e-privacy 2005

"communication freedom in the age of business"

Firenze - 28.05.2005

Federico Moro
fm@khamsa.net
KHAMSA SA

alcuni concetti

questione di percezzione*

- "Su Internet si riesce facilmente a ottenere l'anonimato" [NO]
- l'utilizzo di strumenti digitali lascia molte più tracce di quanto si pensi [SI]
  - tali tracce sono facilmente elaborabili da un calcolatore

*errore volontariamente prodotto

la posta elettronica

- Ogni intestazione e-mail riporta l'elenco dei server mail che lo hanno instradato:

```
Return-Path: <francesco@noprivacy.federicomoro.tld>
Received: (from mail@localhost)
by sigmalogon.propagation.tld (8.11.6/8.11.6) id j4RF47b26297
for anotherhop@noprivacy.federicomoro.tld; Fri, 27 May 2005 17:04:07
+0200
Received: from server.meta.cpr.it (server.meta.cpr.it
[131.114.32.230])
by sigmalogon.propagation.net (8.11.6/8.11.6) with ESMTP id
j4RF43W26286
for <info@federicomoro.tld>; Fri, 27 May 2005 17:04:07 +0200
Received: from localhost (localhost [127.0.0.1])
by server.meta.cpr.it (8.12.7/8.12.4) with SMTP id j4REYusr021818;
```

la posta elettronica (2)

- Ogni nodo può tener traccia dei messaggi transitati:
  - i log “finiscono” nei backup
  - analisi dei log
- Lo staff IT che gestisce ciascun singolo nodo può accedere alle informazioni trasportate dall’e-mail:
  - contenuto del messaggio
  - mittente, destinatario, percorso, luogo di spedizione

come tutelarci?

- identità: (re)mailing
- contenuto: cifratura

Servizi di anonimato

- Garantiscono l'identità dell'utente
- Riguardano anche altri aspetti legati all'identificabilità
- Dissociano l'identità dell'utente dalle sue azioni

SCENARI D'USO

chi ha bisogno di privacy

Perchè usarli?

- Comunicazioni di emergenza
- Discussioni su temi personali o tabù
- Corrispondenza giornalistica
- Protezione dallo spam
- Anonimato rispetto al futuro
- Discorsi pregiudizievoli (politica, religione, ...)

uso "privato"

- Finchè esisterà anche una sola categoria che ne possa beneficiare, ha senso che tali servizi esistano
- Alcuni esempi:
  - Privati cittadini vs Pubblici cittadini
  - Giornalisti

uso corporate

- Attività di intelligence su concorrenti
- Combattere lo spionaggio industriale
- Feedback da parte di dipendenti
- Trattative legali
- Altre attività strategiche

(ab)uso

- Solo i terroristi necessitano dell'anonimato
- No! ci sono anche i pedofili, la mafia e l'anonima sequestri esisteva prima di internet
- Potremmo vietare gli aerei, i bambini, gli affari...
- Gli "abuser" sono generalmente meno sofisticati e più diretti di quanto si pensi

fornire anonimato

- Fornire soluzioni commerciali di anonimato è complesso e difficile
  - Gestione pagamenti (anonimi)
  - Alti costi operativi
  - Domanda incerta
  - Limiti legali
  - Complicazioni derivanti dall'abuso

acquistare anonimato

- accedere a risorse anonime è altrettanto difficile
  - Gestire i pagamenti (anonimi)
  - Incertezza del grado di riservatezza
  - Disponibilità del servizio ed efficienza
  - Restrizioni locali e legali
  - Facilità d'uso

REQUISITI

aspettative, limiti e problemi

l'aspettativa

- Anonimato
- Riservatezza
- **Ripudiabilità**
- **Usabilità**

Ripudiabilità

- Facoltà di dissociarsi da una specifica azione compiuta
- Diverse prospettive:
  - ripudiabilità: e-voting
  - non-ripudiabilità: contratti, trattative commerciali

usabilità

- Dipende dallo scopo di utilizzo
  - Privato - Commerciale - Legale
  - Bi-direzionalità
  - Qualità del servizio
    - latency
    - reliability
  - Facilità d'uso

in definitiva

- Un buon sistema di comunicazione dovrebbe offrire all'utilizzatore:
- scelte
  - anonimato, riservatezza dei contenuti, ripudiabilità
- garanzie
  - usabilità, QOS, bidirezionalità, affidabilità

