Anonyme Remailer Netze

Was ist ein anonymer Remailer?

- Ein Mailserver (meistens) der eine Mail anonym macht
- Es gibt verschiedene Arten Remailer:
  - Einfache Remailer (Header strippen/vertuschen)
  - Kryptierte (Typ1 Remailer)
  - Mixmaster (Typ2 Remailer)
  - Remailernetze
  - Nymserver
- Nymserver bieten eine anonyme (aber feste) Mailadresse

Wieso sollte man einen Remailer benutzen

- Probleme beim Aeussern von gewissen politischen/philosophischen Standpunkten
- Probleme mit dem Arbeitsgeber
- Probleme mit der Justiz
- Beispiele :
  - Schwule, Drogenabhaengige, Kranke Menschen
  - Betrug in der Firma,
  - revolutionaere Ideen,
  - Sicherheitsluecken

Wie funktionniert ein Cypherpunk Remailer?

- Jeder Remailer hat einen oeffentlichen PGP Key
  - Diese Keys kann man anfragen, oder auch auf dem Netz finden
  - zB auf http://www.publius.net/rlist.html
- Jede Mail bekommt einen Header fuer den Remailer
  - Headerformat: http://www.skuz.net/potatoware/reli/UserMan.htm
- Beispiel:

```
::
Anon-To: realname@xyz.com
```

- Jede Mail wird mit dem Public-Key des Remailers kryptiert
- Dann kommt nochmal ein Header der die Kryptierung angibt
- Endlich wird die Mail verschickt

Was kann ein Cypherpunk Remailer?

- Weiterleiten einer Email (war ja auch klar :)
- Verarbeiten von kryptierten Anweisungen (s. oben)
- Entfernen von Headers
- Entfernen von Informationen in der Mail
- Hinzufuegen neuer Header (hash-header zB.)
- Verschluesseln von Teilen der Email

Was sind Remailernetze?

- Ein Remailer kann eine Email weiterleiten
- Ein Remailer kann Mails an andere Remailer weiterleiten
- Remailernetze: Verschachtelung von Remaileranweisungen
- Beispiel:

```
::
Anon-To: realname@xyz.com

Bla
```

- Kryptieren der Nachricht mit der Key von remailer@bla.com
- Header fuer neuen Remailer

```
::
Anon-To: remailer@bla.com

::
Encrypted: PGP

...
```

- Kryptieren mit Key von remailer@blub.com
- Header fuer remailer@blub.com, usw...

Was sind die Schwaechen von Cypherpunk Remailern?

- Unkryptierte Mails sind unsicher (war auch irgendwie klar)
- Ein Remailer reicht nicht (kennt sowohl Quell- als Zieladresse)
- Reorderingangriff:
  - Verzoegerung gibt es zwar, aber durch DOS verhindbar
- Verfolgen durch Groesse
- Replay-Attacken

Wie funktionniert ein Mixmaster Remailer?

- Mixmaster ist ein Remailer des Typs II
  - http://www.obscura.com/~loki/
- Benutzt nicht PGP, sondern ein eigenes Verfahren
- Paddet jede Nachricht auf eine bestimmte Groesse
- Sortiert Nachrichten zufaellig neu
- Verwirft schon verschickte Nachrichten
- Benutzt ein eigenes Remailernetz
- Man kann natuerlich TypI und TypII verbinden

Was ist ein Nymserver?

- nymserver ermoeglichen das anonyme Mailschicken und -empfangen
- Zu einem nym gehoeren
  - ein PGP Key, Config Parameter, ein Reply Block
- PGP Key dient der Authentifizierung (Config oder schicken)
- Key dient auch der Verschluesselung von einkommenden Mails
- Mails sollten anonym an den Nym zum weitersenden geschickt werden
- Reply-Block enthaelt den Pfad zurueck
- Ein bekannter Nymserver ist nym.alias.net
  - http://publius.net/n.a.n.help.html
- Mails kann man auch auf einer Newsgroup ausliefern lassen

Client software, die man haben sollte

- PGP natuerlich
- Premail erleichtert die Arbeit ungemein
- Private Idaho unter Windows
- Mixmaster, um Remailer vom TypII benutzen zu koennen
- Diese ganze Software kann man auf ftp://utopia.hacktic.nl ziehen

Quellen

- http://publius.net/
- ftp://utopia.hacktic.nl
- http://www.obscura.com/~loki/
- http://www.skuz.net/potatoware/reli/UserMan.htm
- http://www.stack.nl/~galactus/
- http://www.iks-jena.de/mitarb/lutz/anon/