モノのインターネット

自動車向け IoT セキュリティ

最も一般的な攻撃に対する防御

自動車向け IoT セキュリティ

最も一般的な攻撃に対する防御

進化する攻撃者

過去数十年間の情報セキュリティの分野で、1 つのパターンが浮上しています：それは、攻撃者優位の状況が続いており、その勢力が急速に拡大していることです。今日では、コンピューターシステムに侵入するツール、情報、技術が今まで以上に入手しやすくなりました。これに対して、コンピューターシステムの防御には継続的な努力、強固なハードウェアアーキテクチャ、熟練したエンジニアが必要となりますが、多くの場合は不十分な状態となっています。

5 年前にラスベガスで開催された Black Hat Briefings で、Lab Mouse Security の Don A. Bailey は、史上初のリモート操作による車両ハッキングの事例を報告しました。今日、世界最大のハッカーコンベンションの 1 つである DEF CON では、車両ハッキングに特化したワークショップが開催され、ハードウェアツール、無料ソフトウェア技術、複雑なセキュリティコントロールをバイパスする典型的な戦略が紹介されています。

ハッキングへの関心が高まるにつれて、プロの情報セキュリティ研究者が守るべき倫理上の境界線内にとどまる人ばかりではなくなりました。一線を超えてしまう人もおり、明らかな脆弱性が存在する場合、自らの利益となる操作を行おうと犯罪者たちが集まってくるでしょう。

攻撃者の中には、「ランサムウェア」と呼ばれる新しいマルウェアの一種を利用して、被害やが「身代金」を支払うまで主要システムへのアクセスを制限する者もいます。このような攻撃の多くは、重大な損害をもたらす恐れがあります。

例えば、2015 年 12 月には、ウクライナの小さな地域において、送配電網を運用するための電気設備に侵入したマルウェアが 3 週間の停電を引き起こしました。

このマルウェアは 2007 年からインターネット上で広がり始めましたが、最近では産業用のコントロールシステムを操作不能にしたり、ハードウェアに損害を与えるまでに進化しています。上記の事例は、ハッカー攻撃による世界初の停電事故でした。

モノのインターネット（IoT）が発展し、産業用システム間のつながりが強化されるようになると、このような攻撃はますます増加すると考えられます。エンジニアと経営者は、自分たちの IoT ソリューションが攻撃される可能性ではなく、いつ攻撃が発生するのかを自問する必要があります。このような攻撃に対して効果的な防御を行い、全体的なセキュリティ技術を強化する唯一の方法は、開発当初からソリューションにセキュリティを組み込むことです。

攻撃パターン

攻撃者は、IoT を支える産業や技術から生まれた様々な手段に基づいて作られた IoT ソリューションをターゲットにする傾向があります。

IoT は本質的に、物理的につながっているコンピューターシステムが革新的な新しいサービスを提供することを可能にする、クラウド、ネットワークパーシステンス、埋め込み技術の組み合わせであります。言い換えれば、IoT は既存技術を使用して相互作用と自動化を可能にすることを意味します。

