PGP luci e ombre.

Storia e evoluzione dello strumento per la privacy piu' usato al mondo

E-Privacy 2005

Firenze 28 / 05 / 2005

Obbiettivi

- Comprendere le potenzialità di PGP
- Conoscerne la storia
- Valutare le implementazioni disponibili
- Considerare le prospettive future

PGP: Panoramica generale

Cosa è PGP

- Strumento di crittografia a chiave pubblica nato per le masse
  - Cifratura
  - Firma digitale
- Key management decentralizzato
  - No Certification Authority
  - Si Web of Trust
- Standard IETF OpenPGP

A cosa serve

- Cifratura, Firma, Autenticazione
  - Email
  - Files/Disk
  - Files/Disk Wiping (low cost data destruction)
  - Fonia
  - Instant Messaging
  - Fantasia?

Chi lo usa

- Chiunque!
- Persone qualunque
- Avvocati / Notai / Manager
- Forze dell'ordine
- Istituti finanziari (regolamentazioni interne/ esterne, rapporti con clienti)
- Ambasciate
- Ma anche...organizzazioni criminali di ogni genere
- In generale è usato in

Ambienti ad elevata competitività

OpenPGP vs X509v3

- È possibile centralizzare, autorizzare, “legalizzare” con certificati X.509v3
- La firma digitale come strumento di certificazione dei documenti e delle email:
  - Firma Digitale
  - Posta Elettronica Certificata
- Allora perché OpenPGP quando c’è già S/MIME con i certificati X509v3?
- Gerarchie vs Relazioni Sociali
- Controllo vs Libertà

Web of Trust

- L’affidabilità di una chiave è determinata dall’affidabilità delle “persone” che la hanno firmata.
- Key Signing party
- Key Servers

La storia di PGP

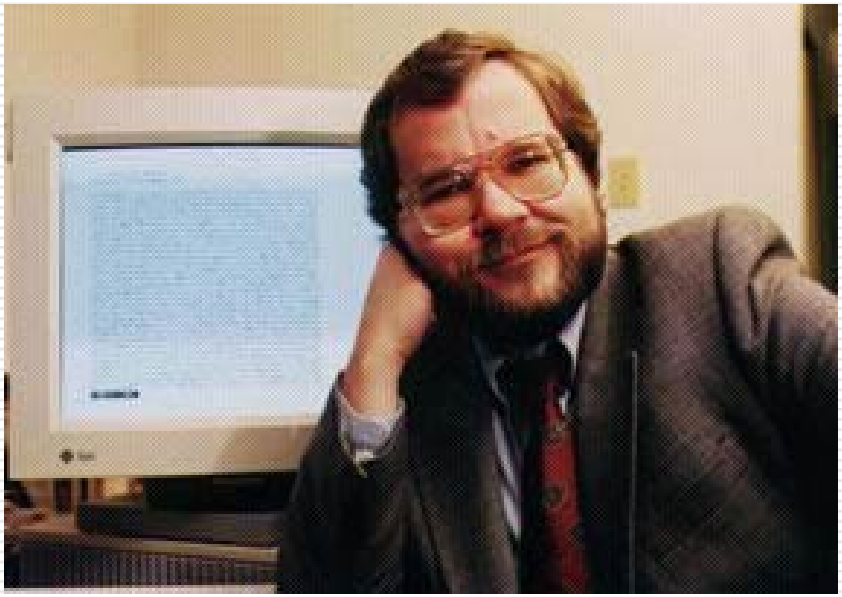
Panoramica di OpenPGP dalla nascita a oggi

Il contesto del concepimento

- È l'epoca del DES a 56bit
- Gli strumenti crittografici sono considerati armi
- USA, 1991. Il Senate Anticrime Bill 266 recita:
- "It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law."
- USA, 1993. L'NSA propone il "Clipper Chip"

La nascita

- 1991: Philip Zimmermann rilascia la versione 1.0 di PGP



I perchè

- It's personal. It's private. And it's no one's business but yours.
- PGP empowers people to take their privacy into their own hands.There has been a growing social need for it. That's why I wrote it.

