Articolo tratto da Apogeo On-Line

Nei computer del prossimo futuro potrà girare soltanto software autorizzato (indovinate da chi), in modo da offrire finalmente diritti digitali realmente protetti all'industria del software, del cinema e del disco. I primi prototipi sono già in vendita. Effetti collaterali trascurabili: l'eliminazione definitiva di Linux e delle libertà degli utenti.

I piani di Microsoft per il futuro dell'informatica sono stati rivelati in questi giorni con un'anteprima nelle pagine di MSNBC/Newsweek: in un'iniziativa denominata Palladium, Microsoft si è alleata con Compaq, HP, IBM, Intel e AMD per creare una nuova generazione di software da abbinare a processori nei quali saranno integrate direttamente potenti funzioni di sicurezza. Sicurezza realizzata non più soltanto a livello software, come adesso, ma anche a livello hardware, come nei sistemi militari. L'obiettivo dichiarato è rendere più sicuro l'uso dei computer, che stando alle promesse di Microsoft diventeranno immuni ai virus, elimineranno lo spam, proteggeranno i nostri dati personali e consentiranno finalmente transazioni commerciali online sicure e l'avvio di servizi legali di distribuzione di musica e film attraverso Internet. Una vera rivoluzione, insomma, che dovrebbe arrivare concretamente entro il 2004, quando uscirà la prossima versione di Windows (denominata provvisoriamente Longhorn) e saranno pronti questi nuovi processori, ma che sta già entrando nelle nostre case e nei nostri uffici. Il portatile Thinkpad T-30 di IBM è già acquistabile con un sottosistema di sicurezza conforme allo standard Palladium (noto più tecnicamente come TCPA). La X-Box è in sostanza una versione 1.0 di un PC dotato di Palladium, come ho descritto recentemente. Il sistema di attivazione di Windows XP, che richiede un nuovo codice di sblocco se si cambia significativamente il proprio hardware, è un esempio (solo software) di Palladium. A prima vista, questa sembra la classica Ottima Idea che porterà benefici a tutti. Microsoft venderà una nuova versione di Windows, i produttori di hardware venderanno una nuova generazione di PC, e gli utenti della Rete, che da sempre reclamano sicurezza, finalmente navigheranno protetti. Per capire perchi in realtà Palladium è la materializzazione dei nostri peggiori incubi ci vuole una parentesi tecnica.

Come funziona Palladium/TCPA

Come descritto da Ross Anderson, dell'Università di Cambridge, in una FAQ ricca di dettagli, Palladium/TCPA si basa sul fatto che l'intera architettura del PC, anzichi essere aperta e pubblica, viene blindata: la comunicazione fra i vari componenti (tastiera, dischi, monitor) è cifrata, proprio come fa (parzialmente) l'X-Box, e il PC si avvia partendo da un chip speciale il cui contenuto è cifrato. Questo chip è un componente di monitoraggio che sorveglia costantemente lo stato del sistema e ne controlla il funzionamento (donde il nome Palladium, che non si riferisce all'elemento chimico ma all'omonima statua della dea Atena che sorgeva a Troia e proteggeva la città). All'accensione, il chip verifica il contenuto della ROM di boot e, se è quello previsto dai creatori del chip, ne consente l'esecuzione; poi verifica che l'hardware installato sia costituito esclusivamente da componenti autorizzati. Infine il chip verifica la porzione iniziale del sistema operativo e ne consente il caricamento soltanto se è conforme a quanto previsto. A questo punto la palla passa al sistema operativo, che carica le proprie parti rimanenti e si incarica di verificare continuamente che le applicazioni eseguite siano a loro volta certificate come sicure. Tutte queste verifiche e certificazioni consentono di avere un computer il cui stato è sicuramente conforme alle specifiche del produttore dell'hardware e del software. In altre parole, non può contenere modchip (i circuiti che si aggiungono adesso alle console per ampliarne le potenzialità) o programmi non autorizzati, che possano ad esempio intercettare un flusso di dati (un film o una canzone) per farne copie abusive. È una scatola chiusa nella quale non pur entrare nessuno, neppure l'utente. I sistemi anticopia introdotti finora sono sempre stati fallimentari perchi basati esclusivamente sul software, che per natura è facilmente modificabile. Palladium, invece, usa anche hardware dedicato. Rispetto al software, decifrare e modificare l'hardware è enormemente più

impegnativo, per cui questo sistema ha ottime possibilità di essere inviolabile non solo per l'utente comune ma anche per l'hacker più attrezzato.

