UEFI Secure Boot

Il prezzo della libertà

Davide Bolcioni

Autunno 2011

- Articolo sul blog di Matthew Garrett (Red Hat)

  Un PC conforme alle linee guida per Windows 8 che abbia la sola chiave Microsoft rifiiuterà di avviare un CD di installazione Linux, così come rifiuterà di avviare una qualsiasi distribuzione Linux eventualmente installata sul suo disco usando un altro PC

- Articolo su `lwn.net`
- Articolo su Punto Informatico

Requisiti per il logo Windows 8

- Per avere il logo Windows 8 un OEM deve
  - Attivare Secure Boot
  - Impedirne il controllo tramite programma
    - **Quale** programma ?
  - Assicurare che vengano impediti aggiornamenti del firmware non autorizzati
    - Autorizzati **da chi** ?

UEFI Secure Boot

- All'avvio viene eseguito il firmware UEFI
  - Svolge lo stesso ruolo del **BIOS**
- Esamina le memorie di massa che trova
- Riconosce le partizioni avviabili
- Segue una politica per avviare qualcosa
  - L'unico che trova
  - Il primo
  - Chiede all'utente

UEFI Secure Boot

- I file avviabili includono una firma
  - Firmati con una chiave privata
    - Nel caso di Windows 8, una di Microsoft
- Il firmware cerca la chiave pubblica corrispondente
- Il file viene letto e la firma viene verificata
  - Se non corrisponde, quel file non viene avviato
  - Tecnologia analoga a SSL
    - Ingegnerizzata da Intel
    - Sicura quanto lo *home banking*

Conseguenze

- Windows 8 da HD si avvia
  - Firmato dalla chiave Microsoft
    - Presumibilmente presente (OEM certification)
- Windows 8 da CD o USB si avvia
  - Idem
- Linux da CD si avvia ?

  La chiave è presente ?

Le chiavi del regno

- Chi controlla le chiavi UEFI controlla il PC
  - Il produttore del PC controlla la chiave iniziale
  - Quelle di Microsoft ci saranno
    - I produttori di PC non possono ignorare Windows
  - Red Hat potrebbe, probabilmente pagando
    - Non necessariamente in tutti
  - Canonical potrebbe, probabilmente pagando
    - Non è un costo da poco
  - Debian avrebbe presumibilmente difficoltà

Fornitore e consumatore

- Il fornitore sceglie le chiavi presenti
- Opzione per disabilitare la verifica della chiave
- Il fornitore può scegliere varie politiche
  - Solo la chiave Microsoft
  - La chiave Microsoft e la propria
  - La chiave di chiunque paghi abbastanza
  - Una chiave da dispositivo rimovibile (dopo)
  - Interfaccia di gestione delle chiavi
    - Aggiungi, Rimuovi, Abilita, Disabilita, ...

Il mercato PC

- Dominato da Microsoft
  - I produttori di PC non possono inimicarsela
- Margini (relativamente) modesti
  - Qualità di hardware e driver in declino
  - Spinta a ridurre i costi di supporto
  - Spinta ad accordi per software preinstallato
  - Obsolescenza programmata
- Futuro incerto
  - Cloud, smartphone e tablet

A pensar male - 1

- Ufficialmente per motivi di sicurezza
  - Strumenti di ripristino ?
- Stratagemma per tagliare le gambe a Linux
  - Quota di mercato in crescita
    - In particolare nei mercati emergenti
- Acquirente ostaggio delle scelte del fornitore
  - Scelte presenti ma soprattutto future
    - Software a corredo
    - Installazione OEM vincolata

A pensar male -2

- L'avvio è solo il primo passo
  - Una rana si può bollire viva ... piano piano
  - Con UEFI controllo cosa viene avviato
  - Ciò che viene avviato controlla che S.O. parte
    - Le chiavi sono nel TPM (aka Palladium)
  - Il S.O. controlla la chiave dei programmi avviati
    - Possono andare in esecuzione solo se autorizzati
      - Autorizzati da chi ?
  - Niente più software liberamente modificabile
    - Dà fastidio, perchè consente ai peones di scegliere

Attestazione

- Il software può proteggersi dalla copia e dall'uso fuori dai termini di licenza
  - Si collega via Internet per verificare
  - Questo controllo non può essere rimosso
- Si torna a pagare la licenza di ogni programma
  - Niente abuso del software OEM
  - Posso impedire la circolazione dell'usato
- Software in abbonamento, a consumo, a tempo
- Intrattenimento *pay per view*

Farsi pagare

- I produttori di PC possono farsi pagare
  - Per ciascuna chiave nel firmware UEFI
- I produttori di S.O. possono farsi pagare
  - Per ciascuna applicazione autorizzata
- I produttori di applicazioni possono farsi pagare
  - Per l'applicazione stessa
  - Per i contenuti che riproducono
  - Per autorizzare eventuali add-on
- I produttori di contenuti possono farsi pagare

Il momento di dire no

- Chi controlla le chiavi controlla il PC
- Proposta Intel: chiavi su CD e USB (PXE ?)
- Il momento di dire no al controllo è adesso
  - No alle chiavi, no al cloud, no all'attestazione
- Come con i brevetti software
  - Ci hanno provato e ci riproveranno
- Petizione della FSF

`http://www.fsf.org/campaigns/secure-boot-vs-restricted-boot`