LESERFORUM

Nicht aufgeben, besser machen!

Editorial von Jürgen Schmidt über Probleme mit PGP, c't 6/15, S. 3

„Lasst PGP sterben!" klingt für mich wie der Wunsch eines Managers, ein nicht richtig funktionierendes Programm durch ein neues abzulösen, ohne dass dem Manager klar ist, wie wichtig Wartung und Pflege des existierenden Programms ist, weil es *jetzt* gebraucht wird und ein echter Nachfolger nicht wirklich in Sicht ist. Aber Software, die gebraucht, aber nicht gepflegt wird, weil man sie lieber gar nicht mehr hätte, führt meistens in eine Katastrophe. Denn 10 Jahre später wird die nicht gewartete Software immer noch gebraucht.

Ich bin daher ein Freund davon, beides zu tun, PGP zu fixen und an neuen Dingen zu arbeiten.

Genau das passiert übrigens gerade. In der Post-Snowden-Zeit sehen wir jede Menge Projekte, die mal an Verbesserungen, mal an neuen Mechanismen arbeiten. Und wie es aussieht, wird die Zeit langsam reif, all diese Ansätze zu konsolidieren und ggf. sogar zusammenzuführen. So könnte zum Beispiel eine moderne Schlüsselverwaltung, wie sie gerade bei keybase.io entsteht, mit existierenden PGP-E-Mail-Programmen verheiratet werden.

All das werden alle PGP-basierenden Projekte und Tools im April diskutieren. Denn da kommen endlich mal all diese Projekte zusammen, um gemeinsam die nächsten Schritte im Umgang mit E-Mail-Verschlüsselung zu diskutieren.

Hört also auf zu jammern und gebt uns bitte noch etwas Zeit (oder macht mit).

Nicolai Josuttis, enigmail.net

Nicht annähernd alltagstauglich

Ich hüte beruflich eine Exchange-Server-Infrastruktur und werde seit Jahren mit Verschlüsselungsanforderungen konfrontiert. Mal ist es ein Amt, das auf „papierlos" umgestellt hat, aber nur „verschlüsselte" Mails akzeptieren will – mal kommt unser Rechtsanwalt mit neuen Erkenntnissen …

Tatsache ist, dass keines der heute erhältlichen Verschlüsselungssysteme auch nur annähernd alltagstauglich ist. Neben der erwähnten fehlenden Schlüsselaustausch-Infrastruktur ist das vor allem die fehlende Unterstützung durch Software. PGP ist dabei das Schlimmste – keiner kann das bedienen, und wenn am Ende verschlüsselte Mails in meinem Eingang liegen, findet diese die Suche nicht mehr.

Stefan Heinz

Seit Jahren in Arbeit

Editorial von Jürgen Schmidt über Probleme mit PGP, c't 6/15, S. 3 und Die Schlüsselfalle, S. 160

Ein Vergleich von Online-Protokollen wie TextSecure mit Offline-Protokollen wie OpenPGP ist nicht möglich. Ein Meeting hat ja auch ganz andere Erfordernisse als ein Briefwechsel. Briefe und Berichte können aber durch Meetings nicht ersetzt werden. Wir benötigen Offline-Verfahren, da sie auch funktionieren, wenn das Netz zusammengebrochen ist. Wer „Citizen Four" gesehen hat, wird sich auch daran erinnern, wie Snowden zwischen Online- und Offline-Laptop unterscheidet.

Mail-Adressen sind durch das DNS festgelegt; deswegen sollten Schlüssel auch dort gesucht werden. Hierzu gibt es seit Jahren RFCs, und GnuPG implementiert seit 2006 verschiedene Verfahren hierzu. Diese sind auch Teil des STEED-Konzepts, wozu es in der c't 20/12 [Vertrauen auf den ersten Blick, S. 190, die Red.] bereits einen Artikel gab. Leider stehlen sich die Provider aus der Verantwortung und wiegen die Öffentlichkeit in Sicherheit durch Schwachsinn wie „E-Mail made in Germany" oder gar Verweis auf den „Hintertürdienst" De-Mail.

