E-PRIVACY 3,14-16

TOOLS per giornalisti

Efrem Zugnaz

Ordine dei Giornalisti del Friuli Venezia Giulia

Camera di Commercio di Udine, sala Valduga – 14 marzo 2016

Open Source PASSWORD MANAGER – GESTIRE LE PASSWORD (diverse) DA UN UNICO PUNTO

https://www.keepassx.org/

Downloads

Source code

Source code tarball v2.0.2

Mac OS X

Binary bundle for MacOS X >= 10.7
Binary bundle v2.0.2

Windows

Binary bundle for Windows >= Vista (requires security update MS09-015 on Vista)
ZIP bundle v2.0.2

Verify downloads

GPG signatures

All downloads and Git tags are signed with the key 0xFE22C6FD83135D45

Git development repository

GitHub: https://github.com/keepassx/keepassx

Version 0.4

Downloads of the 0.4 series

Release archive

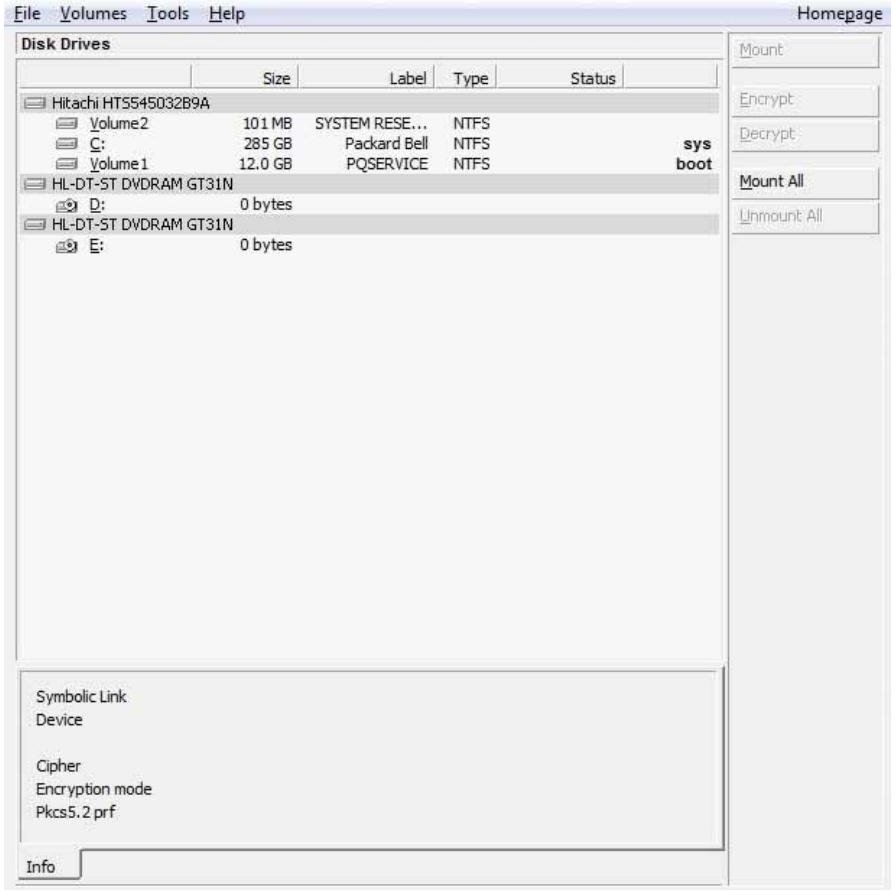
Downloads of old release

http://keepass.info/

DiskCryptor: Cifrare HD e chiavette …

Supporta AES, Twofish, Serpent encryption algorithms, incluse le loro combinazioni!!!.
PadLock extensions on VIA processors.
storage devices.

Open license GNU GPLv3.

