

M O C A 2008

Introduzione all'uso dei remailer anonimi

Leandro Noferini - Inoferin@cybervalley.org



MOCA 2008

Di cosa parleremo

- Cosa sono i remailer anonimi
- Come funzionano
- Come si usano
- Altri servizi

Non parleremo della gestione di un remailer anonimo



MOCA 2008

Qual'è il problema

L'uso della cifratura nella posta elettronica non elimina completamente i problemi relativi alla privacy perché in ogni caso restano visibili

la quantità dei messaggi

la dimensione dei messaggi

data e ora di spedizione e ricevimento

partecipanti alla discussione



Cos'è un remailer anonimo

Un remailer anonimo è un programma che filtra i messaggi di posta elettronica che riceve per eliminare tutti gli header che permetterebbero l'identificazione del mittente del messaggio

Permette l'invio di:

messaggi di posta elettronica

articoli sui newsgroups (usando i gateway)

Nym



M O C A 2008

Tipi di remailer

- tipo I - cypherpunk
- tipo II - mixmaster
- tipo III - mixminion

Qui parleremo fondamentalmente dei remailer di tipo II mixmaster perché sono quelli attualmente maggiormente diffusi e affidabili



MOCA 2008

Caratteristiche comuni

Funzionano con la tecnica delle chiavi pubblica/privata

Usano la tecnica del trasporto di cipolle
onion routing

Si basano sull'

uso di tutta la rete dei remailer

Assicurano l'anonimato anche rispetto all'operatore
del remailer stesso

(seguendo correttamente le norme)



MOCA 2008

Funzionamento (tipi I e II)

- riceve il messaggio
- eventualmente lo decifra
- opera sul messaggio
- reinvia il messaggio

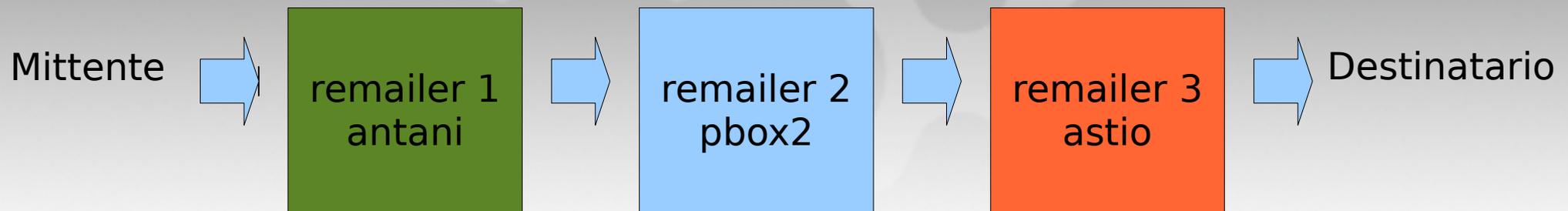
Funzionamento quasi tutto in automatico

LFG

MOCA 2008

Uso - linee generali

Il mittente sceglie la catena e ne scarica le chiavi pubbliche



MOCA 2008

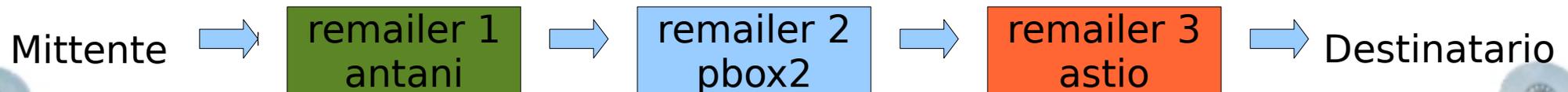
Uso - linee generali

Il mittente prepara il testo per il destinatario

richiesta per l'ultimo reloader di reinvio al destinatario finale

TESTO DEL MESSAGGIO

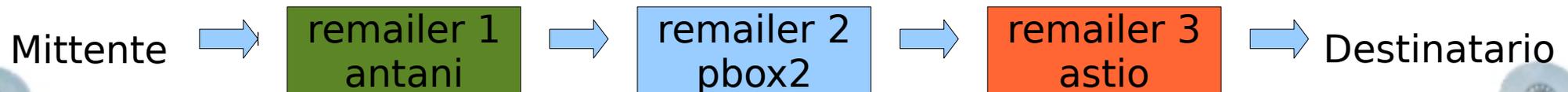
(puo' essere gia' crittato con la chiave del destinatario finale)



