Mach-NX：Root-of-Trust システム

Bob Wheeler
主席アナリスト

2020 年 12 月

www.linleygroup.com

Mach-NX：Root-of-Trust システム

Bob Wheeler

The Linley Group 主席アナリスト

堅牢なシステム・セキュリティには多層アプローチが必要であり、セキュア・ブート・プロセスが Root-of-Trust の出発点とならなければなりません。ラティスセミコンダクターは業界リーダーとしての地位を活かし、新世代 Mach-NX ファミリの発表により、セキュア制御プラットフォームをさらに進化させました。こうした新製品は増大する脅威の一歩先を行くプラットフォーム・セキュリティを提供すると同時に、お客様の設計負担を軽減します。このホワイトペーパーはラティスセミコンダクターのスポンサーシップにより、筆者自身の意見や分析に基づいて執筆したものです。

ファームウェアから始まるセキュア・システム

脅威が増大する今日の環境において、複雑なシステムには「ゆりかごから墓場まで」のセキュリティが必要です。その第一歩となるのはセキュアなサプライチェーンの確立で、それにより、デバイスのプログラミング、システムの製造、流通、設置中にシステムのセキュリティが絶対に侵害されないようにしなければなりません。システムの運用が始まれば、脆弱性のパッチやセキュリティ・プロトコルのアップグレードのために、セキュアな OTA（Over the Air）アップデートが必要になります。最後に、システムはデータ流出防止のためにセキュアな廃棄措置を必要とします。

システム・セキュリティに重点を置いている伝統的な市場としてはデータセンタ、サービス・プロバイダ、クリティカル・インフラなどがあります。マルチテナントのパブリック・クラウド・データセンタは内部から多くの脅威が発生する可能性があり、ペリメータ・セキュリティは時代遅れになっています。その結果、データセンタのシステムにはシステム内部から発生するソフトウェア攻撃に対する保護が必要になります。攻撃のターゲットとなるのはコンピューティング・サーバ、ストレージ・システム、ネットワーク・スイッチ/ルータです。サービス・プロバイダ・ネットワークでは基地局、ブロードバンド・アクセス機器、ルータ、さまざまなゲートウェイが潜在的な攻撃ターゲットとなります。ユーザープレーン・データを暗号化した時でさえ、攻撃によってマネジメント・プレーンのセキュリティが侵害され、システム内部へのバックドアが作られることがあります。

広い視点から見ると、産業制御システムには防衛、公共施設、電力網、輸送などのクリティカル・インフラで展開されるシステムが含まれます。とりわけ国レベルでセキュリティの侵害を試みている巧妙な集団が存在する中で、各国政府はまず始めに、こうした分野で展開されているシステムのセキュリティ保護に関心を抱きました。しかし、サイバー犯罪者は資金的利益を獲得するために、次第に他の業界の同様のシステムをターゲットとするようになりました。例えば、ランサムウェア攻撃により工場が操業停止に追い込まれる可能性があります。もう１つの新たなターゲットとなっているのは、接続や自動化がますます進むと同時に、OTA ファームウェア・アップデートを受けるクルマが増えている自動車分野です。

ブートタイム・セキュリティの出発点となるのはファームウェアで、複雑なシステムの場合、マルチステージ起動プロセスを備えており、攻撃表面がさらに大きくなっています。システム・ファームウェアにはブートタイム認証と OTA アップデート暗号化/認証が必要とされます。

攻撃あるいは故障を検知した場合、システムは安定したセキュアな状態に即座に復帰しなければなりません。

こうしたシステムのいくつかが採用しているのがトラステッド・プラットフォーム・モジュール（TPM）で、暗号鍵がセキュアに保存されている場所で Root-of-Trust（RoT）を生成します。しかし、TPM の実装形態は専用ハードウェア・モジュールからファームウェア/ソフトウェア・ベース・アプローチに至るまで、多岐にわたります。研究者は実際に使用可能な手段によって秘密鍵を見つけられるという脆弱性を、独立認証を受けた実装例を含むさまざまな実装形態で発見してきました。このように、TPM でさえもすべてのシステム・ファームウェアをセキュリティの侵害から完全に保護することは不可能です。