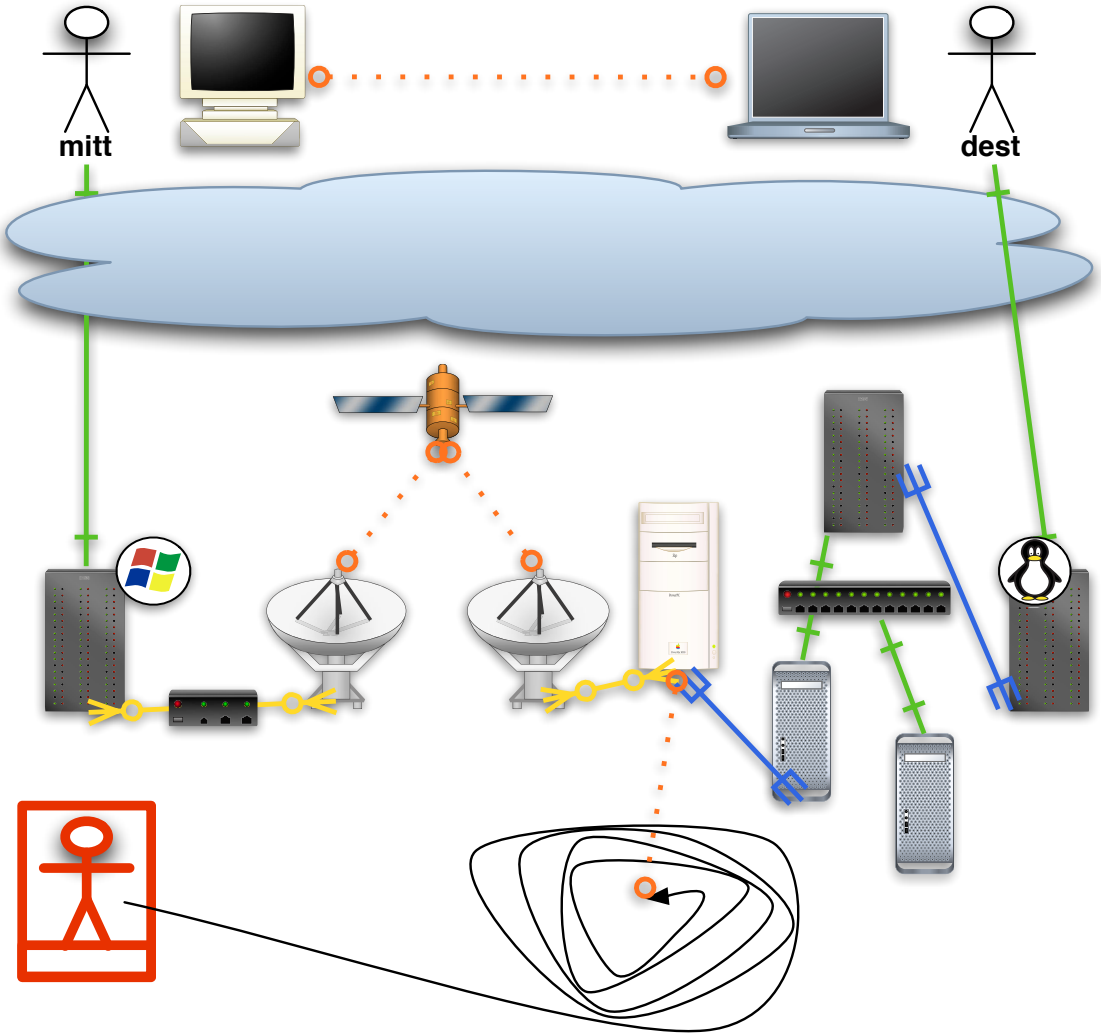
I MECCANISMI

remailer, tecnologia, legislazione

il canale di comunicazione

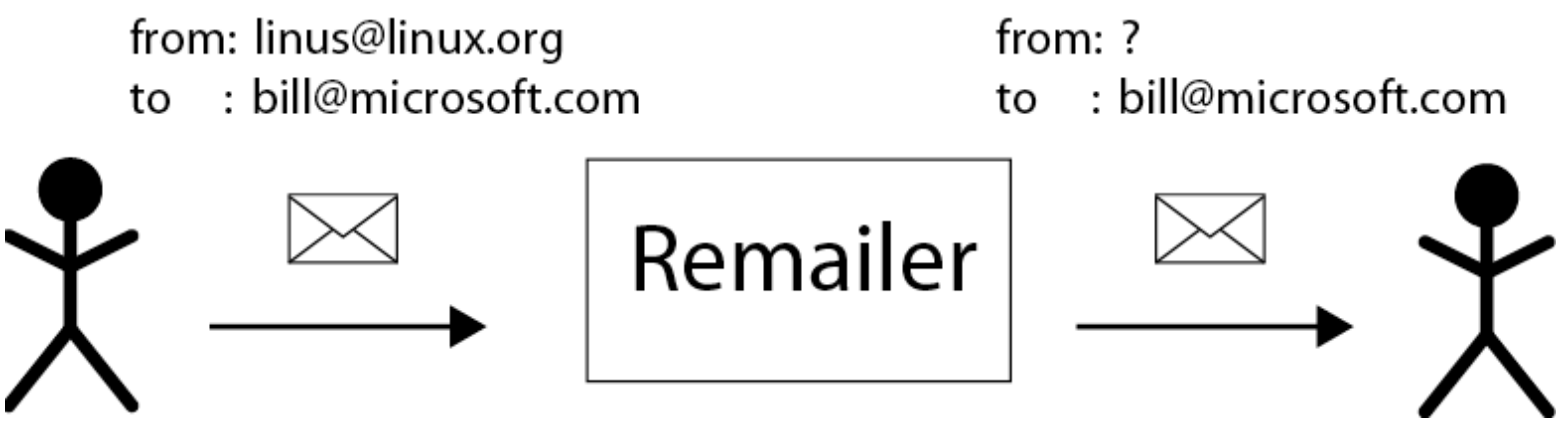
- Un mittente, un ricevente: soggetti identificabili
- una catena di mezzi di comunicazione:
  - soggetti difficili da identificare
