GSMA Connected Living

自動車向け IoT のセキュリティ セキュリティ 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

進化するアタッカー

過去数十年間の情報セキュリティの分野で、明らかな傾向がひとつあります。それはアタッカーが勝利していること。しかもその勝利のスピードが加速しています。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、技術が以前にも増して入手しやすくなりました。これに対して、防御する側には地道な努力、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です。

5年前に開催されたラスベガスのブラック・ハット・ブリーフィングで、Lab Mouse Securityのドン・A・ベイリーが、史上初めて遠隔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ひとつであるDEF CONではカーハッキングに特化したワークショップが開かれ、ハードウェアのツール、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潜り抜ける秘伝の戦略が提供されています。

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留まる人ばかりではなくなりました。なかには一線を越えてしまう人もいます。明らかに脆弱なポイントは、自らの利益となる操作をしようと犯罪者たちが集まってくるでしょう。

アタッカーのなかには、「ランサム（身代金）ウェア」と呼ばれるマルウェアを使用し、お金を支払うまで主要システムの使用を止めてしまう者もいます。このような攻撃の多くは、重大な損失をもたらす恐れがあります。

2015年12月には、ウクライナの狭い地域で、配電網を動かす電源装置に入り込んだマルウェアが3週間の停電を引き起こしました。

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史上初の電力事故でした。

IOTが進展して産業用のシステムが一層つながりを強めると、このような攻撃はますます増えていくものと考えられます。エンジニアと経営者は、自らのIOTソリューションが攻撃される可能性ではなく、いつそれが起こるのか自問する必要があります。このような攻撃に効果的に対抗し、全体のセキュリティ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備え付けることです。

攻撃パターン

アタッカーは、IoTを支える産業や技術から生まれた様々な手段を寄せ集めて、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の本質は、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の提供を可能にする、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す。言い換えれば、IoTは既存の技術を使って相互作用と自動化を可能にしたものです。

従って、アタッカーは既に確立された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探し出すことができるのです。

次の頁の図１は、自動車向けIoTソリューションの構成要素の一部を示しています。

図1－自動車向けIoTの共通構成要素と機能

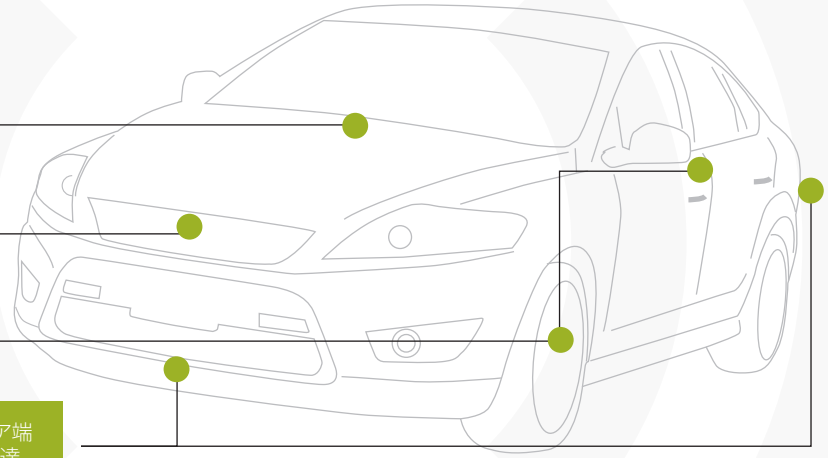
最新の自動車向けIOTの機能

最新のテレマティックスシステムがデータを収集し、エンターテインメントを提供し、診断結果を映像化

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

道路状況を感知して、センサーが安全な通り道に誘導

ワイヤレスコミュニケーションシステムが近くのピア端子と交信し、安全上重要なメトリックスと警告を伝達



よく使用されるIoT技術の攻撃対象は以下の通りです。

- ピア端子認証の弱点
- 実践的な暗号の不正変更
- エンドポイントの正当性のギャップ
- 重要アプリケーションと重要でないアプリケーションの未分類
- 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

多少知識のあるアタッカーであれば、物理的なデバイスが孤立コミュニケーションネットワークに最も侵入しやすポイントだということは誰でも知っています。物理的デバイスのセキュリティは難しい問題で、IoTの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突くことです。

コアのテレマティックシステムの安全性が卓越したエンジニアリングによって確保されていても、そのほかの自動車コンピューターシステム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、複雑さと費用面から安全性を維持することが難しいものです。

次の頁の図2は、自動車向けIoTソリューションが攻撃を受け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

