デザインソリューション
エンベデッドセキュリティ

強力なセキュリティで汎用入出力を操作

はじめに

エンベデッド電子認証は、機器に取り付けられたリ、機器の内部で使用され、サブシステム、アクセサリや周辺機器に偽造品が使用されることを防ぎます。さらに、電子認証を採用することによって、メーカーは製品の使用方法および性能をより包括的に制御することができます。用途に応じて、電子認証は製品の信頼性、精度、安全性、そして、OEMの研究開発投資保護のためのセキュリティの維持に役立ちます。

脅威

図1の「モノのインターネット」リモートロック開閉アプリケーションを考えてみます。サーバーは、「開」の命令をネットワーク接続された、リモートの、「スマート」ロック機構(ネットワーク対応コントローラ内蔵)に送信します。侵入者がロックを解除するのを防ぐために、リモートサーバーからの命令の真正性を検証することが絶対に必要です。また、偽造品と交換されていないことを確認するために、ロックの真正性も検証することが望まれます。サーバーとロックの相互認証は、ロック自体の内部に電子認証デバイスを配置することによって実現可能です。ロックとサーバーは互いにチャレンジを送信します。それぞれのチャレンジに対するレスポンスが条件を満たすものであれば、相互認証が確保されます。認証プロセスが成功裏に完了すると、「合格」信号がコントローラに送信され、コントローラは目的のアクション、具体的にはロックの解除を実行することができます。

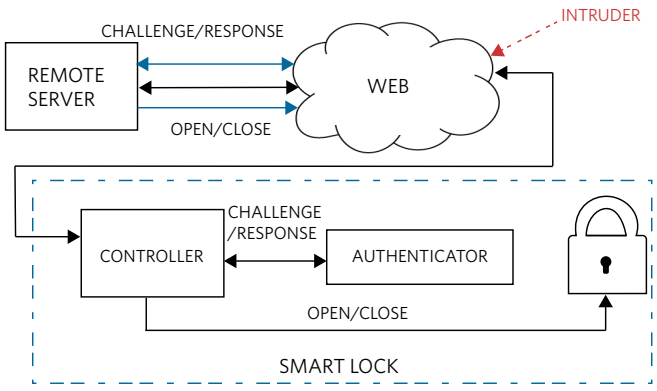

図1. 標準的なリモートロック開閉アプリケーション

しかし、この構成には潜在的に脆弱なポイントがあります。コントローラは解錠と施錠のアクションに関する最終的な責任を負います。セキュリティ確保されていないコントローラは侵入者からの攻撃に対して脆弱で、侵入者はコントローラの制御を奪って認証デバイスからの合否結果を無視するように設定する可能性があります。その後、侵入者はロックを自由に開閉することができます。

ソリューション

明らかに、セキュリティ確保されていないコントローラからロック開閉の責任を他に移し、この脆弱性を克服することが望まれます。これを実現する方法の1つは、サーバーの認証のみでなく、ロック機構の開閉に対する責任も負うことができる電子認証デバイスを使用することです。

MaximのDS28C36は、セキュア汎用入出力(GPIO)を備えた初めての電子認証デバイスです。従来どおり必要な相互認証の機能を実行しながら、セキュアな状態制御および状態検出を備えた2つの専用GPIO端子によって、リモートサーバーからロックへのすべての命令が強力な暗号プロトコルを使って処理されることを確保します。先ほどのリモートロック解除のシナリオで推奨されるDS28C36の使用法を図2に示します。

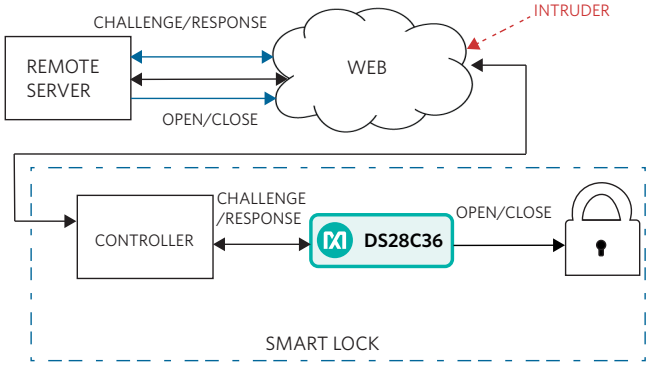

図2. DS28C36を使用したセキュアリモートロック開閉

このシナリオでは、認証はリモートサーバーとDS28C36の間で行われます。侵入者の攻撃があった場合、DS28C36はGPIOをディセーブルし、ロック機構の制御の喪失を防ぐことができます。図3は、ECDSA認証を使用してセキュアなロック制御を実現するためのリモートサーバーとDS28C36の間の暗号シーケンスの概要を示しています。セキュアGPIO機能を備えた唯一の電子認証デバイスであることに加えて、DS28C36はリプレー攻撃の検出と防止も可能です。

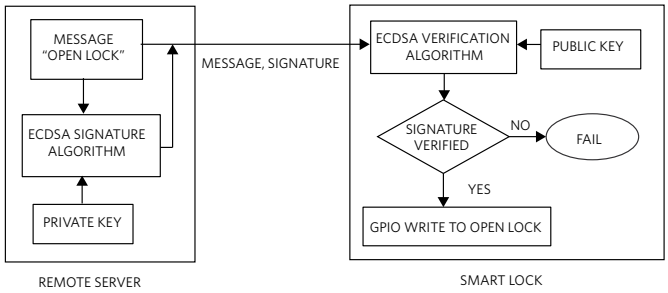

図3. ECDSA認証GPIO制御の暗号シーケンス

機能

DS28C36は、非対称ECDSAと対象SHA-256ベースのHMACの両方による双方向セキュア認証、オプションのECDSAまたはSHA-256認証によるユーザープログラマブルメモリのセキュア保護、暗号化ホスト-デバイスおよびデバイス-ホスト伝送とECDHベースの鍵確立との組み合わせによる機密データのセキュアストレージ、オプションのセキュア認証による状態制御と状態検出を備えたGPIO、およびオプションのGPIO合否表示によるシステムセキュアブート/ダウンロード検証などの広範な機能一式を内蔵しています。

結論

ほとんどの電子認証デバイスはホストコントローラに接続された周辺機器の真正性を保証することができますが、両者の間のセキュア通信は保証しません。MaximのDS28C36は、革新的な2つのセキュリティ制御されたGPIO端子の内蔵によって、この問題に対応可能な唯一のセキュア認証用デバイスとなっています。この機能の恩恵を受けるその他のアプリケーションには、アクチュエータ、バルブ、およびリレーのセキュアな制御が必要な産業オートメーションがあります。

さらに詳しく:

認証アプリケーション

DS28C36のデータシート

デザインソリューションNo. 11

設計サポートが必要な場合は、Eメールにてお問い合わせください。
https://www.maximintegrated.com/jp/support/overview.html/TechSupportFormJapan

マキシム・ジャパン株式会社
〒141-0032 東京都品川区大崎1-6-4 大崎ニューシティ4号館20F maximintegrated.com/jp