セキュリティをもっとセキュアに

More Secure Security

執筆者

Jan Pelzl 博士：
ESCRYPT 社
マネージング
ディレクター

Thomas Wollinger 博士：
ESCRYPT 社
マネージング
ディレクター

Car-2-Car 通信を不正アクセスから保護

Car-2-Car 通信は、次に路上走行にやってくる大進化です。車両同士がメッセージや警告をやり取りできるようになれば、危険を事前に察知して交通の流れにさらにうまく対処できるようになります。ただし、Car-2-Car 通信に使用されるオープンな通信インターフェースは不正なアクセスから守られなければなりません。メーカーや研究機関では、パイロットプロジェクト等を通じて、IT 分野で実績のあるセキュリティアプローチを活用しセキュリティ対策の開発に懸命に取り組んでいます。そして、ESCRYPT はその最前線にいます。

Car-2-Car(C2C)および Car-2-X(C2X)通信により、メーカーや OEM はスマートな技術を用いてドライバーをサポートし、事故を防げるようになります。将来、道路利用者は警告やメッセージのやり取りを直接、自動的に行うようになるでしょう。ドレスデン工科大学の輸送・経済研究所（The Institute for Transport & Economics at Technische Universität Dresden）は、全車両の少なくとも 10 パーセントが C2C 通信に対応するだけで、交通渋滞に起因する運行の遅れを半分以上も減らすことができると確信しています*。ドライビングダイナミクスに干渉する可能性のあるアプリケーションについては、利用者の信頼が絶対に必要です。やり取りされるメッセージの完全性および機密性は常に保証されなければなりません。これは、C2C 通信のオープンな無線インターフェースの性質とは逆の方向を目指す考え方です。メッセージが短距離無線通信で送受信されている場合、対応する送信器・受信器一式をセットアップすれば通常はだれでもその通信に参加できます。

公開鍵基盤（PKI）の中の認証局（CA）が鍵管理の中の大変重要な部分を担っています。ESCRYPT は鍵管理について必要な、暗号鍵を使用する最先端のソリューションを提供しています。ESCRYPT の「鍵管理ソリューション（Key Management Solution）」は、電子組込みシステムが認証、リリース、あるいは通信をセキュアに行わなければならないあらゆる場所で使用できます。このソリューションは、お客様自身で運用することもできますし、ESCRYPT による鍵管理サービスとしてご利用いただくこともできます。

課題

Car-2-Car 通信の利用者は絶え間なく動いている（走行）ため、交信時間を短くすることが必要です。通信インフラとの交信が保証されない可能性もあります。そのため、C2C 保護概念の重要なポイントとなるデジタル署名を従来の IT アプリケーションとは異なる方法で実装しなければなりません。走行中絶えずネットワーク経由で通信し、認証システムから証明書の発行・検証を行い、その証明書が有効か無効かを確実に判断できる方法が現状確立されてないので、証明書の有効期間を非常に長くする必要があります。また、車両とドライバーの移動プロファイルが不正に集計されるのを防ぐため、証明書を匿名化する必要があります。

車載装置は IT システムです

C2C 通信では、ある程度の TCP/IP プロトコルを使用します。攻撃者にとってはこれが侵入経路となり、攻撃者は十分に証明されたパケットフォーマットを不当に利用して多数のツールを使用することができます。PRESERVE や SEVECOM などといった研究プロジェクトは、できるだけ万能な防御アプローチを構築しようとしています。個々のシステム、データ、通信接続、および機能を分析し、その防御能力を完全性、可用性、および信憑性という保護目標に基づいて評価します。その結果、潜在的な攻撃者の動機および能力もまた、考慮された一連の保護要件カテゴリに定義されます。この徹底した分類により、保護方策をそのコストと有効性に応じて非常に効率的に策定することができます。

メーカー、研究プロジェクト、および Car-2-Car コミュニケーションコンソーシアム（C2C-CC）などの団体が、長年にわたって数多くのタスクに取り組んできました。2014 年 2 月には、ヨーロッパで欧州電気通信機構（ETSI）および欧州標準化委員会（CEN）により、ネットワークで結ばれた車両間の通信に関する基本的規格が発表されました。これらの団体は米国および日本にある同様の団体と協力し、無線周波数およびデータフォーマットを含む数々の事柄に関して合意に達しました。

*）出典： www.berliner-zeitung.de