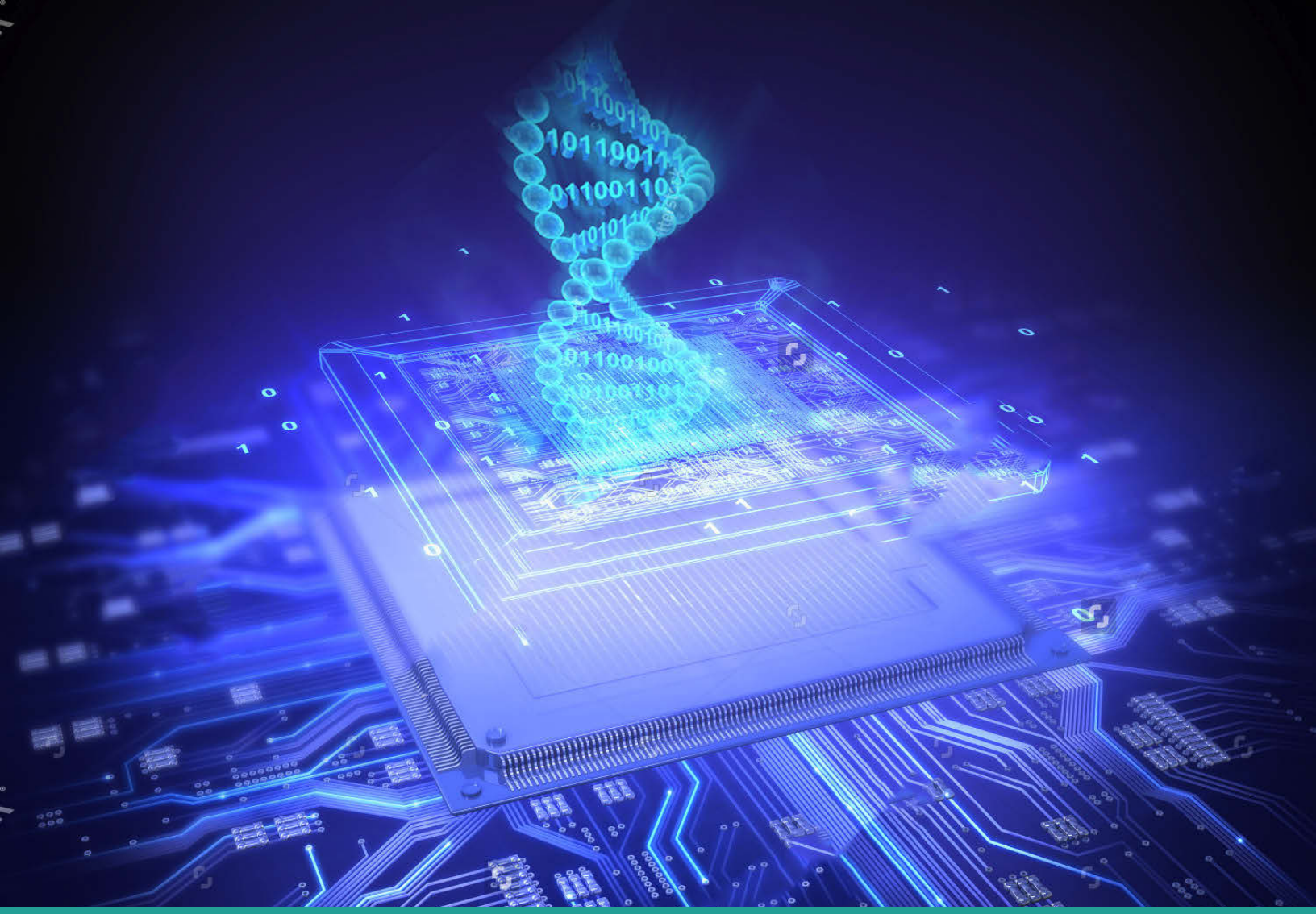

クローン不能、ターンキーエンベデッドセキュリティはどのようにして設計を完全に保護するか

筆者：Scott Jones、マキシム・インテグレーテッド、
エンベデッドセキュリティ担当マネージングディレクター

2017年11月

maxim integrated™

要約

サイバー犯罪による損失は2016年に24%増加して13億3000万ドル以上になりました。しかもこれらは、FBIのインターネット犯罪苦情センターによって追跡管理された犯罪のみを現わしたものです。ハッキングやその他のセキュリティ侵害についてのニュースの見出しは毎日のように発生しています。しかし、多くの製造メーカーにとってデザインセキュリティは未だに後回しにされています。これは部分的に、セキュリティの実装は時間とリソースの面で高コストだという誤解が原因です。この論文ではこれらの誤解を排除し、侵入攻撃に対する強力な保護を提供する最新のターンキー方式の、コスト効率に優れたエンベデッドセキュリティについて解説します。