MOCA 2008

Uso - linee generali

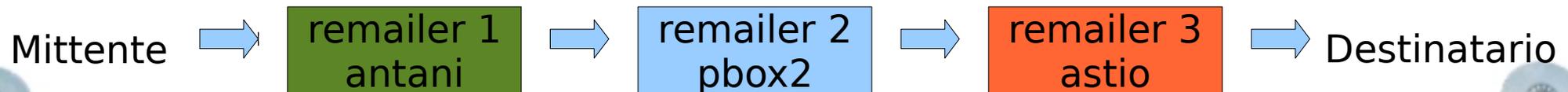
Il mittente cifra il testo usando la chiave dell'ultimo remailer



MOCA 2008

Uso - linee generali

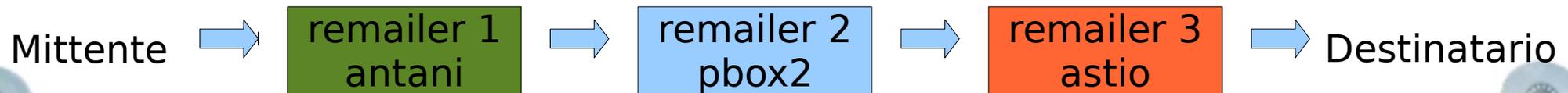
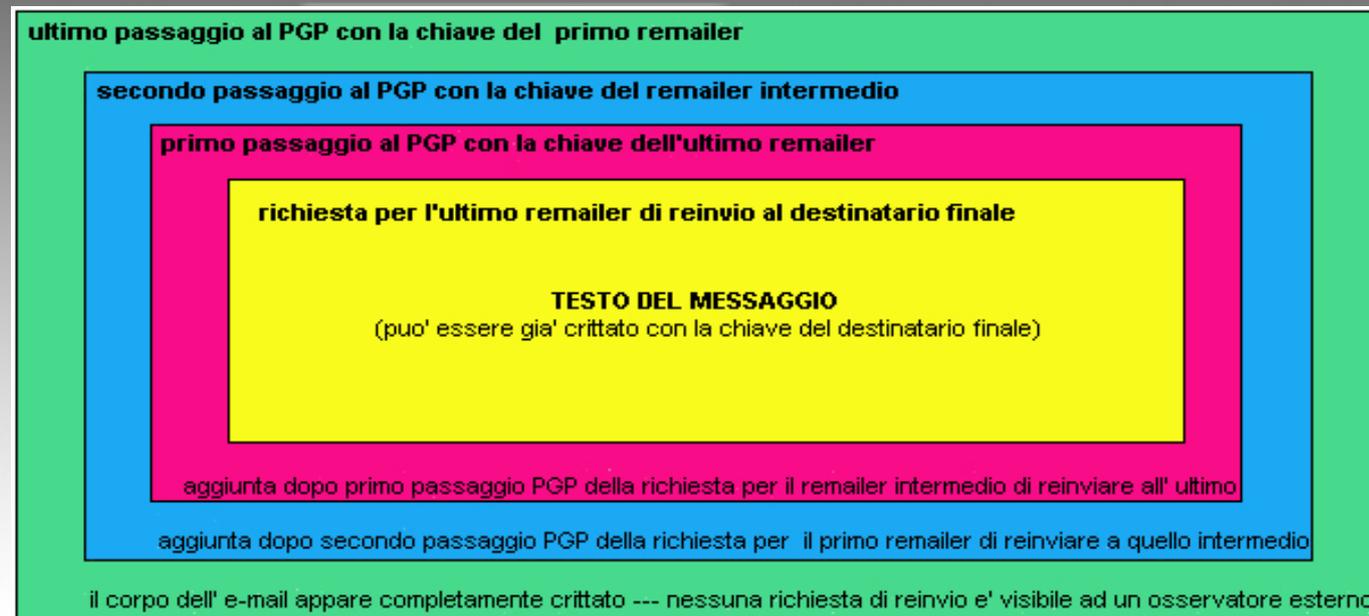
Il mittente cifra il messaggio ottenuto usando la chiave del remailer intermedio