  - come fidarsi di soggetti non solo non identificati, ma spesso non identificabili?

Realtà vs Percezione



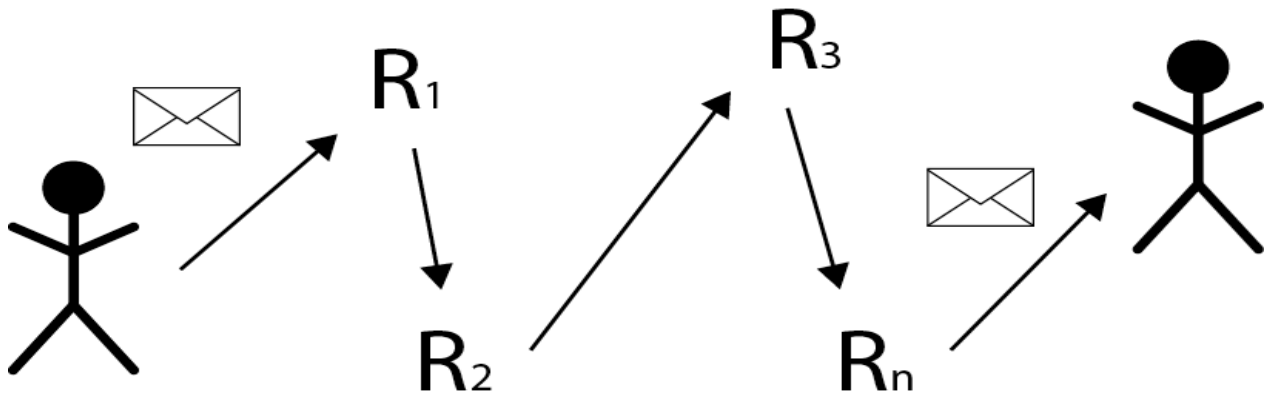
Remailers

- Un sistema di remailing permette l'invio di messaggi anonimi
- Il remailer nasconde l'indirizzo del reale mittente



