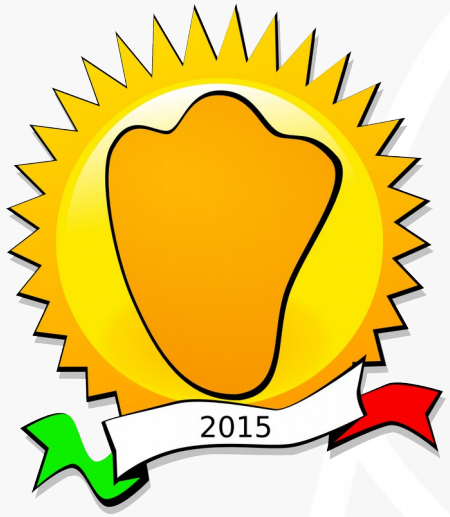
Riservatezza digitale

Missione impossibile?



Davide Mainardi

- Appassionato di informatica dal 1995.
- Ingegnere informatico laureato al Politecnico di Torino.
- Prima volta con GNU/Linux nel 2006.
- Cerco in tutti i modi di utilizzare **software libero** od ***open source***. Quando lavoro, nel tempo libero, da solo, con la famiglia o con gli amici.

I bei tempi andati

In passato, non più di dieci anni fa, per poter accedere ad internet era necessario un **computer** ed una **connessione "fissa"**.

I bei tempi andati

Non era semplice trovare foto di **gattini**.

I bei tempi andati

La parola **blog** veniva confusa con **borg** o con **blob**.

Ed oggi?

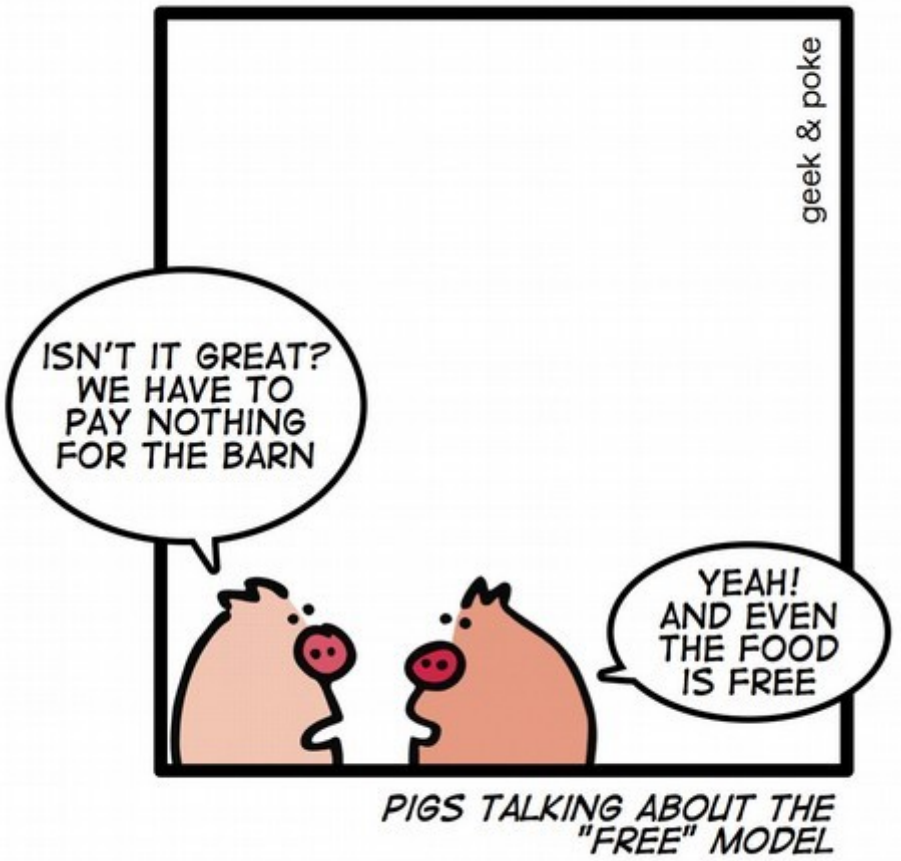
- Possiamo connetterci ad internet da **qualsiasi luogo**, e con **qualsiasi dispositivo** elettronico evoluto.
- I servizi web più famosi e più affidabili sono **gratuiti**.

Utopia

- Viviamo forse nel **migliore dei mondi possibili**?
- Internet è il luogo più bello al mondo? Dove tutti i sogni diventano realtà?

Realtà

- I colossi del web offrono **gratuitamente** i propri servizi.
- Purtroppo tu **non utilizzi** il prodotto.
- **Tu sei il prodotto!**



Realtà

Se ognuno di noi è il prodotto, che cosa viene venduto?

- Il nostro **tempo**?
- La nostra **libertà**?
- La nostra **anima**?

Realtà

- Ogni servizio internet “gratuito” si occupa di stilare il nostro **profilo** dettagliato.
- Esso **viene venduto** ad aziende pubblicitarie.
- Permettendo di lanciare campagne pubblicitarie **estremamente mirate**.
- In questo modo vengono ridotti i costi **massimizzando l'investimento**.

Il nuovo petrolio

- Le **informazioni personali** sono diventate dei **beni preziosi**.
- Stanno alla base del **funzionamento** dei più grandi colossi del web, e non solo...
- ***Personal data is transparent gold.***

Privacy

L'utente medio è portato a pensare:

- **Se mi registro al sito** e fornisco le mie generalità allora (**“loro”**) **possono sapere** chi sono e che cosa faccio.
- **Se non mi registro** allora posso tranquillamente navigare in pace ed in anonimato.