保護、検出、復元

システム・ファームウェア保護方法の 1 つが、関連フラッシュ・メモリの読み取りと書き込みに使われるシリアル・ペリフェラル・インタフェース（SPI）信号のモニタリングです。図 1 はサウスブリッジ（あるいは PCH）とベースボード・マネジメント・コントローラ（BMC）の双方に接続したフラッシュ・メモリ付きサーバの例を示しています。SPI パスへのスイッチ・デバイスの挿入により、プログラマブル・ロジック・デバイス（PLD）はコマンドのための SPI 信号のモニタリングが可能になります。PLD は認証済み/非認証済みアクセス・テーブルに対するコマンドとアドレスを検証できます。非認証済みアクセスを検出すると、スイッチを使用してフラッシュ・デバイスへのコマンドの到達を阻止します。さらに、BMC 上で動作するマネジメント・コード向けにこうしたイベントのロギングを行います。

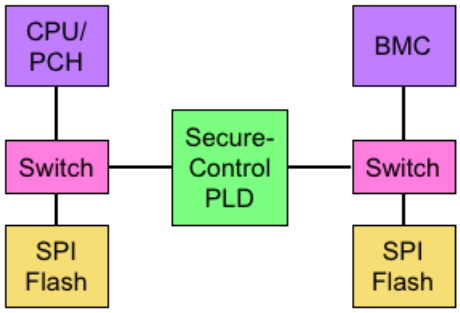

図 1：PFR システム・アーキテクチャ。セキュア制御 PLD は SPI モニタリングなどの PFR 機能の実装と同時に制御機能のハンドリングが可能

また、SPI アクセスの保護に使用される PLD はさまざまなシステム制御機能のハンドリングも可能です。その代表的な例としてシーケンシング、ファン制御、フロントパネル・ボタン、LED などの電源制御や、消費電力、熱、物理的状況などのさまざまなセンシング機能があります。こうした機能の多くは I^2C インタフェースを使用していることから、PLD は BMC 向けに信号のバッファリングとマルチプレクシングも実行できます。

米国立標準技術研究所（NIST）はネットワーク/システム・セキュリティ向けのアルゴリズム、プロトコル、フレームワークの制定と仕様作成を行っています。最近の例としては、NIST SP 800-193 のプラットフォームファームウェアレジリエンス（PFR）向けガイドラインがあります。PFR の中核となる原則は不正に対するプラットフォーム・ハードウェアの保護、不正の検出、不正から完全な状態への復元です。

BMC と CPU の起動イメージ保護のため、関連ホストのリセット状態からの離脱を可能にする前に、セキュア制御 PLD はファームウェアを認証できます。認証に含まれるのはフラッシュからのファームウェア・データの読み取り、ダイジェストの生成、フラッシュからのデジタル署名の読み取りのほか、結果検証のための適切な非対称暗号化の使用です。PFR ガイドラインはリファレンスによってのみ暗号アルゴリズムを規定していますが、レガシーのアルゴリズムが長鍵を必要とすることから、実際には今日では楕円曲線暗号（ECC）が好まれています。NIST のベースの義務となっているのは 112 ビット相当のセキュリティで、RSA 署名のために 2,048 ビット鍵を必要とします。対照的に、楕円曲線 DSA（ECDSA）は同じ暗号強度を実現するためにわずか 224 ビットの素体しか必要としません。192 ビット相当の強度のために ECDSA が 384 ビットを使用するのに対し、RSA は 7,680 ビットを必要とします。

ファームウェア保護には、認証済みアップデート・メカニズムも含まれます。PFR ガイドラインには規定されていませんが、トランスポートのために OTA アップデートの暗号化も可能です。ファームウェア・イメージ暗号化は対称アルゴリズムを使用しており、現在のさまざまな実装方法では Advanced Encryption Standard（AES）を採用しています。ベースのセキュリティには 128 ビット鍵（AES-128）が必要ですが、センシティブなアプリケーションの場合には現在、256 ビット鍵が一般的に使用されています。AES-256 の使用により、ブロック暗号化は 384 ビット ECC ハッシング（SHA-384）とメッセージ認証（HMAC-384）を上回る強度を実現します。イメージが復号化された場合には、イメージがフラッシュに書き込まれる前にデジタル署名の検証が可能です。