はじめに

なぜ未だにデザインセキュリティは見過ごされているのか？

IoT製品の開発はサイバー攻撃に対する防御を上回るペースで進んでいる

昨年、通信業界の巨人Telefonicaは、サイバー犯罪に対する防御がモノのインターネット(IoT)ソリューションの開発に遅れを取り続けていることによる悲惨な結果について警告したレポートを発行しました。

「単に私たち自身のデータのプライバシーや、デジタルIDのセキュリティだけの問題ではありません。今後数年間で、私たちの生活はインターネットに接続された機器に囲まれることになり、それらの機器が私たちの一挙手一投足をデジタル化し、日常の活動を情報に変換し、あらゆる相互作用をネットワーク全体に配信し、この情報に従って私たちと相互作用することになります。いまだかつて、物理的な生活の中での私たちの行動とデジタルの世界がこれほど接近したことはありません」と、同社はレポート「Scope, scale and risk like never before: Securing the Internet of Things[1]」の中で述べています。

しかし、セキュリティ侵害の勢いは依然として衰えていません。信用情報大手のEquifaxでは今年の夏に大規模なデータ漏洩が発生し、ハッカーが米国在住の人々の氏名、社会保障番号、生年月日、住所、および一部のクレジットカード番号、ならびにイギリスおよびカナダ在住の人々の個人データへのアクセス権を手に入れました。今年の春には大規模なWannaCryランサムウェア攻撃が、ヨーロッパ、南米、アジア、および北米の少なくとも150カ国でコンピュータに影響を与え、病院、大学、メーカー、企業、および官公庁の業務を妨害しました。2016年の秋には、Miraiマルウェアの亜種をベースとするボットネットが原因で、ハッキングされたCCTVビデオカメラとDVRによる大規模なインターネット障害が発生しました。これらの主要な、広く報道されている事件1つ1つの陰で、多数のより小規模な出来事が起きており、それらも顧客と企業にとって同様に心配な問題です。また、より多くの製品やシステムがネット接続され、ハッカーはますます高度化しているため、対処すべきリスクがあらゆる業界に存在することも言うまでもありません。たとえば、以下のようなシナリオが考えられます。

- 産業：従来の隔離されたシステムから現在の完全にネットワーク化されたシステムへの移行によって機器がリモート攻撃に晒されます。
- 医療：機密データに関するプライバシーの問題、データ完全性の問題、および医療機器/装置の認証された操作の必要性があります。
- 銀行：身元を視覚的に保証することができなくなるため、オンラインバンキングの指数関数的な増大によってリスクが拡大します。
- 小売：モバイル機器はオープンアーキテクチャ化が進んでいますが、金融/支払い端末として動作するため、トランザクションおよび通信がセキュアであることを確保する必要があります。
- 通信：各種の攻撃に対する保護のために、エンドツーエンドのセキュリティが必須です。
- 自動車：2015年にホワイトハットハッカーによってJeepがリモートから制御された[2]のを覚えていますか？自動車は急速に車輪の付いたコンピュータ化し

ており、ハッキングがリスクにさらされたままになっています。

デザインセキュリティを無視すると、収益の喪失、ブランドの評判低下、さらには人的被害まで、高いコストを招きます。侵害が発生したあとでシステムを修正するのは、効果の面で低すぎ、遅すぎる場合がほとんどです。実際のところ、設計サイクルの早い段階でセキュリティを組み込むほど、それだけ良い結果につながります。ハードウェアベースのセキュリティは、ソフトウェアベースのものより効果的であることが実証済みです(ハードウェアベースとソフトウェアベースのデザインセキュリティの比較については、ホワイトペーパー「なぜすべてのアプリケーションにハードウェアベースデザインセキュリティが必須か」をお読みください)。しかも幸いなことに、セキュアICを使用するハードウェアベースの方式は必ずしも大量の労力、リソース、または時間を必要としません。