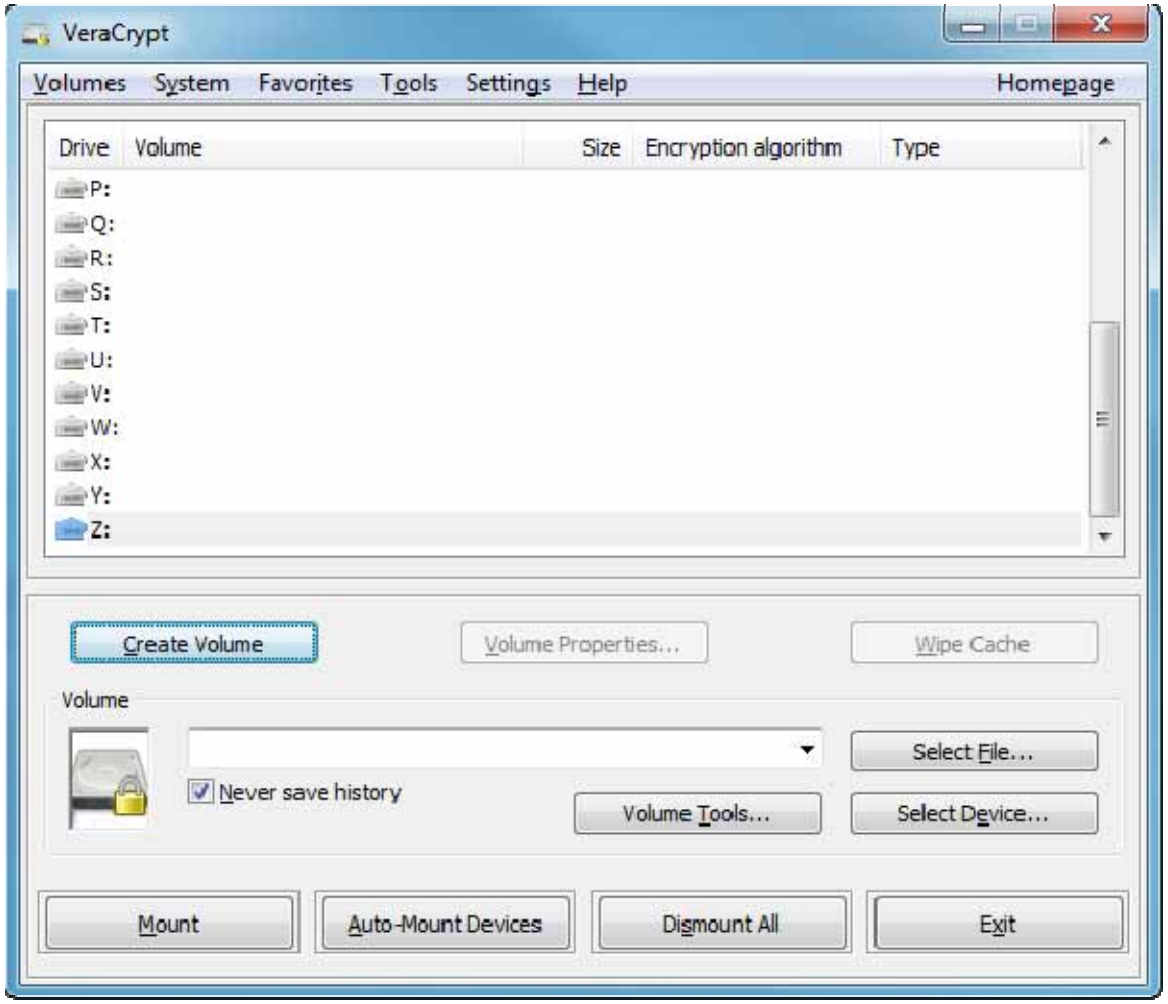


https://diskcryptor.net/wiki/Main_Page

Veracrypt (Truecrypt)

VeraCrypt è un "on-the-fly" (OTFE).

