Beilage zur HUch! 53
Schwerpunkt: Datensicherheit
April 2008

HOW TO...

Email-Verschlüsselung mit Thunderbird, GnuPG und Enigmail

Hier vorgestellt wird das Verschlüsseln und das Signieren von Emails mittels Thunderbird und GnuPG. Thunderbird ist ein Email-Client, der in etwa die Funktionen von Microsoft Outlook bietet; GnuPG („GNU Privacy Guard“) ermöglicht verschiedene Formen von Verschlüsselung. Zwischen diesen beiden vermittelt ein Plugin namens Enigmail, das im Thunderbird installiert werden muss. Andere Kombinationen von Software sind denkbar. Aus praktischen Gründen wird hier allerdings nur diese Kombination für GNU/Linux, Windows- und Mac-Betriebssysteme vorgestellt.

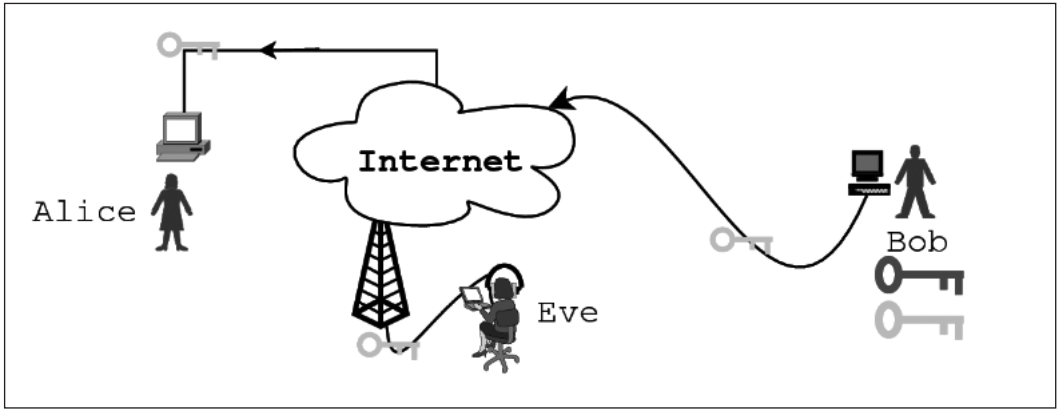
Problemstellung

Bei der Email-Kommunikation im Internet stellen sich grundsätzlich zwei Probleme: Das Problem der Privatsphäre und das Problem der Authentizität. Um dies weiter zu verständlichen ist ein kurzer Exkurs in die Funktionsweise des Internets nötig. Verschickt mensch eine Email, so wird diese über verschiedene Server und Router weitergeleitet, bis sie schließlich in der gewünschten Mailbox landet. Jede dieser Vermittlungsstellen empfängt die Mail, erzeugt eine Kopie und leitet diese weiter. Es gilt die Regel: „Every act on the internet is a copy.“ Aus dieser Tatsache ergibt sich das Problem der Privatsphäre, denn im Prinzip kann jede Vermittlungsstelle auch mehrere Kopien erstellen und diese an beliebig viele weitere Empfänger_innen senden. Dies passiert für Versender_innen und Empfänger_innen unsichtbar.

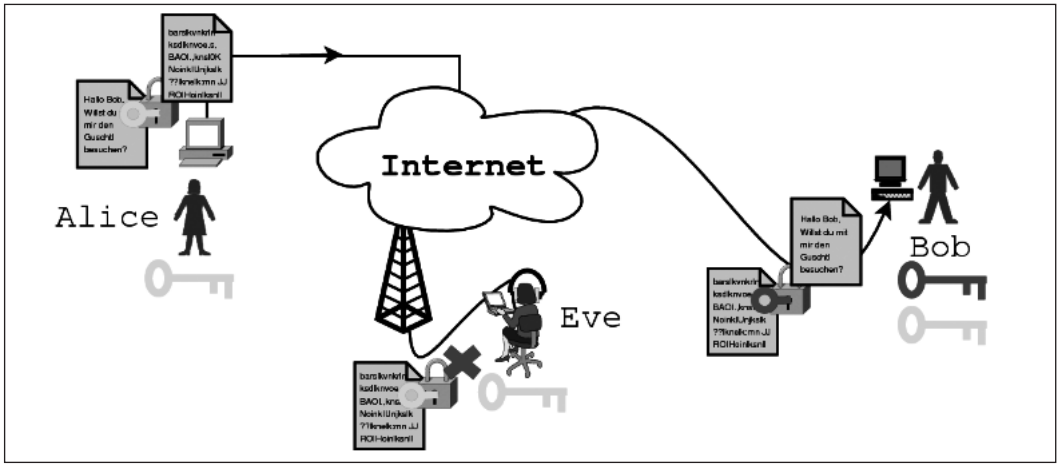
Das zweite Problem der Authentizität ergibt sich ebenfalls aus der Tatsache, dass jede Mail über verschiedene Vermittlungsstellen geleitet wird. Jede dieser Stellen kann theoretisch und praktisch die Email manipulieren.

Das Public-/Private-Key-Verfahren

Das Public-/Private-Key-Verfahren adressiert beide oben genannten Probleme. Es funktioniert so: Wer verschlüsselte Emails senden und empfangen will, generiert sich auf dem heimischen Rechner ein Schlüsselpaar, also zwei Schlüssel, die zueinander gehören. Der öffentliche Schlüssel ist völlig unbedenklich und kann an alle, mit denen mensch in verschlüsselte Kommunikation treten will, verschickt werden. Der private Schlüssel ist wie der Name schon sagt privat und sollte nicht in falsche Hände gelangen. Daher ist dieser Schlüssel zusätzlich mit einer Passphrase geschützt. Der private Schlüssel befindet sich also selbst in nochmals verschlüsselter Form auf der eigenen Festplatte und kann nur durch Eingabe der Passphrase entschlüsselt werden.
Die folgenden zwei Graphiken veranschaulichen das Prinzip:



Bob verschickt seinen öffentlichen Schlüssel an Alice. Eve (von englisch „Eavesdropper“ – Lauscher_in) kann den öffentlichen Schlüssel problemlos abfangen, das ist aber nicht schlimm.



Alice benutzt Bob‘s öffentlichen Schlüssel um eine Nachricht an Bob zu verschlüsseln. Da nur Bob in Besitz des passenden privaten Schlüssels ist, kann Eve die Nachricht zwar abfangen, aber nicht entschlüsseln.

Verschlüsselte Emails senden und empfangen

Will ich nun eine Email verschlüsseln, so benötige ich den öffentlichen Schlüssel meiner Kommunikationspartner_in. Mit diesem Schlüssel verschlüssele ich meine Nachricht; das Ergebnis ist ein unleserlicher Zahlen- und Buchstabensalat. Die Empfängerin kann nun mittels ihres privaten Schlüssels, den sie erst durch Eingabe der Passphrase entschlüsseln muss, die Email aufmachen.
Erhalte ich dagegen eine verschlüsselte Mail, so muss ich mit Hilfe meiner Passphrase meinen privaten Schlüssel entschlüsseln und damit wiederum die Email entschlüsseln. Die entschlüsselte Mail erscheint dann wieder im Klartext. Mit diesem Verfahren ist also der Inhalt der Mail auf seiner Reise durchs Netz geschützt. Heutige Email-Programme unterstützen dieses Verfahren, so dass sich der Vorgang des Ver- und Entschlüsselns nutzerseitig auf wenige Mausklicks beziehungsweise die Eingabe der Passphrase beschränkt.

Emails signieren

Um die Authenzität der Email zu gewährleisten, wird im Prinzip das selbe Verfahren verwendet, nur andersherum. Bevor die Email verschickt wird, generiert das Emailprogramm aus dem Inhalt der Email und meinem privaten Schlüssel eine Prüfsumme, die beim Senden mit übermittelt wird. Das Emailprogramm der Empfängerin kann eine mathematische Beziehung zwischen dem Text der Mail, der Prüfsumme und meinem öffentlichem Schlüssel überprüfen. Stimmt diese Beziehung, so ist klar, dass die Prüfsumme nur mit Hilfe meines privaten Schlüssels und nur aus dem vorliegenden Text generiert worden sein kann. Damit kann die Empfängerin feststellen, dass erstens die Email von mir kommt (da nur ich im Besitz meines privaten Schlüssels nebst zugehöriger Passphrase bin) und zweitens, dass am Inhalt der Mail nichts manipuliert wurde.

