

Cancellare le tracce. Online e non solo.

Come aumentare il livello di privacy, usando software Open Source e seguendo una serie di semplici regole.

La nostra dipendenza dal software, sia per utilizzare programmi locali sia per accedere a servizi online, continua ad aumentare. Una conseguenza è che esistono davvero tanti modi, tutti più o meno invisibili, in cui lasciamo continuamente tracce molto precise di *tutto* quel che facciamo, sia nei nostri computer sia all'esterno, su Internet. Certo, fino a un certo punto questa notevole perdita di privacy è inevitabile, altrimenti non potremmo pretendere che un word processor riapra proprio l'ultimo documento su cui avevamo lavorato, oppure che un sito Web ci riconosca da una visita all'altra. Allo stesso tempo, sarebbe sbagliato lasciare tutti i software con cui veniamo a contatto (ovvero chi gestisce i corrispondenti servizi online) raccogliere *tutte* le informazioni possibili su di noi, se non è *realmente* indispensabile per le varie attività o se c'è la possibilità che dati personali vengano anche scambiati con altri siti. Fortunatamente, almeno se si utilizza software Open Source, ottenere un livello di protezione sufficiente per le attività dell'utente medio, è sia gratis sia relativamente facile, se si ha un'idea adeguata di alcuni pericoli e delle soluzioni corrispondenti.

Un esempio pratico

Per capire che quelle appena esposte non sono considerazioni puramente

teoriche basta pensare all'uso di Internet più comune oggi in Italia, ovvero Facebook. I pulsanti "Mi piace", "Condividi" o altri tipi di interazioni con Facebook sono ormai presenti su siti Web di tutti i tipi. Il problema (a prescindere da opinioni personali su Facebook) è che usarli o semplicemente visitare una pagina che li contiene non rimane necessariamente *dentro* Facebook, e anche quando lo fa potrebbe avere conseguenze imbarazzanti. Si pensi, tanto per fare un esempio assai verosimile e assolutamente innocente, a un utente che visiti continuamente portali immobiliari, perché vuole andare a vivere da solo. Se anche uno solo di quei portali fosse collegato a Facebook, quest'ultimo se ne accorgerebbe e potrebbe cominciare subito a piazzare annunci immobiliari nella bacheca dell'utente.

D'altra parte, ormai dovremmo sapere tutti che Facebook è gratis proprio e solo perché guadagna in quel modo, quindi nessun problema, giusto? Certo... fino al momento in cui *qualcun altro* vede quella bacheca, per esempio l'ignaro consorte dell'utente!

Abbandonare definitivamente

Facebook neutralizzerebbe esclusivamente *quella* particolare "spia" dei nostri movimenti ovviamente questa non è una vera soluzione. Ormai lo stesso problema esiste con qualsiasi social network e servizio online, incluso Gmail.

Come funziona il tracciamento online

Nell'ambito di questo articolo, il termine tracciamento indica tutte le tecniche utilizzate dai vari fornitori di servizi Web per riconoscere e seguire i singoli utenti, anche quando si spostano continuamente da un sito all'altro o ritornano solo a distanza di mesi. Tutti questi dati vengono automaticamente analizzati per ricostruire, come minimo, gusti abitudini e bisogni di ogni visitatore. Nel migliore dei casi, il risultato è utilizzato solo per mostrare a ognuno di noi tutti e solo i banner pubblicitari su cui potremmo effettivamente fare clic. Nel peggiore, per rivenderli o scambiarli con terze parti, da governi ad altre aziende.

Il sistema di tracciamento più semplice e più antico fra quelli oggi in circolazione, è costituito dai *cookie* (biscotti). Si tratta di piccoli file di testo, contenenti codici di riconoscimento alfanumerici, che i vari siti spediscono ai nostri browser, o si fanno rispedire per riconoscerli,

Time Zone	2.85	7.19	
Screen Size and Color Depth	13.63	12668.59	
System Fonts	20.46	1437885.5	esint10, esfs10, cmr10, DejaVu S L, Lc Devan
Are Cookies Enabled?	0.42	1.34	
Limited supercookie test	0.99	1.98	

I nostri browser si fanno riconoscere con sorprendente accuratezza: quello nell'immagine era l'unico su quasi un milione e mezzo con una certa configurazione di font installate!



come se fossero la tessera di abbonamento a un club. Alcuni cookie sono limitati a un solo sito, nel senso che la loro esistenza è nota solo al server che li ha inizialmente consegnati, altri no. Nel primo caso solo il sito emittente può chiedere ai nostri browser di mostrarci i suoi cookie quando torniamo a visitarlo. I cookie veramente insidiosi dal punto di vista della privacy sono però quelli che possono essere richiesti anche da server diversi. È grazie a loro che un portale generico può scoprire quali *altri* siti abbiamo già visitato, magari in sessioni diverse.

