Free Software Foundation recommendations for free operating system distributions considering Secure Boot

John Sullivan

Executive Director

June 30, 2012

(http://www.fsf.org/campaigns/secure-boot-vs-restricted-boot/whitepaper-web)

(Raccomandazioni di Free Software Foundation per le Distribuzioni di Sistemi Operativi Liberi considerando il Secure Boot - UEFI)

*(traduzione Italiana a cura di **Alberto Guglielmo**)*

Introduzione

Abbiamo lavorato sodo negli ultimi svariati mesi per cercare di porre un freno al **Restricted Boot** che rappresenta un grosso pericolo per la libertà degli utenti, gli obbiettivi del software libero e la sua diffusione. Con il paravento della sicurezza un computer controllato dal **Restricted Boot** si rifiuterebbe di caricare qualsiasi sistema operativo che non sia uno di quelli approvati in precedenza dal fabbricante. Il **Restricted Boot** toglie il controllo dalle mani degli utenti per porlo in in quelle di qualcun altro.

Per rispettare la libertà degli utenti e proteggerne realmente la sicurezza i fabbricanti di computer debbono fornire agli utenti o un modo per disabilitare queste restrizioni o un sistema *garantito* che permetta all'utente di installare il sistema operativo che desidera.

I distributori di sistemi con restrizioni, normalmente esprimono preoccupazioni sulla sicurezza. Essi affermano che se e' possibile eseguire sulle macchine che loro vendono del software non approvato da loro esse saranno preda di virus e malware. Solamente permettendo l'esecuzione del solo software da loro approvato essi possono proteggerci.

Queste affermazioni ignorano bellamente il fatto che siamo *noi* a doverci proteggere da *loro*. Noi non vogliamo macchine che eseguano solamente il software approvato da *loro*, noi vogliamo macchine che eseguano solamente il software approvato da *noi*. Possiamo anche decidere di dar fiducia a qualcun altro per poter decidere cosa approvare, ma non dovremo mai essere obbligati a farlo con restrizioni tecnologiche o legali. Il software che impone queste restrizioni e' esso stesso malware. Aziende come Microsoft che cercano di imporre queste restrizioni hanno a loro volta un passato veramente poco lusinghiero a proposito di sicurezza, il che rende le loro pretese di limitarci per il nostro bene vuote ed ingannevoli.

La **GNU** General Public License (GPLv3) difende la nostra liberta' contro queste limitazioni. Quando compri o affitti un computer contenente software coperto dalla GPLv3, la licenza garantisce la tua liberta' di utilizzare versioni modificate di tale software su quelle apparecchiature. Gia' la GPLv2 richiedeva che gli utilizzatori fossero sempre in grado di farlo, ma una delle migliorie apportate dalla GPLv3 richiede che le liberta' garantite da tutte le versioni GPL non possano essere limitate da hardware che si rifiuti di eseguire software modificato

A proposito di misure di sicurezza del processo di bootstrap, la GPLv3 prevede un unico semplice dovere: provvedere funzionalità e chiare istruzioni all'utenza per disabilitare o modificare radicalmente le restrizioni al bootstrap in modo che sia in grado di installare ed eseguire versioni modificate di qualsiasi software coperto da GPLv3.

Il Secure Boot e' una di queste misure, definita da uno standard UEFI, ma la discussione intorno a lui si e' svolta principalmente a proposito delle regole imposte da Microsoft nel Logo del suo S.O. Windows 8. Queste regole stabiliscono ciò che i distributori di computer debbono fare per far approvare a Microsoft i loro sistemi. Parte di queste regole include l'implementazione del Secure Boot in modi peculiari.

Per essere aderenti alle regole di Microsoft, come attualmente pubblicate, i distributori di architetture x86 devono fornire agli utilizzatori sia la possibilità di personalizzare il Secure Boot con le proprie chiavi che quella di disattivarlo completamente.

Secure Boot, realizzato correttamente, implementa la visione della sicurezza propria del software libero, perché da' agli utilizzatori, siano essi individui, agenzie governative o industrie, il controllo delle loro macchine. Il nostro esperimento concettuale per dimostrarlo e' semplice: Microsoft teme che produttori di malware possano impossessarsi di macchine che eseguono

Windows, ma noi vediamo Windows stesso come un virus e desideriamo impedirgli di funzionare sulle nostre macchine. Secure Boot ci da' la possibilità di impedire a Windows di eseguire su una macchina? Eccome: e' sufficiente rimuovere la chiave di Microsoft dal firmware di boot ed aggiungere la nostra e/o quelle di altri sviluppatori di software libero di nostra fiducia.

