自動車のセキュリティに対する脅威と対策への提言

シノプシス　セキュリティ IP担当テクニカル・スタッフ・メンバー　Mike Borza

車載アプリケーション向けIPを開発する際に設計チームが考慮すべきセキュリティの重要な問題点について、シノプシスのセキュリティ IP担当テクニカル・スタッフ・メンバーのMike Borzaがご説明します。

最近の自動車はあらゆる面でネットワーク化が進んでおり、サブシステムおよびSoCを設計する際には従来の物理的な安全対策だけでなく、より広範な安全対策が必要となってきます。最新のコネクテッド・カーは、ボディおよびパネル・サブシステムから、自動車電子制御装置（ECU）、先進運転支援システム（ADAS）、インフォテインメント・プラットフォームに至るまで、ハッカーによるセキュリティ攻撃の標的となりうる要素が多数存在します。日進月歩で巧妙化するセキュリティ攻撃の脅威に対して常に最新の対抗策をとるには、脅威の種類、システムが抱える脆弱性、最新の標準規格について理解しておくことが重要です。

自動車のセキュリティに対する脅威

最近の自動車は単なる移動の手段ではなく「走る高性能コンピュータ」へと進化しており、外部環境との接続によって自宅やオフィスと同じ環境を再現できるようになっています。このため自動車も、ノートPC、スマートフォン、企業ネットワークがこれまで受けてきたのと同じようなセキュリティ攻撃に脅かされるようになっています。しかも実際にセキュリティ攻撃を受けた場合の被害は甚大で、車両盗難はもとより、ドライバーと同乗者の安全が脅かされる危険があります。また、法的訴訟によって自動車メーカーのブランドが失墜する危険もあります。

ハッカーが電子システムのセキュリティを攻撃する動機や手段はさまざまです。現在最も一般的なのは、車両の窃盗という単純な動機による攻撃です。ロンドン警視庁によると、昨年イギリス国内で盗難被害にあった車両の半分がキーレス車両であったと推定されています※1。ドライバーの利便性を高めるため従来の機械式キーから無線方式のキーレス・イグニッション・システムへの移行が進む中、暗号メカニズムの強度が十分でないとスマート・キーと車両との間でやりとりされる信号が傍受・解読される可能性があります。

車両の盗難以外にも、自動車には金銭目的で行われるセキュリティ攻撃がいくつかあります。たとえば、中古車を不正な価格で販売するために自動車のオドメーターを改ざんして走行距離を戻すという古典的な不正行為は、今やハッカーの仕事となっています。また、駐車料金や高速料金の支払いに使用するモバイル決済システムも自動車への搭載が進んでいます。ドライバーの携帯電話と自動車が接続するようになると、自動車への攻撃を足場にして携帯電話の銀行アプリやその他の個人情報を攻撃することが可能になります（もちろんその逆方向の攻撃もありえます）。また、自動車の現在地を追跡すれば所有者の自宅を突き止めることはもちろん、いつ留守にしているかも分かるため、家屋への侵入も容易になります。これ以外にも、窃盗目的の攻撃の標的となる弱点は数多く存在します。

企業ネットワークが攻撃を受けた場合と同様に、自動車がセキュリティ攻撃を受けた場合も、攻撃者からの脅迫、不信感を募らせた購入者や車両の誤動作を経験した被害者からの訴訟などによってメーカーのブランドが失墜する可能性があります。しかも攻撃は金銭目的だけとは限りません。走行

