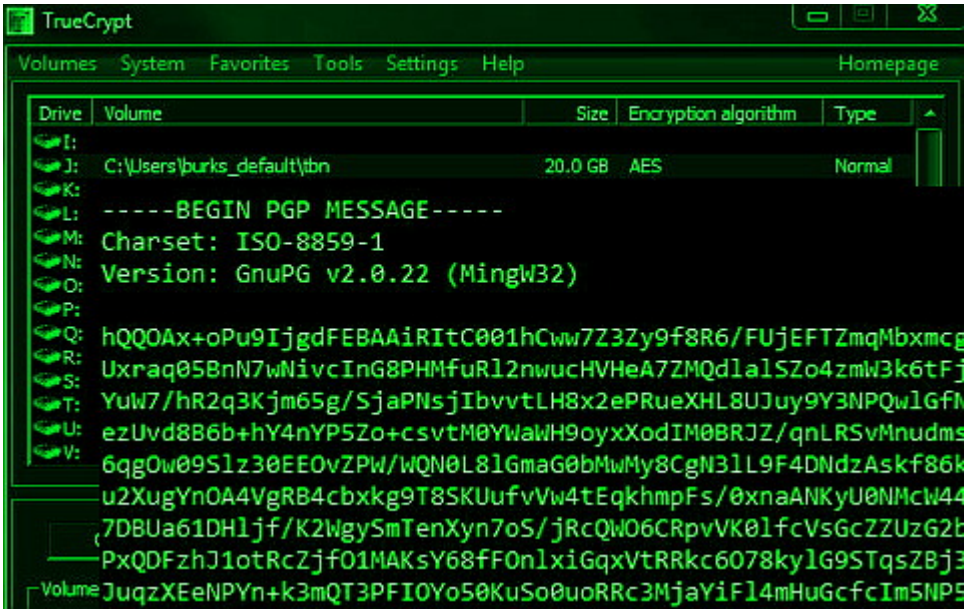
Operation Socialist oder: Verschlüsselung funktioniert



Schließlich ist es in demokratischen Gesellschaften keine Illusion der Freiheit, zu sagen, dass wir nicht angemessen erklären können, warum die Medien so einseitig berichten, als ob sie vom Staat genau instruiert würden, was sie drucken oder auf den Bildschirm bringen sollen. Warum tendiert eine so große Zahl von Journalisten, die sich nur auf ihre ‚Freiheit' berufen, auf eigenes Risiko zu publizieren, dahin, ganz spontan und ohne Zwang immer wieder eine Weltauffassung zu reproduzieren, die sich innerhalb der selben ideologischen Kategorien bewegt? Warum verwenden sie immer wieder ein so eingeschränktes Repertoire innerhalb des ideologischen Feldes Selbst Journalisten, die sich als Störenfriede verstehen, scheinen oft von einer Ideologie imprägniert zu sein, zu der sie sich nicht bewusst bekennen und die sie stattdessen 'schreibt'. (…)

Deshalb nützt es nichts, wenn Leute sagen, 'natürlich leben wir in einer freien Gesellschaft, die Mediensind frei' darauf zu antworten. 'nein, sie agieren nur unter Zwang des Staates'. Wenn es es doch nur täten! Wir müssten dann nur die vier oder fünf Aufsichtsbeamten durch Leute von uns ersetzen." (Stuart Hall: Ideologie, Identität, Repräsentation – Ausgewählte Schriften 4, Argument Verlag Hamburg 2004, S. 47)

Das frage ich nicht immer, wenn ich die Berichte über die zahllosen aktuellen Überwachungs"skandale" lese. The Intercept berichtet ausführlich, wie der britische Geheimdienst den belgischen Provider Belgacom mit Malware infizierte. Was lehrt uns das? Nichts, wenn man den Medien glaubt. Niemand stellt die Systemfrage. Empörung ist aber nichts, was weiterhilft.

Ich empöre mich sowieso nicht, weil ich von der herrschenden Klasse und ihren Helfershelfern gar nichts anderes erwarte. So what? Kann es wirklich sein, dass kein einziger Journalist in ganz Deutschland auf die Idee kommt zu fordern, man müsse vielleicht den Kapitalismus an sich ein wenig kritischer sehen?