Ma allora dov'e' il problema?

In teoria non dovrebbero esserci problemi. In pratica la situazione è più complicata. Cosi' come e' proposto oggi il Secure Boot impedisce di utilizzare software libero. E' già sufficientemente brutto che praticamente ogni computer che viene venduto abbia Windows preinstallato. Per persuadere gli utilizzatori a provare del software libero, dobbiamo già ora convincerli a rimuovere il sistema operativo che che gli hanno fornito con il computer (o ripartizionare i loro hard-disk per far spazio al nuovo sistema operativo, con il dubbio di rischiare di perdere i loro dati nel farlo).

Con il Secure Boot i nuovi utenti di software libero debbono compiere un ulteriore passo per poterlo installare. Dal momento che questi sistemi operativi non hanno chiavi installate di default nel firmware di ogni computer, come invece Microsoft ha, gli utilizzatori debbono disabilitare il Secure Boot prima di poter eseguire l'installatore del nuovo sistema. I produttori di software propietario potrebbero (n.d.t. e sicuramente lo faranno) presentare quest'operazione come “disabilitare la protezione di sicurezza sul computer” che potrebbe far pensare ai potenziali utilizzatori che il software libero e' insicuro.

Senza dubbio questo e' un ostacolo di cui non avevamo bisogno proprio ora, ed e' assolutamente discutibile che l'incremento di sicurezza ottenibile con il Secure Boot compensi le difficoltà che causerà in pratica ai nuovi utilizzatori che tenteranno di provvedere alla loro sicurezza sfuggendo a Microsoft Windows.

E' anche un problema perché il Logo Windows 8 attualmente richiede senza eccezioni la presenza del Restricted Boot su tutti i sistemi ARM, che comprendono tipi di computer largamente diffusi come tablet e telefonini. Esso impone che gli utenti non siano in grado di disattivare le restrizioni al boot o inserire le proprie chiavi di sicurezza. Oltre ad essere inaccettabili nella loro stessa formulazione queste richieste sono un rovesciamento dell'iniziale posizione pubblica di Microsoft, che dichiarava che Windows 8 non avrebbe impedito l'installazione di altri sistemi operativi. Con questo inganno Microsoft ha dimostrato che di loro non ci si può fidare. Mentre noi stiamo barcamenandoci con le loro direttive, dobbiamo tenere ben presente che potrebbero benissimo cambiare idea piu' avanti ed espandere le restrizioni proprie degli ARM ad altri tipi di hardware.

La miglior strada per uscire da questo (a parte l'avere tutti i computer con software libero preinstallato) e' di far si' che i sistemi operativi liberi siano anch'essi installabili per default su ogni computer senza dover disattivare il Secure Boot. Nelle ultime settimane abbiamo visto due delle maggiori distribuzioni di GNU/Linux, **Fedora** ed **Ubuntu**, tracciare due differenti percorsi nel tentativo di raggiungere questo obbiettivo.

L'approccio di Fedora

L'approccio ufficiale scelto da Fedora per il rilascio della sua distribuzione sarebbe quello di partecipare ad un programma di sviluppo Microsoft-Verisign in modo da ottenere una chiave che possa essere usata per certificare un bootloader “*cuneo*”. Questo a sua volta caricherebbe GRUB 2, il ben noto programma di bootstrap GPLv3, che a sua volta caricherà il kernel del sistema, in questo caso Linux. Essendo la chiave di Fedora “garantita” da Microsoft, verrebbe riconosciuta dal firmware della maggioranza dei computer, desktop o laptop, in giro per il mondo.

Fedora inoltre suggerisce che questo approccio venga adottato anche dalle distribuzioni derivate dalla versione ufficiale rilasciata da Fedora, o da qualsiasi altro produttore di sistemi Operativi Open Source. Ognuno potrebbe pagare 99$ ed ottenere la propria chiave garantita da Microsoft con cui firmare il software che vuole eseguire e/o distribuire.