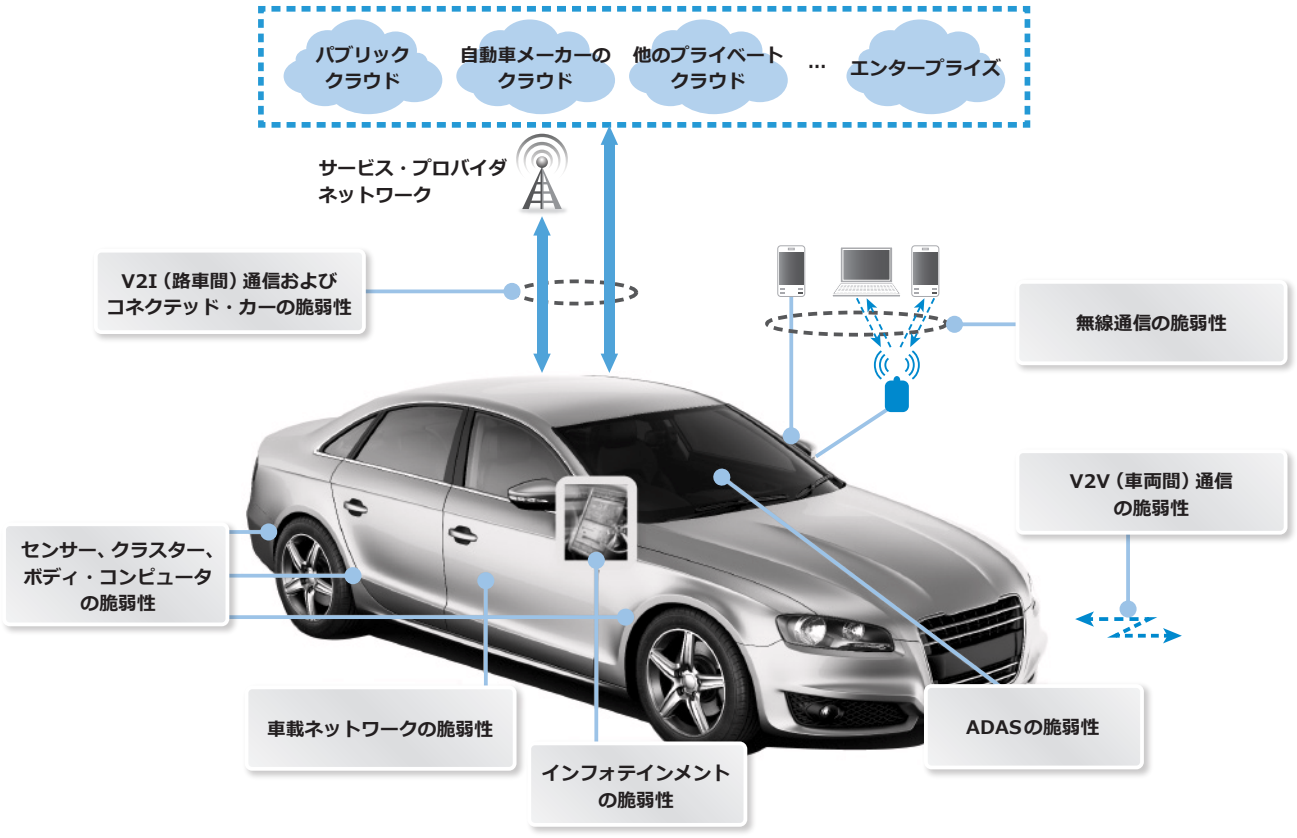

図1. 自動車のセキュリティに対する一般的な脅威

次ページに続く▶

前ページより続く ▶

中に車両の基幹サブシステムが乗っ取られると、個人または公衆の安全が脅かされることになります。

サブシステムの脆弱性

車両内のいたるところに電子システムが搭載され、サブシステム同士の通信が増えるにつれ、自動車が攻撃を受けるリスクが高まっています（図1 P3掲載）。また、車載ネットワークに多くの機能が接続されるようになると、1つのサブシステムへの攻撃が成功した場合、そこを足場にして別のサブシステムが攻撃され、さらに被害が拡大します。実際問題として、1つでもセキュリティが不完全なサブシステムがあると、そのサブシステムに接続している別のサブシステムに意図せぬ影響が及び、最終的には車両全体が被害を受けます。

自動車メーカーは、ADAS、コネクテッド・カー、V2X（車両間、路車間、車両・歩行者間、車両・住宅間など）通信、インフォテインメントなど主要な車載アプリケーションのすべてに包括的なセキュリティ対策を講じる必要があります。

先進運転支援システム（ADAS）

ADASは非常に高い安全性が要求されるシステムであるため、バックアップ・カメラ、死角検出システム、車線逸脱検出システムなどの機能を担うIPを含め、万全のセキュリティ対策が必要です。ADASは車載インフォテインメント・システムとも接続されており、ADASの情報はインフォテインメント・システムのディスプレイに表示されます。したがってインフォテインメント・システムに脆弱性があるとそこから車載システムへの侵入を許し、次々とサブシステムが乗っ取られる可能性があります。

コネクテッド・カー

自動車メーカーは、車室内でも自宅と同じ体験が得られる自動車の開発に取り組んでいます。その目標を達成する上で鍵となるのが、車両に内蔵されたネットワーク接続機能です。Apple®、Google™、Microsoft®の各社が発表しているコネクテッド・カー・プラットフォームは、モバイル機器の機能、インフォテインメント、自動車アプリ、デジタル診断 / 監視、高度なナビゲーション機能を車載コンソールから利用できるようにすることを目指しています。

