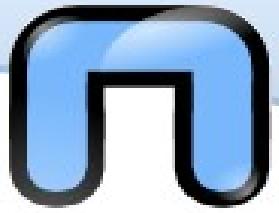
netstudent

Strumenti Open Source per la Difesa della Privacy

<max@netstudent.polito.it>

Corso GNU/Linux Avanzato
Torino, 2010.05.25



Obiettivi

- Focalizzare concetti cardine quali privacy, gestione dei rischi, sicurezza, crittografia ed anonimato.
- Fornire una vista d'insieme sui problemi legati alla privacy delle informazioni digitali e sulle tecnologie impiegabili come soluzioni.
- Presentare i software open source che contribuiscono alla tutela della privacy e indicare puntatori utili per approfondirne il funzionamento.

Sommario

- Il concetto di Privacy.
- Difesa delle informazioni memorizzate sul proprio computer.
- Difesa delle informazioni trasmesse in rete.
- Difesa delle informazioni memorizzate presso terze parti fornitrici di servizi online.

Privacy - 1

Una definizione di “privacy”:

il diritto che un individuo ha di mantenere private le informazioni che riguardano la sua persona e di comunicarle pertanto solo quando e a chi vuole.

Privacy - 2

- Quali categorie di informazioni possiamo desiderare mantenere private?
  - Orientamento politico, fede religiosa, abitudini sessuali, dati clinici.
  - Composizione famigliare, residenza, spostamenti.
  - Dati e rapporti di lavoro, informazioni fiscali, status sociale.

Privacy – 3

Perchè nascondere queste informazioni agli altri?

"*Se non sei un delinquente, non hai nulla da nascondere*"

Ma allora come mai:

- i risultati delle analisi mediche, le comunicazioni bancarie,.. sono inviati in busta chiusa o trasmessi al telefono esclusivamente al paziente/cliente interessato?
- rispettiamo l'obbligo di segreto professionale?
- votiamo con scrutinio segreto?
- l'identità dei minorenni è tutelata nei media?

Privacy - 4

- Dall'esperienza di tutti i giorni nel mondo reale è evidente che esistono ragionevoli motivi per mantenere private informazioni sulla propria persona.
- La tipologia e la quantità delle informazioni che è desiderabile non vengano rese pubbliche varia in base alla sensibilità dell'individuo e al contesto in cui ci si trova.
- La fuga di dati personali può causare imbarazzo, discriminazione, danno alla reputazione pubblica e professionale, rischio di truffa e furto d'identità, persecuzione, perdita di tutela e diritti (es assicurazioni)...

Privacy ed ICT - 1

- L'evoluzione delle tecnologie informatiche e delle telecomunicazioni pone un numero crescente di rischi per la privacy degli utenti e richiede metodi di protezione delle informazioni complessi e maggiore consapevolezza da parte degli utenti.
- Le informazioni trasmesse in rete possono essere memorizzate su più computer e persistere per un tempo sconosciuto (es: e-mail).
- Ogni comunicazione in rete lascia molteplici tracce sui computer mittente e destinazione (es: client/server log, cache).
- Non è banale cancellare completamente un dato e ogni sua traccia da un computer.

Privacy ed ICT - 2

•Esistono software che abbinati a buone pratiche permettono di difendere la segretezza dei propri dati personali.

•Come nel mondo reale, anche in quello digitale è necessario sacrificare alcuni vantaggi se si vuole ottenere un elevato livello di privacy (es: posta assicurata): velocità di elaborazione, comodità d'uso, possibilità di recupero dei dati, limiti alla disponibilità delle informazioni,...

•Scegliere le soluzioni che implementano la privacy significa stabilire dei compromessi per gestire i rischi.

Gestione dei Rischi - 1

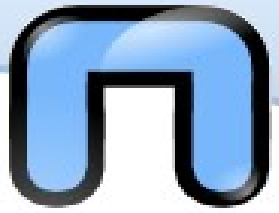
- Per definire le soluzioni da implementare per tutelare la propria privacy bisogna analizzare, valutare e gestire i seguenti punti:
  - Asset: beni (informazioni) che hanno un valore per chi li possiede e si desidera proteggerli (es: e-mail, transazioni online,...).
  - Minacce: danni che possono essere provocati agli asset (es: perdita di confidenzialità, integrità, disponibilità,...).

Gestione dei Rischi - 2

- Rischi: probabilità che una specifica minaccia si concretizzi e danni che l'asset colpito riporterebbe (es: se tengo tutti i miei dati a casa anzichè portarli con me sul portatile o una chiavetta USB è meno probabile che qualcuno riesca ad accedervi). Attenzione a non sovrastimare e attuare soluzioni complicate per minacce improbabili o sottostimare e non reagire alle minacce più comuni e frequenti.
- Avversari: persone o entità che possono costituire una minaccia nei confronti di un asset (es: concorrenti, colleghi, criminali, controparti in contenziosi legali, ricattatori, governi,...)

Gestione dei Rischi - 3

- Si considerano le interazioni tra asset, minacce, rischi ed avversari e si definiscono le protezioni da implementare per garantire il livello di privacy desiderato:
  - Quali asset si tentano di proteggere?
  - Quali rischi sussistono per questi asset?
  - In che misura le protezioni scelte mitigano questi rischi?
  - Le soluzioni implementate pongono altri rischi non presenti in origine?
  - Queste soluzioni quali costi e compromessi impongono?



Sicurezza e Privacy - 1

- Affinchè i software per la protezione della privacy possano svolgere il proprio compito efficacemente, il computer su cui girano deve essere amministrato attuando tutte le migliori pratiche per la messa in sicurezza del sistema operativo e delle applicazioni.
- La *sicurezza* è condizione necessaria, ma non sufficiente, per la privacy.

Sicurezza e Privacy - 2

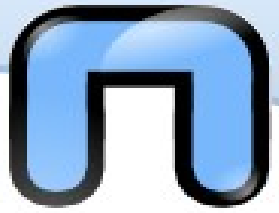
- Fanno parte del processo di messa in sicurezza:
  - Hardening del sistema: bootloader password, eliminazione servizi inutili, ssh key auth, flag nosuid/noexec/.. partizioni fs, utenti e permessi, logging, sincronia data/ora ntp, sudo, firewall, patch kernel,...
  - Installazione aggiornamenti software e verifica firma OpenPGP o hash.
  - Protezione da malware: antivirus, browser plugin noscript, verifica certificati server web HTTPS (anche self-signed, malformati o scaduti con il plugin Perspectives per FF3 http://www.cs.cmu.edu/~perspectives/firefox.html).

Privacy dati locali - 1

- Regole auree per proteggere la privacy dei dati memorizzati in locale sul proprio computer:
  - Un avversario non può accedere a ciò che non c'è. Sviluppare una policy di data retention: tenere sul computer i dati personali che sono davvero necessari e di uso frequente, archiviare su supporti rimovibili tutti i dati importanti (possibilmente cifrandoli) e cancellare tutte le informazioni che non servono. Definire la frequenza di archiviazioni e cancellazioni e per quanto tempo tenere i dati archiviati prima di distruggerli.

Privacy dati locali - 2

- *Cifrare* tutto quello che non è stato archiviato o cancellato!
- Limitare la disponibilità dei dati cifrati. Raggruppare i dati che si vogliono proteggere in base alla frequenza di accesso e alla loro importanza, cifrarli con chiavi diverse e tenerli separati nel filesystem. Durante la sessione di lavoro decifrare solo i gruppi di dati che servono così che un avversario che violi il sistema non abbia accesso alla totalità dei dati protetti.



Cifratura di dati locali - 1

- Software per la cifratura del disco in modalità trasparente:
  - dm-crypt e FreeOFTE
  - loop-AES
  - TrueCrypt e DiskCryptor
  - geli http://www.tollari.org/~err/index.php?page=bsd#geli full encrypted system
- Software per la cifratura di file:
  - GNU Privacy Guard (GPG)
  - Elettra