(Es tut mir leid, aber ich habe es aufgegeben, deutsche Mainstream-Medien zum Thema Überwachung zu rezipieren: ich ärgere mich zu sehr über den Quatsch, den ich dort lesen muss – die Hälfte von dem, was gesagt werden müsste, fehlt, und der Rest ist meistens missverständlich und fehlerhaft.

Sogar Heise nehme ich nicht aus: *…die anvisierten Ingenieure ‚gejagt' worden. Die konnten dann individuell mit Malware angegriffen und ihre Computer infiziert werden. Dafür seien sie wohl per ‚Man-in-the-Middle'- oder ‚Man-on-the-Side'-Angriff auf eine gefälschte LinkedIn-Seite geleitet worden, wo ihnen Malware untergeschoben wurde.*"

Fakten, Fakten, Fakten will ich wissen – sollten die Betroffenen wirklich so bescheuert gewesen sein, um auf simple Phishing-Angriffe hereinzufallen? Dann geschieht ihnen ganz recht, und man könnte zusätzlich beruhigt sein, dass dem englischen Geheimdienst offenbar nicht viel einfällt. LinkedIn: „Connect, share ideas, and discover opportunities" – muahahahaha.)

Die gute Nachricht: Verschlüsselung funktioniert, wobei die Verschlüsselung der Inhalte noch wesentlich sicherer ist als Transportverschlüsselung, weil es weniger Fehlerquellen und Angriffspunkte gibt. Ein Journalist, der den Unterschied gar nicht kennt und ihn auch nicht erwähnt, hat eben auch nichts begriffen und verwirrt die Leute nur, die sich gern mit dem Thema beschäftigen, aber nicht wissen, wie sie das anstellen sollen.

Interessant, dass Stuart Hall „wir" schrieb und damit die

„Linke“ meinte. Auch so etwas würde ein deutscher Journalist nie wagen, und schon gar kein Wissenschaftler hierzulande.

Und wir rufen den Deutschen zu:

Die Stuttgarter Zeitung (via Fefe) zitiert Günther Oettinger. „‚Übertreibt es nicht mit dem Datenschutz‘, rief er den Deutschen zu. Wer Daten perfekt schütze, der könne sie nicht mehr nutzen.“

Das kann man mal so unkommentiert hier stehen lassen.

Ich weiss, wo du gestern (und auch sonst) gewesen bist

Mir fiel auf, dass einige Leute, die ein Konto bei Google haben, gar nicht wissen, welche Features sich dort verbergen, Google Calendar (Google Kalender) zum Beispiel. Ich empfehle, sich die Einstellungen anzusehen und nach Wunsch zu konfigurieren und sich der Risiken und Nebenwirkungen bewusst zu sein. (Ja, ich nutze Google Calendar.)

Alle sind verdächtig

Heise: „Die britische Innenministerin Theresa May nimmt einen erneuten Anlauf, um verdächtige Internetznutzer identifzierbar zu machen. Ein Gesetzentwurf sieht vor, dass Internet-Provider dafür sorgen sollen, dass Kunden eindeutig per IP-Adresse identifiziert werden können,…“

It will therefore require internet providers to retain Internet Protocol – or IP – address data to identify individual users of internet services.

Ach ja. By the way: „The Tor software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.“

Durch das geltende Recht vor Missbrauch gesichert oder: Beamen schadet ihrer Gesundheit nicht

Heise über die Gesundheitskarte und den Datenschutz, wie das Bundesozialgericht den definiert:
Die Ausgabe einer eGK sei „in ihrer gegenwärtigen Gestalt und ihren gegenwärtigen wie zukünftigen Pflichtangaben und Pflichtanwendungen“ durch überwiegende Allgemeininteressen gerechtfertigt. Auch die Argumentation des Klägers, dass er nicht kontrollieren könne, ob seine persönlichen Daten auf der Karte sicher seien, wurde vom Gericht verworfen. Seine Daten seien durch das geltende Recht vor Missbrauch gesichert. Die vom Kläger behauptete unzureichende Datensicherheit ist nach Ansicht des Gerichtes derzeit nicht feststellbar, weil sich die Telematik-Infrastruktur noch im Teststadium befindet.