Oltre i cookies: trucchi Flash o Html5

Se i cookie fossero l'unico modo di violare la privacy di chi naviga online la vita sarebbe più semplice, ma purtroppo non è più così da un pezzo. Invece le contromisure anti cookie vanno comunque usate, se non altro perché potrebbero essere le uniche possibili quando non si può assolutamente modificare la configurazione del computer (si pensi a luoghi di lavoro, Internet Kiosk e simili), ma non è possibile fermarsi lì.

A parte i cookie (e le microimmagini invisibili inserite nelle pagine Web, che funzionano in modo simile) i controllori più insidiosi che ci seguono sul Web vengono generati localmente, dai nostri stessi browser. In generale, si tratta di oggetti che hanno più o meno la stessa funzione dei cookie ma generati, gestiti e scambiati da codice scaricato direttamente da Internet perché parte di qualche pagina Web. È per questo che le normali funzioni di filtraggio dei cookie, di cui i browser si occupano senza intermediari, sono

inefficaci contro di loro.

Al momento, il caso più comune di questo tipo è quello dei Locally Shared Objects (Lso). Questi oggetti binari vengono creati e scambiati con i server dai vari plugin Flash che ormai troviamo integrati in tantissime pagine Web. Un gioco Flash, ad esempio, potrebbe servirsi di un Lso per conservare punteggio e preferenze degli utenti.

Altri meccanismi sfruttabili nello stesso modo, cioè per spiare tutto quel che facciamo online, sono disponibili in molte tecnologie sviluppate per rendere il Web più dinamico. L'*Isolated Storage* di Microsoft Silverlight, per esempio, è nato per creare nel computer degli utenti uno spazio sicuro e isolato, appunto, dal resto del computer. Tale spazio era stato inizialmente concepito per farci girare applicazioni Silverlight scaricate da Web, quindi potenzialmente pericolose, senza rischi per la sicurezza. Purtroppo, può essere utilizzato anche per nascondervi dati equivalenti ai cookie. Html5, con la sua capacità di conservare dati in locale in vari formati, presenta lo stesso problema. C'è poi chi riesce a lasciare e recuperare dati per la nostra identificazione addirittura dalle stesse cache dei browser, oppure forzandoli a connettersi a Url fittizi, che poi rimangono nella storia delle pagine già visitate.

Questa molteplicità di opzioni per il tracciamento ha indotto alcuni programmatori a parlare di cookie "zombie", capaci cioè di rinascere in diverse forme quando si cerca di distruggerli. In pratica, se si eliminano solo i cookie testuali ma gli stessi dati rimangono dentro un Lso, basterà quest'ultimo per trasmetterli al server e quindi



L'indirizzo Ip non serve solo per farsi rintracciare su Internet, ma corrisponde anche alla nostra reale posizione fisica, sia pure in maniera approssimata.

identificare l'utente alla visita successiva. Di conseguenza, più che di zombie si dovrebbe parlare della mitologica Idra, che poteva essere uccisa solo tagliandole contemporaneamente *tutte* le teste.

L'esempio migliore, e più inquietante, di ciò che stiamo illustrando è la libreria Open Source chiamata evercookie (<http://samy.pl/evercookie>). Si tratta di uno strumento tanto potente per un webmaster che volesse tracciare a tutti i costi i visitatori del suo sito, quanto preoccupante per i sostenitori della privacy sempre e comunque. Questo codice JavaScript è in grado di salvare dati identificativi in *dodici* modi diversi, che includono tutti quelli di cui abbiamo appena parlato! Il bello, per così dire, di evercookie è che non conosce mezze misure. Ogni volta che gira, il suo codice provvederà a convertire e salvare qualsiasi dato, anche in uno solo di quei formati, in tutti gli altri.

