Privacy e sicurezza ai tempi del cloud

Francesco P. Lovergine
<frankie@fsfe.org>

Free Software Foundation Europe
Fellowship Group Bari

Foundation

http://www.fsfe.org/

Who am I ?

- OSMapper dal 2008
- Ricercatore CNR dal 1997
- Debian Developer dal 2000 →
- FOSS activist da sempre
- Presidente LugBARI 2002–2009
- Geek per nascita :-)

Outline

- La questione delle libertà digitali
- La questione della privacy e sicurezza
- Cos’è e quali sono i pericoli del **SaaSS**
- Come (provare a) difendere noi stessi
- Come (provare a) difendere gli altri
- Utenti, developer e altre vittime

Statement

“Se una compagnia vi invita ad usare il suo server per fare le vostre attività informatiche, non cedete, e non usate SaaSS. Non comprate, né installate ‘thin clients’, quei computer così poco potenti che vi costringono a fare tutto il vero lavoro su un server, a meno che questo non sia un server vostro.

Per amore della vostra libertà, usate computer veri, tenete i vostri dati lì ed eseguite le vostre attività informatiche sulla vostra copia di un programma libero.”

– RMS

Le 4 libertà del free software

- Libertà 0: Libertà di eseguire il programma per qualsiasi scopo. La libertà di usare un programma significa libertà per qualsiasi tipo di persona od organizzazione di utilizzarlo su qualsiasi tipo di sistema informatico, per qualsiasi tipo di attività e senza dover successivamente comunicare con lo sviluppatore o con qualche altra entità specifica. Quello che conta per questa libertà è lo scopo dell'utente, non dello sviluppatore; come utenti potete eseguire il programma per i vostri scopi; se lo ridistribuite a qualcun altro, egli è libero di eseguirlo per i propri scopi, ma non potete imporgli i vostri scopi.
- Libertà 1: Libertà di studiare il programma e modificarlo. L'accessibilità al codice sorgente è una condizione necessaria per il software libero, altrimenti non avrebbero senso neanche la libertà 0 e la 2.
- Libertà 2: Libertà di ridistribuire copie del programma in modo da aiutare il prossimo.
- Libertà 3: Libertà di migliorare il programma e di distribuirne pubblicamente i miglioramenti, in modo tale che tutta la comunità ne tragga beneficio. Questa libertà comprende quella di usare e rilasciare le versioni modificate come software libero. Una licenza libera può anche permettere altri modi di distribuzione; insomma, non c'è l'obbligo che si tratti di una licenza con copyleft. Tuttavia, una licenza che imponesse che le versioni modificate non siano libere non si può categorizzare come licenza libera.

Ma mentre nessuno guardava ...

- I paradigmi IaaS, PaaS e soprattutto SaaS stanno implementando un nuovo (?) paradigma subdolo:

  Service as a Software Surrogate

- Un diverso e più sottile modo di minare le libertà digitali degli individui.
- Si richiede di abdicare alle quattro libertà (e qualche altra...) in nome di una presunta comodità d'uso.

Rischi ancora più ampi

- Social networks
- Internet of Things
- Personal device
- *The next Big Thing…*

Quanti percepiscono effettivamente i rischi connessi agli attuali trend digitali?

Quali sono i rischi?

- Limitazione delle libertà digitali.
- Riduzione della privacy oltre il percepito a livello superficiale.
- Security threats per dispositivi e servizi di fatto pervasivi.
- Dipendenza da sistemi e servizi inerentemente “a termine” e al di fuori di qualsiasi patto sociale.
- I monopoli generano mostri. Sempre.

Mitigare il rischio

- L’unico ~~computer~~dispositivo sicuro è un ~~computer~~dispositivo disconnesso. Esserne coscienti è il primo passo.
- Privilegiare soluzioni *in house* sempre e comunque. Una soluzione IaaS/PaaS è meno deleteria di una soluzione SaaS (per es. OwnCloud invece di Dropbox).
- Non usare un servizio quando un programma funziona altrettanto bene (per es. usare Libreoffice invece di Google Docs).
- Aggiungere propri livelli di encryption a quelli presumibilmente adottati dai servizi di uso comune (es. storage cloud). → duplicity over Dropbox
- Minimizzare le informazioni personali condivise.
- Diversificare le soluzioni.
- Privilegiare soluzioni, formati e protocolli aperti e standard.
- Minimizzare il numero di dispositivi trusted ed il numero di app e servizi/applicazioni “a black box”.
- Le informazioni realmente (soggettivamente o oggettivamente) private ed importanti devono essere ospitate criptate e solo su sistemi su cui si ha un totale controllo.
- Protocolli peer-to-peer possono essere usati per implementare soluzioni completamente distribuite

Come salvare la nonna digitale?

- Obbiettivamente difficile!
- Il digital divide è meglio di un uso inconsapevole di strumenti potenzialmente pericolosi.
- Diffondere consapevolezza, soprattutto tra i minori ed i non addetti.
- La via più complicata è spesso quella più giusta.
- La maggior parte delle aziende sono condannate. Occorre individuare opportunità di vantaggio competitivo nella scelta di soluzioni fuori cloud o non convenzionali per spingere le aziende a soluzioni diverse.
- Network no-profit/gruppi di utenza possono essere una soluzione da esplorare

Discussione