La crittografia open source ed il progetto GnuPG

di Enrico Zimuel (enrico@enricozimuel.net)

20 Settembre 2003

Metro Olografix Crypto Meeting - Pescara

convegno "mocm metro olografix crypto meeting"

http://www.olografix.org

Note sul copyright (copyfree):

Questa presentazione può essere utilizzata liberamente
a patto di citare la fonte e non stravolgerne il contenuto.

Questa presentazione è stata creata con OpenOffice 1.0
www.openoffice.org

- **Sommario:**
  - **La crittografia e l'open source**
  - **Il progetto GnuPG**
  - **Caratteristiche tecniche**
  - **Il Backend ed il Front-End**
  - **La crittografia del GnuPG**
  - **La release attuale 1.2.1**
  - **Confronto con il PGP**
  - **Lo standard OpenPGP (RFC2440)**

La crittografia e l'open source

- Risulterà strano ma uno dei principi fondamentali della crittografia, utilizzato ancora nei moderni sistemi crittografici è stato individuato nel lontano 1883 dal linguista franco-olandese August Kerckhoffs nel suo celebre articolo “La cryptographie militaire” apparso nel Journal des sciences militaires.
- **Principio di Kerckhoffs**: *“La sicurezza di un sistema crittografico è basata **esclusivamente** sulla conoscenza della chiave, in pratica si presuppone noto a priori l’algoritmo di cifratura e decifrazione.”*
- Conoscenza algoritmo = libera distribuzione codici sorgenti = uno dei principi fondamentali dell'open source!

La crittografia e l'open source

- "Se un sistema è veramente sicuro, lo è anche quando i dettagli divengono pubblici" Bruce Schneier
- Sicurezza = Trasperenza !
- Questa apparente contraddizione può essere spiegata solo grazie all'ausilio della matematica come base teorica della crittografia.
- La sicurezza di un sistema crittografico è intrinseca al sistema poiché basata su principi matematici.
- Sicurezza teorica = Sicurezza pratica? Purtroppo NO, i problemi sorgono in fase di applicazione dei concetti teorici (ad esempio esiste un algoritmo teoricamente sicuro, l'algoritmo di Vernam, ma non può essere implementato correttamente).

Il progetto GnuPG

• Il progetto tedesco GnuPG (GNU Privacy Guard) nasce nel 1997 per opera di **Werner Koch**, sviluppatore indipendente interessato alla crittografia open source.

• L'obiettivo del progetto è la realizzazione di un engine crittografico, alternativo al Pgp, totalmente open source basato su algoritmi crittografici standard e non proprietari.

• Il progetto è sviluppato utilizzando il linguaggio di programmazione C standard Ansi, facilmente trasportabile.

Il progetto GnuPG

• Basato su di un sistema di crittografia “ibrido”, simile al Pgp, con algoritmi simmetrici (crittografia tradizionale) e asimmetrici (crittografia a chiave pubblica).

• Rappresenta, allo stato attuale, un vero e proprio engine crittografico in grado di cifrare/decifrare, firmare ed autenticare file e messaggi di posta elettronica (standard MIME).

Caratteristiche tecniche

- Standard OpenPgP (RFC 2440)
- Standard di sicurezza Pgp e Pgp2 migliorato
- Decifra, verifica msg Pgp 5,6,7
- Supporto algoritmi crittografici ElGamal, DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 e TIGER
- Algoritmi di compressione: Zip, Zlib
- Supporto modulare per nuovi algoritmi crittografici
- Gestione delle date di scadenza per chiavi e firme

Caratteristiche tecniche

- Gestione forzata degli User Id standard
- Supporto multi-lingue: English, Danish, Dutch, Esperanto, French, German, Japanese, Italian, Polish, Portuguese (Brazilian), Portuguese (Portuguese), Russian, Spanish, Swedish, Turkish
- Sistema di help on-line
- Supporto integrato per HKP keyservers (wwwkeys.pgp.net).
- Supporto opzionale per la gestione di messaggi anonimi