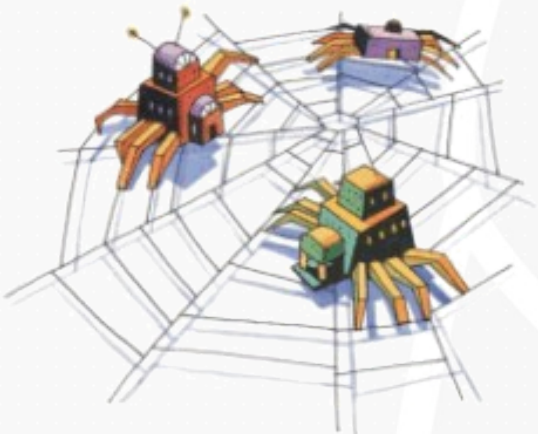
Motori di ricerca

- La pagina iniziale dei motori di ricerca offre un senso di sicurezza.
- Per alcuni utenti **Google significa Internet**.

Motori di ricerca - funzionamento

Crawling

Un crawler [...] è un software che analizza i contenuti di una rete (o di un database) in un modo metodico e automatizzato, in genere per conto di un motore di ricerca.



Wikipedia - it.wikipedia.org/wiki/Crawler

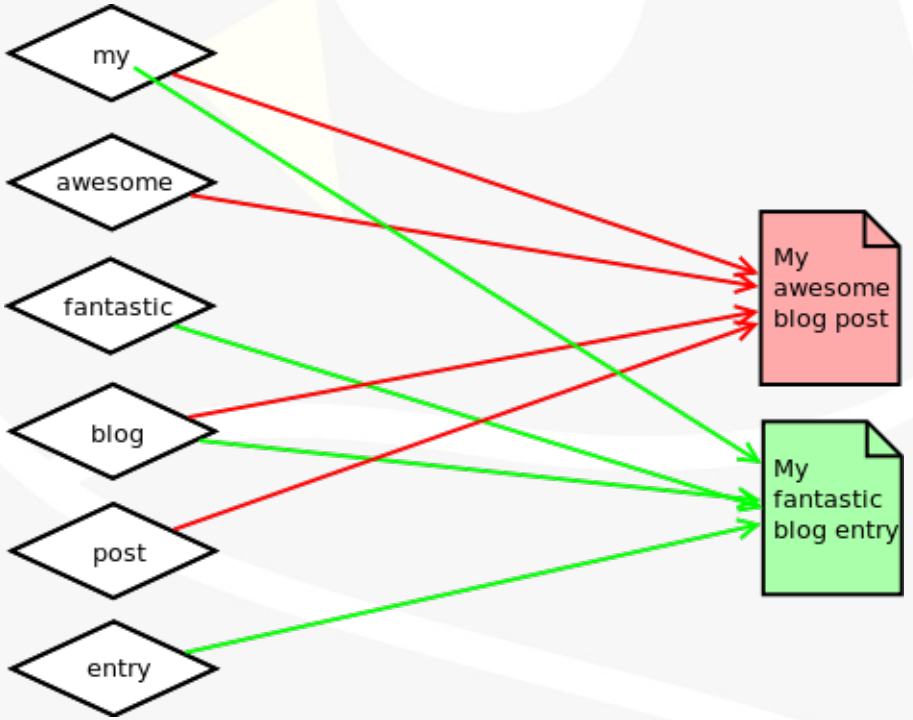
Motori di ricerca - funzionamento

- **Organizzazione** delle informazioni raccolte:
  - 40 miliardi di URL occupano 320 TeraByte
  - 40 miliardi di pagine occupano 12 PetaByte.
- **Compressione** ed ottimizzazione dei dati.
- **Bilanciamento** tra:
  - Aggiornamento dell'indice;
  - carico dei server;
  - consumo di banda.

Motori di ricerca - funzionamento

Costruzione di un indice invertito.

Ogni parola deve essere collegata a tutte le pagine in cui ricorre e le posizioni di ciascuna occorrenza in ciascuna pagina.



Motori di ricerca - funzionamento

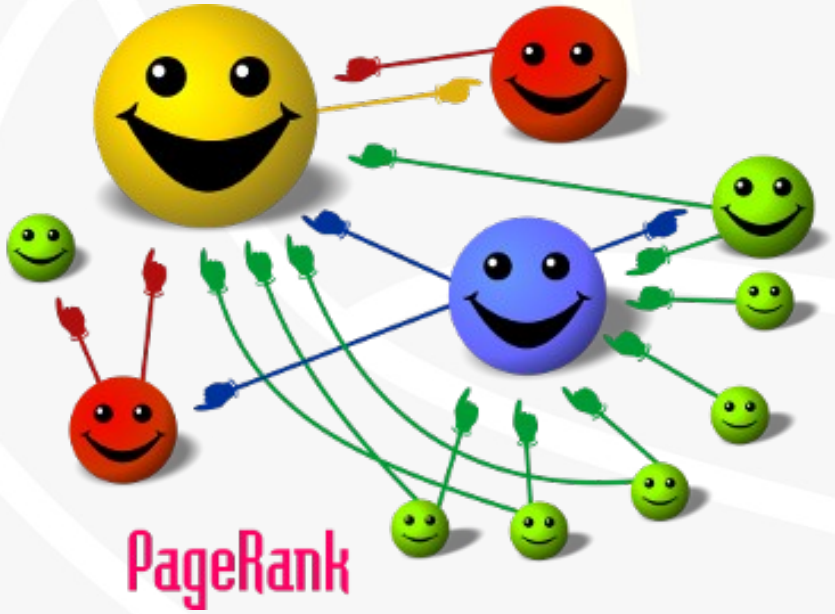
Rispondere alle *query* degli utenti, scegliendo in una frazione di secondo i documenti rilevanti e ordinandoli per rilevanza, in modo da presentarne una decina in prima pagina:

- le *query* vengono smistate su centinaia di server.
- Il risultato viene fuso in un unico documento che viene inviato all'utente.