L'utente come nemico

Questo modo di progettare computer ha delle conseguenze molto interessanti. Quella più ovvia è la fine della pirateria software, musicale e cinematografica domestica: se il flusso audio/video è cifrato lungo tutto il percorso all'interno del PC e oltretutto non è possibile installare programmi non autorizzati che lo registrino, come si fa a crearne copie abusive? Forti di questa garanzia, finalmente discografici e magnati di Hollywood potranno offrirci i loro prodotti via Internet, legalmente e (va da sé) a pagamento. Analogamente, i programmi saranno forse copiabili (per motivi di backup), ma non potranno essere eseguiti senza la relativa autorizzazione individuale. La conseguenza meno ovvia è che lo stesso sistema consente ai suddetti discografici e magnati di decidere che cosa possiamo vedere e ascoltare, nonché quando e quante volte possiamo farlo. I programmi di lettura (il Windows Media Player, per intenderci) saranno scritti in modo da suonare soltanto musica autorizzata. Dite addio alla vostra collezione di MP3, anche se sono legittimamente tratti dai CD che possedete e avete pagato. E non pensate nemmeno di installare un altro programma meno schizzinoso (come WinAmp): non funzionerà, perché non è software autorizzato. Applicando questa tecnologia al software, le conseguenze si fanno ancora più interessanti. Supponiamo che siate affezionati alla vostra copia di Office, che ha sempre funzionato ragionevolmente bene e conoscete a menadito, per cui non sentite il bisogno di spendere denaro per la nuova versione. Attualmente potete tenere Office sul vostro PC a tempo indeterminato. Ma con Palladium, all'uscita di Office 2004 Microsoft potrebbe bloccare l'esecuzione del vecchio Office sul vostro PC, obbligandovi ad acquistare la nuova versione. Benvenuti nell'era del software a tempo. Si prega di infilare un'altra monetina nella fessura, grazie. In altre parole, tutto ciò che passa per il nostro computer sarà controllato da un sistema di autorizzazioni gestito dai produttori di musica, film, hardware e software. L'utente non avrà modo di autorizzare nulla. Potrà soltanto aprire il borsellino ogni volta che qualche pezzo grosso di Hollywood decide di rifarsi la Jacuzzi. L'utente è cortesemente pregato di pagare e tacere: anzi, per dirla con Ross Anderson, per imporre i diritti digitali su un PC è indispensabile trattare l'utente come un nemico.

La morte di Linux e Apache

Un'altra conseguenza di Palladium/TCPA: se sui futuri PC potranno girare soltanto programmi autorizzati, il software libero e quello gratuito sono spacciati. I codici di autorizzazione non saranno certamente gratuiti: c'è un'infrastruttura di certificazione da mantenere e qualcuno la dovrà pagare. Di conseguenza, nessuno potrà più offrire freeware, ad eccezione dei grandi gruppi commerciali che possono permettersi di lavorare in perdita pur di togliere l'ossigeno alla concorrenza. Il vivace sottobosco dei piccoli programmatori indipendenti, che ci hanno regalato programmi storici come il già citato WinAmp, il mitico PKZip, Napster, WinMX e infinite altre chicche, sparirà. Fondamentalmente, ogni software scritto per Windows dovrà essere certificato. Da Microsoft, ovviamente: il che significa che spetterà a Microsoft decidere quali programmi sono degni di entrare nel suo regno blindato. Questo potere si presta a ogni sorta di abuso. È difficile pensare che Bill Gates autorizzerà WinAmp, o i lettori Divx, o qualsiasi suite di applicazioni per ufficio diversa da Office, quando sono in diretta concorrenza con i suoi prodotti. E che dire di Linux? In teoria è possibile realizzare una versione di Linux compatibile con i computer blindati dall'architettura TCPA, ma in pratica quel che ne viene fuori è l'ombra del Linux che conosciamo adesso. Innanzi tutto ci vuole un filantropo che paghi la procedura di certificazione (ogni software autorizzato deve essere esaminato per garantirne la sicurezza) per ogni singola versione del kernel e per ogni componente aggiuntivo del sistema operativo. Addio, quindi, alle distribuzioni Linux stracolme di software gratuito. Addio, naturalmente,