そのため、攻撃者は確立されている戦略と既存のツールを利用して、IoT ソリューションの脆弱性を特定することができるのです。

図 1 は、自動車向け IoT ソリューションを構成する可能性のあるコンポーネントの一部を示しています

図 1 – 自動車向け IoT のコンポーネントと機能

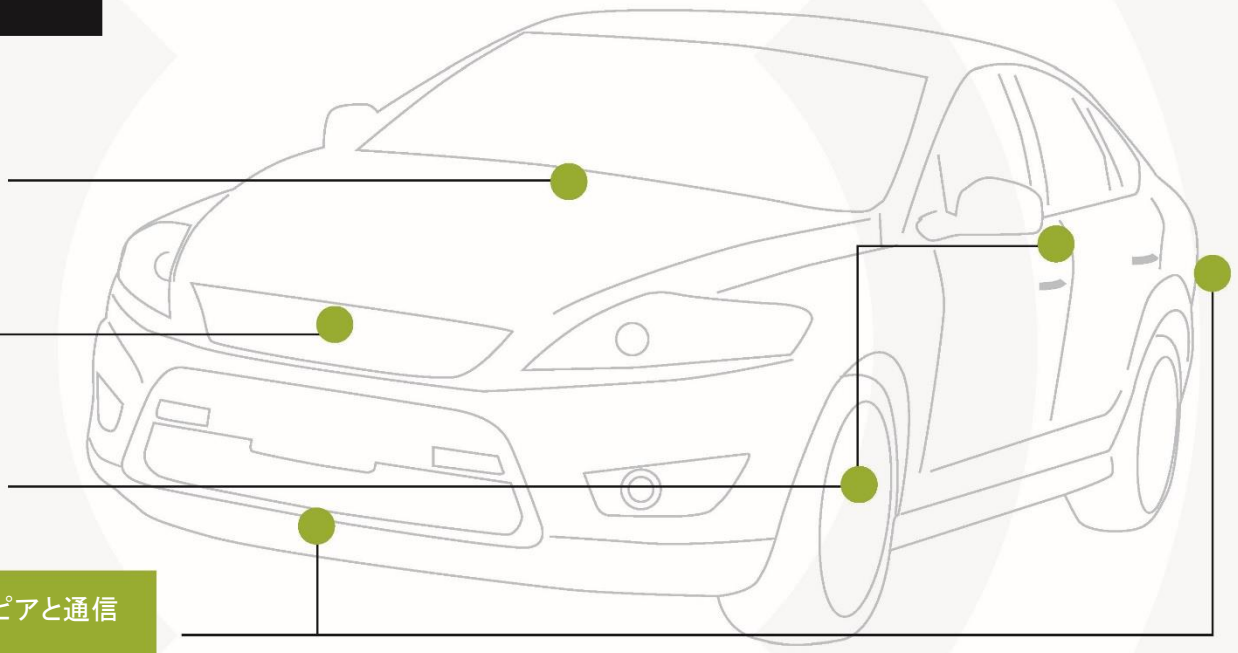
最新の自動車向け IoT の機能

最新のテレマティクスシステムがデータを収集し、エンターテイメントを提供するとともに、診断結果の可視化を実現

中央コンピューターシステムがリアルタイムでの意思決定を誘導

センサーが道路状況を感知して、安全な経路に誘導

ワイヤレスコミュニケーションシステムが近くのピアと通信を行い、安全上重要なメトリクスと警告を伝達



IoT 技術への攻撃に使用される一般的な戦略:

- ピア認証の脆弱性
- 実践的な暗号の改ざん
- エンドポイントの完全性(インテグリティ)の差
- 重要なアプリケーションと重要でないアプリケーションのセグメンテーションの欠如
- ソフトウェアアプリケーションの欠陥
- ビジネスロジック上の弱点

知識のある攻撃者であれば、物理的なデバイスが隔離されたコミュニケーションネットワークに最も侵入しやすいポイントであるということは誰でも承知しています。物理的デバイスのセキュリティは困難な問題となっており、IoT エコシステムを破壊する最も簡単な方法は、ネットワークコミュニケーションか物理的なエンドポイントの弱点を悪用することです。

卓越したエンジニアリング技術によってコアとなるテレマティクスシステムの安全性を確保したとしても、車両コンピューターネットワークの残りの部分を構成するセンサーや ECU(電子制御ユニット)などのエンドポイントは、複雑性とコストの面から安全性を確保することが難しくなっています。