Motori di ricerca - funzionamento

Calcolare i criteri di *ranking* che sono utilizzati durante le ricerche, per selezionare i risultati più rilevanti per una *query* e ordinarli:

- *Page rank* (it.wikipedia.org/wiki/PageRank);
- SEO.



Motori di ricerca - funzionamento

Personalizzazione dei risultati delle ricerche, in base a:

- precedenti ricerche;
- posizione dell'utente;
- riformulazione delle *query* ;
- periodo di attività (orario, giornaliero, settimanale).

Motori di ricerca - funzionamento

Gestire la pubblicità

Motori di ricerca - funzionamento

Google, a partire dal 2012, **raccoglie ed analizza il Knowledge Graph**:

> *[...] è il primo passo verso una ricerca semantica: grazie a questa funzione, il motore di ricerca di Google associa alle parole cercate un oggetto e metterà in relazioni oggetti in modo da avere una ricerca più veloce e accurata.*

Wikipedia

it.wikipedia.org/wiki/Google_Knowledge_Graph

Motori di ricerca - funzionamento

- Di solito cerchiamo **ciò che ci piace** o **ciò di cui abbiamo bisogno**.
- Ogni volta che inviamo una richiesta forniamo automaticamente i nostri dati:
  - indirizzo IP pubblico;
  - modello e versione del Sistema Operativo;
  - modello e versione del browser web;
  - il testo della ricerca.

Motori di ricerca e privacy

Google, Yahoo!, Bing e gli altri motori di ricerca

come gestiscono questi dati?

Motori di ricerca e privacy

- Tutti i nostri dati vengono **salvati** ed **analizzati**.
- I più comuni effetti a discapito della privacy sono:
  - ***tracking***;
  - ***filter bubbling***.

Tracking

Website visitor tracking (WVT) is the analysis of visitor behaviour on a website. [...] Use of WVT technologies can be controversial when applied in the context of a private individual; [...] When it is done without the knowledge of a user, it may be considered a breach of browser security.

Wikipedia - en.wikipedia.org/wiki/Website_visitor_tracking

Filter bubblig

La bolla di filtraggio è il risultato del sistema di personalizzazione dei risultati di ricerche su siti che registrano la storia del comportamento dell'utente. [...] L'effetto è di isolare l'utente da informazioni che sono in contrasto con il suo punto di vista, effettivamente isolandolo nella sua bolla culturale o ideologica.

Wikipedia it.wikipedia.org/wiki/Bolla_di_filtraggio

Datagate

Il ***datagate*** è il nome che la stampa italiana ha dato allo scandalo delle **intercettazioni di massa** effettuate dagli Stati Uniti.

Datagate

Il 10 giugno 2013 il quotidiano inglese **The Guardian** pubblica un'intervista esclusiva nella quale viene reso noto il sistema di sorveglianza statunitense **PRISM**.


Exclusive

The whistleblower

I can't allow the US government to destroy privacy and basic liberties

theguardian

guardian.co.uk

Edward Snowden, 29, emerges from hiding in Hong Kong

IT contractor says his concerns were ignored and he had to go public

Glenn Greenwald Hong Kong
Julian Borger

PRISM

Monday 10.06.13
Published in London and Manchester
£1.40 (IR €1.40)

Oxbridge bias
London and the south-east dominate entries
Page 7 »

Gillian Anderson
Star of The Fall who never sang Hollywood's tune
Page 10 »

Rafa's triumph
Nadal wins record eighth French Open title
Sport Page 1 »

MIF
MANCHESTER INTERNATIONAL FESTIVAL
4 – 21 July 2013
See page 3

Datagate

Edward Snowden, ex-dipendete di un contractor per l'NSA, rivela i dettagli della più grande operazione di spionaggio globale (dei dati internet) da parte del governo statunitense.

Datagate

Grazie alla collaborazione con i giornalisti **Glenn Greenwald**, **Laura Poitras** (e molti altri) negli ultimi anni siamo venuti a conoscenza di molte informazioni riservate.

Nei mesi seguenti, ed ancora oggi, è stata fatta luce su altri aspetti e tecniche fino ad oggi ancora **top-secret**.