Può creare un disco virtuale crittografato mediante l'utilizzo di un file o crittografare un'intera partizione oppure, su Windows (eccetto Windows 8 e Windows 10 con UEFI o GPT), l'intero hard disk con un'autenticazione all'avvio.



https://veracrypt.codeplex.com/

TrueCrypt
TrueCrypt is a freeware utility used for on-the-fly encryption (OTFE)
https://truecrypt.ch/

AES Crypt is an advanced file encryption utility that integrates with the Windows shell or runs from the Linux command prompt to provide a simple, yet powerful, tool for encrypting files using the Advanced Encryption Standard (AES). A Java library is also available for developers using Java to read and write AES formatted files.
NOTE: Crypt4All is the first Android program compatible with AES Crypt
http://www.aescrypt.com/

CipherShed
https://ciphershed.org/

EncFS – GOOD 4 CLOUDS!!
http://www.arg0.net/encfs
http://www.howtogeek.com/121737/how-to-encrypt-cloud-storage-on-linux-and-windows-with-encfs/

Windows BitLocker

Windows BitLocker & "Bitlocker To Go" Drive Encryption is a data protection feature in **Windows Vista Enterprise and Windows Vista Ultimate for client computers and in Windows Server 2008**.
BitLocker protects against data theft or exposure on computers that are lost or stolen, and offers more secure data deletion when computers are decommissioned.
Bitlocker To Go (BTG) is essentially Bitlocker for external drives. It's full volume encryption for all your USB drives:
https://technet.microsoft.com/en-us/library/cc732774.aspx

LibreCrypt

LibreCrypt (formerly DoxBox) Supports numerous hash (including SHA-512, RIPEMD-320, Tiger) and encryption algorithms (Including AES, Twofish, and Serpent) in several modes (CBC, LRW, and XTS), giving more options than any other disk encryption software

https://github.com/t-d-k/LibreCrypt

GostCrypt

The Gostcrypt project has been launched at the end of 2013 as fork of the (late) Truecrypt project.
http://www.gostcrypt.org/

FileVault

FileVault is a method of using encryption with volumes on Mac computers.
Created by Apple FileVault is a method of using encryption with volumes on Mac computers. Encryption and decryption are performed on the fly.
FileVault 2 uses full disk, XTS-AES 128 encryption to help keep your data secure.
Using FileVault 2, you can encrypt the contents of your entire drive.
http://support.apple.com/kb/HT4790

Free File Camouflage

With Free File Camouflage you can hide and protect your files inside a jpeg image!
http://www.myportablesoftware.com/freefilecamouflage.aspx

…. E centinaia di prodotti a pagamento per tutte le piattaforme


Install
Choose a security key:
Disk encryption protects your files in case you lose your computer. It requires you to enter a security key each time the computer starts up.
Any files outside of Ubuntu will not be encrypted.
Choose a security key:
Good password
Confirm the security key:
Warning: If you lose this security key, all data will be lost. If you need to, write down your key and keep it in a safe place elsewhere.
For more security:
Overwrite empty disk space
The installation may take much longer.
Quit
Back
Install Now

MAIL e COMUNICAZIONE CIFRATE:

