La privacy ai tempi di PRISM

VigLug - Linux Day 2013

A cura di Andrea Boero (mail@tsumi.it) -

Premesse (1)

L'argomento è nebuloso:

- Poche notizie certe e dimostrabili con prove concrete ed inconfutabili
- Tante smentite e pochi chiarimenti da parte delle autorità coinvolte

L'argomento andrebbe affrontato da un punto di vista altamente tecnico:

- La giornata del Linux Day dovrebbe essere quanto più possibile accessibile a tutti, non-tecnici compresi
- L'argomento è complesso ed articolato, non può essere affrontato in modo adeguato in mezz'ora

Premesse (2)

Come affronteremo quindi la questione?

- Qualche considerazione “filosofica” che aiuti ciascuno a giudicare autonomamente l'argomento privacy con un atteggiamento più critico
- Un esempio pratico di quanto sia fragile la nostra privacy online

Una breve panoramica

Alla fine di Maggio Edward Snowden si rifugia ad Hong Kong.

A distanza di pochi giorni il quotidiano “The Guardian” comincia a pubblicare documenti riservati fornitigli da Snowden che rivelano:

- Una raccolta massiccia dei metadati relativi alle telefonate passanti su suolo Americano [1]
- La presunta esistenza di PRISM, un progetto che con la “collaborazione” di grandi aziende dell'IT permetterebbe l'accesso “diretto” alle informazioni conservate sui server di suddette compagnie [2]

Seguono immediate smentite da parte delle aziende coinvolte e parziali ammissioni di Obama sul progetto tentando però di sminuirlo.

Qualche tempo dopo Snowden ottiene asilo politico in Russia, dove si troverebbe tuttora.

[1] http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
[2] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Altre notizie non confermate

Nei mesi successivi ulteriori dettagli vengono alla luce come:

- Presunte intercettazioni a danno dei cittadini e dei governi Europei, tornate peraltro sotto i riflettori proprio in questi giorni [1] [2] [3]
- La presunta collaborazione dei servizi segreti di altri stati, tra cui Inghilterra ed Italia, alla raccolta dei metadati ed all'intercettazione della dorsale internet [4]
- Presunte attività volte ad inserire negli standard e negli applicativi commerciali backdoor e vulnerabilità finalizzati ad aggirare i sistemi di cifratura [5]
- La presunta esistenza di un sistema, Tempora, volto all'intercettazione a tappeto per successiva analisi dei dati trasmessi sulla dorsale internet [6]

Purtroppo la maggior parte notizie a riguardo non sono supportate da prove concrete a parte i documenti riservati forniti dallo stesso Snowden.

La loro discussione non sarà pertanto oggetto di questo talk, come anticipato.

[1] http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies
[2] http://www.repubblica.it/esteri/2013/10/23/news/usa_hanno_intercettato_il_cellulare_di_angela_merkel-69293020/
[3] http://www.repubblica.it/esteri/2013/10/21/news/datagate_registrate_milioni_di_telefonate_francesi_parigi_scioccante_ora_spiegazioni-69059578/
[4] http://www.repubblica.it/esteri/2013/10/24/news/nsagate_la_germania_convoca_l_ambasciatore_usa-69322576/
[5] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[6] http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Cosa sono i metadati

"When it comes to telephone calls, nobody is listening to your telephone calls. That's not what this program is about. As was indicated, what the intelligence community is doing is looking at phone numbers and durations of calls."

Barack Obama – 07/06/2013 [1]

- They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.
- They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.
- They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.

Why Metadata Matters – EFF – 07/06/2013 [2]

[1] http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president
[2] https://www.eff.org/deeplinks/2013/06/why-metadata-matters

Figurati se a qualcuno importa quello che dico!

Leigh Van Bryan, 26 anni, bloccato alla frontiera USA, sospettato di terrorismo ed interrogato per un Tweet ironico.

"Free this week, for quick gossip/prep before I go and destroy America."

Il tweet incriminato

"Mr Bryan confirmed that he had posted on his Tweeter website account that he was coming to the United States to dig up the grave of Marilyn Monroe."

Dal rapporto dalla Homeland Security [1]

[1] http://www.bbc.co.uk/news/technology-16810312

Come se avessi qualcosa 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

Una dimostrazione pratica

C'è qualche volontario?

L'esempio dei pulsanti social

- Si trovano nella maggior parte dei siti
- Non si notano più di tanto, fanno parte delle funzionalità del sito stesso
- Caricano contenuti da server esterni
- Come effetto collaterale inviano alcune informazioni su chi siamo e su che pagina stiamo visitando

```
<a href="https://twitter.com/share" class="twitter-share-button" data-via="tsumi_it"
data-lang="it">Tweet</a>
<script>!function(d,s,id){var js,fjs=d.getElementsByTagName(s)
[0],p=/^http:/.test(d.location)?'http':'https';if(!d.getElementById(id))
{js=d.createElement(s);js.id=id;js.src=p+'://platform.twitter.com/widgets.js';fjs.parent
Node.insertBefore(js,fjs);}}(document, 'script', 'twitter-wjs');</script>
```