Datagate

Mai fino ad ora abbiamo avuto così tante informazioni sui programmi di **sorveglianza di massa**. Tra i più famosi possiamo citare:

- **PRISM** it.wikipedia.org/wiki/PRISM_(programma_di_sorveglianza)
- **TEMPORA** it.wikipedia.org/wiki/Tempora
- **XKEYSCORE** it.wikipedia.org/wiki/XKeyscore

Datagate

Su **Wikipedia** è possibile controllare la lista dei **progetti di sorveglianza governativi**

en.wikipedia.org/wiki/List_of_government_surveillance_projects

Datagate

ECHELON, Data Retention Directive, INDECT, Schengen Information System, Golden Shield Project, Frenchelon, Nachrichtendienstliches Informationssystem, Project 6, Central Monitoring System, Lawful Intercept and Monitoring, DRDO NETRA, NATGRID, SORM, Titan traffic database, Onyx, Impact Nominal Index, Interception Modernisation Programme, Mastering the Internet, UK National DNA Database, Tempora, Royal Concierge, Boundless Informant, BULLRUN, Carnivore, Comprehensive National Cybersecurity Initiative, DCSNet, Fairview, Financial Crimes Enforcement Network, Magic Lantern, Main Core, MAINWAY, MUSCULAR, MYSTIC, Nationwide Suspicious Activity Reporting Initiative, NSA ANT catalog, PRISM, Room 641A, Special Collection Service, Stellar Wind, Tailored Access Operations, Terrorist Finance Tracking Program, Intelligence Community, Utah Data Center, X-Keyscore, GhostNet, Stuxnet

Eccellenza italiana

]HackingTeam[

Hacking team

Hacking Team è una società di Information technology *con sede a Milano che vende servizi di intrusione offensiva e sorveglianza a governi, organi di polizia e servizi segreti di tutto il mondo [...].*

Wikipedia - it.wikipedia.org/wiki/Hacking_Team

Hacking team

Il 5 luglio 2015 l'account Twitter della società fu violato da uno sconosciuto che pubblicò l'annuncio di una fuga di dati (data breach) partita dai sistemi informatici di Hacking Team. Il messaggio iniziale [...] dava i collegamenti a oltre 400 gigabyte di dati, tra cui asseritamente e-mail ad uso interno, fatture e codice sorgente;

Wikipedia - it.wikipedia.org/wiki/Hacking_Team

Hacking team

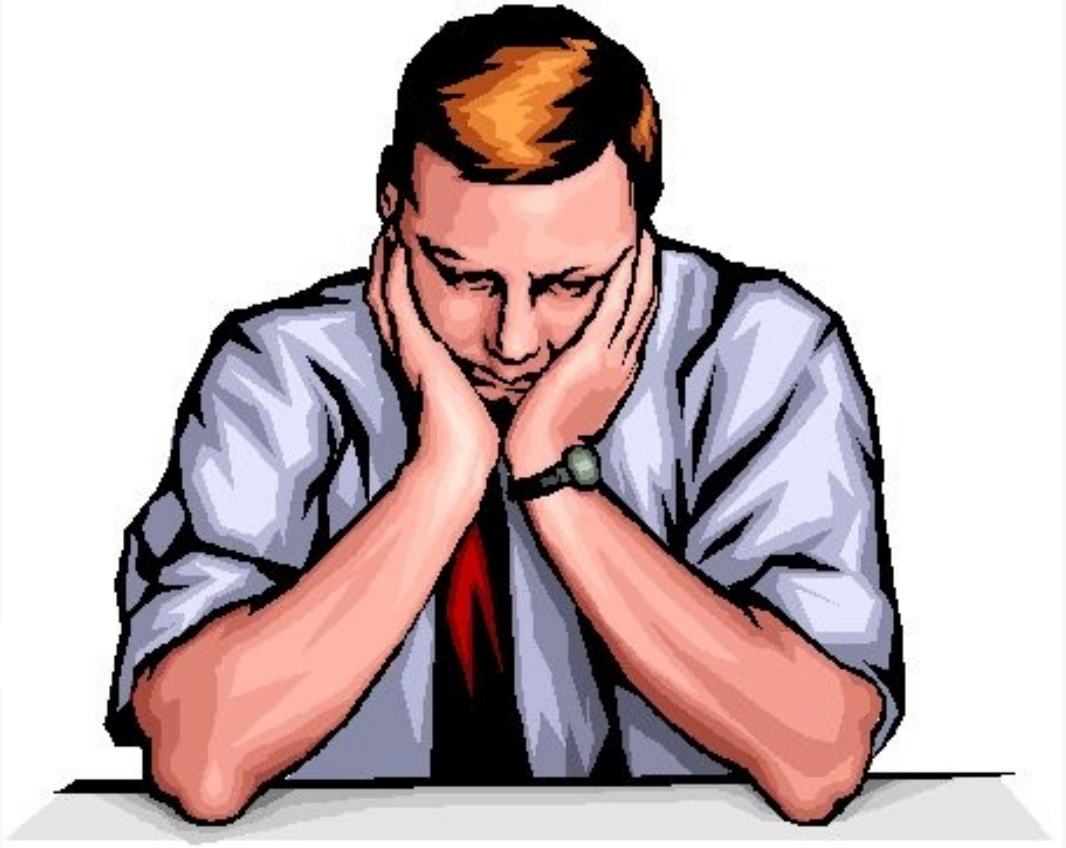
Hacking Team è stata criticata per la vendita di prodotti a governi come quelli del Sudan, Bahrein e Arabia Saudita.

Wikipedia - it.wikipedia.org/wiki/Hacking_Team

E quindi?

La perdita della privacy nelle comunicazioni elettroniche **è realtà.**

Un conto è avere delle **idee**, un altro è **averne le prove**.



Conclusioni

Lo **spionaggio su internet** è **realtà**.

Non siamo mai soli al computer quando “navighiamo”.

Conclusioni

“Chi non ha nulla da nascondere non ha nulla da temere.”

Ne siamo sicuri?

Contromisure

Fortunatamente la **riservatezza** nelle comunicazioni elettroniche è un concetto ancora attuabile.

Contromisure legislative

Possiamo **noi** (le persone comuni) far **cambiare le leggi** a favore di una maggiore **riservatezza**?

Contromisure legislative

Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014.

