

E-Mail jenseits der Überwachung

Unix / Linux

21. Dezember 2011

Zusammenfassung

Auch bei der Nutzung von GnuPG oder S/MIME für die Verschlüsselung von E-Mails ist es mitlesenden Dritten möglich, Absender und Empfänger zu protokollieren und anhand der erfassten Daten Kommunikationsprofile zu erstellen. Insbesondere die Vorratsdatenspeicherung und die darauf aufbauenden internationalen ESTI-Standards für Geheimdienste und Strafverfolger zeigen, dass diese nicht verschlüsselbaren Informationen für die Überwachung bedeutsam sind.

Es gibt mehrere Projekte, die einen überwachungsfreien Austausch von Nachrichten ermöglichen und somit beispielsweise für investigative Journalisten und deren Informanten den nötigen Schutz bieten und die Erstellung von Kommunikationsprofilen für E-Mails behindern.

1 Anonyme E-Mail Accounts

Im Kapitel Anonymisierungsdienste gibt es Anleitungen, wie man mit JonDo & Thunderbird oder mit Tor & Thunderbird einen anonymen E-Mail Account nutzen könnte. Als E-Mail Provider kann man einen zuverlässigen Anbieter im Web nehmen. Außerdem bieten I2P und Tor spezielle Lösungen:

- Das Invisible Internet Project (I2P) bietet mit Susimail einen anonymen Mailservice inklusive SMTP- und POP3-Zugang und Gateway ins Web oder mit I2P Bote einen serverlosen, verschlüsselten Mailedienst.
- TorMail gibt es als Hidden Service unter <http://jhiwjllqpyawmpjx.onion> mit POP3 und SMTP Service und ist auch aus dem Web unter xxx@tormail.net erreichbar.
- Tor Privat Messaging unter <http://4eiruntyxxbgfv7o.onion/pm/> ist ein Tor Hidden Service im Onionland, um Textnachrichten unbeobachtet auszutauschen. Der Dienst kann nur im Webinterface genutzt werden.

Hinweis: Informationen über Langzeitkommunikation können ihr Pseudonym deanonymisieren. Anhand der Freunde in der E-Mail Kommunikation sind Schlussfolgerungen auf ihre reale Identität möglich. Wenn sie einen wirklich anonymen E-Mail Account für eine bestimmte Aufgabe benötigen - z.B. für Whistleblowing - dann müssen sie einen neuen Account erstellen. Löschen sie den Account, sobald sie ihn nicht mehr brauchen.

2 alt.anonymous.messages

Um die Zuordnung von Absender und Empfänger zu erschweren, kann man das Usenet nutzen. In der Newsgruppe *alt.anonymous.messages* werden ständig viele Nachrichten gepostet und sie hat tausende Leser. Jeder Leser erkennt die für ihn bestimmten Nachrichten selbst. Es ist eine Art schwarzes Brett.

Es ist sinnvoll, die geposteten Nachrichten zu verschlüsseln. Dafür sollte der Empfänger einen OpenPGP-Key bereitstellen, der keine Informationen über seine Identität bietet. Normalerweise enthält ein OpenPGP-Schlüssel die E-Mail Adresse des Inhabers. Verwendet man einen solchen Schlüssel ist der Empfänger natürlich deanonymisiert.

Außerdem sollte man seine Antworten nicht direkt als Antwort auf ein Posting veröffentlichen. Da der Absender in der Regel bekannt ist (falls keine Remailer genutzt wurden) kann aus den Absendern eines zusammengehörenden Thread ein Zusammenhang der Kommunikationspartner ermittelt werden.

3 Mixmaster Remailer

Der Versand einer E-Mail über Remailer-Kaskaden ist mit der Versendung eines Briefes vergleichbar, der in mehreren Umschlägen steckt. Jeder Empfänger innerhalb der Kaskade öffnet einen Umschlag und sendet den darin enthaltenen Brief ohne Hinweise auf den vorherigen Absender weiter. Der letzte Remailer der Kaskade liefert den Brief an den Empfänger aus.

