Federico Massi - info@federicomassi.it

TAILS

UNO STRUMENTO PER LA PRIVACY IN RETE

Cosa è TAILS?

TAILS è un sistema operativo live[1] mirato alla conservazione della privacy.[2]

1 Non serve installarlo (parte da DVD o da USB).

2 Permette di **aggirare la censura** e di **non lasciare tracce sul PC** utilizzato.

TAILS è, per l'appunto, l'acronimo di
"The Amnesic Incognito Live System".

Tails

theamnesicincognitolivesystem

The Amnesic Incognito Live System

TAILS “non ricorda” le tue informazioni

TAILS mira a preservare l’anonimato online

TAILS può essere avviato indipendentemente dal S.O. del computer in uso

COSA CONTIENE

Come sistema operativo, TAILS è **basato su Debian GNU/Linux**.

Attinge da e combina i migliori progetti di anonimato e riservatezza (OpenPGP, Tor, LUKS, HTTPS Everywhere, OTR,...).

Protegge i dati della chiavetta USB con una cifratura del disco, grazie a LUKS.

Protegge la digitazione di password e dati sensibili, con una tastiera virtuale che mette al riparo dai keylogger.

Anonimizza i metadati dei file, con MAT (solo i metadati, non fa miracoli!)

Cripta e firma le email con la cifratura OpenPGP.

TAILS:

NULLA DI NUOVO, MA...
UN COMODO PACCHETTO PRONTO ALL'USO

DEBIAN

Un’ottima base di partenza

DEBIAN GNU/Linux è un **sistema operativo composto solo da software libero**, proposto e curato dalla Debian Project. Parte integrante di questo prodotto è la gestione degli oltre 56’000 pacchetti software.

È il “progenitore” di distribuzioni come Ubuntu, Kali, Elementary, Raspbian, Knoppix, SteamOS.

Nonostante i grandi pregi tecnici, la parte più interessante del progetto riguarda l’organizzazione democratica e l’etica del software libero all’interno della comunità degli sviluppatori.

LUKS

Protezione dei dati sulla chiavetta

(Acronimo per ***L**inux **U**nified **K**ey **S**etup)*

LUKS è un **software per la crittografia del disco**; protegge le informazioni contenute nella chiavetta USB convertendole in un codice che non è facilmente decifrabile senza password.

TOR

Protezione dell’anonimato durante la navigazione

(Acronimo per ***T**he **O**nion **R**outer*)

TOR **permette di avere comunicazioni dati anonime**; dirige il traffico dati in una rete di nodi sparsi in tutto il mondo dopo averle crittate a strati (da cui la cipolla, *onion*) e facendo apparire l'ultimo nodo come l'origine della comunicazione.

Questo garantisce una protezione base (non totale) dell'anonimato del visitatore nei confronti del sito, e permette di aggirare diversi blocchi che impediscono l'accesso a siti censurati.

OpenPGP

Crittografia dei messaggi

(***P**retty **G**ood **P**rivacy*)

OpenPGP è uno standard per i **messaggi protetti con crittografia** asimmetrica (cioè con una chiave pubblica per crittare e una chiave privata per decrittare).

Data la grande complessità del calcolo per decodificare i dati protetti, OpenPGP rende in pratica impossibile leggere un messaggio da chi non abbia la chiave privata.

Ovviamente, è fondamentale la cura nel custodire la chiave.

HTTPS Everywhere

Protezione dagli attacchi MITM

HTTPS Everywhere è un'estensione per browser che **forza per tutti i siti la connessione HTTPS** invece della HTTP.

Questo serve a evitare gli attacchi MITM (***M**an **I**n **T**he **M**iddle*), in cui un terzo soggetto si intromette in uno scambio di informazioni accedendo e/o modificando le informazioni che vengono scambiate tra i soggetti originali.

OTR

Protezione della messaggistica

(***O**ff **T**he **R**ecord*, in via confidenziale)

OTR è un protocollo che permette **instant messaging con crittografia**, protezione delle chiavi generate in caso di violazione delle chiavi passate (*forward secrecy*), possibilità di smentire l'autentificazione dell'utente (*deniable authentication*) per mantenere alto il livello di anonimato.

MAT

Anonimizza i metadati dei file

(***M**etadata **A**nonymisation **T**oolkit*)

MAT **elimina i metadati dai principali tipi di file**. Ad esempio, in una foto eliminerà le informazioni sulla fotocamera usata, su data e ora dello scatto, sulla posizione geografica; in un pdf eliminerà il nome dell'autore e le informazioni sul computer dove è stato generato il file.

Non rimuove watermark o altri metodi di marcatura; inoltre lascia la possibilità di individuare contesti e riferimenti (linguistici, culturali, grafici e fotografici) ma garantisce una prima generale anonimizzazione.

USI PRATICI DI TAILS

TAILS si presta all'utilizzo di chiunque non sia un esperto ma voglia conservare la sua privacy online, soprattutto grazie alla rapidità con cui può essere pronto all'uso e alla documentazione (sotto forma di semplificazioni che rimandano a link e approfondimenti) accessibile dal sito (dove gradiscono collaborazioni di traduttori per l'italiano).

