未来のクルマを守る！
IBM Research LabのIoTセキュリティー最前線

Associate Director,
IBM Cybersecurity Center of Excellence,
IBM Research
Yaron Wolfsthal

ベン・グリオン大学にあるIBM Cybersecurity Center of Excellenceセンター長として、多国籍の研究チームを率いて最先端のソリューション開発を行っている。IEEEシニア・メンバーであり、50以上の著作がある。コンピューター・サイエンス博士、経営学修士（MBA）。

Global Solution Leader for Vehicle Security,
Business Development & Strategy
Global Automotive Industry,
IBM Germany
Giuseppe Serio

コネクテッド・カーのセキュリティーに関するIBMグローバル・ソリューション・リーダー。自動車業界を中心としたさまざまなフィールドにおける25年以上の経験と専門知識を基に、IBMのクルマのセキュリティー・ソリューションに関するビジネス開発およびストラテジー策定に注力。

Security Researcher,
IBM Cybersecurity Center of Excellence
Yair Allouche

IBM CCoEのセキュリティー・リサーチャー。コネクテッド・カーに関するセキュリティー・ソリューションの開発に従事。2013年、ベン・グリオン大学にて通信システム工学科の博士号を取得。

はじめに

19世紀の終わりに自動車が登場して以来、自動車業界は市場の要求に応え続けてきました。その結果、自動車は最先端のエレクトロニクスやITを組み込み、自動車に乗る人々に快適さとエンターテインメントを実現する高性能な移動手段へと進化しました。特にここ数年、「つながるクルマ（コネクテッド・カー）」はネットワーク社会を支える基盤の一つと位置付けられ、関連する付加価値サービスが次々と生み出されています。コネクテッド・カーがもたらす新しい価値は、みるみるうちに業界に浸透し、2020年までに2億5000万台ものコネクテッド・カーが出荷されると予測されています[1]。ステークホルダーが享受できるコネクテッド・カーのさまざまな付加価値サービスには、**表1**のようなものがあります。

コネクテッド・カーに潜むリスク

もともと純粋な機械に過ぎなかった自動車は、いまや車輪の付いた複雑なITデバイスと言えるほどに進化しています。これにより、コネクテッド・カーには前述したような進歩や利点が生まれましたが、一方でセキュリティー侵害のリスクやデータ・プライバシーに関する懸念も存在することになりました。

表1. コネクテッド・カーの付加価値サービス例

ステークホルダー	付加価値サービス例
自動車オーナー	ソーシャル・ナビゲーション（例：渋滞情報をシェアできるアプリWaze）、個人向けにカスタマイズされたインフォテインメント、自動運転サポート
自動車メーカー	新しいビジネス・モデルと収益（例：自動車保険用の実走行距離連動型（PAYD）モデル）、アフターマーケット・サービスの変革（例：修理時期の予知）、OTAによる車載コンピューター（ECU）のファームウェア・アップデートの実現
企業	リアルタイムのフリート・マネジメントなど、最適化された輸送サービス
地方自治体	渋滞管理や排ガス規制などのスマート・シティー・サービス

自動車メーカーにとっては、ドライバーの安全が常に最重要事項であり、これまでに車線維持システムや横滑り防止装置、アンチロック・ブレーキ・システムといったドライバー支援システムが開発されてきました。ここ10年間で自動車に乗る人の安全は劇的に向上しましたが、自動車がインターネットにつながり外部から自動車内部にアクセスできるようになったことで、自動車メーカーにとってサイバー・セキュリティーのリスクが現実的な問題となっています。

コネクテッド・カーは人類が開発した非常に複雑なソフトウェア駆動型システムの一つであるため、現代の自動車はサイバー・セキュリティー・リスクに直面することになりました。現在の標準的な高級車には、1億行ものソフトウェア・コードが組み込まれており[2]、これは、スイスにある世界最大の大型ハドロン衝突型加速器を動かすソフトウェアの約2倍のサイズに相当します。車載ソフトウェアおよびファームウェアは、車載制御ネットワーク(Controller Area Networks、以下CAN)に接続されている70〜100個もの制御用コンピューター(Electronic Control Units、以下ECU)を管理しています。また、自動車は現在、自分以外の車やインフラストラクチャー・システムと接続するために複数の通信プロトコルを使用しています。コネクテッド・カーはさまざまな通信機能(Bluetooth、USBポート、近距離無線通信など)を有しているがゆえに、さまざまなサイバー攻撃の脅威にさらされていると多くの研究者が明らかにしています[3]。