- Pubblicato sulla Gazzetta Ufficiale n. 126 del 3 giugno 2014
- In vigore dal 04 giugno 2015

Cookielaw (cookiegeddon)

“I gestori di siti web [...] sono tenuti a fornire agli utenti in relazione ai cookie [...] nel momento in cui si accede alla home page [...] deve immediatamente comparire in primo piano un banner di idonee dimensioni contenente le seguenti indicazioni:”

Estratto del provvedimento

Cookielaw (cookiegeddon)

- *“che il sito utilizza cookie di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete;*
- *che il sito consente anche l'invio di cookie "terze parti" (laddove ciò ovviamente accada);*
- *il link all'informativa estesa, che deve contenere le seguenti ulteriori indicazioni relative a: […]”*

Estratto del provvedimento

Cookielaw (cookiegeddon)

- *“l'indicazione che alla pagina dell'informativa estesa è possibile negare il consenso all'installazione di qualunque cookie;*
- *l'indicazione che la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso (ad esempio, di un'immagine o di un link) comporta la prestazione del consenso all'uso dei cookie;”*

Estratto del provvedimento

Cookielaw (cookiegeddon)

- *“[…] il caso di omessa informativa [...] è prevista la sanzione amministrativa del pagamento di una somma da **seimila** a **trentaseimila** euro [...].*
- *L'installazione di cookie [...] in assenza del preventivo consenso degli stessi comporta [...] pagamento di una somma da **diecimila** a **centoventimila** euro [...].*
- *L'omessa o incompleta notificazione al Garante […] è sanzionata con il pagamento di una somma da **ventimila** a **centoventimila** euro[...].”*

Cookielaw (cookiegeddon)

Cookielaw (cookiegeddon)

Riferimenti alle pagine del sito web del Garante della Privacy:

- garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884
- garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4006878
- garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167231

Contromisure legislative?

Meglio affidarsi alle leggi della natura che alle leggi dello stato

This is the beginning of a moment where we the people begin to protect our universal human rights with the laws of nature rather than the laws of nations

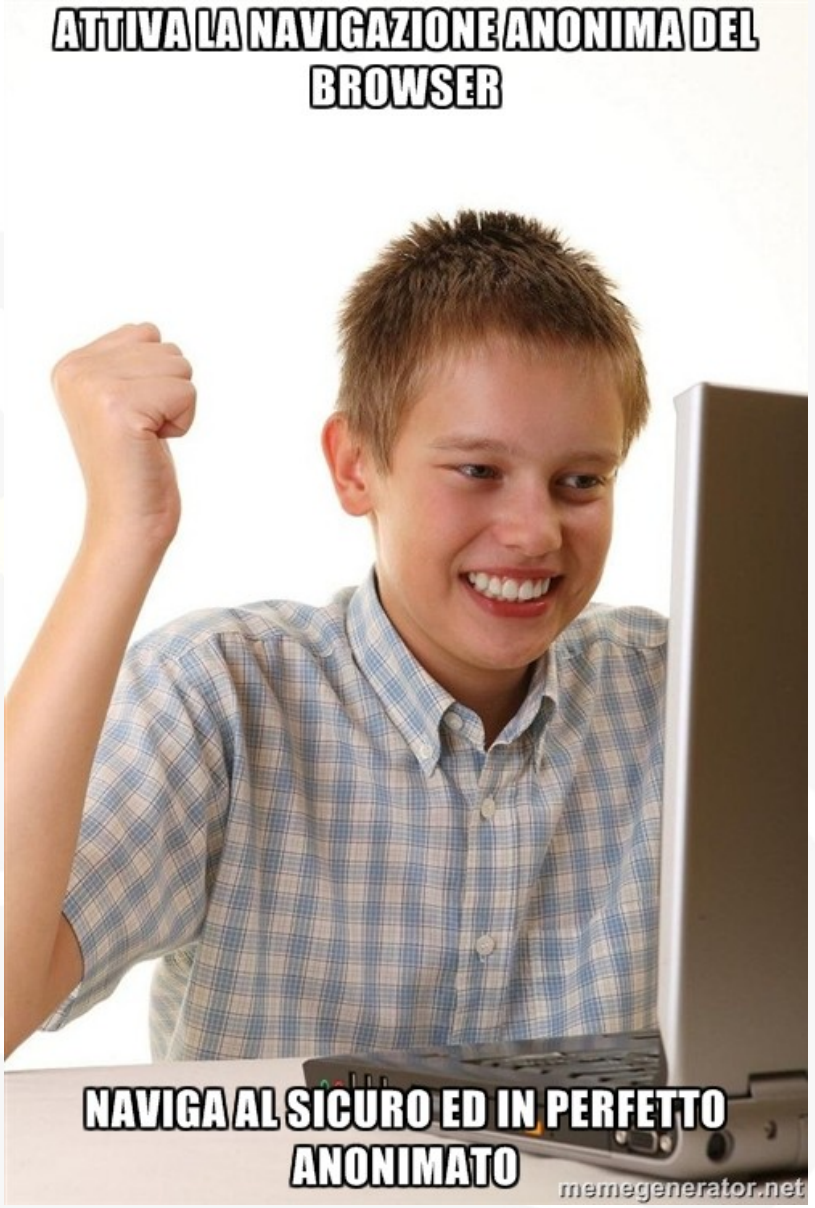
Edward Snowden

resetthenet.tumblr.com/post/87793640365/edward-snowdens-statement-in-support-of-reset-the-net

Contromisure elettroniche?

