企業のサーバーファームウェアを保護する新しいアプローチ

ラティスセミコンダクター　ホワイトペーパー

2018年10月

FPGAベースのRoof of Trustデバイスを活用して、新しいNIST SP 800 193仕様に基づくハードウェアにプラットフォームファームウェアレジリエンス（PRF）を実装することで、サーバーファームウェアを新たなレベルでサイバー攻撃から保護することが可能になります。新しいラティスのPRF開発ツールキットはFPGAベースのPFRソリューションの実装を簡素化します。

もっと詳しく:

www.latticesemi.com/PFR

お問い合わせはこちら:

www.latticesemi.com/contact
www.latticesemi.com/buy

所在地:

Lattice Semiconductor
111 5th Ave., Suite 700
Portland, Oregon 97204
United States

Phone: 1 (503) 268-8000

概要

殆どの企業向けサーバーはファームウェア（起動後にすぐにコンポーネントブートを処理するソフトウェア）を保存するための独自の不揮発性SPI Flashメモリキャッシュを持った複数の処理コンポーネントが含まれています。Flashメモリの使用は、フィールド内のアップグレードやバグ修正をサポートするのに便利である一方、悪質な攻撃に対しては脆弱です。ファームウェアへの不正アクセスによって、ハッカーは悪質なコードをFlashメモリに密かにインストールし、標準的なシステムレベルの検出方法から半永久的に逃れています。

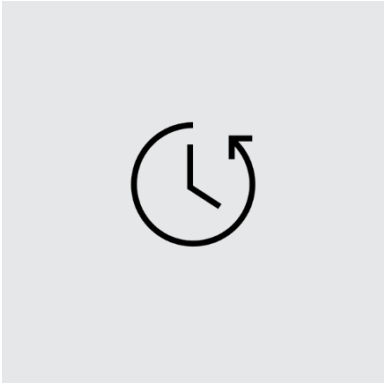
対策として、いくつかの処理コンポーネンツはチップ上のハードウェア回路を使って不正なファームウェア改変を検出します。しかし、そのような対策をしていないボード上の他の処理コンポーネンツは依然として攻撃されやすく、サーバー全体が危険にさらされています。この課題に取り組むため、アメリカ国立標準技術研究所（NIST）は2018年にNIST SP 800 193仕様を発表し、プラットフォームファームウェアレジリエンス（PFR）として知られる一定のセキュリティ対策を定義しました。PFRによって、サーバー内の全てのファームウェアに対する攻撃が包括的に防止されます。この仕様は3つの基本原則に基づいています。

保護

ファームウェアを攻撃から保護

検出

SPI flashに保存された
不正なファームウェアを検出



復元

不正なファームウェア
のインストールから復元

PFR機能は外部のハードウェア（シリコン）のRoof of Trust （RoT）デバイスに依存しています。FPGAベースのRoTデバイスを使ってPFRソリューションを実装する方が、MCUベースよりも安全、スケーラブルで、堅牢です。ラティスの新しいPFR開発ツールキットはサーバーOEMが最新で強力なセキュリティの大躍進を迅速に活用するための道を開きます。システム設計者やシステムインテグレーターはより簡単にFPGAベースのRoTデバイスを設計・実装・維持でき、セキュリティの深い専門知識がなくてもPFR準拠が可能になります。

目次

サイバー攻撃に脆弱なサーバーファームウェア

サーバー攻撃による損害は2021年までに6兆USドルに上ると予想されています。サーバー攻撃の攻撃元は以下のように、セキュリティ対策を回避する新しい方法を絶えず探しています。

- サーバーに保存してある独自データ（クレジットカード番号、企業IPなど）を見る/盗む
- サーバーを通過するデータを見る/盗む
- サーバーを乗っ取り、他のターゲットへのDDoS攻撃に関与する
- 1つや複数のサーバーのハードウェアコンポーネンツを作業不能にさせ、サーバーを妨害する（“ブリック・サーバー”として知られる

新しい機能を追加したりバグを修正したりするため、オペレーティングシステムやアプリケーションは定期的にアップデートされていますが、それはサーバーに侵入しようとするハッカーにとっては好都合です。そのため、企業は自分たちのオペレーティングシステムやアプリケーションソフトウェアを保護するためにセキュリティリソースや戦略を重要視する傾向にあります。しかし、その他にもあまり知られていない、サーバーをハッキングするためのアタックベクターがあります。それは、ファームウェアです。

