» The Linux Foundation

オープン プラットフォームにおける UEFI Secure Boot への対応

James Bottomley, CTO, Server Virtualization at Parallels
& Linux Foundation Technical Advisory Board Chair

Jonathan Corbet, Editor at LWN.net
& Linux Foundation Technical Advisory Board Member

2011 年 10 月

The Linux Foundation
http://www.linuxfoundation.org

オープン プラットフォームにおける UEFI Secure Boot への対応

“Secure boot (セキュア ブート)” は、最近の UEFI (Unified EFI) 仕様で規格化された技術です。secure boot は、ハードウェアによって検証された、マルウェアのない オペレーティング システム (OS) ブートストラップを可能とし、システム実装時のセキュリティを向上させます。secure boot をハードウェアに正しく実装できれば、Linux などのオープン オペレーティング システムも、これを有効に利用することができます。このホワイト ペーパーでは、オープン システムにおいて、システムのオーナーの権利に悪影響を与えず、しかもプロプライエタリ ソフトウェア ベンダーの要件を満たしながら、UEFI secure boot の仕様を実装する方法について説明します。

推奨事項をまとめると、以下のようになります。

- UEFI secure boot が有効なすべてのプラットフォームを setup モードで出荷し、オーナーがどのプラットフォーム鍵 (PK) をインストールするか制御できるようにする。また、オーナーが必要に応じて、後からいつでもシステムを setup モードに戻すことができるようにする。
- 最初の OS ブートストラップでは、setup モードでプラットフォームを検出し、各自の鍵交換鍵 (key-exchange key: KEK) をインストールし、さらにプラットフォーム鍵をインストールして、secure boot を有効にする。
- セキュア モードで実行中のシステムにプラットフォーム オーナーが新しい鍵交換鍵を追加してデュアル ブート システムを設定できるように、ファームウェアベースのメカニズムを確立する。
- リムーバブル メディアによる簡易ブートのためのファームウェアベースのメカニズムを用意する。
- OS 中立かつベンダー中立な認証局が将来的に設置され、サードパーティのハードウェア/ソフトウェア ベンダー向けの鍵交換鍵を発行する。

以上を推奨する理由について、これから説明します。

UEFI Secure Boot のしくみ

UEFI 仕様 (バージョン 2.3.1) は少々難解で、2,139 ページもあります。しかし、secure boot の機能に関するセクションは、包括的でわかりやすく、オープン プラットフォームで利用する際にも大変参考になります。UEFI による設計については、この仕様書のセクション 27.5 で簡潔に説明されていますが、ここで、その two-key システムについて簡単に説明しましょう。

UEFI 仕様 (セクション 27.5) は、プラットフォーム鍵 (PK) と一組の鍵交換鍵 (KEKs) を定義しており、前者はプラットフォーム オーナー (ハードウェアの持ち主) が管理するように設計され、後者は OEM と OS ベンダーが管理するように設計されています。この「管理する (control)」とは、これらの鍵が公開鍵/秘密鍵のペアであり、秘密鍵を知っている人物はその鍵の管理者だということです。しかしその鍵をインストールするには公開鍵さえあればよいため、鍵交換鍵は、それらを管理していない人物でもインストールすることができます。

このように分離することは極めて重要です。なぜなら、プラットフォーム オーナーは、鍵交換鍵の管理者の権能を脅かすことなく、信頼できる鍵を決定し、確実に OS を安全に起動できるからです。

オープンシステムにおける動作

オープン システムで secure boot を問題なく機能させるには、すべての UEFI secure boot プラットフォームが、プラットフォーム鍵のインストールされていない setup モードで出荷される必要があります。そうすれば、プラットフォーム オーナーは、各自のプラットフォーム鍵をインストールするか、あるいは OS のインストール プロセスに任せることで、プラットフォームを安全に管理することができます。また、オーナーがその PC を

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
info@linuxfoundation.org

再販したい時や、プラットフォーム鍵を管理できなくなった時に備えて、プラットフォームを setup モードに戻すメカニズムも必要です。これは現行の Trusted Platform Module（TPM）に良く似たメカニズムです。