Sistemi operativi supportati

GNU/Linux con x86, alpha, mips, sparc64, m68k o powerpc CPUs
FreeBSD con x86 CPU.
OpenBSD con x86 CPU. NetBSD con x86 CPU.
AIX v4.3,
BSDI v4.0.1 con i386,
HPUX v9.x, v10.x e v11.0 con HPPA CPU,
IRIX v6.3 con MIPS R10000 CPU,
MP-RAS v3.02,
OSF1 V4.0 con Alpha CPU,
OS/2 versione 2.
SCO UnixWare/7.1.0.
SunOS, Solaris su Sparc e x86,
USL Unixware,
Mac OS,
Windows 95,98,2000,XP e Windows NT con x86 CPUs.

Il Backend

- Sistema compatto a linea di comando sintassi:
  gpg [options] [files]

- Funzionalità ed interfaccia simile al Pgp.

- Utilizzabile come engine per applicazioni crittografiche.

- Gestione ottimizzata del flusso dati input/output (standard pipe).

Esempi d'utilizzo

• Generazione di una nuova coppia di chiavi pubbliche e private:
gpg –gen-key

• Cifratura del file msg.txt con la chiave pubblica di enrico@enricozimuel.net:
gpg -e -r enrico@enricozimuel.net msg.txt

• Decifrazione del file msg.txt: **gpg -d msg.txt**

• Firma di un file msg.txt: **gpg -s msg.txt**

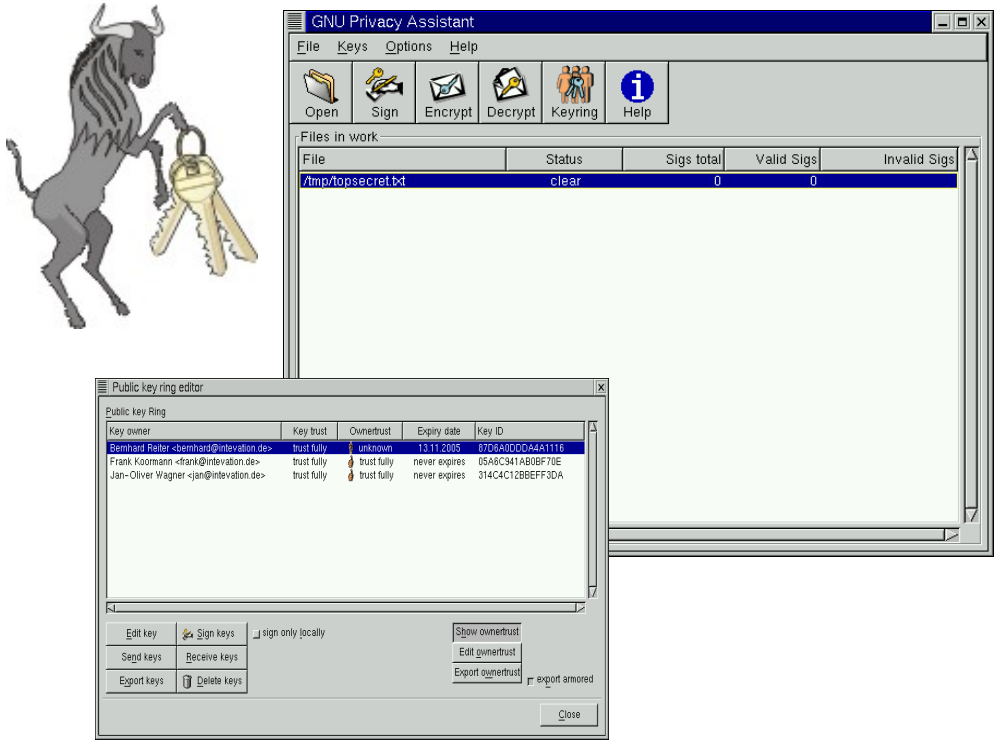
• Firma e cifratura del file msg.txt per l'utente enrico@enricozimuel.net:
gpg -se -r enrico@enricozimuel.net msg.txt

• Cifratura simmetrica del file msg.txt: **gpg -c msg.txt**

Il Front-end

• Esistono diverse interfaccie per GnuPG, la più famosa è GPA GNU Privacy Assistent, basata su GIMP Tool Kit (GTK).