ファームウェアはサーバーコンポーネント（CPU、ネットワークコントローラ、RAIDオンチップソリューション等）の起動直後に最初に実行されるブート可能なコードが含まれています。コンポーネントのプロセッサはファームウェアが有効な起点であるとみなしてブートし、サーバーの設定に合わせてより高レベルな機能を段階的に検証し、ロードします。場合によっては、処理コンポーネントはファームウェアを使用して、全体の動作寿命を通して必要な機能を実行します。

ISACAが2016年に実施した調査では、回答者の半数においてハードウェアのセキュリティが企業における優先事項と回答し、少なくとも1件以上企業のシステムファームウェアがマルウェアに感染した事例があり、更にその17%は重大な影響を及ぼしたと報告されています。

ファームウェアのセキュリティ概要

サーバーファームウェアはサプライチェーン上の様々な段階でハッキングされる恐れがあります：

- OEM中：製造中に悪質な動作で感染されたファームウェアをインストールする
- システムインテグレータ：顧客の要件に合うようにサーバーを構成する際に不正なファームウェアがインストールされる
- 顧客に輸送中：サーバーのパッケージが開けられ、ケーブルを通して不正なファームウェアをダウンロードすることで、ハッカーは悪質なコードをコンポーネントのSPIメモリにダウンロードする
- 現場で起動中：ハッカーは自動化ファームウェアのアップデートを傷つけ、正当なアップデートを偽のファームウェアで置き換えて既存の保護システムを通過

現在、通常のサーバーメインボードは少なくとも2つの標準ファームウェアを使用しています。ユニファイド・エクステンシブル・ファームウェア・インタフェース（UEFI）とベースボードマネジメントコントローラ（BMC）で、これらのインターフェースはある程度のファームウェア保護を提供しますが、限られています。

ユニファイド・エクステンシブル・ファームウェア・インタフェース（UEFI）

UEFI（以前はBIOSとして知られていた）はサーバーのファームウェアにオペレーティングシステムにサーバーのファームウェアをロードするソフトウェアのプログラムです。製造中にインストールされ、UEFIは、どのハードウェアコンポーネンツをサーバーが持っているかを確認し、コンポーネンツを起動させてオペレーティングシステムへと渡します。この標準はセキュアブートと呼ばれるプロセスを通して、不正なファームウェアを検出します。これは、不正なファームウェアが検出された場合にハードウェアコンポーネントをブーティングから守るセキュリティ機能です。しかし、セキュアブートの実装やサポートはコンポーネントやベンダー間で異なるため、コンポーネントのセキュリティ内にハッカーが悪用する隙があります。もし、違法なファームウェアがセキュアブートを通り抜けたり、セキュアブートのプロセス内にに入ったとしたら、UEFIはコンポーネンツのファームウェアを正規のバージョンに復元し、機能を継続することはできません。

ベースボードマネージメントコントローラ(BMC)

BMCはマザーボード上にある専門のマイクロコントローラーであり、センサーを使用したり独立した接続でシステムアドミニストレーターと通信するコンピューターやネットワークサーバー、そしてその他のハードウェアデバイスの物理的状態を監視する役割を果たしています。多くのBMCは自身のファームウェアインストールを監視し、それらが合法的であるかどうかを検証します。しかしながら、他のサーバーコンポーネントに同じのことはできません。BMCはまた、悪質なコードがボード上のファームウェアを攻撃するのを防止することができません。例えば、もし悪質なコードがコンポーネントのSPIメモリの使用されていない場所へインストールされたら、BMCはそれらのコードがサーバー内全てのコードストリームへの侵入を止めることはできません。

