IoT (モノのインターネット) の参照アーキテクチャ

digicert®

概要

モノのインターネット (IoT) は、 すでに数十億人の人々の役に立っています。何千種類ものスマートなコネクテッドデバイスが、世界中の人々に新しい体験をもたらし、コスト削減を実現しています。時には数十億ドルの削減になることもあります。たとえば、コネクテッドカー、 ロボットによる製造、 よりスマートに進化した医療機器、スマートグリッド、そして無数の産業用制御システムがすでに使われています。しかし、コネクテッドデバイスが増加するとセキュリティリスクも増大します。IoT の豊かだが脆弱な環境を狙って、脅威は急速に進化しているのです。深刻なリスクとしては、人への危害や、長期のダウンタイム、さらに、パイプラインや溶鉱炉、発電所などの設備の破壊があります。こうした設備や IoT システムの中には、すでに攻撃や物的被害を受けたものもあります。したがって、IoT デバイスや IoT システム (特に産業用インターネット向けのもの) の開発や運用に携わる人にとって、セキュリティは今や必須の考慮事項となっているのです。

では、IoT のセキュリティはどうすれば実現できるのでしょうか。IoT システムは多くの場合非常に複雑で、クラウドから接続層までくまなくカバーするエンドツーエンドのセキュリティソリューションが必要です。しかも、 従来のセキュリティソリューションに対応できるだけの処理能力を持たない、 リソースの限られた IoT デバイスをサポートしなければなりません。単独の特効薬は存在しません。いくらドアに鍵をかけても、 窓が開けっぱなしでは完全とはいえません。セキュリティは包括的なものでなければならないのです。そうでないと、 攻撃者は簡単に鎖の輪の最も弱い部分を突いてきます。もちろん、 従来の情報技術 (IT) システムによって IoT システムのデータを処理することも多いですが、IoT システム自体にも独自のセキュリティを追加する必要があります。IoT セキュリティは 4 つの土台によって実現できます。その 4 つとは、**通信の保護、デバイスの保護、デバイスの管理、システムの理解**です。

これらの土台を組み合わせれば、 強力で導入の容易なセキュリティアーキテクチャの基盤が形成され、 IoT のセキュリティ脅威の大半を (高度で複雑なものも含めて) 軽減することができます。このホワイトペーパーでは、これらの土台と、その必要性、そして容易かつ効果的な導入のための戦略について解説します。短い文書 1 つでは、 業界ごとに固有の重要な情報をすべて事細かに記すことはできません。そこで、このホワイトペーパーでは、自動車、エネルギー、製造、医療、金融サービス、行政、小売、物流、航空、消費者など、あらゆる業界に当てはまるアドバイスを提供し、 多くの業界の参考になる例を紹介します。まず、土台そのものについて簡単に解説します。

通信の保護

通信の保護では、 デバイスがリモートシステムを信頼できるかどうかを判断するため、 暗号化と認証が必要とされます。楕円曲線暗号などの新しい技術を利用すれば、 IoT で使用される 8 ビット、8 MHz のようなリソースの限られたチップでも、従来の技術の 10 倍 の処理が可能です。これにより、認証用のすべての「鍵」を管理するという大きな課題が解消されます。トップクラスの認証局 (CA) である DigiCert 社が発行した「機器用証明書」の鍵は、すでに十億台以上の IoT デバイスに組み込まれており、 携帯電話の基地局やテレビなど、 幅広いデバイスの相互認証を実現しています。

digicert®

デバイスの保護

デバイスを攻撃から守るには、コード署名 (すべてのコードが承認を受けて実行されるようにする) と、ランタイム保護 (コードがロードされた後に悪意のある攻撃によって上書きされないようにする) が必要です。コード署名は、コードがデバイスにとって安全であるとして「署名」された後に改ざんされていないことを、暗号によって保証します。これは「アプリケーション」レベルでも「ファームウェア」レベルでも可能であり、モノリシックなファームウェアイメージしかもたないデバイスでも利用できます。センサーやハブなどの重要なデバイスはすべて、署名されたコードのみを実行し、署名のないコードは絶対に実行しないように設定しておく必要があります。

しかし、コードが実行を開始した後も、デバイスの保護は続ける必要があります。そこで有効なのが、ホストベースの保護です。ホストベースの保護は、さまざまな IoT オペレーティングシステムに対し、ハードニング (堅牢化)、ロックダウン、ホワイトリスト、サンドボックス化、ネットワークへの侵入防止、ビヘイビア (振る舞い) ベースのセキュリティおよびレピュテーション (評判) ベースのセキュリティ (ブロッキング、ロギング、アラートなど) を提供します。最近は、クラウドにアクセスしたり限られたデバイスに過度に負担をかけたりせずに実行できる、IoT 対応のホストベースの保護も登場しています。

デバイスの管理

残念なことですが、出荷後しばらくしてから重要なデバイスに脆弱性が見つかり、パッチが必要になることがあります。重要なシステムの難読化コードでも、リバースエンジニアリングされ、脆弱性が見つかり、更新が必要となる場合があるのです。そのようなとき、デバイスを 1 台 1 台更新するため社員を差し向けるのは大変ですし、デバイスの台数が多い場合にはなおさらです。そのため、デバイスには出荷前にあらかじめ無線 (OTA) 管理機能を組み込んでおく必要があります。

