Bollettino telematico di filosofia politica

bfp

Richard Stallman

Puoi fidarti del tuo computer?

Traduzione dall'originale inglese di Maria Chiara Pievatolo.

Da chi dovrebbe prendere ordini il nostro computer? I più pensano che i loro computer debbano ubbidire a loro, e non a qualcun altro. Con un progetto detto "trusted computing" (computing affidabile) grandi concentrazioni mediatiche, comprendenti l'industria cinematografica e discografica, assieme con aziende informatiche come Microsoft e Intel, vogliono fare in modo che il nostro computer non obbedisca a noi, ma a loro. Non è la prima volta che nel *software* proprietario vengono incluse funzioni malevole: questo progetto, tuttavia, le renderebbe universali.

Il *software* proprietario comporta, in sostanza, che non sia possibile controllare quello che fa: infatti non si può né studiare il suo codice sorgente né cambiarlo. Non è sorprendente che abili uomini d'affari trovino modi per usare questo tipo di controllo allo scopo di mettere l'utente in una posizione svantaggiosa. La Microsoft l'ha fatto parecchie volte: una versione di Windows era progettata per riferire alla Microsoft quale *software* fosse installato sull'*hard disk* dell'utente; un recente aggiornamento "di sicurezza" in Windows Media Player richiedeva all'utente di dare il suo consenso a nuove restrizioni. Ma la Microsoft non è da sola: il programma di condivisione di musica Kazaa è progettato in modo tale da permettere ai soci di KaZaa di affittare l'uso dei computer degli utenti ai loro clienti. Queste funzioni malevole sono spesso segrete, ma anche quando se ne è conoscenza è difficile rimuoverle, perché non si dispone del codice sorgente.

In passato questi erano casi isolati. Il "trusted computing" farà sì che si diffondano capillarmente. "Treacherous computing" (computing inaffidabile) è un nome più appropriato, perché questo progetto è studiato per assicurare che il computer disobbedisca sistematicamente all'utente. È pensato, in effetti, per impedire che il nostro computer funzioni come una macchina aperta a tutti gli scopi. Ogni operazione dovrà richiedere un permesso esplicito.

L'idea tecnica alla base del *treacherous computing* è l'inclusione nel computer di un sistema di cifratura e firma digitale, le cui chiavi sono tenute segrete all'utente (la versione della Microsoft è chiamata "Palladium"). I programmi proprietari useranno questo sistema per controllare quali programmi l'utente può far girare, a quali documenti o dati può accedere, e a quali programmi può passare questi dati. Questi programmi scaricheranno da Internet sempre nuove regole di autorizzazione e le imporranno automaticamente al lavoro dell'utente. Se l'utente non consentirà al computer di ricevere periodicamente dalla rete le nuove regole, alcune funzioni dei programmi saranno disabilitate automaticamente.

Naturalmente, Hollywood e le industrie discografiche prevedono di usare il *treacherous computing* per i sistemi DRM (*Digital Restrictions Management*) perché i video e la musica scaricata possano essere fatti girare soltanto su un determinato computer. La condivisione sarà completamente impossibile, almeno per i file autorizzati ottenuti da queste aziende. Ma noi, il pubblico, dovremmo avere sia la libertà sia la capacità di condividere le cose. Immagino che qualcuno troverà il modo di produrre versioni non cifrate, pubblicarle e condividerle, e perciò il DRM non avrà un successo completo: ma questo non è un argomento a discarico del sistema.

Rendere la condivisione impossibile è abbastanza brutto, ma c'è di peggio. Si progetta di impiegare le stesse funzioni per i messaggi di posta elettronica e i documenti. Avremo così messaggi che spariscono entro due settimane o documenti leggibili solo sui computer di una determinata azienda.

Immaginate di ricevere dal vostro capo un messaggio di posta elettronica che vi dice di fare qualcosa che giudicate rischioso; un mese dopo, quando la cosa vi si ritorce contro, non potrete usare il messaggio per dimostrare che la scelta non è stata vostra. "Metterlo per iscritto" non vi protegge quando l'ordine è scritto con l'inchiostro simpatico.

Immaginate di ricevere dal vostro capo un messaggio di posta elettronica che stabilisce una linea di condotta illegale o moralmente inaccettabile, come strappare i documenti contabili dell'azienda o mettere a repentaglio la sicurezza nazionale. Oggi potete inoltrare questi messaggi ad un giornalista e denunciare tali attività. Col *treacherous computing*, il giornalista non sarà in grado leggere il documento; il suo computer si rifiuterà di obbedirgli. Il *treacherous computing* sarà un paradiso per la corruzione.