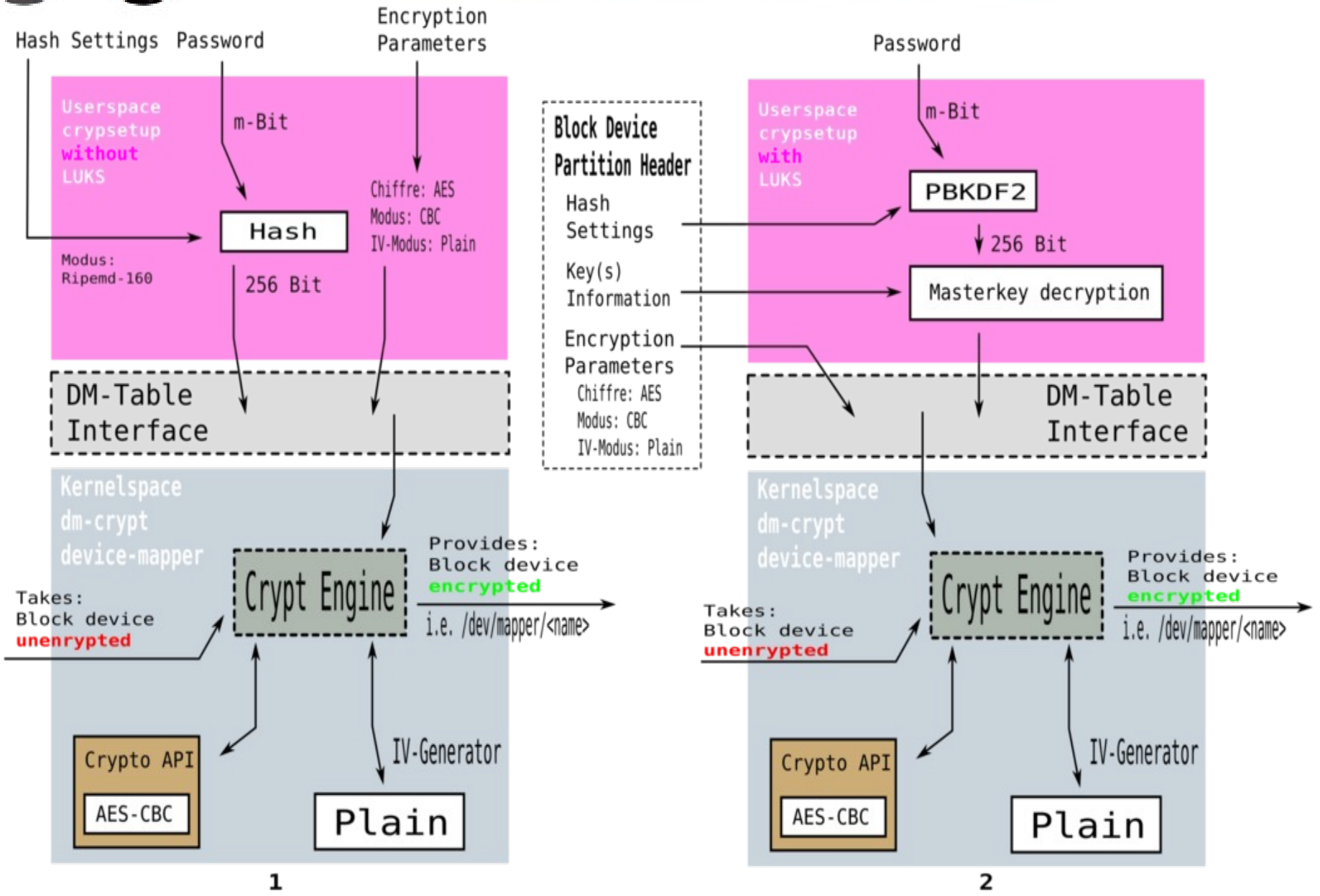
dm-crypt e FreeOFTE - 1

- Sottosistema di cifratura del disco incluso nel kernel Linux 2.6+, licenza GPL, http://www.saout.de/misc/dm-crypt/
- Usa le routine del framework crittografico Crypto API del kernel Linux, disponibili molti algoritmi di cifratura (AES, Blowfish, Twofish, Serpent) e tutti i principali block cypher e funzioni di hash.
- É implementato come target del device mapper e può essere impilato ed operare al di sopra di partizioni, volumi RAID software, volumi logici LVM e file. Quando il filesystem cifrato viene montato è richiesta la passphrase per sbloccare la masterkey, quindi le operazione di lettura e scrittura avvengono in modo trasparente all'utente come se si operasse su un volume in chiaro.

dm-crypt e FreeOFTE - 2

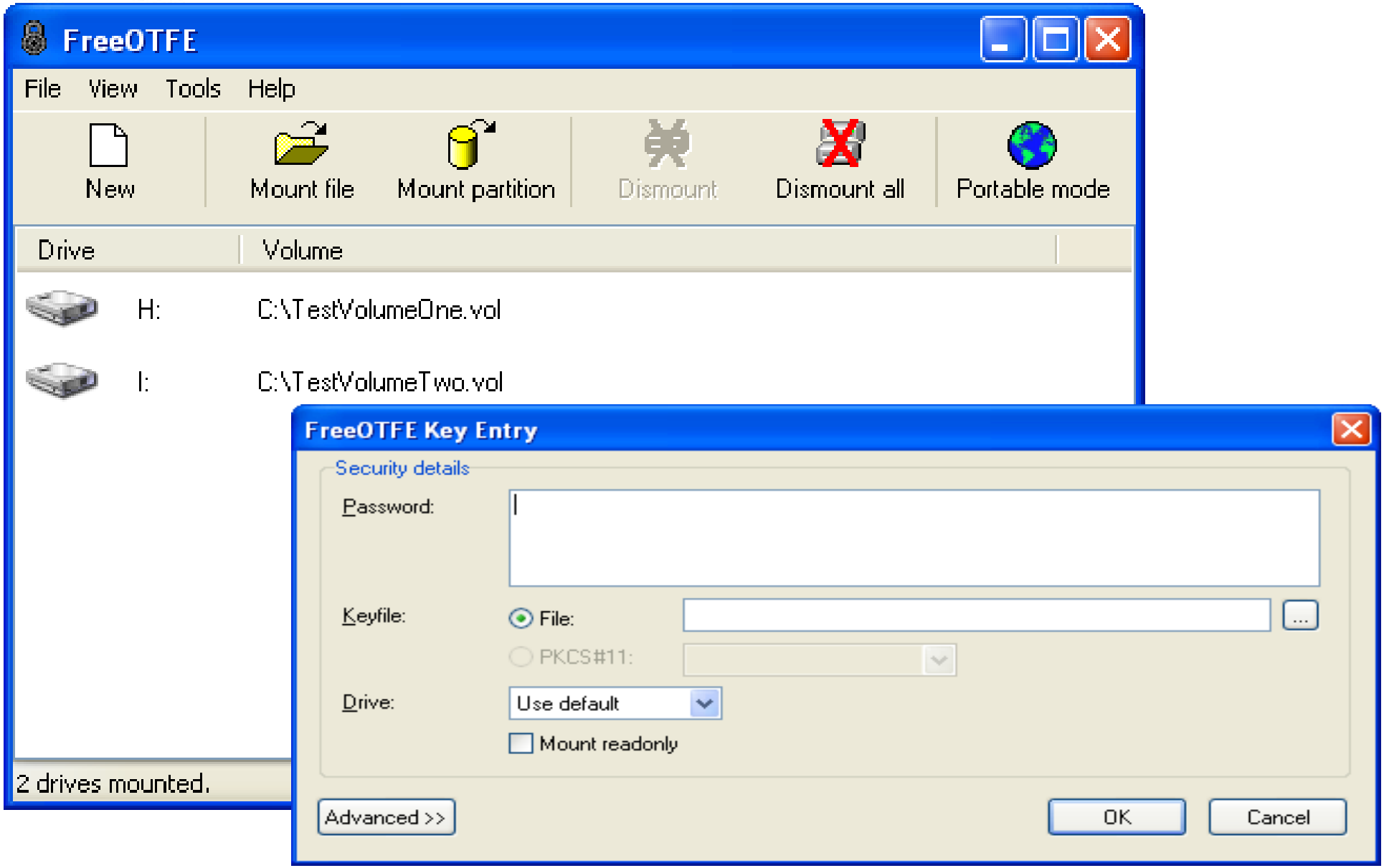
- dm-crypt attraverso l'intefaccia cryptsetup supporta LUKS (Linux Unified Key Setup), un formato standard per la memorizzazione di dati cifrati su disco garantisce interoperabilità tra distribuzioni. Le informazioni di setup sono tutte contenute nell'header del block device virtuale: questo consente gestione di password utente multiple e migrazione dei dati indolore. http://code.google.com/p/cryptsetup/
- dm-crypt supportato anche dall'installer di Debian.
- Setup and manage on-disk encryption with dm-crypt and LUKS http://sunoano.name/ws/public_xhtml/dm-crypt_luks.html
- I volumi creati con dm-crypt possono essere letti da Windows 2000/XP attraverso FreeOFTE, licenza GPL, http://www.freeofte.org/

dm-crypt e FreeOFTE - 3



Immagini tratte da http://sunoano.name/ws/public_xhtml/dm-crypt_luks.html . Si applicano le indicazioni sul copyright riportate sul sito.

dm-crypt e FreeOFTE - 4



Immagini tratte da http://www.freeotfe.org . Si applicano le indicazioni sul copyright riportate sul sito.

loop-AES - 1

- Patch per kernel Linux 2.0+, licenza GPL.
  http://loop-aes.sourceforge.net/
- É implementato come modulo kernel che sostituisce loop.o/loop.ko aumentandone le funzionalità grazie al supporto per numerosi algoritmi di cifratura (AES, Serpent, Blowfish, Twofish)
- “Loop devices are block devices that do not store any data directly but loop all reads and writes to underlying block device or file, possibly encrypting and decrypting data in the process. Normally you don't write to a loop device directly, but set up a file system on it. The file system will then read from and write to loop device.”