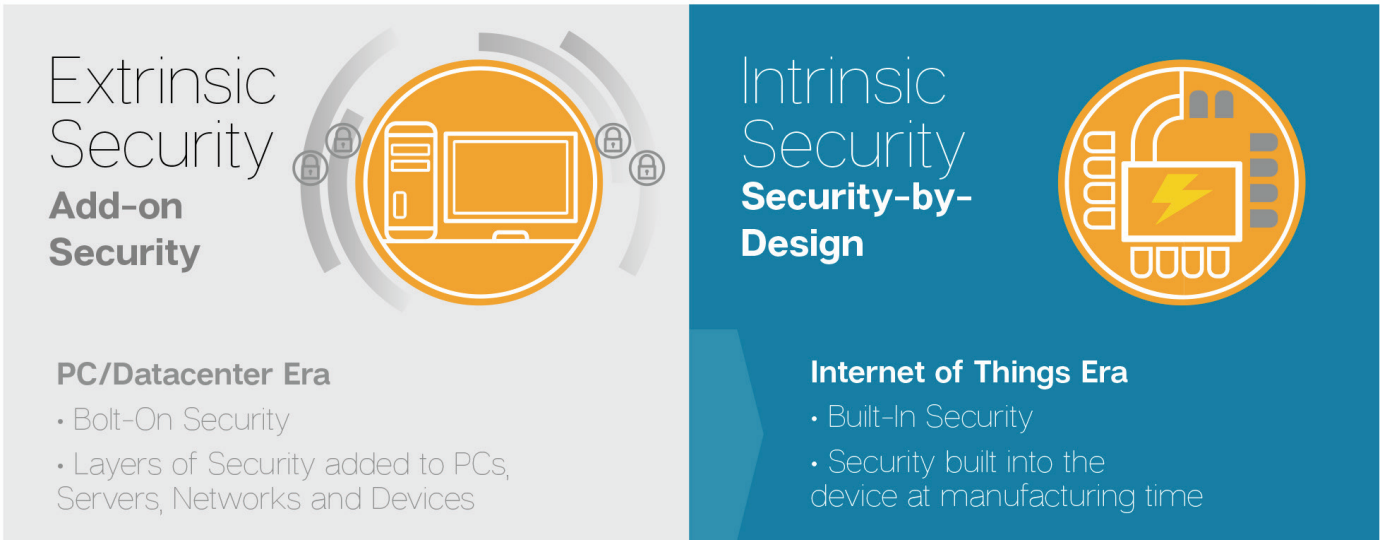
システムの理解

すべてにしっかり鍵をかけ、システムをきちんと管理していても、そうした対策をすべて打ち破り、システム内に足掛かりを作ることのできる脅威は存在します。そこで、IoT セキュリティ分析機能を使用し、ネットワークの状況を十分に把握することが大切です。セキュリティ分析機能は、異常が発生したとき、それが疑わしいものか、危険なものか、あるいは悪質なものかを通知してくれます。

重大な背景: 重要な進化

ほとんどの IoT デバイスは、「閉じられて」います。工場から出荷されたデバイスに、ユーザーが後からセキュリティソフトウェアを追加することはできません。そのような改変を行うと保証が無効となってしまう場合がほとんどです。したがって、IoT デバイスにはセキュリティを初めから組み込んで、「セキュア・バイ・デザイン (設計によるセキュリティ)」を実現しなければなりません。つまり IoT の場合、サーバーやデスクトップ PC、ノート PC などの従来のシステムに「後から追加する」セキュリティから、工場から出荷する前にシステムの中に「組み込む」セキュリティに進化させる必要があるのです。多くのセキュリティ企業は、従来のセキュリティ技術 (暗号化、認証、完全性検証、侵入防止、安全な更新機能) も含め、工場で組み込んで提供するという「内蔵型」のセキュリティを経験したことがありません。IoT モデルではハードウェアとソフトウェアの結びつきが強いので、IoT セキュリティソフトウェアが高度なセキュリティハードウェア機能をより簡単に活用できる場合があります。こうした機能を、「最小公倍数」的なハードウェアで動作する「外付け型」のセキュリティレイヤを作ることしか求められていない従来のセキュリティ企業は見落としがちです。多くのチップメーカーはすでにセキュリティ機能をハードウェアに組み込んでいます。ハードウェアレイヤは、通信の保護やデバイスの保護を行うハードウェアサポート型のセキュリティに必要とされます。しかし、包括的セキュリティでは必要と

される最初のレイヤにすぎません。包括的セキュリティでは、上述した機能 (鍵管理、ホストベースのセキュリティ、OTA インフラストラクチャ、 セキュリティ分析機能) が完全に統合されている必要があります。セキュリティの 4 つの土台のうちどれか 1 つでも対策を怠れば、攻撃者の気まぐれに運命を委ねることになります。



産業用インターネットと IoT のおかげで、身の回りにあるモノが「ネットワーク化されたインテリジェンス」を備えるようになり、セキュリティ対策にも注意を払わなければならなくなりました。私たちの生活は、日々の移動手段である飛行機、電車、自動車に依存しています。また、医療インフラや公共インフラにも依存しています。おかげで、私たちは都市に密集して生活したり働いたりすることができます。信号機、 医療機器などの設備が不正に操作されたとしたら、 どれほどの災難が引き起こされるかは、 想像に難くありません。市民や消費者は、自分の家や車が何者かにハッキングされることを望みません。また、自動生産の停止によって生産が滞った場合に、どのような損害が発生するかも、次第に明らかになっています。そこで、このホワイトペーパーでは、IoT のためのエンドツーエンドのセキュリティとはどのようなものかを定義し、効果的かつ容易に導入できるようにするためのガイダンスを提供します。

作り話ではありません:

石油掘削装置、水力発電所、産業インフラへのハッキング

セキュリティの研究者は、石油掘削装置、パイプライン、ウォーターポンプ、産業施設、送電網などへのハッキングは作り話ではなく、現実であることを明らかにしています。

digicert®

通信の保護

IoT のための強力な信頼モデル

セキュリティは、 基礎の上に実現します。弾力性に富むセキュリティの基礎として欠かせないのが、暗号化、認証、そして「鍵管理」です。優れたオープンソースライブラリの中には、IoT デバイスのようなリソースの限られたデバイスでも非常に効率よく暗号化を実行できるものがあります。しかし、いまだに多くの企業が危険を顧みず IoT の鍵管理をすべて独力で行おうとしています。一方、世界中の百万社以上の企業と、数十億人のユーザーを対象に、1 日当たりおよそ 40 億ドルもの電子商取引を保護している、シンプルかつ強力な信頼モデルがあります。この「信頼モデル」を使用すると、自社のシステムによって他社のシステムを安全に認証し、 システム間の暗号化通信を安全に開始することができます。この「信頼モデル」は、現在のコンピューティングにおける安全な相互運用の土台となっており、 極めて強力な数少ない認証局 (CA) に基づいています。これとまさに同じ CA によって、毎年数十億台のデバイスにすでに証明書が埋め込まれています。この機器用証明書を使用すると、たとえば、携帯電話から一番近い基地局へ安全に接続するための認証、電力会社のスマートメーターの認証、ケーブルテレビ業界のセットトップボックスの認証など、さまざまな認証が可能になります。強力な認証を行うには、証明書、鍵、クレデンシャルが不可欠ですが、強力な CA があれば、これらの安全な生成、発行、登録、管理、失効を簡単に行うことができます。IoT 関連のセキュリティ証明書は大量なので、機器用証明書は安い単価で大量に販売されます。

認証はなぜ大切なのでしょうか。確認されていないデバイスや確認されていないサービスからデータを受け取ることは、とても危険です。そのようなデータが原因でデバイスが破損したり危殆化したりする危険性もありますし、デバイスの制御が攻撃者に奪われ、 ユーザーが被害を受けたり、 あるいはそのユーザーを通じて他の人に害が及んだりする危険性もあります。強力な認証を使用して危険な接続を制限すれば、デバイスやサービスの制御を保持しながら、デバイスをこのような脅威から守ることができます。デバイスの接続相手が同種の他のデバイスであろうと、クラウドベースのサービスのようなリモートサービスであろうと、通信は必ず保護されなければなりません。すべての通信で、堅牢な相互認証と信頼が必要です。このように考えると、 機器用証明書をなおざりにするのは賢明とは言えません。

強力な相互認証を容易にするため、 さまざまな標準が策定されています。証明書のフォーマットの標準も存在します。強力な CA では標準フォーマットとカスタムフォーマットを両方ともサポートしています。多くの場合、 証明書の管理は SCEP (Simple Certificate Enrollment Protocol)、EST (Enrollment over Secure Transport)、 OCSP (Online Certificate Status Protocol) などの標準プロトコルを使用し、 無線 (OTA) を通じて簡単に行うことができます。証明書、 鍵、 クレデンシャルの処理は強力な CA によってサポートされるので、 実際の認証は TLS (Transport Layer Security) や、 DTLS (Datagram TLS) などの強力な標準 (SSL と同種のプロトコル) によって簡単に実現できます。IoT システムのエンドツーエンドのセキュリティで

は、エンドポイントが互いに認証を行う相互認証が不可欠です。さらに、TLS または DTLS による認証が完了したら、両エンドポイントは暗号鍵を交換 (または導出) し、 通信を開始します。盗聴者はこの通信を復号化することはできません。多くの IoT アプリケーションではデータの完全なプライバシーが必要とされますが、証明書と TLS/DTLS プロトコルがあれば、容易に実現できます。しかし、プライバシー保護が絶対に必要というわけではない場合、「取得した時点」でセンサー上で署名されていれば、データの認証は誰から受けても構いません。そうすれば、リンクレベルの暗号化の負担を減らすことができます。これは、マルチホップのアーキテクチャでは特に重要視される場合があります。

暗号演算用の IoT チップのコストと消費電力について心配する向きも少なくありません。しかし、忘れてはならないのは、楕円曲線暗号 (ECC) は IoT チップのようなリソースの限られたチップでも、従来の暗号化より 10 倍以上速く、より効率的であることが証明されているということです。ECC は、 セキュリティのレベルを下げることなく、 10 倍の速度と効率性を達成しているのです。しかも ECC は、 セキュリティレベルが RSA 2048 と同等で、「業界のベストプラクティス」であることも実証されています。このことは、 8 ビットプロセッサや、 処理速度がメガヘルツレベル、 キロヘルツレベルの 32 ビットプロセッサなど、 極めてリソースの限られたチップで実証済みです。これらのチップの中には、マイクロワットレベルの環境発電が多用される場合でも動作するほど消費電力の低いものもあります。スリープのサイクル間に断続的に動作する低消費電力デバイスのために、DTLS が TLS を拡張して、 策定されました。さらに、 これらの 32 ビットチップは非常に低価格です。したがって、 セキュリティが必要とされる場合には、 コストや消費電力を理由に妥当な基準値を下回るほどセキュリティレベルを下げるのは望ましくありません。以上の理由から、 セキュリティが必要とされる場合、 IoT デバイスの認証用の鍵の長さについて、次のガイドラインを提案しています。(a) エンドエンティティ証明書の場合、最低 224 ビット、推奨 256 ビットまたは 384 ビットの ECC。(b) ルート証明書の場合、最低 256 ビット、推奨 384 ビットの ECC。

今日では、各 Web サーバーの証明書を自分のブラウザにいちいち手作業でインストールするなど想像できませんし、 あらゆる証明書を盲目的に信頼して損害を被ることも考えられません。そのため、ブラウザごとに信頼できる「ルート」をいくつか用意し、これによってすべての証明書を評価するようになっています。信頼できるルートをブラウザに組み込むことにより、 Web 上に存在する数百万台ものサーバーでセキュリティが実現したのです。年間数十億台のデバイスがインターネットに接続されるようになった今日、 デバイスに信頼できるルートと機器用証明書の両方を組み込んでおくことが同じく重要です。