Programmi per l'elaborazione di testi come Microsoft Word potrebbero usare il *treacherous computing* quando salvano i documenti, per assicurarsi che non siano leggibili da *word processor* concorrenti. Oggi, per far sì che i *word processor* liberi riescano a leggere i documenti Word, dobbiamo carpire i segreti di questo formato con laboriosi esperimenti. Se Word cifrerà i documenti usando il *treacherous computing* quando li salva, la comunità del *software* libero non avrà nessuna possibilità di sviluppare programmi capace di leggerli, e, se ci riuscisse, questi potrebbero essere vietati dal Digital Millennium Copyright Act.

I programmi che usano il *treacherous computing* scaricheranno sempre nuove regole di autorizzazione dalla rete e le imporranno automaticamente al nostro lavoro. Se alla Microsoft, o al Governo americano, non piace quanto diciamo in un documento scritto da noi, si potrebbero spedire nuove istruzioni che ordinino ai computer di impedire a chiunque di leggerlo. Ogni computer ubbidirebbe, una volta scaricate le regole più recenti. La vostra scrittura sarebbe soggetta ad una cancellazione retroattiva alla maniera di *1984*. Anche l'autore potrebbe non essere in grado di leggere quanto ha scritto.

Si penserebbe che, una volta individuate le male azioni di un programma di *treacherous computing* ed esaminati i suoi effetti dolorosi, sia possibile decidere se accettarle o no. Sarebbe miope e sciocco accettarle; ma il problema è che l'accordo che si crede di star concludendo non è stabile. Una volta che si è venuti a dipendere dall'uso di un programma, si è catturati, e loro lo sanno. Per questo possono cambiare le condizioni dell'accordo. Alcuni programmi scaricheranno automaticamente aggiornamenti che faranno qualcosa di diverso, e loro non vi permetterano di scegliere se aggiornarli o no.
Oggi possiamo evitare le costrizioni del *software* proprietario non usandolo. Se si adopera uno GNU/Linux o un altro sistema operativo libero, e se non ci si installano programmi proprietari, si controlla quello che fa il nostro computer. Se un programma libero ha una funzionalità malevola, altri sviluppatori della comunità la elimineranno e si potrà usare la versione corretta. Si possono anche far girare programmi e strumenti liberi su sistemi operativi non liberi; questo non rende pienamente liberi, ma molti utenti lo fanno.

Il *treacherous computing* mette a repentaglio la stessa esistenza dei sistemi operativi liberi e dei programmi aperti, perché non potremmo neppure farli girare. Alcune versioni di *treacherous computing* richiederanno che il sistema operativo sia autorizzato da una determinata azienda. I sistemi aperti non potranno essere installati. Altre versioni richiederanno che ogni programma sia specificamente autorizzato dal produttore del sistema operativo. Su tale sistema, non si potrebbero far girare programmi liberi; e se capissimo come farli girare e lo dicessimo a qualcuno, questo potrebbe essere un reato.

Negli Stati Uniti ci sono già proposte di legge per imporre a tutti i computer di adottare il *treacherous computing* e proibire di connettere a internet i vecchi computer. Il CBDTPA (noi lo chiamiamo "Consume But Don't Try Programming Act") è una di queste. Ma anche se non ci obbligassero giuridicamente a passare al *treacherous computing*, la pressione ad accettarlo potrebbe essere enorme. Oggi si usa spesso il formato Word per le comunicazioni, anche se questo causa vari tipi di problemi (vedi anche http://www.gnu.org/philosophy/no-word-attachments.html). Se i documenti nel formato Word più recente fossero leggibili solo da macchine che adottano il *treacherous computing*, molti passerebbero a queste, se considerassero la cosa solo in termini di azione individuale (prendere o lasciare). Per opporci al *treacherous computing* dobbiamo unirci e affrontare la situazione come una questione di scelta collettiva.

Per altre informazioni sul *treacherous computing* vedi http://

www.cl.cam.ac.uk/users/rja14/tcpa-faq.html.