図 2 は、自動車向け IoT ソリューションが攻撃を受ける可能性があるパターンを示しています。

図 2 – 自動車向け IoT の環境でよく見られる攻撃パターン。

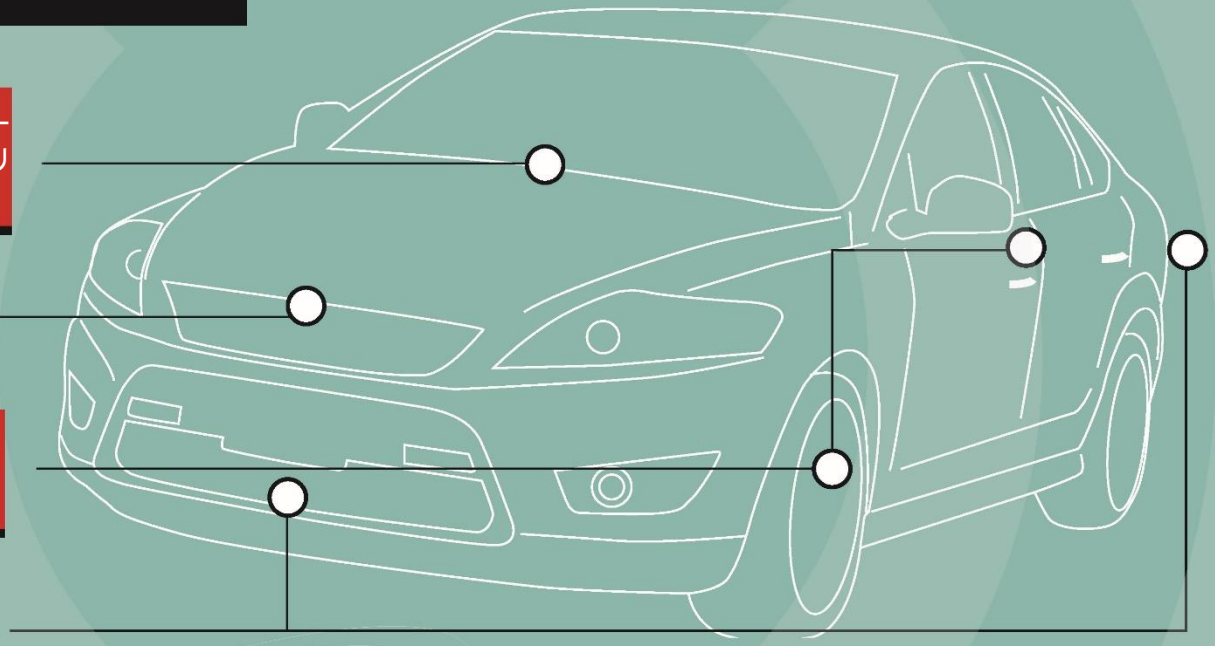
自動車向け IoT 機能に対する攻撃パタ

テレマティクスのバックエンドサービスでのなりすまし、ファームウェアアップデートの改ざん、コミュニケーションのセキュリティ欠陥、サードパーティー・アプリケーションによる「脱獄」.

ECU の意思決定をコントロールするローカルまたはリモートの CANbus 装置

通常ワイヤレスプロトコルの弱点によるリモートコード実行またはセンサーデータのなりすまし

セキュリティ証明書または鍵階層の悪用による重要コミュニケーションチャネルの操作



費用対効果が高い解決方法

これまでご紹介した問題は、システミックなものでも解決不能なものでもありません。実際には、IoT ソリューションに対する攻撃を阻止するための費用対効果が非常に高い方法があります。

管理インターフェイスのセキュリティは、多くの場合製品やサービスのアーキテクチャとは切り離して対応する必要がありますが、以下の 4 つの方法により、エンドポイントデバイス上で利用できる管理インターフェイスのセキュリティを確保することができます。

- **ネットワークとアプリケーションのセキュリティにトラステッド・コンピューティング・ベース（TCB）の使用を要求する**
- **すべてのネットワークコミュニケーションの機密性と完全性を保証する**
- **アプリケーションの動作を制限する**
- **耐タンパー性を強化する**

1.トラステッド・コンピューティング・ベース（TCB）の使用

トラステッド・コンピューティング・ベース（TCB）とは、重要な暗号とアプリケーションベースのトークンの使用とセキュリティを義務付けるポリシー、手順および技術の集合体であります。プラットフォームの信頼性を決定付けるための基盤となるものです。技術的に優れた TCB が製品のコアとして使用されている場合、その製品は業界において信頼のおける製品であるとみなされます。TCB を使用することで、以下のことが可能となります：

- ハードウェアの複製やスプーフィングの可能性を低減または排除する
- サービス内で認証済みコンポーネントの使用を義務付ける
- アプリケーションのフィールド内またはリモート OTA アップデートの費用対効果を改善する
- サービスのコンポーネント間の信頼性と互換性を向上させる
- 製品寿命を向上させる

「GSMA IoT セキュリティ・ガイドライン」では、トラステッド・コンピューティング・ベース（TCB）に関する詳細情報を提供しています。同ガイドラインは、以下よりダウンロードしていただけます。http://www.gsma.com/iot/iot-security-guidelines

2.ネットワークコミュニケーションのセキュリティ

T2 番目に重要な IoT セキュリティの特性は、ネットワークコミュニケーションです。ネットワーク内のすべてのコンポーネントは。互いに認証可能であり、該当する場合は機密扱いでデータの伝送を行うことができる必要があります。これらのコンポーネント間では、データの傍受、改ざんまたはなりすましを確実に防止するために、検証可能な完全性を有した通信を行う必要があります。