loop-AES - 2

- Pro: sviluppato da molto tempo e la sua sicurezza è comprovata e ritenuta in genere più elevata rispetto a dm-crypt, buone prestazioni, molte configurazioni possibili http://loop-aes.sourceforge.net/loop-AES.README
- Contro: non è incluso nel kernel, scritto e mantenuto dal solo Jari Ruusu.
- Al pari di dm-crypt, loop-AES consente di cifrare con chiavi generate casualmente lo swap ed i filesystem che si vogliono “ripulire” ad ogni avvio del computer.
- É possibile cifrare anche il filesystem montato in /, mantendo /boot in chiaro su disco o su un CD-ROM o USB key (autenticazione multifattore).

loop-AES - 3

```
opuntia:~# cat /etc/fstab
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
/dev/hda1       /boot           ext2    defaults        0       2
/dev/loop1      /               ext3    defaults,errors=remount-ro      0       1
/dev/mapper/vgSystem-lvSwap none    swap    sw,loop=/dev/loop0,encryption=AES256  0 0
/dev/mapper/vgSystem-lvUsr /usr ext3 loop=/dev/loop2,encryption=AES256,
        cleartextkey=/etc/crypto/usrkey 0 0
/dev/mapper/vgSystem-lvVar /var ext3 loop=/dev/loop3,encryption=AES256,
        cleartextkey=/etc/crypto/varkey 0 0
/dev/mapper/vgSystem-lvTmp tmp ext2    defaults,nosuid,loop=/dev/loop4,encryption=AES256,
        phash=random/1777 0 0
/dev/mapper/vgSystem-lvData /data ext3
defaults,noauto,nosuid,loop=/dev/loop5,encryption=AES256,
        gpgkey=/etc/crypto/datakey.gpg 0 0
/dev/mapper/vgSystem-lvStorage  /storage ext3 defaults,nosuid,loop=/dev/loop6,
        encryption=AES256,cleartextkey=/etc/crypto/storagekey 0 0
```

loop-AES - 4

```
opuntia:~# losetup -a
/dev/loop/0: [000d]:1917 (/dev/mapper/vgSystem-lvSwap) offset=4096 encryption=AES256
      multi-key-v3
/dev/loop1: [0001]:84 (/dev/mapper/vgSystem-lvRoot) encryption=AES256 multi-key-v3
/dev/loop2: [000d]:1919 (/dev/mapper/vgSystem-lvUsr) encryption=AES256 multi-key-v3
/dev/loop3: [000d]:1921 (/dev/mapper/vgSystem-lvVar) encryption=AES256 multi-key-v3
/dev/loop4: [000d]:1923 (/dev/mapper/vgSystem-lvTmp) encryption=AES256 multi-key-v3
/dev/loop6: [000d]:1929 (/dev/mapper/vgSystem-lvStorage) encryption=AES256 multi-key-v3
opuntia:~# mount
/dev/loop1 on / type ext3 (rw,errors=remount-ro)
/dev/hda1 on /boot type ext2 (rw)
/dev/mapper/vgSystem-lvUsr on /usr ext3 (rw,loop=/dev/loop2,cleartextkey=/etc/crypto/usrkey,
      encryption=AES256)
/dev/mapper/vgSystem-lvVar on /var ext3 (rw,loop=/dev/loop3,cleartextkey=/etc/crypto/varkey,
      encryption=AES256)
/dev/mapper/vgSystem-lvTmp on /tmp ext2 (rw,nosuid,loop=/dev/loop4,phash=random/1777,
      encryption=AES256)
/dev/mapper/vgSystem-lvStorage on /storage ext3 (rw,nosuid,loop=/dev/loop6,
      cleartextkey=/etc/crypto/storagekey,encryption=AES256)
```

loop-AES - 5

- Practical Privacy How-To: installazione di un server Debian GNU/Linux 5.0.1 (Lenny) con filesystem di root cifrato:

  http://netstudent.polito.it/wiki/index.php/HowTo_Debian_Encrypted_Root

- Una guida in Italiano scritta per questo corso che descrive passo a passo il procedimento di installazione di Debian GNU/Linux su un PC che fungera' da server di rete ed i cui contenuti su hard disk saranno completamente cifrati con loop-AES ed algoritmo AES256, ad eccezione di una partizione di boot minimale in chiaro.
- All'avvio del computer sara' necessario inserire un'unica passphrase per decifrare i filesystem di sistema e permettere l'avvio del sistema operativo. La chiave di cifratura principale e' protetta con GPG e puo' risiedere nella partizione di boot o su una chiavetta USB (autenticazione multi-fattore), sono fornite le configurazioni per entrambe le soluzioni.

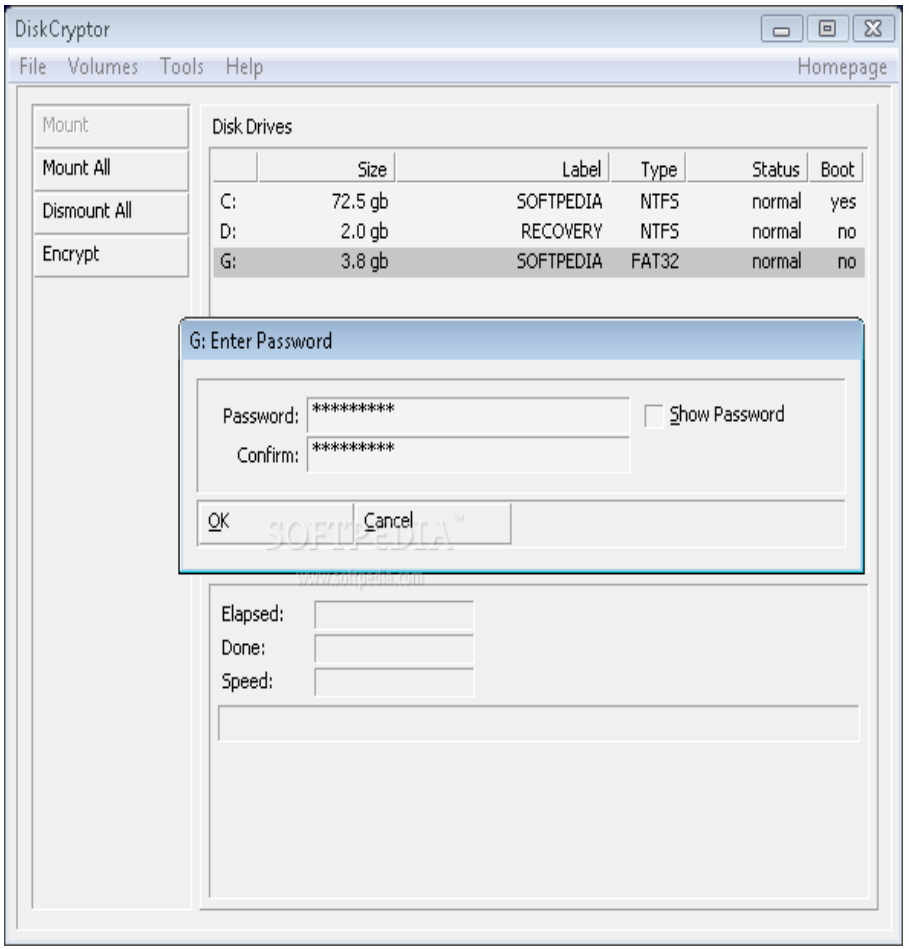
TrueCrypt e DiskCryptor - 1

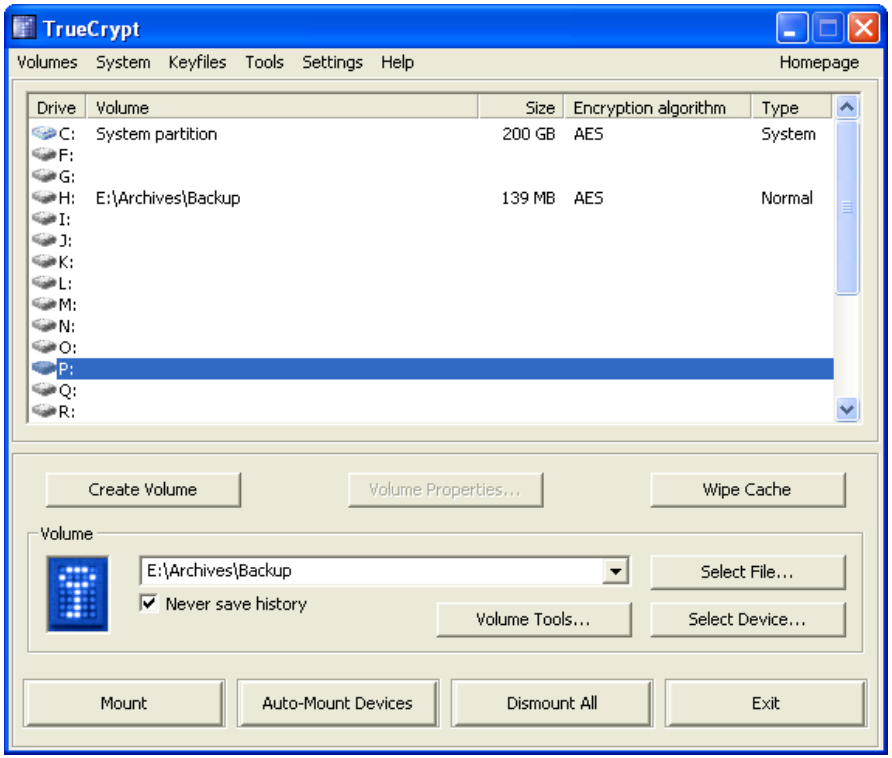
- TrueCrypt è una applicazione per la creazione di dischi cifrati virtuali contenuti in un file, una specifica partizione o un intero disco. Gira su Windows2000 SP4+, OSX 10.4+, Linux 2.4+, licenza restrittiva non opensource, ma codice sorgente disponibile. http://www.truecrypt.org/
- Supporta gli algoritmi crittografici AES, Serpent e Twofish e diverse loro combinazioni a cascata: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent,...
- Può crittografare la partizione di boot, creare ed eseguire un intero sistema operativo nascosto e cifrato, la cui esistenza può essere negata (*plausible deniability*).