セキュリティなしの代償

恐らくあなたは製品を迅速に市場投入するとともに開発コストを低く抑える必要があるという大きなプレッシャーを受けているでしょうが、侵害に関連するコストを慎重に検討しましたか？表1の仮説的な最終製品が示すように、セキュリティなしで済ますと実際には最終的により高コストになる可能性があります。

ハードウェアベースのセキュリティが堅牢性を提供する理由は、1つにはサイバー犯罪者が設計の物理層を変更するのは困難だからです。さらに、物理層が存在することで、マルウェアがオペレーティングシステムに侵入して設計の仮想化層を貫通することが不可能になります。設計サイクルの最初から開始することによって、設計の基本レベルおよびそれに続くすべての層にセキュリティを内蔵することができます。

内部の、書換え不能メモリからコードを実行するマイクロコントローラなどのセキュアICを使用することは、電子機器のハードウェアを侵害しようとする攻撃に対する防御になります。マイクロコントローラのROMにはスタートアップコードが保存されますが、これは書換え不可能なため「信頼の根幹」と考えられます。この変更不可能な、したがって信頼性のあるソフトウェアを使って、アプリケーションソフトウェアの署名を検証および認証することができます[3]。ハードウェアベースの「信頼の根幹」方式をゼロから実装する場合、設計に含まれる潜在的な侵入ポイントをより多く閉鎖することができます。

デザインセキュリティを無視すると収益の喪失につながる

セキュリティICなし	
1,000万ユニットの売上高(単価10ドル)	$100M
15%の偽造によるマイナス	-$15M
純売上	**$85M**
製品コスト、1,000万ユニット(単価3ドル)	-$30M
利益	**$55M**

セキュア認証用IC (単価0.5ドル)を使用	
1,000万ユニットの売上高(単価10ドル)	$100M
0%の偽造によるマイナス	$0M
純売上	**$100M**
製品コスト、1,000万ユニット(単価3.5ドル)	-$35M
利益	**$65M**

表1:偽造による資産の損失は最終的にセキュリティ実装のコストを上回る。

セキュア認証用ICはコスト効率に優れたIP保護である

セキュアマイクロコントローラやセキュア認証用ICなどのエンベデッドセキュリティICは、各センサーノードからクラウドまで、システム全体を保護するターンキーソリューションを提供します。しかし、すべてのセキュリティICが同様に作られているわけではありません。たとえば、一部のセキュアマイクロコントローラは、コスト、消費電力、または複雑なファームウェア開発が必要なためIoT機器やエンドポイントには適していません。それに対して、ファームウェアの開発を必要とせずにエンベデッド、コネクテッド製品用に完全なセキュリティを実装する暗号コントローラもあります。そのような例の1つがマキシムのMAXQ1061 DeepCover®デバイスです。このコプロセッサは、最初から設計に組み込むことも既存の設計に統合することも可能で、機密性、真正性、およびデバイスの完全性を保証します。

セキュア認証用ICの場合、デバイスは固定機能の中核的な暗号操作一式、セキュアキーストレージ、およびIoTとエンドポイントのセキュリティに最適なその他の関連機能を提供する必要があります。これらの機能を備えたセキュア認証用ICは、IPの保護、クローンの防止、およびペリフェラル/IoT機器/エンドポイントの認証のためのコスト効率の良い手段になることができます。

エンベデッドセキュリティ技術を評価する際には、他に何を検討すべきでしょうか？暗号解読侵入、物理タンパリング、およびリバースエンジニアリングなどの脅威に対する保護が可能な、組込み暗号エンジンとセキュアブートローダを備えたセキュアマイクロコントローラを検討してください。カリフォルニア州メンローパークを拠点とするデジタルセキュリティおよび民生用製品エンジニアリング企業であるDesign SHIFTは、ORWLセキュアデスクトップPC用にそれらの機能を必要としていました。ORWLは認証の2つの要素を要求し物理攻撃に対する保護を提供しますが、同社がORWLを設計したときに強力な信頼の根幹セキュリティが必要になりました。Design SHIFTは、MAX32550 DeepCover ARM® Cortex® -M3セキュアマイクロコントローラが解決策になると考えました。