PFR ガイドラインには、Root-of-Trust for Detection（RTD）と呼ばれる検出機能も規定されています。こうした機能の背景にあるのは、システム・ファームウェアあるいはクリティカルなデータに対する攻撃が成功しても、RTD のセキュリティ侵害は阻止するというアイデアです。前述のように、SPI モニタリングを実装することにより、PLD は RTD として機能するだけでなく、事前定義済みフラッシュアクセス・ルールを侵害する攻撃も防止できます。起動時にはアクティブ・ファームウェア・イメージの認証により、成功した攻撃の検出が可能です。不正の検出時には、システムはできればローカルに保存したファームウェア・イメージを使用して、認証済み状態への復元が必要です。古いファームウェア・バージョンには既知の脆弱性が存在し得ることから、バックアップ・イメージはスタティックな状態が不可能なことに注意してください。

ラティスはシステム制御機能のために使用される PLD を最初に発表した後、半導体、知的財産（IP）、ソフトウェアをさらに改良し、単一デバイスに RoT、システム・ファームウェア保護機能や複数の制御機能を搭載しました。新世代の Mach-NX は実証済み MachXO3D と専用 IP、ソフトウェア、サービスの成功をベースとしています。

Mach-NX、迅速で強力な暗号化を実現

セキュア制御要件を満たすため、Mach-NX は多数の I/O とプログラマブルなハードウェア・ロジックを組み合わせています。Mach-NX のコンフィギュレーション（ビットストリーム）はオンチップ・フラッシュに保存され、2 つの暗号化イメージのマネジメントが可能です。起動時にプライマリ・ビットストリームの認証と同時に SRAM へのダウンロードが行われます。認証に失敗すると、デバイスはセカンダリ（「ゴールデン」）ビットストリームからの自動再起動が可能です。Mach-NX は汎用用途とユーザー暗号鍵の保存のために、ユーザー・フラッシュ・メモリ（UFM）も搭載しています。1,064K ビット UFM は暗号化され、デュアル・ブートがディスエーブルされると 2,669K ビットに増加します。

システム・セキュリティの重要なブロックであるセキュアエンクレーブは暗号化プロトコル、真の乱数生成器（TRNG）、デバイスごとにユニークな改変不可能 ID を実装しています。ECDSA や ECDH などの ECC プロトコルを、最大 384 ビットの素体とともに処理します。また、鍵長が最大 256 ビットの AES により、ブロック暗号化をサポートします。このブロックは公開/秘密鍵ペアの生成に TRNG を使用します。さらに、マネジメント・コンポーネント・トランスポート・プロトコル（MCTP）上でトランスポートされるセキュリティ・プロトコル/データ・モデル（SPDM）を通じて、標準認証インタフェースを提供します。

図 2 が示すように、Mach-NX はマネジメント/制御ファームウェアを駆動するハードウェア RISC-V コアを追加しています。このコンパクトな 32 ビット・マイクロコントローラは RV32I 命令セットを実行し、割り込みコントローラ、タイマ、JTAG デバッガを内蔵しています。ラティスは以前、同コアをソフト IP として提供していましたが、今回はハードウェア化により他の機能のためにプログラマブル・ロジックの容量を空けました。これにより、Mach-NX は合計 11K ロジック・セルのサポートが可能になりました。利用可能になったロジック・セルと UFM により、フィールド・アップグレードのための余地が生まれたことから、将来のセキュリティ要件にも対応できます。

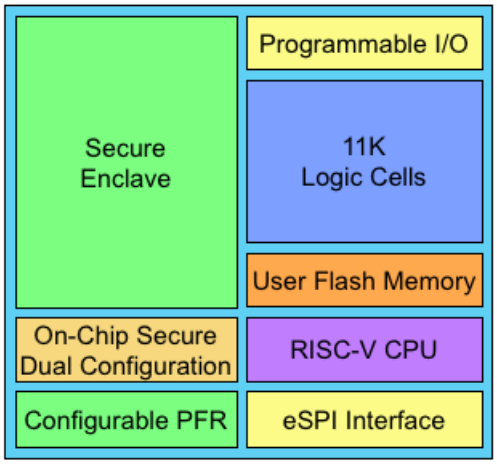

図 2：Mach-NX のブロック図。新チップはハード RISC-V CPU、ハード・セキュリティ・ブロック、フラッシュ・メモリ、プログラマブル・ロジック、多数の I/O を搭載

Mach-NX のもう 1 つの新機能が拡張 SPI（eSPI）インタフェースで、従来のロー・ピン・カウント（LPC）バスを BMC 接続に置き換えています。eSPI インタフェースは SPI 電気的/タイミング仕様に新プロトコルを重層化していることから、SPI との下位互換性を持っています。前世代製品と同様に、新チップは制御機能向けに 1.2V～3.3V の LVCMOS、LVTTL、LVDS を提供する最大 379 ピンのフレキシブルな I/O を搭載しています。すべてのパッケージ・オプションは、PCB レイアウトを容易にする 0.8mm ピッチを採用しています。