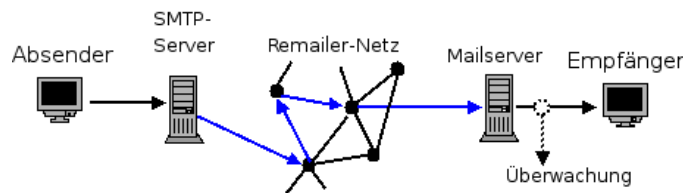


Abbildung 1: Konzept einer anonymen E-Mail

Technisch realisiert wird dieses Prinzip mittels asymmetrischer Verschlüsselung. Der Absender wählt aus der Liste der verfügbaren weltweit verteilten Remailer verschiedene Server aus, verschlüsselt die E-Mail mehrfach mit den öffentlichen Schlüsseln der Remailer in der Reihenfolge ihres Durchlaufes und sendet das Ergebnis an den ersten Rechner der Kaskade. Dieser entschlüsselt mit seinem geheimen Schlüssel den ersten Umschlag, entnimmt dem Ergebnis die Adresse des folgenden Rechners und sendet die jetzt (n-1)-fach verschlüsselte E-Mail an diesen Rechner. Der letzte Rechner der Kaskade liefert die E-Mail an den Empfänger aus.

Mitlesende Dritte können lediglich protokollieren, dass der Empfänger eine E-Mail unbekannter Herkunft und evtl. unbekanntes Inhalt (verschlüsselt

mit OpenPGP oder S/MIME) erhalten hat. Es ist ebenfalls möglich, Beiträge für News-Groups anonym zu posten.

Um die Traffic-Analyse zu erschweren, wird die Weiterleitung jeder E-Mail innerhalb der Kaskade verzögert. Es kann somit 2...12h dauern, ehe die Mail dem Empfänger zugestellt wird! Sollte der letzte Remailer der Kette die Nachricht nicht zustellen können (z.B. aufgrund eines Schreibfehlers in der Adresse), erhält der Absender keine Fehlermeldung. Der Absender ist ja nicht bekannt.

Wichtig: da die E-Mail keine Angaben über den Absender enthält, funktioniert der *Antworten-Button* der Clients auf der Empfängerseite nicht! Der Text der E-Mail sollte einen entsprechenden Hinweis enthalten!

3.1 Remailer-Webinterface nutzen

Die einfachste Möglichkeit, eine anonyme E-Mail zu schreiben, besteht darin, ein Webinterface zu nutzen. Es gibt verschiedene Angebote im Internet:

- <https://www.awxcnx.de/anon-email.htm>
- <https://www.cotse.net/cgi-bin/mixmail.cgi>

Verglichen mit der lokalen Installation eines Remailer Clients ist dies die zweitbeste Möglichkeit, eine anonyme E-Mail zu versenden. Den Betreibern der Server liegen alle Daten im Klartext vor und sie könnten beliebig loggen. Die Installation von Quicksilver (für Windows) oder Mixmaster (für Linux) finden sie in der Online-Version des Privacy-Handbuch.

4 Fake Mailer

Im Webinterface eines Fake-Mailers können sie eine beliebige Absender Adresse angeben. Um anonym zu bleiben, sollte man Fake Mailer nur mit Anonymisierungsdiensten nutzen. Es besteht kein Schutz gegen Aufdeckung des Absenders durch den Betreiber des Dienstes.

- <https://emkei.cz>

Im Gegensatz zu Remalern dauert es nicht mehrere Stunden, bis die Mail zugestellt wird. Es ist aber möglich, dass diese Mails in Spam-Filtern hängen bleiben, da viele Spam-Filter diese Absender Adresse und die IP-Adresse des sendenden Servers in ihre Bewertung einfließen lassen. Man sollte zusätzliche Spam-Merkmale im Text der Nachricht vermeiden.