IoT のデータ管理では、データが常に安全な状態に保たれていなければなりません。私たちの生活は、データの機密性よりも、システムの正確性や、完全性、適切に動作する可用性に左右されることが少なくありません。情報やデバイスの認証や、情報の発信源が重要視されることもあります。しかし、データは単に A 地点から B 地点に送られるだけではなく、 いくつもの地点で保存されたりキャッシュされたり処理されたりするのが普通です。したがって、データが取得されたり保存されたりした場合は、いつ、どこであっても必ず署名が行われなければなりません。それによって、 情報の改ざんのリスクを低下させることができます。取得した時点でデータオブジェクトに署名し、その署名をデータと共に転送するのが (データが復号化された後であっても)、 一般的かつ有益なエンジニアリングパターンとなりつつあります。

IoT (モノのインターネット) がハッキングの主な標的に

今後 1 年の間に、自動車と交通システムがハッカーの標的になる可能性があります。

digicert®

デバイスの保護

IoT を動かすコードの保護

電源を入れると、デバイスはいくつかのコードを実行して起動します。このとき、実行するようプログラムされたことだけが実行されるようにすることと、 悪質な行為をするよう何者かによって再プログラムされないようにすることが重要です。つまり、デバイス保護の最初のステップは、デバイスがこちらの望むコードだけを起動して実行するように、コードを保護することなのです。幸い、多くのチップメーカーはすでに「セキュアブート」機能をチップに組み込んでいます。同様に、「よりハイレベルな」コードに対しては、OpenSSL のように長年の実績があるオープンソースのクライアント側ライブラリが多数提供されており、 簡単に利用できます。これにより、コードの署名を確認したり、 認証された発行元のコードだけを受け入れたりすることもできます。こうした背景から、ファームウェア、ブートイメージ、ハイレベルな組み込みコードへの署名が、 いずれも一般的になりつつあります。これには、オペレーティングシステムなどの下位のソフトウェアコンポーネントに署名したり、アプリケーションだけでなくデバイス上のすべてのコードに署名したりすることも含まれます。このような方法により、重要なコンポーネント、センサー、アクチュエータ、コントローラ、リレーなどがすべて、 署名されたコードだけを実行し、署名されていないコードは実行しないよう、適切に設定することができるのです。

適切なルールを設定するなら、「署名のないコードは信頼するな」となるでしょう。そこからさらに、「署名のないデータは信頼するな。特に、 署名のない構成データは絶対に信頼するな」となるでしょう。署名検証ツールや、 セキュアブートのためのハードウェアのサポートが進歩しつつある現在、 多くの企業にとって次なる課題は、コード署名と組み込みソフトウェア保護のための「鍵の管理」と「鍵へのアクセスの制御」です。CA の中にはコード署名プログラムの安全な管理を容易にするホステッドサービスも提供しているところがあります。これにより、コードへの署名や署名の失効ができるのは誰か、その署名や失効の鍵をどのように保護するかを、厳重に管理することができます。

セキュリティのためにソフトウェアの更新が必要で、 更新によるバッテリーへの影響に気を付けなければならない組み込み環境では、 更新する個々のブロックあるいはチャンクごとに署名と更新を行い、 モノリシックイメージ全体 (またはバイナリファイル全体) に署名をしないことが非常に重要です。ソフトウェアへの署名をブロックまたはチャンクごとに行うことで、 セキュリティを犠牲にすることなく、また、セキュリティのためにバッテリーを大量に消費することなく、 よりきめの細かい更新が可能になります。こうした柔軟性は、 必ずしもハードウェアのサポートを必要とせず、小さなプリブート環境でも実現できます。これは多くの組み込みハードウェア上で動作します。

バッテリー寿命を重視するなら、イメージを恒久的に焼き付けることによって、誰も置換や更新ができないようデバイスを構成するとよいでしょう。しかし、 世間に出回っているデバイスは、 悪意ある目的のためにリバースエンジニアリングが行われる可能性を想定しなければなりません。デバイスがリバースエンジニアリングされ、脆弱性が見つかって悪用された場合、できるだけ早くその脆弱性にパッチを適用する必要があります。コードの難読化や暗号化を行えば、 リバースエンジニアリングに相当時間がかかるようになるため、 大多数の攻撃者を防ぐことができますが、 リバースエンジニアリングを完全に阻止することはできません。国家レベルのリソースや、 高度な国際的犯罪組織のリソースがあれば、 難読化や暗号化で保護されたプログラムであってもリバースエンジニアリングは可能であると考えられます。特に、コードは復号化しないと実行できないためです。そのような

組織に脆弱性を発見され悪用されたら、 パッチが必要となります。したがって、 デバイスには出荷前にあらかじめ無線 (OTA) 更新機能を組み込んでおく必要があります。OTA 更新機能 (ソフトウェア更新とファームウェア更新を含む) は、 強力なセキュリティ態勢を維持する上で非常に重要です。それにはさまざまな理由があり、後ほど「デバイスの管理」のセクションで詳細に説明します。しかし、 難読化、きめ細かいコード署名、OTA 更新のすべてが効率的かつ効果的に機能するよう、 いずれはこれらをしっかりと連携させる必要があるでしょう。

きめ細かいコード署名とモノリシックなコード署名は共に、「通信の保護」のセクションで述べた、 同じ証明書ベースの信頼モデルを使用していますし、コード署名に ECC を使用すれば、高速で低消費電力でありながら高度なセキュリティを実現するというメリットが同様に得られます。そのため、セキュリティが必要とされる場合の IoT コード署名用の鍵の長さについて、次のガイドラインを提案しています。(a) エンドエンティティ証明書の場合、最低 224 ビット、推奨 256 ビットまたは 384 ビットの ECC。(b) ルート証明書の場合、最低 521 ビットの ECC。署名されたコードは一般に署名から数年後、 数十年後まで使用すると想定されるため、 それだけ長期にわたって安全性を維持できるだけの強力な署名でなければなりません。