TrueCrypt e DiskCryptor - 2

- DiskCryptor è un'alternativa libera ed opensource a TrueCrypt, consente la cifratura di tutte le partizioni del disco, inclusa quella di sistema. Supporta Windows2000+. http://diskcryptor.net/index.php/Main_Page
- Fino alla versione 0.4 il formato delle partizioni e dei dati cifrati era totalmente compatibile con quello di TrueCrypt. Dalla versione 0.5 usa il proprio formato di partizioni.

TrueCrypt e DiskCryptor - 3

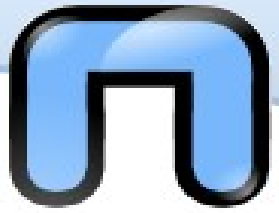




Immagini tratte da http://www.truecrypt.org/ e http://diskcryptor.net/ .
Si applicano le indicazioni sul copyright riportate sui siti.

GPG - 1

- Implementazione dello standard OpenPGP (RFC4880) per la cifratura e firma dei dati e delle comunicazioni. Disponibile per Linux, *BSD, OSX, Windows95+. Licenza GPL. http://www.gnupg.org/
- Usato soprattutto per la trasmissione sicura delle e-mail, ma può essere adoperato per cifrare file in locale sia con algoritmi crittografici a chiave pubblica che simmetrici (CAST5).
- GPG4Win: comoda distribuzione per Windows, include anche WinPT, un assistente che risiede nella traybar e consente di cifrare e decifrare facilmente file e clipboard.

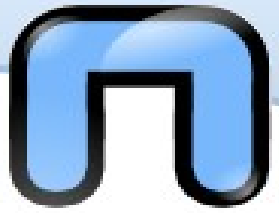


GPG - 2

```
$ echo "trust no 1" | gpg --symmetric --armor > cyphered.gpg

$ cat cyphered.gpg
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.6 (GNU/Linux)

jA0EAwMC16L9iQt557ZgySGyjxUgm/ao6VIoidiaYgzkyv7OMfwFbGa3yYqMfsMI
RD4=
=iPZa
-----END PGP MESSAGE-----

$ gpg -d cyphered.gpg
gpg: CAST5 encrypted data
gpg: encrypted with 1 passphrase
trust no 1
gpg: WARNING: message was not integrity protected
```

Elettra - 1

- Elettra è un tool per la creazione di archivi contenenti file gzipped e cifrati AES-128 che possono essere selettivamente estratti inserendo passphrase diverse. Gira su Linux, OSX e cygwin. Licenza non opensource, ma codice sorgente disponibile.
  http://www.winstonsmith.info/julia/elettra/
- Realizza la *deniable encryption*: è possibile sostenere che il plaintext estratto dall'archivio sia l'unico presente al suo interno. Questo grazie all'inserimento di padding e byte casuali all'interno dell'archivio.
- Interfacccia a riga di comando e GUI.
- http://www.phrack.org/issues.html?issue=65&id=6#article



Elettra - 2

```
$ ls -l /tmp/ls-manpage /tmp/ps-manpage
-rw-r--r-- 1 user user  7132 Jan  8 05:57 /tmp/ls-manpage
-rw-r--r-- 1 user user 36287 Jan  8 05:57 /tmp/ps-manpage

$ ./elettra encrypt /dev/shm/output 15% /tmp/ls-manpage::weirdness \
/tmp/ps-manpage::foxnewsshower

$ ls -l /dev/shm/output
-rw-r--r-- 1 user user 42615 Jan  8 06:13 /dev/shm/output

$ ./elettra decrypt /dev/shm/output weirdness /dev/shm/

$ ls -l /dev/shm/
-rw-r--r-- 1 user user  7132 Jan  8 06:32 ls-manpage
-rw-r--r-- 1 user user 42615 Jan  8 06:13 output
```

Cifratura di dati locali - 2

- dm-crypt e loop-AES si prestano ad essere usati sia su workstation che su server.
- Studi hanno mostrato che la plausible deniability fornita dall'OS hidden di TrueCrypt è fallace e tracce della presenza del sistema nascosto rimangono nel sistema contenitore (lista degli ultimi file aperti, thumbnails di anteprima, swap, hibernate file..)
- É sempre preferibile cifrare completamente il disco per assicurare fughe di informazioni tra l'area cifrata e quella in chiaro (es: shell history, file temporanei, lista file recenti,..)
- Per i server che necessitano di essere avviati senza l'immissione manuale della passphrase esistono protocolli che ovviano a questo problema, quali Mandos. http://wiki.fukt.bsnet.se/wiki/Mandos

Privacy dati locali - 3

- Dalla robustezza della passphrase dipende la resistenza dei dati cifrati agli attacchi, sceglierla con cura seguendo ad esempio il metodo http://world.std.com/~reinhold/diceware.html.
- Utilizzare applicazioni quali KeepPassX (Linux, OSX, Windows, Licenza GPL http://www.keepassx.org/) per conservare le password lunghe e complesse che non si riescono a memorizzare. Non tenere mai una password sullo stesso mezzo fisico su cui risiede l'asset che essa protegge, a meno che non sia cifrata.

Privacy dati locali - 4

- Attenzione ai log mantenuti dalle applicazioni che possono includere informazioni riservate (es: pidgin).
- Evitare di elaborare file le cui specifiche di formato sono chiuse e complesse (es: MS Office, Adobe,...) perchè possono memorizzare informazioni in più rispetto a quelle visibili. http://md.hudora.de/presentations/#hiddendata-dc