技術的に優れた TCB がない場合、ネットワークコミュニケーションのセキュリティを確保することが困難となる恐れがあり、多くの場合本番環境での予期せぬ動作につながります。例えば、多くの新しい IoT 製品では、Bluetooth Low Energy（BLE）、Zigbee、Thread などのパーソナル・エリア・ネットワーク（PAN）コミュニケーション技術が使用されています。

これらのプロトコルには、信頼できないネットワーク上で通信を行っているピア間において安全なセッションを構築することを可能にする、新しいセキュリティ機能が含まれています。

これらの最新プロトコルにおけるセッションの安全性を確保するために使用されている暗号アルゴリズム（楕円曲線ディフィー・ヘルマンなど）は、数学的には適切なものですが、データの機密性と完全性を保証することができません。

これは、これらの技術には信頼の基点（Root of Trust）がなく、メモリの耐タンパー領域に鍵が保管されておらず、完全なセッションの安全性を確実に確保するために必要な特定の処理能力がない可能性があるためです。

攻撃者となる可能性がある人が最初の目標にするのは、ネットワークコミュニケーションの分析です。そのため、あらゆる IoT 製品やサービスにとって、ネットワークコミュニケーションの安全性が最も重要であるとみなすのは極めて当然のことです。

3.アプリケーション動作の制限

アプリケーションのセキュリティ確保は、多くの困難を乗り越えてきた優れた企業にとっても極めて困難な問題です。メーカーのエンジニアチームによって設計されたコアアプリケーションに対して徹底した監査を行うことができますが、現代のアーキテクチャでは、サードパーティー・アプリケーションを IoT エンドポイントに導入することができる場合が多くなっています。ユーザーは、アプリケーションストアで数十万のサードパーティー・アプリケーションにアクセスすることができるため、すべてのアプリを徹底的に監査することはほとんど不可能です。

アプリケーションのセキュリティを確保するための適切な方法は、アプリケーションの機能だけでなく、重要なシステムデバイスやリソースへのアクセスを制限する「jail」、仮想マシン、コンテナまたはその他のアブストラクションレイヤにアプリケーションを隔離することです。

この方法により、ソフトウェアに欠陥があったとしても、アプリケーションから攻撃者が侵入し、CANbus のような重要なリソースにアクセスすることはできなくなります。アプリケーションを以下のように設定することが特に重要です：

- ホストオペレーティングシステムに影響を与える権限昇格ができないようにする
- 低レベルのドライバーまたはデバイスへのアクセス権を与える機能をなくす
- 他の重要なアプリケーションの動作に影響を与えることができないようにする
- 他のアプリケーションのメモリやリソースへの書き込みや読み取りを行う機能をなくす
-

これらのルールを厳守することで、攻撃者がサードパーティー・アプリケーションを悪用してコードを実行する権限を取得したり、アプリケーションに「小さな抜け道」があったとしても、その影響を定量化し、被害をアプリケーションへのセキュリティ侵害だけにとどめることができます。他のアプリケーションやサブシステム、ホストオペレーティングシステムに被害が及ぶことはありません。

4.耐タンパー性を強化する

大部分の IoT 攻撃は物理的なデバイスをチャネルとして実行されるため、攻撃が発生するリスクを軽減するためには、これらのデバイスの分析を阻止することが現実的な方法となり得ます。

攻撃者によって管理されている物理的デバイスは常にセキュリティ侵害のリスクがありますが、物理的な耐タンパー性を利用して攻撃プロセスを混乱させたり、攻撃の現実性や費用対効果が低下するまで攻撃のコストを引き上げたりすることができます。

例えば、感光ヒューズを使用することで、デバイスのケースが開くとメモリを消去させることができます。同様に、デバイスのケーシングに回路を埋め込むことで、デバイスが開けられた場合にコイン型電池を切断し、重要なメモリコンポーネントを消去させることもできます。

この他にも、攻撃者がリバースエンジニアリングやデバイスセキュリティの侵害を成功させるには、非常に多くの時間、専門知識、装置が必要となるように、費用対効果の高い措置を構築することも可能です。

