Anonymous remailers e pseudonym servers...
...in breve

Gianni Bianchini
giannibi@firenze.linux.it

LinuxDay 2002 - Siena, 23 Novembre 2002

Preliminari - PGP/GnuPG e posta crittografata

Lo standard PGP (come la sua implementazione libera, GnuPG) è uno strumento di comunicazione sicura ed autenticazione basato sull'uso di meccanismi di cifratura asimmetrica. Gli algoritmi usati sono, ovviamente, pubblici.

- Cifratura simmetrica
  - Una sola chiave è usata per cifrare e decifrare
  - Necessità di chiavi condivise e trasmesse mediante canale sicuro
  - Ogni chiave vale per una comunicazione privata uno-a-uno
- Cifratura asimmetrica (a chiave pubblica)
  - Presenza di due chiavi, pubblica e segreta (privata)
  - La chiave pubblica è a disposizione di chiunque voglia comunicare con il destinatario cui appartiene
  - Solo la chiave privata può decifrare ciò che è cifrato con la chiave pubblica (e per alcuni algoritmi, viceversa)
  - È estremamente complesso risalire dalla chiave pubblica alla chiave privata

Preliminari - PGP/GnuPG e posta crittografata

- Algoritmi ibridi
  - Il sistema a chiave pubblica viene utilizzato per condividere in modo sicuro il segreto usato per la cifratura simmetrica (chiave di sessione), che viene generato ex-novo per ogni nuova comunicazione
- Firma digitale
  - È il risultato dell'applicazione ad un documento di una funzione di *hash*, ovvero tale che
    - Deve essere difficile individuare due documenti che producano lo stesso risultato
    - Deve essere difficile risalire dal risultato al documento
  - Il valore di hash viene cifrato con la chiave privata dell'autore
    - È possibile verificare l'autenticità a fronte della chiave pubblica
    - Non è possibile per terzi modificare la firma in corrispondenza ad una modifica (falsificazione) del documento se non conoscendo la chiave privata dell'autore

In pratica...

- Generazione di una coppia di chiavi
  - Scelta della dimensione
  - Impostazione della data di scadenza
  - Scelta della passphrase
- Manutenzione
  - Accorgimenti per la protezione della chiave privata
  - Gestione della propria rete di fiducia, firma delle chiavi
- Rendere disponibile la chiave pubblica
  - Uso di keyserver
- Impiego del programma GnuPG (gpg) direttamente o tramite interfacce
  - Client di posta con supporto per cifratura/firma PGP/GnuPG

In pratica...

- Cifrare...

```
$ echo ciao | gpg -e -a -r giannibi@firenze.linux.it > segreto
$ cat segreto
-----BEGIN PGP MESSAGE-----
Version:  GnuPG v1.0.6 (GNU/Linux)
Comment:  For info see http://www.gnupg.org

hM4DVNPUyail4OsQAvkBJOGCMJ/hn0QVLzMlLZy9dUPHiN6RDX3esP1Tvbyt39pR
Np4you4N7YDqNPDRC9HQ31OiOdehRx7qNLeaDuMa9bfH8uFOq/N8ErZ/LjXWBBR4
+K5oNbIaNvzO0y29v+EC/ihENUXMpze/TSySt0UE4GgbIBOXB/weqjrAViUvx9O8
kLMHvQw58Sy6MOJZHRs2abNlKpKvC+c4N9W/JlE4Gfvrk7A4i2B/gv+6dWdWXhUD
n3Euy5SRlVZ6DACY7z4dYskbGDux8Wjj785cD0OFwDnF+8gyG4ZhI/aMX3de
=uwj+
-----END PGP MESSAGE-----
```

In pratica...

- Decifrare...

```
$ gpg -d segreto
You need a passphrase to unlock the secret key for
user:  Gianni Bianchini <giannibi@firenze.linux.it>
768-bit ELG-E key, ID A8A5E0EB, created 1999-09-01 (main key ID
C5D54F84)

Enter passphrase:

gpg:  encrypted with 768-bit ELG-E key, ID A8A5E0EB, created
1999-09-01
      Gianni Bianchini <giannibi@firenze.linux.it>
ciao
```

Anonymous remailers

- Un anonymous remailer è un mail server con la capacità di ricevere e rispedire messaggi in modo che sia estremamente difficile risalire al mittente originario
  - Messaggi email
  - Usenet groups
- Sostituzione dei campi dell'header dei messaggi che permettono l'individuazione dell'origine (`From:`, `Sender:`, `Received:`, ecc.)
- Possibilità (necessità) di uso in catena e combinato con la crittografia forte
  - Impossibilità di individuare il contenuto della comunicazione
  - Impossibilità di tracciare il percorso della comunicazione
  - Possibilità di celare la stessa esistenza dello scambio
- Anonimato forte vs. anonimato debole