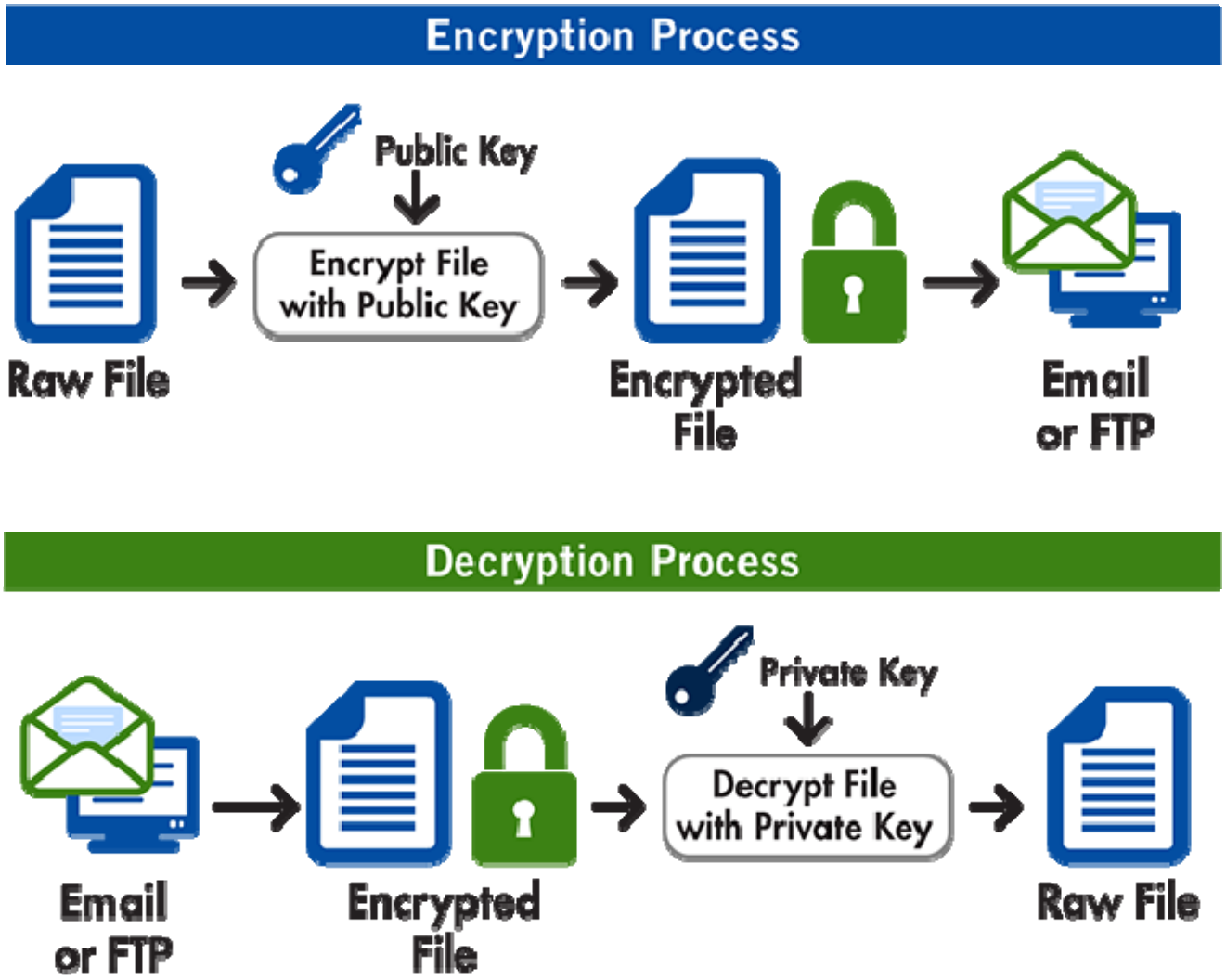
OpenPGP ALLIANCE

Phil Zimmermann in 1991

RFC 4880

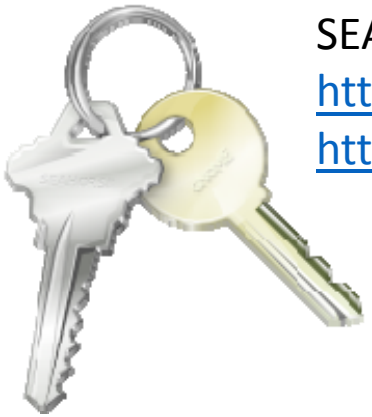
Standard Internet per l'interoperabilità dei messaggi tramite crittografia assimmetrica

GNU PG
https://gnupg.org/



Thunderbird

http://guide.debianizzati.org/index.php/Mail_criptate_e/o_firmate_con_standard_OpenPGP_usando_Icedove/Thunderbird_ed_Enigmail



SEAHORSE
https://wiki.gnome.org/Apps/Seahorse
https://fedoraproject.org/wiki/Creating_GPG_Keys

EVOLUTION
http://www.secure-my-email.com/clients_evolution.php
https://fedoraproject.org/wiki/Using_GPG_with_Evolution