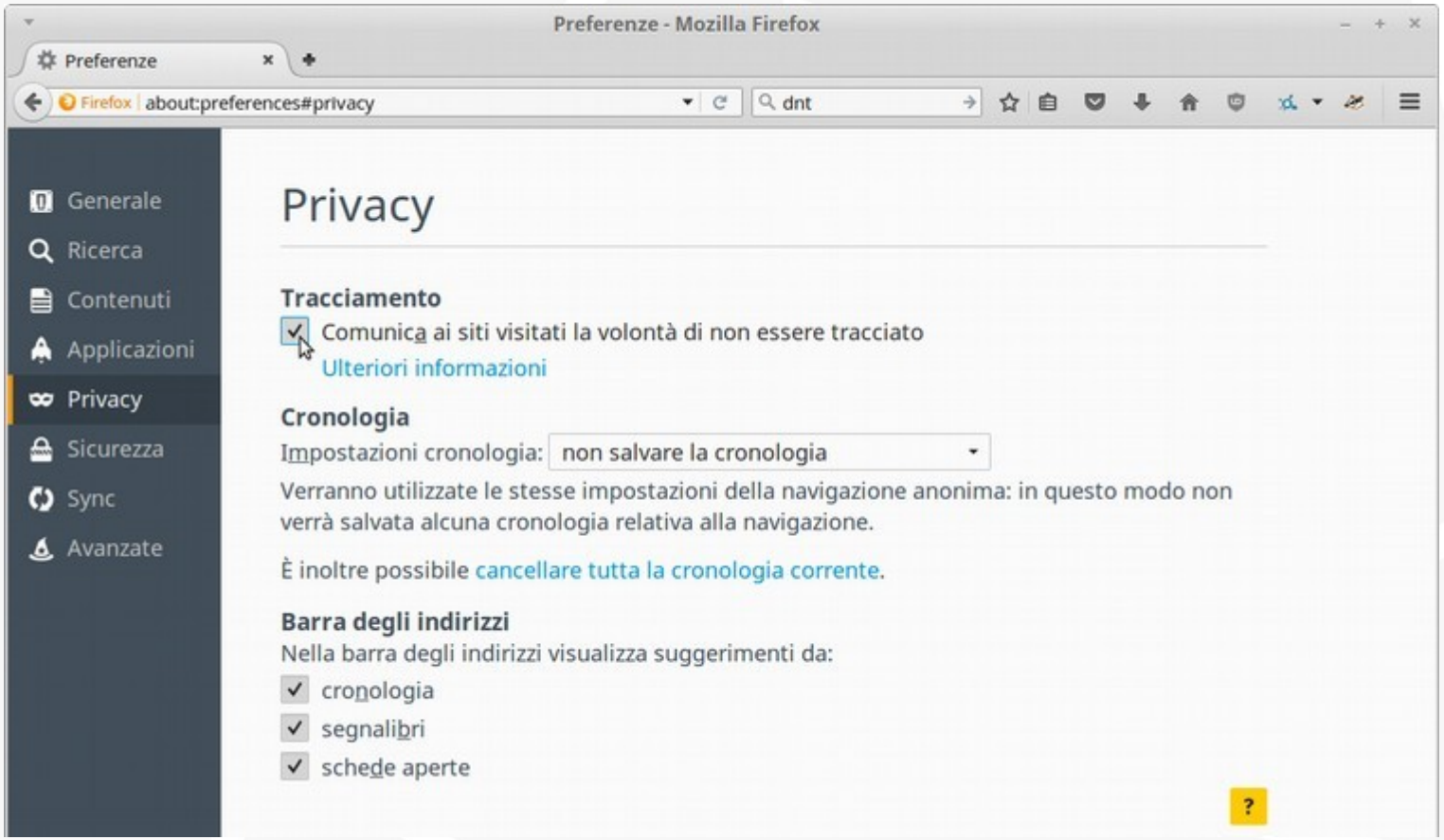
I più moderni *browser web* offrono la possibilità di non salvare la cronologia.

Si entra nel cosiddetto **Incognito Mode**.



Contromisure elettroniche? DNT

Nei più comuni *browser web* è anche presente l'opzione **Anti Tracciamento dei Dati**.



Contromisure elettroniche? DNT

Purtroppo **Do Not Track** in realtà significa **Do Not Target**, ovvero la possibilità di non essere bersaglio delle pubblicità mirate (anche se il *tracking* viene comunque effettuato).

Contromisure elettroniche? DNT

Purtroppo **Do Not Track** viene effettuato dai siti in maniera completamente volontaria.

Di solito l'opzione specificata nel *browser web* è **completamente ignorata**.

In altre parole: **è inutile**!

