Privacy: la sfida del 21esimo secolo

ViGLug – Linux Day 2015

A cura di: Andrea Boero (mail@tsumi.it)
Video introduttivo prodotto da: La Quadrature du Net (http://www.laquadrature.net/)

Premesse (1)

Lo scandalo del Datagate è cosa nota e, nonostante l'argomento sia ancora in parte nebuloso, il problema esiste e **non possiamo ignorarlo**.

*- Quindi ora **che si fa**?*

*- Bisogna dare un **giro di vite**.*

*- Sì, ma **come**?*

*- E' ora di cominciare una **migrazione**.*

Premesse (2)

Impossibile presentare una soluzione tecnica

- La soluzione è **soggettiva**, risponde alle mie necessità
- La soluzione è **incompleta**, il lavoro è tutt'ora in corso
- La soluzione potrebbe non essere **la migliore possibile**

Quindi come affrontiamo l'argomento?

- Capire **perché** l'argomento “privacy” ci interessi tutti
- Dare delle basi per capire ed approcciare correttamente il problema

Non ho nulla da nascondere

[…] Il ministero dell'interno ha disposto che venga compiuta una esatta rilevazione degli ebrei residenti nelle province del Regno […]

[…] Si attende di conoscere non oltre il 18 corrente se in codesto Comune vi siano o meno ebrei indicandone le generalità […]

[…] Il lavoro di rilevazione deve essere effettuato con riservatezza assoluta, con la massima precisione e celerità, e non deve dare comunque appiglio ad alcun allarme trattandosi di rilevazioni ad esclusivo fine di studio. […]

"Urgente Riservatissima" - 14 Agosto 1938 [1]

Le leggi razziali in Italia vengono promulgate **il mese successivo**.

[1] http://www.isrecsavona.it/pubblicazioni/carte%20della%20persecuzione/sezione%20prima/pagina%201.htm

A me non importa

Ad alcune persone
“non importa”
della privacy ...

… e pensano che
tanto la cosa
non riguardi gli altri.

In realtà, ogni volta
che si comunica,
si crea un piccolo
spicchio di privacy ...

Dire “non mi importa”
della mia privacy
non è solo mancanza
di amor proprio ...

… che è responsabilità
di entrambi

… è anche mancanza
di rispetto verso gli altri ...

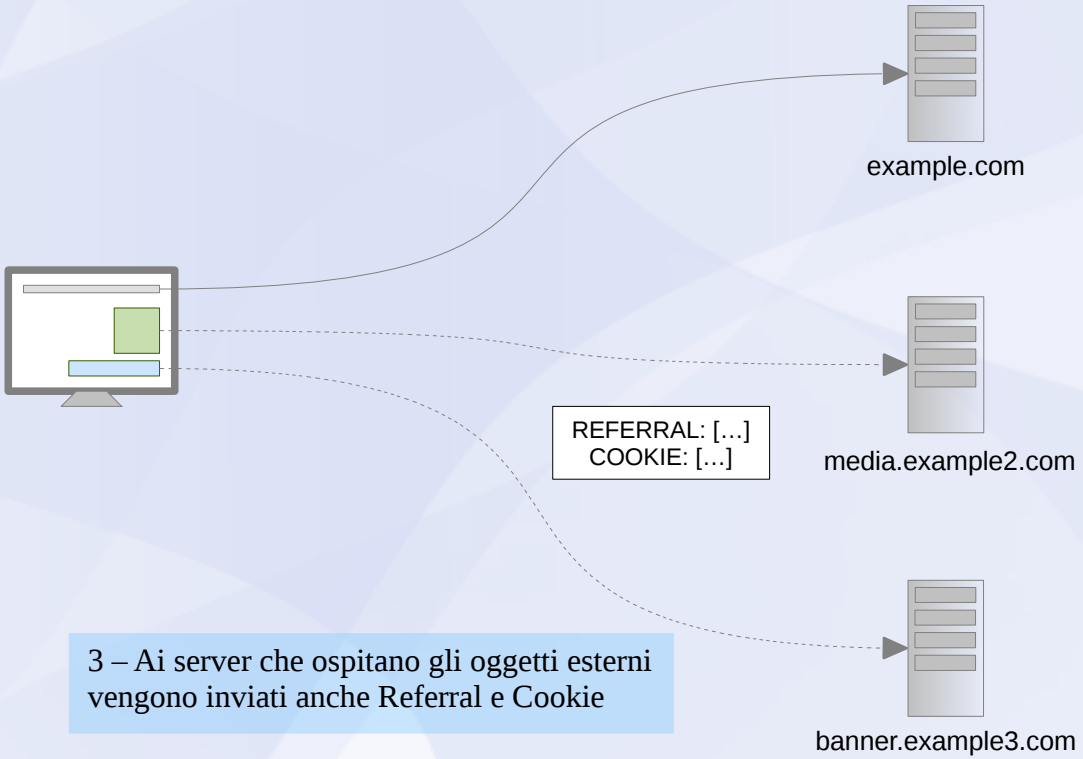
… è un po' come dire che
non ci importa di loro.