Diffusione e Esportazione

- Negli stati uniti era vietato esportare strumenti crittografici che supportassero una specifica lunghezza della chiave
- Distribuito come “US only” nel 1991 su Peacenet ha avuto la sua diffusione grazie anche a Kelly Goen

- Telefoni pubblici, Redbox, Accoppiatore Acustico e il gioco è fatto:
  - PGP risiede su tantissime BBS, gruppi USENET, siti FTP negli stati uniti (US ONLY!)…. Per qualche minuto, prima di arrivare un europa, giappone e australia!
- Dal 1993 al 1996 Philip Zimmermann e Kelly Goen sono indagati dalla dogana statunitense e dal gran jury

La versione 2.0 con l'Europa

- Coinvolti sviluppatori svizzeri, neo zelandesi e statunitensi
- Rilasciata ad Amsterdam per superare le limitazioni sull'export
- L'algoritmo simmetrico svizzero IDEA entra in PGP

Dalla GPL all'impresa

- Maggio 1996(finiti i problemi legali!) Philip Zimmermann fonda la PGP Inc.
- Fino alla versione 2.5 era GPL
- La prima release è PGP 5.0
  - Licenza "free for non commercial use"
  - Codice sorgente visualizzabile ma non distribuibile

PGP Non è più "Free Software!"

Nuovi problemi legali

- RSA Data Security denuncia Philip Zimmermann per violazione di patent
  - L'algoritmo RSA era sotto patent, ora scaduto!
  - Si risolve in nulla di fatto

PGP acquisto dalla NAI

- La società NAI acquisisce il “prodotto” PGP
- Lo sviluppo è orientato alla creazione di una “security suite” PGP (data-mail-disk-vpn-firewall-voice)
- Philip Zimmerman lavora ora per la NAI (la stessa che riceve dalla NSA la commessa per sviluppare SELinux)

OpenPGP: gli standard

- Promosso dalla NAI nel novembre 1998 per standardizzare PGP
- RFC 2440 (“OpenPGP Message Format”) a seguito del RFC 1991 (“PGP Message Exchange Format”)
- Attualmente supportato dalla “OpenPGP Alliance”:
  - Authora - Glück & Kanja - Gnu Privacy Guard - Hush Communications - LokTek - Network Associates - PGP Corporation - Qualcomm - SSH - Tovaris - Toxik Technologies - Veridis - Zimmermann & Assoc

Ipotesi di complotto?

- Philip Zimmerman rilascia una intervista raccontando di avere ricevuto pressioni per l'inserimento di backdoor e non rilascio del codice sorgente nelle release successive
- Giorni dopo i toni cambiano ma…

2002: Le cose non si mettono bene

- Philip Zimmerman lascia la NAI
- NAI mette in vendita la divisione PGP per mancanza di profitti
- La comunità è allarmata e incuriosita

PGP Corp: Nuove strategie

- Viene acquisita la tecnologia e il brand PGP
- Nuova immagine
- Nuova linea di prodotti
  - PGP 9
  - PGP Universal Server
  - PGP Centralized Administration (ADK feature!)
  - Edizione gratuita sempre più limitata!
    - Ma con soli 59 EUR la Home Edition…

Le comunità reagisce

- Imad Alfaied continua lo sviluppo e il supporto di PGP nella versione chiamata C-KT (Cyber Knights Templar) http://www.ippgp.com
- Il ministero dell'interno tedesco finanzia lo sviluppo di GnuPG, implementazione OpenSource dello standard OpenPGP
- Iniziano a comparire società che producono soluzioni "OpenPGP compatibile"

PGP CKT di Imad Alfaied (1)

- Il giovane Imad Alfaied continua il supporto di PGP 6.5.8 (di cui sono disponibili i sorgenti)
- PGP-CKT viene supportato su Windows XP
- Vengono implementate feature “alternative” come chiavi da 16k bit
- Ultima release rilasciata 6.5.8ckt06

PGP CKT di Imad Alfaied (2)

- 11 Luglio 2001:

  "From: Imad R. Faiad matic@cyberia.net.lb

  Newsgroups: comp.security.pgp.tech

  "And please do not mentioned the ckt builds again, because it is no more."

