Il remailer mixmaster

spialaspia@inventati.org

v0.7 27/12/2009

Guida all'installazione e all'uso del remailer mixmaster e del suo client

1. Il client del remailer mixmaster

1.1 Installazione

Il client del mixmaster per unix viene compilato partendo dal pacchetto completo del remailer (se usate debian saltate questa parte, è sufficiente un apt-get install mixmaster per installare il client).
Scaricare il file mixmaster-2.9.0.tar.gz dal sito http://www.sourceforge.net/projects/mixmaster nella vostra home directory, e scaricare anche la signature per verificarne l'autenticità. Poi decomprimere il pacchetto:

$ tar xzvf mixmaster-2.9.0.tar.gz

$ cd mixmaster-2.9.0

Eseguire il comando ./Install, vi chiederà la directory dove installare il client, scelta consigliata /Mix
Alla domanda successiva:
Do you want to set up a remailer? [y]
rispondete con "n" per compilare solo il client.
A questo punto l'installazione è completa, provate a lanciare il client per verificare che tutto funzioni
/Mix/mix -S

Attenzione: molte distribuzioni linux hanno una versione di openssl senza il supporto per l'algoritmo idea. Questo impedisce al client del mixmaster di poter usare i nym server.
In questo caso potete scaricare il file openssl-0.9.7.tar.gz dal sito http://www.openssl.org e copiare la directory openssl-0.9.7 contenuta nel pacchetto nella directory Src/ che è una sottodirectory di mixmaster-2.9.0
In questo modo il supporto idea sarà inserito nel client del mixmaster anche se il vostro sistema non ha il supporto per idea.

1.2 Configurazione

Nel file mix.cfg ci sono dei parametri che possono essere modificati, queste sono le impostazioni di default:

```
SENDMAIL        /usr/bin/sendmail -t
######################## Client configuration: ##########################
REMAIL          n
#NAME           your realname
#ADDRESS        user@host
SENDPOOLTIME    6h
CHAIN           *,*,*,*
NUMCOPIES       1
DISTANCE        2
MINREL          98
RELFINAL        99
```

```
MAXLAT          36h
```

la prima è ovvia, definisce il vostro mailer e il fatto che il remailer non è attivo (abbiamo compilato solo il client).

E' meglio modificare la riga relativa al SENDMAIL in:

SENDMAIL /usr/bin/sendmail -t -findirizzo@host.esistente.org

questo perchè altrimenti il remailer a cui indirizzate il messaggio potrebbe rifiutarlo perchè si vedrebbe arrivare il messaggio da una macchina che in realtà in rete non esiste se il vostro mailer non è settato per definire un indirizzo esistente per il campo "From" impostato sui messaggi in uscita dal vostro PC.

SENDPOOLTIME definisce ogni quanto il mixmaster deve controllare il pool per spedire eventuali messaggi presenti se è stato lanciato in daemon mode.

CHAIN definisce la catena dei remailer usata di default, gli asterischi indicano una scelta random.

NUMCOPIES definisce il numero di copie del essaggio da inviare (default: 1)

DISTANCE impostato a 2 significa che se nella stessa catena compare 2 volte lo stesso remailer (es. "remailerX"), il msg dovrà passare attraverso altri 2 remailer prima di poter tornare al remailer "remailerX".

MINREL e RELFINAL definiscono che l'affidabilità dei remailer scelti a caso per le catene deve essere almeno pari, rispettivamente, al 98% e al 99%. L'affidabilità è un parametro contenuto nelle statistiche consultate dal client.

MAXLAT indica che i remailer scelti a caso dovranno avere una latenza massima di 36 ore.

I campi NAME e ADDRESS sono utili solo nel caso in cui usiate quei (pochi) remailer che permettono di definire il campo From: del messaggio finale al posto del classico From: Anonymous

Se desiderate costruirvi un'identità però a questo punto è meglio usare un nym.

1.3 Tenere aggiornati chiavi e statistiche

Per avere una lista dei remailer disponibili sempre aggiornata è utile usare lo script getmix.sh http://remailer.paranoici.org/scripts/getmix.sh che scarica chiavi e statistiche dei remailer.

Copiatelo in /usr/local/bin e date il comando

chmod +x /usr/local/bin/getmix.sh

per renderlo eseguibile.

E' buona regola lanciarlo regolarmente per restare aggiornati, ad esempio ogni volta che ci si collega in rete inserendo nel file

/etc/ppp/ip-up

una riga che lancia lo script getmix.sh, oppure mettendolo nel cron se siete connessi 24h/24

1.4 Utilizzo del client del mixmaster

Per utilizzare il client basta lanciarlo con: $ /Mix/mix e vi troverete davanti un'interfaccia spartana in ncurses, la prima riga vi dice quanti messaggi avete nel pool (potete spedirli premendo il tasto "s") come indicato nel menu. Le altre opzioni sono:

- "m" per spedire una mail
- "p" per scrivere in un newsgroup
- "r" se volete leggere e rispondere in modo anonimo a msg criptati o meno presenti in una mailbox o in un file.
- "d" per generare messaggi "vuoti" che disturbino le analisi del traffico che entra/esce dalla vostra macchina.
- "s" come detto per spedire i messaggi presenti nello spool
- "q" per uscire dal client.

Se si sceglie di spedire una mail vi verrà chiesto di inserire l'indirizzo del destinatario e il subject, dopodichè vi troverete in una schermata con qualche opzione per modificare i dati appena inseriti, un'opzione "n" per gestirsi un nym, l'opzione "c" per definire una catena di remailers attraverso cui spedire il messaggio (altrimenti verrà instradato attraverso 4 remailer scelti a caso), un'opzione "y" per criptare il msg con la chiave pubblica pgp del destinatario, e infine l'opzione "e" per scrivere il messaggio che vogliamo spedire.

è possibile leggere i messaggi contenuti in una mailbox premendo il tasto "r" e indicando il percorso della mailbox, il default è /var/spool/mail/utente. Una volta apparsa la lista dei messaggi è possibile cancellare (tasto d), rispondere (tasto r), forwardare (tasto m) o forwardare in un newsgroup (tasto p) il messaggio selezionato facendolo passare attraverso una catena di remailer.