MOCA 2008

Uso - linee generali

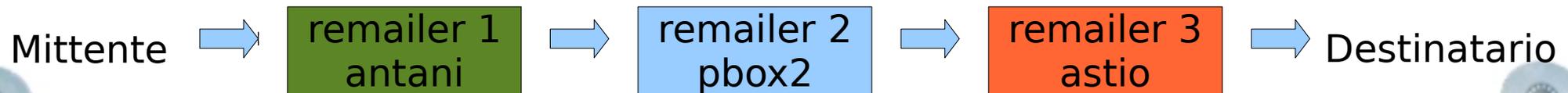
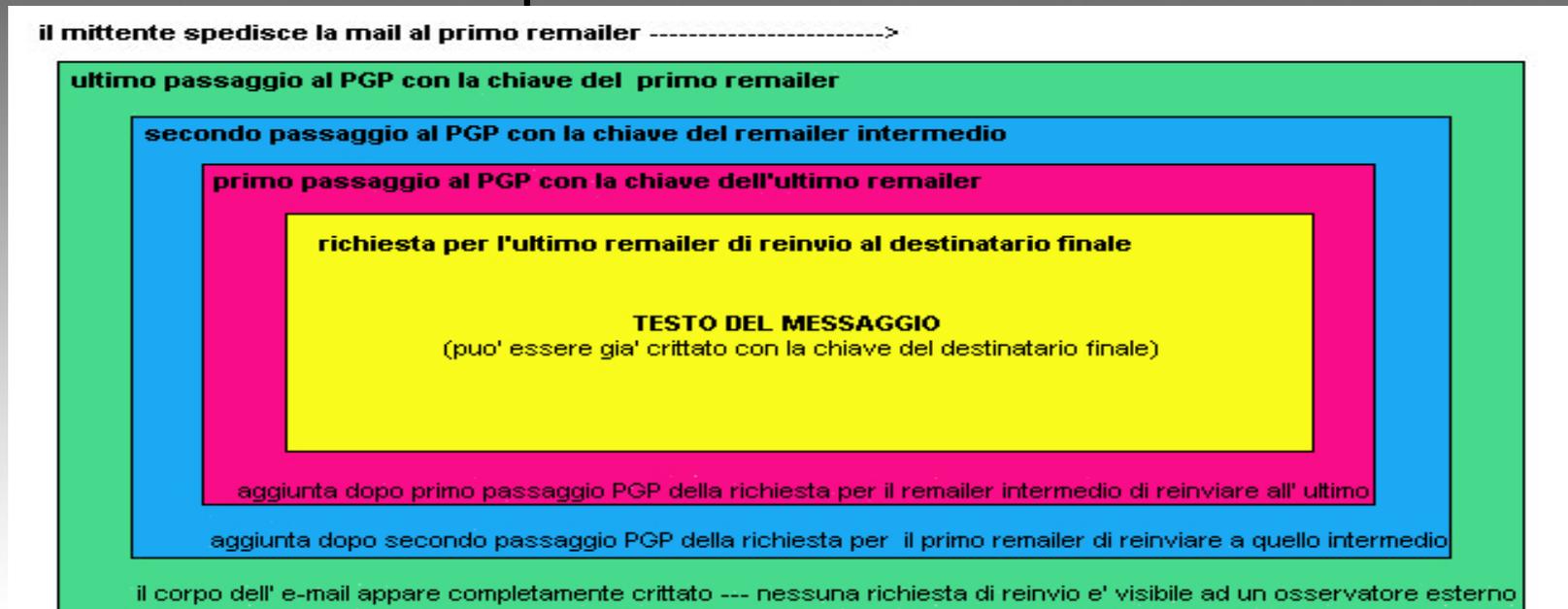
Il mittente cifra il messaggio ottenuto usando la chiave del primo remailer



MOCA 2008

Uso - linee generali

Il mittente spedisce il messaggio ottenuto verso il primo remailer



M O C A 2008

Questa è l'immagine originale dal libro Kryptonite

il mittente spedisce la mail al primo remailer ----->

ultimo passaggio al PGP con la chiave del primo remailer

secondo passaggio al PGP con la chiave del remailer intermedio

primo passaggio al PGP con la chiave dell'ultimo remailer

richiesta per l'ultimo remailer di reinvio al destinatario finale

TESTO DEL MESSAGGIO

(puo' essere gia' crittato con la chiave del destinatario finale)

aggiunta dopo primo passaggio PGP della richiesta per il remailer intermedio di reinviare all' ultimo

aggiunta dopo secondo passaggio PGP della richiesta per il primo remailer di reinviare a quello intermedio

il corpo dell' e-mail appare completamente crittato --- nessuna richiesta di reinvio e' visibile ad un osservatore esterno



M O C A 2008

Aspetto dei messaggi Messaggio normale

Received: by best123bingo.com (PowerMTA(TM) v3.5r6) id hfd8g80kg0kj for
<Inoferin@cybervalley.org>; M
on, 14 Jul 2008 09:13:35 -0400 (envelope-from <promotion@best123bingo.com>)
Date: Mon, 14 Jul 2008 08:44:02 -0400 (EDT)
From: Prism <promotion@best123bingo.com>
Reply-To: promotion@best123bingo.com
To: Inoferin@cybervalley.org
Message-ID: <8630945112345133056.1216039442333.EMail.promotion@best123bingo.com>