Werner Koch, GnuPG

IETF fördert PGP

Die Arbeitsgruppe DANE der Internet Engineering Task Force arbeitet daran, DNSSEC und DANE zum Propagieren der PGP-Schlüssel zu nutzen. DNSSEC sichert das weltweit verbreitete Domain Name System kryptografisch ab. DANE setzt es zur Authentisierung ein, beispielsweise validieren SMTP-Server ihre TLS-Zertifikate damit gegenseitig.

Die kommende Spezifikation „DANE/Openpgpkey" definiert, wie der öffentliche PGP-Schlüssel in einer DNSSEC-gesicherten DNS-Zone abgelegt wird. Anders als bei den PGP-Keyservern behält der Besitzer die Kontrolle darüber und kann ihn ersetzen oder entfernen.

Mit dem Kommandozeilen-Tool `openpgpkey`, das zum Hash-Slinger-Paket der Linux-Distribution Fedora gehört, können Entwickler schon mal Erfahrungen sammeln. Das sind zwar erst die Anfänge, aber man kann schon das Potenzial erkennen. Die Arbeiten könnten im ersten Halbjahr 2015 abgeschlossen sein. Was dann noch zu einer komfortablen Lösung fehlt, sind Tools, die das Veröffentlichen, Beziehen und Prüfen von Schlüsseln automatisieren.

Carsten Strotmann

Windows nicht zwangsläufig

Altes Blech, Was sich bei gebrauchten PCs lohnt – und was nicht, c't 6/15, S. 82

Zitat: „Die Preisuntergrenze liegt bei 75 Euro – so viel kostet das billigste Windows 7 oder 8 im Einzelhandel." Wieso nehmen Sie an, dass man zwangsläufig Windows verwenden muss? Es gibt kostenlose Alternativen, die technisch besser sind und für die große Mehrheit der Benutzer alle benötigte Software nativ an Bord haben. Gerade die anvisierte Käufergruppe, die entweder Geld sparen möchte oder aus ethischen Gründen zu Gebrauchtgeräten greift, könnte an diesen Windows-Alternativen interessiert sein.

Martin Rogge

Bewusst schlechte Neugeräte

Unübersichtliche Schnäppchenjagd, Der schwere Stand gebrauchter Notebooks, c't 6/15, S. 84

Seit einigen Jahren scheint sich der Preisdruck so immens gesteigert zu haben, dass immer mehr Hersteller bewusst technisch schlechtere Geräte bauen, weil diese dann ein paar Euro billiger sind. Bei den Notebooks hat sich Lenovo zum Beispiel von den eigentlich schon ikonographischen (und in allen Tests zu Recht gelobten) Tastaturen mit dem 7-Zeilen-Layout verabschiedet hin zu den gleichen schlechten Tastaturen mit miserablem Layout, das auch alle anderen Hersteller haben. Die damals erhältlichen Modelle mit 4:3- oder 16:10-Bildschirmen wurden in späteren Serien durch vermutlich billigere 16:9-Screens ersetzt und geniales Hardware-Design, etwa das Clam-Shell-Ge-

häuse oder der Trackpoint mit eigenen Tasten, wurde ebenfalls gestrichen. Leider loben Sie in Ihren Tests die Lenovo-Geräte weiterhin, obwohl sie außer dem Namen nichts mehr mit den bekannten Profigeräten der IBM-Thinkpad-Ära zu tun haben. Wenn man sich also ein Gerät wie ein X201 oder W500 gebraucht kauft, hat man genügend Rechenleistung und ein Gerät, das bei sorgsamer Behandlung noch sehr lange durchhalten wird und bei dem man sich nicht täglich mit den genannten Nachteilen rumärgern muss.

Ein ähnliches Bild bei den Monitoren: Wenn man IPS-Monitore aufgrund des Glitzerns und des IPS-Glows nicht benutzen möchte, bleiben einem nur noch TN-Displays, es sei denn, man kauft sich gebrauchte Displays mit S-PVA Panel. Wenn man dabei zu besseren Geräten etwa von Eizo greift, lassen sich dank Hardware-Kalibrierbarkeit selbst Geräte mit mehreren tausend Stunden Betriebsdauer noch sehr gut verwenden.

