まとめと提言

セキュリティは自動車メーカーにとって新しい問題で、なおかつ対策の重要性は高まる一方です。セキュリティと安全、信頼性は非常に密接に関連しており、もはや安全と信頼性を切り離して考えることはできません。車載システムがサイバー攻撃に対して脆弱であれば、その自動車を安全と見なすことはできなくなります。

最近の自動車にはインテリジェントな運転支援機能が多数搭載されており、これらのサブシステムは車載ネットワークで相互に接続されています。しかしネットワーク接続はそれ自体が1つのセキュリティ・リスクとなります。つまり、車載ネットワークの中でさほど重要性の高くないサブシステムであっても、その部分のセキュリティが弱いとそこからの侵入を許し、車両全体に攻撃が広がる可能性があります。

自動車のセキュリティ規格はまだ発展途上の段階にあります。とすると、盗難や悪意のある攻撃から車両を保護するために自動車メーカーは何をすればよいでしょうか。

機能安全と同様、セキュアな車載システムを実現するには、設計チーム内の文化を変革し、今までとは違った意識とスキルセットを持つ必要があります。たとえば、これまでFMEA（故障モード影響解析）などのツールを使用して部品の故障が車両全体の安全と信頼性に与える影響を理解していたのと同じように、サイバー攻撃の脅威とリスクを考慮してハッカーがシステムのどの部分を突いてどのような攻撃を仕掛けてくる可能性があるかを理解することが必要となります。

インターネットから車両にダウンロードされるマルウェアなど新しい脅威に対抗するには、企業ネットワークやエンドユーザーのコンピューティング機器のセキュリティ対策同様、自動車業界も継続的にセキュリティ・パッチを配布して最新の脅威にいち早く対応する方法を構築する必要があるでしょう。

自動車メーカーがセキュリティ・ソリューションを調達する際は、セキュリティを重視する文化を持ち、セキュアな製品の開発実績が豊富なサプライヤが提供するシリコン実証済みのものを選ぶことが重要です。

メーカーはソフトウェアのセキュリティと信頼性に関してベスト・プラクティスに基づいた方針を採用する必要があり、そのためにはソフトウェア開発プロセス全体でサイバーセキュリティへの対抗方針を示してくれるサプライヤを選ぶ必要があります。

ネットワーク型システムを設計する際は、最も脆弱なサブシステムを常に意識することが重要です。インフォテインメント・センターにも基幹サブシステムと同程度のセキュリティ対策をしておかないと、そこからハッカーが容易に侵入してさらなる攻撃を仕掛けてくる可能性があります。

セキュアなシステムを構築するためには、設計が完了した後でセキュリティ機能を付け足していくのではなく、仕様定義と設計の最初の段階からセキュリティを考慮したアプローチをとってゼロベースでシステムを構築する必要があります。設計段階からセキュリティを組み込んでおけば、無線経由で継続的にセキュリティ・パッチを配布して自動車の寿命の最後まで最新の脅威に対応できるようになります。

自動車に関するセキュリティ規格はまだ発展途上にあります。このため、自動車メーカーは組込みハードウェアおよびソフトウェアのセキュリティに関して豊富なノウハウがあり、ベスト・プラクティスについてのアドバイス、および脅威 / リスク・アセスメントのサービスを提供してくれる経験豊富なパートナーを選ぶことが重要となります。このようなアプローチをとれば、日進月歩で巧妙化する脅威に対して確実に対抗できるでしょう。

参考文献

※1 ウェブページ：The Telegraph "Thousands of cars vulnerable to keyless theft, according to researchers" By Rob Crilly. 18 Aug, 2015
http://www.telegraph.co.uk/news/uknews/11808814/Thousands-of-cars-vulnerable-to-keyless-theft-according-to-researchers.html

※2 ウェブページ：WIRED "Hackers Remotely Kill a Jeep on the Highway — With Me in It" By Andy Greenberg. 21 July, 2015
http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

著者紹介

Mike Borza：シノプシスのセキュリティIP担当テクニカル・スタッフ・メンバー。安全工学を手がけた後、20年以上にわたりセキュリティ・システム工学に従事。先ごろシノプシスが買収したElliptic Technologies社の設立者の1人で、同社CTOとして活躍。IEEE 802.1のセキュリティ・タスク・グループで積極的に活動中。過去には802.1ARセキュア・デバイスIDの規格編集も担当。prpl Foundationの設立メンバーであり、prplセキュリティ・エンジニアリング・グループの共同議長。マックマスター大学（カナダ）にて電気工学の修士号を取得。

Event / Seminar Report
イベント / セミナー・レポート

ご報告

IoTセミナー開催のご報告

2016年3月1日、東京コンファレンスセンター・品川にて「IoTセミナー」を開催いたしました。IoT エッジ・デバイス・マーケットにおけるシノプシスのWired / Wirelessインターフェイス、プロセッサ、そしてセキュリティ IPの各方向性と戦略のご説明に加え、ルネサス様、エーアイコーポレーション様、ベリフォア様よりIoTエッジデバイス向けに最適なDesignWare® ARC®プロセッサを活用したお取り組みの実例をご紹介頂きました。
非常に多くのお客様にご来場いただき、熱気あふれるセミナーとなりました。

オートモーティブ・ソフトウェア・フロンティア2016出展のご報告

2016年3月10日 ～ 11日、ソラシティ カンファレンスセンターにて開催された「オートモーティブ・ソフトウェア・フロンティア2016」に出展し、「ディープラーニングで実現する自動運転の将来」ならびに「車載ソフトウェア開発における脆弱性管理のアプローチ」と題した2つの講演を行いました。DesignWare Embedded Vision ProcessorならびにCoverity® / Defensics®、Protecodeをご紹介するブースにも多くの方に足をお運びいただきました。

ご来場誠にありがとうございました