

Mi hanno rubato  
il laptop!  
Cosa succederà ora  
ai miei dati?

Alessio L.R. Pennasilico  
mayhem@sikurezza.org  
<https://www.sikurezza.org>





# \$ whois mayhem

- ✓ Socio ed attivista di ILS, LUGVR, Metro Olografix, OpenGeeks/OpenBeer, AIP, AIPSI, recursiva.org, Sikurezza.org e Spippolatori.
- ✓ 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](http://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 dei pro e contro degli strumenti disponibili.

# Sommario

- La crittografia ci serve?
- Quali sono gli strumenti a nostra disposizione?
- Quale di questi soddisfa le nostre esigenze?

# Informazioni?

Le informazioni, e la loro gestione, sono spesso il fulcro operativo di molte aziende moderne.

La loro perdita, diffusione o alterazione può determinare, anche indirettamente, pesanti perdite economiche.

# DLG.196/2003

La legge italiana ha regolamentato delle misure minime di sicurezza, atte a preservare le informazioni da noi possedute su terzi.

Esiste comunque la necessità legale (ed operativa) di misure idonee a proteggere i nostri dati.

# Laptop

I nostri computer traboccano di informazioni che non vorremmo e/o non dovremmo rendere pubbliche.

I laptop in particolare contengono molte informazioni e sono spesso in dotazione a figure chiave della nostra struttura.

# Furto o smarrimento

Perdere il possesso di un notebook mette uno sconosciuto in grado di accedere senza alcuna riserva a tutte le informazioni in esso contenute.

(es. documenti, accessi, password)

# Come preservarci?



Quali strumenti abbiamo a disposizione per impedire l'accesso alle informazioni a chi non ne sia il legittimo proprietario?

# GPG

GNU Privacy Guard è un programma diffusissimo per gestire la crittografia delle e-mail.

Tra le sue funzionalità è prevista la possibilità di firmare e/o crittografare dei file su disco.

# GPG: PRO

- ✓ Utilizza algoritmi crittografici forti
- ✓ Utilizza crittografia asimmetrica
- ✓ Possibilità di criptare i dati rendendoli accessibili a più persone

# GPG: Contro

- \* è necessario criptare/decriptare ogni singolo file ad ogni accesso
  - \* non lavora in real-time
- \* non permette di criptare l'area di memoria di swap

# GPG: workaround

E' possibile usarlo per  
criptare/decriptare un file di  
loopback allo spegnimento/avvio  
della macchina.

# crypto-loop

Con questo sistema Linux ha introdotto la possibilità di tenere un file di loopback criptato in real-time su disco, demandandone la gestione direttamente al kernel.

# crypto-loop: PR0

- ✓ non necessita di patch: integrato anche nei kernel e negli userland meno recenti
- ✓ è in grado di utilizzare tutti i ciphers supportati dal kernel
  - ✓ lavora in real-time

# crypto-loop: Contro

- x “facile” da sovvertire
- x più lento degli altri sistemi
- x verrà presto dismesso dal kernel
- x non permette di criptare lo swap
- x sconsigliato con fs journalled

# dm-crypt

Per criptare file di loopback o partizioni, swap memory compresa, è possibile utilizzare questo nuovo strumento basato sul device mapper, quindi comunque nativo.

# dm-crypt: PRO

- ✓ integrato nel kernel e nello userspace
- ✓ “semplice” da configurare e da gestire
  - ✓ più veloce di cryptoloop
- ✓ supporta file system journalled

# dm-crypt: Contro

- x è necessario utilizzare un kernel più “recente”
- x nelle prime implementazioni, e se non settato correttamente, è vulnerabile ad alcuni attacchi
- x in alcune situazioni risulta più lento di loop-AES



# Loop-AES

Loop-AES è un sistema sviluppato per sopperire ai problemi rilevati negli altri metodi di gestione dell'encryption con particolare attenzione verso le performance.

# Loop-AES: PRO

- ✓ AES è uno degli algoritmi ritenuti più sicuri
- ✓ questa implementazione è incredibilmente veloce

# loop-AES: Contro

- x patch esterne al kernel ed allo userland che richiedono molta cura nel setup e nella manutenzione
- x più “difficile” da impostare

x

# OpenBSD: svnd



L'equivalente di Loop-AES per OpenBSD si presta purtroppo ad attacchi offline basati su dizionario. E' molto veloce, ma supporta solo Blowfish.

# FreeBSD: GBDE

L'equivalente di Loop-AES per FreeBSD, utilizza crittografia forte con diversi algoritmi, autenticazione a due fattori, e l'utilizzo di un salt per evitare attacchi offline basati su password. E' ritenuta l'implementazione più sicura tra quelle illustrate.