anche ad Apache, il server Web più diffuso del pianeta. Il movimento open source è completamente spiazzato. Diventa poi impossibile compilarsi un kernel su misura (non sarebbe certificato e quindi eseguibile), installare una patch e più in generale contribuire allo sviluppo di Linux. La flessibilità e libertà che sono la linfa vitale del successo di Linux sono strangolate. Anche se tutti questi ostacoli venissero superati e si arrivasse alla distribuzione di pacchetti RPM con firma digitale compatibili con Palladium/TCPA, resta il fatto che se sui nostri PC c'h un chip che decide quali programmi possiamo eseguire e persino quali file possiamo aprire, non siamo più padroni delle nostre macchine. In sostanza, Microsoft, IBM, HP e tutta l'allegra brigata del TCPA sono root sui nostri computer a casa e in azienda. E in più, tanto per gradire, hanno debellato ogni altra possibile concorrenza presente e futura. Molto, molto astuto.

Compromessi ingannevoli

Chi se ne frega, potrebbero dire in molti. Se quattro sfigati devono rinunciare a Linux in cambio della sicurezza planetaria, pazienza, ne vale la pena. E poi perché dovremmo installare altri programmi sul nostro PC, quando Microsoft include già tutto quello che ci serve? In fin dei conti, la separazione fra hardware e software nei computer è un'anomalia che in tutti gli altri apparecchi in casa e in ufficio non esiste. Quando acquistiamo un cellulare, un microonde, un videoregistratore, una Playstation o una telecamera, non pretendiamo di potervi installare un software alternativo; e grazie a questa integrazione fra hardware e software, questi apparecchi non vanno in crash come i PC. Forse sono dunque i PC ad essere stati progettati male, e Palladium rimedia a questa anomalia.

Il problema è che Palladium/TCPA non è concepito per proteggere noi utenti come ci vogliono far credere: è concepito per tutelare gli interessi dei produttori di hardware, software e media. Per esempio, è vero che un computer TCPA non eseguirà un virus (sarebbe software non certificato), ma non farà nulla contro un worm o una semplice pagina Web che contenga script che sfruttano una falla del sistema operativo. Non ci proteggerà dai furti dei codici delle carte di credito, che usano meccanismi su cui il TCPA non ha alcun effetto. Non ci proteggerà contro i crash delle applicazioni che ci fanno perdere ore di lavoro: il fatto che un programma sia certificato non ne garantisce affatto la robustezza. Per contro, consentirà alle industrie del software, del disco e del cinema di mungerci a loro totale piacimento. Proteggerà loro contro ogni tentativo di difendere i nostri diritti.

Diritti fondamentali

Quando parlo di diritti non mi riferisco soltanto al diritto di riversare su cassetta un CD regolarmente acquistato o di acquistare un DVD mentre si è in vacanza all'estero e vederselo a casa. Parlo anche di diritti un pochino più fondamentali. Nell'intervista a MSN/Newsweek, Bill Gates pronuncia questa frase:

> Ci siamo avvicinati al problema pensando alla musica, ma poi ci siamo accorti che l'e-mail e i documenti sono ambiti molto più interessanti.