これまで度々公表されているとおり、大手自動車メーカーの多くは、自動車に内在するセキュリティーの脆弱性をハッカーに攻撃されています。報道によると、自動車メーカーがセキュリティー・パッチを適用するために行ったリコールの対応費用は1億ドルに上るとも言われており、これは企業価値の損失にもつながります。

セキュアなコネクテッド・カーを実現するためのアプローチ

自動車業界は、セキュアなコネクテッド・カーを実現するための研究開発に多額の投資をしています。複数のベンダーが追究しているのが、車両向けに特化した侵入検知システム(Intrusion Detection System、以下IDS)です。組み込みデバイスとして実装されているIDSは、精巧な解析アルゴリズムによって自動車内の通信ネットワークを常時点検するもので、脅威が検知されると、通信チャネルをブロックしたりアラートを上げたりするなどの措置がとられます。また、コネクテッド・カーの設計上の制約として、おのおののECUに個別にセキュリティー対策を講じることは技術的に難しいため、対象となるECUを鳥瞰的に保護できるIDSは、現時点で最適なソリューションの一つであると言えます。

車載IDSというアプローチにはメリットもある一方で、制約もあります。車載IDSは、主にCANバスを介したECU間の通信トラフィックを検知し判別します。特にIDSが高度な分析手法と十分な経験則を有していれば検知した情報は有効と言えますが、車両自体の分析から得られる洞察は、コネクテッド・カーに対するセキュリティー・イベントの一部でしかありません。このアプローチで検知できる攻撃もいくつかありますが、結託攻撃などIDSでは検知されない巧妙な攻撃も多く存在します。

また、自動車メーカーのコスト軽減目標や消費者の高価格への抵抗感によって、デバイスに使用するプロセスやメモリーといったリソースにも制約が生じます。そのため、車載IDSが実現するセキュリティーのパフォーマンスと品質には限界があるのです。

大局的には、コネクテッド・カーの包括的なセキュリティー・ソリューションを実現するためには、これらの相反する要求を調整し、デザインにおけるさまざまな課題に取り組むことになります。前述のとおり車両レベルで検知できる脅威は限定的で、車車間ネットワークの動的な変化や拡張性を鑑みると、サーバーに車両のセキュリティー・データをアップロードしたりネットワークを管理したりするには膨大な処理能力・通信コストがかかってしまいます。そのため、サーバー・ベースのアーキテクチャーも適切な

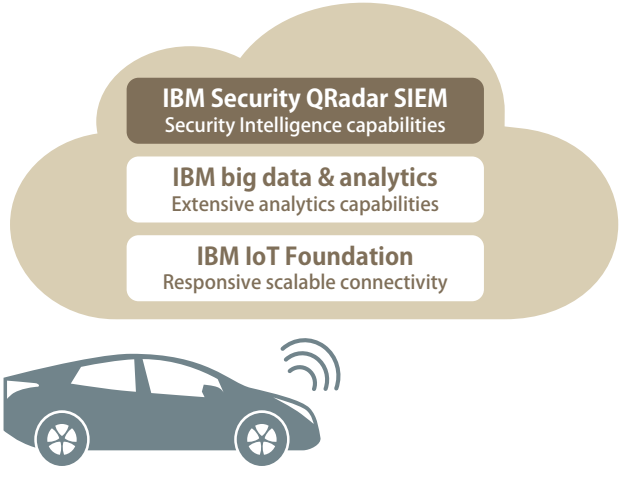

図1. 未来のクルマを守るIBM Researchの最新ソリューション

ソリューションとは言えないでしょう。包括的でリアルタイムなセキュリティーを実現するソリューションという観点では、デザイン段階におけるこれらのトレードオフを調整し、さまざまな機能を統合していくことが重要です。

IBM Research Labが発表した革新的な侵入検知システム

IBMは2015年9月、ドイツのフランクフルトで開催された国際モーター・ショー(IAA2015)[4]で、セキュアなコネクテッド・カーを実現するソリューションのプロトタイプを発表しました。イスラエルにあるIBM Cybersecurity Center of Excellenceの研究[5]に基づいて開発されたこのソリューションは、車載コンポーネントとクラウド上のサーバー・コンポーネントが通信するクライアント・サーバー・アーキテクチャーです(**図1**)。このソリューションは、異常検知における斬新なアプローチを採用し、車両内部だけではなく車車間ネットワークの健全性を損なわせる攻撃を識別できます(**図2**)。