# Solo per \*nix?

Ma questi strumenti esistono solo per sistemi operativi unix-like?

No, esistono alcuni tool analoghi per altri sistemi operativi.

# Ne parliamo?

Si, ma facciamo attenzione!

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

# TrueCrypt

E' uno strumento opensource pensato per criptare partizioni o device (ad esempio chiavi USB). Funziona sia con Linux che con Windows, permettendo di utilizzare lo stesso device da entrambe gli ambienti operativi. Prevede la possibilità di "nascondere" il proprio utilizzo.

# TrueCrypt: PRO

- ✓ è multiplatforma
- ✓ si nasconde tramite steganografia
- ✓ utilizza diversi ciphers, più o meno forti/veloci

# TrueCrypt: Contro

- x Non cripta l'area di swap
- x Nella modalità file di loopback richiede che la partizione che ospita il “container” sia formattata con blocchi di 512 B

# Quale scegliere?

Non esiste una risposta universale.

Dipende dal compromesso che riusciamo a stabilire tra necessità di riservatezza, semplicità di utilizzo e funzionalità necessarie disponibili.

# Più contemporaneamente?

Non è possibile utilizzare più di uno di questi meccanismi sullo stesso sistema.

Il principale motivo è la personalizzazione degli strumenti in userspace.

# Policy

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

# Il problema delle chiavi

Lascereste le chiavi di casa nascoste in giardino?

La riservatezza della chiave è il presupposto fondamentale per l'efficacia di questi strumenti.



# Dispositivi USB

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

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

# Backup

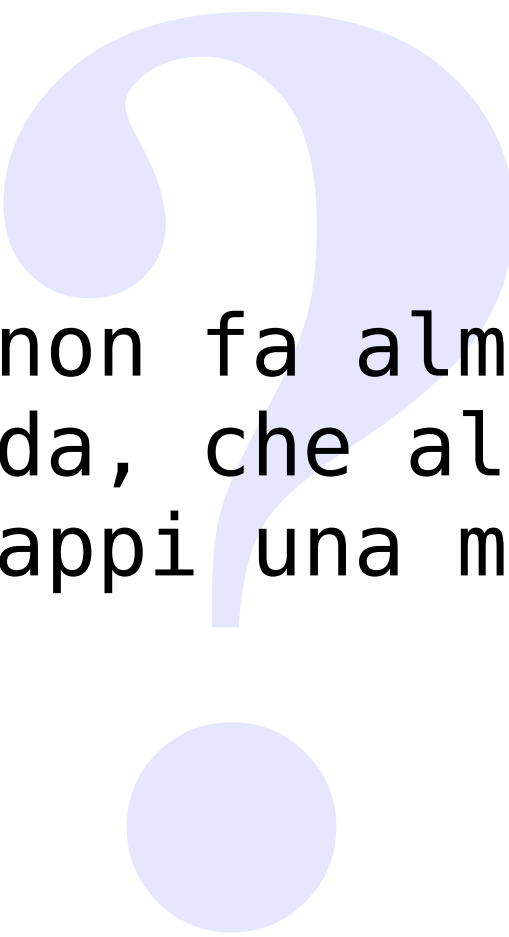

Obbligatorio per legge, va considerato comunque uno strumento indispensabile, a maggior ragione se utilizziamo la crittografia.

In tale scenario anche i supporti di backup devono essere gestiti adeguatamente.

# e le performance?

Sicuramente lavorare su un disco criptato presuppone da parte del sistema un maggior numero di operazioni.

Nella maggioranza dei casi la differenza di performance rilevabile dall'utilizzatore è assolutamente trascurabile.



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

# Bibliografia

- ✓ gpg: <http://www.gnupg.org/>
- ✓ cryptoloop: <http://www.tldp.org/HOWTO/Cryptoloop-HOWTO/>
- ✓ vulnerabilità di cryptoloop: <http://lwn.net/Articles/67216/>
- ✓ dm-crypt: <http://www.saout.de/misc/dm-crypt/>
- ✓ loop-aes: <http://loop-aes.sourceforge.net/loop-AES.README>
- ✓ confronti tra dm-crypt e loop-aes:  
[http://docs.indymedia.org/view/Local/UkCrypto#Linux\\_Implementations](http://docs.indymedia.org/view/Local/UkCrypto#Linux_Implementations)
- ✓ truecrypt: <http://www.truecrypt.org/>
- ✓ paragone <http://www.onlamp.com/lpt/a/6384>
- ✓ [http://www.infoanarchy.org/wiki/index.php/Hard\\_Disk\\_Encryption](http://www.infoanarchy.org/wiki/index.php/Hard_Disk_Encryption)
- ✓ \$ 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.