Quando i browser lasciano firma e indirizzo

Oltre ai sistemi di tracciamento che i browser, volenti o nolenti, raccolgono dall'esterno, occorre preoccuparsi anche di quelli che di fatto esistono nei nostri computer ancora prima di iniziare a navigare. Per vedere con i vostri occhi ciò di cui stiamo parlando, provate a fare clic sul pulsante "Test Me" del sito <https://panopticklick.eff.org>. Dopo pochissimi secondi questo servizio della Electronic Frontier Foundation produrrà una tabella simile a quella nella figura a pagina 172.

Il suo significato è presto detto: i valori

Quante altre informazioni si trasmettono?

Come abbiamo appena visto, per sapere cosa racconta il vostro browser, o dove sembra che si trovi visto da Internet, basta visitare siti come Panopticklick. Quella però non è l'intera storia. Le perdite di dati possono avvenire dall'interno, cioè tramite trojan che trasmettono dati riservati; oppure iniziare anche prima di uscire su Internet, all'interno della rete locali aziendali o pubbliche, magari Wi-Fi, a cui si è connessi. Verificare quali e quanti dati sensibili sono a rischio per motivi del genere, cioè perché vengono trasmessi in chiaro e/o senza ragione, è relativamente semplice con analizzatori di traffico come l'Open Source Wireshark (<http://wireshark.org>). Questo programma cattura tutto il traffico in transito sulla Lan a cui è connesso, riconoscendo e segnalando automaticamente vari tipi di pacchetti o stringhe (per esempio password) richiesti dall'utente.

Distribuzioni Linux “usa e getta”

Per una distribuzione Linux girare in modalità “Live”, significa partire da un mezzo non scrivibile come Cd o Dvd, e poi girare senza problemi anche se non c'è alcuna possibilità di salvare dati da nessuna parte. Server e altre applicazioni che devono creare file temporanei per funzionare lo fanno in speciali cartelle, create appositamente a ogni avvio nella Ram del computer ospite.

Tutte le distribuzioni Linux possono essere modificate per funzionare in questo modo, anche se non ne sono già capaci nella loro versione standard. Quelle descritte nei paragrafi successivi sono fra le più interessanti di quelle specificamente sviluppate per lavorare come descritto nell'articolo principale della rubrica.

BitBox

www.sirrix.com/content/pages/BitBox_en.htm

È un ambiente virtuale per la navigazione sicura sviluppato dall'Ufficio federale tedesco per la Sicurezza Informatica per essere usato dai dipendenti pubblici. La versione per singoli utenti è scaricabile da tutti e consente di navigare online, anche su siti basati su tecnologie interattive potenzialmente pericolose, senza pericolo di compromettere il sistema operativo principale e i dati degli utenti. Il browser di BitBox gira in una macchina virtuale preconfigurata che viene creata ex-novo ogni volta. Lo scambio di file con il resto del sistema è possibile solo attraverso una cartella, che viene automaticamente analizzata per scoprire eventuali virus e altri rischi per la sicurezza.

Ipredia

www.ipredia.org

Offre navigazione, condivisione di file e comunicazioni anonime via Internet I2P tramite browser, e client email, Irc e BitTorrent. Rispetto alle altre distribuzioni che presentiamo, la sua caratteristica peculiare è quella di affidarsi al sistema di routing anonimo I2P, meno popolare di Tor ma per certi aspetti più sicuro.

Liberté Linux

<http://dee.su/liberte>

Questa versione Live di Linux Gentoo potrebbe essere la più interessante per chi vuole navigare tranquillo anche se ha solo conoscenze elementari di Linux. Nel pacchetto sono inclusi suite da ufficio, Gimp, supporto per video Html5 e altre applicazioni multimediali e interfaccia (tastiera inclusa) in diverse lingue. Dal punto di vista della sicurezza, Liberté provvede automaticamente prima di fermarsi a cancellare tutto quanto ha scritto in Ram, e usa

varie tecniche di anonimizzazione specifiche per reti Wi-Fi. Tutte le comunicazioni via Internet sono automaticamente instradate nella rete Tor (o I2P, su richiesta). Allo stesso tempo, è disponibile un browser separato “insicuro”, specificamente per registrarsi con hot spot Wi-Fi che altrimenti rifiuterebbero connessioni via Tor.