またこれは、広範囲にわたる攻撃対象領域を想定したエンド・ツー・エンドのセキュリティー・ソリューションで、自動車のセキュリティーとプライバシーに関する以下の点を特に考慮しています。

- CANバス上のデータの改ざんを防止する(耐タンパー性)車内ネットワーク・セキュリティー
- OTA(over-the-air)アップデートを含む、車外ネットワーク接続の保護
- ECU、インフォテインメント・アプリ、モバイル・アプリ、Webポータル/ゲートウェイAPIなどのアプリケーション・レベルのセキュリティー

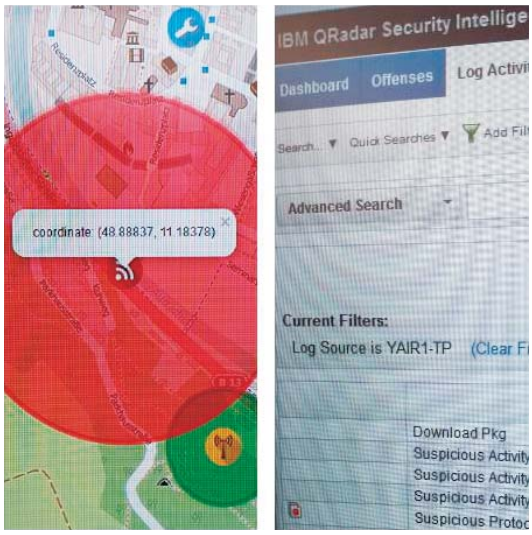

図2. IBMの最新ソリューションによってキャプチャーしたジャミング攻撃

IBM Cybersecurity Center of Excellenceとは

イスラエルにあるIBM Cybersecurity Center of Excellence(CCoE)は、2014年にネゲブのベン・グリオン大学キャンパス内に創設されました。

このセンターでは、大学研究者、政府機関、お客様、パートナーと協業しながら、次々に出現するサイバー攻撃の脅威とこれに対抗するソリューションを研究しています。CCoEが注力する技術領域には、セキュリティー分析、クラウドおよびネットワークのセキュリティー、安全なアプリケーション開発、生体認証、コグニティブ・サイバー保護、コネクテッド・カーのセキュリティーなどがあります[5][6]。

- 権限のあるユーザーのみが車両とデータにアクセスするためのID管理
- 車載用インフォテインメント・システム(例:Apple社のCarPlayなどで、頻繁にモバイルOSが更新される)や消費者向けモバイル・アプリに対するモバイル・セキュリティー

終わりに

コネクテッド・カーを総合的に守るためには、いくつかの基本機能が必要です。例えば、車両単体と車車間ネットワークの双方から効率的にセキュリティー・イベントを収集して記録する機能や、車両内、車車間、さらには交通インフラ全体の異常を検出できるセキュリティー分析アルゴリズムなどです。

IBMがIAA2015で発表したこの侵入検知システムは、アナリティクス、クラウド、セキュリティーに関する革新的な技術が組み合わされています。これこそIBMの強みであり、コネクテッド・カーをサイバー攻撃から守るための画期的なソリューションです。このシステムは、大切な資産である自動車を目に見えない未知の攻撃者から守り、ハッキングからのリカバリーを可能にする、リアルタイムの総合ソリューションなのです。

[参考文献]
[1] Gartner: Press release January 26, 2015, http://www.gartner.com/newsroom/id/2970017
[2] information is beautiful: Codebases, http://www.informationisbeautiful.net/visualizations/million-lines-of-code/
[3] Checkoway,S., McCoy,D., Kantor,B., et al.: Comprehensive Experimental Analyses of Automotive Attack Surfaces, http://www.autosec.org/pubs/cars-usenixsec2011.pdf
[4] IAA 2015, http://www.iaa.de/en
[5] IBM Cyber Security Center of Excellence, https://www.research.ibm.com/haifa/ccoe/index.shtml
[6] Cyberspark web site, http://www.cyberspark.org.il/