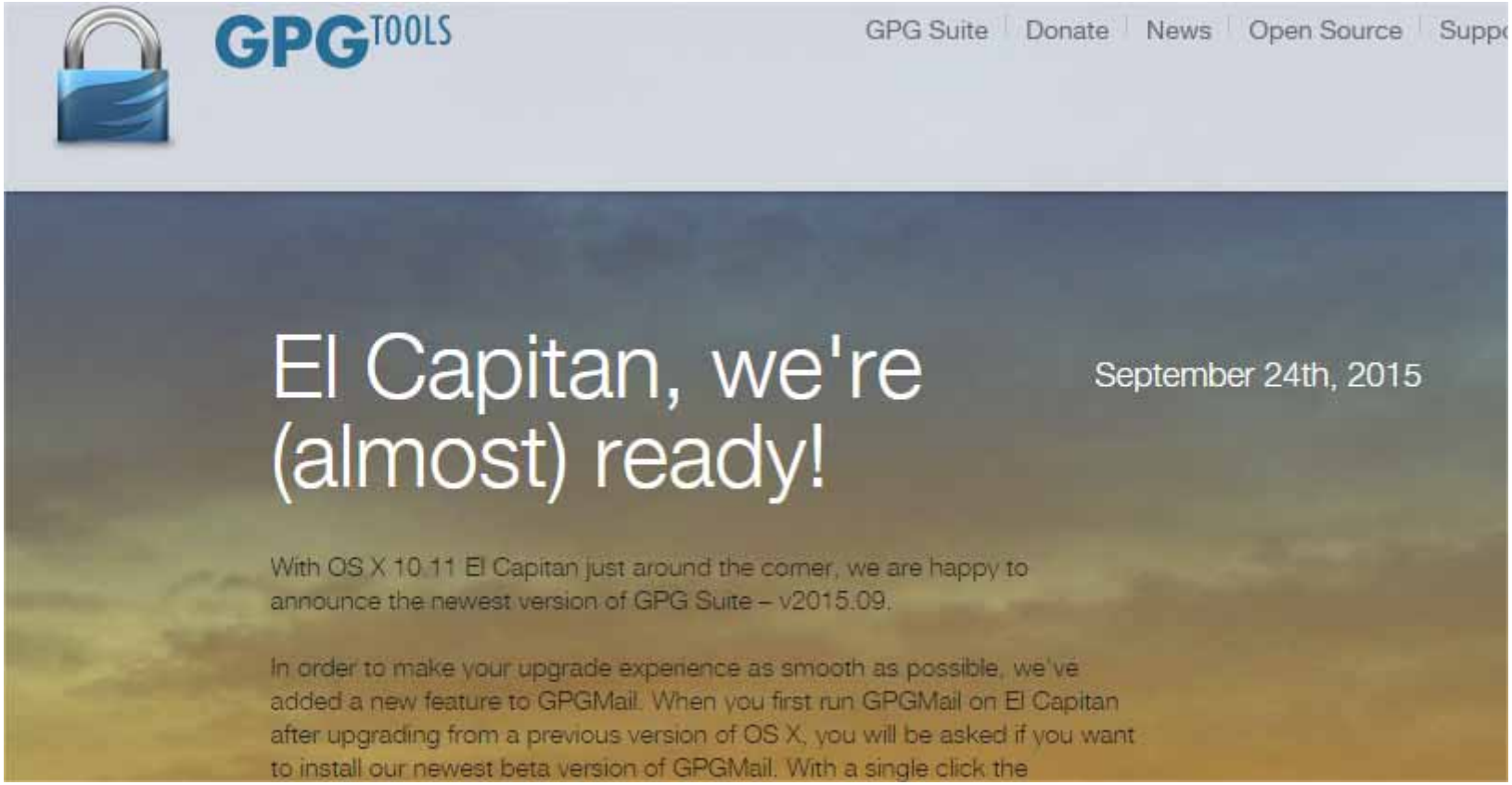
KGPG
https://www.kde.org/applications/utilities/kgpg/

