

HACKMEETING 2007

Introduzione all'uso dei remailer anonimi

Leandro Noferini - Inoferin@cybervalley.org



HACKMEETING 2007

Di cosa parleremo

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

Non parleremo della gestione di un remailer anonimo



HACKMEETING 2007

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



HACKMEETING 2007

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



HACKMEETING 2007

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)



HACKMEETING 2007

Funzionamento (tipi I e II)

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

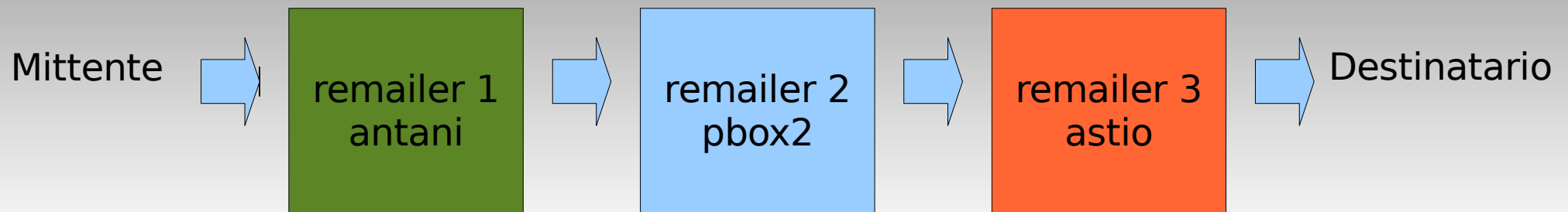
Funzionamento quasi tutto in automatico



HACKMEETING 2007

Uso – linee generali

Il mittente sceglie la catena e ne scarica le chiavi pubbliche



HACKMEETING 2007

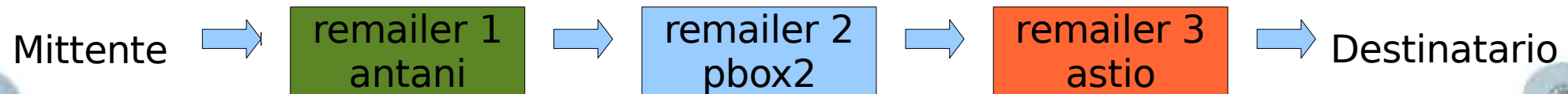
Uso – linee generali

Il mittente prepara il testo per il destinatario

richiesta per l'ultimo reloader di reinvio al destinatario finale

TESTO DEL MESSAGGIO

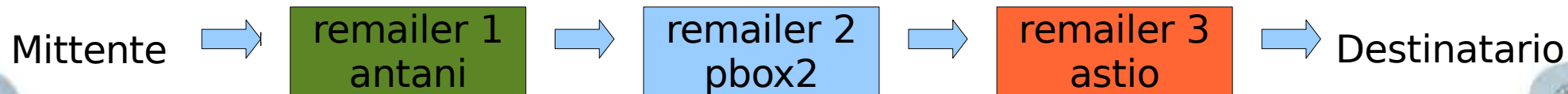
(puo' essere gia' crittato con la chiave del destinatario finale)



HACKMEETING 2007

Uso – linee generali

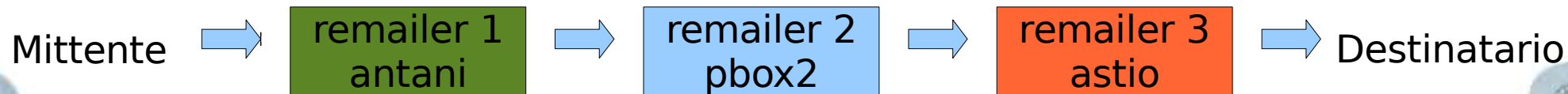
Il mittente cifra il testo usando la chiave dell'ultimo remailer



HACKMEETING 2007

Uso – linee generali

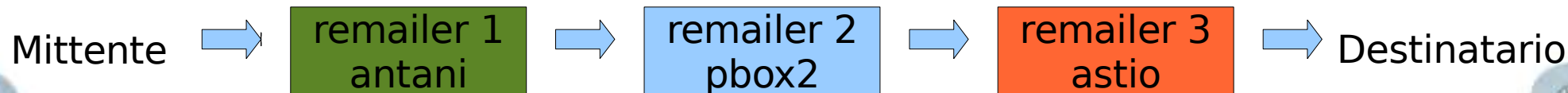
Il mittente cifra il messaggio ottenuto usando la chiave del remailer intermedio