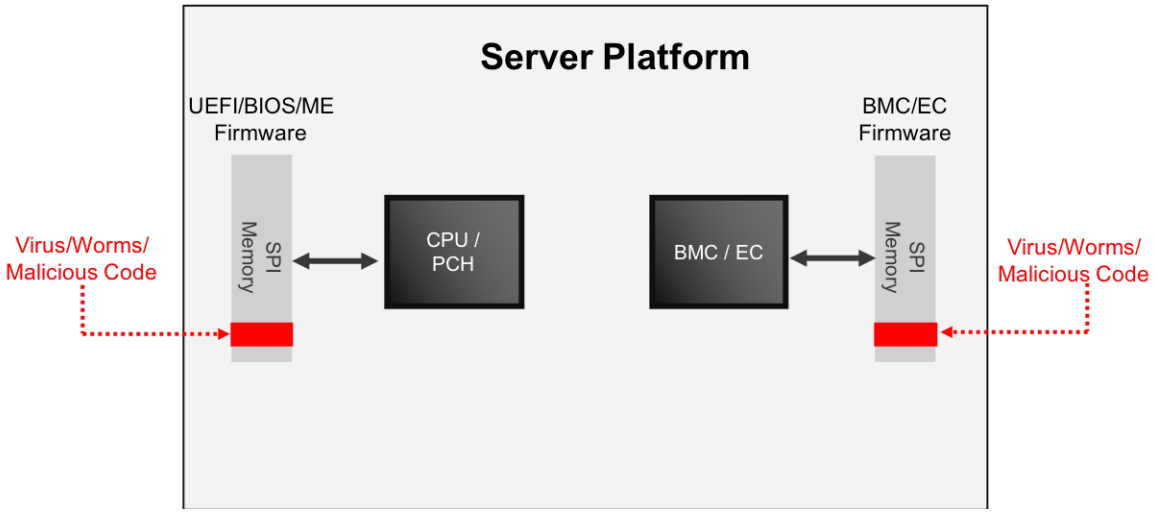


図1：ユニファイド・エクステンシブル・ファームウェア・インタフェース（UEFI）とBMCインターフェースは限定されたファームウェア保護を提供します。

プラットフォームファームウェアレジリエンス (NIST SP 800 193仕様)

現在のファームウェア基準における安全性の欠陥に対処するため、2018年5月にNISTはUEFIとBMCを含む全てのファームウェアに包括的な保護を提供するための新基準を公開しました。NIST SP 800、別名PFRは、破壊的な攻撃の可能性に対抗してプラットフォームファームウェアとデータをサポートする技術的なガイドラインや提案を提供します。こういった仕様はシステム内の全てのファームウェアを保護する統一的な方法を提供し、通常のシステム運用には侵入が不可能なように作られています。また、不正なファームウェアがインストールされようとしていると判断された場合には、いかなるコンポーネントも無効にすることができます。 PFRはまた、個々のコンポーネントがサポートするあらゆるセキュリティ上の機能から独立して動作します。

仕様書にはファームウェアを保護するための3つの基本方針の概要が書かれています：

- 保護 - SPIメモリーの保護された領域への不正な書き込みアクセスや、全て、または一部のファームウェアが削除されるのを防ぐことで、コンポーネントのファームウェアを信頼できる状態に保ちます。いくつかの場合においては、保護された領域への読み取りアクセスもブロックされます。

- 検出ーコンポーネントプロセッサが起動する前に、OEMからのファームウェアアップデートを認証する機能。もし破損した、もしくは不正なファームウェアが検出された場合、復元処理がなされます。

- 復元ーもし感染、もしくは破損したファームウェアが検出された場合、プロセッサが以前の信頼されているバージョンのファームウェア（ゴールデンイメージと呼ばれます）を起動させます。もしくは、プロセッサが信頼された処理を通して新しいファームウェアを使い、全システムの復元さえも可能にします。

PFRにおけるハードウェアベースのRoof-of-Trustの必要性

NISTの仕様書によると、安全なPFRの実行にはハードウェアであるRoTデバイスが保護や検出、そして復元をサーバー内のファームウェアに行うことが必要です。NISTに準拠したRoTデバイスは、起動前またはその他の外部コンポーネントのサポートなしで、保護や検出、そして復元を自身のファームウェアで行わなければいけません。ハードウェアRoTソリューションはまた、以下の機能を備えている必要があります。

- スケーラブルーRoTデバイスはナノ秒レベルの応答時間で外部SPI画像上の保護や検出、そして復元機能を果たさなければいけません。こういった処理は、サーバーの性能を保つために専用の処理またはI/Oポートを必要とします。

- 通り抜け不可–不正なファームウェアは、感染されたファームウェアを備えたサーバーを起動するRoTデバイスを通り抜けることができないようにするべきです。

- 自己防衛 - RoTデバイスは外部攻撃から自身を守るために、常に進化するアタック・サーフェス（不正なユーザーがアクセスできるデバイスやシステムの全ての側面）に動的に対処しなければいけません。