1.5 Se usate Debian

Se usate debian un semplice apt-get install mixmaster vi installerà sia il client che il server, il file di configurazione sta in /etc/mixmaster (client.conf) per il resto vale più o meno quanto visto sopra. Per tenere aggiornate le statistiche non è necessario scaricare il getmix, c'è uno script analogo incluso nel pacchetto debian.

1.6 Usare i nym server

Come prima cosa dovete avere le statistiche aggiornate nella directory del client, quindi i file: mlist.txt mlist2 rlist.txt rlist2 type2.lst e pubring.mix devono essere presenti.

Poi bisogna crearsi il nym: non appena lanciato il client, si vede che la seconda voce è n)ym, quindi premendo il tasto "n" si accede ad una schermata per la creazione/gestione dei nym. (vi verrà chiesta una password che sarà utilizzata per proteggere con crittazione convenzionale il file che contiene le chiavi segrete usate per i nyms). Premere "c" per creare un nuovo nym Vi viene chiesto di inserire un alias, quindi facciamo un ipotetico "smith" Poi il nome delle pseudonym, quindi di nuovo "smith" a questo punto vi appare la lista dei nym server attivi su cui è possibile creare il nym, sceglietene uno premendo la lettera corrispondente e poi invio. E' comunque possibile in seguito creare lo stesso nym su un altro nymserver ripetendo la procedura.

Vi appare un'altra schermata, come questa in figura:

Reply block

Nella prima riga vi viene chiesto che tipo di reply block volete: se un messaggio mail, un messaggio che finisce sempre in un newsgroup (es. alt.anonymous) o traffico di copertura. Tralasciando l'ultimo caso, in genere si opta per farsi mandare tutti i messaggi su un newsgroup o in una casella di posta. La procedura è la stessa, l'unica differenza è che per i messaggi spediti sui newsgroup è possibile specificare un subject in modo da rendere più semplice individuare quali sono i propri messaggi in mezzo a tutti gli altri. Comunque, prendiamo in considerazione il caso più comune di reply block classico, con tutti i messaggi che finiscono in una casella e-mail. Questa è la scelta già selezionata, per cui premendo "m" vi ritrovate nella schermata in cui si sceglie il reply block.

Creazione di un nym

Ci sono 4 sezioni, nella prima (chiamata semplicemente "Nym") ci sono i dati che avete già scelto, ossia il nome del nym e il server.

Nella seconda (Nym creation), premendo "c" vi appare la lista dei remailer attraverso cui potete scegliere la catena di remailer usata dal messaggio per arrivare al nym server, i remailer si selezionano premendo la lettera corrispondente che appare alla sinistra del nome. E' buona regola utilizzare remailer con alte percentuali di affidabilità (i primi della lista), e bisogna stare attenti a non selezionare come ultimo remailer della catena un remailer middleman, nel caso comunque compare la scritta "INTERMEDIATE", che significa che dopo

questo remailer ce ne deve essere un altro, oppure bisogna cambiare remailer (backspace per cancellare la scelta precedente).

Una volta scelta la catena si può definire quante copie del messaggio spedire, in genere 1 è sufficiente, comunque spedirne 2 non causa problemi, al limite il server una la cancella perchè la riconosce come doppione.

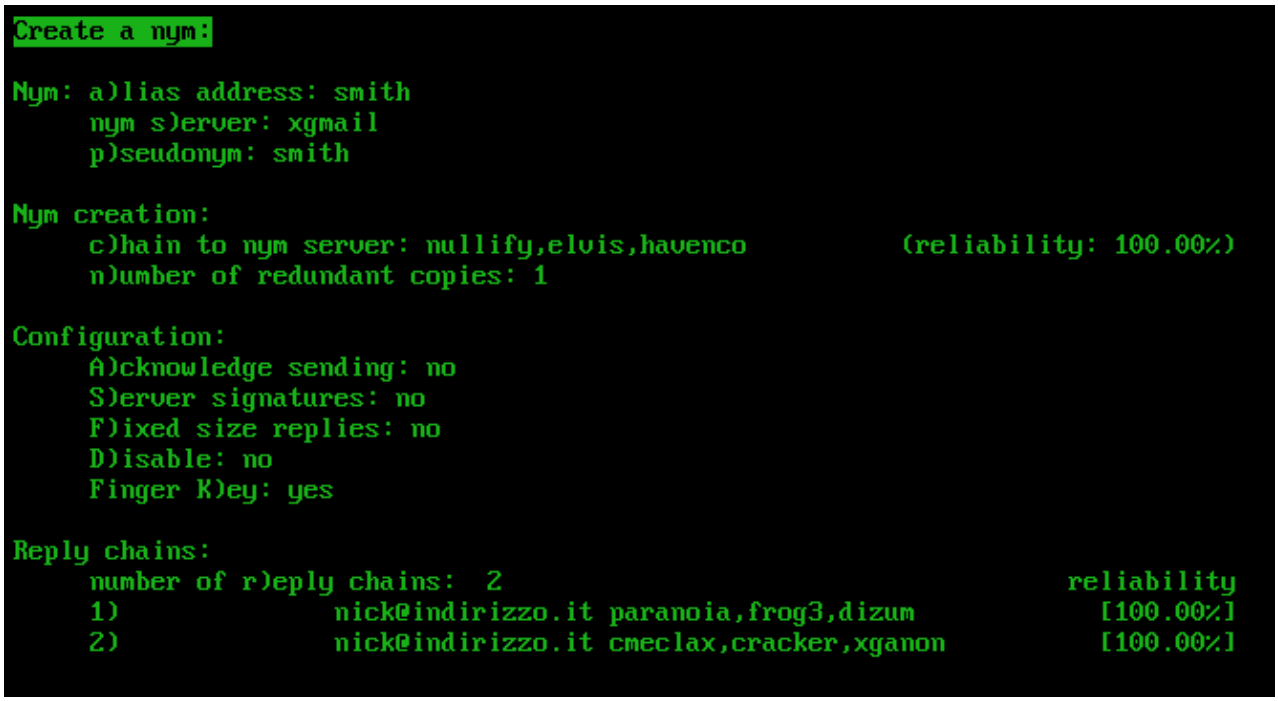
Poi abbiamo la terza sezione (Configuration): si possono definire parametri generali non critici come la possibilità di ricevere un avviso ogni qual volta spediamo un messaggio etc. etc., per una spiegazione più approfondita leggetevi la traduzione in italiano della guida del nym server su http://www.ecn.org/crypto/crypto/

E infine la quarta e più importante sezione, quella del reply block vero e proprio. Innanzitutto è possibile specificare più di un reply block, questo per usare magari 2 diverse catene di remailer in modo che se una non funzioni comunque non rischiamo di perdere i messaggi. Se funzionano entrambe riceveremo 2 copie dei messaggi ma il client le riconosce e ce ne mostrerà solo una.