「多くのソフトウェア担当者は、ハードウェアの制御を失ったらもう終りだと言っています」と、Design SHIFTのCEOであるOlivier Boireau氏は語っています。「信頼の根幹を確立することで、強力な保護という安心が提供されます」。

物理的複製防止機能技術による保護の強化

セキュリティICに採用され始めているより先進的なレベルの暗号が、物理的複製防止機能(PUF)です。PUFは、ICデバイスの複雑で可変な物理的/電気的特性から導かれる関数です。PUFは製造時に付加されるランダムな物理的要素(予測不能かつ制御不能)に依存するため、複製やクローンはほぼ不可能です[4]。PUF技術は関連するICのデジタル指紋をネイティブに生成し、認証、ID、偽造防止、ハードウェア-ソフトウェアバインディング、および暗号化/復号を提供するアルゴリズムをサポートするための固有の鍵/シークレットとして使用することができます。

マキシムのPUF回路は、基本的なMOSFETデバイスで自然に発生するランダムなアナログ特性を使って暗号鍵を生成します。このソリューションを、ChipDNA™技術と呼んでいます。特許取得済みの方式によって、各PUF回路によって生成される固有のバイナリ値が温度と電圧およびデバイスの経年にわたって再現可能であるという保証が確保されています。高レベルのセキュリティは、固有のバイナリ値

が実際にはチップ上の不揮発性メモリに保存されないという事実に由来します。その値は必要なときにPUF回路によって生成され、その後消滅します。それによって、従来のセキュアデバイスが秘密鍵の発見を目論む、不揮発性メモリへの侵入型物理攻撃を受ける可能性があったのに対し、存在しないものを盗むことはできないため、PUFベースのデバイスにはこの種の攻撃に対する弱さがありません。その上、PUFベースのデバイスが侵入型物理攻撃を受けた場合は、攻撃自体がPUF回路の電気的特性を変化させる原因になるため、この種の攻撃がさらに妨げられます。ChipDNA PUF技術は、プロセス、電圧、温度、および経年にわたる優れた信頼性を実証しています。さらに、NIST[5]ベースのランダム性テストスイートに沿ったPUF出力の評価は成功に終り、結果は合格でした。図1は、ChipDNA PUF技術のさまざまな使用例(内蔵メモリの暗号化、外付けメモリの暗号化、および認証鍵の生成)を示しています。

PUF技術を使用した初のセキュア認証用IC

ChipDNA PUF技術を特長とするマキシムの最初のセキュアICは、セキュア認証用ICのDS28E38で、侵入型物理攻撃に対するコスト効率の良い保護を提供するように設計されています。DS28E38 (図2)は、以下を提供します。

- FIPS186 ECDSAベースのチャレンジ/レスポンス認証
- ChipDNAでセキュリティ確保された保存データ、オプションのECDSA-P256プライベート鍵ソース
- ユーザーメモリおよびパブリック鍵(公開鍵)証明書用の2kbのEEPROMアレイ