- 自己検出 - RoTデバイスは、通り抜けできない暗号型のハードウェアブロックを使うことで不正なファームウェアを検出できる必要があります。

- 自己復元 - RoTデバイスは、不正なファームウェアを発見したときにゴールデンファームウェアイメージに自動的に切替できなければいけません。それによってサーバーは動作し続けることが可能になります。

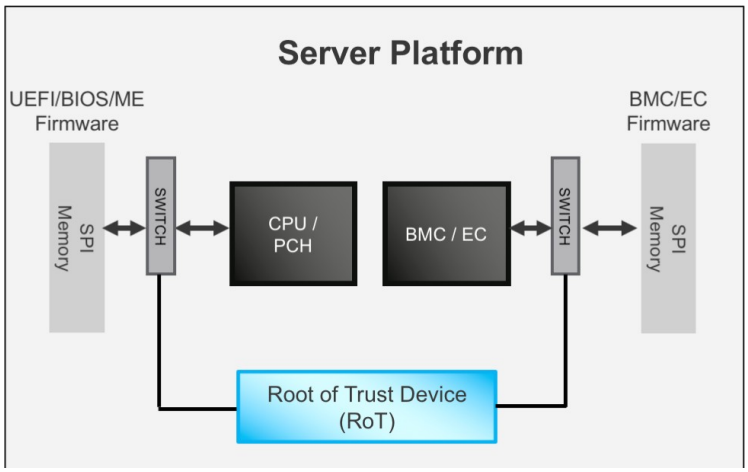


図2: NIST SP 800-193:プラットフォームウェアレジリエンス

図2では、RoTデバイスは起動して最初に全てのコンポーネントファームウェアを暗号で検証し、そして不正な変更を検出しています。もしRoTが破損を見つけた場合、信頼されたファームウェアの復元プロセスを開始します。極端な例では、ボード上の全てのファームウェアが感染された場合、RoTデバイスはBMCを復元するために、デバイスに備えられている復元ファームウェアを実装することでシステムを完全に復元することができます。BMCが信頼されたファームウェアから起動したあとは、RoTはボードレベルでの電源が入った状態の手順で行うことができます。この手順では全てのコンポーネントが作動し、最後のゴールデンファームウェアから起動され、通常のオペレーションを開始します。

SPIメモリーを今後の破損から守るため、RoTはSPIメモリーとそれに付随するプロセッサ間の全てのSPIのデータ通信を積極的に監視し、悪質なファームウェアを検出してそれがインストールされることを阻止します。

NIST準拠のPRF実装

ハードウェアベースのRoTデバイスは定義上、シリコン内に実装されなければいけません。そして、このために一番良く使われているシリコンプラットフォームはMCUもしくはFPGAです。

FPGAとMCUの特性や特徴を検証すると、FPGAプラットフォームが大規模にPFRを一番よく対応できるということが分かります

MCUを使ったRoot-of-Trust実装

図3で見られるように、MCUを使ったPFRを導入するために使われる3つのコンポーネントは以下の通りです。

- RoT MCU - RoT MCUは検出や復元、そして保護機能があります。RoT実装の中心となるコンポーネントです。
- 制御PLD - このデバイスは全てのボードレベルでの電源やリセットの機能を、ファンコントロールやSGPIO、I²Cバッファリング、シグナル統合、そしてメインボードを起動するために必要な帯域外通信などのその他のファンクションと統合します。RoT MCUは制御PLDにボードの電源を入れるよう指示します。もし極端な復元を必要とする場合、RoT MCUが制御PLDに対して、信頼された復元プロセス内で使われているボードのセクションのみに電源を入れるよう指示します。
- 保護PLD - 全てのコンポーネントプロセッサとSPIメモリデバイス間のSPIトランザクションを同時に監視することにより、ボードを包括的に保護するPRF実装を可能にします。