Io consiglio di usare 2 catene di remailer che non abbiano remailers in comune. Quindi iniziamo premendo "r" e digitando "2" Dopodiche premendo "1" per impostare la prima catena, ci ritroviamo nella schermata precedente, in cui dobbiamo stabilire la destinazione dei messaggi premendo "d" e digitando il proprio indirizzo e-mail), e la catena (chain) digitando "c" e selezionando qualche remailer (3 è un buon numero).

Poi premiamo di nuovo invio per ritrovarci nella schermata di configurazione della figura 2, a questo punto si vedrà la catena del reply block n.1 impostata, e premendo "2" potremo definire anche la seconda come abbiamo fatto in precedenza.

Tornando alla schermata della configurazione premendo invio vedremo qualcosa di simile a questo, con le varie catene impostate:



Configurazione nym

A questo punto premendo invio vi viene chiesta una password per creare le chiavi necessarie,e viene preparato il messaggio da spedire al server. (vedrete che nella schermata iniziale apparirà il numero "1" di fianco all'indicatore dei messaggi presenti nel pool). A questo punto basta che premete "s" per spedire il messaggio se siete collegati in rete o se avete un smtp in funzione sulla vostra macchina che mette in coda il messaggio, oppure aspettate di entrare in rete e poi digitate:

/Mix/mix -S per spedire i messaggi presenti nel pool.

La richiesta è partita, e nel giro di poche ore dovrebbe arrivarvi un messaggio di conferma.

l client del mixmaster è "in attesa" di questo messaggio, quindi quando vi arriva un messaggio criptato che voi non riuscite a decriptare, dovete darlo in pasto al client.

Per fare ciò avviate il client, e poi selezionate "r" per leggere i messaggi presenti in una mailbox.

Dategli il percorso giusto della mailbox dove sono conte nuti i messaggi criptati, e lui li decritterà rendendoli disponibili per la lettura.

Se avete impostato reply block multipli e vi arrivano 2 copie dei messaggi, una sarà eliminata automaticamente.

Una volta usciti dal client del mixmaster , se riaprite la vostra mailbox con il vostro solito programma di posta ci troverete dentro i messaggi decrittati.

Se invece vi arrivano messaggi a cui volete rispondere usando un vostro nym come mittente potete seguire la procedura descritta prima, ossia rispondere al messaggio avendo cura di specificare il nym con cui volete rispondere, basta che selezionate con il tasto "n" un nym, altrimenti di default è impostata la modalità "anonymous" che vi permette di risponde re usando semplicemente i remailer e non il nym.

2. Il remailer mixmaster

Installazione e configurazione di un remailer mixmaster

2.1 Preparazione all'installazione da sorgenti (versione 2.9.0)

Creare un nuovo utente e chiamatelo ad es. anon

adduser anon

Verificare di avere installati sul proprio sistema sia GPG che PGP 2.6.3i per gestirsi chiavi DH e RSA.

Se utilizzate debian volendo esiste il pacchetto già compilato

Se invece volete compilarvelo come utente anon scaricare il file mixmaster-2.9.0.tar.gz dal sito http://www.sourceforge.net/projects/mixmaster nella home directory dell'utente anon (e scaricare anche la signature per verificare l'autenticità del file) e decomprimere il pacchetto:

tar xzvf mixmaster-2.9.0.tar.gz

cd mixmaster-2.9.0

Eseguire il comando ./Install e rispondere alle domande con le scelte che trovate nel log di installazione che segue.
Tra parentesi tonda trovate dei commenti.