図 3 は、自動車向け IoT ソリューションのセキュリティを確保するために利用できる戦略の一部を示しています。

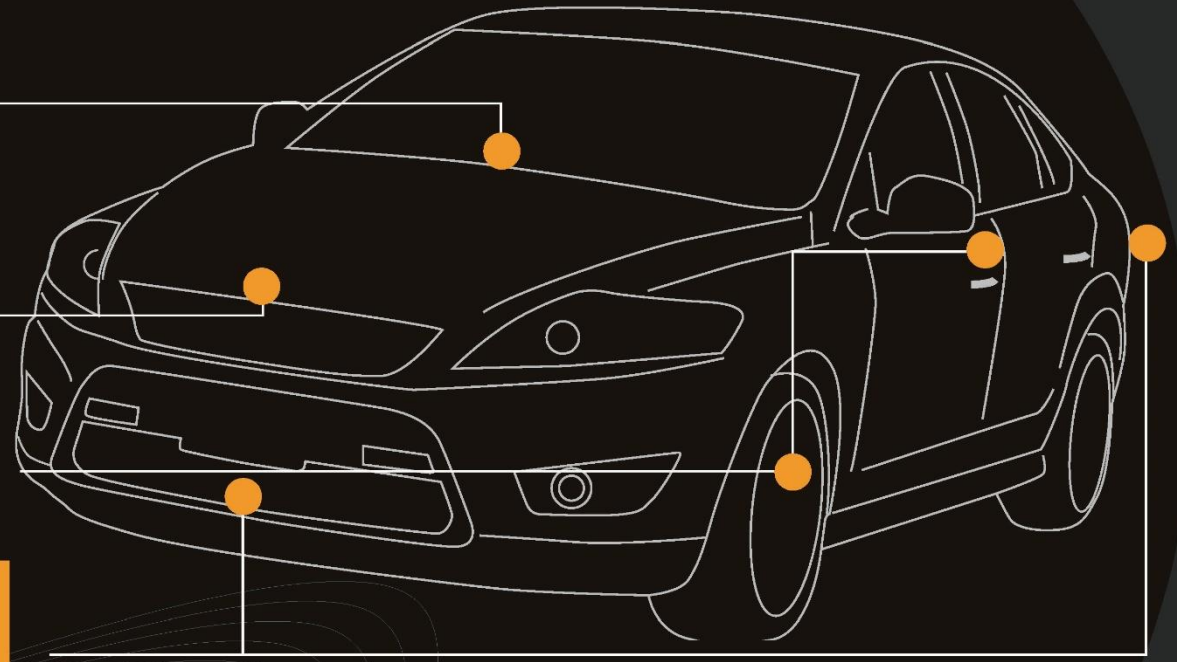
実践的な自動車向け IoT セキュリティ戦略

ローミングやプロトコルダウングレードによりモバイルネットワークのセキュリティが不安定な場合でも、アプリケーションレベルでのコミュニケーションセキュリティを強化して最高水準の機密性と完全性を確保する

長期的なエンジニアリングコストを削減し、デバイスの寿命を向上させるために、コアとなるアーキテクチャの信頼性を構築する

軽量センサーエンドポイント上でも、ピア認証を実装してデータの機密性やメッセージの完全性を確保する

カスタムアプリケーションがセキュリティ侵害を受けた場合、重要なコンポーネントに影響を与える攻撃者の能力を低下させるために、重要なアプリケーションとそうでないアプリケーションをセグメントする



要約

マスコミではセキュリティリスクが大々的に報じられていますが、IoT ソリューションのセキュリティを確保することは可能です。費用対効果が高いセキュリティ対策はアーキテクチャを出発点として、微調整を行うことで IoT の製品やサービスのエコシステム全体を悪用から確実に保護することができます。しかし、そのためにはエンジニアリングチームが時間をかけて、セキュリティを一から構築する必要があります：IoT ソリューションのセキュリティはアドオンで実装することはできないため、製品設計の基盤として構築しなければなりません。

一般的な IoT リスクの軽減方法に関する詳しい推奨事項については、「GSMA IoT セキュリティ・ガイドライン」を参照してください。
http://www.gsma.com/iot/iot-security-guidelines

GSMA の IoT に関する最新ニュースについては、以下のリンクにアクセスしてください。

GSMA 公式ウェブサイト：**www.gsma.com／IoT**

ニュースレター登録：**http://www.gsma.com/IoT/sign-up-for-newsletter/**

LinkedIn で GSMA をフォロー：**http://gsma.at/IoT**