5 PrivacyBox der GPF

Die PrivacyBox (<https://privacybox.de>) ermöglicht es, anonyme Nachrichten zu empfangen. Sie sollte in erster Linie Journalisten, Bloggern u.a. eine vorratsdatenfreie und anonyme Kontaktmöglichkeit für Informanten bieten, steht

aber allen Interessenten offen. Es können nur Nachrichten empfangen werden. Die Nachrichten müssen auf der Kontaktseite des Empfängers geschrieben werden.

Die PrivacyBox nimmt keine E-Mails an und bietet auch keine Möglichkeit, E-Mails zu versenden. Es ist so etwas, wie ein Toter Briefkasten.

Politische Aktivisten sollten beachten, dass die PrivacyBox von einem deutschen Verein betrieben wird, der bspw. Linken Gruppen keinen Schutz gegen Ermittlungen nach §129a durch das BKA bieten kann. Die PrivacyBox ist ein Single Point, der über fast alle Informationen inklusive unverschlüsselter Inhalte der Nachrichten verfügen kann. Das LulzSec-Fiasco des VPN-Dienstes *Hide my Ass* zeigt, wie leicht Single Points kompromittiert werden können.

Ich habe die PrivacyBox lange Zeit uneingeschränkt empfohlen. Als Administrator und Hauptentwickler konnte ich sicher sein, dass keine Daten gespeichert wurden und es keine Kooperation mit Geheimdiensten gab. Im Sommer 2011 hat der Vorstand der GPF gegen meinen Wunsch einen zweiten Administrator für die PrivacyBox bestätigt, der meiner Meinung nach als informeller Mitarbeiter unter dem Decknamen SSysiphos für die Dienste arbeitet (neusprech: als "Vertrauensperson"). Der Vorschlag, dass alle Mitglieder des Vorstand inkl. des neu bestätigten Admin eine eidesstattliche Erklärung zur Nicht-Kooperation mit Geheimdiensten abgeben, wurde nicht angenommen.

Ich habe die Administration und Weiterentwicklung der PrivacyBox sowie meine Mitgliedschaft in der GPF niedergelegt. Aus heutiger Sicht ist das Projekt PrivacyBox ähnlich wie VPN-Dienste einzustufen. Mehr war mit den bescheidenen Mitteln eines Vereins nicht realisierbar.

Die PrivacyBox bietet viele Sicherheitsfeatures. Sie ist als Tor Hidden Service und I2P eepsite erreichbar und bietet client-seitige Verschlüsselung im Browser. Es liegt aber in der Verantwortung der Nutzer, diese Feature auch zu nutzen!

6 Mixmaster für Unix/Linux

6.1 Mixmaster installieren (Source)

Die Sourcen von Mixmaster stehen unter <http://mixmaster.sourceforge.net> zum Download bereit. Für die Übersetzung werden die Entwicklerpakete folgender Komponenten benötigt, welche von nahezu allen Distributionen bereitgestellt werden:

- vi Editor
- ncurses Bibliothek
- OpenSSL Bibliothek
- PCRE Bibliothek

- zlib Bibliothek
- OpenPGP Programm (z.B. GnuPG)

Nach dem Download ist das Archiv zu entpacken und in das neu angelegte Verzeichnis zu wechseln. Hier ist das Kommando `./Install` einzugeben.

Die Installationsroutine stellt einige kurze Fragen und bietet sinnvolle Vorgaben. Als Installationsverzeichnis ist es sinnvoll `$HOME/Mix` zu übernehmen. Die Frage *Do you want to set up a remailer?* ist mit ENTER zu verneinen.

Die Meldung *Client installation complete.* zeigt den erfolgreichen Abschluss der Installation an.

Im Anschluß können die Remailer Listen initialisiert werden. Diese Listen enthalten die benötigten Informationen über nutzbare Remailer, die unterstützten Features und die öffentlichen Schlüssel der Remailer und sollten bei der Versendung einer E-Mail nicht älter als 24h sein.

```
> ~/.Mix/mixmaster --update-pinger-list
> ~/.Mix/mixmaster --update-stats=noreply
```

Sollte der Server *noreply* nicht erreichbar sein, können *deuxpi* oder andere Pinger genutzt werden. Eine vollständige Übersicht über alle Mixmaster-Pinger bietet <http://www.noreply.org>. Zukünftige Updates der Listen können dem Daemon *mixmaster-smtp* überlassen werden.