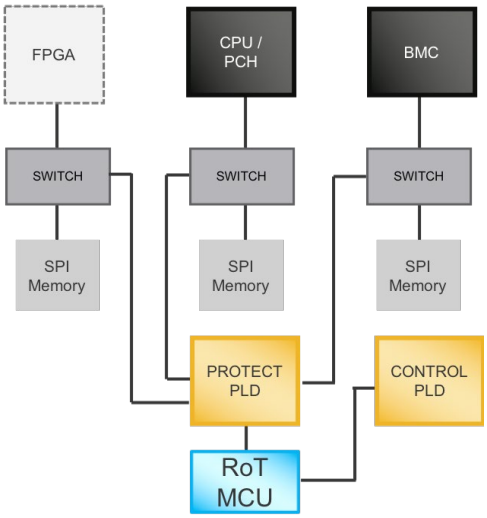


図3：MCUベースの3つのコンポーネントソリューションはPFR実装の制限があります

ファームウェア攻撃が起こった場合、MCUベースのPFRシステムは以下のような措置を講じます（実装順）

1. RoT MCUは不正なファームウェアを検出し、暗号化測定を継続して実行することで全てのSPIメモリデバイスを検証します
2. 感染したファームウェアが検出されたら、復元プロセスは保護PLDがブートソースSPIメモリを管理するか、制御または保護PLDを介してRoT MCUによって監視されることで開始されます
3. サーバーが完全なブート完了させたあと、保護PLDは、すべてのSPIトランザクションを同時に監視し、今後の攻撃をブロックし、違反が検出されたときにはRoT MCUに通知します。

PRRに対するMCUベースのアプローチには制限があります。例えば、図3に示す回路で使あれている制御PLDは、それ自身のファームウェアを保護することはできないので、このアーキテクチャはNIST PFR仕様に完全に準拠してるとはいえません。制御PLDのコードを変更してRoT MCUを無効にすることもできます。また、永久的にサービスを不能にする（PDoS）攻撃でこれらのPLDを消去してシステムを動作不能にし、サーバーを起動できなくする可能性があります。PLDセキュリティの隙を保護し、制御することにより、コンポーネントが輸送中またはシステム統合中はファームウェア攻撃から保護することが困難になります。 MCUベースの方法はRoT回路全体を通り抜ける攻撃を検出するために追加のシステムレベルプロセッサが必要です。

FPGAを使ったRoot-of-Trust実装

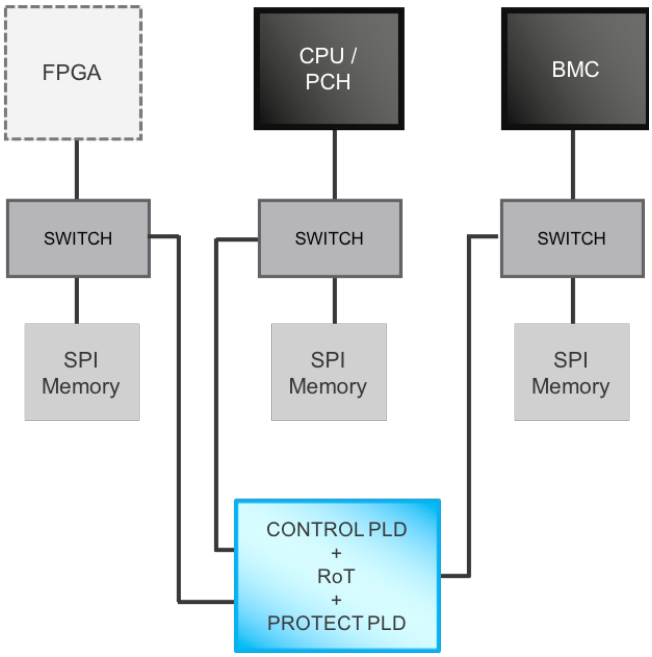


図4：このRoT FPGAはRoT MCUと制御PLDと保護PLDを堅牢でスケーラブルで通り抜け不可能なシングルチップソリューションに統合します。

RoT FPGAはMCUベースのソリューションを使った3つのコンポーネントを1つのRoTデバイスに統合し、多くの利点をもたらすPFRに準拠しています。デバイスは制御PLD機能を統合するため、RoT機能を通りぬけたり、ボードの安全な動作を改変することは不可能です。したがって、RoT FPGAはより堅牢で、MCUベースのRoTデバイスに含まれる脆弱性に悩まされることはありません。

PFR開発ツールキットはFPGAベースのRoT実装を簡素化し、市場投入までの時間を短縮

ラティスは今、FPGAベースのRoT実装を簡素化するPRF開発ツールキットを提供しています。サーバーコンポーネントOEMとFPGAベースのPFRを実装するシステムインテグレータはより早く、市場の需要に応えることができます。このラティスのツールキットは(ソフトウェアのライブラリ機能と保護PLD機能を含む)PFRを実装する3つの開発ボードとソフトウェアを含んでいます。ボード制御PLD機能は、ラティスのDiamondソフトウェアツールを使ってRoT FPGAに追加されます。ラティスPFR開発ツールキットには以下のボードがあります。