Fedora non “impone” agli utilizzatori di agganciarsi al programma di sviluppo Microsoft. Essi possono produrre e utilizzare delle loro chiavi personali a costo di un maggior lavoro. Il programma Microsoft e' la strada scelta da loro per le distribuzioni Fedora ufficiali, ma essi forniranno anche degli strumenti software e supporto per quelli che vorranno utilizzare le chiavi generate in proprio.

C'è molto da apprezzare nel pensiero di Fedora, come esposto da Matthew Garrett. La loro procedura dimostra attenzione alla libertà degli utenti; è chiaro che il team Fedora si è immaginato una soluzione che potrebbe funzionare non solo per la loro specifica distribuzione GNU/Linux, ma per quante altre distribuzioni ed utenti si possano immaginare. La loro elaborazione ha tenuto conto della desiderabilità del fornire agli utenti la possibilità di firmare ed eseguire il software da loro modificato senza essere trattati da cittadini di seconda classe. Non sorprende, che con questi obbiettivi siano usciti con una proposta che così com'è stata descritta sia rispettosa e compatibile con la GPLv3.

Sfortunatamente, se da un lato e' accettabile per la licenza del GRUB 2 ed ogni altro software GPLv3 compatibile, dall'altro vediamo due seri problemi legati all'approccio Microsoft:

1. Gli utilizzatori che vogliono che il loro software venga eseguito in un ambiente Secure Boot devono fidarsi di Microsoft per fare il boot della versione ufficiale di Fedora. Il formato di firma del Secure Boot attualmente permette una sola firma in un eseguibile – pertanto il bootloader *cuneo* di Fedora potrà essere firmato solo dalla chiave garantita da Microsoft. Se un utente rimuove dal firmware la chiave di Microsoft, la distribuzione ufficiale di Fedora non sarà più utilizzabile con il Secure Boot attivo
2. Noi respingiamo e non supportiamo la raccomandazione che altri si associno al programma di sviluppo Microsoft. A parte I 99$, che potrebbero essere un ostacolo per molti in giro per il mondo, il procedimento per associarsi al programma e' discutibile. Una lista, peraltro incompleta, dei problemi che ciò comporta include:
    - termini restrittivi in ordine di una mezza dozzina di contratti che debbono essere firmati.
    - un forzato consenso a “*ricevere pubblicati mirata ed email periodiche da parte di Microsoft*”
    - la necessita' di fornire prova autenticata del possesso di documento di identità governativo e carta di credito.

Queste sono condizioni inaccettabili per poter modificare ed utilizzare il proprio sistema operativo. Per il momento dovremmo invece sperare nell'approccio di Fedora al supporto di distribuzioni non ufficiali – provvedere strumenti e software per chi vorrà installare ed utilizzare le proprie chiavi.

Il software firmato con proprie chiavi ha il difetto di non funzionare senza ulteriori interventi nella maggioranza dei computer cosi' come verranno forniti. Ci rendiamo conto che questo sia un problema e quindi oltre ad insistere e contribuire alla documentazione sul rendere il processo necessario semplice da seguire, ci sforzeremo di risolvere questo problema con l'azione politica contro fabbricanti di hardware e compagnie di software proprietario che impediscano l'utilizzo del software libero. Incoraggiare I distributori di software libero e gli utenti a dar fiducia a Microsoft come precondizione per poter esercitare le proprie libertà semplicemente non e' una soluzione accettabile.

L'approccio Ubuntu

Anche Ubuntu ha annunciato un progetto che e' ulteriormente specificato in un'email alla mailing-list degli sviluppatori Ubuntu. La loro linea d'azione riguarda il software distribuito secondo tre differenti canali:

1. Le macchine vendute come “Certificata Ubuntu”, preinstallate con Ubuntu, avranno inserita nel loro firmware una chiave specifica per Ubuntu generata da Canonical.. Inoltre dovranno avere installata, stanti le procedure di certificazione, la chiave di Microsoft.
2. I CD di Ubuntu, distribuiti separatamente dall'hardware, dipenderanno dalla presenza della chiave Microsoft per il boot, qualora sia attivo il Secure Boot.
3. Immagini del bootloader di Ubuntu distribuite online dal repository ufficale Ubuntu saranno firmate dalla chiave proprietaria di Ubuntu.