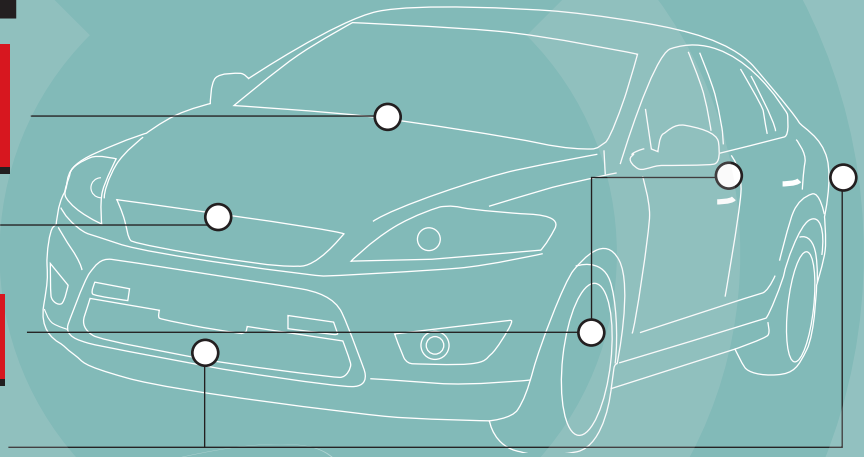
自動車向けIOT機能に対する攻撃パターン

テレマティックスのバックエンドサービスでのなりすまし、ファームウェアのアップデート改ざん、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装置類

遠隔からのコード実行、通常のワイヤレスプロトコルの弱点をついたデータ偽装

セキュリティ証明書または鍵階層を悪用した重要コミュニケーションチャネルの操作



費用効率の良い解決方法

これまでにご説明したものは、組織的なものでも解決不可能なものでもありません。実際に、高い費用効率でIoTソリューションへの攻撃を阻止する方法があります。

そもそも管理インターフェイスのセキュリティは、おおむねサービスや製品のアーキテクチャとは切り離して対応しなければなりませんが、以下の4つの方法はエンドポイントデバイスで管理インターフェイスをセキュリティ向上のために利用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信頼計算処理ベースの使用を要求する。
- ネットワークコミュニケーションがすべて機密性を保ち正当性があること確実にする。
- アプリケーションの動作を制限する。
- タンパーレジスタンスを強化する。

1. 信頼計算処理ベースの使用

信頼計算処理ベース(TCB)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、技術の集合体で、プラットフォームの信頼性定義の基礎となるものです。技術的に強健なTCBが商品のコアにあれば、その商品はその分野で信頼がおける商品だとみなされます。TCBを使用すれば、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の低減さらには排除
- サービス内で認証済み構成要素の使用強制
- アプリケーションのフィールド内または遠隔OTAアプデートの費用効率改善
- サービスの構成要素間の信頼性と相互作用性の向上
- 製品寿命の延長

信頼計算処理ベースに関し、GSMAはIoTセキュリティガイドラインでより詳しい情報をご提供しています。以下よりダウンロードが可能です。 **http://www.gsma.com/connectedliving/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

2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構成要素はお互いに認証可能で、必要な場合は対外秘でデータのやり取りができなくてはなりません。これらの構成要素間では、傍受・改ざん・なりすましを排除して、データの正当性を確認できる交信をする必要があります。

ネットワークコミュニケーションにおいて、技術的に強健なTCBが無い場合のセキュリティ維持は困難で、プロダクション環境で予期せぬ動作につながる事例も多く見られます。例をあげましょう。現在多くの新しいIoT製品は、低エネルギーBluetooth（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テクノロジーを使用します。

これらのプロトコルは、信頼性の無いネットワーク上でもネットワークピア端子間で安全性の高いセッションを可能にする、新しいセキュリティ機能を備えています。

しかしこれらの最新プロトコルの、セッションの安全確保のための暗号アルゴリズム（例えば楕円曲線Diffle-Hellman）は数学的には正しいのですが、データの機密性と正当性は担保されていません。

というのも、これらの技術には信頼のルートが無く、キーの保存場所のメモリーエリアにはタンパーレジスタンスもなく、すべてのセッションのセキュリティに必要となる確実な処理能力を備えていない可能性があるからです。

アタッカーになる可能性のある人が、まず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、どのようなIoTの製品やサービスにとっても、ネットワークコミュニケーションのセキュリティが最も重要だと考える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安全性確保は極めて困難で、百戦錬磨の企業にとっても至難を極めます。製作会社のエンジニアチームによって設計されたコアのアプリケーションを徹底的に評価することはできますが、近年のアーキテクチャではサードパーティー・アプリケーションがIoTのエンドポイントにロードされている場合が多くあります。ユーザーは、アプリケーションストアで何百、何千ものサードパーティー・アプリケーションにアクセスできるので、それらすべてを徹底的に評価することは到底不可能です。

アプリケーションの安全性を確保する正しい方法は、アプリケーションを「監獄」、仮想マシン、コンテナ、または重要なシステムデバイスやリソースへの接近や機能を制限するもう一つのアブストラクションレイヤの中に入れて隔離することです。

