イーサネットのセキュリティ

Ethernet Security

執筆者
Norbert Fabritius
Ramona Jung
ESCRYPT GmbH
セキュリティエンジニア

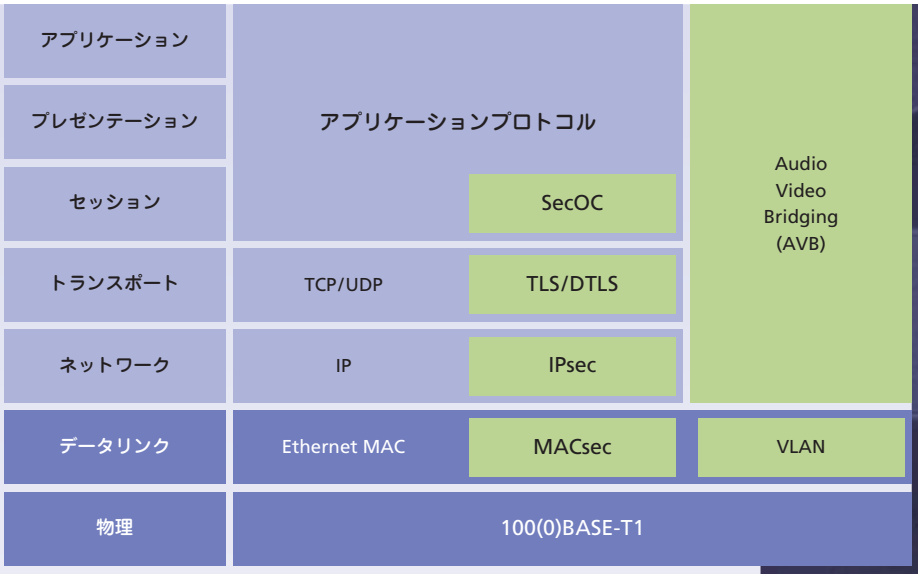
Dr. Jan Holle
ESCRYPT GmbH
セキュリティエンジニア&
プロダクトマネージャ

ESCRYPT は ETAS GmbH の 100% 子会社です。組み込みシステム向けのセキュリティソリューションを提供しています。

プロダクションキーサーバーによるセキュアな鍵管理

イーサネットは、データセンターやコンシューマーセクターで広く使用される IT 規格として 40 年以上にわたって定着しており、今や自動車業界も席巻しています。E/E アーキテクチャは当初、クロスドメイン通信を行わないシステムに適用されていましたが、今日ではドメインの境界を越えて展開されるようになっています。その結果、セキュリティや安全性、また確実な応答挙動時間をめぐってさまざまな問題が持ち上がり、実用的なイーサネットソリューションが求められています。

さまざまな安全関連プロトコル
（緑色の部分）



車載システムにおいては、データ転送の高速化が急ピッチで進んでいます。それに対応するため、CAN や FlexRay などの従来のバスシステムをサポートし、その安全を守る新しいイーサネットが業界内で新たに登場しています。インフォテインメント分野で生まれたイーサネットの技術は、今日ではクロスドメインの車載システムにも使用されるようになりました。

データバスがセキュアに、単独または他のデータバスとの通信で確実に機能するためには、十分に考え抜かれたロバストなソリューションが必要です。このソリューションは、従来のバスとのシームレスなデータ交換だけでなく、イーサネットコンポーネント間の通信にも対応できるものでなければなりません。必要に応じて、イーサネット（Ethernet）の規格を車載システムの具体的な要件に適合させることが非常に重要です。従来の IT ソリューションをそのままに、または少し修正するだけで使用できる場合もありますが、新しいソリューションを開発しなければならない場合もあります。その判断は、ビデオ信号などのような大量のデータを取り扱う際に、最大限のセキュリティや安全性、また確実な応答挙動時間を実現するために、どのような方法を選択するかによって決まります。