Schritt 1: Programme installieren

a) Unter Linux
Im Paketmanager der jeweiligen Distribution (für Ubuntu und Debian wird meist Synaptic verwendet) einfach die Pakete *thunderbird*, *gnupg* und *enigmail* installieren. Auf Debian-basierten Distributionen reicht der Befehl:

$ apt-get install thunderbird gnupg enigmail
[als Root-User ausführen.]

b) Unter Windows
Unter Windows müssen die Programme einzeln heruntergeladen werden:

- *Thunderbird* findet sich unter http://www.mozilla.com. Dann auf Thunderbird klicken und das Paket in der gewünschten Sprache herunterladen. Ein Doppelklick auf Thunderbird_Setup.exe installiert das Programm

- *GnuPG* findet sich unter ftp://ftp.gnupg.org/gcrypt/binary/. Die momentan aktuellste Version ist 1.4.8, also die Datei: gnupg-w32cli-1.4.8.exe. Ein Doppelklick installiert das Programm.

- Das *Enigmail*-Plugin muss unter https://addons.mozilla.org/de/thunderbird/addon/71 heruntergeladen werden. Die heruntergeladene xpi-Datei muss im Thunderbird unter *Extras -> Addons -> Installieren (dort die heruntergeladene xpi-Datei auswählen)* installiert werden. Dann den *Thunderbird* neu starten.
  Dass die Programme korrekt installiert sind erkennt mensch unter anderem daran, dass das *Thunderbird*-Menü nun um den Eintrag „*OpenPGP*“ erweitert wurde.

c) Unter MacOS
Unter MacOS wird analog zur Installationsbeschreibung für Windows verfahren. Die *GnuPG*-Pakete für Mac finden sich unter: http://macgpg.sourceforge.net/.

Schritt 2: Email-Konto unter Thunderbird einrichten.

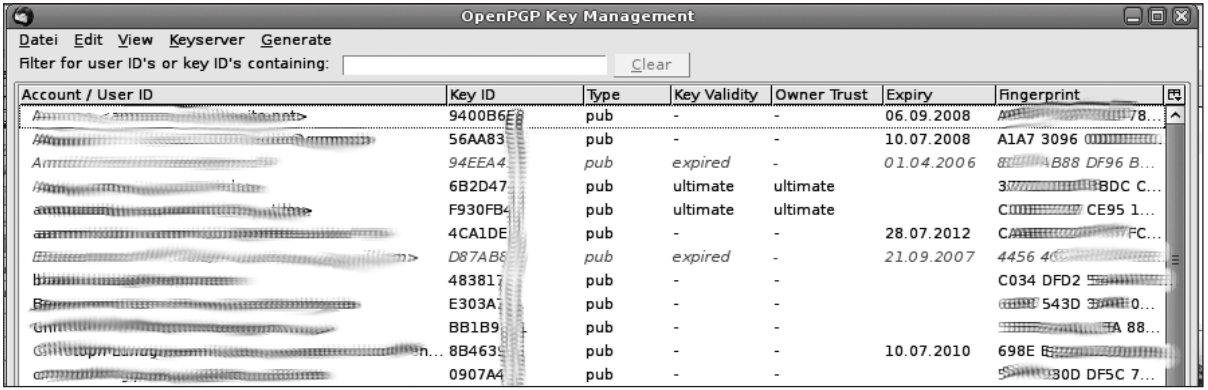
Dieser Schritt kann an dieser Stelle nicht ausführlich behandelt werden. Bei den meisten Email-Providern wie beispielsweise *GMX, google, yahoo* usw. findet sich eine Anleitung, wie die am weitesten verbreiteten Email-Programme zu konfigurieren sind. Folgende Angaben werden benötigt:

• Die Email-Adresse. • Adresse des Mail-Eingangsservers. • Login und Passwort für den Mail-Eingangsserver.
• Adresse des Postausgangsservers. • Das vom Posteingangsserver verwendete Protokoll (in der Regel POP3).
• Login und Passwort für den Postausgangsserver.

Mit einer kurzen Email an sich selbst kann getestet werden, ob alles richtig eingestellt ist.

Schritt 3: Ein Schlüsselpaar generieren

Im *Thunderbird* im Menü *OpenPGP* und dort „key management“ aufrufen.



Im Thunderbird Key-Manager werden alle vorhandenen Schlüssel übersichtlich verwaltet.

Anmerkungen zum Key-Manager:

Im Key-Manager werden alle Schlüssel, die sich im Laufe der Zeit ansammeln, übersichtlich gespeichert. Dort lassen sich Key-ID, Fingerprint, Geltungsdauer etc. ablesen. Auch die eigenen privaten Schlüssel können hier eingesehen werden.

public key fingerprint

Der fingerprint eines öffentlichen PGP-Schlüssels besteht aus 10 Blöcken zu je 4 Zeichen. Der Fingerprint wird mittels eines mathematischen Algorithmus (Hash) aus dem öffentlichen Schlüssel generiert. Um die Sicherheit zu erhöhen ist es möglich, nach Erhalt eines öffentlichen Schlüssels die entsprechende Kommunikationspartner_in beispielsweise telefonisch zu kontaktieren und den fingerprint mündlich abzugleichen. So ist sichergestellt, dass wirklich mit dem richtigen public key verschlüsselt wird und nicht eine unberechtigte dritte Person einen gefälschten public key eingeschmuggelt hat.
Beispiel für einen public key fingerprint:
2914 0768 68E5 BC65 80E5 7D4C 60FA 1AA7 7023 405A
In der Praxis wird allerdings meist auf diesen Abgleich verzichtet.

key-ID

Die Key-ID sind die letzten acht Ziffern des fingerprints. Aus praktischen Gründen wird in einigen Fällen lediglich die ID eingesetzt, allerdings ist sie wegen ihrer Kürze nicht dazu in der Lage, einen Schlüssel zweifelsfrei zu identifizieren.

Anmerkungen zur Passwortsicherheit!

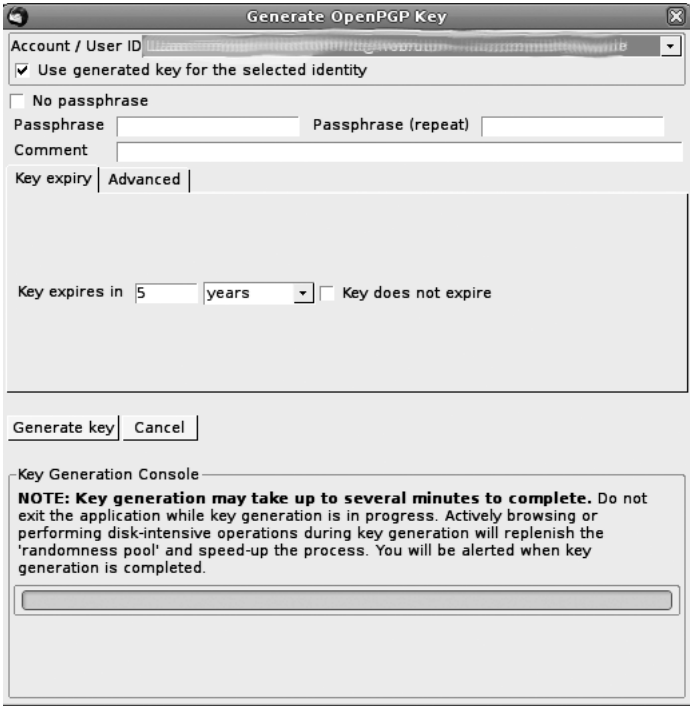
Hier gehen die Meinungen etwas auseinander, wie lang ein Passwort sein sollte, um wirklich sicher zu sein. Klar ist allerdings, dass es Groß- und Kleinschreibung sowie Zahlen und Sonderzeichen enthalten sollte. Nicht enthalten sein sollten ganze Wörter oder Sätze. Als Eselsbrücke empfiehlt es sich, sich einen Satz zu merken und die jeweiligen Anfangsbuchstaben als Passwort zu verwenden.
Ein Beispiel: *Wegen des „Linksrucks" in der SPD-Führung verlor die Partei 43% bei den Landtagswahlen.*
Ergibt als Passwort: Wd"L"idSPD-FvdP43%bdL.
Dieses Passwort kann als sehr sicher gelten (jetzt natürlich nicht mehr, weil es veröffentlicht wurde). Es hat 22 Zeichen, für unsere Zwecke hier sollte allerdings ein Passwort von mindestens 15 Zeichen Länge völlig ausreichen.