Schon klar. Das geltende Recht definiert, was Recht ist. Dem Gericht kann man keinen Vorwurf machen, sondern „dem

Gesetzgeber“, der Blödsinn als rechtens definiert. Im Klartext heisst das doch: Man kann nicht feststellen, ob die Daten missbraucht werden (können), weil die Telematik (wie Informationen verknüpft und verarbeitet werden) der Gesundheitskarte noch gar nicht fertig ist, sondern zur Zeit noch getestet wird.

Man muss das auf das Beamen übertragen. Man testet noch an Insekten, ob das Beamen lebender Wesen von einem Ort zum anderen möglich sei. Das sei aber auch ungefährlich für Menschen, hat ein deutsches Gericht entschieden, da das geltende Recht verbiete, einem Menschen durch Beamen Schaden zuzufügen. Außerdem diene das Beamen den überwiegende Allgemeininteressen.

Truecrypt ist sicher

Truecrypt ist sicher, wenn man es richtig anwendet. Heise zitiert heute einen Polizisten, der das Passware Kit Forensic eingesetzt haben will:
Heute gelang mir der Zugriff auf eine Truecrypt-Partition in einem sehr wichtigen Fall. Alle relevanten Informationen für den Fall waren darauf gespeichert. Andere Produkte hatten zuvor versagt.

Ich sehe hier keine zwei unabhängige Quellen, die heranzuziehen für eine solch windige These Journalisten in der Pflicht sind, sondern nur eine nicht nachprüfbare Propaganda-Behauptung des Software-Herstellers. Selbst wenn das wahr sein sollte, handelt es sich um ein nachvollziehbares Szenario, wie im Heise-Forum ganz richtig angemerkt wird:

„If the target computer with the encrypted volume is powered off, encryption keys are not stored in its memory, but they

could be possibly recovered from the hiberfil.sys file, which is automatically created when a system hibernates.

NOTE: If the target computer is turned off and the encrypted volume was dismounted during the last hibernation, neither the memory image nor the hiberfil.sys file will contain the encryption keys. Therefore, instant decryption of the volume is impossible. In this case, Passware Kit assigns brute-force attacks to recover the original password for the volume.

Das heißt: Ein Angriff ist unter Umständen möglich, wenn ein Truecrypt-Container *nicht* per *dismount* geschlossen, sondern der Rechner nur heruntergefahren wurde, also dann, wenn der Nutzer sind fahrlässig verhalten hat.

Sorry, aber das *muss* in einen solchen Artikel, sonst ist das reine Panikmache.

Es gibt absolute Anonymität im Internet

Spiegel online, gewohnt „investigativ“: „Ziel der Aktion [gegen den Handel mit illegalen Drogen im Darknet] sei es aber gewesen, das allgemeine Vertrauen in die Anonymität des Internets, auch des sogenannten Darknet, nachhaltig zu erschüttern. ‚Es gibt keine absolute Anonymität im Internet‘, sagte sie. Wie die Ermittler die Betreiber identifizieren konnten, blieb unklar.“

Das Ziel haben sie nicht erreicht. Mein Vertrauen ist nicht erschüttert – weil ich den dämlich-dümmlichen Berichten in den Medien, die sich – wie Spiegel online – für die Propaganda der Überwachungs-Lobby missbrauchen lassen, nicht glaube, sondern

selbst recherchiere. Das hat mich eine Viertelstunde gekostet, zu viel Recherche-Zeit für deutsche Mainstream-Qualitätsmedien.

I'm laughing so hard at this.

Es gibt absolute Anonymität im Internet – wenn man keine Fehler macht.

Secure Messaging Scorecard

Die Electronic Frontier Foundation (EFF) hat eine Checkliste für die Sicherheit von Messengern publiziert.
In the face of widespread Internet surveillance, we need a secure and practical means of talking to each other from our phones and computers. Many companies offer „secure messaging" products – but are these systems actually secure? We decided to find out, in the first phase of a new EFF Campaign for Secure & Usable Crypto.