典型的 IT の諸問題とソリューション

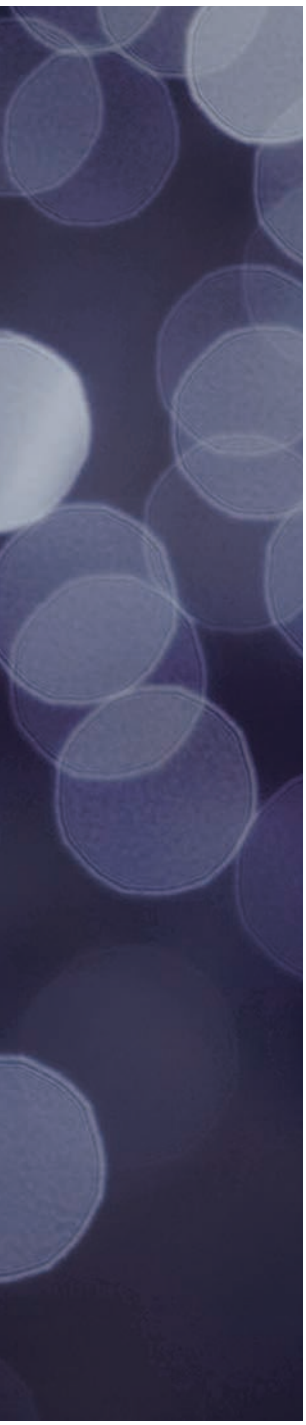
イーサネットの分散型構造により、冗長化または動的ネットワークパスを用いることで、単一障害点となる集中管理のエンティティの使用を回避することができます。ただし、この分散型構造そのものにも疑問が生じます。たとえば、イーサネットネットワークのすべてのメンバーが同じ特権を持っている場合、あるメンバーがネットワークに不正にアクセスしようとしているのを検知してそれを禁止するには、どうすればよいでしょうか。また、ネットワークマニピュレーションを識別して阻止するには、どうすればよいでしょうか。

この問題の対応として、たとえば仮想ネットワーク（VLAN）を使用してネットワークトラフィックの分配を行うようなソリューションの確立があります。本来、ネットワークポートは各種 VLAN のスイッチに割り当てられるものでしたが、今ではイーサネットフレームとポートに依存しない VLAN をマーク（「タグ」）によって関連付けることもできます。このタグ付けは IEEE 802.1Q 規格に規定されています。しかし、ネットワークトラフィックを論理的に分けるだけでは、不審なデバイスによるネットワークへの接続を防ぐことはできません。また、マニピュレーションやスパイ行為からも、条件付きでしかネットワークを保護することができません。これらの防御を完全に行うためには、暗号化認証または暗号化が必要です。この問題に対応する、昔ながらの IT ソリューションも存在します。初期のソリューションでは、データフォーマットや Transport Layer Security（TLS）などの規格を通じて上位のプロトコルレイヤに注目しましたが、その後のソリューションでは、さらに下位のレイヤに関するセキュリティメカニズムも追加されました。これには、IPsec による IP パケットの暗号化（レイヤ 3）や、MACsec（IEEE 802.1AE）によるイーサネットフレームの暗号化（レイヤ 2）が含まれます。これらのソリューションもまた業界標準により規定されています。

さらに、以下のようなセキュリティコンポーネントも利用できます。従来型のファイアウォールは、フィルタルールに基づいて、ネットワークまたはエンドポイントに出入りするパケットの許可をコントロールします。現代のバリアントはさらに、ディープパケットインスペクション（DPI）でトラフィック内のパケットのペイロードまでを分析して検査することができます。不正侵入検知システム（IDS）と不正侵入防御システム（IPS）はこれを基礎に構築されるもので、これにより管理者もコントロールオプションを使用できるようになります。

現代の車載ネットワークのセキュリティ要件

現代の車両のネットワークアーキテクチャと従来の IT で使用されていたネットワークアーキテクチャには、多くの類似点があります。しかし、技術基準や防御目標は両者の間で大きく異なります。



車両においては、搭乗者の安全と所有資産が最優先されるため、システムの可用性とネットワークトラフィックの信憑性が重要視されます。さらに、「ネットワークコンポーネントは事実上遅延なく決定論的手法でなければならない」という、車両運転におけるリアルタイムの重要性が関与します。
これらの要件は、データのパケット通信時間の保証を必要としない、パケットベースのネットワークがベストエフォート型のイーサネットの性質に明らかに反しています。また、車載 ECU の計算能力は限られているため、安全目標を達成してリアルタイム要件を実現するのは困難です。