Schlüssel Generieren

Im Key-Manager im Menüpunkt „Generate“ die Option „new pair“ auswählen (siehe nebenstehende Abbildung). Dort unter „Account / User-ID“ die Emailadresse auswählen, für die ein neuer Schlüssel generiert werden soll. Dann unter „Passphrase“ das ausgewählte Passwort eingeben (siehe unbedingt den Punkt Passwortsicherheit) und zur Sicherheit nochmals wiederholen. Das Feld „Comment“ kann leer bleiben oder irgendeine Beschreibung des Schlüssels enthalten. Dieser Comment wird unverschlüsselt mit übertragen, deswegen sollte hier keinesfalls etwas stehen, dass Rückschlüsse auf die verwendete Passphrase zulässt. Im Feld „Key expires“ kann angegeben werden, wie lange der Schlüssel gültig sein soll. „Key does not expire“ ist eine gute Wahl. Ein Klick auf „Generate Key“ startet die Schlüsselerzeugung. Während der Generierungsprozess läuft kann mensch ein paar Anwendungen starten oder andere Aktivitäten ausführen. Dies erhöht die Entropie im Computersystem und führt damit zu Zufallszahlen von höherer Qualität.

.. und widerrufen

Nach der Schlüsselgenerierung kommt die Aufforderung ein „revocation certificate“ zu erstellen. Dieses kann verwendet werden, um den Schlüssel zurückzurufen, beispielsweise wenn er kompromittiert wurde oder ein neuer Schlüssel verwendet werden soll. In diesem Falle sendet mensch das Revocation-Certificate an die Kommunikationspartner_innen und erklärt damit den Schlüssel für ungültig. Es empfiehlt sich also, ein solches Zertifikat zu erstellen und (beispielsweise gemeinsam mit Sicherheitskopien des öffentlichen und des privaten Schlüssels, siehe unten) irgendwo sicher aufzubewahren. Bei Erstellen des Zertifikats muss die Passphrase erstmals verwendet werden. Herzlichen Glückwunsch, das Schlüsselpaar ist erstellt.



Mit dem ‚Generate Key' Dialog kann mensch einfach und schnell ein neues Schlüsselpaar generieren.

Schritt 4: Sicherheitskopien erstellen

Vorweg eine Warnung: Sollte der private Schlüssel verloren gehen oder aber die eigene Passphrase vergessen werden, so gibt es keine Möglichkeit, die so verschlüsselten Emails jemals wieder zu lesen. Deswegen muss mensch sich die Passphrase genau einprägen.
Im Falle eines Festplattencrashs oder ähnlichem wären die privaten Schlüssel verloren, daher sollten alle Schlüssel sowie das Revocation-Certificate auf einem externen Medium (beispielsweise USB-Stick) gesichert werden.
Unter Linux finden sich die entsprechenden Dateien (und auch alle importierten öffentlichen Schlüssel anderer Leute) im Verzeichnis /home/<USERNAME>/.gnupg. Einfach das gesamte Verzeichnis sichern.
Unter Windows finden sich die Dateien unter:
C:\Dokumente und Einstellungen\<USERNAME>\Anwendungsdaten\gnupg
Dabei sollte <USERNAME> durch den eigenen Benutzernamen ersetzt werden.

Schritt 5: Emails verschlüsseln und signieren

Um eine Email verschlüsseln zu können, wird der öffentliche Schlüssel der Kommunikationspartner_in benötigt. Diesen kann mensch sich einfach zuschicken lassen und dann importieren. Das funktioniert mit einem Rechtsklick auf die der Email angehängte asc-Datei und Klick auf „importieren“.
Um eine verschlüsselte Nachricht zu verschicken im *Thunderbird* einfach auf „Verfassen“ klicken. Die gewünschte Emailadresse eingeben und im Menü unter „OpenPGP“ die beiden Punkte „sign email“ und „encrypt email“ auswählen. Dass die Mail wie gewünscht verschlüsselt und signiert wird, erkennt mensch an den beiden kleinen grünen Symbolen unten rechts (ein Bleistift für die Signatur und ein Schlüssel für die Verschlüsselung). Dann wie gewohnt die Email schreiben. Dabei ist zu bedenken, dass die Betreffszeile nicht mitverschlüsselt wird, hier sollen also keine sensiblen Daten eingegeben werden. Beim Verschicken der Email wird mensch aufgefordert, die Passphrase einzugeben. Wie oben beschrieben ist dies nötig, um den eigenen privaten Schlüssel zu öffnen, mit dem die Mail signiert werden soll. Angenommen mensch wollte die Mail nur verschlüsseln, aber nicht signieren, so wäre die Eingabe der Passphrase nicht nötig. Ein Klick auf „Senden“ startet den Verschlüsselungsvorgang und versendet die Mail.

Schritt 6: Verschlüsselte und signierte Emails empfangen.

Erhält mensch eine verschlüsselte Email, so wird die Eingabe der Passphrase gefordert. Nach Eingabe erscheint die entschlüsselte Mail. Wiederum kann mensch an den beiden grünen Symbolen am unteren Rand des Fensters erkennen, dass sowohl Verschlüsselungs- wie Signaturvorgang erfolgreich waren. Sollte das Bleistift-Symbol rot bleiben so kann dies bedeutet, dass der öffentliche Schlüssel der Kommunikationspartner_in noch nicht importiert wurde.

Passphrase merken:

Falls mensch nicht jedesmal die Passphrase eingeben will, kann im *Thunderbird*-Menü unter „OpenPGP“ -> „Preferences“ eingestellt werden, dass die Passphrase für längere Zeit im System erhalten bleibt.

Voila.

ACKW
Allgemeiner Computer Konfrontations Workshop
http://computergruppe.h48.de

Anonym durchs Internet mit TOR (The Onion Router) und Privoxy

Problemstellung

Im Internet verrät mensch beim Aufruf einer jeden Webseite seine Internet-Protocol-Adresse. Diese Adresse (im folgenden kurz IP genannt) ist eine eindeutige Identifikationsnummer. Jede_r Internetnutzer_in bekommt sie von ihrem oder seinem Internetprovider zugeteilt. Dadurch wissen Server, an welchen Rechner sie ihre Daten schicken sollen und von wem die Anfrage dazu kam. Die IP ist also unersetzlich, um im Internet unterwegs zu sein.

Diese Daten können sehr leicht von der jeweiligen Internetseite und von allen Servern, durch welche die Anfrage gelaufen ist, gespeichert werden. Darüber hinaus sind die Internetprovider seit Januar 2008 verpflichtet, sechs Monate lang zu speichern, welche Nutzer_in zu welcher Zeit welche IP-Adresse hatte.

Eine mögliche Lösung: TOR

Hier soll vorgestellt werden, wie es mit relativ wenig Aufwand möglich ist, Internetseiten zu besuchen, ohne dabei die eigene Identität preiszugeben.

Eine mögliche Lösung für anonymes Surfen ist die Benutzung des TOR-Netzwerkes. TOR ist eines der bekanntesten Anonymisierungsprogramme. Es hat den großen Vorteil, dass es kostenlos ist und zugleich eine sehr gute (wenn auch keine 100 prozentige – siehe unten) Anonymisierung gewährleistet. Zu den Nachteilen gehört, dass es die Surfgeschwindigkeit z.T. erheblich verlangsamt.

Wie funktioniert TOR?

TOR schickt die Datenpakete verschlüsselt über drei zufällig ausgewählte Server (so genannte TOR-Knoten), bis der letzte Server, die so genannte „Exit-Node“, sie (unverschlüsselt!) zum eigentlichen Webserver (z.B. zu der gewünschten Seite) schickt. Das Datenpaket ist anfangs dreifach verschlüsselt. Jeder der Server entschlüsselt eine „Schicht“, die lediglich die Information enthält, wohin er den Rest, dessen Inhalt vor ihm verborgen bleibt, weiterschicken soll. Dadurch ist es möglich, dass keiner der beteiligten Server den gesamten Weg des Datenverkehrs kennt, sondern nur den jeweils vorherigen und den nachfolgenden Punkt des Daten-Weges.