2.2 L'installazione vera e propria

Attenzione: molte distribuzioni linux hanno una versione di openssl senza il supporto per l'algoritmo idea. Questo impedisce al remailer di generare una chiave RSA.
In questo caso potete scaricare il file openssl-0.9.7.tar.gz dal sito http://www.openssl.org e copiare la directory openssl-0.9.7 contenuta nel pacchetto nella directory Src/ che è una sottodirectory di mixmaster-2.9.0
In questo modo il supporto idea sarà inserito nel client del mixmaster anche se il vostro sistema non ha il supporto per idea.

```
# ./Install

 Mixmaster directory? [/home/anon/Mix]
 Do you want to set up a remailer? [y]
 Do you want to compile the passphrase into the binary? [n]
 Use the source if the pre-installed library causes compilation problems.
 Use source? [n]

 (Le domande che seguono sono parametri che andranno nel file mix.cfg
 che potrà comunque essere modificato in seguito)

 Install as middleman? [n]
 (i remailer middleman accettano e inviano posta solo ad altri remailer;
 questa modalità può essere utile ad es. nel caso in cui il remailer sia
 usato da qualcuno per fare spamming e l'operatore subisca pressioni per
 chiuderlo.)

 The e-mail address of your remailer:
 (inserite l'indirizzo del vostro remailer)

 Do you want Mixmaster to send auto-replies to messages it does not
 understand (If the address <anon@esempio.it> is also used
 for mail to be read by a human, type `n')? [y]
 (se si attiva questa opzione il mixmaster risponderà con un messaggio
 di spiegazioni alle e-mail che non interpreta come messaggi correttamente
 inviatigli nel formato mixmaster (altre spiegazioni più sotto)).

 An address to appear in the `From:' line of anonymous messages:
 (inserite l'indirizzo che deve comparire come mittente
 dei messaggi che transitano dal vostro remailer; di solito si usa nobody)

 Address for complaints to be sent to:
 (è buona definire un indirizzo come abuse che sarà l'indirizzo usato per
 inviare lamentele all'operatore).

 Choose a name for your remailer.  It will appear in remailer status messages.
 Long name: [Anonymous Remailer]

 Choose a name to be used in the `From:' line of remailed messages.
 Anon long name: [Anonymous]

 A short name to appear in lists:
 (questo sarà il "nome" del remailer con il quale sarà definito nelle liste
 pubbliche dei remailer attivi; è importante che non sia più lungo di
 8 caratteri e che non contenga lettere maiuscole).
```

```
Accept Mixmaster (Type II) messages? [y]
(per accettare messaggi nel formato mixmaster (type II) )

Accept PGP (Type I) remailer messages? [y]
(per accettare messaggi nel formato cypherpunk (type I) )

Mixmaster will log error messages and warnings. Do you want to log
informational messages about normal operation as well? [y]
(il remailer non logga gli IP, però può generare dei log
riguardo la sua attività, problemi, errori e operazioni compiute,
utile soprattutto nella fase iniziale di debug)

Filter binary attachments? [y]

Allow users to add themselves to the list of blocked addresses? [y]
(il remailer controlla se l'indirizzo di destinazione di un messaggio
è presente in un file di testo, e in caso affermativo non lo spedisce;
se un utente riceve spamming dal remailer può chiedere che l'operatore
lo inserisca nella block list, oppure può farlo da solo se questa
opzione è attivata).

Do you want to allow posting? Newsgroups can be restricted in dest.blk.
y)es, post locally; use m)ail-to-news gateway; n)o.
Allow posting to Usenet? [m]

Mail-to-news gateway: [mail2news_nospam@nym.alias.net]

Pool size: [20]
(se arriva un messaggio finisce nel pool e ne esce dopo tot tempo, tanto
maggiore quanto più è grande il pool dei messaggi, se però è troppo
grande possono esserci problemi di latenza perchè i messaggi restano
troppo nel pool prima di uscire; un valore basso è utili per le prove).

Mailbox for non-remailer messages: [/home/anon/Mix/mbox]
(mailbox per i messaggi che il remailer non riconosce perchè non
contengono istruzioni di remailing)

Set .forward to the following line:
"|/home/anon/Mix/mix -RM"
Do that now? [n]
(potete scegliere se usare questo formato oppure dire no e usare procmail
che è più versatile, spiegato più avanti)

Risposte automatiche impostate:
Mail to <anon@esempio.it> with Subject: remailer-help => help.txt
Mail to <anon@esempio.it> with Subject: remailer-adminkey => adminkey.txt
Remember to add your Remailer Admin public PGP key to the adminkey.txt file.
Mail to <anon@esempio.it> with line DESTINATION-BLOCK => blocked.txt
Other mail to <anon@esempio.it> => usage.txt

If you arrange for mail to <abuse@esempio.it> and <nobody@esempio.it>
to be forwarded to <anon@esempio.it>:
Mail to <abuse@esempio.it> => abuse.txt
Mail to <nobody@esempio.it> => reply.txt

Mixmaster installation complete.
```

2.3 Installazione del pacchetto debian precompilato

Se volete evitare la compilazione esiste per debian il pacchetto mixmaster

Una volta installato con "apt-get install mixmaster" verrà creato l'utente mixmaster.

Ora modificate il file di configurazione /var/lib/mixmaster/Mix/mix.cfg (che è un symlink che punta a /etc/mixmaster/remailer.conf).

per la spiegazione delle varie voci vedete il capitolo precedente e la man page di mixmaster, la cosa più importante è che definiate la PASSPHRASE, altrimenti le chiavi non saranno generate.

dopo averlo modificato create i msg usati dal remailer per rispondere in automatico ad alcune richieste:

/usr/lib/mixmaster/mixmaster-rebuild

e generate le chiavi:

mixmaster -G

questo dovrebbe creare sia la chiave mixmaster che la chiave gpg

In /etc/mixmaster sono contenuti alcuni file di configurazione:

allpingers.txt - lista dei pinger che raccolgono le statistiche dei remailer

client.conf - configurazione del client del remailer

filter.conf - qui si definisce quali header il remailer deve filtrare/accettare

network.conf - il contenuto della variabile network definita in questo file determina quando vengono aggiornate le statistiche e le chiavi dei remailer (tramite l'esecuzione di mixmaster-update, uno script eseguito giornalmente con cron). se la variabile NETWORK è impostata a "PPP" questo avviene ogni volta che si entra in rete (utenti con modem classico) se si imposta come "permanent" questo avviene giornalmente (utenti con connessione fissa) se non si imposta non viene mai fatto l'aggiornamento in automatico

update.conf - quì si definisce il pinger da cui prelevare le statistiche

sistemate i permessi dando un

chown -R mixmaster.mixmaster /var/lib/mixmaster

2.4 Post-installazione

A questo punto come root dobbiamo impostare in /etc/postfix/aliases (questo dipende dal vostro MTA) due alias di posta per far arrivare all'utente anon i messaggi destinati ad abuse e nobody, e anche quelli per il remailer-admin.

```
abuse: mixmaster
nobody: mixmaster
```

```
remailer-admin: mixmaster
```

e lanciare il comando postalias /etc/postfix/aliases per aggiornare il database degli alias

Ora il remailer dovrebbe funzionare, ma bisogna fare ancora qualcosa prima di renderlo pubblico in modo che sia utilizzabile in catena:

Nel file mix.cfg sono anche definite le mailbox dove vengono salvati i msg errati (ad es. non crittati con la chiave del remailer), messaggi che vanno in bounce, richieste per l'utente abuse, errori vari e richieste di blocco delle persone che non vogliono che il remailer gli mandi i messaggi.

Per avere le mailbox facilmente accessibili con mutt bisogna impostare nel file .muttrc dell'utente anon:
set folder=~/Mix
Le mailbox saranno poi accessibili con mutt inserendo nel file .muttrc una riga come questa :
mailboxes +mbox.mix +mbox.abuse +mbox.block etc. etc.

Il remailer va annunciato alla lista dei remailer operators remops@remailer.org.uk
remailer-operators@anon.lcs.mit.edu e al newsgroup alt.privacy.anon-server

Se si sceglie di gestire con procmail i msg in ingresso si devono mettere queste istruzioni nel .procmailrc dell'utente mixmaster:

```
:0
*
"|/usr/bin/mixmaster -RM"
```

Se usate il pacchetto debian ricordatevi di riavviare il servizio mixmaster ogni volta che modificate il file mix.cfg e anche di eseguire mixmaster-rebuild, di modo che le risposte automatiche siano ricostruite.