これにより、ソフトウェアに欠陥があっても、アプリケーションからアタッカーが侵入し、CANbusのような重要なリソースに近づく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可能性のある特権を与えない。
- 低い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ない。
- 他の重要アプリケーションの動作に影響を与えさせない。
- 他のアプリケーションのメモリーやリソースへ書き込み・読み込みをさせない。

このようなルールがしっかりと守られていれば、アタッカーがサードパーティー・アプリケーションを不正利用してコードの実行方法を取得しても、あるいはアプリケーションに「小さな抜け道」がある場合でも影響を数量化することが可能で、アプリケーションだけのセキュリティ侵害に限定することができます。他のアプリケーションやサブシステム、またはホストオペレーティングシステムには影響が及ばずに済みます。

4. タンパーレジスタンスの強化

殆どのIoT攻撃は物理的なデバイスのチャネルを通ってきますので、攻撃の可能性を減らすには、これらのデバイスの解析を防止するのが現実的な方法です。

もちんアタッカーの手にある物理的デバイスは常にセキュリティ侵害の可能性がありますが、物理的なタンパーレジスタンスを使って攻撃プロセスを混乱させたり、費用効率が悪くて攻撃する意味がなくなる程度まで攻撃のコストを引き上げることができます。

例えば、感光ヒューズを使用することで、装置のケースが開くとメモリを消去させることができます。同じように、デバイスのケーシングに回路を埋め込むことで、コイン型電池を引き離し、デバイスが開けられた場合に重要なメモリの構成要素を消去させることもできます。

この他にも、アタッカー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破壊を成功させるには、非常に多くの時間と専門知識と装置が必要となるような、費用効率の高い防衛策を作り出すことは可能です。

図3は、自動車向けIoTソリューションのセキュリティ保全のための戦略の一部を説明しています。

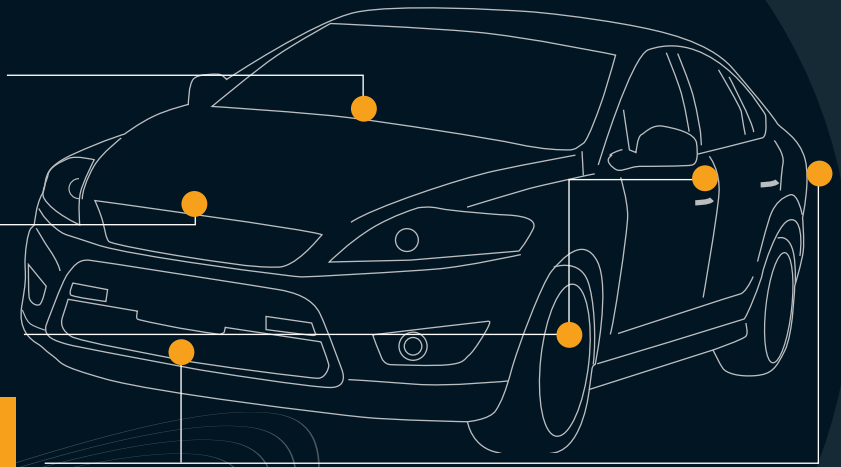
実践的な自動車向けIOTセキュリティ戦略

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確かな場合でも、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の機密性と正当性を確保する。

長期のエンジニアリングコストを引き下げ、デバイスの寿命を延ばすために、コアとなるアーキテクチャの信頼を築く。

軽量センサーエンドポイントでも、ピア端子認証を実装してデータの機密性やメッセージの正当性を確保する。

もしカスタムアプリケーションがセキュリティ侵害を受けている場合、重要な構成要素に影響を与えるアタッカーの能力を弱めることができるので、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分類する。



要約

マスコミではセキュリティ上の懸念がさかんに喧伝されていますが、IoTソリューションの安全性を確保することは可能です。費用効率の良いセキュリティはアーキテクチャレベルを出発点とし、僅かな修正で、IoTの製品やサービス全体を不正使用から確実に守ることができます。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、セキュリティをボトムアップで築き上げていく必要があります。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ものではなく、製品設計の基盤となるものです。

一般的なIoTリスクの削減方法に関するさらに詳しい推奨内容については、GSMAのIoTセキュリティガイドラインをご参照ください。
http://www.gsma.com/connectedliving/iot-security-guidelines

「つながる生活」に関するGSMAの最新ニュースは以下の方法によりご確認ください。

ウェッブサイト: **www.gsma.com/connectedliving**
ニュースレター登録: **http://www.gsma.com/connectedliving/sign-up-for-newsletter/**
LinkedInでフォロー: **http://gsma.at/LinkedInConnectedLiving**