不正アクセスに対する防護

Protection against Unauthorized Access

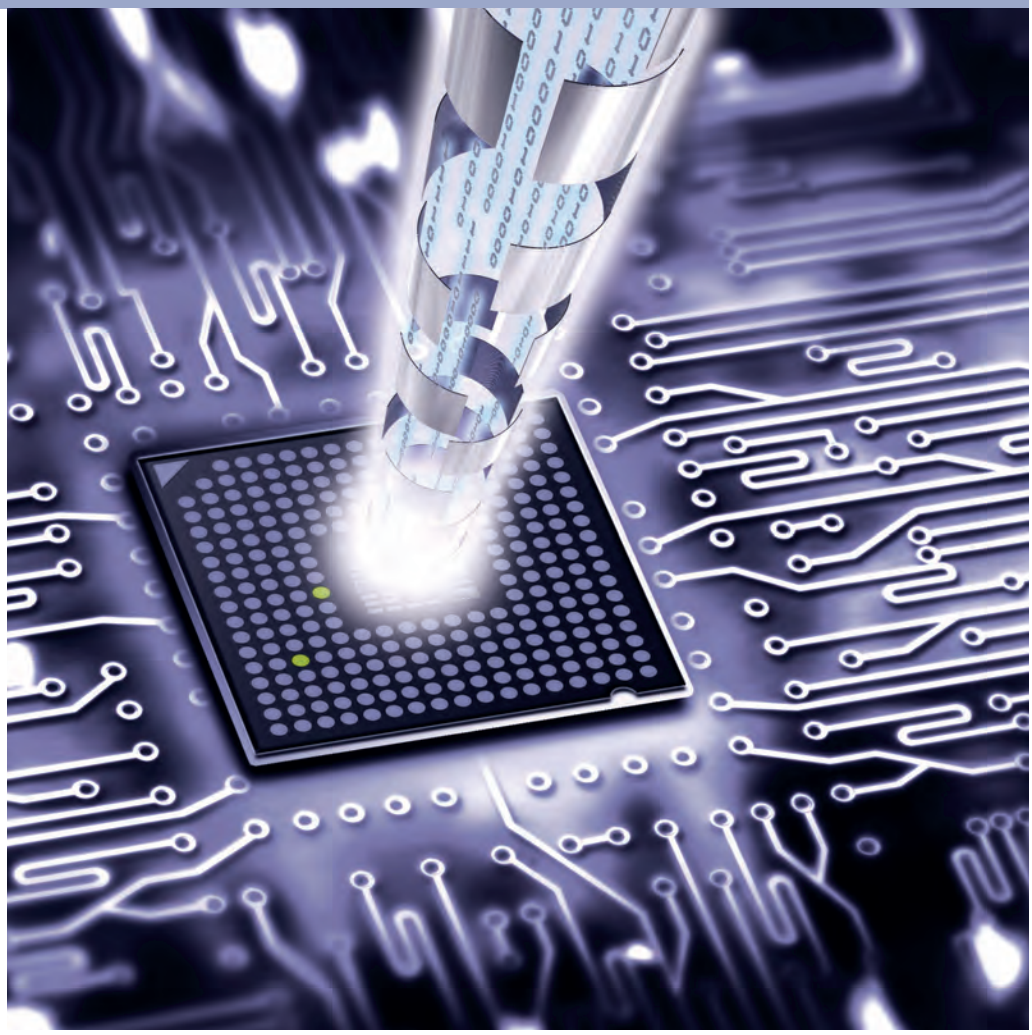
ソフトウェアとハードウェアのインテリジェントな相互作用が ECU を守ります

コネクテッドビークルシステムには不正アクセスに対する防護が必要です。ハードウェアセキュリティモジュール（HSM）がこの機能を提供していますが、HSM はこれまで自動車アプリケーションに適応したものではありませんでした。しかし、Bosch 社の HSM およびさまざまな半導体メーカーにより実現された派生製品のおかげで、もはや今までとは状況が異なるようになりました。ESCRYPT はこれらの製品の需要の高まりにタイミングを合わせて CycurHSM を発表しました。これは、HSM を自動車 ECU 用として実行可能なセキュリティーソリューションに適応したファームウェアソリューションです。

執筆者

Christopher Pohl
ESCRYPT GmbH
ボーフム上級
セキュリティ
エンジニア

Dr. Frederic Stumpf
ESCRYPT 社
シュトゥットガルト支部長



サイドウィンドウが粉々になり、エアバッグとナビは使い物になりません。非常に面倒なことですが、少なくとも損害は明白です。車両の IT システムが改ざんされてしまった場合はそうはいきません。この類の不正介入は目に見えない脅威となり、リスクの可能性は車両と ECU のつながりが増していくにつれてますます高まりつつあります。