> Per fermare il *treacherous computing* occorrerà che un gran numero di cittadini si organizzi. Abbiamo bisogno del tuo aiuto! La Electronic Frontier Foundation (www.eff.org) e Public Knowledge (www.publicknowledge.org) stanno facendo una campagna contro il *treacherous computing*, e così anche il Digital Speech Project (www.digitalspeech.org) appoggiato dalla FSF. Visitate i loro siti web e sostenete il loro lavoro.
> Si può contribuire anche scrivendo agli uffici di relazioni col pubblico di Intel, IBM, HP/Compaq, o di qualunque altro produttore di computer dicendo che non si vuole esser costretti a comprare sistemi di "trusted" computing e perciò non si vuole che vengano prodotti. Questo può far valere il potere dei consumatori. Se lo fate per conto vostro, mandate copie delle vostre lettere alle organizzazioni di cui sopra.

Note finali

1. Il Progetto GNU distribuisce GNU Privacy Guard, un programma che applica sistemi di cifratura a chiave pubblica e firma digitale e può essere usato per inviare messaggi di posta elettronica sicuri e privati. È utile esaminare quanto GPG differisca dal *treacherous computing* e vedere cosa rende l'uno comodo e l'altro pericoloso.
Quando qualcuno impiega GPG per spedire un documento cifrato, e il ricevente usa GPG per decodificarlo, il risultato è un documento non cifrato che può essere letto, inoltrato, copiato o persino ri-cifrato per essere inviato in sicurezza a qualcun altro. Un'applicazione di *treacherous computing* consentirebbe all'utente di leggere le parole sullo schermo ma non di produrre un documento non cifrato da utilizzare in altri modi. GPG, un *software* libero, rende disponibili agli utenti delle funzionalità di sicurezza, e sono loro ad usarle. Il *treacherous computing* è progettato per imporre restrizioni agli utenti: in questo caso sono gli utenti ad essere usati.
2. Microsoft presenta Palladium come una misura di sicurezza e afferma che proteggerà dai virus, ma questa pretesa è evidentemente falsa. Una presentazione di Microsoft Research dell'ottobre 2002 ha affermato che una specifica del Palladium è la possibilità di far continuare a girare i sistemi operativi e i programmi esistenti; dunque, i virus continueranno ad essere in grado di fare tutto quello che possono fare oggi.
Quando Microsoft parla di "sicurezza" riferendosi a Palladium, non intende quello che con questo termine intendiamo normalmente, e cioè proteggere il computer da cose che l'utente non vuole. Intende invece proteggere le copie dei dati dell'utente sulla sua macchina dall'accesso da parte sua in modi che altri non vogliono. Una diapositiva di quella presentazione elencava alcuni tipi di segreti che Palladium potrebbe mantenere, inclusi "segreti di terze parti" e "segreti dell'utente" - ma metteva "segreti dell'utente" tra virgolette, riconoscendo che questo non è veramente lo scopo per il quale Palladium è stato progettato.
Quella presentazione faceva spesso uso di altri termini frequentemente associati con un contesto di sicurezza, come "attacco", "codice malevolo", "spoofing" e, appunto, "trusted". Ma nessuno di questi termini significa quello che indica normalmente, "Attacco" non significa che qualcuno sta cercando di danneggiarci, ma che l'utente sta tentando di copiare della musica. "Codice malevolo" significa codice installato dall'utente per fare qualcosa che qualcun altro non vuole che la sua macchina faccia. "Spoofing" non vuol dire che qualcuno cerca di ingannare l'utente, ma che l'utente vuole ingannare Palladium. E così via.
3. Una precedente dichiarazione degli sviluppatori di Palladium esponeva l'assunzione fondamentale che chiunque abbia sviluppato o raccolto informazione dovrebbe avere un controllo totale su come gli altri la usano. Questo rappresenterebbe un sovvertimento rivoluzionario delle idee di morale e di diritto finora invalse e creerebbe un sistema di controllo senza precedenti. I problemi specifici di questi sistemi non sono dunque casuali ma dipendono da questo fine fondamentale. E' questo fine che dobbiamo rifiutare.

Come contattarci | Come collaborare | Ricerche locali | Notifica degli aggiornamenti

Il Bollettino telematico di filosofia politica è ospitato presso il Dipartimento di Scienze della politica della Facoltà di Scienze politiche dell'università di Pisa, e in mirror presso **www.philosophica.org/bfp/**

Per contribuire, si vedano le **istruzioni per gli autori.**

A cura di:
Brunella Casalini
Emanuela Ceva
Dino Costantini
Nico De Federicis
Corrado Del Bo'
Francesca Di Donato
Angelo Marocco
Maria Chiara Pievatolo

Progetto web
di Maria Chiara Pievatolo

Periodico elettronico
codice ISSN 1591-4305
Inizio pubblicazione on line: 2000