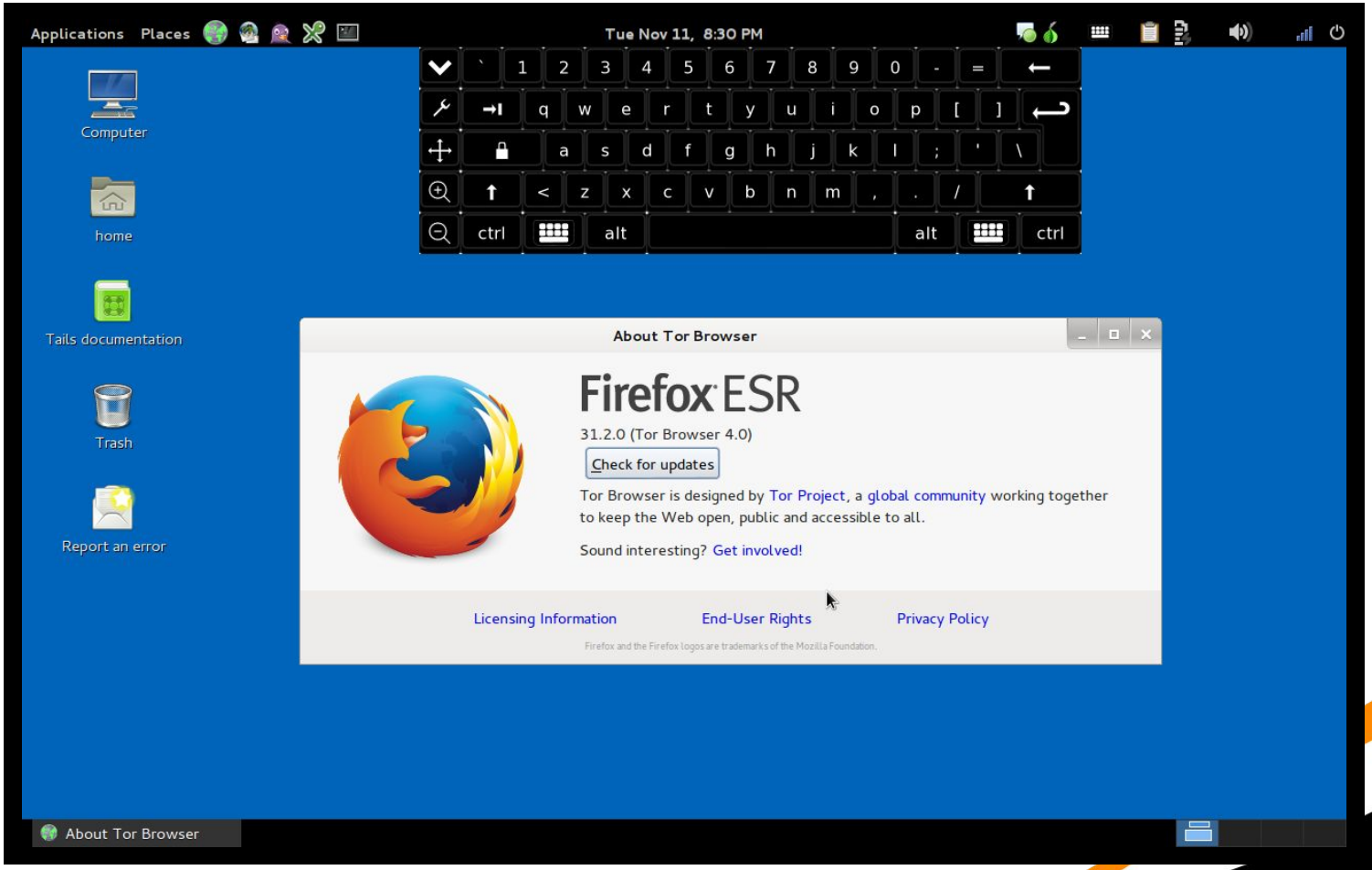
Diventa uno **strumento di particolare importanza per alcune professioni**, come giornalisti, personale di ONG e attivisti in luoghi dove sia difficile esprimersi in contesti democratici, personale di aziende in viaggi di lavoro che hanno bisogno di accedere con sicurezza e semplicità a Internet.

COME USARE TAILS

TAILS si avvia come un normale sistema Live, da DVD o da chiavetta USB.

COME USARE TAILS

Dopo l'avvio avremo esteticamente un Linux Debian. Semplicemente.



COSA NON FA TAILS

TAILS non protegge ovviamente da tutto.

HARDWARE MODIFICATI e KEYLOGGER: TAILS non protegge da dispositivi che registrano l'input della tastiera ma suggerisce l'uso della tastiera su schermo per password e altre informazioni sensibili.

ATTACCHI DA BIOS O FIRMWARE: Nessun sistema operativo può mettere al riparo da questi attacchi, per questo è sempre più importante favorire hardware che abbiano almeno firmware Open Source.

ALCUNE VULNERABILITÀ DI TOR: ad esempio la sorveglianza degli exit node (e qui ci salva la crittografia end-to-end), o una sorveglianza globale (le ingenti risorse di enti o governi possono permettere l'identificazione con alcuni metodi).

IDENTIFICAZIONE DALL'ISP CON L'USO DI CRITTAZIONE E TOR: le misure di sicurezza che adotti usando TAILS ti differenziano dal normale utente di Internet.

INDIRIZZI UTILI

SITO WEB DEL PROGETTO TAILS

https://tails.boum.org/

SITO WEB DI DEBIAN

https://www.debian.org/

SITO WEB DEL PROGETTO TOR

https://www.torproject.org

SITO WEB DI OpenPGP

http://openpgp.org/