit dem Fingerprint kommt man auf den Schlüssel. Weil, den kann man vom Keyserver oder dem DNS[60] holen. … Es ist sehr schwierig, Metadaten[61] zu analysieren. Das können wir momentan auch gar nicht leisten. Wir sollten einen Schritt nach dem anderen machen. Und deswegen schlage ich – wie schon vor 9 Jahren – vor, dass die Schlüssel ins DNS gehören. Der Mailserver muss nachsehen … um den MX host[62] zu finden … und genau so kann er nachgucken, … den Local Part der Mailadresse kann man auch ins DNS mappen und darüber den Fingerprint finden. Da gibt's ein RFC zu für den entsprechenden DNS-Record. Das ist der CERT-Record, Typ 37. Das ist auch schon Jahre alt. Ist auch in GnuPG schon alles implementiert. Es müssten sich nur die, die die Hoheit über die Zone-Files[63], über das DNS haben, das ist immer der Mail-Provider[64], die müssen sich einfach nur bereit erklären, zumindest dem Benutzer die Möglichkeit geben ihren Fingerprint im DNS abzulegen. So wie ich mir das letztendlich vorstelle, ist das in den Account-Daten einfach ein Feld, wo man seinen Fingerprint rein pasten kann. Das landet dann im Zone File und kann einfach abgefragt werden. Damit hat man erst mal den richtigen Key. Ob der Key wirklich passt, ist nicht kryptografisch gesichert, dazu sollten wir etwas anderes benutzen. Dafür sollten wir dieses SSH-Modell benutzen. Dieses 'Trust on first use'[65] oder 'Trust on first contact' … wo einfach die Kommunikationsmuster, die man hat, also wie oft man mit jemandem kommuniziert hat daran eingehen, ob zustimmen, ob ein Schlüssel gültig ist, ob der wirklich zum Kommunikationspartner passt. Und damit kann man auf alle Fälle entdecken, dass da plötzlich Man-in-the-Middle[66] ist, das der Schlüssel ausgetauscht wurde. Wer SSH benutzt, kennt dieses Problem: „Ja, der Host Key gewechselt und so“. Es fällt dann sehr auf. Und dann muss man halt nachsehen, was man da macht. Das ist eigentlich so dass, was wir machen müssen. Geht aber nicht alleine. Wir Hacker können das, wenn wir eigene Mail-Server betreiben. Wenn wir unsere eigene Domain haben, können wir das natürlich machen. Aber das hilft den meisten natürlich nicht. Deswegen sind die Mail-Provider halt aufgerufen, da mitzuhelfen.

IE: Und die DNS-Provider. Also, was es maximal gibt, ist, dass man irgendwie TXT Records[67] setzen kann. Das habe ich mal gesehen, aber das war's dann auch schon.

WK: Ja, ich habe das 2006 implementiert. Da ging das mit TXT Records … was man immer so klassisch gemacht hat … bei TXT kann man was reinschreiben, kann man mit DNS experimentieren. Dieses System heißt Public Key

59 http://de.wikipedia.org/wiki/Hashfunktion
60 http://de.wikipedia.org/wiki/Domain_Name_System
61 http://de.wikipedia.org/wiki/Metadaten
62 http://de.wikipedia.org/wiki/MX_Ressource_Record
63 http://de.wikipedia.org/wiki/Zonendatei
64 http://de.wikipedia.org/wiki/E-Mail-Anbieter
65 http://en.wikipedia.org/wiki/Trust_on_first_use
66 http://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff
67 http://de.wikipedia.org/wiki/TXT_Ressource_Record

Association[68] … Das ist genau das gleiche, was jetzt auch drin ist. Ich hab das ein bisschen erweitert. Es gibt im Zuge von DANE[69] gibt es auch DANE for OpenPGP[70] … Da ist praktisch genau das selbe wieder gemacht worden, was ich da auch schon gemacht habe, wieder ein neuer Record Typ definiert worden. Aus irgendwelchen Gründen wollte der Autor den alten nicht benutzen, den es schon gibt, der eigentlich alles kann. Macht genau das gleiche. Ist halt ein Schritt in die Richtung. Und wenn das unterstützt wird, finde ich das gut.