Lightweight Portable Security

www.spi.dod.mil/lipose.htm

Lps Linux è una distribuzione sviluppata e certificata per il telelavoro sicuro dall'Aeronautica degli Stati Uniti. L'interfaccia grafica, ovviamente solo in inglese, ricorda quella di Windows Xp, e contiene soltanto Firefox e poche altre applicazioni per il lavoro d'ufficio.

Privatix

www.mandalka.name/privatix/

È un derivato di Debian specializzato per la navigazione sicura. Contiene le applicazioni desktop base di Debian più numerose funzioni preconfigurate per cifrare documenti e comunicazioni. Le impostazioni del sistema possono essere salvate separatamente su partizioni cifrate di chiavi Usb o dischi rigidi.

Ubuntu Privacy Remix

Anche se affronta, in linea generale, lo stesso problema della sicurezza descritto nel resto della rubrica, questa versione ufficiale di Ubuntu lo fa con un approccio davvero unico. Ubuntu Privacy Remix, o Upr brevità, è talmente paranoica che impedisce sia di connettersi in rete sia di accedere a dischi fissi locali! Tutto il sistema, dal kernel in su, è modificato leggere o salvare file esclusivamente da dischi rimovibili cifrati. Anche se, per ovvie ragioni, Upr non può essere usata per navigare su Internet, Upr potrebbe comunque essere la soluzione ideale per chi, pur non essendo un esperto informatico, debba lavorare su documenti talmente importanti e riservati da non poter rischiare di esporli a virus o copie non autorizzate.

XTailsx

<https://xtailsx.boum.org/index.en.html>

Costruita sulla versione stabile di Debian, Xtailsx è un desktop completo di Gimp e OpenOffice ottimizzato per comunicazioni cifrate. Oltre a un browser preconfigurato con tutti i plugin descritti nell'articolo principale, Xtailsx contiene sia un client (Claws Mail) preconfigurato per posta elettronica cifrata sia il plugin Otr (Off-the-Record Messaging) per Pidgin, per proteggere le conversazioni chat.

nella seconda colonna misurano quanto è unica, cioè utile per riconoscervi quando vi spostate da un sito all'altro, senza usare alcun tipo di cookie, la “firma digitale” del vostro browser. In questo contesto per firma digitale di un browser si intende semplicemente la sua configurazione, così come viene trasmessa a tutti i siti che visita: modello, versione, sistema operativo, fuso orario in cui si trova, tipo e versione di tutti i plugin e font installate e così via. In teoria, i browser hanno un motivo preciso per descriversi con tanta esattezza. Informazioni del genere potrebbero infatti essere utili ai server per spedire a ogni browser pagine ottimizzate per le sue capacità.

A livello di privacy, però, le controindicazioni sono evidenti. Il browser usato per il test (reale!) è l'unico, fra i quasi un milione e mezzo visti da Panoptick fino a quel momento, ad avere quella particolare configurazione di font. Questo rende così lo usa tracciabile con grandissima accuratezza quando si sposta da un sito all'altro: basta confrontare le “firme” richieste da ogni server per capire quanti dei loro visitatori sono in realtà la stessa persona (o meglio, a essere pignoli, lo stesso browser dello stesso computer). Queste analisi diventano ancora più precisi quando alla firma dei browser si aggiunge la loro geolocalizzazione. Questa non è altro che l'individuazione del luogo da cui ci si sta connettendo a Internet, a partire dall'indirizzo Ip del proprio computer.

Come si vede dalla figura a pagina 173, tratta dal portale www.mio-ip.it, la localizzazione è approssimativa (il computer utilizzato era al centro di Roma), ma abbastanza precisa da essere utilizzabile per un tracciamento, anche senza cookie e senza conoscere nome e cognome del navigatore.