Subject: Diamond Forever
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
X-Mailer-MsgId: bG5vZmVyaW5AY3liZXJ2YWxsZXkub3Jn
X-Mailer-CSID: 17_909

```
<html>  
  <head>  
    <title></title>  
  </head>  
  <body topmargin=3D"0">  
    <table cellpadding=3D"0" cellspacing=3D"0" width=3D"550" align=3D"c=
```



M O C A 2008

Aspetto dei messaggi Messaggio da remailer

From: Borked Pseudo Mailed <nobody@pseudo.borked.net>

Comments: This message did not originate from the Sender address above.

It was remailed automatically by anonymizing remailer software.

Please report problems or inappropriate use to the
remailer administrator at <admin@pseudo.borked.net>.

To: e-privacy@firenze.linux.it

Message-ID: <9ec16233d60412f46b7ac4b5b9850a8f@pseudo.borked.net>

Date: Fri, 11 Jul 2008 03:36:04 -0600 (MDT)

X-Mailman-Approved-At: Sat, 12 Jul 2008 15:55:41 +0200

Subject: [e-privacy] Open WiFi Owners Off the Hook In Germany

MIME-Version: 1.0

Content-Type: text/plain; charset="iso-8859-1"

Content-Transfer-Encoding: quoted-printable

Sender: e-privacy-bounces@firenze.linux.it

Errors-To: e-privacy-bounces@firenze.linux.it

<http://news.slashdot.org/article.pl?sid=3D08/07/11/0346233>

[http://arstechnica.com/news.ars/post/20080710-open-wifi-network-viable-defe=
nse-against-infringement-chargeat-least-in-germany.html](http://arstechnica.com/news.ars/post/20080710-open-wifi-network-viable-defense-against-infringement-chargeat-least-in-germany.html)



MOCA 2008

Quanto detto fino ad adesso vale per i remailer di tipo I – cypherpunks

Vale solo in linea generale per i remailer di tipo II e III

Per questi è necessario l'utilizzo di un'interfaccia apposita



Uso dei remailer di tipo II mixmaster

Le interfacce possibili sono di due tipi

- per windows esistono due programmi che fanno da interfaccia grafica
- per gli altri sistemi operativi si deve usare il programma per il server usato in modo client

MOCA 2008

Uso dei remailer di tipo II mixmaster

Interfacce per Windows

- **Jack B. Nimble**
- **Quicksilver**
- **Reliable** il quale funziona anche come server
(anche se tempo fa fu pubblicato uno studio che ne rivelava le
molte vulnerabilità)