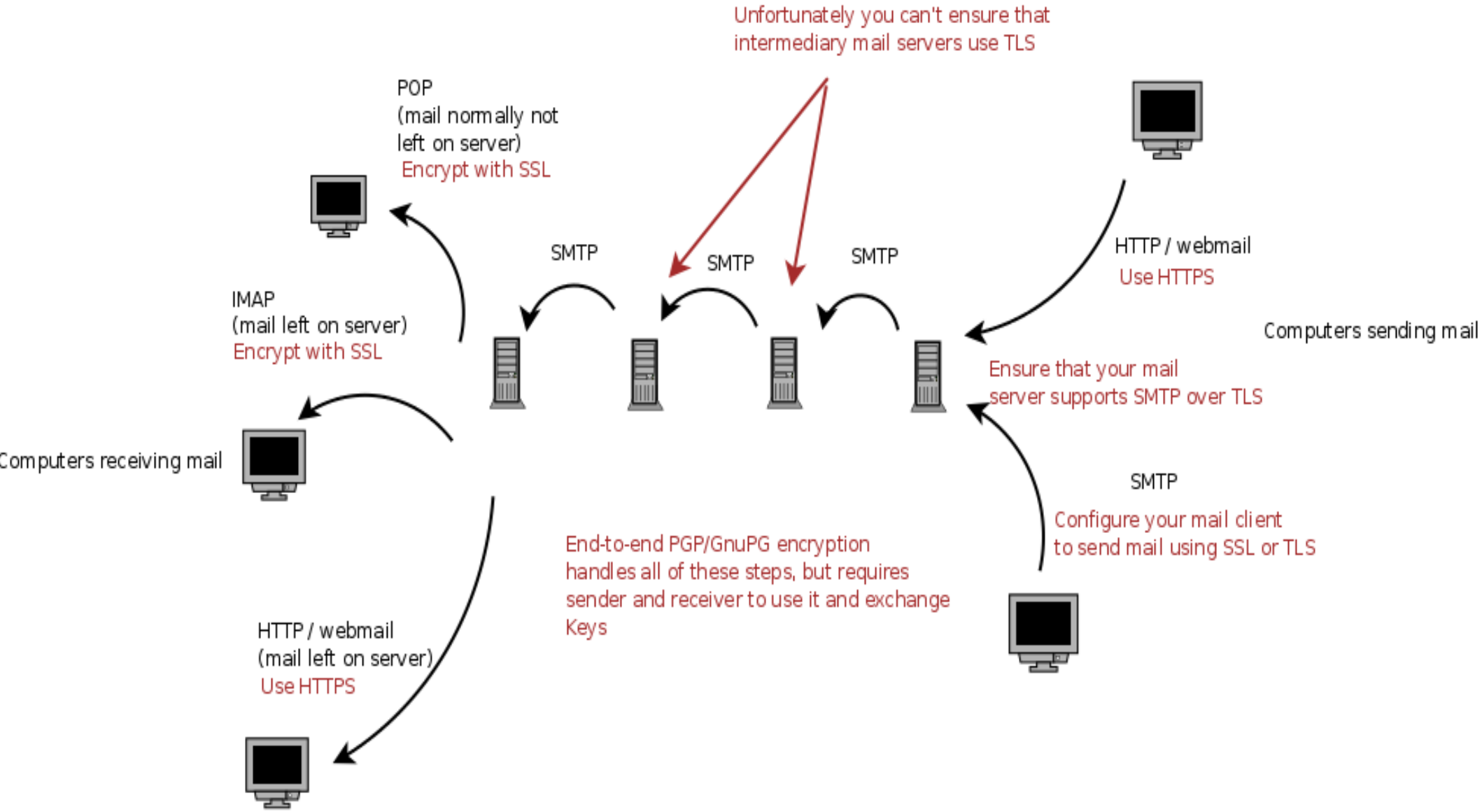
Privacy dati locali - 5

- Utilizzare strumenti di cancellazione sicura dei file e dello spazio libero su disco:
  - Windows: Eraser http://www.heidi.ie/eraser/
  - Linux/BSD: `shred -n 127 -z -u file`
    `dd if=/dev/zero of=/directory/junkfile ;`
    `rm /directory/junkfile`
- Prima di dismettere memorie di massa, distruggere in modo sicuro il loro contenuto:
  - Darik's Boot and Nuke http://dban.sourceforge.net/

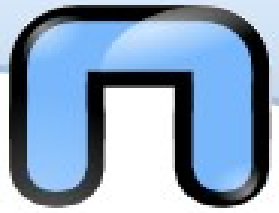
Privacy dati in rete - 1

- Quando affrontiamo il problema della privacy delle comunicazioni in rete dobbiamo tenere presente che tipicamente i dati che scambiamo col destinatario attraversano un numero variabile di nodi dei quali non ci possiamo fidare. É necessario considerare al pari di avversari i nodi di transito dei nostri pacchetti ed agire per limitare la loro possibilità di ledere la riservatezza delle nostri comunicazioni. Un attaccante può gestire un nodo sovvertendone il funzionamento o inserirsi nella tratta di rete che collega due nodi per modificare o intercettare le connessioni in corso.
- Considereremo la privacy di varie applicazioni: e-mail, instant messaging, navigazione web.

Privacy delle e-mail - 1

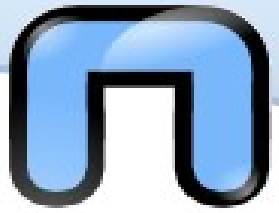


Immagini tratte da https://ssd.eff.org . Si applicano le indicazioni sul copyright riportate sul sito.



Privacy delle e-mail - 2

- Per posticipare considerazioni sul grado di fiducia del server, consideriamo uno scenario dove l'utente voglia inviare e ricevere e-mail da una postazione remota sfruttando il proprio server di posta casalingo.
- La crittografia è di nuovo la principale alleata per garantire la riservatezza delle nostre informazioni.
- Invio di e-mail tramite webmail su HTTPS (verificare attentamente il certificato del sito, aiutandosi anche con plugin del browser stile Prospectives) o dal mail client via SMTP over SSL/TLS. Si evita che un attaccante possa intercettare la posta inviata sulla connessione tra l'utente e il proprio mail server.



Privacy delle e-mail - 3

- Ricezione di e-mail tramite webmail su HTTPS o IMAP over SSL, la posta letta tipicamente rimane sul server e una copia può essere memorizzata lato client. Ricezione tramite POP over SSL, la posta letta tipicamente viene cancellata dal server ed una copia è memorizzata sul client. Si evita che un attaccante possa intercettare la posta ricevuta sulla connessione tra l'utente e il proprio mail server.
- Lato client e server valgono tutte le buone pratiche per tutelare la privacy delle mail memorizzate in locale citate nella sezione Privacy Dati Locali.

Privacy delle e-mail - 4

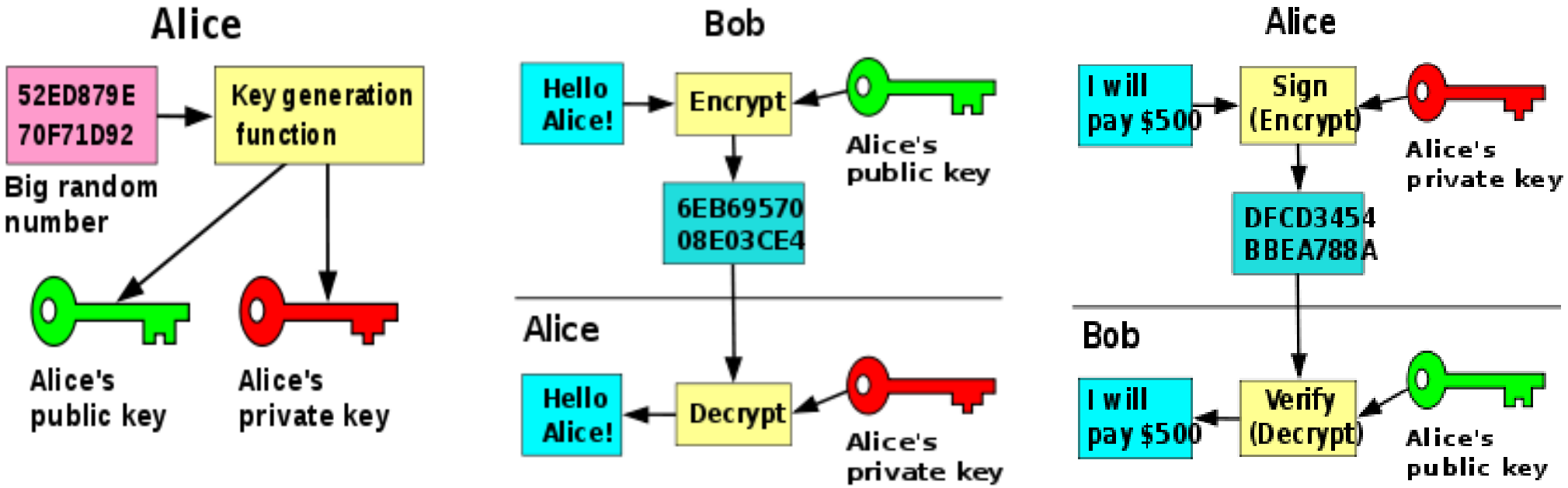
- Problemi:
  - Non c'è garanzia che tra il nostro mail server e quello del mittente/destinatario la trasmissione dei dati avvenga tramite SMTP cifrato: abbiamo protetto solo il segmento di rete tra il nostro client e il nostro server. Il messaggio può essere intercettato o alterato in transito.
  - Non c'è certezza che l'identità della persona con cui si corrisponde sia effettivamente quella dichiarata o presunta. Anche se si implementano tutti gli accorgimenti per garantire la confidenzialità della comunicazione, sussiste il rischio che l'attaccante abbia preso il controllo dell'account della persona a cui pensiamo di scrivere o sia in grado di forgiare mail false e intercettare le risposte.

Privacy delle e-mail - 5

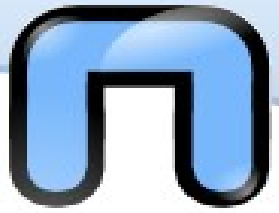
- Soluzione: crittografia a chiave pubblica e standard OpenPGP.
- Crittografia simmetrica:
  - Messaggio in chiaro + Algoritmo di cifratura + Chiave = Messaggio cifrato
  - Algoritmo di decifratura + Chiave + Messaggio cifrato = Messaggio in chiaro
- Crittografia a chiave pubblica:
  - Messaggio in chiaro + Algoritmo di cifratura + Chiave Pubblica di Bob = Messaggio cifrato per Bob
  - Messaggio cifrato per Bob + Algoritmo di decifratura + Chiave Privata di Bob = Messaggio in chiaro

Privacy delle e-mail - 6

- Firma a chiave pubblica (integrità + autenticità):
  - hash(Messaggio in chiaro) + Algoritmo di cifratura + Chiave Privata di Alice = Firma del messaggio
  - Firma del messaggio + Algoritmo di decifratura + Chiave Pubblica di Alice = Verifica della firma del messaggio



Immagini tratte da http://en.wikipedia.org/wiki/Public-key_cryptography . Si applicano le indicazioni sul copyright riportate sul sito.