6.2 Mixmaster-SMTP installieren

mixmaster-smtp ist ein kleines Perl-Script, welches einen SMTP-Server bereitstellt, der von beliebigen E-Mail Clients versendete Mails an Mixmaster zur anonymen Versendung weiterleitet. Außerdem übernimmt es das Update der Remailer Listen bei Notwendigkeit.

Die **Sourcen** stehen unter <https://www.awxcnx.de/wabbel.htm> zum Download bereit. Nach dem Entpacken des Archives könnte man das Script und die Manualpage mit `./Install` nach `/usr/local/bin` bzw. `/usr/local/man/man1` kopieren. Dieser Schritt ist aber nicht zwingend nötig. Das Script im Unterverzeichnis *bin/* startet aus beliebigen Verzeichnissen.

Das Script benötigt einige Perl Module für die Arbeit. Diese können als User *root* via CPAN installiert werden:

```
# perl -MCPAN -e shell
```

Nachdem die Fragen zur Initialisierung des CPAN-Moduls beantwortet wurden, sind am CPAN-Prompt folgende Kommandos einzugeben:

```
cpan> install Net::Server::Daemonize
cpan> install Net::Server::Mail::ESMTP
cpan> exit
```

Im Anschluss sollte das Script *mixmaster-smtp* problemlos starten. Die nötige Konfiguration wird in der Regel korrekt erkannt. Kleine Anpassungen sind weiter unten beschrieben.

Das Archiv enthält im Verzeichnis *init.d* drei Startscripte (für Debian/Ubuntu, Gentoo und SuSE), um den Daemon beim Booten automatisch zu starten. Diese werden wie folgt installiert:

- Debian / Ubuntu

```
# cp init.d/mixmaster-smtp.debian /etc/init.d/mixmaster-smtp
# update-rc.d mixmaster-smtp defaults
```

- SuSE Linux

```
# cp init.d/mixmaster-smtp.suse /etc/init.d/mixmaster-smtp
# insserv mixmaster-smtp
```

6.3 Mixmaster konfigurieren

Die Konfiguration erfolgt in der Textdatei *\$HOME/.Mix/mix.cfg* oder global für alle User in der Datei */etc/mixmaster/client.conf*. Linux wird an dieser Stelle seinem Ruf als Volltext-Adventure gerecht.

Für die Versendung an den ersten Remailer der Kaskade wird ein Name für den Absender und eine Absenderadresse benötigt. Es sind folgende Zeilen in der Konfiguration hinzuzufügen:

```
NAME      realer Name
ADDRESS   reale E-Mail Adresse
```

Mixmaster sollte für die Versendung der anonymen E-Mails an den ersten Remailer der Kaskade möglichst den lokalen Mail Transfer Agenten nutzen, um eine überflüssige Protokollierung durch den Mailserver des Providers zu vermeiden. Wenn *sendmail* funktioniert, ist folgende Vorgabe korrekt:

```
SENDMAIL  sendmail -t
```

Soll statt dessen ein lokaler oder externer SMTP-Server für die Versendung genutzt werden, ist statt SENDMAIL folgende Zeile hinzuzufügen:

```
SMTPRELAY  mail.server.tld
```

Erfordert der SMTP-Server eine Anmeldung via SMTP-Auth, sind folgende Zeilen in der Konfigurationsdatei hinzuzufügen:

```
SMTPUSERNAME  SMTP-UserName
SMTPPASSWORD  SMTP-Passwort
```

Ausserdem sind in der Konfiguration die Schlüsselringe für OpenPGP-Verschlüsselung anzugeben. Verwendet man GnuPG, sind folgende Zeilen korrekt:

```
PGPPUBRING /home/<username>/.gnupg/pubring.gpg
PGPSECRING /home/<username>/.gnupg/secring.gpg
```

6.4 Mixmaster-SMTP konfigurieren

Mixmaster-SMTP nutzt die Konfigurationsdatei `$HOME/.Mix/smtp.conf` oder global für alle User in der Datei `/etc/mixmaster/smtp.conf`. Ein Beispiel ist im Verzeichnis `conf` des Quellpaketes enthalten.