«Anche bloccando i cookies si può rimanere esposti a sistemi di identificazione che sfruttano Flash o Html5»

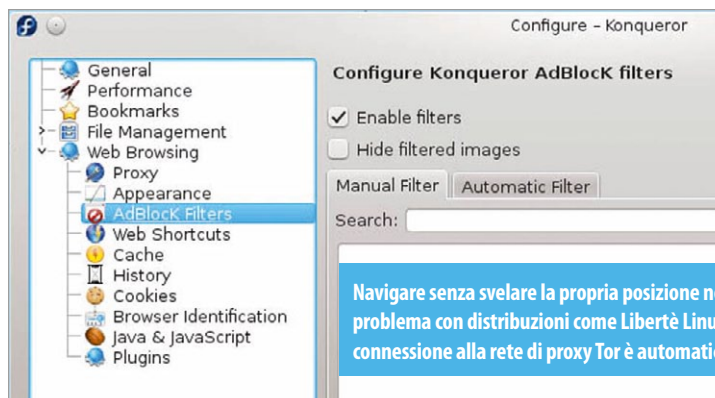
Come proteggersi

Nella prima, lunga parte dell'articolo ci siamo deliberatamente dilungati sui vari modi in cui si possono trasmettere dati sensibili, semplicemente perché si è connessi a Internet o si naviga sul Web. Questo era necessario per far capire natura e portata del rischio, ma ora occorre passare all'azione. Come fare per limitare i danni?

I browser più popolari per Linux, ovvero Chrome, Firefox e Konqueror, permettono tutti di bloccare tutti o parte dei cookie, o eliminare quelli rimasti da precedenti sessioni. Sono disponibili anche protezioni dal phishing, che avvertono quando si sta per entrare in siti potenzialmente falsi, e opzioni per disabilitare *completamente* l'esecuzione automatica di script. Purtroppo l'ultima misura, che pur riduce notevolmente sia i rischi di tracciamento tramite firma del browser sia l'esposizione ad attacchi veri e propri, ha lo stesso effetto anche sull'utilizzabilità di parecchi siti. L'opzione anti-tracciamento di Firefox è ancora meno utile, perché di fatto è una richiesta di non essere tracciati che i singoli siti sono liberi di ignorare.

Estensioni di Firefox

Le cose migliorano installando plugin per Firefox (o i loro equivalenti per Chrome e Safari) come Ad-Block Plus (Abp) o NoScript. Il primo blocca tutti i banner pubblicitari elencati in una lista di cui scarica periodicamente l'ultima versione da Internet. NoScript è un filtro come Abp ma più generale: anziché i soli banner, evita lo scaricamento di tutto il codice JavaScript elencato nella sua lista nera, che ovviamente l'utente può configurare a piacere. Nemmeno NoScript, comunque, può



garantire protezione assoluta da siti che sfruttano evercookie. Questi due plugin, così come il Phishing Protector scritto appositamente per Facebook, sono tutti scaricabili da <https://addons.mozilla.org>. Quello chiamato HTTPS Everywhere, invece, si trova sul sito della EFF che ne cura lo sviluppo (www.eff.org/https-everywhere): la sua funzione è costringere tutti i siti in grado di farlo a comunicare con Firefox solo tramite connessioni cifrate (Https, appunto) invece di quelle Http standard, che trasmetterebbero tutto in chiaro password comprese.

Tor

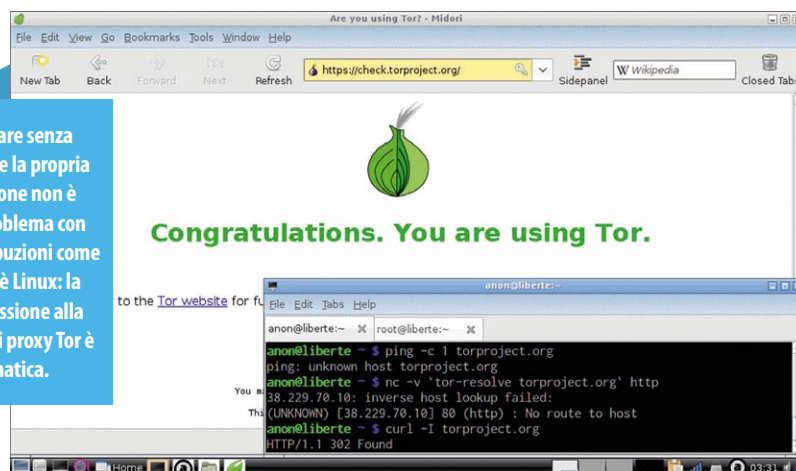
Pur con qualche limite, le soluzioni viste finora proteggono gli utenti dall'essere riconosciuti e seguiti online o dall'intercettazione dei dati che scambiano con i siti che visitano. Nessuna di loro però evita la geolocalizzazione. Quando questo è un problema, il modo più semplice di affrontarlo è navigare attraverso Tor (www.torproject.org): una serie di proxy, cioè di passaggi intermedi che, pur rallentando la navigazione, rendono molto più difficile capire da dove è