Privacy delle e-mail - 7

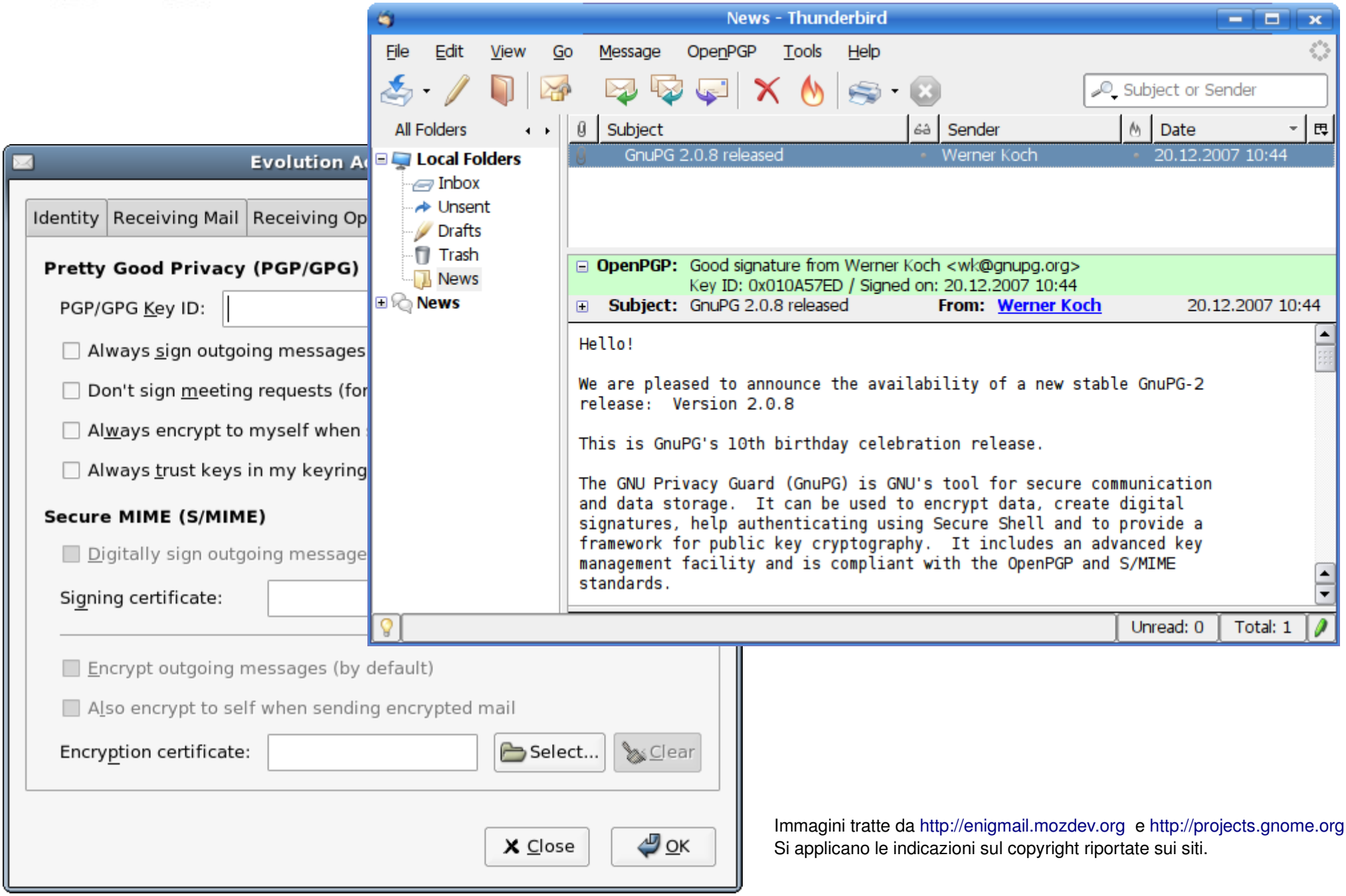
- Le chiavi pubbliche sono distribuite sui keyserver e possono essere prelevate da chiunque. L'autenticità della chiave pubblica è comprovata via firma digitale o web-of-trust.
- Un paio di chiavi può essere associato a più identità (nome, cognome, indirizzo e-mail).
- Integrazione di OpenPGP nei più diffusi mail client:

Enigmail (Thunderbird/SeaMonkey) http://enigmail.mozdev.org/

Plugin GPG per Sylpheed/Claws http://www.claws-mail.org/

Supportato in Evolution, KMail, mutt,..

Privacy delle e-mail - 8



Immagini tratte da http://enigmail.mozdev.org e http://projects.gnome.org .
Si applicano le indicazioni sul copyright riportate sui siti.

Privacy delle e-mail - 9

- Grazie ad OpenPGP possiamo superare l'inaffidabilità dei nodi tra il nostro mail server e il mail server del nostro interlocutore e godiamo di confidenzialità, integrità e autenticazione per la nostre comunicazioni via e-mail.
- Ricordarsi di verificare l'attendibilità della chiave pubblica del destinatario.
- Attenzione a non diffondere dati privati su di sè o sui propri contatti attraverso informazioni contenute nei metadati della chiave pubblica e via web-of-trust.

Instant messaging - 1

- Pidgin (ex GAIM), Kopete, Adium,...: grande numero di protocolli supportati - MSN, Yahoo!, jabber, ICQ,...
- Tramite alcuni accorgimenti è più semplice tutelare la privacy rispetto al caso dell'e-mail.
- Corretta impostazione delle funzionalità di logging: disabilitare la registrazione delle conversazioni o quantomento tenere i log su una partizione cifrata. In alternativa accettare il rischio che chiunque acceda al computer possa consultare lo storico delle conversazioni. Tenere presente che anche l'interlocutore potrebbe loggare.
- Non fidarsi dei server ai quali le applicazioni di instant messaging si appoggiano.

Instant messaging - 2

- Off-The-Record Messaging (OTR), disponibile per Adium, Pidgin, Kopete,... su Linux, *BSD, OSX, Windows. Licenza LGPL/GPL, http://www.cypherpunks.ca/otr/
- Libreria/Plugin che si integra coi principali client IM ed offre:
  - Crittografia a chiave pubblica per rendere i messaggi scambiati illeggibili a tutti fuorchè alle due parti della covnersazione.
  - Autenticazione della persona con cui si chatta tramite verifica del fingerprint della chiave o immissione di un segreto condiviso comunicato out-of-band.

Instant messaging - 3

- Crittografia a chiave pubblica per rendere i messaggi scambiati illeggibili a tutti fuorchè alle due parti della conversazione.
  - Plausible deniability: non c'e' firma digitale dei messaggi, per cui terze parti non possono dimostrare che la conversazione sia avvenuta davvero tra due identità precise. É garantito che i messaggi scambiati durante una conversazione siano autenticati e integri, ma una volta chiusa la sessione OTR chiunque può generare messaggi facendoli apparire provenienti da una delle due parti.
  - Perfect forward secrecy: la perdita delle chiavi private non permette la compromissione delle passate conversazioni.

Navigazione web - 1

- La navigazione web lascia numerosissime tracce della nostra attività sia sul computer dove lanciamo il browser che sul server web remoto, nonchè su altri server che non abbiamo esplicitamente visitato.
- Controllare e limitare i log mantenuti dal proprio browser attraverso la corretta impostazione dei security settings (svuotamento della cache, della cronologia di download e pagine visitate, eliminazione dei cookies al termine della sessione, sessioni autenticate, password e contenuti delle form salvati,..)

Navigazione web - 2

- Cookies: informazioni persistenti che un sito web imposta sul browser e il browser comunica al sito web ad ogni visita successiva, utili in transazioni e-commerce, comodi per migliorare l'esperienza di navigazione, molto invasivi della privacy (es: advertisement). É ragionevole impostare la cancellazione automatica dei cookies all'uscita dal browser. Cookie sharing anti creazione profili e tracciamento: Scookies FF plugin http://www.autistici.org/bakunin/scookies/
- Evoluzione della tecnologia cookie nei browser recenti e in HTML5: DOM storage pseudo-cookies (in FF: about:config / dom.storage.enabled=”false”), Adobe Flash cookies (FlashBlock FF plugin http://flashblock.mozdev.org/), client side storage.

Navigazione web - 3

Immagini tratte da https://ssd.eff.org . Si applicano le indicazioni sul copyright riportate sul sito.

Navigazione web - 4

- Controllare l'attività Javascript per prevenire infezioni da Malware, NoScript FF plugin http://noscript.net/
- Preferire HTTPS a HTTP quando disponibile (verificare sempre certificati, anche aiutandosi con strumenti stile Prespectives).
- Anche attuando queste precauzioni, sul server web visitato rimane traccia dell'indirizzo IP del client. Inoltre un attaccante che possa monitorare le richieste web inviate dal computer della vittima (analisi del traffico) è in grado di costruire un profilo degli interessi, abitudini, contatti in base ai siti visitati.