• Altri front-end: Seahorse (Gnome), GnomePgp (Gnome), Geheimniss (Kde), TkPgp, pgpgpg (interprete di script pgp per gnupg), Mutt (gnupg email), MailCrypt (Emacs), pgp4pine, pgpenvelope, exmh, etc.



Un Front-end per sistemi Ms Windows

• WinPT è Windows Privacy Tools (WinPT) è un insieme di applicazioni multilingua per la firma e la crittografia digitale basato su GnuPG.

• Molto simile ai front-end del PGP per sistemi Win32, notevolmente più ridotta di dimensioni.

• La versione attuale è la 1.0rc2 (2a release candidate)

• E' distribuito con licenza GPL all'indirizzo http://www.winpt.org/

• Sullo stesso sito del progetto WinPT è possibile trovare il plug-in di GnuPG per i client di posta elettronica Outlook Express ed Eudora

La crittografia del GnuPG

• Basata su algoritmi standard non proprietari (possibilità di espansione con moduli software personalizzati).
Gli algoritmi di default sono:

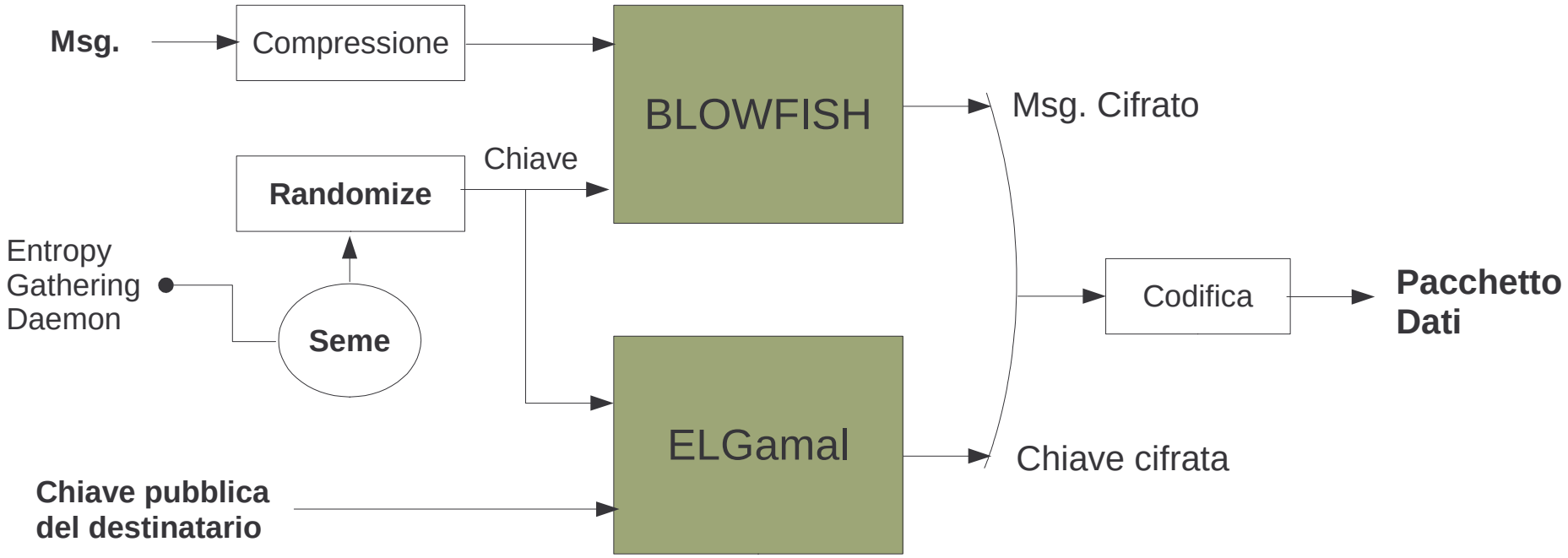
• DSA e Elgamal (asimmetrico) utilizzato per la generazione delle chiavi, la cifratura/ decifratura dei dati e la firma digitale

• Blowfish (simmetrico) per la cifratura “veloce” dei dati

• RIPE-MD-160 per la cifratura della *passphrases*

• Il Sistema utilizzato dal GnuPG per la cifratura e la decifrazione è del tipo ibrido= simmetrico + asimmetrico

La schema crittografico ibrido del GnuPG (esempio di encryption di un messaggio)



La release attuale, la 1.2.3

- La release attuale, la 1.2.3 rilasciata il 22 Agosto 2003, è una release stabile.