Christoph Wagner

Falsche Vergleiche

Sie vergleichen ein hochwertiges HP Elitebook mit 300-Euro-Notebooks von Aldi oder aus dem Mediamarkt. Selbst ein fünf Jahre altes HP Elitebook (oder Business-Notebook anderer Hersteller) finde ich immer noch hochwertiger und wartungsfreundlicher als diese „Plastikbomber“ aus dem Billig-Markt.

Haben Sie schon mal versucht, für so ein Plastik-Teil Ersatzteile zu finden, geschweige denn ein Service-Manual? Oder mal versucht, so einen verclipsten Plastikbomber zu demontieren? Bei Business-Notebooks ist das kein Problem. Für HP bekomme ich in der Regel alle Ersatzteile, die ich benötige, gebraucht zu günstigen Preisen oder notfalls eben etwas teurer direkt von HP. Dank Ersatzteilnummer ist es dann auch das richtige Teil. Sie sollten also gebrauchte Business-Notebooks immer in Relation zu neuen Business-Notebooks setzen, nicht zu billigen Consumer-Produkten. Richtig finde ich aber Ihre Aussage, dass man bei gebrauchten Notebooks möglichst immer die hochwertigste Ausstattung (Display, Prozessor) der Serie kaufen sollte.

Joachim Schulz

Lärmschutz für Schlagzeuger

Ruhe, bitte, Headsets mit aktiver Geräuschunterdrückung im Praxistest, c’t 6/15, S. 108

Zu dem Kasten auf Seite 113 (Ohrschützer statt Kopfhörer) möchte ich Ihnen folgenden Hinweis geben: Es gibt im Musikfachhandel spezielle Kopfhörer für Bühne/Studio, die besonders auf laute Situationen (besonders am Schlagzeug) zugeschnitten sind. Diese Kopfhörer sind vom Aufbau her mit den von Ihnen erwähnten Kapselgehörschützern vergleichbar. Die Außendämpfung ist gefühlt mit „Mickymäusen“ vergleichbar. Diese Kopfhörer besitzen auch integrierte Treiber, sodass die Kombination Kapselgehörschutz/In-Ear nicht notwendig ist.

Geeignete Kopfhörer wären z. B. der MF-5000DR von Monacor für 50 Euro oder der t.bone HD990D von Thomann (27 Euro). Letztgenannter Kopfhörer hat laut Datenblatt eine Außengeräuschdämmung von 22 dB(A). Klanglich sind die sicher nicht mit hochwertigen In-Ears oder High-End-Kopfhörern vergleichbar, aber in lauten Umgebungen sind sie sicher ein guter Kompromiss für den Preis.

Markus Kafurke

Die Revolution kam nicht

Überholen, ohne einzuholen, Welche Speicherchip-Technik nach NAND-Flash kommt, c’t 6/15, S. 144

Ihr Titel provozierte bei mir einen Flash – aber keinen NAND-Flash, sondern einen im Gehirn: Eine Melodie begann zu spielen, nämlich die des Liedes „Überholen ohne einzuholen“ von der Platte „Für uns, die wir noch hoffen“ aus dem Jahr 1973 von Pannach, Fuchs und Kunert, die als antistalinistische Gruppe in der DDR Musik machten und vorher Renft-Combo hießen. Als junger Mensch habe ich an die Machbarkeit einer besseren, nicht-kapitalistischen Welt geglaubt; wir hatten 1977 in Darmstadt ein Komitee für „demokratische Rechte und Freiheiten in ganz Deutschland“. Ich war beteiligt daran, dass die drei DDR-Musiker in der Otto-Berndt-Halle der Technischen Hochschule auftreten konnten – vor immerhin 1000 Leuten.