2.5 Tenere il remailer dentro un file system crittato

Un remailer dovrebbe sempre essere ben protetto, quantomeno le chiavi. E' possibile crittare tutto il disco, oppure scegliere di crittare solo alcune parti del remailer in modo da avere un piccolo file container crittato che contenga i dati più sensibili. Se scegliete questa seconda opzione quì di seguito trovate una breve spiegazione di come fare:

Innanzitutto, studiatevi come si crea un container crittato con dmcrypt (potete trovare una piccola guida in questo stesso sito).

La dimensione del container dipende da cosa volete tenerci, il remailer inizialmente non occupa molto spazio, pochi Mb. Sono due le cose che possono occupare molto spazio: innanzitutto il pool dei messaggi, e secondariamente le mailbox dei messaggi di errore (soprattutto se non vengono controllate giornalmente).

Supponiamo di voler mettere nel container quello che sta dentro /var/lib/mixmaster:

Copiate il contenuto di /var/lib/mixmaster in una directory temporanea, a questo punto create un container crittato e montatelo in /var/lib/mixmaster.

Copiateci i file originariamente presenti in /var/lib/mixmaster

Il file /var/lib/mixmaster/Mix/mix.cfg è un symlink che punta a /etc/mixmaster/remailer.conf

Visto che in questo file è contenuta la passphrase della chiave del remailer è meglio eliminare il symlink e spostare questo file nel container crittato:

```
# cd /var/lib/mixmaster/Mix
# rm mix.cfg
# mv /etc/mixmaster/remailer.conf ./mix.cfg
# ln -s /var/lib/mixmaster/Mix/mix.cf /etc/mixmaster/remailer.conf
```

ora, in questo modo il pool del remailer è anch'esso contenuto nel container crittato, questo può causare problemi di carico e di spazio, volendo si può spostare il pool in /var/spool/mixmaster ad esempio e fare un symlink a questa directory.

Create uno script per montare il container all'avvio, che faccia partire anche postfix (e disabilitate l'avvio automatico di postfix che non deve partire finchè il container non è montato).

E' possibile sfruttare il container per tenerci anche la chiave TLS di postfix e se sulla stessa macchina girano altri servizi anche le chiavi di questi ultimi.

Questo è un esempio dello script per debian, da mettere in /etc/init.d :

```
#!/bin/sh
#
# monta la partizione crittata e avvia i servizi che ne abbisognano.
#


# immagine da montare
image_file=/root/mixmaster_container.img

# posti dove montarla
targets="/var/lib/mixmaster"

# servizi che dipendono dal container crittato
aux_svc="postfix mixmaster mixminion"

# nome del device mapper
devicem="secret"

# file di stato (memorizza quale fosse il loop device)
LOOPDEVFILE=/var/run/certs.loopdev


test -e $image_file || exit 1
test -x /sbin/cryptsetup || { echo "Install the 'cryptsetup' package." ; exit 1 ; }
test -e /proc/crypto || { echo "Install crypto support in the kernel." ; exit 1 ; }


case "$1" in

start)

        loop_device=`losetup -f`
        test -e $loop_device || exit 1

        echo $loop_device > $LOOPDEVFILE

        losetup $loop_device $image_file || exit 1
```

```
        # dmcrypt
        echo "Starting encryption..."
        /sbin/cryptsetup -c aes -s 256 -h ripemd160 create $devicem $loop_device
        if [ $? -gt 0 ]; then
          echo
          echo "ERRORE - cryptsetup fallito."
          exit 127
        fi

        # mount partition
        echo -n "Mounting decrypted partition..."
        for mp in $targets
        do
          echo -n " $mp"
          mount -o rw,exec /dev/mapper/$devicem $mp
        done
        echo "."

        # controllino, evitiamo casini coi servizi che partono a muzzo
        if ! test -e /var/lib/mixmaster/Mix/secring.mix ; then
          echo "ERROR - something went wrong"
          exit 1
        fi

        # start more services
        echo "Starting more services..."
        for s in $aux_svc
        do
          invoke-rc.d $s start
        done

        ;;


stop)

        if [ ! -e $LOOPDEVFILE ]; then
          echo "No crypto partition state file found... Unmount by hand."
          exit 3
        fi
        loop_device=`cat $LOOPDEVFILE`
        if [ "x$loop_device" = "x" ]; then
          echo "Crypto partition state file is corrupted."
          exit 4
        fi

        echo "Stopping services depending on encrypted container"
        for s in $aux_svc
        do
          invoke-rc.d $s stop
        done

        echo -n "Unmounting partitions... "
        for mp in $targets
        do
          echo "$mp "
          umount -f $mp 2>/dev/null
        done
        echo "."

        echo -n "Stopping encryption..."
```

```
        /sbin/cryptsetup remove $devicem
        echo "done."

        losetup -d $loop_device

        ;;


reload)

        # fast restart, non scomoda i servizi
        echo -n "Re-mounting partitions..."
        for mp in $targets
        do
          echo -n " $mp"
          umount -f $mp 2>/dev/null
          mount -o rw,exec /dev/mapper/$devicem $mp

        losetup -d $loop_device

        ;;


reload)

        # fast restart, non scomoda i servizi
        echo -n "Re-mounting partitions..."
        for mp in $targets
        do
          echo -n " $mp"
          umount -f $mp 2>/dev/null
          mount -o rw,exec /dev/mapper/$devicem $mp
        done
        echo "."

        ;;


*)
        echo "$0 {start|stop|reload}"

esac


exit 0
```

2.6 Il remailer operator (remop)

Bisogna creare una chiave PGP/GPG che avrà uno user-ID remailer-admin@esempio.it, con questa chiave si firmeranno tutti i messaggi postati nella mailing list dei remailer-operators.

Bisogna creare l'utente remailer-admin@esempio.it in /etc/aliases che verrà indirizzato all'utente mixmaster

Per firmare tutti i msg in uscita dalla mailbox, usando mutt come client di posta di può impostare il .muttrc in questo modo:

```
my_hdr From: remailer-admin@esempio.it
set pgp_autosign
```

```
set pgp_sign_as="remailer-admin@esempio.it"
my_hdr X-PGP-Key-fingerprint: A9 32 4A CB 3C 4B 5D DA  AB 34 BC A6 4D C8 44 5C
set realname="remailerX Admin"
```

la chiave del remop va esportata nel file /Mix/adminkey.txt (se usate il pacchetto debian va messa in /etc/mixmaster/remailer/adminkey.txt), in modo che venga inviata a chi ne fa richiesta con un messaggio all'indirizzo del remailer con il subject "remailer-adminkey"

Inoltre è buona norma firmare con la chiave del remop la chiave gpg del remailer.