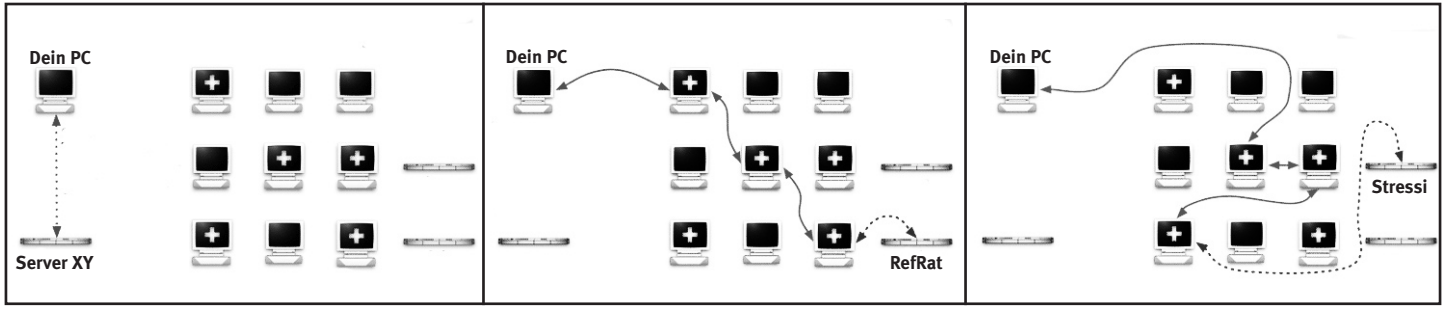
Das bedeutet, dass bereits der zweite TOR-Server nicht die Identität der Nutzer_in kennt. Es bedeutet auch, dass die Anonymisierung bereits funktioniert, wenn einer der beteiligten Server vertrauenswürdig ist.

Da die Daten bereits verschlüsselt zum ersten TOR-Server geschickt werden, weiß auch der Internet-Anbieter nicht auf welche Seite zugegriffen wird und was für Daten ausgetauscht werden. Der Anbieter weiß lediglich, dass

eine Verbindung mit dem TOR-Netzwerk aufgebaut wird.

Eine Website, die auf diese Weise aufgerufen wird, kann also die IP-Adresse der Nutzer_in nicht sehen, sondern nur die der „Exit-Node“, welche irgendwo auf der Welt stehen kann. Spätestens alle zehn Minuten wird ein neuer Weg über drei zufällig ausgewählte Server aufgebaut. Es befinden sich auf der ganzen Welt mehrere tausend TOR-Server und jede_r Nutzer_in kann mit zwei Mausklicks einen eigenen Server auf seinem oder ihrem Rechner eröffnen und somit das Netzwerk unterstützen. Dies macht es nahezu unmöglich, das gesamte Netzwerk zu überwachen.

Wie TOR funktioniert, sollen die folgenden drei Graphiken verdeutlichen:



1:Das TOR-Programm auf deinem Rechner holt sich eine Liste mit TOR-Knoten von Server XY, einem so genannten Verzeichnisserver. Die mit einem + versehenen Server stellen TOR-Knoten dar.

2: Das TOR-Programm auf deinem Rechner wählt einen zufälligen Pfad über drei Knoten zum Zielserver (z.B. www.refrat.de). Durchgezogene Verbindungen sind verschlüsselt; Gestrichelte unverschlüsselt.

3: Wenn du auf eine andere Seite zugreifen möchtest (z.B. stressfaktor.squat.net), wählt dein TOR-Client einen zweiten zufälligen Pfad. Wiederum gilt: durchgezogen = verschlüsselt; gestrichelt = unverschlüsselt

Die beteiligten Programme

TOR und Privoxy

Auf den folgenden Seiten wird dargestellt wie die TOR-Software und zusätzlich *Privoxy* installiert werden.

Privoxy ist ein so genannter Proxy-Server. Durch diesen geht die Kommunikation mit dem Internet und er filtert dabei Daten heraus, die normalerweise mit übertragen würden und die die eigene Identität preisgeben könnten. Darüber hinaus filtert *Privoxy* u.a. Werbung und Pop-ups aus Internetseiten.

Warum Privoxy?

Was den Einsatz von *Privoxy* außerdem notwendig macht, ist, dass Webbrowser keine Internet-Adressen verarbeiten, sondern nur IP-Adressen. Nach der Eingabe einer Internetadresse (z.B. www.refrat.de) schlägt er also auf einem Namen-Server im Internet nach, zu welcher IP-Adresse (z.B. 216.321.2.33) dieser Name gehört, bevor er über das TOR-Netzwerk die Seite aufruft. Damit wäre die Anonymität dahin. Privoxy schickt diese Abfrage bereits durch das TOR-Netzwerk

Vidalia

In den Installationspaketen für Windows und Mac ist zusätzlich *Vidalia* enthalten, ein Programm zum einfachen Bedienen von TOR. Es bietet eine graphische Oberfläche mit der mensch TOR an- und ausschalten kann. Eine Weltkarte zeigt, wo sich die aktuell benutzen Server befinden. Auch der Pfad durch das TOR-Netzwerk lässt sich mit *Vidalia* ändern. Letzteres kann sehr nützlich sein, wenn mensch eine besonders langsame Verbindung erwischt hat.

Firefox

Es wird unter anderem vom TOR-Projekt selbst empfohlen *Firefox* als Webbrowser zu benutzen. Neben einigen Funktionen, die das Benutzen von TOR bequemer machen gibt es weniger Sicherheitslücken und mehr Einstellungensmöglichkeiten für Privatsphäre als etwa beim Internet Explorer von *Microsoft*.
Firefox ist kostenlos und kann unter dieser Adresse für Winows, Mac und Linux heruntergeladen werden:
http://www.mozilla-europe.org/de/

Schritt 1: TOR herunterladen und installieren

Die jeweils aktuelle Version für alle gängigen Betriebssysteme findet sich auf der Download-Seite des TOR-Projektes.
http://www.torproject.org/download.html.de

a) Windows und Mac
Für Windows und Mac gibt es Pakete bestehend aus TOR, *Privoxy* und *Vidalia* (inkl. *torbutton* für *Firefox* – siehe unten). Einfach die Datei herunterladen und doppelklicken, um die Installation zu starten. Wir wollen alle drei Programme.

b) Linux
Wer ein aktuelles Debian oder Ubuntu installiert hat, dem genügt ein einfaches 'apt-get install TOR privoxy' im Terminal bzw. ein Klick auf TOR und auf *privoxy* in den Paketquellen (beide in den ‚universe'-Quellen zu finden).

Schritt 2: Konfiguration

a) Windows:
Die drei Programme kommen schon aufeinander abgestimmt und werden nach der Installation automatisch gestartet. Rechts unten (neben der Uhr) erscheinen nun zwei Symbole: ein Kreis mit „P" darin für *Privoxy* und eine Zwiebel für *Vidalia*. Grüne Zwiebel heißt: TOR läuft, rot durchgestrichene Zwiegel meint: TOR läuft nicht. Zum Starten oder Stoppen von TOR: Auf die Zwiebel klicken und ‚start' bzw. ‚stop' wählen.

b) Mac:
Die drei Programme kommen schon aufeinander abgestimmt. *Pivoxy* startet automatisch beim nächsten Hochfahren des Computers. *Vidalia* starten: Anwendungen --> *Vidalia*
Jetzt erscheint ein Zwiebelsymbol im Dock; grün: TOR läuft; rot durchgestrichen: TOR läuft nicht.
TOR wird gestartet, indem am oberen Bilschirmrand ‚Start' im Menü ‚TOR' ausgewählt wird.

c) Linux:
TOR kommt normalerweise schon korrekt konfiguriert. Wir kümmern uns also um Privoxy. Hier müssen drei kleine, einfache Änderungen in der Datei Namens *config* vorgenommen werden. Diese ist in der Regel in */etc/privoxy* zu finden (nach der Installation natürlich) und muss mit einem Schreibprogramm mit root-Rechten geöffnet werden.

Ganz oben an den Anfang der Config-Datei fügen wir diese Zeile ein:

forward-socks4a / localhost:9050 .

Der Punkt "." am Ende der Zeile ist wichtig!
Da Privoxy standardmäßig recht viel loggt (d.h. dokumentiert, was es so tut) und wir das nicht möchten, kommentieren wir folgende zwei Zeilen aus, d.h. wir versehen diese Zeilen mit einer Raute (#) am Anfang, was bewirkt, dass sie vom Programm ignoriert werden:

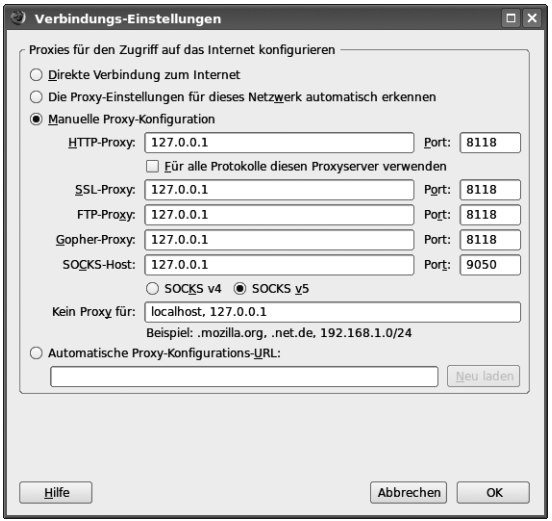
logfile logfile (daraus wird: # logfile logfile)
jarfile jarfile (daraus wird: # jarfile jarfile)

Diese Zeilen sind relativ weit unten, also am besten mit der Suchfunktion finden.
Datei speichern!
Anschliessend wird Privoxy neu gestartet, um die Änderungen zu übernehmen: Dazu geben wir

/etc/init.d/privoxy restart

in einem Terminal ein.

