Embedded Security Testing in Virtual Vehicles

仮想車両で組み込みセキュリティのテストを実施

XiL テスト環境を利用してハッキングを詳細にシミュレート

ソフトウェアで制御される現代の車両システムは、機能的な安全だけでなく、サイバー攻撃に対する防御力も必要です。ハッキングされた ECU がセキュアな状態を保てるかどうかを車両全体についてテストするためのソリューションとして、ETAS と ESCRYPT は仮想化技術に注目しました。ここでは、セキュリティテストに XiL* テクノロジーの長所を生かすことができます。

執筆者

Jürgen Crepin
ETAS GmbH
マーケティング
コミュニケーション
上級エキスパート

Dr. Tobias Kreuzinger
ETAS Inc.
（米国ミシガン州
アナーバー）
テスト・評価上級マネージャ

– ハッカーが車両システムにアクセスしてセンサ信号を傍受し、その信号の代わりに不正なデータを ECU インターフェースに入力する。すると突然、ドライバーは反応することができなくなり、外部からコントロールされた車両の中に閉じ込められてしまう … – このような恐ろしいシナリオをフィクションの世界に留めておくには、信頼できるセキュリティソリューションが必要です。

しかし、ハッカー攻撃のテストを行うことなど可能なのでしょうか。つまり、セキュリティ対策が車両システムを確実に防御していることを証明することはできるのでしょうか。機能安全の領域では、通常の運転中も停車中も諸機能が設計どおりに反応することをハードウェアインザループ（HiL）システムで検証することができます。すべての ECU とデータネットワークを含む車両全体のシミュレーションを利用して、ソフトウェアテストや分散されたセンサシステムと車両との相互作用評価を行いますが、その技術的基礎となるのは、ETAS LABCAR のようなリアルタイム HiL システムや ETAS COSYM コ・シミュレーション、または ETAS ISOLAR-EVE で生成される仮想 ECU などです。

新しい選択肢：セキュリティインザループ

セキュリティテストの場合、「トゥルーポジティブ（真陽性）技法」、つまり予想される挙動のテストは、あまり効果的ではありません。開発の時点では、実際の攻撃シナリオはたいてい未知のものであり、既知のセキュリティギャップであれば事前に埋めることができるからです。それよりも脆弱性の系統的な探索の方に重点が置かれ、ソフトウェアインザループ（SiL）や HiL のテスト環境はそのような探索にも適しています。

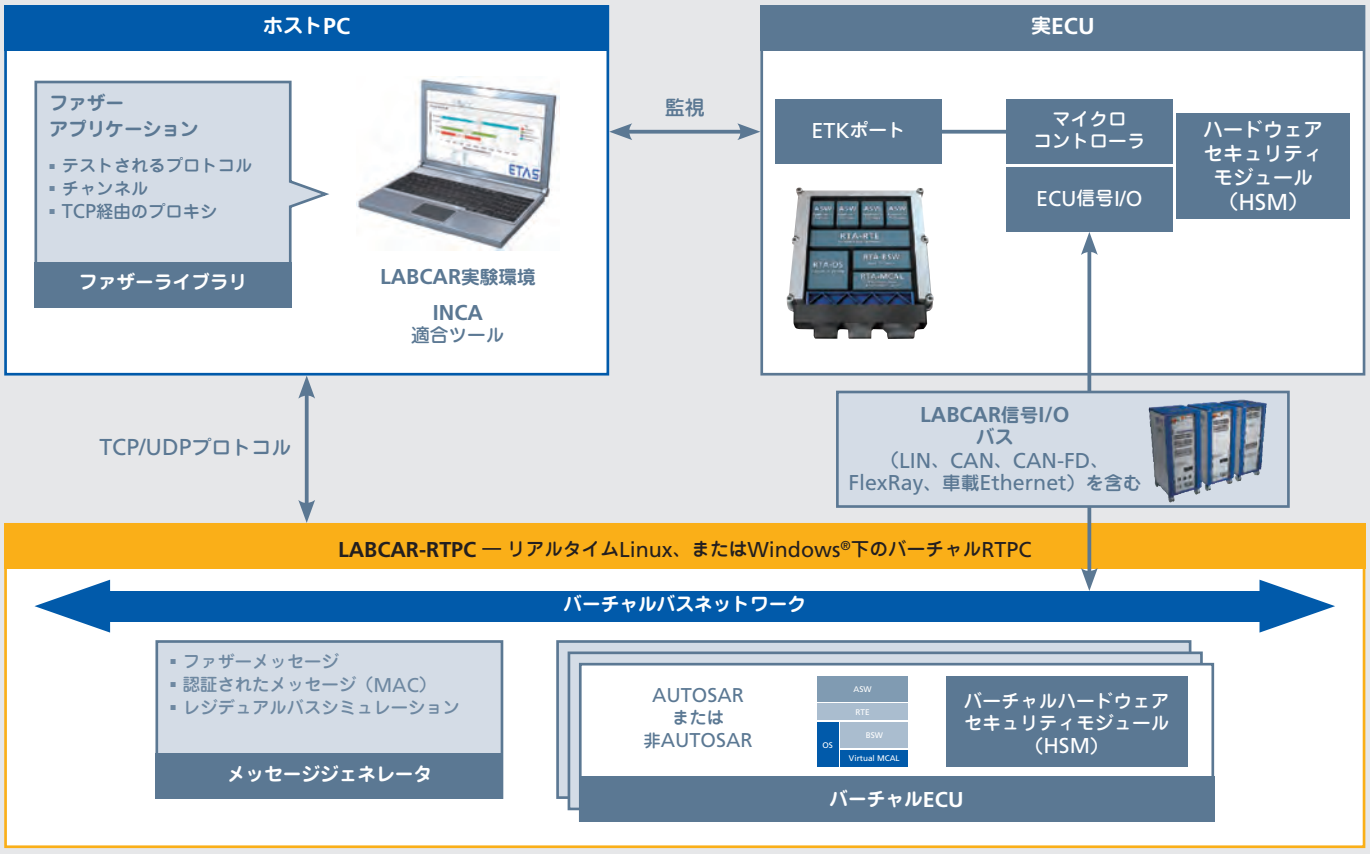
そこで課題となるのは、さまざまな領域の能力を融合させる方策です。セキュリティの専門家は XiL のテスト手法をよく理解しておく必要があり、XiL テストエンジニアは従来の IT 環境で用いられる手法について認識しておく必要があります。そうすれば、組み込みシステムに潜在する脆弱性を両方向から認識することができます。ここで特に注目すべきものはセキュリティ関連の車両機能で、そのためのセキュリティテストは最初から一貫性を持って計画し、効率的に実行しなければなりません。ETAS と ESCRYPT は早い段階でこの課題を認識し、安全性や XiL メソッド、自動車セキュリティなどの各分野におけるノウハウを集約し、両者の長所を結集したソリューションを生み出しました（図を参照）。LABCAR ハードウェア、Linux ベースのシミュレーションターゲット LABCAR- RTPC（Real-Time PC）、および仮想 ECU ソリューション ISOLAR-EVE を基礎に構築した仮想テスト環境で、ECU インターフェースに対する攻撃や、ECU の諸機能を不正操作する試みを、車両全体を対象にシミュレートすることができます。