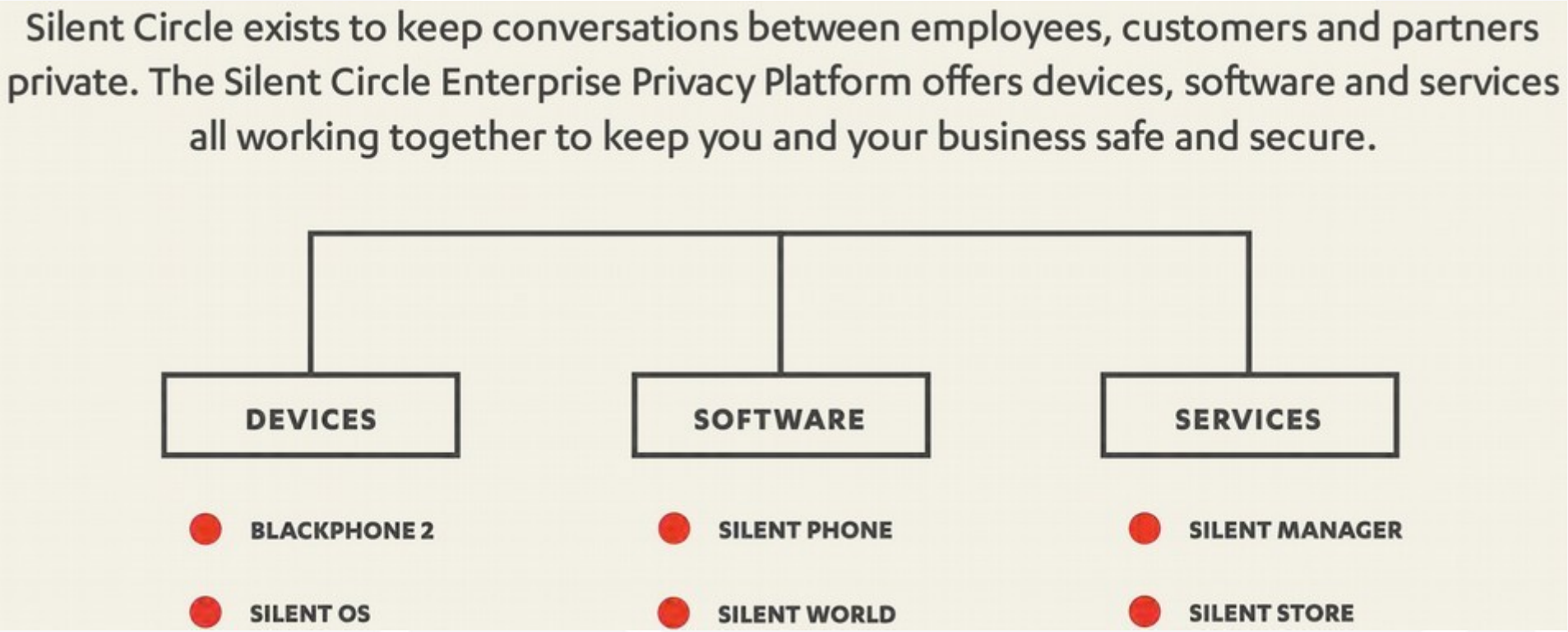
Contromisure commerciali – Blackphone 2

- È uno *smartphone* sviluppato dalla Silent Cirle.
- L'hardware e le prestazioni sono quelle comuni a uno *smartphone* commerciale di livello alto.

Contromisure commerciali – Blackphone 2

- In commercio a partire dalla fine di settembre 2015.
- Il **prezzo è elevato**, pari a quello di un “top di gamma”.
- È il **componente hardware** dell'universo “sicuro” creato dalla Silent Circle.

Contromisure commerciali – Blackphone 2



silentcircle.com/uploads/misc/SilentCircleMarketingResources_Sep2015.pdf

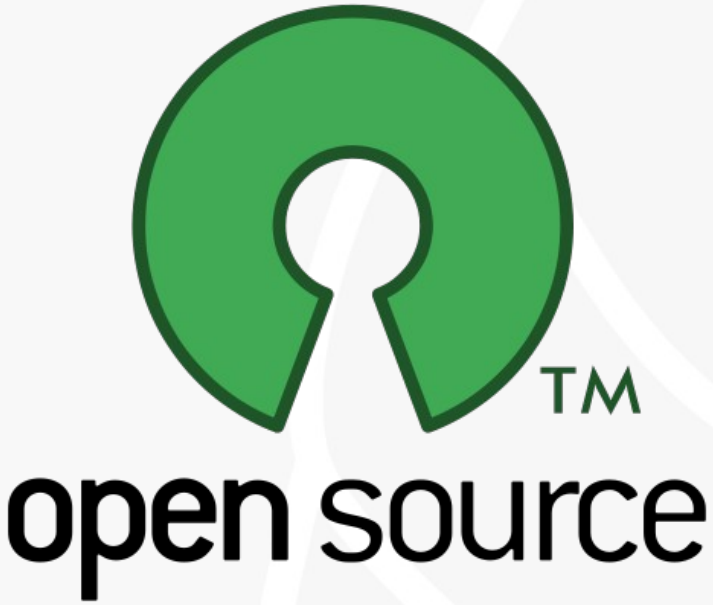
Che fare?

Come facciamo ad essere sicuri che le varie soluzioni presenti in commercio **ci proteggano**?

- Possiamo fidarci e basta.
- Possiamo pagare e fidarci.
- Possiamo **controllare noi stessi** il funzionamento del software.

Soluzione

Il codice sorgente del ***free software*** (e del software ***open source***) è accessibile e modificabile liberamente da ognuno di noi.



Soluzione

L'utente medio è ora pieno di domande:

- Dove si trovano questi software?
- Come faccio ad usarli?
- Capirò come fare?
- Posso usare la mia solita password 'mariorossi'?

Da dove iniziare?

PRISM break

prism-break.org

Electronic Frontier Foundation

www.eff.org

Surveillance Self Defense

ssd.eff.org

The Digital First Aid Kit

digitaldefenders.org/digitalfirstaid

The Guardian Project

guardianproject.info

PRISM Break

prism-break.org è un sito che raccoglie tutte le tecnologie che ognuno di noi può utilizzare per tutelare la propria privacy su internet.