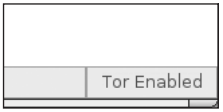
Zu Schritt 3c auf Seite 17: Netzwerkeinstellungen am Beispiel Firefox



Schritt 3: Anwendungen zur Benutzung von TOR konfigurieren (mit torbutton oder von Hand)

Jetzt müssen wir nur noch dem Webbrowser (und evtl. anderen Anwendungen) mitteilen, dass er alle Anfragen ans TOR-Netzwerk schicken soll und nicht direkt zu den Seiten. Empfohlen wird die Benutzung von *Firefox* mit dem Plug-In *torbutton*. Es nimmt die notwendigen Einstellungen in *Firefox* automatisch vor und ermöglicht das an- und ausschalten von TOR per Mausklick (auch auf Grund der verringerten Surfgeschwindigkeit nicht zu verachten)

Wenn *torbutton* installiert wurde, erscheint in *Firefox*, nachdem es neu gestartet wurde, rechts unten entweder „Tor Enabled“ in grün oder „Tor Disabled“ in rot. Per Mausklick kann hin- und hergeschaltet werden.



das isser: der torbutton

a) Win/Mac mit Firefox
Bei der Installation von *Vidalia* (im Paket von Schritt 1 enthalten) wird das Plug-In *torbutton* für *Firefox* mitinstalliert, falls *Firefox* verwendet wird. Direkt herunterladbar hier: *https://addons.mozilla.org/firefox/2275/*

b) Linux mit Firefox:
Das Plugin torbutton kann separat heruntergeladen werden: Einfach auf: *https://addons.mozilla.org/firefox/2275/* und dort auf ‚torbutton installieren‘ klicken.

c) Linux/Mac/Windows:
Alternativ kann (wenn kein Firefox und *torbutton*: muss) mensch dem Browser die Einstellungen per Hand mitteilen: In *Firefox* (bei anderen Browsern ist es ähnlich – einfach die Netzwerkeinstellungen suchen..) erreicht mensch die Proxy-Einstellungen so: *Bearbeiten -> Einstellungen -> Erweitert -> Netzwerk -> Verbindung -> Einstellungen*

Diese ändern wir wiefolgt (siehe Abbildung links):
Wir wählen: Manuelle Proxy-Konfiguration und geben als HTTP-Proxy *localhost* oder *127.0.0.1* ein
(das ist das selbe – einmal in Menschen-, einmal in Computersprache) und als Port *8118* ein.
Ebenso für SSL-, FTP- und Gopher-Proxy (die nächsten drei Zeilen).
In der letzten Zeile (SOCKS-Host) geben wir auch *localhost* bzw. *127.0.0.1* ein, aber als Port: *9050*.

Alternativer noch einfacherer Schritt (nur Windows):

Wer einfach nur unter Wahrung seiner Privatssphäre im Internet surfen möchte, dem steht für Windows *TorPark* als one-click-to-surf-Lösung zur Verfügung. Mensch erhält einen schon voreingestellten Browser inklusive aller nötigen Programme. Auch für Unterwegs auf USB-Stick verwendbar.
Herunterladbar unter anderem hier:
http://www.foebud.org/datenschutz-buergerrechte/vorratsdatenspeicherung/torpark-privacydongle-2-0.zip/view

Schritt 4: Funktion überprüfen

Am Ende prüfen wir noch die Funktion des Ganzen (Sind wir tatsächlich über TOR unterwegs?):
Beispielsweise *http://www.ip.cc* zeigt die IP-Adresse an, mit der gesurft wird. Diese kann mensch mit der eigenen IP-Adresse vergleichen. Die eigene IP wird folgendermaßen ermittelt:
Mac OS X, Linux, BSD, etc: *ifconfig* in einem Terminal eingeben.
Windows: Terminal öffnen (Startmenü --> Ausführen. Dort *cmd* eingeben). Im Terminal: *ipconfig /a* eingeben.
Wenn die IP-Adressen nicht übereinstimmen: rock 'n roll!

Schritt 5: Andere Anwendungen

Auch andere Anwendungen können über TOR umgeleitet werden. Dazu müssen sie gemäß den obigen Servereinstellungen an Tor verwiesen werden. Für das Emailprogramm *Thunderbird* gibt es ebenfalls den *torbutton*, der die Servereinstellungen übernimmt.

Für Emails ist die Benutzung von TOR aber nur bedingt sinnvoll. Anonymität ist nur gewährleistet, wenn TOR konsequent und bereits bei der Einrichtung der Adresse genutzt wird. Bereits **ein** Zugriff auf die Mails vom heimischen Internet ohne TOR genügt und die Emailadresse ist der eigenen Identität zuordenbar. Von da an kann mensch sich die zukünftige Verwendung von TOR beim Abrufen dieser Emailadresse schenken.

Wichtiges zum Schluss

TOR kann nicht alle Anonymitätsprobleme lösen. Es verschleiert lediglich die Kommunikationswege und das auch nur bei richtiger Handhabung (das Verwenden von Privoxy ist schonmal ein wichtiger Schritt)

Javascript, Flash, Cookies und andere Fehler

Das nützt natürlich alles nichts, wenn mensch mit TOR und allem pipapo auf der nächstbesten Seite seinen oder ihren Namen und Adresse in ein Formular einträgt.

Einige Dinge, die das Surfen, bunter und bewegter machen, wie **javascript und flash**, sollten zur Wahrung der Privatsphäre **deaktiviert** werden, da sie Daten übermitteln, die auf die Identität zurückschließen lassen (bei *Firefox*: *Bearbeiten --> Einstellungen --> Inhalt und Datenschutz*). Ebenso sollte mit cookies (das sind kleine Textdateien, die Webseiten auf Rechnern speichern, zum Beispiel um sie wieder zu erkennen) verfahren werden.

Dies geht natürlich nicht immer. Manche Seiten, die mensch benutzen möchte, verlangen cookies. Hier muss also individuell entschieden werden, wann mensch wie anonym sein möchte.

Browser bieten diesbezüglich diverse Einstellungsmöglichkeiten. Mensch kann zum Beispiel cookies nur von bestimmten Seiten zulassen oder alle privaten Daten bei Beenden des Browsers automatisch löschen lassen.

Manche Menschen verwenden auch zwei Browser: einen zum anonymen Surfen, einen anderen zum schnellen, unsicheren Surfen.

TOR verschlüsselt nicht

TOR verschleiert nur die IP-Adresse, es verschlüsselt nicht die komplette Kommunikation. Unverschlüsselte Daten können immer von Anderen eingesehen werden. Insbesondere auch von Betreibern von Exit-Nodes. Um Verschlüsselung muss sich also bei Bedarf zusätzlich gekümmert werden (z.B. durch die Verwendung von GnuPG für Emails und SSL-Verschlüsselung im Internet –> erkennbar am ‚s' in https://...). Das gilt besonders für Daten, die Auskunft über die eigene Identität geben.

TOR ist nicht 100 Prozent sicher

TOR kann, wie alle gängigen Anonymisierungsdienste keine 100 prozentige Anonymität bieten, selbst wenn es bestmöglich genutzt wird. Mit erheblichem Aufwand ist es beispielsweise möglich den Zugriff auf eine bestimmte Website nachzuweisen. Wenn der betreffende PC und die betreffende Website überwacht werden, kann statistisch analysiert werden wann und wo Datenpakete geflossen sind und darüber können Rückschlüsse auf die Identität gezogen werden. Ein solcher Aufwand dürfte jedoch nur in seltenen Fällen betrieben werden.

Fingerabdrücke nachmachen
Mit PC, Sekundenkleber und Holzleim

Wozu eine Fingerabdruckattrappe?