Mach-NX はラティスの新 Nexus ラインナップの製品で、サムスンの 28nm 完全空乏型シリコン・オン・インシュレータ（FD-SOI）プロセスを使用しています。FD-SOI はリーク電流が低いことで知られていますが、消費電力は多くのセキュア制御アプリケーションにとって第二の課題となっています。しかし、このプロセスのもう 1 つのメリットは、放射線に起因するソフトエラーの大幅な低減です。ファブリック・コンフィギュレーションが SRAM に保存されることから、シングル・イベント・アップセット（SEU）によって復元不可能な故障が引き起こされる可能性があります。こうしたロジック密度のデバイスでは、FD-SOI は実質的に SEU を除去します。

コンプリートなスタックを実現

お客様の設計負担を軽減するため、ラティスは PFR などを実装する IP、ソフトウェア、サービスによりコンプリートなセキュア制御プラットフォームを実現しています。PFR IP を備えた Mach-NX のコンフィギュレーションのため、ラティスは Propel Builder と呼ばれるドラッグアンドドロップの開発ツールを提供しています。PFR 設計に必要とされるソフト IP としては SPI マスタ、SPI モニタ、I^2C モニタのほか、RISC-V CPU とプログラマブル・ロジック間のレジスタベース・インタフェースがあります。その名称が示すように、SPI モニタは外部 SPI スイッチ・デバイスと接続し、SPI フラッシュ・アクセスのモニタと非認証済みコマンドの阻止を行います。ソフト PFR ブロックは 2.6K セルを消費し、ユーザー・ロジックに対して 8.4K セルの利用を可能にします。

Sentry PFR リファレンス・デザインの一部として、ラティスは組み込み RISC-V コア上で動作するファームウェア向けにソース・コードを提供しています。3 つの主要な PFR ソフトウェア・コンポーネントはセキュリティ・マネジメント、ログ・マネジメント、帯域外通信を行います。各コンポーネントがアプリケーション・コード向けに 1 セットの API を提供するのに対し、低レベル API はソフトウェア/ハードウェア IP ブロックへのアクセスを提供します。ラティスは保護、検出、復元機能を示すサンプル・アプリケーションを提供しています。Propel SDK により、お客様は PFR ファームウェアの修正、コンパイル、デバッグが可能になります。

生産レベルの PFR 設計はそのサプライチェーンでのみセキュアなことから、ラティスは Mach-NX の改変不可能 ID と連動する SupplyGuard セキュリティ・サービスを提供しています。ラティスはお客様ごとに個別の部品番号を割り当て、お客様の製品に対し暗号鍵によるファクトリ・プログラミングを行います。お客様はこの鍵を使用し、署名/暗号化済みビットストリーム付きデバイスのプログラミングを行います。デバイス ID により、お客様のシステムはデバイスの確実なプログラミングが可能になり、ビットストリームのスキャニングを防止できます。この方法により、お客様の IP とともにビットストリームの整合性を保護します。お客様の固有鍵なしではデバイスの再プログラミングは不可能です。この「ロック」機能により、改ざんのリスクなしで、セキュアでない製造設備の使用が可能になります。

他のアプローチ

Mach-NX はユニークな製品であることから、PFR アプリケーションで直接的な競争に直面しません。他のベンダの FPGA を使用する際、お客様はサード・パーティのソフト IP として暗号化ブロックのライセンスを受ける必要があります。さらに、ソフト IP を使用した MCU の例示化と同時に、サード・パーティ・ブロックとの統合も必要になります。多くの FPGA は外部フラッシュ・コンフィギュレーション・メモリも必要とします。表 1 に示すように、他の FPGA はシステム・ファームウェア認証に対する性能が大幅に低くなります。認証時間が増えるにつれて起動時間が増加し、起動時間はアップタイムを減少させます。多くのクラウド・サービスはアップタイムを規定したサービスレベル・アグリーメント（SLA）を含んでおり、起動時間は SLA メトリクスに直接影響を与える可能性があります。「ファイブ・ナイン」（99.999%）を実現するにはダウンタイムを年間 5.3 分未満に抑える必要があり、システム起動時間はクラウド・データセンタでは重要な意味を持っています。