Potete importare la chiave del remailer nel pubring dell'utente mixmaster, firmarla ed esportarla:

gpg --import /var/lib/mixmaster/Mix/pgpkey.txt

gpg -u remailer-admin@esempio.it --sign-key mixmaster@esempio.it

gpg -a --export mixmaster@esempio.it > /var/lib/mixmaster/Mix/pgpkey.txt

2.7 Tips and tricks

Bounces

Può capitare che un remailer abbia dei problemi e quindi i messaggi destinati a lui vadano in bounce per qualche giorno. Quando il remailer torna online dobbiamo rimandargli tutti i messaggi, e per facilitare questa operazione potete usare questo script:

Resend

Dopo aver salvato in un file in formato mailbox tutti i messaggi, lanciando lo script con questa sintassi:

./resend file_mailbox indirizzo_del_remailer

i messaggi saranno rispediti.

Bloccare lo spam

Oltre ai soliti filtri a livello dell'MTA esistono diversi script per cercare di limitare lo spam. Uno dei più interessanti e sicuramente il Nilsimsa, che potete trovare a questo indirizzo:

http://ixazon.dynip.com/~cmeclax/nilsimsa.html

In pratica controlla che nel pool del mixmaster non ci siano dei messaggi che si "somigliano" oltre una certa soglia, e nel caso li mette in quarantena in attesa di essere esaminati.

E' un tool molto utile, anche se appesantisce un pò il lavoro di remailer administrator perchè poi i messaggi in quarantena vanno esaminati.

Fondamentalmente nilsimsa controlla se i messaggi che arrivano al remailer sono molto simili tra di loro, e se lo sono li cataloga come flood e li mette in quarantena, in attesa di essere esaminati e approvati/respinti.

scompattate il file nilsimsa-0.2.4.tar.gz nella home dell'utente che controlla il remailer, ad esempio /home/anon

tar zxvf nilsimsa-0.2.4.tar.gz

che creera' la directory nilsimsa-0.2.4; entratevi e date i comandi

./configure && make

Potrebbe verificarsi un errore per la mancanza di termio.h, in questo caso dovete installare la libreria ncurses-dev.

Potete non effettuare il make install, previsto dalle istruzioni di installazione, per evitare la necessita' di avere le permission di root e mantenere tutti i file del remailer nella directory /home/anon

rinominate la directory

mv nilsimsa-0.2.4 nilsimsa

entrate nella directory nilsimsa/scripts ed editate i 3 script che vi si trovano, dando la path assoluta; in pratica, in tutte le righe che iniziano con

nilsimnsa .....

inserite la path all'inizio

/home/mix/nilsimsa/scripts/nilsimsa .....

Create la directory festi in /home/anon/Mix

cd /home/anon/Mix mkdir festi

facendo attenzione che abbia gli stessi permessi della directory pool

Con nilsimsa viene distribuito uno script (**finddups**) che va eseguito spesso, nel nostro caso noi lo facciamo girare ogni 2 minuti sul pool dei messaggi.

*/2 * * * * /Mix/nilsimsa/scripts/finddups

Se avete un POOL troppo piccolo o se avete impostato un SENDPOOLTIME troppo basso o un RATE troppo alto nel mix.cfg potreste avere problemi, nel senso che i messaggi potrebbero entrare ed uscire dal pool prima che nilsimsa li possa controllare.

Questo job lancia lo script finddups, che scandisce i file della directory pool (i messaggi del remailer) e sposta nella directory festi gli eventuali gruppi di messaggi molto simili. Inserisce poi nel file /home/mix/Mix/rules una riga che contiene l'impronta del gruppo di file spostati e la lettera "D". Questa riga provochera' lo spostamento di eventuali altri file simili che giungessero successivamente, anche se arrivassero uno per volta.

La directory festi tendera' quindi a riempirsi; usando a mano lo script catsimsa, a cui dovete fornire come argomento una intera liea del file rules, potete visualizzare i file relativi, per decidere se sono da gettare (spam, flood ..) oppure se sono legittimi (ad es. i ping dei pinger echolot)

Nei primi tempi dovrete provare ogni nuova riga di rules, per vedere se i messaggi sono dei ping; quando ne trovate uno, modificate la riga relativa sostituendo "D" con "A".

Potete anche aggiungere un commento aggiungendo un cancelletto a fine riga, e proseguendo con il commento vero e proprio. Attenzione a conservare lo spazio bianco che c'e' a fine riga; il cancelletto inseritelo dopo.

Rimettete poi i messaggi legittimi in pool con lo script mvsimsa, a cui come al solito va fornita la relativa riga di rules come argomento.

Ripetete l'operazione per tutte le nuove righe di rules (vi conviene inserire un commento per distinguere quelle che avete testato dalle altre che verranno aggiunte in futuro)

A questo punto cancellate tutti i file rimasti nella directory festi.

Durante un flood, su un remailer pienamente operativo possono essere generati anche 100Mb di file al giorno, sia nella directory festi, che nella mailbox dell'utente mix che nei file /home/anon/Mix/mbox.xxxx.

Oltre ai due scripts catsimsa e mvsimsa che aiutano nell'utilizzo di nilsimsa, io uso anche questi due:

delsimsa, per eliminare una serie di messaggi con lo stesso "nilsimsa code", o come in questo caso per parcheggiarli in una directory apposita.

```
#!/bin/sh
# delsimsa <nilsimsa code> <threshold>
cd ~/Mix/festi
~/Mix/nilsimsa -c $1 -t $2 ~/Mix/festi/m* | grep ^1 | cut -c 3- | \
 xargs -i mv {} ~/Mix/festi/deleted/
```

checksimsa, per avere una lista di tutti i file ordinati secondo il loro "nilsimsa cose", in questo modo è più semplice individuare i gruppi di file identici.

```
#!/bin/sh
cd ~/Mix/festi
~/Mix/nilsimsa -v -H ~/Mix/rules ~/Mix/festi/m* | sort -k 3
```

Se un remailer cambia IP ma il DNS non si aggiorna

Quando un remailer cambia IP ma il DNS non si aggiorna i messaggi per quel remailer vanno in bounce.

Si può però forzare l'MTA a spedire i messaggi destinati ad un certo indirizzo non all'MX per quel dominio ma direttamente ad un indirizzo IP, senza passare dal DNS.