L'idea, insomma, è di applicare le protezioni di Palladium non solo a musica, video e software, ma anche ai documenti. Gli esempi proposti nell'articolo sono rassicuranti: l'utente potrà scrivere e-mail che soltanto le persone autorizzate potranno copiare o inoltrare ad altri, e potrà creare documenti Word che saranno leggibili solo per una settimana. Tranquilli, ci viene detto, l'utente è sovrano. Ma il meccanismo di Palladium funziona anche nell'altro senso. Una macchina Palladium pur essere impostata in modo da bloccare l'accesso a pagine Web ritenute pericolose. Ad esempio, un pirata decide di mettere online una copia di un film, o un pedofilo pubblica la propria collezione fotografica di brutalità. Invece di perdere tempo con costose cause e indagini internazionali, è possibile riprogrammare da remoto tutti i computer Palladium in modo che non possano accedere a questi siti. Per

restare al passo con i pirati, infatti, le autorizzazioni di Palladium sono gestite tramite server centrali e sono revocabili e aggiornabili in qualsiasi momento. È un sistema molto efficiente, ma chi lo controlla? Usare Palladium significa togliere l'amministrazione della giustizia ai tribunali e metterla nelle mani delle aziende. Supponiamo che io scriva sul Web qualcosa di sgradito a Microsoft: chi mi dice che l'azienda di Redmond non userà Palladium per oscurarmi? Se qualcuno pubblica una brutta recensione dell'ultimo disco di Celine Dion, la Sony otterrà un'ingiunzione per usare Palladium per bloccarla? Se qualcuno rivela che il prossimo film di Star Trek è una boiata colossale, la Paramount lo zittirà? Se le mie idee politiche o religiose sono sgradite nel mio paese, il governo ordinerà ai server di Palladium di farle sparire dal Web? La tentazione è forte, anche perchi il sistema è rapido e indolore. Niente tribunali, niente cause, niente avvocati: due comandi su un terminale, e il gioco è fatto. Gli utenti Palladium non si accorgeranno neppure della censura. Non sapranno mai che è avvenuta.

Il finto pulsante di spegnimento

Va detto che secondo le specifiche del TCPA tutte le sue funzioni sono disattivabili dall'utente, che è libero di avviare il proprio PC nella maniera tradizionale. Questa facoltà è sicuramente stata introdotta per tranquillizzare gli utenti preoccupati delle proprie libertà, ma in realtà è un'operazione di facciata. Avviando il PC senza TCPA, non potrete usare nessuno dei suoi programmi certificati. Potrete forse far girare programmi non certificati (quelli attuali, per esempio), che però non riusciranno a comunicare con le periferiche, che per motivi di protezione del copyright si aspetteranno soltanto dati certificati. Se così non fosse, potreste stamparvi un libro scaricato da Internet oppure masterizzarvi un CD. Le cose peggiorano ulteriormente quando cercherete di andare sul Web. Se il sistema prende piede, in nome della sicurezza i siti Web commerciali rifiuteranno le connessioni dagli utenti che non usano macchine protette da Palladium. Questo costituirà un grande incentivo ad acquistare queste nuove macchine, il cui numero crescente spingerà sempre piy siti ad abbracciare Palladium, creando un effetto valanga identico a quello ottenuto nei browser da Internet Explorer: già ora molti siti non sono visitabili con browser diversi da quello Microsoft. Occasione da non perdere Per le grandi aziende, Palladium è davvero la Soluzione Finale: Linux e Apache eliminati, pirati dei media debellati, i programmatori indipendenti sul lastrico. Chi controlla Palladium controlla tutti i computer e, dietro gentile richiesta, controlla anche la libertà di lettura. Un quadretto desolante. Considerati i nomi e i capitali che appoggiano l'iniziativa Palladium/TCPA, sembra che ci si debba arrendere all'inevitabile. Soprattutto dopo gli eventi dell'11 settembre, c'è un'insensata corsa mondiale ad abbracciare incondizionatamente qualsiasi tecnologia che prometta anche vagamente di darci maggiore sicurezza. È fondamentale, invece, distinguere fra sicurezza reale e paccottiglia commerciale. Lottare contro questo abominio si può: lo abbiamo già fatto con successo in passato con il famoso numero di serie unico annidato nei Pentium III e poi rimosso a furor di popolo dalle generazioni successive. Il primo passo di questa lotta è diffondere la consapevolezza del problema. Questo è il mio piccolo contributo in proposito.

da Apogeo on line del 02/07/02 di Paolo Attivissimo

http://www.apogeonline.com/webzine/2002/07/02/01/200207020102