このような理由から、定評のあるセキュリティ技術に修正を加えて車載ネットワークに実装するということはよくあります。たとえば、ネットワークのフェイルセーフ特性を強化するために VLAN を使用する場合があります。この場合、ネットワークを、それぞれ異なる防御が必要な複数の仮想ゾーンに分割し、それらの仮想ゾーンによって安全関連コンポーネントのネットワークトラフィックをリアルタイムに識別できるようにします。そうすれば、特定のトラフィックを必要に応じて他より優先的に扱ったり、他と分離したりすることもできます。優先度の高い VLAN 間の通信に対して優先的に帯域制限を行うことにより、サービス妨害（DoS）攻撃や故障コンポーネントで大量のパケットがネットワークに送り込まれても、スイッチ一つで阻止することができます。

ファイアウォールか、それより強力な IDS/IPS システムを使用することで、互いに異なる防御要件を持つ、隣接する IP ネットワーク同士をより確実に分離し、より正確に監視することが可能になります。それに対し、従来の車載バスシステムは、ブロードキャストメディアであるため、論理的に（つまり、追加の物理バスをインストールしないで）分離することはできません。

既存と新規のセキュリティソリューション

かつて TLS IT セキュリティプロトコルの使用には注意が必要でした。なぜなら、このプロトコルは車両のリアルタイム要件と相反する恐れがあったため、時間を重視しないバックエンドシステムやテスト装置との通信でしか使用を検討することができなかったからです。しかし、TLS 1.3 仕様では大幅な革新が見られました。接続の確立方法が最適化されたため（ゼロ RTT ハンドシェイク）、TLS で保護されたデータをハンドシェイク中の最初のパケットに収容できるようになりました。このため、TLS を使用してもラウンドトリップタイム（RTT）が無駄にかかることはなくなりました。事前共有鍵（TLS-PSK）を使用することで非対称処理が不要になるので、TLS のオーバーヘッドコストも劇的に低減することが可能になります。ただし、当面は、TLS のセキュリティ保証の弱点に関する可能性を念入りに検査することに重点が置かれています。

車両におけるリアルタイム要件は、非対称処理に基づく暗号署名を使用する場合に障害になります。データパケットの信憑性を保護するために、2014 年に AUTOSAR 4.2 の一環として Secure On-Board Communication（SecOC）モジュール仕様が発表されました。SecOC 仕様は非常に柔軟性のある内容なので、Ethernet/IP ベースのトラフィックにも適しています。

同様に、本来スピード重視のビデオデータの送信用に開発された Audio Video Bridging（AVB）のような、各種の Time-Sensitive Networking（TSN）規格も利用可能です。これらの規格は、イーサネットの通信でも適用されるもので、ネットワークリソースの予約、時刻信号の同期化、およびデータストリームの優先順位付けを管理する独自のメカニズムを規定しています。しかも、AVB は従来型のバスデータの伝送も可能です。この規格では、基礎的なテクノロジーとしてのイーサネットを拒絶することなく、リアルタイム仕様を伴う環境の要件を考慮することができます。AVB トランスポートプロトコルの最新バージョン（2016 年末期現在）は、送信されるペイロードデータの暗号化にも、比較的低いハードウェア要件で必要に応じて対応することができます。

車両におけるイーサネットのセキュリティ ― 開発と統合

イーサネットベースのソリューションを車載ネットワークに統合する動きは本格的に進んでいます。イーサネットの規格を使用すれば、将来の車両に期待される各種機能を実装することができます。しかも、この進歩は車両のセキュリティ要件に反するものでは決してありません。セキュリティの専門家による綿密なサポートとお客様に合ったセキュリティソリューションにより、セキュアなイーサネットアーキテクチャの実装を、きわめて複雑であるにもかかわらず成功させることが可能です。これを実現するために、ESCRYPT のイーサネットセキュリティと自動車の分野における長年の経験を活用することができます。このノウハウを生かし、実行可能なセキュリティ概念の構築と分析から、自動車業界のニーズに合わせてカスタマイズしたソフトウェアとハードウェアのソリューションを弊社の幅広い製品への実装まで、イーサネット統合の全段階にわたってお客様をサポートいたします。
イーサネット規格は、インテリジェントなセキュリティソリューションやセキュリティ製品に保護されながら、40 年以上にもわたるサクセスストーリーにエキサイティングな次章が書き加えられていきます。そして、それらの新たな章は、自動車業界において、かつてないほどの脚光を浴びるようになるはずです。