Panasonic
AUTOMOTIVE

パナソニック株式会社
〒571-8501 大阪府門真市大字門真1006番地

2017年10月10日

自動運転・コネクティッドカーに必須となるサイバーセキュリティ技術

サイバー攻撃に対抗する
オートモーティブ侵入検知・防御システムを開発

【要旨】

パナソニック株式会社 オートモーティブ＆インダストリアルシステムズ社は、自動運転・コネクティッドカーに対するサイバーセキュリティ対策を実現するオートモーティブ侵入検知・防御システムを開発しました。コネクティッドカーは、インターネットに接続されるため、現在のITシステム同様、世界中からのサイバー攻撃にさらされる可能性があります。
本システムを適用することで、サイバー攻撃をリアルタイムに検知すると共に、検知したサイバー攻撃を防御することが可能となります。また、自動車はライフサイクルの長い商品であり、出荷時に想定していた攻撃よりも進化した攻撃にさらされる可能性があります。本システムを適用することで、進化した攻撃の情報をクラウド側で収集すると共に、対策した新しいルールを自動車に配布・更新することで進化した攻撃も検知できるようになります。

【効果】

サイバー攻撃による車載システムへの攻撃やウィルス等の侵入を検知し、防御システムが攻撃やウィルス等を駆除・無効化することにより、自動運転車・コネクティッドカーの安全走行を確保します。また、今後の車載セキュリティの法規制化への対応が容易となります。

【特長】

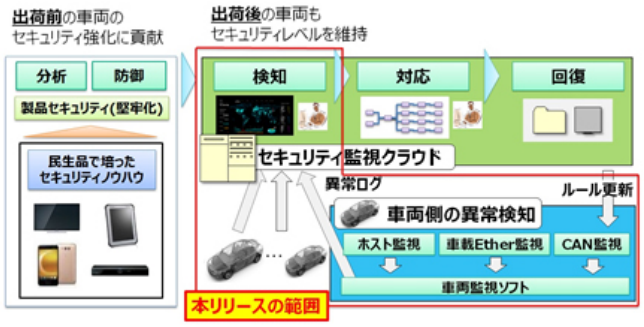
本開発システムは以下の特長を有しています。

1. 攻撃の初期段階であるインターネットからの侵入、さらに第二段階である車載ネットワークへの侵入を検知できます。
2. 車載ネットワークとして、広く普及しているCAN※1に加えて、今後の普及が見込まれるEthernet※2にも対応しており、車両全体の侵入を網羅的に検知することが可能です。
3. 複数の車載機からの情報をクラウドに集約することで、攻撃がセキュリティの脅威として顕在化する前に検知が可能です。

【内容】

本システムは、車載機に搭載する「監視モジュール」及び監視モジュールと連携する「監視クラウド」から構成されています。車載機の監視モジュールは、監視ルールに基づいて車両内部を監視します。既存の監視ルールでは検知できない攻撃を発見した場合、監視クラウドから車載機の監視モジュールの監視ルールを変更・更新することで、新しい攻撃にも対応できるため、出荷後も車両の安全を維持することができます。また、セキュリティの脅威として顕在化する前から攻撃の予兆を捉えることで、対策検討を先んじて実施することも可能となり、攻撃の影響を最小限に抑えることが可能となります。

■オートモーティブ侵入検知・防御システムのイメージ図



【特長の詳細説明】

(1)車載機型ホスト侵入検知技術:攻撃の初期段階であるインターネットからの侵入を検知する独自技術であり、インターネット接続機器(IVI/TCU※3)に搭載して利用します。Linux等のOSや各種セキュリティ機能より取得可能なログの中から明確に攻撃と分かるものに加えて、単独では攻撃と分からない挙動情報を複数組み合わせて攻撃を判断できます。

(2)車載機型CAN侵入検知技術:攻撃の第二段階であるCAN通信への侵入を検知する独自技術であり、CAN接続機器(ECU)に搭載して利用します。利用方法としては、①搭載ECUが受信する不正なCANコマンドをフィルタリングするCANフィルタ、及び②搭載ECUが接続する全てのCANバスを監視して不正コマンドを検知するCAN監視があります。車両の様々な状態を考慮してコマンドの不正を判定するため、ある条件の下では誤検知をほぼ無視できる値に抑えることが可能です。また、単一のコマンド毎に不正判定ができる為、検知後のリアルタイムな防御動作に繋げることも可能です。

(3)車載機型Ethernet侵入検知技術:攻撃の第二段階であるEthernet通信への侵入を検知する独自技術であり、Ethernet接続機器(ECU)に搭載して利用します。搭載ECU(Ethernet Switch ECU等)が受信又は中継する不正なEtherフレームをフィルタリングするEtherフィルタとして利用できます。判定方式は、フレームのヘッダを中心に解析することで軽量に不正判定ができる俯瞰方式と、フレームのデータを中心に解析することで、負荷はかかりますが、より正確に判定できる詳細方式があります。また、これらを組み合わせることで柔軟な検知が可能です。

(4)クラウド型車両侵入検知技術:複数車両の車載機から収集する大量のログを機械学習により解析する独自システムであり、クラウドに配置して利用します。利用方法としては、事前に学習した車載ネットワークモデルにより自動的にセキュリティ上の脅威となる可能性のあるログのみに絞り込んだ後、攻撃分析官が実際に絞り込んだログのみを分析します。また車載機型の各侵入検知技術と連動させることで、攻撃が顕在化する前の予兆を捉えることも可能とします。

※1 CAN(Controller Area Network):CANは自動車用に開発された耐ノイズ性の高いシリアル通信
プロトコルで現在の自動車はCAN通信を介した車載ネットワークを利用し車両全体のECU間通信を行っている。

※2 Ethernet:これまでオフィスや家庭で利用されてきたネットワーク規格で、自動車内のECUや電装品同士の通信に利用することでデータ伝送の高速化、大容量化が期待されている。またIPベースでデータをやり取りできるので外部ネットワーク(クラウド)との連携がより容易になる。

※3 IVI/TCU : IVI(In-Vehicle Infotainment):車載インフォテインメント機器
TCU(Telematics Communication Unit):通信制御コントロールユニット

【参考情報】

本システムは以下の学会展示会で発表及びデモンストレーションを実施予定

・ITS World Congress 2017 (カナダ) / 2017年10月29日～11月2日

・escar EU (ドイツ) / 2017年11月7日～11月8日

以上