KMAIL
https://www.kde.org/applications/internet/kmail/

SHARE PARTY

https://www.gpg4win.org/

Matrice di creazione certificati e chiavi
Gestione con outlook



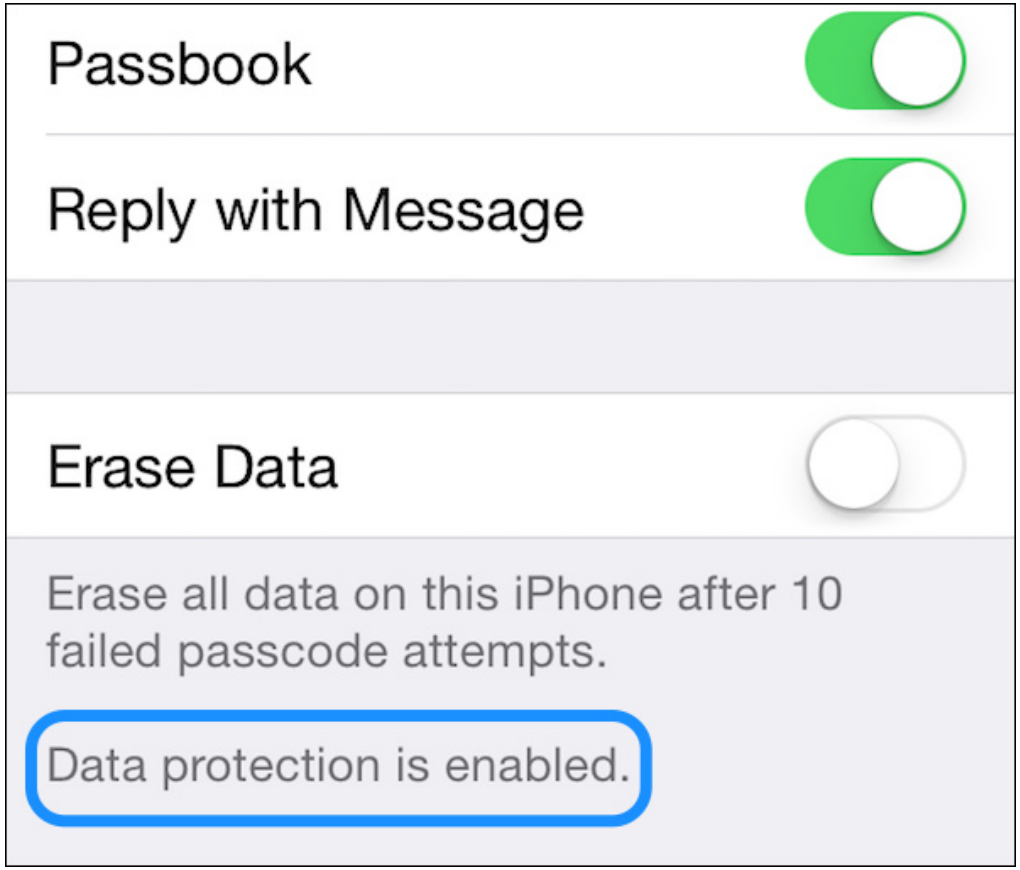
https://gpgtools.org/

Anche per OS X

Tor (acronimo di **The Onion Router**) è un sistema di comunicazione anonima per Internet basato sulla seconda generazione del protocollo di *onion routing*. Tramite l'utilizzo di Tor è molto più difficile tracciare l'attività Internet dell'utente; di fatti l'uso di Tor è finalizzato a proteggere la privacy degli utenti, la loro **libertà** e la possibilità di condurre delle comunicazioni confidenziali senza che vengano monitorate.

OONI (Open Observatory of Network Interference) è una piattaforma costruita per eseguire e pubblicare misurazioni utili ai fini di studiare il fenomeno della censura e della sorveglianza su internet. Essa si compone di un software open source multipiattaforma, che pubblica in formato aperto le misurazioni raccolte, e di un archivio di oltre 150000 misurazioni eseguite in circa 70 stati

https://www.torproject.org/



Dati cifrati, con iOS 8 iPhone è ancora più blindato

SU iPhone 6 e iPhone 6 Plus è decisamente aumentato con il nuovo sistema di cifratura dei dati integrato su iOS 8 (apple A8)

iDevice (ndr per intenderci quelli equipaggiati dal chip Apple A7) avevano compiuto passi da gigante rendendo assai difficoltoso il cracking.
Apple non dispone della "backdoor", vale a dire quella specie di chiave di servizio che permette di aggirare tutte le varie procedure di sicurezza.
James Comey, direttore dell'FBI, di recente ha fatto notare come a Cupertino abbiano esagerato (forse troppo) con la privacy..