Diese Anleitung stammt vom Chaos Computer Club (CCC). Mit Hilfe dieser Methode gelang es einer Person vom CCC vor laufender Kamera innerhalb kurzer Zeit sich in einen Computer einzuloggen, der mit einem Fingerabdruckscanner gesichert war. Vermutlich wird diese Anleitung für die wenigsten Leser_innen praktischen Nutzen haben. Es soll hier lediglich verdeutlicht werden, wie einfach angeblich sichere Systeme überlistet werden können.

1: Fingerabdruck finden

Um eine Attrappe eines Fingerabdrucks herzustellen braucht mensch zu erst einmal einen passenden Fingerabdruck. Abdrücke enstehen durch das Anhaften von Fett und Schweiß der Haut an den berührten Gegenständen. Besonders gut erhaltene Fingerbilder findet mensch an Gläsern, Türklinken und Hochglanzpapier.

Bild 1: Sichbarmachen mit Graphitpulver

Bild 2: Sichtbarmachen mit Sekundenkleber

2: Fingerabdruck sichtbar machen

Um Fingerabdrücke für die weitere Verarbeitung sichtbar zu machen bedient mensch sich der Verfahren aus der Kriminalistik. Farbiges Pulver wird mit einem weichen Pinsel vorsichtig über den Abdruck verteilt und bleibt am Fett haften. (Bild 1)
Eine andere Möglichkeit bietet der Einsatz von Cyanoacrylat, einem Hauptbestandteil von Sekundenkleber. Von diesem bringt mensch eine kleine Menge in einen Flaschenverschluß und stülpt diesen über den Abdruck. (Bild 2)
Das ausgasende Cyanoacrylat reagiert mit den Fettrückständen des Fingerabdrucks zu einer festen weißen Substanz (Bild 3).

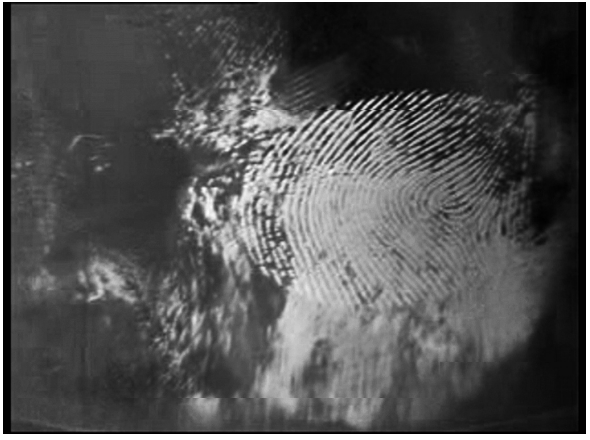


Bild 3: Cyanoacrylat (von Sekundenkleber) im Einsatz

Bild 4: Digitalisierung des Abdrucks

3: Fingerabdruck digitalisieren

Die durch Sekundenkleber oder mittels aufgepinselter Pigmente sichtbar gemachten Abdrücke werden mit einer Kamera oder einem Scanner digitalisiert. (Bild 4)
Im Anschluss werden die Bilder des Abdrucks mit Hilfe eines Graphikprogramms nachbearbeitet. (Bild 5)

4: Dreidimensionales Abbild erstellen

Zuerst braucht mensch ein genaues Abbild des Fingerabdrucks, um daraus eine Attrappe herstellen zu können. Die einfachste Variante ist, die Bilder mit einem Laserdrucker auf Folien zu drucken. Der Toner lagert sich dabei zu dreidimensionalen Strukturen ab.

Bild 5: Nachbearbeiten des Abdrucks

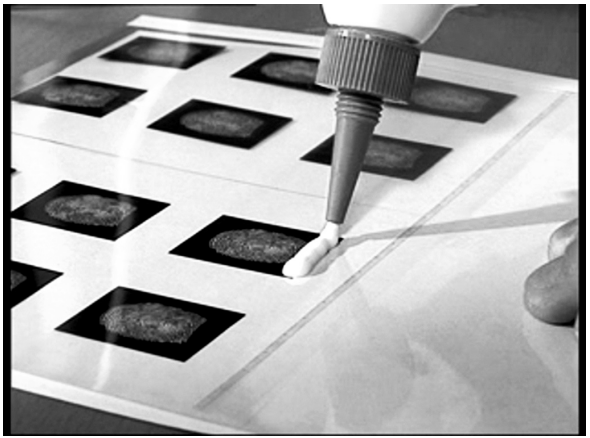


Bild 6: Holzleim für die Attrappen

5: Attrappe herstellen

Die Strukturen des Ausdrucks können als Abformgrundlage verwendet werden. Als Material für die Attrappe selbst eignet sich Holzleim besonders gut. (Bild 6)
Zur Erhöhung des Feuchtigkeitgehalts und zur besseren Verarbeitbarkeit kann mensch dem Leim eine kleine Menge Glycerin zusetzen. Gut durchmischt bringt mensch die Masse in einer dünnen Schicht auf die Form bzw. den Ausdruck. (Bilder 7 und 8). Getrocknet wird der Leim durchsichtig.

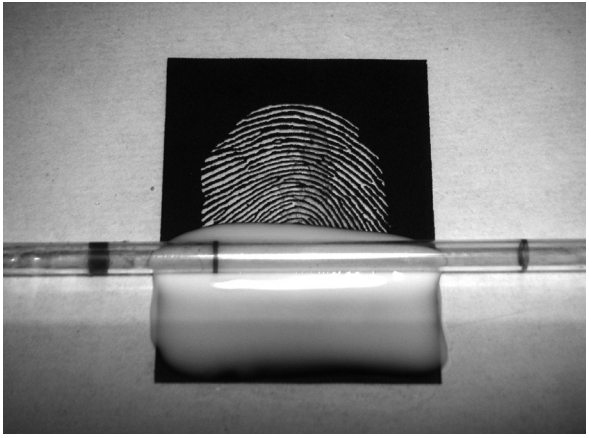


Bild 7: Aufbringen des Klebers

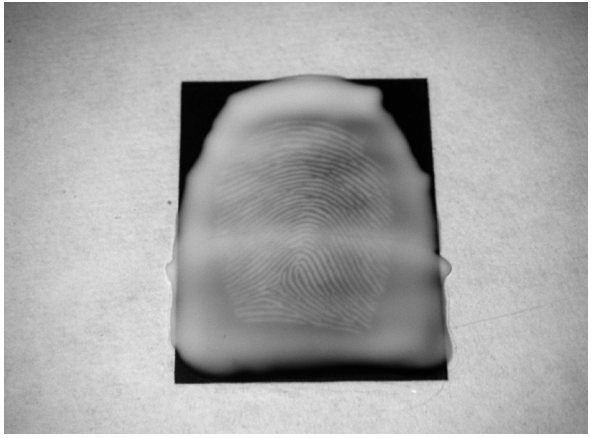


Bild 8: Kleberschicht auf Abdruck

Attrappe fertigstellen

Nach dem Trocknen zieht mensch die Kleberschicht von der Folie ab (Bild 9) und schneidet sie auf Fingergröße. Die Attrappe kann mensch sich nun mit Maskenkleber auf den eigenen Finger kleben (Bild 10)

Übrigens

Auf dem Titel dieser Beilage kann der Fingerabdruck von Innenminister Wolfgang Schäuble bewundert werden. Der CCC hatte ihn in der Ausgabe #92 ihrer Vereinszeitschrift ‚Datenschleuder' veröffentlicht. Er wurde laut CCC auf einem Wasserglas sichergestellt, das von Schäuble bei einem öffentlichen Auftritt benutzt worden war. Der Ausgabe lagen die Vorlage und eine fertige Attrappe bei. Der CCC hofft mit diesem Eingriff in Schäubles Privatsphäre die Diskussion um die Erfassung biometrischer Daten neu anzufachen.

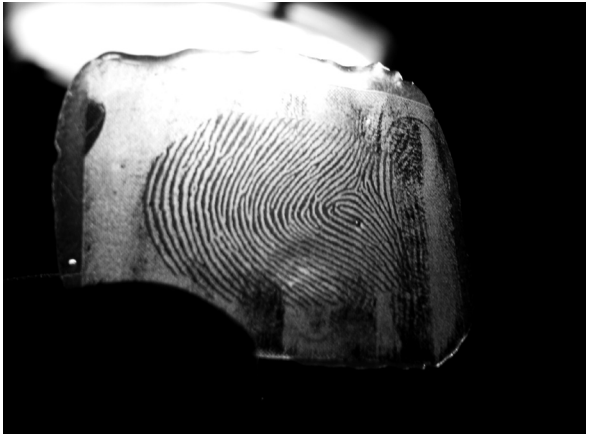


Bild 9: Fertige Attrappe

Bild 10: Die neue Identität ist fertig.