Nei primi due casi, a causa dell'obbligo di avere la chiave Microsoft presente, il loro metodo presenta gli stessi inconvenienti di quello ufficiale di Fedora. Gli utenti debbono dar fiducia a Microsoft per poter caricare Ubuntu ufficiale. La loro procedura di certificazione peggiora la situazione perché significa che nessuno può vendere macchine certificate Ubuntu senza necessariamente dare fiducia anche a Microsoft.

Come per Fedora, in ogni sistema con Secure Boot implementato correttamente gli utenti Ubuntu saranno in grado di aggiungere le loro chiavi o quella di Ubuntu.

La nostra preoccupazione principale con l'approccio Ubuntu e' che, a causa del fatto che temono di non rientrare più nella GPLv3, essi vogliono sostituire nei sistemi con Secure Boot il GRUB 2 con un bootloader con licenza diversa e sprovvista delle protezioni tipiche della GPLv3 a garanzia della libertà degli utenti. La loro preoccupazione dichiarata e' che qualcuno possa fornire un Computer con il Restricted Boot (che gli utenti non possono disattivare) certificato Ubuntu. Quindi per essere aderente alla GPLv3, Ubuntu teme che potrebbe essere costretta a divulgare le sua chiavi private in modo che gli utilizzatori siano in grado di installare software modificato anche sui sistemi con limitazioni.

Questo timore e' infondato e dovuto ad una cattiva interpretazione della GPLv3. Noi non siamo stati capaci di immaginare alcuno scenario dove Ubuntu avrebbe potuto essere costretta a divulgare una propria chiave privata di firma a causa di un fabbricante o distributore di computer che fornisca Ubuntu su una macchina con Restricted Boot. In una simile situazione sarebbero il fabbricante e/o il distributore, e non Canonical o Ubuntu, ad essere tenuti a fornire agli utilizzatori le informazioni necessarie per permettere loro di eseguire versioni modificate di software.

Non solo, cercare di neutralizzare il pericolo del Restricted Boot indebolendo la licenza del bootloader va nel senso opposto. Con una licenza più permissiva le aziende avranno una specie di permesso aggiuntivo per ostacolare la possibilità degli utilizzatori di eseguire software modificato. Invece di lavorare per assicurare che questa situazione non possa avverarsi , per esempio forzando implementazioni corrette del Secure Boot che essi dicono di “supportare attivamente nelle loro linee guida del firmware”, Ubuntu ha scelto una strada che *permettere esplicitamente* il Restricted Boot.

Nessun rappresentante di Canonical ha consultato la FSF su questi problemi prima dell'annuncio della loro policy. Ed e' un peccato perché la FSF, oltre ad essere l'interprete principale della licenza in oggetto, e' anche il detentore della licenza del GRUB 2, il principale pezzo di di software coperto da GPLv3 in discussione.

Non e' comunque troppo tardi per cambiare. Noi esortiamo Ubuntu e Canonical a ribaltare questa decisione, ed offriamo tutto il nostro aiuto per appianare ogni dubbio sulle licenze. Inoltre

speriamo che Ubuntu, come Fedora, supporti attivamente gli utilizzatori nel generare ed utilizzare le loro chiavi di firma personali per eseguire e distribuire ogni versione del software, e non imporre l'installazione di una chiave di Canonical per poter godere dei benefici completi del loro sistema operativo.

Cosa sta facendo la FSF per contribuire alla soluzione del problema?

Secure Boot genera molti problemi a proposito della protezione della libertà degli utilizzatori e della promozione degli ideali del software libero e del suo utilizzo. La loro soluzione richiede un approccio da vari lati. La verifica delle soluzioni proposte da popolari distribuzioni GNU/Linux ne e' un aspetto, ma questo non ci esime dal prendere misure pro-attive di nostra iniziativa:

- Continueremo a coagulare pubblico consenso attorno alla nostra opposizione al Restricted Boot. Oltre 30.000 persone e 25 organizzazioni hanno aderito alla nostra dichiarazione che chiedere di non acquistare alcun computer su cui non si sia in grado di installare un sistema operativo libero, e di pregare gli altri di non farlo. Abbiamo avuto molto piacere nella scorsa settimana di aggiungere Debian GNU/Linux come organizzazione che supporta ufficialmente questa dichiarazione. Subito dopo si sono aggiunte Trisquel e gNewSense. Quando sarà necessario fare ulteriori azioni per la nostra libertà, perché verranno impiegati a tappeto Secure Boot e Restricted Boot, noi avremo voce in capitolo grazie a questa base di appoggio. Se non avete ancora firmato **fatelo ora**.
- Combatteremo il tentativo di Microsoft di imporre il Restricted Boot sulle architetture ARM, come smartphones e tablets. Come in ogni altro computer gli utilizzatori devono essere in grado di installare sistemi operativi liberi su questi dispositivi. Sorveglieremo il comportamento di Microsoft per essere sicuri che non ingannino nuovamente il pubblico espandendo queste descrizioni ad altre architetture.
- Noi collaboreremo con (e se necessario eserciteremo pressioni su) fabbricanti e distributori di hardware per rendere le istruzioni di interazione con il Secure Boot estremamente chiare, cosi' che gli utilizzatori siano in grado di disattivarlo e/o modificarne le chiavi approvate con la minor difficoltà possibile e nessun orientamento preventivo. Ci adopereremo inoltre per essere certi che gli utenti possano cambiare *tutto* il software installato sulle loro macchine, firmware di boot compreso.
- Offriremo le nostre risorse di consulenza sulle licenze e sull'aderenza ad ogni sviluppatore di software libero per aiutarli ad assicurarsi di essere aderenti alla GPL ed alle altre licenze quando implementano il Secure Boot. Verificheremo le distribuzioni firmate di software GPLv3 per assicurarci che rispettino le necessarie libertà degli utilizzatori, incluso il provvedere istruzioni e materiali per l'installazione.
- Abbiamo anche iniziato ad esplorare modi in cui la FSF possa lavorare con i costruttori a vantaggio dell'intera comunità del software libero, per far sì che i sistemi operativi liberi siano installabili con le impostazioni di default del Secure Boot.
- Continueremo a collaborare con aziende come Lemote, Freedom Included, ZaReason, ThinkPenguin, Los Alamos Computers, Garlach44 ed Ina Tux per rendere disponibili computers con *preinstallate* distribuzioni GNU/Linux completamente libere
- Continueremo a collaborare a fornire l'informazione su quali computers e componenti siano meglio compatibili con il software libero, oltre a far conoscere quali macchine abbiano il

Restricted Boot. La maggior parte di queste informazioni si trovano su: http://h-node.org

Conclusioni e raccomandazioni

Quello che abbiamo sin qui illustrato e' la nostra posizione basata sui dettagli pubblicati da tutte le parti fin qui coinvolte, continueremo a verificare la situazione man mano che verranno implementati questi piani, o verranno apportate modifiche.

La nostra attenzione e' concentrata sulla valutazione su ciò che viene proposto come soluzione ai problemi sollevati dal Secure Boot. sulla base di quanto proteggerà la libertà degli utilizzatori, per raccomandare le migliori in tal senso e per impedire tentativi di cambiare il Secure Boot in Restricted Boot.

Le migliori soluzioni attualmente disponibili per le distribuzioni di sistemi operativi sono:

1. Supportare completamente le chiavi generate dagli utenti, anche fornendo strumenti e documentazione dettagliata per il bootstrap e l'installazione sia di versioni ufficiali che modificate della distribuzione usando questo metodo
2. Utilizzare un bootloader GPLv3 per aiutare a proteggere gli utilizzatori dai pericoli del Restricted Boot
3. Evitare di richiedere, o anche solo incoraggiare, gli utilizzatori a dar fiducia a Microsoft o altra compagnia che produca software proprietario
4. associarsi alla FSF ed al più vasto movimento per il software libero nel fare pressione sui distributori di computer per facilitare la semplice ed indipendente installazione di sistemi operativi liberi su ogni computer

Noi faremo tutto il possibile per aiutare le distribuzioni di sistemi operativi liberi a seguire questa strada, e lavoreremo a livello politico per ridurre le difficoltà pratiche che l'adesione a questi principi possa porre alla conveniente installazione di software libero. La FSF vuole con forza che ognuno sia in grado di installare facilmente un sistema operativo libero – la nostra meta piu' ambiziosa e' che tutti lo facciano, e l'esperienza di provare il software libero e' un ottimo modo per comunicare l'importanza degli ideali del software libero a nuove persone. Ma non possiamo ammettere che per brevità o semplicità utilizzatori finali diano fiducia ad entità il cui obbiettivo e' la scomparsa del software libero. Se questo e' il compromesso necessario meglio disattivare il Secure Boot.