Se utilizzate postfix la procedura è questa:

```
file /etc/postfix/transport:

| cypherpunks.to                smtp:[213.130.163.34]
```

In questo caso le mail per il dominio cypherpunks.to vengono spedite direttamente alla porta 25 dell'IP 213.130.163.34

Poi nel file /etc/postfix/main.cf definite la transport map:

transport_maps = hash:/etc/postfix/transport

e poi come root ricostruite la transport map

postmap /etc/postfix/transport

Fare un upgrade delle chiavi del remailer

Ogni tanto le chiavi del remailer andrebbero sostituite con chiavi nuove.Per iniziare fatevi una copia dei vari keyring

Generate una nuova coppia di chiavi con

$ mix -G

Questo generera' nuove chiavi mixmaster, RSA e DH. Controllate di avere due chiavi nel file secring.mix, e spostate la chiave nuova in cima al file, spostando la vecchia sotto.

Eliminate il file key.txt e richiedete la chiave al remailer, lui rigenerera' il file con la nuova chiave pubblica ricostruendola dalla chiave privata.

Passiamo ora alle chiavi PGP/GPG:

Quando e' stata (o sono state, se avete anche la chiave RSA) prodotta la chiave, il file pgpkey.txt si dovrebbe essere aggiornato con le nuove chiavi.

Con questo comando:

$ gpg --no-default-keyring --secret-keyring ./secring.pgp --list-secret-keys

dovreste vedere sia le vecchie che le nuove chiavi con un output simile a questo:

```
./secring.pgp
-------------
sec  1024D/07BF4D7E 2002-09-29 Anonymous Remailer <anon@esempio.it>
ssb  1024g/B0C9007C 2002-09-29

sec  1024R/485671B1 2003-03-18 Anonymous Remailer <anon@esempio.it>

sec  1024R/495574F5 2003-03-18 Anonymous Remailer <anon@esempio.it>

sec  1024D/FBEED8AF 2003-03-18 Anonymous Remailer <anon@esempio.it>
ssb  1024g/D539A465 2003-03-18
```

l'ordine e' cronologico, in cima la chiave piu' vecchia, in fondo l'ultima generata.

Stessa cosa per il file pgpkey.txt

Ricordate che se cancellate il file pgpkey.txt, richiedendo la chiave al remailer con un messaggio dal subject "remailer-keys" il file sara' ricreato partendo dalle chiavi private presenti nel file secring.pgp

Annunciate il cambio di chiavi e postate le nuove chiavi sulla lista dei remailer operators e nel newsgroup alt.privacy.anon-server

Quindi eliminate dal file pgpkey.txt le vecchie chiavi, in modo che chi richieda le chiavi al remailer ottenga solo le chiavi nuove.

Dopo un paio di settimane eliminate le vecchie chiavi dai keyrings, in genere la cosa migliore e' fare un:

$ gpg --no-default-keyring --secret-keyring ./secring.pgp --delete-secret-keys keyID

dove KeyID e' il keyID della chiave che volete eliminare.

Firmare le nuove chiavi con le vecchie chiavi

Quando si generano nuove chiavi e' buona norma firmarle con la chiave del remailer administrator e con le vecchie chiavi. Supponendo che la chiave del remailer operator sia nel keyring dell'utente anon, importate le nuove chiavi pubbliche del remailer:

$ gpg --import pgpkey.txt

$ gpg --secret-keyring ./secring.pgp -u remailer_admin_keyID --sign-key new_remailer_keyID

$ gpg --secret-keyring ./secring.pgp -u old_remailer_keyID --sign-key new_remailer_keyID

In questo modo abbiamo importato le nuove chiavi, e le abbiamo firmate con la chiave del remailer admin e con le vecchie chiavi del remailer.

(la password delle vecchie (e nuove) chiavi e' scritta nel file mix.cfg)

Adesso esportiamo le chiavi firmate

$ gpg --export -a new_remailer_keyID > pgpkey.txt

Statistiche del remailer

Potete tener d'occhio come funziona il vostro remailer visitando queste pagine:

http:/www.noreply.org/

oppure createvi un vostro pinger installando il programma echolot.

2.8 Creare una pagina di statistiche del remailer

Per costruire una pagina che riassuma un po' di statistiche del remailer mi sono appoggiato a diversi script, molti dei quali scritti dall'admin del remailer arancio che ora e' chiuso e quindi gli script non sono piu' disponibili dal suo sito, quindi li riporto qui', modificati quel tanto che basta per adattarli al remailer paranoia.

Questo e' il crontab dell'utente anon:

```
# preleva le statistiche dei remailer ogni 6 ore.
```

```
0 */6 * * *     anon    /home/users/anon/scripts/getmix2.sh 2>/dev/null

# ogni ora richiede le statistiche al remailer
1 * * * *       anon    echo "ping" | /usr/bin/mail -s "remailer-stats" \
   anon@paranoici.org > /dev/null 2>&1

# generazione statistiche remailer
21 * * * *     anon     /home/users/anon/scripts/parse-stats.sh
25 */4 * * *   anon     /home/users/anon/scripts/stat2html.sh
10 0 * * *     anon     /home/users/anon/scripts/message-counter.sh
```

getmix2.sh viene lanciato ogni 6 ore e scarica chiavi e statistiche dei remailer da un sito (a scelta), potete anche indicarne uno non presente nel file, una lista dei pinger funzionanti si trova qui':

http://www.noreply.org/allpingers/

Ogni primo minuto di ogni ora viene mandata una mail al remailer richiedendo le sue statistiche, nel .procmail dell'utente anon c'e' poi questo:

```
:0 :
* ^From: Paranoia Remailer <anon@paranoici.org>
* ^Subject: Statistics for the paranoia remailer
/home/users/anon/tmp/stats-tmp
```

quindi le statistiche vengono salvate in /home/users/anon/tmp/stats-tmp

parse-stats.sh alle 3 di notte genera dal file stats-tmp due file, uno e' /home/users/anon/stats/remailer-stats.txt, che verra' usato da message-counter.sh, l'altro e' /home/users/anon/tmp/remailer-stats.txt da cui saranno prelevati i dati per i grafici di mrtg

message-counter.sh questo script lanciato ogni giorno alle 00:10 legge i dati delle statistiche e crea una tabella html (/home/users/anon/stats/messages.html) con il numero di messaggi processati dal remailer, divisi in cpunk, mix e totali.

stat2html.sh questo script viene lanciato ogni 4 ore, preleva le statistiche del nostro remailer da 5 diversi pinger (l'affidabilita' espressa in % e la latenza), mostra i dati giornalieri in una tabella html per i singoli pinger e calcola la media. Crea anche i file di testo che saranno poi utilizzati da MRTG per creare i grafici di questi dati, in modo che siano disponili su base giornaliera, settimanale, mensile e annuale. Puo' creare anche una tabella che evidenzia lo stato di salute generale della rete dei remailer.