Tja, die Revolution kam nicht und heute muss man sich Gedanken machen, ob vielleicht diese Mail von mir an Sie irgendeinen geheimen Scorewert verschlechtert. Der Liedtext ist jedenfalls, wenn man sich in sozialen Organisationen jedweder Art bewegt, immer noch aktuell. Und ob der von Ihnen gewählte Titel eine journalistisch hintersinnige Attacke auf das eigene Blatt, eine Art stiller Protest für Connaisseure ist, wird ein Geheimnis bleiben, jedenfalls solange der Zugriff auf den Hirnspeicher noch nicht eröffnet ist.

Die Zeitschrift c’t gefällt mir gut – einerseits, weil mir das systemkonforme Neuheitenschnüffeln zusagt, andererseits aber auch, weil Ihre Zeitschrift ein wahres Kaufverhinderungsblatt ist: Genau gelesen kommt man ein ums andere Mal zum Schluss, dass es in vielen Sparten vernünftige Produkte letztlich einfach nicht gibt. Und aus diesem Grund unterstützt dann auch meine Frau die Lektüre.

Hamid Moghareh-Abed

Der Titel zitiert die berühmte Parole Walter Ulbrichts, die ursprünglich wohl von einem sowjetischen Kybernetik-Professor stammt. Mir kam der Spruch in den Sinn, weil mir seit mehr als einem Jahrzehnt großspurige Ankündigungen angeblich überlegener Speichertechniken auf den Schreibtisch flattern, die sich aber dann doch fast nie durchsetzen.

Die Katze wars

Endlich durchschlafen, Windows an unerwünschtem Aufwachen hindern, c’t 6/15, S. 166

Vielen Dank für Ihren Artikel. Er hat mir geholfen, ein lange vorhandenes Ärgernis zu beheben. Mein Kater nutzt die Nachtzeit gerne, um über die Tastatur zu streunern oder die Maus zu „bepföteln“. Zur Freude meiner Stromrechnung kann der PC jetzt wieder durchschlafen.

Thomas Steinfeld

Ergänzungen & Berichtigungen

Sicherheitslücke bei Qustodio

Filter, Zeitwächter und Verpetzer, c’t 6/15, S. 54

Die Lenovo-Bundling-Adware Superfish ist durch eine Sicherheitslücke in die Schlagzeilen geraten, die bei verschlüsselter Web-Kommunikation einen Man-in-the-Middle-Angriff ermöglicht. Wie sich inzwischen gezeigt hat, hängt diese Sicherheitslücke mit der SSL-Unterbrechungstechnik „SSL Digestor“ des Herstellers Komodia zusammen, die nicht nur bei Superfish zum Einsatz kommt. Vielmehr ist unter anderem auch der in c’t 6/15 vorgestellte Windows-Client des Kinderschutzsystems „Qustodio“ betroffen. Dessen Einsatz zur Überwachung von Windows-Rechnern stellt somit ein Sicherheitsrisiko dar und ist so lange nicht zu empfehlen, bis eine neue Softwareversion die genannte Sicherheitslücke schließt. Näheres dazu auf heise.de/-2557619

Die Cloud im Raspi

Sync- und Heimserver Ionas, c’t 6/15, S. 66

In der Produktbeschreibung im Kasten hat sich ein Fehler eingeschlichen: Die USB-Festplatte hat, wie im Text erwähnt, 1 TByte Speicherplatz, nicht 1 GByte.

Unübersichtliche Schnäppchenjagd

Der schwere Stand gebrauchter Notebooks, c’t 6/15, S. 84

Das Lenovo ThinkPad T420 hat anders als im Artikel beschrieben doch kein USB 3.0. Auch an der Docking-Station findet sich nur USB 2.0. Immerhin hat es einen ExpressCard-Schacht, sodass bei Bedarf USB-3.0-Adapter einsteckbar sind.

Der optimale Photoshop-PC

PC-Hardware für die Bedürfnisse von Photoshop, c’t 6/15, S. 148

Am Ende des Textes ist von einem Core i7-4970 die Rede. Dort hat sich ein Zahlendreher eingeschlichen. Die korrekte Bezeichnung lautet Core i7-4790.