Non li conosco per cui non mi dilungherò di più

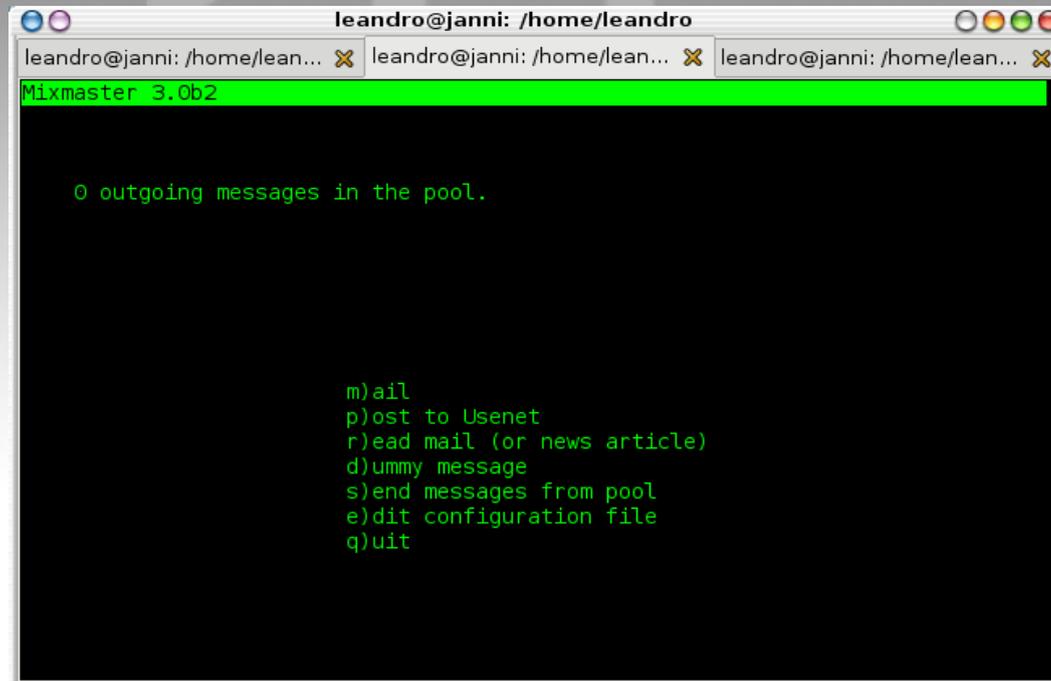


MOCA 2008

Uso dei remailer di tipo II mixmaster

Uso del client mixmaster

codice portabile per cui gira su quasi tutti i sistemi operativi
interfaccia fatta con ncurses (per cui molto spartana)



```
leandro@janni: /home/leandro
leandro@janni: /home/lean... ✕ leandro@janni: /home/lean... ✕ leandro@janni: /home/lean... ✕
Mixmaster 3.0b2

0 outgoing messages in the pool.

m)ail
p)ost to Usenet
r)ead mail (or news article)
d)ummy message
s)end messages from pool
e)dit configuration file
q)uit
```



MOCA 2008

Uso dei remailer di tipo II mixmaster

Uso del client mixmaster con mutt

mutt è un programma di posta elettronica molto ben realizzato e con molte possibilità di configurazione comprende anche una propria gestione del client mixmaster direttamente usando la versione compilata con il supporto
la versione distribuita con debian ha il supporto per mixmaster



MOCA 2008

Uso dei remailer di tipo II mixmaster

Uso del client mixmaster con mutt

```
leandro@janni: /home/leandro
leandro@janni: /home/lean... X leandro@janni: /home/lean... X leandro@janni: /home/lean... X
a:Accoda i:Inserisce d: Cancella q: Abbandona <Return>:OK
1 <random>
2 CM Nm antani mixmaster@firenze.linux.it
3 C austria mixmaster@remailer.privacy.at
4 C Np banana banana@mixmaster.mixmin.net
5 C Nm borked remailer@pseudo.borked.net
6 C Nm bunker mixmaster@mixmaster.thebunker.net
7 CM citrus mix@outel.org
8 C Nm cripto anon@ecn.org
9 CM cside cside@cside.dyndns.org
10 CM cthulu mixmaster@cthulu.joatcrafts.org
11 C Nm cyberiad mixmaster@remailer.cyberiade.it
12 CM Nm deuxpi anon@deuxpi.ca
13 C Nm dizum remailer@dizum.com
14 CM Nm eurovibes mixmaster@eurovibes.org
15 C Nm frell godot@remailer.frell.eu.org
16 C Nm george mix@mixmaster.it
-- Remailer chain [Length: 0]
-- Mutt: Seleziona una catena di remailer.
```



Uso dei remailer di tipo II mixmaster

I pinger

- programmi che elencano e mettono a disposizione le caratteristiche della rete dei remailer
- chiavi dei remailer
- statistiche di funzionamento
- catene interrotte (broken chains)

Devono essere usati dagli utenti per scaricare queste informazioni che così possono essere usate dai client

Stato della rete mixmaster

Attualmente la rete dei remailer non è in buono stato

- sono funzionanti realmente pochi remailer (una decina)
- molti non sono seguiti con attenzione
- lo sviluppo dei remailer di tipo III è fermo
- vengono usati troppo poco

M O C A 2008

Fonti informative

newsgroups alt.privacy.anon-server e alt.privacy

lista di posta elettronica e-privacy@firenze.linux.it

sito del Progetto Winston Smith
<http://www.winstonsmith.info>

alcuni siti collegati ai remailer <http://www.dizum.com>
<http://www.panta-rhei.eu.org>

guide del sito degli autistici <http://www.autistici.org/guide>
libro Kryptonite <http://www.ecn.org/kryptonite>



M O C A 2008

Fonti informative

newsgroups alt.privacy.anon-server e alt.privacy

lista di posta elettronica e-privacy@firenze.linux.it

sito del Progetto Winston Smith
<http://www.winstonsmith.info>

alcuni siti collegati ai remailer <http://www.dizum.com>
<http://www.panta-rhei.eu.org>

guide del sito degli autistici <http://www.autistici.org/guide>
libro Kryptonite <http://www.ecn.org/kryptonite>