iPhone 6 Plus ed **iPhone 6** sono più sicuri? I "vecchi" meccanismi di **cifratura dei file** richiedono l'utilizzo di una password e, attraverso quella procedura nota come **KDF** (Key Derivation Function) la trasformano in chiave cifrata. Qual è il problema? Le password scelte quasi mai sono sufficientemente robuste.
Il ricorso a funzioni del calibro di **PBKDF2** (Password Based Key Derivation Function 2) Rallentano in maniera drastica le prove di login, complicando, e di molto, il cracking.
Apple non ha questo ma punta sull'**UID** (Unique Device Identifier) che altro non è che una **chiave AES 256-bit** archiviata nell'hardware del dispositivo ed ottenibile come versione cifrata del codice solo via software. A Cupertino confermano che non conoscono il codice effettivo. La presenza di "**Secure Enclave**", coprocessore integrato sia su Apple A8 che su Apple A7, serve proprio a salvaguardare le impronte digitali del possessore dell'iPhone ed i dati del codice di accesso.
iPhone 6 e su **iPhone 6 Plus**, l'utente scegliendo una password di 6 caratteri tra lettere minuscole, maiuscole e numeri, i tentativi di cracking necessiterebbero di più di 5 anni e mezzo adottando password e UID basate su funzioni **PBKDF2-AES**.

Android a partire dalla versione 2.3.4 (Gingerbread)
ha introdotto la cifratura (crittografia) del dispositivo e della scheda SD

https://tails.boum.org

Tails (acronimo di The Amnesic Incognito Live System) è un sistema operativo basato su Debian e pensato per preservare **riservatezza** e **anonimato** dei suoi utilizzatori. Tutte le connessioni verso l'esterno vengono inoltrate esclusivamente attraverso il sistema di comunicazione anonima Tor e tutte le connessioni dirette in entrata sono bloccate in quanto non anonime. Il sistema è inoltre progettato per essere utilizzabile direttamente da un supporto rimovibile come un live CD o un live USB e per non lasciare alcuna traccia sul computer, a meno di non ricevere esplicita richieste contrarie da parte dell'utente. La maggior parte del supporto economico allo sviluppo di Tails è stato garantito dal Progetto Tor.

Tails contiene Iceweasel, un browser nato da Mozilla, che ha già pre-installato un client di rete Tor; supporta lo standard **OpenPGP** che serve a cifrare messaggi di posta elettronica e testi; usa Pidgin e il client OTR (Off-the-Record Messaging) che devono essere installati da tutti gli interlocutori, e non dipendono dal protocollo utilizzato per cui permettono di cifrare i messaggi con qualsiasi programam di messaggistica si sitia utilizzando.

TAILS è un software libero realizzato sotto licenza GNU/GPL (versione 3 o superiore).

I VANTAGGI:

TAILS e' una di queste versioni “live”, che appunto:

1.Non lascia traccia del suo utilizzo sul pc

2.Impedisce, anche per sbaglio, di “uscire” dalla rete Tor e di rendersi quindi intercettabile tramite le usuali tecniche di sorveglianza

3.Permette, se usato da chiavetta USB, di utilizzare quando necessario un'area crittografata ed inaccessibile della chiavetta stessa per memorizzzare file, mail e preferenze che fosse necessario conservare.

Ad esempio, un lifesaver del giornalista che debba comunicare con la redazione mentre si trova in paesi poco liberali, od addirittura in zone di guerra.

Account usa e getta
Essere curiosi e Informarsi (Venire ad eventi come questo)
Tenere traccia dei propri date ed averne cura…

http://blog.marsilioeditori.it/files/2012/04/Il_giornalista_hacker.pdf