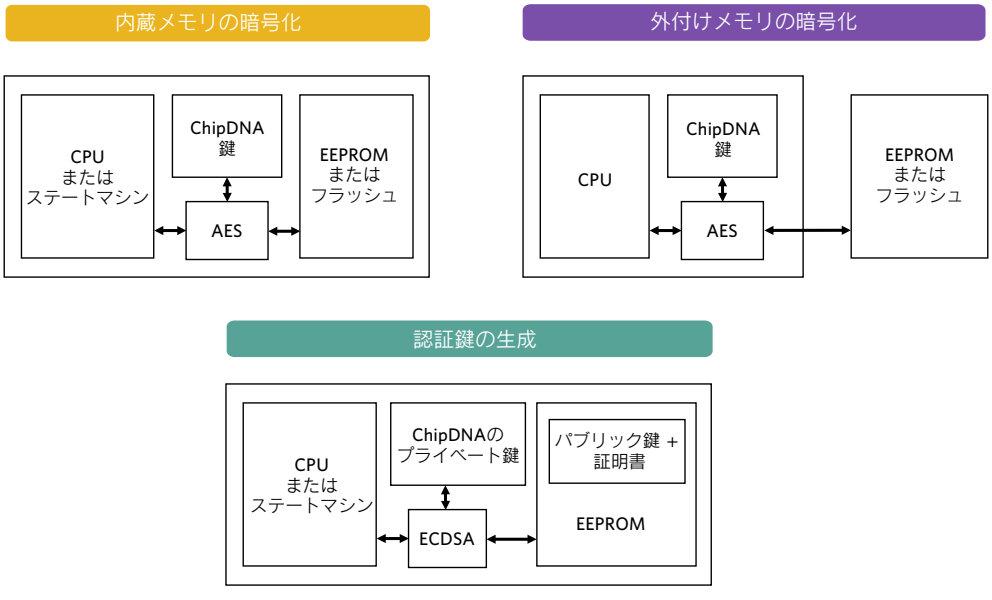

図1：ChipDNA PUF技術のさまざまな使用例

信頼の根幹は書き換えることができない

PUF技術には盗むべき鍵がない

- 認証付き読取りを備えたデクリメント専用カウンタ
- 固有の出荷時設定される読取り専用シリアルナンバー(ROM ID)
- 従来は不可能だった領域でのセキュア認証のための、汎用的、堅牢、高信頼性の相互接続手段を提供する単一接点、1-Wire®寄生インタフェース

DS28E38は、ChipDNA PUF技術を採用した最初の製品に過ぎません。マキシムはエンベデッドセキュリティポートフォリオ全体(セキュア認証用ICとセキュアマイクロコントローラの両方)を拡張しており、ChipDNA技術を使って作られた多数の新製品を今後数か月の間に提供する予定です。

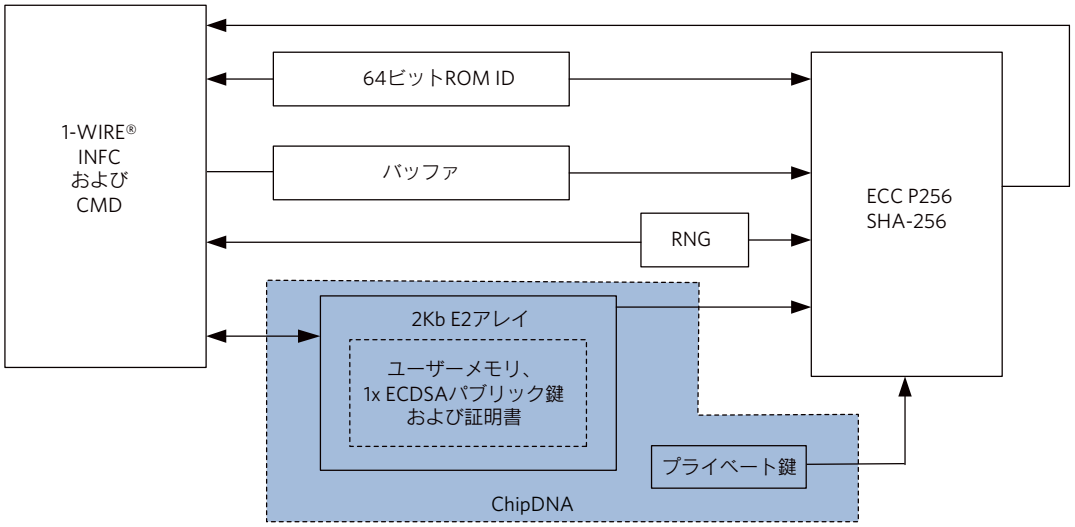

図2：ChipDNA PUF保護を備えた
DS28E38 DeepCoverセキュアECDSA認証用ICのブロック図

まとめ

今日のエンベデッドセキュリティICは、複数層の高度セキュリティ、暗号アルゴリズムのサポート、タンパー検出、およびその他多数の保護手段によって設計を完全に保護するためのターンキー技術を提供します。特にPUF技術は、侵入型および非侵入型攻撃の両方に対する保護のための非常に強力なメカニズムを提供します。結局のところ、存在しない鍵を実際に盗むことはできません。

さらに詳しく

次の設計を保護することができるエンベデッドセキュリティソリューションの詳細については、**エンベデッドセキュリティソリューションのセレクタガイド**をご覧ください。

出典

[1] https://www.telefonica.com/documents/737979/5540857/Telef%C3%B3nica_Security_IoT_Final.pdf/a28293d4-f15a-4f21-8353-317faf892a18

[2] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[3] http://www.embedded.com/design/safety-and-security/4438300/Securing-the-IoT--Part-2---Secure-boot-as-root-of-trust-

[4] https://en.wikipedia.org/wiki/Physical_unclonable_function

[5] https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software