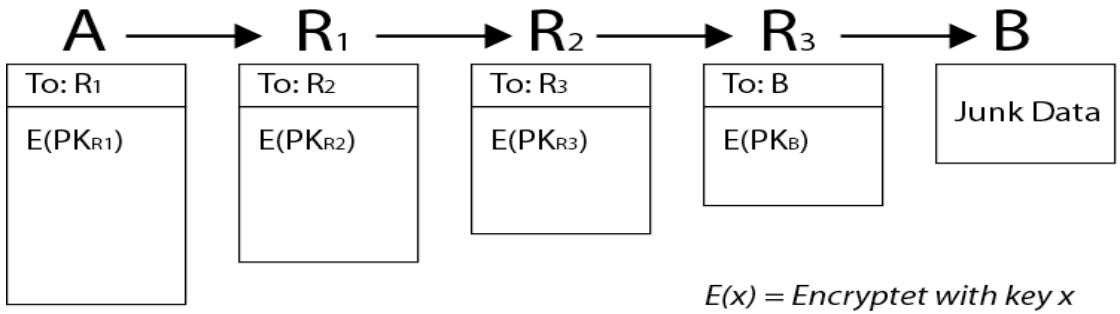
Catene di remailing

- I messaggi possono essere instradati attraverso diversi remailer per aumentare la sicurezza
- Idealmente, un remailer dovrebbe conoscere solo l'*hop* successivo



instradamento a cipolla

- METAFORA: la cipolla
  - è fatta da diversi anelli incapsulati ricorsivamente
  - fa piangere chi la usa (e chi cerca di "tagliarla")
- TECNICA: L'intestazione del messaggio contiene diversi livelli di istruzioni di instradamento, una per hop
  - Ad ogni hop, il livello più esterno viene eliminato
  - Ogni livello è cifrato con la chiave pubblica del destinatario



e la risposta?

il percorso: (re)mailing inverso

il contenuto: cifratura

i "reply blocks"

- Un server pubblica un reply-block, per permettere ad altri server di comunicare con esso.
- i reply blocks sono messaggi e-mail "vuoto", che tengono traccia del percorso inverso e sono opportunamente cifrati ricorsivamente
- Un reply block è una buona implementazione del concetto di pseudonimo !

Proprietà dell'anonimato

- Anonimato perfetto via remailer
  - Non vi è modo di garantire che una transazione (comunicazione) sia stata effettivamente completata.
- Anonimato computazionale
  - Non vi è modo che un avversario possa violare l'anonimato, con strumenti "ragionevolmente" potenti.

Sistemi di remailing

- Cypherpunk
  - insicuro e “vecchio”
- Mixmaster
  - più sicuro, ma non consente risposte
- Mixminion
  - ancor più sicuro, consente risposte

Cypherpunk (tipo 1)

- non trattengono le informazioni degli utenti
- non mantengono log delle attività
- utilizzano un mittente fittizio per mascherare quello reale
- non è consentita la risposta tramite l'utente fittizio
- se non vengono utilizzati client appositi, la procedura di composizione manuale è artificiosa

Mixmaster (tipo 2)

- oltre alle caratteristiche dei remailer di tipo 1, aggiungono sicurezza
- si basano su un protocollo specifico implementato su SMTP
- è possibile impostarli per funzionare anche come remailer tipo 1

Mixminion (tipo 3)

- Sono la nuova generazione di remailer
- oltre alla sicurezza degli “antenati” di tipo 1 e 2, forniscono ulteriore sicurezza e diverse interessanti features
- supportano direttamente le risposte
- richiedono tuttavia un client apposito
- si basano su un protocollo che sfrutta connessioni sicure
- possono essere configurati per funzionare come remailer tipo 1 e 2

"problemi" nel remailing

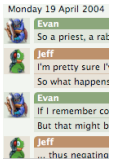
- *Latency*
- Affidabilità
- Difficoltà d'uso in uno scenario "reale" e "quotidiano"
- Integrazione negli strumenti (quicksilver)
- Mancanza del supporto di un indirizzo di ritorno

comunicazione = e-mail ?

multicanalità

- non solo e-mail
- dinamiche sempre più veloci


Fax



Messaggistica istantanea


Voice over IP

- la latency si trasforma da fastidio a reale criticità

SVILUPPI FUTURI

- Cambio generazionale dei sistemi di re-mailing
- Integrazione di reti di forwarding con applicazioni di comunicazione VoIP
- TOR, altri?, i2p

e-privacy 2005

"communication freedom in the age of business"

Federico Moro
fm@khamsa.net

KHAMSA SA