Quindi che fare?

Qualche spunto di riflessione non tanto per risolvere quanto per inquadrare meglio il problema:

- Evitare il rastrellamento dei dati
- Evitare soluzioni verticali
- Usare la cifratura
- Farsi le domande giuste

Evitare il rastrellamento dei dati (1)



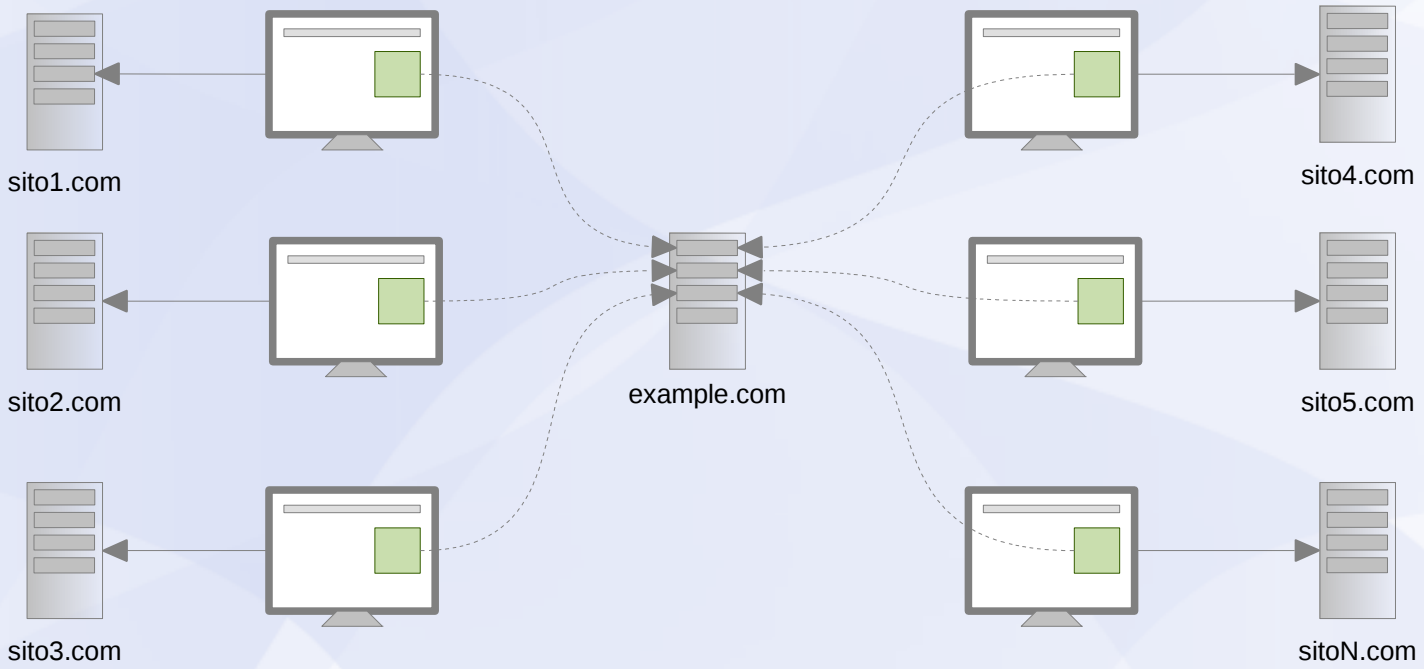
1 – La pagina viene richiesta al server che la ospita

2 – Gli oggetti esterni vengono richiesti ai relativi server che li ospitano

3 – Ai server che ospitano gli oggetti esterni vengono inviati anche Referral e Cookie

Evitare il rastrellamento dei dati (2)

E se un oggetto esterno fosse incluso da un grande numero di siti differenti?



Allora il server che lo ospita potrebbe tracciare buona parte della cronologia di navigazione degli utenti.

Evitare il rastrellamento dei dati (3)

Ma quali contenuti potrebbero avere una tale diffusione?

- I pulsanti social
- I tools per il tracking delle visite
- I circuiti pubblicitari

Esiste un modo per mitigare il problema?

- Plugin per il browser che impediscano il caricamento di questi oggetti esterni come Privacy Badger [1], Disconnect [2] ed uBlock Origin [3].