- Senza spiegazioni Imad elimina ogni file incluso il sito.
- Denuncia della PGP Corporation? Pressioni governative? Impossibilità di controllo sulle release?
- Rimane oggi il mirror contenente l'abbandonware: ftp://ftp.zedz.net/pub/crypto/incoming/pgp658ckt06.zip

GnuPG

- Nasce il 7 settembre 1999 come progetto del governo tedesco
- Oggi alla versione 1.4.1 stable come programma e librerie (GPGME)
- GPG 1.9 supporta S/MIME
- GPG 2.0 sarà un supporto crittografico completo OpenPGP – S/MIME
- Non supporta IDEA essendo questo brevettato. Plugin esterno disponibile.

Cryptoex: L'alternativa a PGP

- Linea di prodotti OpenPGP e S/MIME client e server. Integrazione totale
- 7 Marzo 2005: PGP Corporation compra la Glück & Kanja Technology AG, proprietaria della linea di prodotti OpenPGP Cryptoex
- Morale: Se non puoi combatterli, comprali!

OpenSource OpenPGP

Le soluzioni OpenSource

OpenSource OpenPGP Solutions

- Il problema è l'integrazione e il supporto per le masse
- Il problema è il costo di gestione
- Il problema è la certificazione della qualità

OpenSource OpenPGP Solutions

- Le soluzioni OpenPGP possono essere distinte in:
  - Engine

    Motori con la logica di OpenPGP
  - Plugin di integrazione

    Estensioni abilitati all'utilizzo di OpenPGP in altre applicazioni (email, file manager, disk encryption, disk wipe, etc)
  - Suite applicative

    Click, Click, Click e tutto è installato
  - Sviluppo

    SDK e librerie
  - Servizi

    Servizi che usano OpenPGP

OpenSource OpenPGP Engine

- GnuPG
  - Supporto multipiattaforma molto solido
  - Interfaccia a riga di comando
- BouncyCastle
  - Supporto Java S/MIME, OpenPGP
- MyPG (sperimentale)
  - Progetto sperimentale

OpenSource OpenPGP Plugin

- WinPT
  - Windows Installer
  - Integrato in explorer
  - Integra GnuPG
- GPA (Gnu Privacy Assistant)
  - Key Management grafico
- 3G Data Outlook Plugin
  - Outlook GnuPG support
- Loop-AES - CrossCrypt
  - Linux/Windows encrypted filesystem support
- PSI
  - Secure IM (Jabber/MSN/AIM/ICQ)

OpenSource OpenPGP Suite

- GPP – Gnu Privacy Project
- Suite Applicativa sponsorizzata dal ministero dell'interno tedesco che include:
  - GnuPG
  - WinPT
  - GPA
  - Outlook Plugin

OpenSource OpenPGP Library

- GPGME
  - GnuPG Made Easy
    - Anubis
    - PHPgpg
- Python gpg (pygpg)
- Perl OpenPGP

OpenSource OpenPGP Services

- Anonymous Remailer
  - Mixmaster
- Husmail
  - OpenPGP encrypted email service

- Nuova realtà propongono servizi OpenPGP compliant

OpenPGP: quale futuro?

Il destino di OpenPGP

Progetto Aegypten

- Usare OpenPGP in una infrastruttura S/MIME
- Finanziato dalla *Bundesamt für Sicherheit in der Informationstechnik (BSI)*
- Creare client opensource compatibili con tutti gli standard crittografici

OpenPGP Card

- Kernel Concepts in germania produce OpenPGP Card
- G10 sviluppa il supporto GnuPG OpenPGP Card
- Generazione on chip di chiavi RSA 1024bit OpenPGP
- Sicurezza delle smartcard

OpenPGP Telephony

- Secure Opensource Telephony Challenge
  - X509v3
  - OpenPGP
  - Symmetric Key
- Abbandonware PGP Phone

Conclusioni

Legislazioni restrittive: i fatti nostri

- Non guardiamo solo agli anni 90 degli USA ma al 2005 in europa
- Inghilterra
  - Importanza della Deniability
- Francia
  - Crittografica limitata e controllata
  - Regole complesse per prodotti crittografici

Domande?

Fabio Pietrosanti (naif) / naif@s0ftpj.org

S0ftpj http://www.s0ftpj.org

E-privacy http://e-privacy.firenze.linux.it