	ラティス Mach-NX	他の FPGA	BMC
F/W 認証時間*	5 秒未満	15 秒超	10 秒超
ECC サポート	ハードウェア	サード・パーティ IP	なし
リアルタイム SPI モニタリング？	Yes	Yes	No
F/W 復元時間	5 マイクロ秒未満	100 ミリ秒超	100 ミリ秒超

表 1. Mach-NX と他のソリューションの PFR 機能の比較。ラティス製品は性能と堅牢なセキュリティを組み合わせて提供。*64MB ファームウェア・イメージと 33MHz SPI クロックの時間（出典：ラティス）

さらに、Mach-NX はシステム・ファームウェア認証が失敗した際に迅速な復元が可能です。デュアル SPI メモリをサポートしており、一方がプライマリ・ファームウェアを保存するのに対し、他方はゴールデン・バージョンを維持します。認証が失敗した場合、Sentry ファームウェアがプライマリからセカンダリ SPI に切り替えることから、起動プロセスはそのまま進行できます。そのバックグラウンドでは、Sentry ファームウェアが認証済みファームウェア・イメージをプライマリ SPI フラッシュにコピーします。他のソリューションの場合、起動プロセスの進行前にファームウェア・イメージをコピーする必要があります。

他の PFR 実装の 1 つは BMC を使用することになっていますが、この方法にはさまざまな制約があります。第 1 に、汎用 BMC は楕円曲線暗号のサポートがなく、提供する認証は弱くなります。BMC は外部フラッシュ・メモリに依存しており、サプライチェーンの脆弱性を招きますが、Mach-NX や SupplyGuard ではこれを防止します。最後に、インライン SPI モニタリングのサポートも欠如しており、外部 PLD を使用しこの機能を追加する必要があります。Mach-NX はいずれのケースでも PLD を必要とする PFR と制御機能を実装可能です。

最近、カスタム・プラットフォーム・セキュリティ・チップの開発が増加傾向にありますが、こうしたチップの一部はスマートフォン向けに設計されており、生体認証が含まれています。しかし、Google は自社のクラウド・サーバ向けに Titan セキュア・マイクロコントローラのバージョンを開発しました。他のハイパースケール・クラウド・オペレータも同様のチップを開発可能ですが、多くの OEM 企業はカスタムチップ開発に必要な経営資源を割くことに積極的ではありません。汎用ソリューションでありながらカスタマイズ可能なソリューションの提供により、ラティスはカスタム半導体開発の負担を不要にしながら同じレベルの機能を提供します。

まとめ

ラティスは現在、FPGA の開発にとどまらず、最適化した半導体、ソフトウェア、ツール、サービスで構成される包括的なセキュア制御プラットフォームを提供しています。システム設計から機器の廃棄に至るまでのお客様の全製品サイクルを検討し、各ステージでの脆弱性に対応しています。Mach-NX はラティスの長年にわたるセキュア制御の経験を活かし、暗号化の強化、BMC インタフェースのアップグレード、カスタム機能やフィールド・アップデートのためのプログラマブル・ロジックの負担軽減により、現場で実証済みの MachXO3D をさらに改良しました。同様に重要なのは、Sentry リファレンス・デザインがお客様の時間とリソースの要件を低減し、お客様のシステムへの PFR の組み込みを可能にしていることです。

サーバにより堅牢なプラットフォーム・セキュリティの普及が可能になりましたが、常時オン・ネットワーク接続によって多くのシステムがサイバー攻撃のリスクにさらされることになり、

プラットフォーム・セキュリティ市場は拡大を続けています。ネットワーキング/通信機器、産業制御システム、航空宇宙システム、自動運転車はすべて、ますます増大する脅威のターゲットになっています。ラティスは製造からフィールド・アップグレードに至るまで、こうした分野のお客様の設計製品をセキュアに保護し、サポートしています。

Bob Wheeler は The Linley Group の主席アナリスト兼 Microprocessor Report シニア・エディタ。Linley Group はマイクロプロセッサや SoC の設計に関する最も包括的な分析を提供しています。ビジネス戦略だけでなく、内部技術の分析も行っています。エンベデッド・プロセッサ、モバイル・プロセッサ、サーバ・プロセッサ、AI アクセラレータ、IoT プロセッサ、プロセッサ IP コア、イーサネット・チップなどについて詳細な記事を提供しています。詳細については、www.linleygroup.com/をご覧ください。