Electronic Frontier Foundation

*[...] è un'organizzazione internazionale non profit di avvocati e legali rivolta alla tutela dei **diritti digitali** e della **libertà di parola** nel contesto dell'odierna era digitale.*

Wikipedia

it.wikipedia.org/wiki/Electronic_Frontier_Foundation

EFF's SSD - ssd.eff.org

Il 23 ottobre 2014 la Electronic Frontier Foundation pubblica la **Surveillance Self Defense**.

La SSD è una guida (teorica e pratica) utile a coloro che vogliono difendersi dalla sorveglianza digitale.

The Digital First Aid Kit

L'obiettivo del Digital First Aid Kit è di dare un **primo supporto** alle persone che hanno a che fare con le minacce elettroniche più comuni.

Il Kit offre una serie di **strumenti** di auto-diagnosi utili ai difensori per i diritti umani, ai blogger, agli attivisti ed ai giornalisti; così come delle **linee guida** per assistere digitalmenete chi si trova sotto attacco.

The Guardian Project

The Guardian Project è una **comunità globale** di sviluppatori software, designer, avvocati, attivisti ed istruttori impegnati nella creazione o nel miglioramento di programmi per la **sicurezza in ambito mobile**.

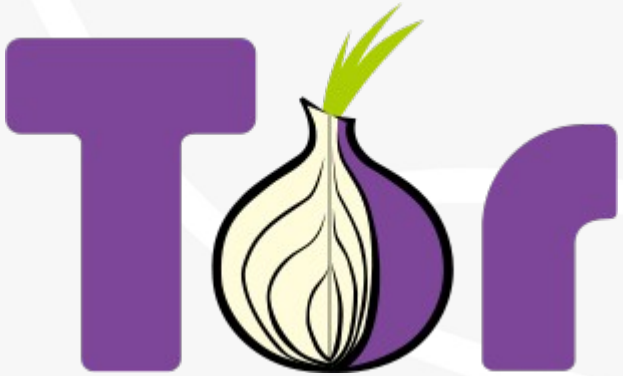
Tecnologie

Al fine di **comunicare con maggiore sicurezza** si può fare affidamento su queste tecnologie:

- TOR;
- PGP;
- OTR;
- XMPP.

TOR

Tor (acronimo di The Onion Router) è un sistema di **comunicazione anonima** per Internet basato sulla seconda generazione del protocollo di *onion routing*.



TOR

È possibile ottenere una connessione anonima ed accedere ai servizi nascosti grazie ad una **struttura stratificata** (a cipolla) ed alla **cifratura differente** nodo dopo nodo.

PGP

Pretty Good Privacy (PGP) è un programma che permette di ottenere **autenticazione** e **privacy crittografica**. Nelle sue varie versioni è probabilmente il crittosistema più usato al mondo.

Utilizza il sistema di **cifratura asimmetrica**.

Off-the-Record Messaging

OTR è un **protocollo di cifratura** che fornisce conversazioni testuali (messaggi) cifrate. OTR usa una combinazione di:

- **AES-128** - algoritmo di cifratura simmetrico con chiave a 128 bit.
- **DH-1536** - algoritmo di scambio chiavi Diffie-Hellman a gruppi di 1536 bit.
- **SHA-1** - algoritmo di hashing con risultato a 160 bit.

Off-the-Record Messaging

In aggiunta alle funzioni di autenticazione e cifratura, OTR fornisce:

- **segretezza in avanti** (perfect forward secrecy);
- **autenticazione negabile** (deniable authentication).

XMPP

Extensible Messaging and Presence Protocol (XMPP) è un insieme di **protocolli aperti** di messaggistica istantanea e presenza basato su XML.

Il software basato su XMPP è diffuso su **migliaia di server** disseminati su Internet.

XMPP

I principali **punti di forza** sono riassumibili in:

- sistema decentralizzato;
- standard aperto;
- diffusione;
- sicurezza;
- flessibilità.

XMPP

Sistemi desktop

Categoria	Software
Sistema operativo	Distribuzione GNU/Linux o BSD (attenzione ad Ubuntu)
Client e-mail	Mozilla Thunderbird (o equivalenti) con add-on per cifratura Enigmail (o equivalenti)
Messaggistica istantanea e VoIP	Jitsi (o equivalenti)
Internet browser	Mozilla Firefox o Tor Browser Bundle
Motore di ricerca	DuckDuckGo

Sistemi mobile

Categoria	Software
Sistema operativo	CyanogenMod, Replicant, Firefox OS
App store	F-Droid
Client e-mail	K-9 Mail con APG (o equivalenti)
Messaggistica istantanea	ChatSecure o Xabber
VoIP	CSipSimple
Internet browser	Orweb, Orfox (con Orbot)
Motore di ricerca	DuckDuckGo
Navigatore	OsmAnd

Troppe configurazioni?

Tails

- Tails è un **sistema operativo Live**.
- Avviabile su **qualsiasi computer** tramite DVD, penna USB o scheda SD.

Tails

Il suo obiettivo è **preservare la privacy e l'anonimato** dell'utente aiutandolo a:

- usare internet in modo anonimo eludendo la censura: tutte le connessioni ad internet sono forzate attraverso la rete **Tor**.
- **Non lasciare tracce** sul computer "ospitante", a meno che l'utente non lo voglia esplicitamente.
- Usare strumenti di **cifratura allo stato dell'arte** per criptare file, e-mail e messaggi istantanei.

Domande?

Domande

Chiarimenti

Approfondimenti

Grazie a tutti

Ing. Davide Mainardi

 @ingMainardi

 is.gd/05kWjX