HACKMEETING 2007

Uso – linee generali

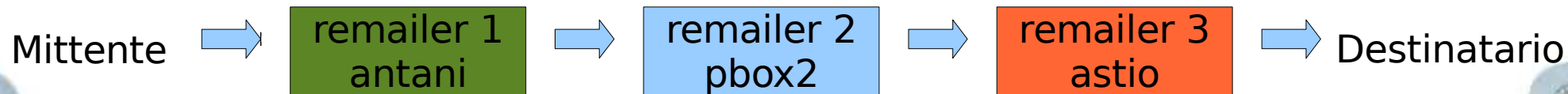
Il mittente cifra il messaggio ottenuto usando la chiave del primo remailer



HACKMEETING 2007

Uso – linee generali

Il mittente spedisce il messaggio ottenuto verso il primo remailer



HACKMEETING 2007

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



HACKMEETING 2007

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



HACKMEETING 2007

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



HACKMEETING 2007

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 ci dilungherò di più

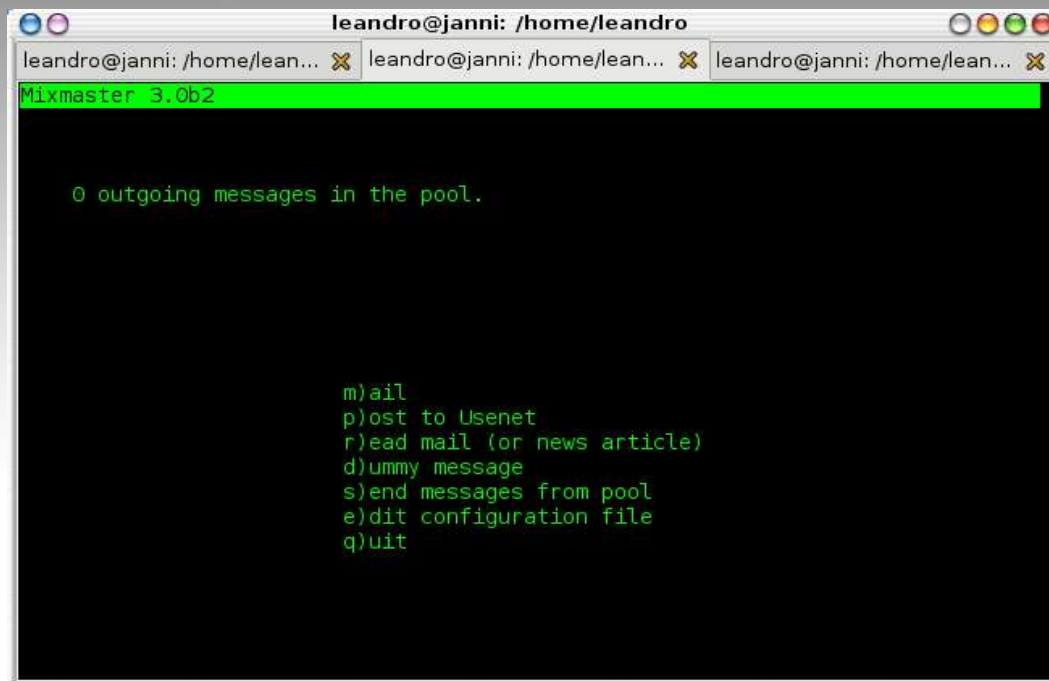


HACKMEETING 2007

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)

A screenshot of a terminal window titled 'leandro@janni: /home/leandro'. The window shows the Mixmaster 3.0b2 interface. The title bar includes window control buttons and the user's name and directory. The terminal content shows the version 'Mixmaster 3.0b2' on a green background, followed by the status '0 outgoing messages in the pool.' and a list of commands: m)ail, p)ost to Usenet, r)ead mail (or news article), d)ummy message, s)end messages from pool, e)dit configuration file, and q)uit.

```
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
```



HACKMEETING 2007

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



HACKMEETING 2007

Uso dei remailer di tipo II mixmaster

Uso del client mixmaster con mutt

```
leandro@janni: /home/leandro
leandro@janni: /home/lean... ✕ leandro@janni: /home/lean... ✕ leandro@janni: /home/lean... ✕
a:Accoda  i:Inserisce  d:Cancello  g: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.
```



HACKMEETING 2007

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



HACKMEETING 2007

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
- la rete è sotto attacco (flood) da molto tempo
- lo sviluppo dei remailer di tipo III è fermo
- vengono usati troppo poco



HACKMEETING 2007

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>