- Il codice in C è stato ottimizzato ulteriormente per il porting su altre piattaforme.

- Si tratta di una versione nata dopo 6 anni di sviluppo con un'architettura crittografica modulare con più di 20 algoritmi implementati.

- Dalla versione 1.0.3, 20 Settembre 2000, è presente il supporto dell'algoritmo RSA.

Il confronto con il PGP

• **PGP:**
Architettura crittografica chiusa (DSS, RSA, IDEA...).
Software proprietario della PGP Corporation Inc. - ex NAI Inc.
Presenza di features “poco trasparenti” vedi bug sulle ADK e discussioni sul rilascio dei codici sorgenti con la nuova release 8.0.2.

• **GNUPG:**
Architettura aperta (algoritmi modulari)
Software non proprietario (libero), licenza GPL.
Ottimizzazione del codice, engine leggero, features essenziali

Il progetto GPGME - GnuPG Made Easy

- GPGME è una libreria “semplificata” per l'accesso all'engine crittografico GnuPG.

- Supporta la gestione dei multi-thread

- Questa libreria fornisce un API crittografica PKI ad alto livello per la cifratura, la decifrazione, la firma digitale ed il management di un set di chiavi pubbliche e private.

- Attualmente la libreria è ancora in fase di sviluppo, esistono versioni instabili per il testing

La libreria libgcrypt

- Libgcrypt è una libreria crittografica in C/C++ di uso universale basata sul codice di GnuPG.

- Fornisce funzioni per tutti i principali mattoni della crittografia: cifrature simmetriche, algoritmi di hash, MAC, algoritmi a chiave pubblica, funzioni per grandi interi, numeri casuali e molte funzioni di supporto.

- E' un utile strumento per poter sviluppare applicazioni crittografiche in maniera efficiente sfruttando un crypto-engine collaudato, affidabile e soprattutto open source.

Lo standard OpenPGP (RFC 2440)

• Primo standard crittografico completo di stampo open source.

• Standard aperto per la cifratura/decifratura dei dati, firma digitale, autenticazione, gestione delle chiavi pubbliche/private

• Tentativo di affermare uno standard libero per applicazioni crittografiche in un ottica di difesa delle libertà digitali

• Perchè solo le istituzioni o grandi aziende possono utilizzare strong encryption?

• Per maggiori info: www.openpgp.org

OpenPGP Smartcards

• Progetto interessante per l'utilizzo di smartcard, PPC Card System, con lo standard OpenPGP

• Caratteristiche del progetto:
  - utilizzo di 3 chiavi indipendenti RSA a 1024 bit
  - generazione della chiave sulla smartcard
  - opzione di import delle chiavi
  - compatibilità ISO 7816-4 e -8

• Il progetto prevede anche lo sviluppo futuro di un modulo PAM in standard POSIX per le operazioni di login tramite smartcard in standard OpenPGP

Riferimenti bibliografici e siti Internet

- "Sicurezza digitale" B.Schneier (Tecniche Nuove, 2000)
- "The GnuPG Privacy Handbook (English)" pdf file
- "Replacing PGP 2.x with GnuPG" pdf file
- "Open source PKI Book" pdf file

- http://www.gnupg.org
- http://www.openpgp.org
- http://www.opensource.org
- http://www.lothar.com/tech/crypto
- http://www.counterpane.com/schneier.html
- http://www.pgp.com
- http://ospkibook.sourceforge.net/
- http://www.winpt.org
- http://www.enricozimuel.net