Wer eine ältere Version von mixmaster vor 3.0rc1 nutzt, muss das Update der Remailer Statistiken in der Konfiguration deaktivieren und sich selbst drum kümmern:

```
REMAILER_UPDATE no
```

Das von P. Palfrader betreute Mixmaster-Paket für Debian GNU/Linux enthält ein eigenes Script für das Update. Wer dieses Paket nutzt, sollte das Update entsprechend konfigurieren:

```
REMAILER_UPDATE debian
```

Wer die Software für den Onion Router (Tor) installiert hat, kann dieses Netzwerk nutzen, um keine Spuren in den Logs des Providers zu hinterlassen:

```
TORIFY_UPDATES yes
```

6.5 Installation für Debian GNU/Linux

Debian GNU/Linux und Ubuntu enthalten ein fertiges *mixmaster*-Paket. Für *mixmaster-smtp* gibt es ein Packet im Wabbel-Repository. Die Einbindung des Wabbel-Repository ist auf der Website <https://www.awxcnx.de/wabbel.htm> beschrieben.

Anschließend spülen die folgenden Kommandos alles nötige auf die Platte und starten den Daemon *mixmaster-smtp*

```
# apt-get update && aptitude install mixmaster mixmaster-smtp
```

Alle Pakete sind sinnvoll konfiguriert. Lediglich die Identität für die Versendung einer E-Mail an den ersten Remailer der Kaskade ist in `/etc/mixmaster/client.conf` zu konfigurieren:

```
NAME      realer Name
ADDRESS   reale E-Mail Adresse
```

Sollte der Provider die Versendung von E-Mails von lokalen Rechnern unterbinden (Spamschutz), ist ein SMTPRELAY wie oben beschrieben, in der Datei `/etc/mixmaster/client.conf` zu konfigurieren.

6.6 Anonyme E-Mails mit Mixmaster versenden

Wer mit dem **Editor vi** vertraut ist, kann Mixmaster auf der Kommandozeile starten, mit dem integrierten Editor eine E-Mail schreiben und anonym versenden.

mixmaster-smtp bietet die Möglichkeit, eine E-Mail mit dem bevorzugten E-Mail Client zu schreiben, zu verschlüsseln und zur anonymen Versendung an Mixmaster zu übergeben. Auch das Update der Remailer Statistiken übernimmt das Script bei Bedarf. Das folgende Kommando in einer Konsole(!) startet den Daemon etwas geschwätzig, wenn er nicht beim Booten gestartet wurde:

```
> mixmaster-smtp --verbose
```

Evtl. ist der vollständige Pfad zum Script anzugeben. Es startet ein SMTP-Server, welcher unter der Adresse *localhost:8025* auf E-Mails wartet. Im E-Mail Client ist ein weiterer SMTP-Server für den Versand zu konfigurieren und evtl. eine Identität anzulegen.

Eine dritte Möglichkeit nutzt einen beliebigen **Texteditor** oder besser eine komplette Textverarbeitung mit Rechtschreibprüfung und Vorlagenverwaltung, um die E-Mail auf Basis der folgenden Vorlage zu schreiben, als TXT-Datei zu speichern und diese mit Mixmaster anonym zu versenden.

```
To:
Subject:
Mime-Version: 1.0
Content-Type: text/plain; charset='utf-8'
Content-Transfer-Encoding: 8bit
```

```
Hallo alle miteinander,
hier beginnt der Inhalt
```

In den ersten beiden Zeilen ist die E-Mail-Adresse des Empfängers und der Betreff der Nachricht einzutragen. Zwischen dem Header und dem eigentlichen Inhalt ist eine Leerzeile frei zu lassen.