Anonymous remailers - tipologie

- Tipo 0 - Pseudo-anonimizzatore (obsoleto)
  - Mappa pseudonimo - indirizzo reale
  - Uso immediato
  - La riservatezza dipende dalla capacità dell'operatore di mantenere segreta la tabella delle corrispondenze
  - Caso anon.penet.fi
- Tipo 1 - Cypherpunk
  - Possibilità di cifratura PGP dei messaggi per il remailer
  - Possibilità di concatenazione (chaining) + cifratura
  - Riordinamento ed introduzione di latenze
  - Uso con normale client di posta + PGP/GPG
- Tipo 2 - Mixmaster

Concatenazione (chaining)

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

Funzionamento remailer Cypherpunk

- Preparazione del messaggio

```
To:  mixmaster@firenze.linux.it
From:  giannibi@firenze.linux.it
Subject:  Sudare sette camicie
----------------------------------------
::
Request-Remailing-To:  marcoc@firenze.linux.it

Sappi che un anonimo ha finito alle 4 di stamani
di preparare una presentazione sui remailer per
il LinuxDay di Siena.
```

Funzionamento remailer Cypherpunk

- Messaggio ricevuto

```
From:  Tarapia Tapioco
   <comesefosse@ntani.firenze.linux.it>
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 <abuse@ntani.firenze.linux.it>.
To:  marcoc@firenze.linux.it
Subject:  Sudare sette camicie
------------------------------------------------
Sappi che un anonimo ha finito alle 4 di stamani
di preparare una presentazione sui remailer per
il LinuxDay di Siena.
```

Uso di GPG con remailer Cypherpunk

- Operazione preliminare: importazione della chiave pubblica del remailer
- Richiesta di reinoltro standard

```
::
Request-Remailing-To:  marcoc@firenze.linux.it

Sappi che un anonimo ha finito alle 4 di stamani
di preparare una presentazione sui remailer per
il LinuxDay di Siena.
```

Uso di GPG con remailer Cypherpunk

- Cifratura della richiesta per `mixmaster@firenze.linux.it` e notifica di messaggio cifrato

```
To:  mixmaster@firenze.linux.it
From:  giannibi@firenze.linux.it
Subject:  Sudare sette camicie
----------------------------------------------------------------
::
Encrypted:  PGP

-----BEGIN PGP MESSAGE-----
Version:  GnuPG v1.0.6 (GNU/Linux)

hIwC8cAPVx+T6qkBA/43Z7ATcC37Ip/+BGGlVEuqIGZu97QvbYeBDwd40i7ctXqa
8x6nqBdaj9Qwzur5scPzo5o510FPdt4XDxut7nMOUq3HbDg1i+O2WfNjXXYdJKS7
fbnpkxU9zKH0Suh8E4/imuDy9F2+7A5lBnX19Fx+ho8FsJ20e6YklUlzuw1FIKYA
AABZOlLMKedrpUbDxAwCXvz27ZmF/w05PLlObJL81RXJQMVq7xnQtyZB5k+Tzuhr
9QsDWo4W73N3LdTRF6CNA1C6+zGIRKbQoyVt1c0e1bsh1Sh0nZI65zILaMs=
=kG6y
-----END PGP MESSAGE-----
```

Uso della concatenazione

- Incapsulamento della richiesta per il remailing da parte dell'anello immediatamente *precedente* della catena

```
::
Request-Remailing-To:  mixmaster@firenze.linux.it

::
Encrypted:  PGP

-----BEGIN PGP MESSAGE-----
Version:  GnuPG v1.0.6 (GNU/Linux)

hIwC8cAPVx+T6qkBA/43Z7ATcC37Ip/+BGGlVEuqIGZu97QvbYeBDwd40i7ctXqa
8x6nqBdaj9Qwzur5scPzo5o510FPdt4XDxut7nMOUq3HbDg1i+O2WfNjXXYdJKS7
fbnpkxU9zKH0Suh8E4/imuDy9F2+7A5lBnX19Fx+ho8FsJ20e6YklUlzuw1FIKYA
AABZOlLMKedrpUbDxAwCXvz27ZmF/w05PLlObJL81RXJQMVq7xnQtyZB5k+Tzuhr
9QsDWo4W73N3LdTRF6CNA1C6+zGIRKbQoyVt1c0e1bsh1Sh0nZI65zILaMs=
=kG6y
-----END PGP MESSAGE-----
```

- Segue cifratura con la chiave di un altro remailer ed invio a quest'ultimo

Considerazioni di sicurezza

- Ovvio ma è bene ripeterlo: senza cifratura per il destinatario il contenuto della comunicazione è intercettabile (se non altro a livello dell'ultimo reinoltro in una catena)
- Uso di un solo remailer: il remailer conosce indirizzo di provenienza e destinazione
  - Presuppone *assoluta fiducia* nella sicurezza e buona fede dell'operatore
- Catena di 3 o più remailer
  - Non è possibile ricostruire il percorso mittente-destinatario
  - L'anonimato è preservato a meno che tutti i remailer della catena siano compromessi
- Forme di attacco avanzate

Lo stato dell'arte

- Remailer di tipo 2 - Mixmaster
  - Immune ad alcune forme di attacco contro il tipo 1
  - Uso cifratura RSAREF (non PGP)
  - Scomposizione dei messaggi in pacchetti multipli di dimensione fissa e relativo reordering solo da parte dell'ultimo remailer
  - Generazione di rumore
  - Necessità di un apposito client

- Il grande neo: gli anonymous remailer non consentono con facilità una comunicazione *bidirezionale*, ovvero non permettono di rispondere in modo agevole all'anonimo mittente

MA...

