

Le bollette le voglio in
busta chiusa.
E la cassetta delle
lettere deve avere una
serratura.

Alessio L.R. Pennasilico
mayhem@recursiva.org
<http://www.sikurezza.org>
GPG Key ID B88FE057

\$ whois mayhem



- ✓ Socio ed attivista di ILS, LUGVR, Metro Olografix, OpenGeeks/OpenBeer, AIPSI, AIP, recursiva.org, Sikurezza.org, no1984 e Spippolatori, CLUSIT e VoIPSA.
- ✓ Svolge attività di consulenza presso diverse aziende, principalmente in merito a tecnologie legate ad Internet, al networking ed alla sicurezza.
- ✓ Security Evangelist @ www.alba.st

\$ whois sikurezza.org



Sikurezza.org è una comunità virtuale di persone che per passione e/o lavoro si interessano di problematiche di (in)sicurezza informatica e della loro diffusione.

Si tratta di un progetto non commerciale portato avanti da volontari.



Finalità

Comprendere se la confidenzialità dei dati è una nostra esigenza e come realizzarla nel modo più adeguato.

Avere un quadro degli strumenti disponibili e come si usano.

Problema

Quando scriviamo una mail
non abbiamo alcuna
garanzia di
confidenzialità.

HTTPS/IMAPS/POP3S - SMTP!

Se siamo così fortunati da poterci collegare al mail server e leggere la posta in modo “sicuro” ricordiamo che lo scambio di mail tra server avviene **prevalentemente** in chiaro.

Soluzione

L'utilizzo della crittografia ci permette di identificare univocamente il mittente, essere certi dell'integrità del messaggio ed eventualmente proteggerlo da occhi indiscreti.

Voglio poter scegliere se
inviare una cartolina o
una lettera.

Basta!

“non faccio nulla di sbagliato,
quindi non ho nulla da nascondere”

**non ha nulla a che vedere con la
crittografia!**

GPG



GNU Privacy Guard è uno dei programmi più usati per proteggere le proprie e-mail.

Utilizza lo standard de facto (RFC 2440), è OpenSource, multiplatforma e gratuito.

to sign

GPG permette di “firmare” le mail
così da rendere il destinatario
certo di due fattori:

**sono davvero io il mittente e
nessuno ha modificato il contenuto**

Alessio Pennasilico

to crypt

```
1 BSCRYPT0@h0*z70=|Hù. ¯#p4Ç|'i#  
2 Ü4?ì|ý|_wfÓ´(ààîÍRĐóMà=W<Lc|z  
3 é#áäÖBnd0)|#|°_B&b'áix+|jP=|E  
4 9t4q±w0ö||I@DXiMá@h,i|>Fqiz4J  
5 È|Öæ|@)bèn9S·E| - µw-]éymíÁ|y  
6 Ê%||*|i0|@_G|c]-|Ú@*xò%EZ  
7 |<I,m ×|~à|pxáçæÃ»i|BádÇÁ{òu  
8 ZVBÚÝx-Óæ|H~ðÁ|N.²JÚRp?Ö9a ð1  
9 (?àCKN-| ¯óm#GS.Ú&|R&´|Áyè± |  
10 &z_úó|Ãät||+zc-Úóm|2ü0*0|Éið*  
11 a}T4Z0úbN@y!;||*|"U|è+vðæ´b9E  
12
```

L'encryption è lo strumento che permette di essere certi che solo il destinatario ed il mittente sono (e saranno) in grado di leggere il contenuto di quel messaggio e-mail.

Chiavi asimmetriche

Scambiare una password tra due persone, magari sconosciute, in modo sicuro, è un problema.

Per questo GPG lavora tramite l'utilizzo di due diverse chiavi:

- ✓ la mia chiave pubblica
- ✓ la mia chiave privata

Chiave pubblica

Liberamente disponibile su Internet, su siti web e keyserver, viene usata dagli altri per verificare la mia firma e/o per criptare i messaggi diretti a me.

Chiave privata

Mi è più cara della mia stessa vita, la ho solo io e ne sono l'unico gelosissimo ed attentissimo custode.

La uso per firmare i messaggi che invio ed è l'unica a poter decriptare i messaggi inviati dagli altri, criptati con la mia chiave pubblica.