IoT (モノのインターネット) がハッキングの主な標的に

今後 1 年の間に、ATM がハッカーの標的になる可能性があります。

digicert®

デバイスの保護

IoT のための効果的なホストベースの保護

これまでに、IoT セキュリティの土台として、IoT の鍵管理と認証の基本、 デバイスの完全性を保護するためのコード署名と構成の署名、 そしてこれらのコードや構成を管理するための基本である「OTA」について説明しました。しかし、通信を保護し、デバイスをきちんと管理して安全にブートできるように保護すれば終わりではありません。ブート後も長期間にわたって保護を続ける必要があります。こうしたニーズに答えるのが「ホストベースの保護」です。

IoT デバイスはさまざまな脅威にさらされます。たとえば、 脆弱性や構成の不備を突かれ、認証された通信を介して悪意のあるデータが送り付けられる可能性もあります。攻撃者はさまざまな弱点を突いてきます。たとえば、(a) コード署名検証ツールやセキュアブートの使用回避、 (b) すり抜けることが可能な、 検証モデルの導入の不備などです。多くの場合、こうした弱点を利用して、バックドアやスニファ、データ収集ソフトウェア、システムから機密情報を抜き取るためのファイル転送機能などがインストールされます。時には、システムの動きを操るためのコマンド & コントロール (C&C) のインフラストラクチャがインストールされることさえあります。さらに恐ろしいことに、 脆弱性を悪用して有害なソフトウェアを「すでに実行中」の IoT システムの動作中のメモリに直接インストールするという悪質なデータ攻撃もあります。この方法だと、再起動時にマルウェアは消滅しますが、再起動されるまでの間に甚大な被害がもたらされます。これは特に恐ろしい攻撃です。なぜなら一部の IoT システムや多くの産業用システムは、ほとんど再起動が行われないからです。こうした攻撃は、 産業用ネットワークや IoT ネットワークに接続された IT ネットワークを介して行われる場合もありますが、 インターネット経由、あるいはデバイスへの直接アクセスによって行われることもあります。最初の感染媒体が何であれ、攻撃に気付かない限り、最初に危殆化したデバイスは信頼されたままであり、今度はそのデバイスが経路となってネットワーク全体に感染します。その攻撃対象が自動車の「車載」ネットワークであっても、工場全体を制御するネットワークであっても同様です。したがって、IoT セキュリティは包括的なものでなければなりません。窓が閉まっていてもドアが開けっぱなしでは「十分とはいえない」のです。あらゆる感染媒体を防ぐ必要があります。

強力なコード署名や検証モデルと組み合わせて、 ホストベースの保護を導入すれば、 さまざまな技術 (システムハードニング、ホワイトリスト、アプリケーションのサンドボックス化、レピュテーション技術、マルウェア対策製品、暗号化など) によって、これらすべての脅威からデバイスを守ることができます。システムの固有のニーズに合わせてこれらの技術を組み合わせれば、各デバイスに最高レベルの保護を実現できます。

システムハードニング、 ホワイトリスト、 アプリケーションのサンドボックス化は、 バックドアを削除したり、 アプリケーションによるネットワーク接続を制限したり、トラフィック量 (インバウンドとアウトバウンドの両方) を制限したりすることで、 ネットワークの保護を実現します。アプリケーションの動作を制限したり、 バッファオーバーフローやゼロデイ攻撃からシステムを守ることで、デバイスの制御を維持したまま、 さまざまなエクスプロイトから保護することもできます。また、これらのソリューションを使用すれば、リムーバブルメディアの不正使用を防いだり、デバイスの構成や設定をロックダウン (機能制限) したり、 ユーザーの権限を必要に応じて降格させることもできます。さらに、 これらのソリューションは、 監査やアラートの機能を備え、 ログやセキュリティイベントをモニタリングすることができます。従来のような署名ベースの技術を実行するのに必要な接続性や処理能力のない環境でも、ポリシーベースの技術は実行できます。

レピュテーションベースのセキュリティ技術を使用すると、 ファイルの古さ、頻度、場所などからファイルの状況を把握することによって、他の方法では検出できないような脅威を検出したり、新しいデバイスが (認証されたデバイスであっても) 信頼できるかどうかの情報を提供したりすることができます。また、 変異するコードを使用したり暗号化スキーマを変化させたりする脅威も検出できます。このような難題を突きつけられた場合でも、危険なファイルを安全なファイルから切り離すことによって、 より速く正確にマルウェアを検出します。

もちろん技術の組み合わせ方はケースバイケースですが、 上記のオプションを組み合わせれば、リソースの限られた環境であってもデバイスを保護することが可能となります。

デバイスの管理

安全で効果的な IoT の管理

前述したように、リバースエンジニアリングが行われたり、脆弱性が発見されたりした場合、デバイスは OTA 更新を行う必要があります。ただし、 OTA 更新のメカニズムを導入すると複雑になるので、 自己責任でこれを避けようとする技術者も少なくありません。優れた OTA メカニズムはさまざまな目的で使用できます。ソフトウェアやファームウェアのセキュリティパッチや機能更新だけでなく、次の目的にも使用できます。

- 構成の更新
- セキュリティコンテンツや、セキュリティ分析のための セキュリティテレメトリ (遠隔計測) の管理
- 適切なシステム機能のための、テレメトリと制御の管理
- 診断と修復
- ネットワークアクセス制御 (NAC) クレデンシャルの管理
- 権限などの管理

これらはすべて安全に行われなければなりません。コード署名やファイル転送の実行以上の安全性が必要です。幸い、 デバイスごとのソフトウェアやファームウェアの一覧の管理や、デバイスの構成を行うための、 OMA (Open Mobile Alliance) などの強力な標準が存在し、多くのベンダーによってサポートされています。中には、数十億台のデバイスを管理できるものもあります。

デバイスごとのセキュリティ管理には、 前のセクションで説明した、ホストベースのセキュリティ技術の構成管理が含まれる場合もあります。セキュリティ技術の中には、 セキュリティコンテンツ (ブラックリスト、ホワイトリスト、ヒューリスティック、侵入防止署名、レピュテーションデータなど) の OTA 更新を必要とするものもあります。ポリシーベースのメカニズムを使用するセキュリティ技術の中には、デバイス上のソフトウェアが他の目的 (機能追加など) のために再イメージングされた場合だけしか更新を必要としないものもあります。しかし、いずれのセキュリティ技術でも、APT (高度で持続的な脅威) に対して有効なセキュリティテレメトリを生成できます。したがって、こうしたホストベース (デバイスベース) の技術によって常にセキュリティテレメトリを収集し、より集中的な分析を行うことが重要です。