iniziata, cioè da dove ci si sta connettendo a Internet. Il modo più semplice di usare Tor è il Tor Button, un plugin Open Source per Firefox scaricabile dal sito.

Computer usa e getta (ovviamente Open Source)

A leggere quanto abbiamo scritto fin qui si potrebbe anche pensare che l'unica possibilità di rimanere anonimi online senza essere hacker di prima forza sia smettere del tutto di navigare, o almeno evitare tutti i social network. D'altra parte, anche volendo, le contromisure di cui abbiamo parlato potrebbero essere quasi inefficaci contro malware vero e proprio, oppure semplicemente inapplicabili in certe occasioni. Il caso più frequente è l'essere costretti a effettuare operazioni delicate, come un bonifico via Internet, da computer di terze persone, che non possiamo certo modificare in alcun modo né analizzare per scoprire virus o altre fonti di problemi.

In teoria, tutte le operazioni davvero sensibili, dal banking online alla scrittura di documenti riservati, dovrebbero avvenire in ambienti sterili,



RISORSE

Gli Lso di Flash sono descritti, in maniera molto accessibile, nell'articolo www.html.it/articoli/local-shared-object-i-cookie-di-flash-1/. Chi volesse scoprire in dettaglio come vengono analizzate le firme dei browser troverà tutte le informazioni corrispondenti all'indirizzo <https://panoptick.eff.org/browser-uniqueness.pdf>.

addirittura sconnessi dalla rete quando, come per scrivere documenti, non ce n'è davvero bisogno. Oltre a questo servirebbe almeno la sicurezza che qualsiasi attacco, sia da Internet sia da malware già presente nel computer, abbia effetti soltanto temporanei sul sistema.

Hai usato Linux? Buttalo

Il modo più semplice per arrivare a questi risultati è servirsi di distribuzioni ausiliarie "usa e getta". Una distribuzione Linux Live, che gira da Cd o chiave Usb, **non** può né conservare cookie e simili, né esporre i propri file a rischi di attacchi da Internet. Per sua stessa natura, infatti, una distribuzione del genere non può avere accesso ai dischi principali se non viene esplicitamente autorizzata. Soprattutto è una distribuzione che svanisce, letteralmente, alla fine di ogni sessione, portandosi dietro qualsiasi cosa buona o cattiva abbia ricevuto via Internet. Navigare nella Rete **soltanto** da una distribuzione del genere vuol dire quindi farlo in un ambiente che non può consentire i tracciamenti di cui abbiamo parlato. La prima controindicazione che potrebbe venire in mente, ovvero il fatto che in quel modo non si perderebbero anche bookmark e dati del genere, si può risolvere conservando i relativi file su chiavi Usb. Questa soluzione è ancora più interessante se si considera che non è nemmeno necessario riavviare il computer ogni volta che si vuole navigare anonimamente. Tutte le distribuzioni ottimizzate per l'anonimità online descritte nell'altro articolo possono infatti essere utilizzate all'interno di macchine virtuali, senza interrompere l'attività del proprio sistema operativo principale.