LABCAR を用いたセキュリティテスト

ETAS がテストシステムを提供する一方で、ESCRYPT は以下にあげるように、有意義なテスト手法を選択する際のセキュリティ関連の専門知識を提供します。

- **侵入（PEN）テスト**：このテストでは、外部からの介入で ECU の挙動を不正操作したり、無許可でデータを読み出

* XiL = モデル、ソフトウェア、ハードウェアインザループ（それぞれMiL、SiL、HiL）の総称



セキュリティテストシステムの基本構造

したり、組み込みシステムを破壊したりすることを試みます。半自動化された ETAS と ESCRYPT の PEN テストインザループでは、理想的なテストカバレッジを確保するために「攻撃ライブラリ」を利用します。このライブラリは、ESCRYPT のコンサルティングプロジェクトから得られる経験によって絶えず拡張されています。

- **ファジング**：ファザー（テスト実行ソフトウェア）は、ハッカーが ECU ポートをあふれさせようとして送り付けてくるランダム入力や意図的に操作されたコマンドを、自動的に生成します。ハッカーによる侵入や不正操作の試みをシミュレートする際は、一般的に、被験用 ECU のプロトコルやソフトウェアシステム、および暗号セキュリティに関する知識を一体化させて信号生成を行うことにより、テスト効率向上を図ります。

- **メッセージ認証（MAC）テスト**：認証済みのソースからの入力を用いてシステムにアクセスできるかどうかを調べます。このテストにおいてテストシステムは、暗号法の暗号鍵やカウンタを生成する機能や、復号時にそれらを解読するためのメカニズムを提供します。

このようなテストでは、個々の ECU や相互接続された複数の ECU の応答から車載 IT システムの脆弱性を系統的に検出することができます。理論上、テストベクタはほぼ無限に存在するので、これを現実的な数に絞り込む必要がありますが、そこで ETAS と ESCRYPT の真価が発揮されます。両者はシミュレーションやテストのためのツールを提供するだけでなく、テスト計画の準備や LABCAR テスト環境の設定に関する適切なサポートも提供しています。
ETAS の XiL テクノロジーと ECU アクセス用ツール（ETK など）は、包括的なセキュリティテストを行うために必要不可欠です。テスト担当者は、PEN、ファジング、および MAC テストの実行中に被験 ECU のメモリと内部データの処理に時刻同期でアクセスすることができ、被験 ECU の機能とプロセスを細部にわたって完全に追跡することができます。必要な範囲を深く分析できるのは、これらのリアルタイムメカニズムと拡張された監視機能があってこそのことなのです。

まとめ

ETAS と ESCRYPT は、自動車セキュリティと XiL ベースで行うテストの分野に関する専門知識を長年にわたって築き上げてきました。私たちはこれらの能力を融合させて ECU ネットワークの包括的防御を確実に行っています。XiL システムに有意義なテスト手順を組み合わせることで、セキュリティメカニズムの検証やセキュリティ脆弱性の検出に理想的に適合させることができ、セキュアな未来のコネクテッドビークルの実現に向けた重要なステップをさらに進めることができます。

次ページでは、
ESCRYPT Testing
Laboratoryが
コンサルティングと
サービスを提供している
各種のテストメソッドを
ご紹介します。