Pseudonym servers

Uno pseudonym server è un sistema che permette in modo automatizzato di stabilire una comunicazione bidirezionale conservando la proprietà di anonimato

- Evoluzione del sistema di remailing tipo 0
- Nemmeno l'amministratore del sistema è a conoscenza della corrispondenza tra pseudonimi ed indirizzi reali.
  Inoltre, è ignota al server la provenienza di ogni messaggio
- Com'è possibile?
  - Uso di PGP
  - Uso dei sistemi di remailing
- Tipologie: alpha (tipo 1), newnym (tipo 2)

Pseudonym servers - funzionamento

- Blocco di risposta (Reply-block)
  - Ad ogni pseudonimo sono associati uno o più *pacchetti di istruzioni* incapsulate, che specificano le modalità di recapito del messaggio al destinatario finale, attraverso una catena di remailer, con comunicazione protetta da PGP
  - Ogni remailer può decifrare solo le istruzioni per l'inoltro al remailer successivo (l'ultimo al destinatario)
- Il nym server mantiene l'associazione tra pseudonimi e reply-block (*non* tra pseudonimi ed indirizzi reali)
- L'amministratore del nym server conosce solo l'indirizzo del *primo remailer* della catena, oltre al reply-block, il cui contenuto però non gli è accessibile

Pseudonym servers - operazioni preliminari

- Importazione della chiave pubblica del nym server `(send|config)@nym.alias.net`
- Scelta dello pseudonimo

  `giannibi@firenze.linux.it` alias `ninabigi@nym.alias.net`
- Creazione coppia di chiavi per `ninabigi@nym.alias.net`
- Creazione del reply-block (anche multipli)
- Invio della richiesta di creazione dell'account, firmata con la chiave dello pseudonimo e contenente la chiave pubblica, a `config@nym.alias.net`

Invio di un messaggio dall'account nym

1. Creazione del messaggio

```
From:  ninabigi
To:  marcoc@firenze.linux.it
Subject:  LinuxDay a Siena

RE

Ho saputo che tieni un interessante intervento sulla e-privacy
```

2. Firma del messaggio con la chiave dello pseudonimo e cifratura per il nym server

3. Invio del messaggio a `send@nym.alias.net` *attraverso una catena di remailer*

N.B. Il nym server non viene a conoscenza della provenienza del messaggio ma ne riconosce l'autenticità!

Ricezione di un messaggio sull'account nym

1. `marcoc@firenze.linux.it` invia un regolare messaggio a `ninabigi@nym.alias.net`

2. Il nym server recupera il reply-block associato allo pseudonimo ed inoltra il messaggio al primo remailer della catena da esso specificata

3. Le istruzioni del reply-block vengono eseguite in sequenza dalla catena di remailer fino a raggiungere il destinatario

Creazione del reply-block (1 remailer)

- Istruzioni per l'ultimo remailer della catena

```
::
Anon-To:  giannibi@firenze.linux.it
Encrypt-Key:  chiaveperconventionalencryption                    (1)
```

- Cifratura per l'ultimo remailer e composizione del blocco

```
::
Anon-To:  mixmaster@firenze.linux.it
Encrypt-Key:  chiaveperconventionalencryption

::
Encrypted:  PGP

-----BEGIN PGP MESSAGE-----
<<< Cifrato di (1) per mixmaster@firenze.linux.it >>>
-----END PGP MESSAGE-----

**
```

Creazione dell'account

- Invio richiesta a `config@nym.alias.net` (tramite remailer)

```
Config:
From:  ninabigi@nym.alias.net
Nym-Commands:  create +acksend +signsend name="Nina Bigi"
Public-Key:
-----BEGIN PGP PUBLIC KEY BLOCK-----
<<< Chiave pubblica di ninabigi@nym.alias.net >>>
-----END PGP PUBLIC KEY BLOCK-----
Reply-Block:
::
Anon-To:  mixmaster@firenze.linux.it
Encrypt-Key:  chiaveperconventionalencryption

::
Encrypted:  PGP

-----BEGIN PGP MESSAGE-----
<<< Cifrato di (1) per mixmaster@firenze.linux.it >>>
-----END PGP MESSAGE-----

**
```

Software client/server libero

- Mixmaster - `http://mixmaster.sourceforge.net`
  - Implementazione dei protocolli tipo 2 e tipo 1
  - Uso in modalità client-only
- Alias nymserver - `finger:source@nym.alias.net`
  - Implementazione dello standard newnym
- Mutt - `http://www.mutt.org`
  - Supporto per uso di anonymous remailers
- Freedom remailer web interface - `http://freedom.gmsociety.org/remailer`