Secret Manuals oder: Emulating an access point

3 Install the agent on the target device with the selected methods.
See "List of installation vectors" on page 138 .

List of installation vectors

Operating systems supported by agents

Operating systems supported by the various desktop and mobile devices are listed b

Device	*Operating System*
Desktop	• Windows • OS X
Mobile	• Android • BlackBerry • Windows Mobile • Symbian • IOS

The Intercept: „Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide – Hacking Team manuals, dated September 2013, provide step-by-step instructions for technicians, administrators, and analysts on how to infect a device and set up spying.“

„The spyware installer might lay in wait in a hotel, or a Starbucks, and gain access to your computer by ‚emulating an access point' – in other words, pretending to be a free wifi hotspot to which the victim connected previously.“

Ich weiß ja nicht, aber wer ist denn so blöde, darauf hereinzufallen? Ich habe mir mal einige dieser Handbücher durchgesehen, vor allem das rcs-9-technician-final.pdf ist interessant. Auf keinen Fall kann die Spionage-software zum Erfolg kommen, wenn der Nutzer sich vernünftig verhält. Und bei Linux auch nicht. Wen wollen sie also ausspionieren? Klein Fritzchen?

Cookies for ever

Aus der Tor-Mailingliste:
The Tor Browser is already having a hard time fighting against the numerous browser fingerprinting scheme that exists today. Telling people they will be anonymous using their normal Internet Explorer is misleading if not dishonest. Using evercookies will be enough to track them across restarts and networks.

Man spricht sich dort definitiv gegen das Projekt „anonabox : a Tor hardware router“ aus, weil es den Leuten Sicherheit nur vorgaukeln würde.

Ich habe etwas zu verbergen!

Heise zitiert Edward Snowden: „Die verbreitete Haltung, ‚ich habe nichts zu verbergen‘, verschiebe die Verantwortung für die Wahrung der Bürgerrechte, argumentierte Snowden: ‚Wenn man sagt, ‚Ich habe nichts zu verbergen‘, sagt man tatsächlich

‚Mich interessiert dieses Recht nicht.‘ Man sagt ‚Ich habe dieses Recht nicht, weil ich […] es rechtfertigen muss.‘ Tatsächlich müssten Regierungen Eingriffe in die Bürgerrechte rechtfertigen, nicht umgekehrt.“

Das Original-Interview (Video) steht in The New Yorker.

Kronjuwel der strategischen Kooperation

Sueddeutsche.de: „NSA und BND arbeiteten in der „Operation Eikonal“ jahrelang zusammen, um Internetdaten und Telefonverkehr in Frankfurt abzufangen. Dass dabei Daten von Bundesbürgern rechtswidrig in die USA gelangten, nahm die Bundesregierung in Kauf. Abgesegnet hat die Sache ein Mann, der auch heute Minister ist.“

Na und? Das wird keine Folgen haben.

Oettinger verspricht mehr Datenschutz

Günther Oettinger verspreche mehr Datenschutz, meldet Heise. O-Ton geleakt:

„Ei heff schkpiekt wiss aua amerikäin frennz ent Partnass abaut siss proplemm, witsch iß not sehr, äss aua chanzellohr sett bifohr“ (Der Rest bleib leider undokumentiert, da sich

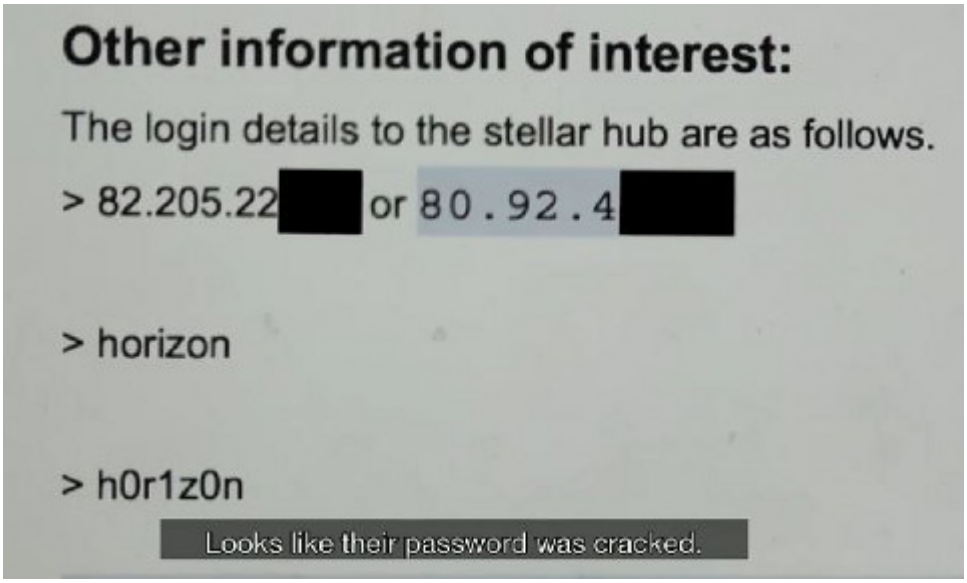
die Stenotypistin hier am Stromkabel ihres Notebooks erhängte.