Scripts:

getmix.sh

parse-stats.sh

stat2html.sh

message-counter.sh

3. Installare un'interfaccia web per il remailer

E' possibile scaricare dal server autistici.org una serie di script che consentono di installare un'interfaccia web per il remailer mixmaster.

Clicca quì per scaricare lo script dell'admin del remailer chicago

Clicca quì per scaricare lo script dell'admin del remailer riot

Clicca quì per scaricare lo script di cotse.net

Qui' di seguito trovate le istruzioni per l'installazione del primo dei tre.

e questo e' un archivio con la cartella di installazione del remailer modificato per il remailer paranoia:

Clicca quì per scaricare lo script dell'admin del remailer chicago modificato per funzionare sul remailer paranoia

Creo la directory /var/www/remailer/webmixmaster

sposto il file webscripts.tar.gz in /var/www/remailer/webmixmaster e lo decoprimo con:

$ tar -xzvf webscripts.tar.gz

Adesso devo modificare qualche file per adattarlo al mio sistema:

file: **gc**

riga 13: sostituisco il percorso con quello dove io ho installato lo script: cd /var/www/remailer/webmixmaster

commento le righe dalla 30 alla 34 perchè non voglio che i file type2.list e pubring.mix raccolti da questo script vadano a sovrascrivere quelli raccolti dal remailer mixmaster con un altro script. Quindi anche alla riga 22 tolgo il "&& \" finale perchè mi basta il wget che preleva il file mlist2.txt

riga 22: sostituisco con l'indirizzo di un pinger attivo (vedi http://www.noreply.org)

riga 50: sostituisco con: cat rems2 | awk '{print $1}' > rems3

riga 55: sostituisco con: cp rems3 /var/www/remailer/webmixmaster/rems

riga 65: sostituisco con: cp outdata /var/www/remailer/webmixmaster/data

riga 69: sostituisco con: cat output | grep Generated > /var/www/remailer/webmixmaster/current

riga 50: sostituisco rem2 con rem3

riga 55: sostituisco rem2 con rem3

file: **web**

riga 5: sostituisco rem2 con rem3

file: **send**

inserisco il percorso dove risiede l'eseguibile del remailer mixmaster: /home/anon/Mix/mix -S

file: **cgi-bin/mixemail-send.cgi**

riga 27: inserisco il percorso dell'eseguibile del mixmaster: $mix = "/home/anon/Mix/mix";

riga 243: sostituisco Chicago col nome del mio remailer

Ovviamente l'eseguibile del mixmaster dovrà essere accessibile all'owner del processo httpd, in genere è l'utente nobody, quindi occhio ai permessi.

file: **cgi-bin/mixnews-send.cgi**

vedi file precedente, stessa variabile da definire alla riga 27 e alla riga 257

file: **cgi-bin/mixemail-user.cgi**

imposto i percorsi dove si troveranno alcuni files delle statistiche:

riga 25: $current = "/var/www/remailer/webmixmaster/current";

riga 28: $data = "/var/www/remailer/webmixmaster/data";

riga 29: $rems = "/var/www/remailer/webmixmaster/rems";

riga 56: print "/var/www/remailer/webmixmaster/current");

file: **cgi-bin/mixnews-user.cgi**

vedi file precedente, bisogna definire i percorsi per le variabili current, data e rems, che sono alle righe 26, 29 e 30, e l'indicazione per il percorso del .cgi alla riga 56

poi c'è da impostare un cron che lanci lo script gc ogni ora:

0 */1 * * * /var/www/remailer/webmixmaster/gc > /dev/null 2>&1

il cron sarà quello dell'utente coi cui permessi gira apache, di solito www-data o nobody.

dare un chmod +x a tutti gli scripts per renderli eseguibili

infine bisogna lavorare su apache creando un virtualhost per webmixmaster.paranoici.org, uno per la porta 80 che rediriga sulla 443, perchè la connessione deve avvenire criptata in https, e uno appunto per la porta 443 che consenta l'esecuzione degli script cgi.

(per far questo va modificato anche il file apache2.conf decommentanto la riga:

AddHandler cgi-script .cgi

Quì sotto è riportato un esempio di file di configurazione per il virtualhost:

```
<VirtualHost *:80>

        ServerName webmixmaster.paranoici.org
        ServerAdmin info@autistici.org

        Redirect permanent / https://webmixmaster.paranoici.org
        #gira le connessioni http sull'https

< /Virtualhost>

<VirtualHost *:443>

        ServerName webmixmaster.paranoici.org
        ServerAdmin info@autistici.org

        SSLEngine on
        SSLCertificateFile /etc/ssl/certs/remailer.pem
        SSLCertificateKeyFile /etc/ssl/certs/remailer.pem

        <Files ~ "\.(cgi|shtml|phtml|php3?)$">
        SSLOptions +StdEnvVars
        < /Files>


        DocumentRoot /var/www/remailer/webmixmaster/

    ScriptAlias /cgi-bin/ /var/www/remailer/webmixmaster
    <Directory "/var/www/remailer/webmixmaster">
        AllowOverride None
        Options ExecCGI -MultiViews +SymLinksIfOwnerMatch
        Order allow,deny
        Allow from all
    < /Directory>
< /VirtualHost>
```

a questo punto basta creare un index.php da mettere nella DocumentRoot come quello qui' sotto che rediriga le richieste verso lo script cgi:

```
<?php
    header( 'Location: https://webmixmaster.paranoici.org/mixemail-user.cgi' );
    exit();
?>
```

e per concludere bisogna generare il certificato SSL per il virtualhost, ma per questo potete facilmente trovare istruzioni complete in rete,

e dovete istruire il DNS affinche' il virtualhost sia associato all'indirizzo IP del vostro server web.