必要になるのは、ハッカーと彼らの潜在的攻撃、ウイルス汚染、および不正アップロードに対して防衛するための方策です。Bosch 社は数年前に、ハードウェアセキュリティモジュール（HSM）が適切な防護技術であることを認識しました。HSM は専用のプロセッサコア、専用の RAM、ROM、およびフラッシュメモリを持ち、明確なセキュリティ機能を搭載しています。しかし、当時販売されていた HSM は非常に高価で取り扱いに注意を要する上、機能も、ごく限られていました。そこで、Bosch 社は車載対応の HSM の仕様を策定し、それを半導体メーカーと共有して市場への浸透を促しました。これは良い結果を生む戦略です。さまざまなメーカーが Bosch HSM の派生製品を製造して市場に参入しています。

Bosch HSM とその派生製品のために標準化されたソフトウェアスタック

2015 年 7 月、ESCRYPT は CycurHSM という、（標準 HSM 仕様と）互換性のあるファームウェアソリューションを発表しました。CycurHSM は、初期ブート、通常運転、およびソフトウェアの更新またはアップグレードを含むすべての動作フェーズにわたって車両システムを不正アクセスから守ります。

ハードウェアとソフトウェアが連携して、この包括的な防御を実現します。各 Bosch HSM はプロセッサ、十分なメモリ、および真性乱数生成器（TRNG）を搭載しています。さらにアクセラレータハードウェアも搭載しているので、Advanced Encryption Standard（AES）に基づく暗号化メッセージの認証コードを瞬時に算出することができます。このハードウェアをベースにして、ESCRYPT は CycurHSM のセキュアブート、実行時チューニング検知、およびセキュアフラッシングなどの機能を実現することができました。またソフトウェアは、自動車アプリケーション向けのリアルタイムオペレーティングシステムとして開発された ETAS の RTA-OS にも依存しています。

最大限柔軟にハードウェアを選択

ESCRYPT は Bosch HSM とその全ての派生製品向けに標準化されたソフトウェアスタックを開発するという構想を抱き、2013 年半ばに CycurHSM についての構想を開始しました。そしてこの目標は達成されました。プロセスをソフトウェアレベルで標準化することにより、お客様はハードウェア設定とは無関係に、どれでもお好みのコントローラを選択できるようになりました。CycurHSM の背後にあるオープンな思想に従い、このソフトウェアの CSAI インターフェース（Client Server Architecture Interface）は、AUTOSAR だけでなく、この規格の域を越える他の全てのアプリケーションにも対応できます。

包括的な防護

CycurHSM は、更新およびアップグレードについて送信者の信頼性を検証するファームウェアのセキュアなフラッシュ機能と同じく、ESCRYPT のモジュール式製品のポートフォリオに組み込まれています。このプロセスに必要な秘密鍵は、車両メーカーまたは専門サービスプロバイダのバックエンドで生成され、信頼できるパートナーとだけ共有されます。ESCRYPT は鍵管理サービスを提供して警備の厳重なデータセンタでこの種の処理を行うだけでなく、このような暗号鍵を生成できるソフトウェアのライセンスも発行します。たとえばセキュアフラッシングなどのようなゲートキーパー機能は、Car-to-X 通信および OTA アップデートを使用する車両には必須です。車両に接続しようとしているソースがデジタル署名を要求されて提供できない場合には、そのデータ転送は HSM により禁止されます。暗号化技術は CycurHSM セキュアブート機能の中核にも使用されていて、ブート処理中に秘密鍵を使用して、ECU ソフトウェアが認証状態であるかどうかを明白に判断します。

このプロセスは順を追って進みます。システムの電源が入ると、ECU ブートチェーンの一環として起動された各コンポーネントは次のコンポーネントの完全性を検証します。そのため、マルウェアが、たとえ工場内の診断デバイスなどのような信頼できるソースから侵入したとしても、遅くともシステムの次回起動時には確実に検知されます。HSM は一つ一つの変化を記録するので、たとえ ECU ソフトウェアが元の状態に戻されてしまっても、改ざんを検知することができます。このようにして、CycurHSM は、悪名高いチップチューニングのグレーゾーンに対して、法のお墨付きを加えるという、おまけをもたらします。

動作中、CycurHSM のランタイムチューニング検知は周期的にチェックを行い、ECU データの持続的な信頼性を確立します。アクセラレータハードウェアがこのテスト、つまり、対称アルゴリズムの AES 署名に基づく非常に効率的なプロセスを実行します。