IE: Der Unterschied bei DANE ist, DNSSEC[71] verschlüsselt. Also zumindest ist sicher gestellt, wenn ich mir das von einem DNS-Server hole, dass da nicht jemand die DNS-Abfrage irgendwie manipuliert hat.

WK: Naja, wenn man DNSSEC vertraut, wenn das funktioniert. Immerhin es funktioniert. Das DNSSEC schadet nicht. Es gibt so ein extra Gefühl von Sicherheit, das ja vielleicht besser darauf passt und man kann's nicht mehr so leicht umleiten und ändern, da gehört schon mehr Aufwand dazu. Man kann sich über DNSSEC nicht wehren, gegen gezielte Angriffe kann man sich sowieso nicht wehren. Auch nicht gegen Massenüberwachung und wenn unsere Geheimdienste da was machen wollen, dann können die das auch machen, das DNSSEC umgehen und … da gibt's genug Probleme. Es ist gut, wenn das DNSSEC drin ist, da hat man ein klein wenig zusätzliche Sicherheit, das wirklich nichts geändert wurde an dem Fingerprint und der Mail. … Aber wirklich notwendig halte ich das nicht, denn sollte der eine Schritt sein, erst mal den Fingerprint finden und der zweite Schritt ist völlig unabhängig davon eine Geschichte aufzubauen, wie der Fingerprint benutzt wurde und daran feststellen, ob sich irgendwas geändert hat, was dann verdächtig sein könnte.

IE: Wer die ganz hohe Sicherheit haben will, der kann ja immer noch den Fingerprint über eine andere Leitung überprüfen. So wie wir das früher gemacht haben, irgend jemanden angerufen und „Lies mir mal deinen Fingerprint vor“ und erst dann habe ich demjenigen vertraut. Das geht ja immer noch, das ist ja deswegen nicht weg.

WK: Ja, sicher, das ist ein alternatives Trust-Modell. Ob PGP, der Standard definiert z.B. überhaupt kein Trust-Modell, stellt nur Verfahren bereit um irgendwas drauf zu implementieren. Es gibt weiterhin das direkte Vertrauen. Ja, Schlüssel in 'ner Mail zu schicken, vorzulesen … Ja klar. Das geht immer weiter. Wer das haben will, der weiß aber jetzt schon, wie er sicher kommunizieren kann, das feststellen kann. Aber die meisten verschlüsseln überhaupt nichts, wissen gar nicht, dass da alle mitlesen können. Vielleicht wissen es jetzt mehr Leute heute, aber vergehen sich gegen gesetzliche Regelungen oder Gesetze, das halt vertrauliche Daten gerade auch bei Behörden immer wieder unverschlüsselt verschickt werden. Ansonsten wird Datenschutz sehr hoch gehalten, aber in diesem Bereich überhaupt nicht. Ja, wir müssen da natürlich helfen,

68 http://techtalk.vernetzt.org/2007/pka-public-key-association
69 http://de.wikipedia.org/wiki/DNS-based_Authetification_of_Named_Entities
70 http://www.secupedia.info/wiki/DNSSEC#DANE.2OPENPGPKEY
71 http://de.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

aber es war bis jetzt immer sehr schwierig, da was zu machen. Ich denke, es hat sich was geändert, durch Snowden.

IE: An der Stelle können wir fast froh sein, dass da mal so ein bisschen Erdbeben kam. Obwohl's ja jetzt schon wieder so abflacht. Jetzt interessiert's schon so langsam keinen mehr. Also wenn man zumindest mit normalen Leuten redet, dann ist es halt schwierig, denen klar zu machen: „Warum soll ich jetzt meine E-Mails verschlüsseln?“ … Das ist halt auch immer die Frage: „Muss ich wirklich alle E-Mails verschlüsseln? Will ich das? Ist der Aufwand es wert?“ Die Diskussion führt man halt auch immer!