プラットフォームは、ファームウェアとドライバーの認証に必要なすべての鍵交換鍵が署名データベースに入れられた状態で出荷されるべきです (セクション 27.6.1)。この署名データベースは、プラットフォームが setup モードにあるときは非アクティブですが、secure boot がアクティベートされると、ファームウェアとすべての拡張ドライバー コンポーネントが適切に認証を行い、OS の起動を進めます (ファームウェアのエレメントが拡張カードに存在すると、鍵交換鍵の一式を取得するのが問題ですが、これについては後ほど触れます)。

secure boot を利用する OS は、まず、(システムがプリインストールされたものでも、外部メディアからインストールされたものでも) そのプラットフォームが setup モードであることを検知します。OS はその後、各 OS 固有のコードに対応した鍵交換鍵をインストールし、さらにプラットフォーム鍵をインストールすることで、プラットフォームを secure モードに切り替えることができます。オープン システムは、初回のブート時に新しいプラットフォーム鍵を生成したうえで、その公開コンポーネントをインストールし、秘密コンポーネントを外部メディアに保存します。

セキュアな OS ブート ローダーは、有効な署名を伴ってインストールされると、OS を認証および実行するための処理を開始します。これらも、署名を用いた同様の方法で実行されます。

この時点では、OS をブートするために使用される鍵交換鍵は、UEFI 仕様にあるように、その OS の作者によって管理されています。しかしながら、プラットフォームのオーナーには、プラットフォームを変更して、それをブートさせる権利があります。この権利は、プラットフォーム鍵の管理者であるプラットフォーム オーナーが、変更された OS 用の新しい鍵交換鍵を生成し、署名データベースにインストールすることで有効になります。プラットフォーム鍵の管理者であるプラットフォーム オーナーは、オリジナルの OS の鍵交換鍵を削除することもでき、そうすることで、そのプラットフォームが、変更された OS だけをブートするようにもできます。プラットフォーム オーナーが、任意に修正された OS を自身で作成した鍵交換鍵でブートできるようにすることは、OSI (Open Source Initiative) が承認したどのオープンソース ライセンスにも違反しません。

デュアル ブート

前述の方法は、setup モードでプラットフォームが出荷された場合の最初のブートに関するものです。プラットフォーム鍵がインストールされると、プラットフォームはユーザー モードで動作し、そこでは、署名データベースに署名を持つ (つまり、署名データベース内の鍵交換鍵で署名された) セキュアな OS だけがブートされます。プラットフォーム オーナーが新たな OS を追加する場合、その OS にはこのような属性が備わっていないため、システムをブートする前に鍵交換鍵を認証およびインストールするメカニズムが必要です。

最も安全な方法は、署名データベースを管理するための EFI ツールセットを用意することです。これによって、ユーザーがインストール メディアを認証し、そこから OS ベンダーの鍵交換鍵を取り出し、署名データベースにインストールすることが可能になります。未承認のメディアが挿入された後、すぐにこのツールが UEFI システムによってアクティベートされれば、プラットフォーム オーナーが、OS のインストールとブート用の鍵を承認するかどうかを決定できます。

すべての OS ベンダーが信頼の連鎖に加わり、有効なルート署名が最初から UEFI 署名データベースに入るようになれば、このような初期ブートの問題は避けることができます(「信頼モデルの確立」の章を参照)。

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
info@linuxfoundation.org

THE LINUX FOUNDATION

クローズド オペレーティング システムのブート

当然ですが、クローズド OS もオープン OS と全く同じようにブートし、かつセキュアな機能を保持することができます。なぜなら、ここにおけるセキュリティは、OS ベンダーによって管理された鍵交換鍵の制御によって保証されているからです。しかし Steven Sinofsky 氏は、"Protecting the pre-OS environment with UEFI (UEFI で OS 起動前の環境を保護する)" というブログ (下記 URL) で、次のような表現をしています。

http://blogs.msdn.com/b/b8/archive/2011/09/22/protecting-the-pre-os-environment-with-uefi.aspx

「一般的なプラットフォーム オーナーは、Microsoft やプラットフォームの OEM サプライヤーに、プラットフォーム鍵の管理 (および署名データベースの管理) を任せたいでしょう。」

この方法は、プラットフォーム オーナーがプラットフォーム鍵の管理者であるという UEFI の勧告に反し、Windows OS だけをそのプラットフォームでブート可能な OS にします。とはいえ、ユーザーが任意の上であれば問題はありません。これは、インストール時に新しいプラットフォーム鍵を生成する代わりに、Microsoft OEM の提供するイグニッション システムが OEM プラットフォーム鍵をインストールできるようにします。プラットフォーム鍵の公開部分だけがイグニッション システムによって運ばれ、プラットフォームのロックダウンを完成させるため、シンプルかつ安全な方法です。この方法は、最新ドラフト バージョンの Windows 8 UEFI ロゴ要件を完全に満たします。

プラットフォーム オーナーは、プラットフォームを安全に setup モードにリセットできることが保証されているため、彼らが望めば、いつでも制御権を取り戻すことができます。