Di chi è questa chiave?

L'unico vero problema che resta è sapere con certezza che la chiave con ID B88FE057 è davvero la mia.

Per questa ragione si firmano le chiavi pubbliche altrui la cui appartenenza è certa.

files

GPG non solo effettua queste operazioni sui messaggi, ma anche sugli allegati.

Prevede la possibilità di firmare e/o criptare anche file su disco.

Il problema delle chiavi

Lascereste le chiavi di casa nascoste in giardino?

La riservatezza della chiave è il presupposto fondamentale per l'efficacia di questo strumento.

Policy

E' necessario scegliere una saggia politica di gestione delle chiavi ed una robusta policy per la scelta delle password.



Dispositivi USB

Per questa ragione conservare i file delle chiavi su un supporto removibile potrebbe essere una saggia decisione.

Non va trascurata l'esigenza di conservare una copia di backup della chiave in un luogo sicuro.

TrueCrypt

E' uno strumento OpenSource,
gratuito e multipiattaforma,
pensato per criptare i nostri dati
riservati, sia sull'hard-disk che
su supporti rimovibili.

steganografia/deniability

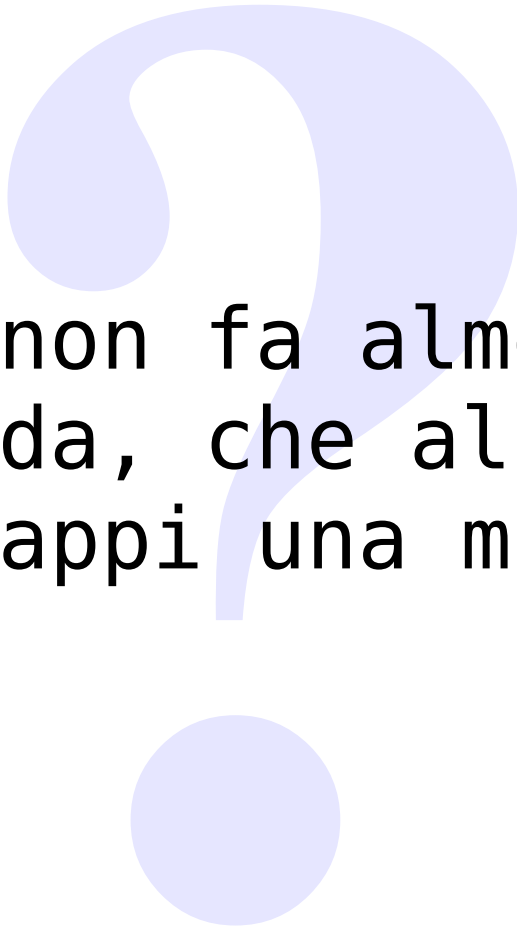

Un volume creato con truecrypt non dovrebbe poter essere identificato.

Prevede l'utilizzo di due password di accesso ai dati: una mi mostra i miei veri dati, l'altra finge di decriptare il volume e mostra dei dati fittizi preparati in precedenza.

Solo per “linux”?

No, ma facciamo attenzione!

Se la mia esigenza è la riservatezza non posso affidarmi a programmi, a sistemi operativi, ad algoritmi di cui non conosco e non posso verificare il funzionamento.



A chi non fa almeno una
domanda, che alzandosi
si strappi una mutanda!

Bibliografia

- ✓ gpg: <http://www.gnupg.org/>
- ✓ OpenPGP: <http://www.ietf.org/rfc/rfc2440.txt>
- ✓ truecrypt: <http://www.truecrypt.org/>
- ✓ <http://sourceforge.net/projects/truecrypt/>
- ✓ \$ apropos && man && google :)

Licenza

Queste slides sono realizzate da Alessio L.R. Pennasilico, mayhem, per sikurezza.org e sono soggette alla licenza Creative Commons nella versione Attribution-ShareAlike 2.0; possono pertanto essere distribuite liberamente ed altrettanto liberamente modificate, a patto che se ne citi l'autore e la provenienza.

Grazie della partecipazione.

Sono a vostra disposizione per
qualsiasi chiarimento o
precisazione.