Cancellare le tracce locali

Chiudiamo ricordando che, oltre a quelle su Internet potrebbe essere opportuno proteggere da sguardi indiscreti (per esempio di colleghi o parenti curiosi) anche tante attività completamente localizzate *all'interno dei nostri computer*, come l'elenco degli ultimi file o programmi che abbiamo utilizzato. Il modo più semplice per farlo, in Ubuntu e altre distribuzioni basate su Gnome, è disabilitare o resettare la registrazione delle attività nell'*Activity Log Manager*. •

Linux News

Linux sempre più avanti: nuovo kernel e scheda per il supercomputing 3.9.0

Lo scorso maggio ha visto l'arrivo del primo kernel Linux 3.9 (ricordiamo che le serie con seconda cifra dispari sono sperimentali) e della scheda Parallela (con due «L», www.parallela.org). Linux 3.9 contiene, fra l'altro supporto per utilizzare dispositivi a stato solido come cache dei dischi rigidi tradizionali e file system Btrfs in configurazioni Raid 5 e 6. Altre modifiche del kernel ne migliorano le prestazioni nelle applicazioni in parallelo su sistemi multiprocessore. Quest'ultima novità potrebbe essere sfruttata anche sulle schede Parallela. Su questi dispositivi, che costano all'incirca cento dollari, chiunque può costruire supercomputer ad alte prestazioni per applicazioni scientifiche basate interamente su software Open Source.

Una Nuova Debian vi aspetta

La distribuzione Debian produce una nuova versione ufficialmente chiamata "stabile" solo una volta ogni qualche anno. Questo approccio, se la rende inadatta per chi ha davvero bisogno di tutte le ultime novità Open Source, è una garanzia preziosa per chi ha esigenze molto diverse ma altrettanto importanti. Lo dimostra Debian 7.0, disponibile da maggio, che utilizza ancora il vecchio kernel Linux 3.2 ma supporta tantissime architetture hardware, dai mainframe System Z di Ibm ai processori embedded Armv7, passando per architetture obsolete come MIPS e PowerPC. Debian 7 è anche la prima versione di questa distribuzione che può supportare simultaneamente programmi sviluppati per diverse architetture. Il supporto al cloud computing tanto di moda in questo periodo è presente tramite OpenStack e Xen Cloud Platform. Sempre parlando di cloud computing, immagini pronte di Debian 7 sono fornite anche da piattaforme pubbliche come Amazon Ec2, Windows Azure e Google Compute Engine.

oDesk e Linux Professional Institute mettono in mostra programmatori ed esperti Linux

oDesk (www.odesk.com) è uno dei più importanti portali al mondo in cui offrire o cercare lavoro da consulente. Il Linux Professional Institute (www.lpi.org), invece, è il maggiore ente di formazione e certificazione Linux al mondo. Un recente accordo fra queste due organizzazioni dovrebbe dare più visibilità a chi ha buone competenze professionali Linux. Le banche dati di oDesk e Lpi, infatti, verranno connesse in modo da mostrare automaticamente su oDesk le certificazioni Lpi dei singoli iscritti. I dettagli del programma sono disponibili all'indirizzo www.lpi.org/partnerships/jobs.

Il campione dei sistemi informatici liberi per ospedali

Gnu Health (<http://health.gnu.org/>) è un software gestionale, interamente Open Source, sviluppato specificamente per ospedali e ambulatori e già adottato da decine di strutture in tutto il mondo, dall'Argentina al Bangladesh e al Qatar. Le sue capacità vanno dalla gestione completa di apparecchiature, personale e cartelle cliniche dei pazienti a quella del bilancio e delle fatture. Oltre a quello puramente tecnico, comunque di tutto rispetto, di Gnu Health va sottolineato quello sociale. Gli autori del sistema collaborano infatti con le Nazioni Unite per raggiungere gli Obiettivi di Sviluppo del Millennio, curando funzioni per monitoraggio e prevenzione di Aids, malaria e tubercolosi.

L'Estremadura è sempre più Open Source. E risparmia milioni

Questa regione autonoma della Spagna è particolarmente all'avanguardia nell'uso di Linux e altro software Open Source nella Pubblica Amministrazione. Già anni fa, ad esempio, decine di migliaia di desktop in scuole e strutture sanitarie pubbliche erano stati equipaggiati con Linex (<http://linex.gobex.es>), uno spin-off di Debian sviluppato in loco. Quest'anno, avendo concluso una dettagliata fase di studio e inventario, la regione ha lanciato la parte operativa di quello che sarà una delle più importanti migrazioni al mondo di desktop pubblici al software libero. Nel corso del 2013, 40mila postazioni dovrebbero passare a Sysgobex, un ambiente per integrare procedure burocratiche e sanitarie e semplificare l'amministrazione di sistema.