Dateien sicher löschen oder: was passiert beim Löschen?

Problemstellung

Werden Dateien von einem Rechner gelöscht, werden die entsprechenden Stellen auf der Festplatte (bzw. dem jeweiligen Speichermedium) mit einer Löschmarkierung versehen, also aus dem Inhaltsverzeichnis der Festplatte gestrichen. Die Dateien existieren aber noch bis dieser Platz mit neuen Dateien überschrieben wurde. Bis dahin können die Dateien mit speziellen Programmen wiederhergestellt werden.
Das ist schlecht, wenn mensch sensible und/oder persönliche Daten löschen möchte. Vielleicht weil mensch eine gebrauchte Festplatte verkaufen möchte oder weil die Staatsanwaltschaft ab und zu vorbeikommt.

Zu Beachten:

Neuere Dateisysteme (Arten die Festplatte zu verwalten), wie sie die meisten gängigen Betriebssysteme anlegen, machen 100 prozenitg sicheres Löschen quasi unmöglich, da Meta-Daten angelegt werden, die beim Löschen von Dateien nicht mitüberschrieben werden.
Um sicher zu gehen, dass sehr sensible Daten nicht mehr auffindbar sind, muss die gesamte Partition (bei Flashlaufwerken wie USB-Sticks: das gesamte Medium) mit einem geeigneten Programm mehrfach überschrieben werden.
Praktikabler ist es, die gesamte Festplatte bzw. das gesamte Speichermedium zu verschlüsseln.

Programme zum sicheren Löschen

Es gibt spezielle Programme, die Dateien löschen und deren Platz auf der Festplatte mehrfach mit Zufallsdaten überschreiben. Nach nur einmaligem Überschreiben ist es immer noch relativ einfach die Dateien zu rekonstruieren.

a) Windows
eraser: http://www.heidi.ie/eraser/download.php
Nach der Installation kann bei Rechtsklick auf eine Datei *erase* ausgewählt werden. In den Programm-Einstellungen können verschiedene Sicherheitsstufen gewählt werden, bis zum maximalen 35-fachen überschreiben.
Dort sollte mensch auch darauf achten, dass die Optionen *Cluster Tip Area*, *File Names* und *Alternate Data Streams* aktiviert sind, um alle Hinweise auf die gelöschten Dateien zu entfernen (Dateinamen z.B.).
Zur Vernichtung bisher gelöschter Daten, bietet *eraser* die Funktion den ‚freien' Festplattenspeicher zu löschen.

b) Mac
OS X: Datei in Papierkorb verschieben. Dann links oben auf ‚Finder' --> ‚Papierkorb sicher löschen'.
Überschreibt die Dateien mehrfach. (mehr nicht)

c) Linux
Wipe ist eine gute Option. Allerdings ohne graphische Oberfläche. In den Paketquellen zu finden. oder hier: http://sourceforge.net/project/showfiles.php?group_id=804

Festplatte Verschlüsseln
Mit (K)Ubuntu Alternate CD-Installation

Problemstellung

Sobald physischer Zugriff auf einen Computer möglich ist, nach Diebstahl etwa, können die darauf befindlichen Daten ausgelesen werden. Zugangspasswörter schützen in diesem Fall nicht.

Die sicherste Methode, sensible Daten vor unbefugtem Zugriff zu schützen, ist das gesamte System zu verschlüsseln. Damit wird auch das im Artikel zum sicheren Löschen angesprochene Problem der Metadaten in neueren Dateisystemen umgangen.

Die Alternate CD

Mit aktuellen Versionen von Ubuntu/Kubuntu/Xubuntu ist es sehr einfach bei der Installation das ganze System zu verschlüsseln. Es kann einfach als Option gewählt werden. Die Installation muss lediglich von der Alternate-CD durchgeführt werden. Die Desktop (Live-) CD mit graphischem Installationsprogramm kann das nicht.

Aktuelle Versionen können u.a. hier heruntergeladen werden (kostenlos natürlich):

http://wiki.ubuntuusers.de/Downloads

Es ist zwar auch möglich ohne Neuinstallation die Festplatte oder Teile davon zu verschlüsseln, doch dies ist vergleichsweise viel komplizierter.

Zwei einfache Szenarien

Im Nachfolgenden werden zwei Szenarien der Installation vorgestellt. Das einfachste ist **Linux als alleiniges Betriebssystem** zu installieren, die voreingestellten Partitionierungen zu übernehmen und dabei die gesamte Festplatte zu verschlüsseln. Etwas mehr Schritte erfordert es, **Linux und Windows nebeneinander** auf dem gleichen PC zu installieren und den Linuxteil der Festplatte zu verschlüsseln. Dabei muss die Partitionierung der Festplatte(n) manuell vorgenommen werden. Beide beschriebenen Möglichkeiten erfordern zumindest die Neuinstallation von Linux.

Die unten stehende Beschreibung basiert auf der Verwendung von KUBUNTU Linux Version 7.10 und MICROSOFT Windows XP, gilt aber ebenso für Ubuntu und Xubuntu. Eine kurze Internetrecherche hat ergeben, dass Versionen vor 7.10 die Festplattenverschlüsselung bei Installation nicht so reibungslos und einfach beherrschen.

Warnungen

Bei der Neuinstallation des Systems gehen die alten Daten verloren. Also vorher sichern, was wichtig ist.

Das Passwort für die Verschlüsselung darf auf keinen Fall vergessen werden (jedoch sollte es auch nicht auf einem Post-It am Bildschirm kleben). Ohne das Passwort befindet sich auf der Festplatte jede Menge Datenmüll.

Einfach: Linux alleine auf dem Computer, gesamte Festplatte verschlüsselt

Der PC muss mit der Alternate-CD im Laufwerk von CD booten. Die Installation erfolgt im „text mode“. In den ersten Stufen der Installation werden die Spracheinstellungen, das Tastaturlayout, die Hardware des PC‘s, das Netzwerk und der Name des Rechners bestimmt bzw. erkannt und eingerichtet. Die entsprechenden Eingaben werden Schritt für Schritt abgefragt.
Nach der Eingabe des Rechnernamens soll in der nächsten Abfrage die Partitionsmethode ausgewählt werden. Wer an dieser Stelle „Geführt - gesamte Platte mit verschlüsseltem LVM“ auswählt, braucht danach nur noch das Passwort für die Verschlüsselung eingeben (mehr als 20 Zeichen! – siehe Anmerkungen zu Passwortsicherheit S.7), ein paar mal „Ja“ auswählen und die restlichen Abfragen für die Systemzeit, username und Passwort etc. abarbeiten. Nach dem Neustart des PC‘s ist die gesamte Festplatte verschlüsselt und das Passwort für die Verschlüsselung muss bei jedem Start eingegeben werden.
Bei dieser Methode legt Linux nur drei Partitionen an: Boot, Root und Swap

Zu einfach? Dann: Verschlüsseltes Linux neben unverschlüsseltem Windows

Häufig brauchen oder wollen Menschen mehr Partitionen für Linux oder neben Linux auch noch Windows als zweites Betriebssystem. Diese Varianten sind ein wenig aufwendiger, da hierfür die Festplatte manuell partitioniert werden muss.
Hier wird der kompliziertere Fall behandelt: unverschlüsseltes Windows neben verschlüsseltem Linux. Ist Windows auf der Festplatte vorinstalliert, kann versucht werden ohne Neuinstallation von Windows mit der Linuxinstallation zu beginnen. Das Installationsprogramm von Linux sollte erkennen dass ein weiteres Betriebssystem installiert ist. Auf die Frage ob dieses weiterhin verwendet werden soll, „Ja“ auswählen. Eventuell ist es möglich die Festplatte zu partitionieren ohne dabei das vorinstallierte Windowssystem zu zerstören. Im Weiteren wird jedoch davon ausgegangen, dass Linux und Windows neu installiert werden sollen.

Es ist in jedem Fall empfehlenswert zuerst Windows und danach Linux zu installieren. Andersrum ist der Aufwand größer, da Windows alle bei der Installation nicht benutzten Partitionen automatisch inaktiviert und den MasterBootRecord überschreibt. Diese Schritte müssten im Nachhinein rückgängig gemacht werden.