信頼モデル (Trust Model) の確立

UEFI モデルの不完全な欠点の 1 つ (認証システムを運用することの複雑さのため、敢えて欠落しているもの) は、現行案に確実な信頼の起点 (root of trust) がないことです。これにより、明らかな欠点が生まれます。すなわち、複数のサード パーティのカードを搭載しているデスクトップ システムの場合、各カードの EFI ドライバーが、署名データベースにそれぞれ専用の鍵交換鍵を置かなければならない、ということです。オープン モデルでは、プラットフォーム オーナーがプラットフォーム鍵を管理しているため、PCI カードが追加されたり、変更されたりするたびに、新しい鍵交換鍵を認証して有効にする、という煩わしい処理が生じます。さらに、クローズド モデルでは、OEM がプラットフォーム鍵を管理しているため、OEM による更新が提供されなければ不可能です。

この問題を解決するために、UEFI は、セクション 27.6.1 において、署名データベースに X509 証明書を置くことを許可しています。X509 信頼モデルは、Web サーバーとブラウザのセキュリティ証明書のベースとなるもので、署名と署名鍵について、その信頼の起点まで到達できます。このようなしくみがあれば、1 つまたは複数の認証局の鍵を UEFI 署名データベースに置き、指定された認証局が鍵交換鍵 (および鍵交換鍵の生成を可能にする署名鍵) をサードパーティに発行し、サードパーティが始めの認証局の信頼の起点を再検証する、ということが可能です。UEFI 仕様 (セクション 27.7.1) では、本来のユーザーが鍵交換鍵を制御できなくなった場合には、鍵のリボーク (取り消し) を行うことを許可しており、十分に機能する認証局の運用には不可欠なしくみです。

このような背景から、すべての関連組織が認証局を設置し、既定で認証局の鍵を UEFI ファームウェア テーブルに置いておくよう提案します。認証局は、署名された鍵交換鍵を UEFI デバイス ベンダー (UEFI ドライバーのため) 、UEFI OEM プラットフォーム ベンダー (ファームウェア イメージのため)、および OS ベンダー (OS を安全にブートするため) に渡す責任を持ちます。このような認証局の運用は、プラットフォームにも OS にも中立で

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
info@linuxfoundation.org

なければならず、信頼とセキュリティの標準を順守する必要があります (おそらくは、さまざまな組織の代表による管理役員会を持つことによって)。しかし、こうすることによって、ドライバーや OS の検証問題の多くは解決するでしょう。なぜなら、認証局の起点の鍵にまで到達できる、リボークされていない鍵交換鍵で署名された製品は、すべてセキュア ブート可能であることが UEFI ファームウェアにより信頼されるからです。

外部リムーバル メディアからのブート

プリインストールされていないすべての OS (事実上すべてのオープン OS) は、USB キー、DVD、CD などの外部メディアからインストールされる (またはライブ CD で試される) はずです。もしも前述のような信頼モデルが確立されれば、こうしたメディアからの secure boot の問題は解決します。なぜなら、オープン OS ベンダーが、信頼の起点に到達できる鍵を使用して、メディアに署名しているからです。しかし、信頼モデルが存在しない場合は、外部メディア イメージの鍵交換鍵や署名が署名データベースに存在しないときに、外部メディアから簡単にブートできる方法が必要です。したがって、システムがユーザー モードでかつ secure boot が有効な状態では、現行のシンプルなハードウェア ベースのユーザー権限チェックを行って、外部の非認証メディアをブートするのがよいでしょう。

まとめ

UEFI secure boot 機能は、ブートストラップ処理のセキュリティを高めるために、プロプライエタリな OS にもオープン OS にも簡単に利用できるよう設計されています。「secure boot は、市場からオープン システムを排除するために使用されかねない」という懸念の声も聞かれますが、前述のように、そのような心配はありません。ベンダーは、setup モードでシステムを出荷し、かつファームウェアに新しい鍵交換鍵を追加する手段を提供すれば、そのシステムは、オープン OS をフルサポートしつつ、Windows 8 ロゴ要件を順守できます。鍵交換鍵を作成するために独立した認証局を設立することは、相互運用を円滑にするためであり、それらのプラットフォームがオープン システムをサポートするために必須なわけではありません。

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
info@linuxfoundation.org

The Linux Foundation は、
Linux の普及促進、保護、ならびに発展に取り組み、
Linux/OSS がクローズドなプラットフォームに対抗するのに必要とされる
統合されたリソースとサービスを提供します。

The Linux Foundation、オープン コンプライアンス プログラム
およびその他の活動については、
http://www.linuxfoundation.jp/ を参照してください。