Nachdem die Nachricht geschrieben wurde, ist die Datei unter einem neuen Namen als TXT-Datei zu speichern, beispielsweise unter *\$HOME/anon-email.eml*.

Diese E-Mail kann mit den folgenden Befehlszeilen versendet werden, welche für häufige Nutzung auch als Shell-Script gespeichert werden können:

```
> ~/.Mix/mixmaster --update-stats=deuxpi
> ~/.Mix/mixmaster -m ~/anon-email.eml
> ~/.Mix/mixmaster -S
> shred -u ~/anon-email.eml}
```

Der erste Befehl aktualisiert die Remailer-Statistiken und kann entfallen, wenn diese nicht älter als 24h sind. Unter Debian GNU/Linux ist *mixmaster-update* zu nutzen.

Die zweite Befehlszeile übernimmt die Nachricht, wählt die Remailer-Kette aus und legt eine vorbereitete E-Mail im Spool-Verzeichnis ab. Der dritte Aufruf von Mixmaster versendet alle Mails aus dem Spool-Verzeichnis und der letzte Befehl beseitigt die Datei, indem sie zuerst mit Nullen überschrieben und anschließend gelöscht wird.

Soll die E-Mail an der Empfänger OpenPGP verschlüsselt ausgeliefert werden, ist die zweite Befehlszeile zusätzlich um die Option `-encrypt` zu erweitern.

Im Prinzip ist es auch möglich, Attachements an eine anonyme E-Mail zu hängen. Viele Remailer entfernen diese jedoch. Einige Remailer lassen Attachements bis zu 100KB passieren. Ich bin der Meinung, man kann auf Anhänge verzichten und werde hier nicht weiter darauf eingehen.

6.7 Anonymes News-Posting mit Mixmaster versenden

Wer mit dem Editor vi vertraut ist, kann Mixmaster auf der Kommandozeile starten, mit dem integrierten Editor ein News-Posting schreiben und anonym versenden.

Eine zweite Möglichkeit nutzt einen beliebigen **Texteditor** oder besser eine komplette Textverarbeitung mit Rechtschreibprüfung und Vorlagenverwaltung, um das Posting auf Basis der folgenden Vorlage zu schreiben, als TXT-Datei zu speichern und diese mit Mixmaster anonym zu versenden.

```
To: mail2news@newsanon.org, mail2news@dizum.org
Newsgroups:
X-No-Archive: Yes
Subject:
Mime-Version: 1.0
Content-Type: text/plain; charset='utf-8';
Content-Transfer-Encoding: 8bit
```

Ich möchte folgendes veröffentlichen: blabla

Zwischen dem Header und dem eigentlichen Inhalt ist eine Leerzeile frei zu lassen.

Ein anonymes News-Posting wird per E-Mail an ein Mail2News Gateway geschickt. Diese E-Mail wird durch die Remailer-Kaskade anonymisiert. Das Gateway wandelt die anonyme E-Mail in ein News-Posting um und schickt es an die Newsgroups. Eine kurze Liste aktueller Gateways:

- mail2news (at) bananasplit.info
- mail2news (at) dizum.com
- mail2news (at) reece.net.au
- mail2news (at) m2n.mixmin.net

Nachdem die Nachricht geschrieben wurde, ist die Datei im TXT-Format unter einem neuen Namen zu speichern, beispielsweise unter $\$HOME/anon-news.eml$. Diese Datei kann mit den folgenden Befehlszeilen an die Newsgroups gesendet werden:

```
> ~/.Mix/mixmaster --update-stats=hermetix
> ~/.Mix/mixmaster -m ~/anon-news.eml
> ~/.Mix/mixmaster -S
> shred -u /home/<username>/anon-news.eml
```

Der erste Befehl aktualisiert die Remailer-Statistiken und kann entfallen, wenn diese nicht älter als 24h sind. Unter Debian GNU/Linux ist *mixmaster-update* zu nutzen.