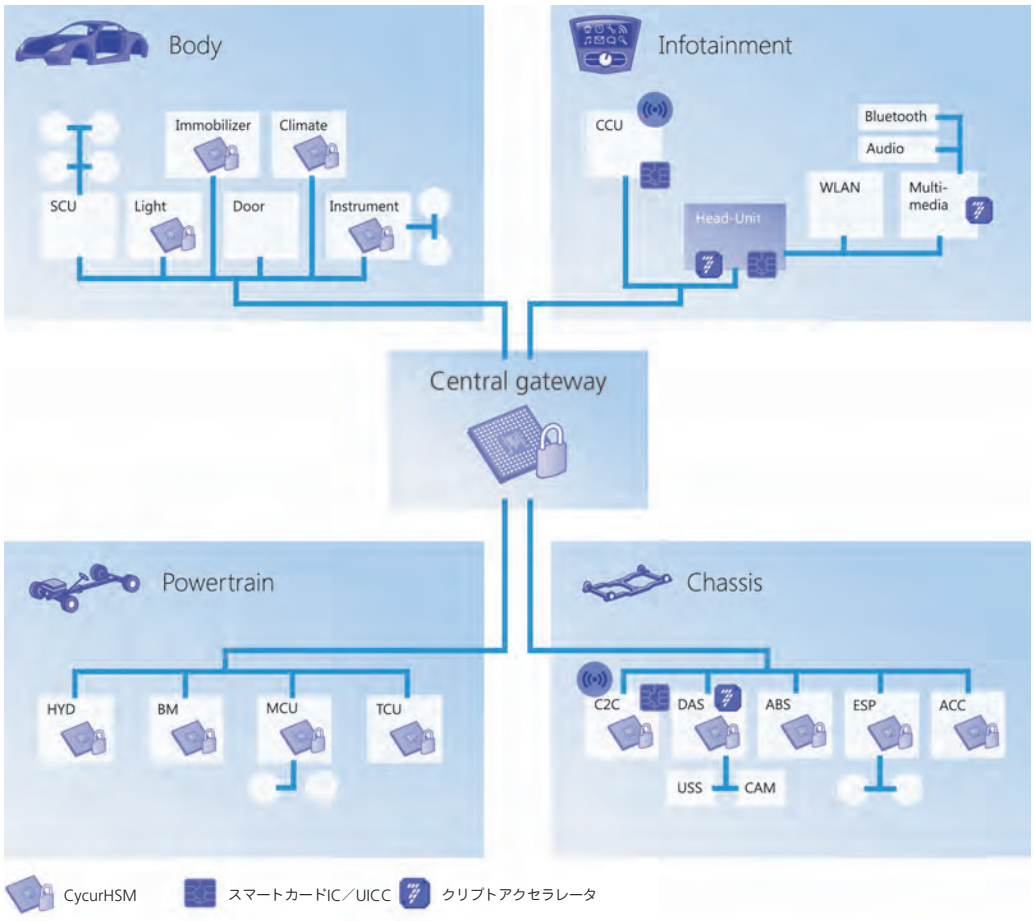
CycurHSM はそのセキュアなオンボード通信機能により、車内の ECU から ECU へと渡されるデータを保護するための第 4 の方法を提供します。ビークルバスを流れるデータトラフィックを、ワイヤレスインターフェースのようなゲートウェイを利用して侵入しようとする脅威から防護します。このために、CycurHSM は ECU から ECU へと渡される途中のデータに AES ベースのメッセージ認証コードを発行します。このコードの生成と検証は CycurHSM が

行うので、当該 ECU はそれを行う必要はありません。CycurHSM はすべての暗号計算を担当して鍵の安全性を保ち、ECU に関する統合セキュリティサービスプロバイダの機能を果たします。

今後の展望

ESCRYPT は、HSM の技術が今後 10 年の間に進化し、新しい車の標準機能になることを確信しています。標準化された CycurHSM ソフトウェアは、この技術の前進に役立つ重要な構成要素になります。HSM ハードウェアと連携して、安全関連の車載 IT システムを不正アクセスから守ります。コネクテッド技術が進歩していくペースを考えれば、CycurHSM は確実に未来に対応したソリューションであると考えることができます。

202x 年のビークルボードネットワーク



SCU	座席制御ユニット
CCU	通信制御ユニット
HYD	ハイブリッドドライブ
BM	バッテリ管理
MCU	モーター制御ユニット
TCU	トランスミッション制御ユニット
C2C	車両間通信
DAS	運転車支援システム
ABS	アンチロックブレーキシステム
ESP	電子安定プログラム
ACC	適応走行制御
USS	超音波センサ
CAM	カメラ
IC/UICC	集積回路／万能集積回路カード