1. RoT FPGA開発ボード

2. サーバーのBMCディベロッパーをシミュレートするPythonスクリプトを起動するECP5 FPGAボードはPythonスクリプトからのコマンドを実行し、コンポーネントのSPIメモリに対する攻撃をシミュレートすることができます。PFRアダプタカードはSPIメモリ内にBMCコードを保存します。開発ボードのRoT FPGA内に実装されたPFR機能は、撃からPFRアダプタカードのファームウェアを保護します。(つまり、FPGAベースのソリューションはNIST PFRに準拠しています)

ラティスのツールキットはセキュリティの深い専門知識なしでPFRに準拠するFPGAベースのRoTデバイスを設計、実装、そして維持することを可能にします。システム設計者は、必要なPFRライブラリ機能をシステムレベルの設計に追加して、ボードの保護、検出、復元を調整することにより、サーバーハードウェア向けのPFR準拠ファームウェアを開発できます。設計者は、取得したコードをボード上のRoT FPGAにダウンロードし、Pythonスクリプトを使用して実装の堅牢性を評価することができます。

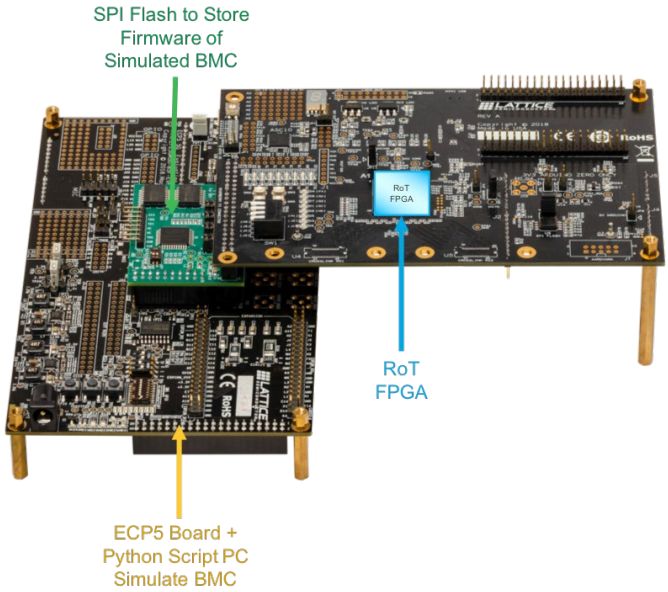


図5:ラティスのFPGA RoT開発ツールキットは3つのボードを搭載しています:RoT FPGA開発ボード、サーバーのBMCをシミュレートするECP5ボード、シミュレートされたBMCファームウェアを保存するSPI Flashボードです。

要約

デジタル領域で運用する組織は、サイバーセキュリティが重大な課題になっています。ハッカーは企業サーバーのファームウェアを標的にして、サーバー上のデータに不正アクセスをしたり、サーバーを半永久的に動作不能にすることさえします。この対策として、FPGAベースのRoTデバイス上のPFR実装は、コンポーネントのサプライチェーンのあらゆる段階での攻撃からファームウェアを保護する、堅牢でスケーラブルで完全型メソッドです。この新しいラティスのPFR開発ツールキットはサーバーセキュリティ向けにRoTデバイスの開発を加速・簡素化する方法を提供します。

[i] https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html
[ii] http://www.isaca.org/Knowledge-Center/Research/Documents/CSX-Firmware_whp_eng_1016.pdf?regnum=461390
[iii] https://whatis.techtarget.com/definition/Unified-Extensible-Firmware-Interface-UEFI
[iv] https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot
[v] https://searchnetworking.techtarget.com/definition/baseboard-management-controller
[vi] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

もっと詳しく:

www.latticesemi.com/PFR

お問い合わせはこちら:

www.latticesemi.com/contact
www.latticesemi.com/buy

所在地:

Lattice Semiconductor
111 5th Ave., Suite 700
Portland, Oregon 97204
United States

Phone: 1 (503) 268-8000

Rev. 0 WP0016