TOR - 1

- TOR è un'applicazione sviluppata per contrastare la minaccia prefigurata nella slide precedente: un attaccante globale che possa osservare ed analizzare tutto il traffico di rete tra client e server.
- “Tor è un overlay network distribuito pensato per anonimizzare le applicazioni a bassa latenza basate su TCP come web browsing, secure shell e instant messaging. I client scelgono un percorso attraverso la rete e costruiscono un circuito. Il traffico fluisce sul circuito in celle di dimensione fissa che ad ogni nodo vengono private di un imbustamento crittografico usando una chiave simmetrica (questo procedimento ricorda il modo in cui una cipolla, in inglese *onion*, viene progressivamente sbucciata ed ha suggerito il nome onion routing) e quindi inoltrate verso il prossimo hop.”

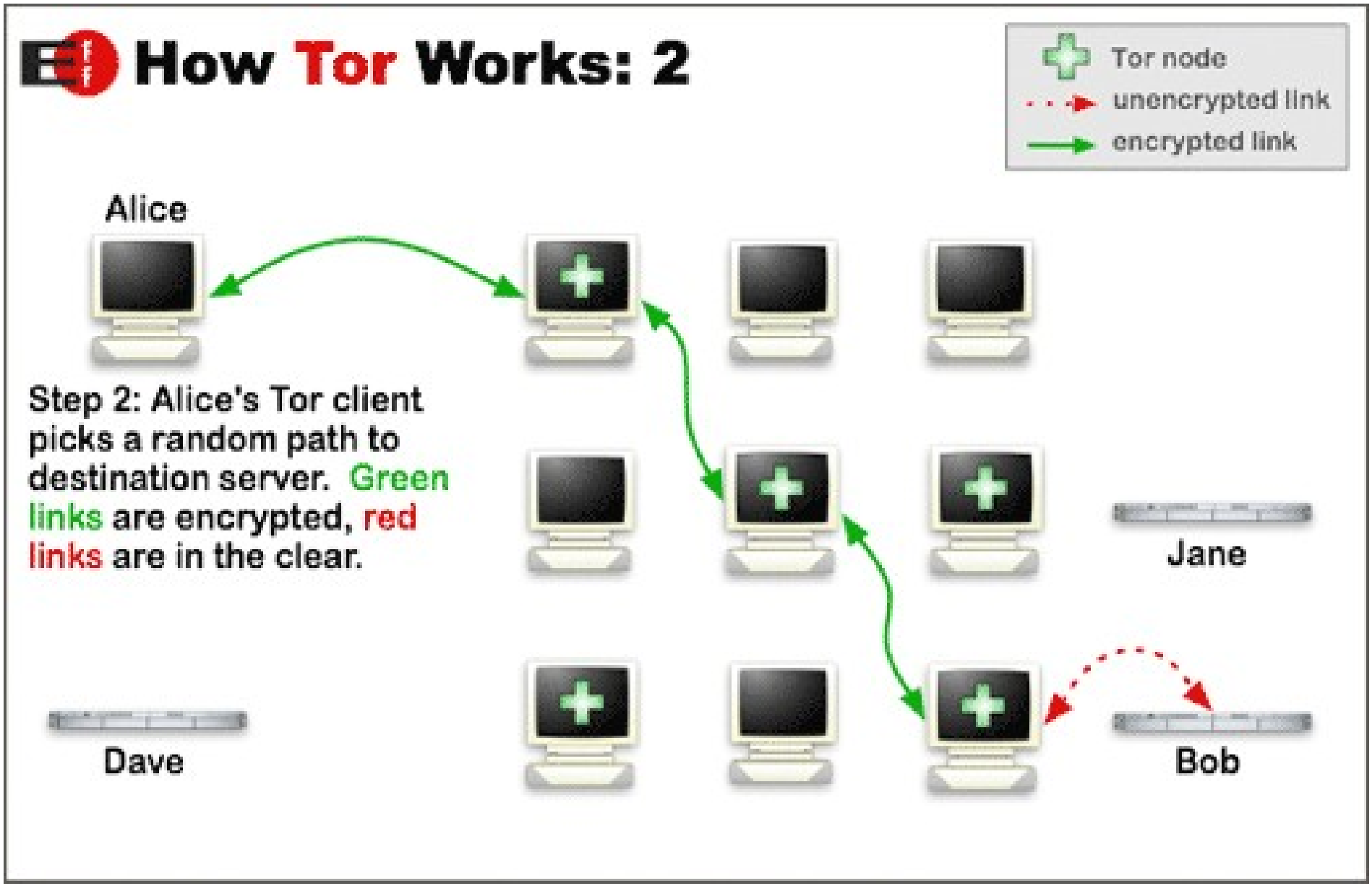
TOR - 2

- Disponibile per Linux, *BSD, OSX, Windows. Licenza Modified BSD/GPL (Vidalia). http://www.torproject.org/
- Implementato come proxy SOCKS ed utilizza alcuni altri software:
  - privoxy http://www.privoxy.org/, un proxy web non-caching, con funzioni di filtraggio delle richieste e degli header HTTP e altre funzionalità per elevare il grado di privacy quali l'eliminazione dei contenuti pubblicitari.
  - TorButton https://www.torproject.org/torbutton/ un'estensione per FF che abilita o disabilita la navigazione via TOR con un clic.

TOR - 3

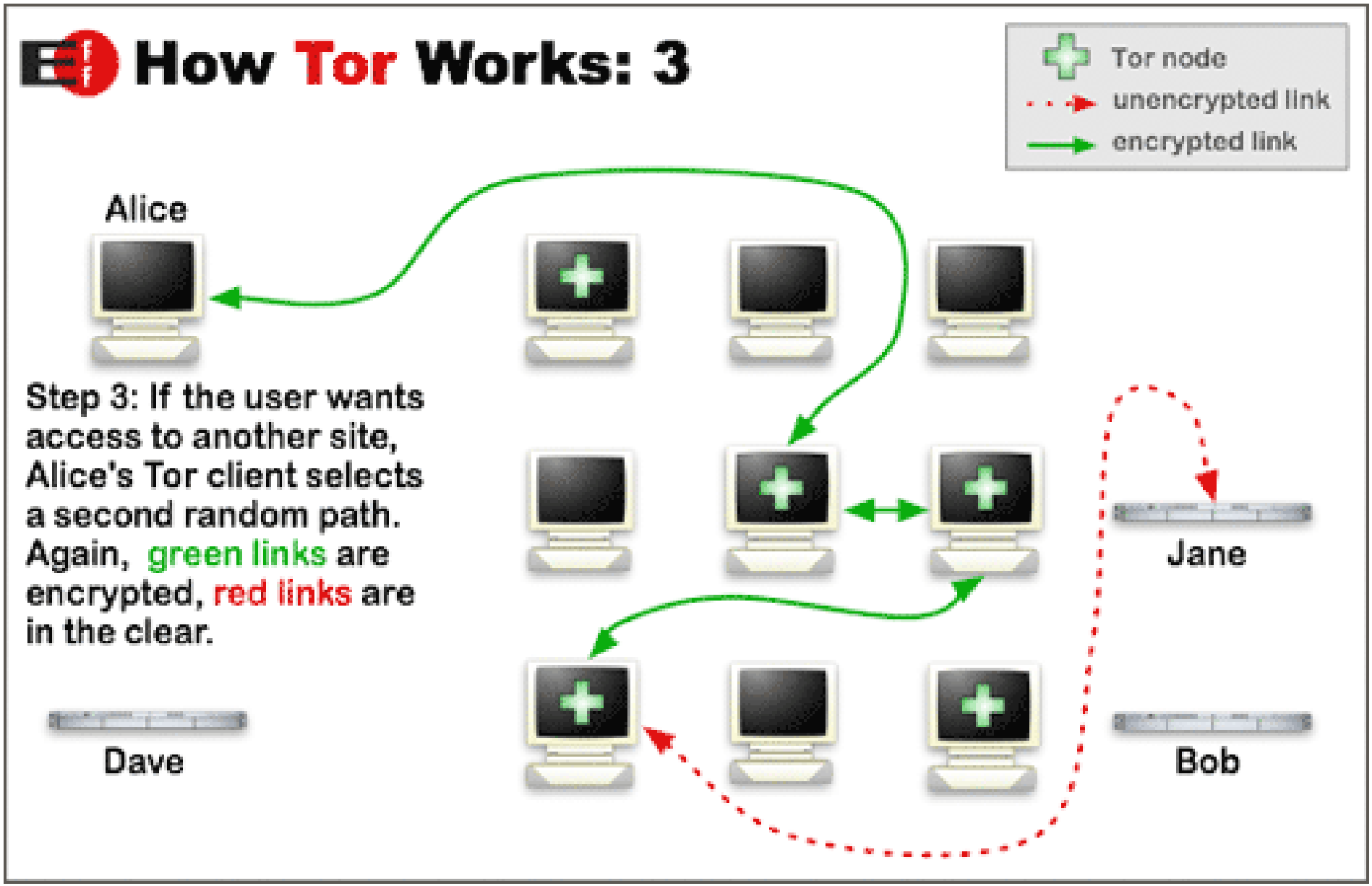
- Per Windows esistono dei comodi boundle portabili che integrano Firefox, TOR, privoxy/polipo, torbutton e vidalia (GUI di controllo).
- Usato in multinazionali per comunicazioni tra filiali distanti e contrastare lo spionaggio industriale, dalle ambasciate governative, da enti umanitari,...
- TOR protegge e anonimizza le connessioni dal computer di origine fino all'uscita della rete TOR, ma non tra l'exit node e il server destinazione! In questo tratto le proprietà CIA vanno garantite con altri mezzi visti in precedenza. (Phishing uffici governativi USA)
- Modalità di funzionamento relay node, hidden service.