各デバイスのコンポーネントのうち、安全な管理が必要なのは、セキュリティコンポーネントだけではありません。多くのデバイスはセンサーデータやテレメトリを生成します。これらは安全に収集され、保存や分析のため安全な場所に送信されなければなりません。制御機能を作動させるデバイスもたくさんあります。これらも慎重に管理すべきであり、 安全性を確保しながら構成パラメータを最新の状態にしておく必要があります。安全性の高い一般的なデバイス管理プロトコルを使用したインフラストラクチャを使用すれば、デバイスの本来の機能と、デバイスのセキュリティコンテンツやテレメトリの両方を、 安全に管理することができます。実際、 自動車の OTA 管理ではすでにこうしたフレームワークが採用されようとしていますし、 店舗内に設置された双方向型のキオスク端末や自動販売機も、すでにこうしたフレームワークによって安全に管理されています。こうした管理フレームワークでは、 エージェントベースの IoT 管理プロトコルと、 エージェントベースでない従来型の管理プロトコルとを組み合わせて使用していることがあり、その場合、管理を簡素化するため、デバイスは標準ベースの管理機能をサポートするように作られています。さらに、これらの技術と組み合わせて、ネットワークスニファから収集した情報を提供する管理フレームワークもあります。

したがって、 IoT システムには最初から更新機能が組み込まれていなければなりません。OTA 更新機能が組み込まれていないと、そのデバイスは永久に脅威や脆弱性にさらされ続けることになってしまいます。OTA 更新機能は、デバイスの構成、セキュリティコンテンツ、 クレデンシャルなどの管理にも使用できます。また、ソフトウェアのインベントリ情報の収集やセキュリティパッチの適用だけでなく、機能の追加や、テレメトリの収集などにも使用できます。しかし、 このような追加機能の有無にかかわらず、基本的な更新機能とデバイスのセキュリティ態勢の管理機能は必ず最初からデバイスに組み込まれていなければなりません。

IoT (モノのインターネット) がハッキングの主な標的に

今後 1 年の間に、建物と都市がハッカーの標的になる可能性があります。

digicert®

システムの理解

前述の対策を超える脅威に対抗するための セキュリティ分析

デバイスの保護、コードの保護、通信の保護をきちんと行い、セキュリティ態勢をしっかりと管理し、可能な限り高度な OTA 管理フレームワークを使用しても、 それでもなおこうした防御を打ち破るリソースと能力を備えた敵は存在します。戦略的な脅威には、 戦略的な軽減技術で対抗する必要があります。デバイスやネットワークハードウェアが収集したセキュリティテレメトリを活用してセキュリティ分析を行えば、その環境で何が起きているかを把握し、隠れた脅威を見つけ出すことができます。

また、 同様に重要なことですが、 これまでに述べた 3 つの土台をデバイス上に実現するのに何年もかかる場合、 暫定的なソリューションとして「モニタリング」や分析が導入されることがよくあります。たとえば、産業用制御システム (製造業、石油、ガス、 公共サービスなど) のレガシーデバイスは、 システム全体のリプレースが行われるまで変更できませんし、 すでに路上を走っている自動車の場合も、内部に組み込まれたマイクロコントローラを「取り外して交換」というわけにはいきません。また、医療業界では、 病院がセキュリティを強化するために機器を変更することはメーカーによって禁じられています。このようなケースでは、異常検出ソリューションが極めて有効です。多くの IoT ネットワークは決定論的な性質を持っているため、 基準を設定しておいて、そこからの逸脱をすぐに発見することができるのです。業界用のプロトコルや IoT プロトコルは種類が多いので問題が難しくなる場合もありますが、 先進的な機械学習を搭載した新しい技術を利用すれば解決できます。このソリューションでは、多くの IoT システムで可用性への要求が高いことを考慮し、「検出」モードはほどほどにして、 誤検出によるシステムダウンが起きないようにします。

別の例として、 レガシー環境と保護された環境の間に位置するゲートウェイがあります。特に、 エコシステムあるいは環境の一部が攻撃されたとき、 早期に検出しないとネットワーク全体に伝播してしまう可能性があります。同様に、 分散型のモニタリングと集中的な分析を最優先で行うべきなのは、「産業用」ネットワークと「IT」ネットワークの間にあるゲートウェイ、デバイスであふれている家庭とインターネットの世界とを分離する住宅用ゲートウェイ、「車載」ネットワークとセルラーネットワークの間のゲートウェイとして機能する自動車のヘッドユニット、 自動車の駆動システムの計器類と車内のインフォテインメントネットワークとの間のゲートウェイなどです。

このような例の多くでは、 ユーザーとセキュリティベンダーとが協力し合い、既存のビッグデータセキュリティ分析インフラストラクチャや、 大規模な脅威情報収集システムを活用して、 ネットワークとエコシステム全体で情報を収集、分析、共有することができます。小売業や重要インフラなどのさまざまな業界で、すでにこうした取り組みが始まっています。そして、こうした取り組みにより、 システム全体を迅速に更新して、 新たに出現した脅威から身を守ることが可能になっています。極めて高度な脅威を検出するためには、高い「データ分析」能力とセキュリティの専門知識をもって分析を行う必要があります。しかし多くの場合、専門外の企業にそこまで高い能力を望むことはできません。そこで、モニタリングや分析の専門家を頼れるよう、マネージドセキュリティソリューションとよく似た「マネージド」ソリューションの導入に舵を切る企業も少なくありません。また、 IoT セキュリティテレメトリのリポジトリを独自に構築し、 そのリポジトリへのアクセスを制御することによって、 複数の分析パートナーの助けを借りて高度な脅威の検出を行っている企業もあります。分析のための製品やプラットフォームの中には、 API や SDK を公開することによってそのような共有を可能にし、その共有を安全に制御できるようにしているものもあります (たとえば、適切なパートナーに対してのみ、関連性のあるデータだけを共有する、パートナーのアクセス権を適切に制限するなど)。