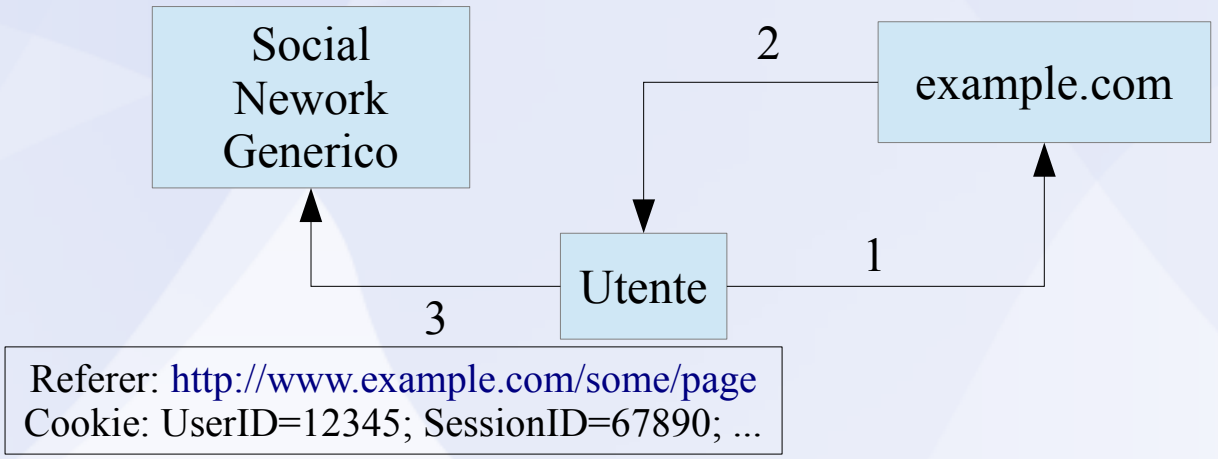
L'esempio dei pulsanti social (2)

Un esempio semplificato:

1) L'utente richiede una pagina del sito example.com

2) Example.com risponde con la pagina richiesta

3) La pagina contiene dei pulsanti social ed il browser richiede al server relativo i dati necessari a visualizzarlo, inviando nel contempo l'URL della pagina che lo ingloba ed i cookie che contenere informazioni sull'utente che la sta visualizzando



L'esempio dei pulsanti social (3)

- La pagina che stiamo visitando viene inviata come referer

```
GET /widgets.js?_=[redacted] HTTP/1.1\r\n
Host: platform.twitter.com\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/535.22+ (KHTML, like Geck
Accept: */*\r\n
Referer: http://www.[redacted]
```

- Come anche i cookie che identificano la nostra sessione di login

```
01c0  41 6c 69 76 65 0d 0a 43  6f 6f 6b 69 65 3a 20 67   Alive..C ookie: g
01d0  75 65 73 74 5f 69 64 3d  76 31 25 33 41 31 33 36   uest_id= v1%3A136
01e0  [redacted]               36 36 39 33 31 38 34 3b   [redacted] 6693184;
01f0  20 73 65 63 75 72 65 5f  73 65 73 73 69 6f 6e 3d    secure_ session=
0200  74 72 75 65 3b 20 74 77  6c 6c 3d 6c 25 33 44 31   true; tw ll=l%3D1
0210  [redacted]               34 3b 20 64 6e 74 3d 31   [redacted] 4; dnt=1
0220  3b 20 72 65 6d 65 6d 62  65 72 5f 63 68 65 63 6b   ; rememb er_check
0230  65 64 3d 31 3b 20 72 65  6d 65 6d 62 65 72 5f 63   ed=1; re member_c
0240  68 65 63 6b 65 64 5f 6f  6e 3d 31 3b 20 5f 5f 75   hecked_o n=1; __u
0250  74 6d 61 3d 34 33 38 33  [redacted]               tma=4383 [redacted]
0260  34 35 31 37 34 35 2e 31  [redacted]               451745.1 [redacted]
0270  [redacted]               36 36 37 33 2e 31 33 38   [redacted] 6673.138
0280  32 34 35 32 32 36 32 2e  34 3b 20 5f 5f 75 74 6d   2452262. 4; __utm
0290  [redacted]               36 38 2e 32 2e 31 30 2e   [redacted] 68.2.10.
02a0  31 33 38 32 34 35 32 32  36 32 3b 20 5f 5f 75 74   13824522 62; __ut
02b0  [redacted]               33 36 38 3b 20 5f 5f 75   [redacted] 368; __u
02c0  74 6d 7a 3d 34 33 38 33  [redacted]               tmz=4383 [redacted]
02d0  36 30 34 34 31 34 38 2e  31 2e 31 2e 75 74 6d 63   6044148. 1.1.utmc
02e0  73 72 3d 28 64 69 72 65  63 74 29 7c 75 74 6d 63   sr=(dire ct)|utmc
02f0  63 6e 3d 28 64 69 72 65  63 74 29 7c 75 74 6d 63   cn=(dire ct)|utmc
```

Soluzioni?

Difendersi con strumenti che filtrino e blocchino le connessioni verso terzi:

- Plugin come AdBlock, Disconnect, ecc

Intervenire attivamente producendo soluzioni più “etiche” e rispettose della privacy:

- Ad esempio implementando i pulsanti social in modo che non richiedano connessioni verso terzi per venire visualizzati

Ed il software libero?

"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

Tornando a PRISM un possibile punto di partenza per cercare soluzioni alternative libere e rispettose della privacy può essere http://prism-break.org/ (*) nato all'indomani delle prime rivelazioni.

(*) 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!

"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