コネクテッド・カーは、メーカーからのアップグレードがハッキングされたり、ウイルスやマルウェアに感染したコンテンツやアプリをオーナーがダウンロードしたりと、さまざまな形でセキュリティ侵害を受ける可能性があります。もちろん、テレマティクス・システム自体も攻撃を受ける可能性があります。

V2X通信

V2Xとは、車両間通信（V2V）や路車間通信（V2I）のほか、車両と歩行者（V2P）、車両とクラウド（V2C）などの通信を総称した用語です。V2Xの中心的な考え方とは、自動車が他の車両や周辺環境と情報を共有してより安全で効率的な運転を実現しようというものです。V2Xによって実現する利点として、衝突回避、渋滞緩和、交通管理、一般道路の利用効率改善、歩行者の安全、駐車場やガソリンスタンドなどのサービスへのアクセスなどがあり、そう遠くない未来に自動運転も実現するでしょう。しかしセキュリティが万全でないと、V2Xインターフェイスもサイバー攻撃の入口として利用される可能性があります。

インフォテインメント

インフォテインメント・センターはドライバーや同乗者にとって特に関心の高い機能で、高性能なコンピュータとタッチスクリーン・インターフェイスを組み合わせて実装されます。通常、このディスプレイは他のサブシステムと共用します。インフォテインメント・システム自体にはそれほど高い安全性は求められませんが、車載ネットワークに接続しているためセキュリティ攻撃の入口として利用される可能性があります。

車載ネットワーク

燃費改善の要求が高まる中、自動車メーカーはあらゆる手を尽くして車両の軽量化に努めており、現在の自動車で2番目に重量の大きいサブシステムはワイヤーハーネスとなっています。ケーブルの重量を最小限に抑えて車載ネットワークを実装するためにEthernetを共有する方法が一般的となりつつありますが、従来の車載バス規格CANよりもEthernetやLANテクノロジの方が攻撃の手口が多く知られており、システムはより多くのサイバー攻撃にさらされることになります。

物理的な配線は必ず攻撃に対して脆弱であるため、上位層に独立したセキュリティ・アプローチを開発する必要があります。そのためにはデータおよびネットワーク・デバイスに暗号化 / 認証を導入し、分散型のインテリジェントなセキュア・ネットワーク内で相互識別および認証を実行する必要があります。事実、最近では侵入検知 / 修復などのネットワーク防御手法が車載ネットワークにも採用される例が増えています。

ソフトウェア

自動車のソフトウェア・システムもハッカーによる攻撃の入口として利用される可能性があります。このことは、2015年に発表されたJeep®へのセキュリティ攻撃実験[※2]で証明されています。これは、セキュリティ研究者たちが10マイル（約16km）離れた場所からノートPCと携帯電話だけを使って車両のオンボード・システムにアクセスして車両の制御を乗っ取ることに成功したというものです。

研究者たちが攻撃の標的としたのは、エンターテインメント・システム、ナビゲーション、ハンズフリー通話を制御する「Uconnect®」ソフトウェアです。ダッシュボード・コンピュータで実行されるこのソフトウェアから自動車のシステムに侵入し、エアコン、カーラジオ、ワイパー、エンジン、ブレーキを乗っ取り、最後には車を減速させて路肩に停車させました。

セキュリティ規格

自動車に関するセキュリティ規格は全体的にまだ発展途上にあります。機能安全規格のISO 26262およびそのASIL分類は1つの基準点となりますが、セキュリティに照準を合わせた具体的な標準の規格化はまだ流動的で、固まっていません。

EUプロジェクトのEVITAからは、セキュリティ関連コンポーネントの改ざん防止、および攻撃からの秘匿データ保護に関する車載ネットワーク設計ガイドラインがいくつか発表されましたが、これらはすでに内容が古くなっています。

暗号鍵の安全な格納方法、暗号アルゴリズム・アクセラレーション、セキュア・ブート・メカニズムなどについて自動車メーカーが共同で策定したHIS-SHE規格もあります。また、SAE（Society of Automotive Engineers）が策定を進めているJ3061規格の「Cybersecurity Guidebook for Cyber - Physical Vehicle Systems」では、これら問題の一部についての対策が取り上げられています。

TPM（Trusted Platform Module）もまだ議論が続いており、発展途上の規格です。また、CAMP、Car 2 Car、ITSなど地域単位のコンソーシアムもありますが、これらの団体が自動車のセキュリティ標準規格をどのように推進していくのかについての詳細は、情報がほとんどありません。

現在は、個々のメーカーが独自の裁量でリスク・アセスメントを実行した後、公開されているガイドラインを参考にするか、または最新の標準規格とベスト・プラクティスを熟知した経験豊富なセキュリティ・パートナーの協力を仰いで製品の計画と開発を行っています。

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。