たとえば、 産業用ネットワークと IT ネットワークを接続する場合なら、さまざまな脅威を優先度別に把握して、脅威が一方の環境から他方へ通り抜けるリスクをできる限り抑えることができるよう、両方の環境にまたがる単一のデータプレーンを作成することをお薦めします。このようなソリューションは、 死角をなくし、各ユーザーがネットワーク全体を見渡せるよう、 さまざまなベンダーのさまざまなデバイスとさまざまなプロトコルにまたがって機能するはずです。

このような分析を通じて「検出と対策」を行うことで、強力な保護技術を補完すれば、 大部分の攻撃に対抗するセキュリティを実現できますし、最も狡猾で手ごわい敵に対してもリスクを軽減することができます。

システムの理解

何を信頼すべきか

今のところ、多くの IoT テクノロジーや IoT システムは、実は単なる「モノのイントラネット」にすぎません。しかし今後、相互に接続する必要のあるシステムが増えてくるにつれ、「何を信頼すべきかを知る」ことが次第に重要になってきます。機器用証明書があれば、 デバイスの来歴や系統を立証できます。しかし、 そのデバイスは今もまだ信頼できるのか、 という質問に答えるためには、 やがて別のサービスが必要になるでしょう。たとえば、レピュテーションベースのサービス、つまり「モノのディレクトリ」のようなサービスです。そのようなディレクトリがあれば、個々のデバイスや IoT システムに関するセキュリティ情報を記録するだけでなく、 デバイスやシステムの間で相互に付与される権限や資格を記録し管理することもできるでしょう。それだけではありません。周囲に IoT デバイスがもっと増えてくれば、自分の興味のある分野の、興味のある機能を備えたデバイスを「発見」することもできるようになるでしょう。このようなモデルなら、 モノのディレクトリを通して離れた場所にあるデバイスを素早く見つけたり、すぐにそのデバイスからデータやサービスの購入に同意したりできるかもしれません。見たことのないデバイスでも、その機能や評判などの詳細情報をすべてディレクトリに登録しておけるようになるかもしれないのです。さらに言えば、 デバイスが「あるユーザーを信頼できるかどうか」を知りたがるようになるとすると、「モノのディレクトリ」でも不十分です。おそらく、デバイス、システム、ユーザーなどを含む「すべてのディレクトリ」が必要となるでしょう。キッチンのシンクでさえ含まれるかもしれません (2015 年、 カリフォルニアで発生した干ばつを受けて行われた、 スタンフォード大学の水道使用量モニタリングプロジェクトでは、キッチンのシンクが「インターネットに接続」された)。

もちろん、「今はまだ」、 スマートなキッチンシンクやスマートな冷蔵庫を持っている人はあまりいません。しかし、インターネット経由で交通情報を取得する自動車や、 インターネット経由で動画を再生するスマートテレビやブルーレイプレイヤー、フィットネス用ウェアラブル機器などを持っている人はたくさんいます。それに、 ATM やディジタルの POS 端末などは、 数えきれないほど多く利用されています。したがって、近い将来、それらをすべて管理するための「モノのディレクトリ」を各自が持つようになるかもしれないのです。しかし、IoT セキュリティを実現するためには、通信の保護、デバイスの保護、デバイスの管理、戦略的脅威に対抗するためのセキュリティ分析のすべてがどうしても必要です。「何を信頼すべきかを知る」ための「ディレクトリ」という「魅力的な」コンセプトはまだ形ばかりの夢物語にすぎず、今はまだ、少なくとも多くの人にとっては、「土台」でもなければ「システムを理解する」ための必須の要素でもないということを、認めないわけにはいきません。この「何を信頼すべきかを知る」ための「ディレクトリ」という「魅力的な」コンセプトを紹介したのは、このような複雑さや規模の大きさを管理する上で今後どのような課題が待ち受けているか、 多くの人々に前もって知ってほしかったからです。また、 中にはすでにそのような課題に直面し、十億台を超えるデバイスの保護に取り組んでいる企業もあるからです。そうした企業にとって、「将来」はすでに現実のものです。そして、それは他人事ではないのです。

IoT セキュリティが包括的でなければならない理由

1 つの例

これまで説明してきた 4 つの土台のうち、1 つもおろそかにはできない理由を示す例として、電車を考えてみましょう。

電車では、 電動モーターコントローラは電車の加速を制御するだけでなく、 電車の回生ブレーキの制御も頻繁に行います。しかし、 加速が制御できなくなった場合の安全対策として機械式ブレーキが搭載されていたとしても、 モーターコントローラに悪質なプログラムが侵入してしまえば、 不均衡な急ブレーキがかけられ、 車両や乗客に被害が及ぶ危険性を阻止することはできません。したがって、コントローラ、ブレーキ、スイッチなどで動作するすべてのコード (電車の動力学的側面を操るすべてのコード) にはきちんと署名が行われ、 すべてのコンポーネントが署名されたコード以外のものは実行しないようにきちんと設定されていることが必要となります。

同様に、電車内の通信や、電車から他のインフラストラクチャへの通信が認証されていないと、 悲惨な結果となります。電車内の加速やブレーキのための制御信号が「なりすまされ」たらどうなるかは、 想像に難くありません。また、 目の前に危険が横たわっているのに、「異常なし」の信号がなりすまされた場合も同様です。

さらに、 ホストベースの保護がなければ、 コントローラ自体がハッキングされる可能性があります。すると、攻撃者は、認証やコード署名のメカニズムと戦わずして、 同様の不正な目的を達成できてしまいます。