Partitionierung bei der Windowsinstallation

1. Partition: ca. 250MB für boot loader. Als erste Partition sollte eine etwa 250 MB große Partition für den boot loader erstellt werden. Der boot loader wird (wenn alles fertig ist) als erstes nach dem Anschalten des Computers gestartet. Es erscheint ein Menu, in dem mensch auswählen kann ob Linux oder Windows gestartet werden soll. Diese Partition wird gebraucht, weil der boot loader nicht in der verschlüsselten Partition liegen kann.
2. Partition: Windows. Als zweites kommt die Windowspartition. Größe ist Geschmackssache (Windows XP braucht selbst etwa 2GB und unter Umständen möchte mensch noch Platz haben, um Dateien zu speichern).
3. Rest für Linux. Der restliche Speicherplatz kann für Linux freigelassen werden.

Partitionierung bei der Linuxinstallation

Nachdem Windows installiert wurde kann die Linuxinstallation wie oben beschrieben begonnen werden. Bei der Abfrage der gewünschten Partitionsmethode wird „Manuell“ ausgewählt. Das Installationsprogramm sollte erkennen dass ein weiteres Betriebssystem installiert ist. Auf die Frage ob dieses weiterhin verwendet werden soll, „Ja“ auswählen. Bei der folgenden „Übersicht der konfigurierten Partitionen und Einhängepunkte“ (im Weiteren „Partitionstabelle“ genannt) müssen einpaar Änderungen vorgenommen werden.
Hinweis: Die automatische Zuweisung der Nummern der Partitionen kann von den im folgenden Text benutzten Bezeichnungen abweichen.

1. Die zweite Partition auf welchem das Windowssystem installiert ist wird ausgewählt und wie folgt verändert:

Benutzen als:	FAT32-Dateisystem
Einhängepunkt (mount point):	/windows
Mount-Optionen:	defaults
Boot-Flag:	Aus

2. Wenn die Einstellungen entsprechend aussehen wird die Option „Anlegen der Partition beenden“ ausgewählt und die Partitionstabelle erscheint wieder. Nun wird die erste 250 MB große Partition ausgewählt und wie folgt verändert:

Benutzen als:	Ext2-Dateisystem
Partition formatieren:	ja, formatieren
Einhängepunkt (mount point):	/boot
Mount-Optionen:	defaults
Boot-Flag:	Ein

3. Zurück in der Partitionstabelle wird nun die dritte Partition auf welcher das Linuxsystem installiert werden soll ausgewählt und wiefolgt verändert:

Benutzen als:	physikalisches Volume für Verschlüsselung
Verschlüsselungsmethode:	Device-mapper (dm-crypt)
Verschlüsselung:	aes
Schlüssellänge:	256
IV-Algorithmus:	cbc-essiv:sha256
Schlüssel:	Passphrase
Daten löschen:	Ja
Boot-Flag:	Aus

4. Zurück in der Partitionstabelle muss nun die Option „Verschlüsselte Datenträger konfigurieren“ ausgewählt werden. Bei der folgenden Sicherheitsabfrage ob die Änderungen auf die Festplatte geschrieben werden sollen, „Ja“ auswählen. Dann noch das Passwort für die Verschlüsselung (mehr als 20 Zeichen! – siehe Anmerkungen zu Passwortsicherheit S.7) eingeben und die Konfigurierung ist abgeschlossen.

5. Zurück in der Partitionstabelle wird die unterste und auf der verschlüsselten Partition einzige Partition ausgewählt und wie folgt verändert:

Benutzen als:	physikalisches Volume für LVM

6. Zurück in der Partitionstabelle muss nun die Option „Logical Volume Manager konfigurieren“ ausgewählt werden. Bei der folgenden Sicherheitsabfrage ob die Änderungen auf die Festplatte geschrieben werden sollen, „Ja“ auswählen. Für den Logical Volume Manager wird zunächst eine Volume-Gruppe mit beliebigem Namen erstellt. Die Größe dieser Volume-Gruppe entspricht dem gesamten zu verschlüsselnden Linuxsystem. Innerhalb dieser Volume-Gruppe können nun beliebig viele Logische Volumes erstellt werden. Als einfachste Variante werden zwei Logische Volumes mit beliebigen Namen erstellt. Das erste Volume als große Systempartition (root) und das zweite Volume als Swap-Auslagerungsspeicher. Der Swap-Auslagerungsspeicher ist üblicherweise doppelt so groß wie der Arbeitsspeicher des PC's (mehr als 512 MB sind aber nicht sinnvoll). Mit der Option „Konfigurationsdetails anzeigen“ können die Größen der erstellten Logischen Volumes überprüft werden.

7. Zurück in der Partitionstabelle wird nun die erstellte verschlüsselte große Datenpartition ausgewählt und wie folgt verändert:

Benutzen als:	Ext3-Journaling-Dateisystem
Einhängepunkt (mount point):	/
Mount-Optionen:	defaults
Name:	Keiner
Reservierte Blöcke:	5%
Typische Nutzung:	standard

8. Zurück in der Partitionstabelle wird nun der erstellte verschlüsselte Swap-Auslagerungsspeicher ausgewählt und wie folgt verändert:

Benutzen als:	Auslagerungsspeicher (Swap)

9. Die Änderungen an der Partitionstabelle sind nun fertig. Die Partitionstabelle sollte z.B. wie folgt aussehen:

IDE1 Master (hda) - 20.0 GB IBM-DJSA-220					
	Nr. 1	primär	255.0 MB B	F	ext2	/boot
	Nr. 2	primär	4.7 GB	K	fat32	/windows
	Nr. 5	logisch	15.1 GB	K	crypto (hda5_crypt)	
Verschlüsseltes Volume (hda5_crypt) - 15.1 GB Linux device-mapper						
	Nr. 1		15.1 GB	K	lvm	
LVM VG lvm, LV root - 14.2 GB Linux device-mapper						
	Nr. 1		14.2 GB	f	ext3	/
LVM VG lvm, LV swap - 838.9 MB Linux device-mapper						
	Nr. 1		838.9 MB	f	Swap	Swap

Wenn die Partitionstabelle entsprechend aussieht wird die Option „Partitionierung beenden und Änderungen übernehmen“ ausgewählt. Den restlichen Anweisungen und Abfragen (Systemzeit, username...) wie üblich folgen.

Fertig ist das Linux-Windows-Kombisystem.

impressum

- **Beilage zur HUch! 53 – April 2008**
- **Anschrift** HUch! Zeitung der Studentischen Selbstverwaltung; Unter den Linden 6; 10099 Berlin; huch@refrat.hu-berlin.de; www.refrat.de/huch
- **HerausgeberIn** ReferentInnenrat der Humboldt-Universität zu Berlin (ges. AStA)
- **Redaktion** Marek Pasterny, Tobias Becker (V.i.S.d.P) **Layout** Tobi **Lektorat** Fehlanzeige **Druck** Hinkelstein Druck – sozialistische GmbH **Auflage** 3.200

Link Liste

Email Verschlüsselung:

Thunderbird:	http://www.mozilla.com.
GPG:	http://gnupg.org/
win:	ftp://ftp.gnupg.org/gcrypt/binary/
mac:	http://macgpg.sourceforge.net/
Enigmail:	https://addons.mozilla.org/de/thunderbird/addon/71
Zum weiterlesen:	http://de.wikipedia.org/wiki/GNU_Privacy_Guard

Anonym Surfen:

TOR:	http://www.torproject.org/
Vidalia:	http://www.vidalia-project.net
Torbutton:	https://addons.mozilla.org/firefox/2275/ (torbutton)
TorPark:	http://www.foebud.org/datenschutz-buergerrechte/vorratsdatenspeicherung/torpark-privacydongle-2-0.zip/view
IP testen:	http://www.ip.cc
Zum weiterlesen:	http://wiki.ubuntuusers.de/Sicherheit/Anonym_Surfen
	http://de.wikipedia.org/wiki/Onion_Routing
	http://de.wikipedia.org/wiki/TOR_%28Netzwerk%29

Dateien sicher löschen:

eraser:	http://www.heidi.ie/eraser/download.php
wipe:	http://sourceforge.net/project/showfiles.php?group_id=804
Zum weiterlesen:	http://wiki.ubuntuusers.de/Daten_sicher_l%C3%B6schen

Festplatte verschlüsseln:

(K)Ubuntu:	http://wiki.ubuntuusers.de/Downloads
Zum weiterlesen:	http://wiki.ubuntuusers.de/System_verschl%C3%BCsseln

Allgemein:

CCC:	http://www.ccc.de
Sicherheit (Linux):	http://wiki.ubuntuusers.de/Sicherheit