Dpo meldet passend dazu: „Angriff auf EU-Digitalkommissar: Günther Oettingers Schreibmaschine von Unbekannten gehackt“.

There must be some other reason

John Gilmore (u.a. Mitglied der EFF) fragt auf cryptome.org, warum man Apple glauben schenken sollte, wenn es um den Schutz der Daten geht.

You have been tasked, key employee!



Spiegel online (Video mit gewohnt nerviger Zwangswerbung

vorab): „German firm Stellar brings internet access to remote locations via satellite. Documents provided by Edward Snowden show, that the companys systems were hacked by the british GCHQ. Stellar-representatives and engineers are shocked.“

Hübsch finde ich die Stelle, an der der Name eines der Angestellten in den Geheimdienst-Dokumenten auftaucht und der Betroffene sichtbar schlucken muss. Das Passwort kann man aber schon beinahe raten…

Ich frage mich, warum sich die Leute aufregen. Wir haben doch schon seit langem das Telekommunikationsgesetz (TKG) §112, das die automatisierte Abfrage für unsere Geheimdienste regelt, die die Daten dann unter Freunden in die USA verschieben.

Das Ende ist nah!

Winfuture: „Fast gar keine Rolle spielt die klassische E-Mail für den persönlichen Austausch unter Jugendlichen. Nur 7 Prozent halten E-Mails für ein wichtiges Kommunikationsmittel.“

Nationale Kryptografie oder: Deutsche Schlüssel

Deutsche Schlüssel nur für Deutsche (via Fefe).
Bruhahahahaha.

Robust encryption? It’s the economy, stupid!

Wired interviewt Edward Snowden:
Nor is he optimistic that the next election will bring any meaningful reform. In the end, Snowden thinks we should put our faith in technology—not politicians. “We have the means and we have the technology to end mass surveillance without any legislative action at all, without any policy changes.” The answer, he says, is robust encryption. “By basically adopting changes like making encryption a universal standard—where all communications are encrypted by default—we can end mass surveillance not just in the United States but around the world.” (S. 7)

Sorry, aber da liegt Snowden total daneben. Die breite Masse interessiert das Thema „Überwachung“ nicht. Das hat seine Gründe. It’s the economy, stupid!

Gamma International Leaked

Allein schon dier Titel lässt einen gruseln: „Govermental IT Intrusion and Remote Monitoring Solutions“. Es gibt jetzt einen Twitter-Account („Phineas Fisher“) zum FinFisher-Hack (vgl. netzpolitik.org, 06.08.2014) und mehr Details auf reddit.com. Interessant, dass man sich auf „Anarchism“ beruft. (Vgl. auch Bahrain Finfisher System logs (Feb 2012)

Skypekit

Ich habe die Skype-Software schon seit langem von meinen Rechnern geworfen, weil Skype bekanntlich Malware ist. Meinen Skype-Account nutze ich via Trillian. Das ging aber nicht mehr. (Ich nutze Skype eigentlich nur, um als Warlord virtuelle Hauereien in Secondlife zu koordinieren.)

Am 12. Juli 2013 wurde durch von Edward Snowden geleakte Informationen bekannt, dass den amerikanischen Geheimdiensten durch Microsoft tatsächlich direkter Zugriff auf den gesamten Skype-Verkehr gewährt wird und sowohl Textchats als auch Telefonate und Videotelefonate nach Belieben von der NSA mitgeschnitten und ausgewertet werden können, da es dem Geheimdienst mit Hilfe des direkten Zugriffs auf die Skype-Server möglich ist, die Skype-Verschlüsselung zu umgehen.

Jetzt habe ich eine Lösung für Windows 7 gefunden: „Skypekit in Trillian noch eine Weile weiter nutzen“.

Ich möchte die technikaffinen Leserinnen und sicherheitbewussten Leser auffordern, mir die Risiken des älteren Skypekit via Trillan aufzuzählen.