このような包括的なセキュリティを必要としているのは、 電車だけではありません。自動車もインターネットに接続される機会が増えているので、 同様のホストベースの保護が必要です。自動車がリアルタイム OS を実行していても、ホストベースの保護を自動車のヘッドユニットに導入することは可能です。もちろん、コードは OTA で更新されるので、 これらのポリシーも同じ OTA システムを使用して OTA で更新できます。もしセキュリティ態勢を OTA によって「変更」する機能がなかったら、 敵はすぐさま変更を行い、弱点を見つけて突いてくるでしょう。

しかし、 これまでに述べた対策をすべて正しく行ったとしても、極めて高度な敵によってそうした対策が破られる可能性は残ります。そこで、そのような戦略的脅威を軽減するため、バックエンドのセキュリティ分析が欠かせません。セキュリティ分析システムは、電車、飛行機、自動車、工場、POS システムなど、あらゆるシステムを対象として、継続的にデータを収集し、基準値を設定することができます。IoT セキュリティ分析では、 この基準値を使用して素早く異常を見つけ、隠れた脅威を検出したり、そのような戦略的脅威と戦うための幅広いセキュリティ分析の一環として、高度な脅威の相関分析を行ったりすることができます。

最後に、 大事なことを指摘したいと思います。それは、 IoT セキュリティは単独では存在しないということです。多くのデバイスは「物理的セキュリティ」を必要としますが、その物理的セキュリティの種類は用途によって千差万別です。家庭内の IoT デバイスなら、 雇っているお手伝いさんに嗅ぎ回られないように何かで覆っておく程度でよいでしょう。しかし、 工場の IoT デバイスなら、何層もの物理的セキュリティが必要になります。たとえば、部屋に出入りするためのカードキーや、電磁波リスク評価で定められたフェンスの距離に関する制限などです。同様に、 人的セキュリティのニーズもさまざまです。ただし、物理的セキュリティ

も人的セキュリティも、 IoT 固有のものではありません。今の時代、多くの企業ではとっくにこれらのセキュリティに対応していますし、 通常の工場生産や従来の IT システムを保護するためだけでも、これらの対応は必須です。そのため、このホワイトペーパーでは、 IoT デバイスの内部とデバイス間の通信において IoT セキュリティを「正しく」設定するため必要条件に焦点を当てました。もちろん、多くの IoT デバイスは、データセンターやクラウドなどで稼働している従来型のバックエンド IT システムとも頻繁にやりとりをしています。そうしたシステムについては、ご自身によって「正しく」セキュリティが設定されることを前提としています。しかし、これだけは心に留めておいてください。「従来型」の IT システムで、IoT デバイスや IoT システムを動作させたり、あるいは IoT デバイスや IoT システムから取得したデータを処理したりしている場合、その「従来型」IT システムのセキュリティが正しく設定されていなければ、 IoT システムに構築されたセキュリティはすべて台無しになります。

IoT がますます普及し、特に自動車や飛行機、産業用機器などの命にかかわるシステムで IoT の活用が進むにつれ、システムにセキュリティを正しく組み込むことが必要になります。セキュリティを最初から「組み込む」ことによって、「セキュア・バイ・デザイン (設計によるセキュリティ)」が実現するのです。多くの場合、失敗の代償はとてつもなく高くつきます。システムにセキュリティを組み込み、今日の脅威に対抗する適切なセキュリティを実現するための最低限の土台に関して業界の合意を形成するという目的の達成に、 このホワイトペーパーが役立つことを願っています。

まとめ

このホワイトペーパーは、導入と拡張の容易な、IoT セキュリティのためのシンプルかつ効果的な参照アーキテクチャを提唱しています。

- デバイスのすべてのコードに暗号による署名と認証を行い、署名されていないコードは実行できないようにすることで、悪意のあるコードによる脅威を軽減します。
- これまでに十億台を超える IoT デバイスを保護してきた、長年の実績がある認証局と信頼モデルを活用し、さらに、リソースの限られた IoT デバイスでも同じレベルのセキュリティを確保できる新たな ECC アルゴリズムを活用することによって、相互認証と暗号化による通信の保護を実現します。
- ホストベースの保護によって悪意のあるデータによる脅威を軽減し、さらにセキュリティ分析によってそれ以外のあらゆる脅威を軽減します。
- 脆弱性や脅威が発見されたら、効果的で安全な、動的システム管理によってそれらを軽減します。

この参照アーキテクチャは、 実績のあるセキュリティ基本原則に基づいています。同時に、 このアーキテクチャを最低限「必要な」セキュリティレベルに絞り込むにあたり、あったら「素晴らしい」けれど前述した要素ほど必要ではない数多くのセキュリティ機能を除外しました。この参照アーキテクチャを最小限の内容にとどめたのは、いくつかの理由があります。私たちはエンジニアリングの専門家として、 セキュリティが必要とされるすべての IoT システムに、 適切かつ容易に実現できる最低限レベルのセキュリティを確立する必要があります。特に保護的セキュリティの

digicert®

専門家が不足していることもあり、 さまざまな業界に同じアーキテクチャを提供できれば、すべての人にとって価値あるものとなります。ここで説明したレベルを「はるかに超える」セキュリティを選ぶ企業もあるでしょう。それは必須ではありませんが、良い選択であり、賞賛すべきことです。業界や、業界内のトップサプライヤやサービスプロバイダには、 前述した最低限のレベルをはるかに超えることを期待しています。しかし、それより大事なことは、4 つの土台のうちどれか 1 つでも「手抜き」をすれば、システムの不正利用によって、あらゆる形の損害を招くことになる、ということです。

詳細情報

製品についてのお問い合わせ:

デジサート・ジャパン合同会社
〒104-0061
東京都中央区銀座6丁目10番地1号
GINZA SIX 8階
https://www.digicert.com
JPN-Info-MPKI@digicert.com
03-4560-3941