[1] https://www.eff.org/privacybadger
[2] https://addons.mozilla.org/it/firefox/addon/disconnect/
[3] https://addons.mozilla.org/it/firefox/addon/ublock-origin/

Evitare soluzioni verticali

Le soluzioni centralizzate non rappresentano un rischio solo per quanto riguarda il tracciamento, ma anche accumulare grandi moli di dati può rappresentare un pericolo:

- Condizioni del servizio nebulose
- Appetibili ai malintenzionati
- Appetibili ai governi

Forse sarebbe consigliabile un approccio più orizzontale, anche hostando i servizi di cui si ha bisogno, sia in ambito personale che professionale:

- Sorveglianza a tappeto molto più difficile ed onerosa
- Buone probabilità che un'eventuale vulnerabilità non colpisca tutti contemporaneamente

Usare la cifratura

“The bottom line is that encryption does work”

Edward Snowden

La crittografia resta una tecnologia valida per difendere la nostra privacy, a patto che sia utilizzata correttamente.

Ha ovviamente delle limitazioni:

- Non ci garantisce l'anonimato (alcuni dati come mittente e destinatario della comunicazione restano in chiaro)
- Sposta sugli endpoint il problema della sicurezza (questi potrebbero non essere sicuri o il nostro interlocutore negligente)

Resta comunque una soluzione migliore di una trasmissione in chiaro:

- Utilizzare sempre HTTPS, dove disponibile (specialmente su reti wifi condivise)
- Cifrare mail e chat con strumenti come GPG o OTR (questo rende sicuro il canale, anche qualora passi su server non fidati)

Farsi le domande giuste (1)

Non fidarsi solo di ciò che ci viene detto ma provare a verificarlo di persona. Certo, non è possibile verificare tutto da soli, ma ci sono un paio di cose che possiamo fare quando ci troviamo davanti ad un qualsiasi applicativo o servizio:

- Informarsi
  - Leggere review e recensioni altrui, specialmente quelle negative, che possono far sorgere i dubbi giusti
  - Cercare informazioni associando parole chiave come “privacy”, “sicurezza” e “backdoor”
- Farsi delle domande
  - I dati che vengono richiesti sono realmente necessari al suo corretto funzionamento?

Farsi le domande giuste (2)

Un esempio concreto, un app flashlight [1] per smartphone, richiede i seguenti permessi:

- Localizzazione GPS
- Accesso a foto e video salvati
- Accesso alle reti wireless
- Identificativo del telefono
- Accesso completo ad internet

Anche a prima vista pare un po' troppo per far solo accendere un led, se poi leggiamo l'informativa sulla privacy ci accorgiamo che i dati di localizzazione vengono esplicitamente raccolti ed utilizzati a scopo commerciale/pubblicitario [2].

Nonostante tutti questi indizi pare che molti non si siano nemmeno posti il problema, l'app infatti conta, secondo lo Store, decine di milioni di installazioni [3].

[1] http://www.techrepublic.com/blog/it-security/why-does-an-android-flashlight-app-need-gps-permission/
[2] http://www.goldenshorestechnologies.com/privacypolicy.html
[3] https://play.google.com/store/apps/details?id=goldenshorestechnologies.brightestflashlight.free

Software Libero,
un buon punto di partenza

“Libertà 1: Libertà di studiare il programma e modificarlo.”

Che implica la possibilità di verificare l'assenza di:

- Backdoor
- Invio silente di dati personali verso terzi
- In generale comportamenti non documentati

Un possibile punto di partenza per cercare soluzioni alternative libere e rispettose della privacy può essere **http://prism-break.org/** (*) che, nato all'indomani delle prime rivelazioni, propone un elenco di possibile soluzioni Open ai più diffusi applicativi e servizi.

(*) PRISM-BREAK non è, e non vuole essere, la soluzione definitiva, potrebbe contenere imprecisioni, essere incompleto o non aggiornato e come qualsiasi soluzione va presa con la dovuta attenzione, nessun software può rimpiazzare il buon senso!

Alternative, una rapida carrellata

OwnCloud

Una piattaforma Cloud completamente Open, self-hosted, con relativi client per l'integrazione con PC e smartphone e con supporto cloud a:

- File sharing
- Calendario
- Contatti
- Feed RSS

Alle quali si aggiungono funzionalità ancora in sviluppo come l'editing a più mani dei documenti.

https://owncloud.org/

F-Droid

Uno Store alternativo per Android che raccoglie solo app OpenSource e che rispettino standard minimi di privacy.

https://f-droid.org/

Diaspora

Una piattaforma di Social Network con tutte le più comuni funzionalità ma con una struttura distribuita e decentralizzata.

https://joindiaspora.com/

Let's Encrypt

Una CA per la creazione di certificati SSL validati e gratuiti promossa da EFF e Mozilla che verrà lanciata a Novembre.

https://letsencrypt.org/

"Chi è pronto a dar via le proprie libertà fondamentali per comprarsi briciole di temporanea sicurezza non merita né la libertà né la sicurezza."

Benjamin Franklin