WK: Ja, ich rede halt auch gerne in der Öffentlichkeit. Die meisten Mails, die ich schreibe, gehen sowieso an Mailinglisten[72]. Und da würde ich die nicht verschlüsseln, das ist ja Quatsch. Die freie Rede oder das man sich äußern kann, ist ja ein absolutes Grundrecht. Aber genau so gut gehört es dazu, dass ich bestimme darüber, wann ich wem etwas mitteilen will und das andere was mithören können. Und letztendlich das Briefgeheimnis[73] ist auch für unsere Demokratie und Gesellschaft ist das einfach total wichtig, dass wir Individuen das selber entscheiden, wann jemand anderes das mithören kann. Und diese ganzen Ideen mit Salamitaktik[74] über Vorratsdatenspeicherung[75] und Hintertüren[76] einbauen …

IE: Sonst fangen die Leute an, ihre Gewohnheiten zu ändern und sich anzupassen, weil man halt davon ausgeht, dass sie das mitlesen.

WK: Ja, also, wir hatten diesen anderen Teil von Deutschland[77] lange Jahre gehabt. Die konnten ja auch damit umgehen, dass sie überwacht wurden. Die wussten das ja auch, dass sie überwacht wurden. Aber man konnte halt nicht mehr so mit jedem reden.

IE: Genau, geht was verloren. Aber im Endeffekt unterstützt GnuPG die Möglichkeit alles im DNS-Record zu speichern. Also ihr habt Wege, die Keys, die Fingerprints irgendwo raus zu lesen. Das es halt einfacher wird. Das ich meiner Mama sagen kann: „Hier, installier dir Enigmail[78,79,80]. Installier dir GPG.“ Oder ich mach das einmal für sie. Und dann kann sie halt mit allen, die die Keys irgend-wo verteilt haben, zumindest verschlüsselt kommunizieren.

WK: Die Mechanismen sind schon seit langem vorhanden. Es hat nur nie breite Tests dafür gegeben. Und breite Tests heißen halt auch, das Nicht-Hacker da was machen, das mal austesten müssen. Sicherlich gibt's noch Fehler oder

72 http://de.wikipedia.org/wiki/Mailingliste
73 http://de.wikipedia.org/wiki/Briefgeheimnis
74 http://de.wikipedia.org/wiki/Salamitaktik
75 http://de.wikipedia.org/wiki/Vorratsdatenspeicherung
76 http://de.wikipedia.org/wiki/Backdoor
77 http://de.wikipedia.org/wiki/Deutsche_Demokratische_Republik
78 http://de.wikipedia.org/wiki/Enigmail
79 http://wiki.ubuntuusers.de/Thunderbird/Enigmail
80 http://www.enigmail.net/

Feinheiten, die man da ändern kann. Aber das können wir alles machen. Das ist gar kein Thema, eine neue Version raus zu bringen. Ja, ich hoffe, das es bald passieren wird. Mal gucken, aber das sage ich schon seit Jahren!

IE: Ja gut, aber jetzt hast du zumindest mal die Aufmerksamkeit und kannst es noch mal los werden. Vielleicht hilft es auch, wenn man ja jetzt auch öfters in den Medien ist. Und … du hast es selbst erzählt, selbst komische Boulevard-zeitungen kommen jetzt auf dich zu und wollen Interviews haben. Also, gut, die kann man ablehnen. Aber trotzdem scheint da jetzt eine größere Öffentlichkeit zu sein und das ist ja gar nicht so schlecht.

WK: Das mit der Öffentlichkeit ist ja fast noch besser als das die Finanzierung geregelt ist. Es gibt halt ein großes Interesse und eine Awareness. Da müssen wir irgendwie gucken, dass wir das noch ein wenig hoch halten. Wenn man das mal zufällig erreicht hat … ja, das sollte man schon nutzen.

IE: Gut. Vielen Dank, Werner Koch und viel Spaß hier noch auf dem Frühjahrsfachgespräch.

81 http://creativecommons.org/licenses/by-nc-sa/3.0/de