TOR - 5



Immagini tratte da http://www.torproject.org/ . Si applicano le indicazioni sul copyright riportate sul sito.

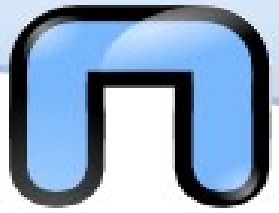
TOR - 6



Immagini tratte da http://www.torproject.org/ . Si applicano le indicazioni sul copyright riportate sul sito.

TOR - 7

- L'anonimato è una forma di Privacy più elevata di quelle viste fin'ora: la facoltà di dichiarare la propria identità solo a chi e quando si desidera. Non basta il proprio computer: si ottiene solo con la collaborazione di molti altri nodi.
- Importanza dell'anonimato (denuncia illeciti/soprusi/episodi mafiosi, partecipazione gruppi di sostegno, divulgazione informazioni critiche di pubblico interesse, blogging)
- TOR non è invulnerabile, ma è attivamente mantenuto e oggetto di ricerca e miglioramento. Funziona bene solo se si prendono tutte le precauzioni viste per la navigazione web (javascript, contenuti dinamici, novità HTML5 possono annullare l'anonimato).
- Approfondimento su http://bfi.s0ftpj.org/dev/BFi14-dev-06.pdf



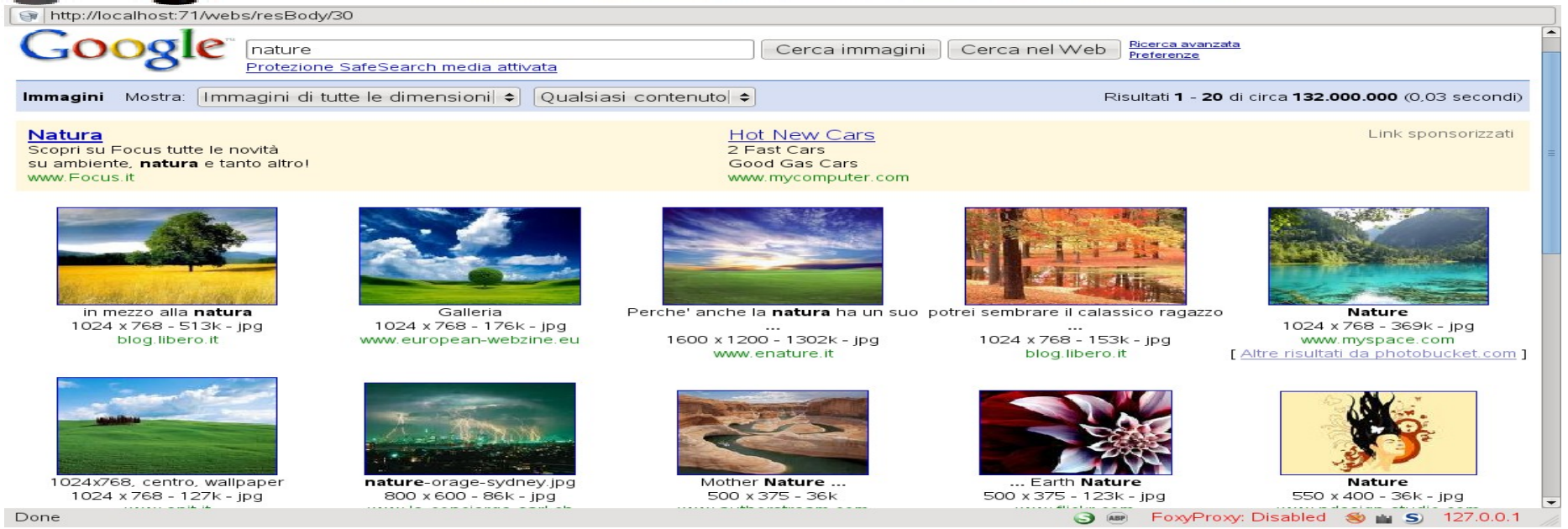
SniffJoke - 1

- IDS/sniffer evasion tool per Linux, Licenza GPL.
  http://www.delirandom.net/sniffjoke/
- Implementato come VPN su cui transitano le connessioni e vengono iniettati pacchetti “hack” inaspettati che ottimisticamente confonderanno la ricostruzione dei flussi effettuata dallo sniffer/IDS locale/dell'ISP/remoto.
- Ptacek, Newsham, Simpson, “Insertion, evasion, and denial of service: Eluding network intrusion detection” (1998)
  http://www.delirandom.net/sniffjoke/Insertion Evasion and denial of service on IDS.pdf

SniffJoke - 2

Immagini tratte da http://www.delirandom.net/sniffjoke/ . Si applicano le indicazioni sul copyright riportate sul sito.

SniffJoke - 3



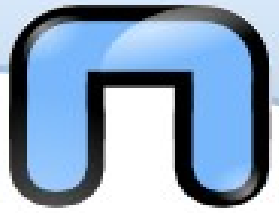
Immagini tratte da http://www.delirandom.net/sniffjoke/ . Si applicano le indicazioni sul copyright riportate sul sito.

Privacy dati presso terzi - 1

- Considerata la complessità delle soluzioni che tutelano la privacy delle informazioni, è ragionevole aspettarci che i siti di servizi web 2.0+:
  - permettano di configurare opzioni di protezione dei nostri dati personali efficaci ed usabili (ad es: limiti visibilità dei profili facebook)?
  - non soffrano di vulnerabilità e conseguenti break-in che conducano al furto o divulgazione dei nostri dati?
  - consentano di cancellare una nostra informazione dopo che l'abbiamo pubblicata? (NO, è realistico assumere che ogni informazione da noi ceduta in rete rimanga perennemente archiviata da qualche parte, es: waybackmachine, google groups, ripubblicazione ad opera di altri utenti)

Privacy dati presso terzi - 2

- Non esistono vere soluzioni a meno di non rinunciare ad usare larga parte di questi servizi.
- Buona regola è usare servizi di società che probabilmente non condividono le informazioni nei loro database, così da complicare il data mining e l'elaborazione dei profili utente.
- Impersonare identità multiple oltre che scomodo non è sufficiente a scongiurare il rischio di correlazione: la rete propria rete sociale ad esempio è un'informazione sufficiente per identificare con un margine di errore trascurabile un utente all'interno di un network. De-Anonymizing Social Networks: http://randomwalker.info/social-networks/
- Gestire la posta con un proprio mail server è già qualcosa.
- Il vero rischio è l'informazione “guidata”.



EOF

Domande?

Grazie dell'attenzione.. buona privacy e buon appetito ;-)

Copyleft

Quest'opera, per volontà dell'autore, è rilasciata sotto la disciplina della seguente licenza

Creative Commons Public License

Attribuzione-Non Commerciale-Condividi allo stesso modo 2.5 Italia

Tu sei libero:

di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare quest'opera

di modificare quest'opera

Alle seguenti condizioni:

Attribuzione. Devi attribuire la paternità dell'opera nei modi indicati dall'autore o da chi ti ha dato l'opera in licenza e in modo tale da non suggerire che essi avallino te o il modo in cui tu usi l'opera.

Non commerciale. Non puoi usare quest'opera per fini commerciali.

Condividi allo stesso modo. Se alteri o trasformi quest'opera, o se la usi per crearne un'altra, puoi distribuire l'opera risultante solo con una licenza identica o equivalente a questa.

Ogni volta che usi o distribuisci quest'opera, devi farlo secondo i termini di questa licenza, che va comunicata con chiarezza. In ogni caso, puoi concordare col titolare dei diritti utilizzi di quest'opera non consentiti da questa licenza. Questa licenza lascia impregiudicati i diritti morali. Le utilizzazioni consentite dalla legge sul diritto d'autore e gli altri diritti non sono in alcun modo limitati da quanto sopra.

Questo è un riassunto in linguaggio accessibile a tutti del codice legale (la licenza integrale) che è disponibile alla pagina web:

http://creativecommons.org/licenses/by-nc-sa/2.5/it/legalcode