IoT セキュリティに HIP を採用？、それとも他に解決策は？

By Stu Bailey, Board of Director, Tempered Networks

IoT は多種多様な“**モノ**”がターゲットです。バーチャルリアリティ（VR）、自動運転とかその他の話題技術とは異なり、IoT のニュースは途絶えることはありません。インターネットに接続する**モノ**は 2020 年までに、200 億～500 億に達すると報告されています。
これらの IoT デバイスすべてを接続するという事は、遠く離れた拠点に電力線を開通させることと同じレベルのスケールであり、個人や企業の人生を変えるようなものです。

現実的に云って容易ではありません。我々は、何とかして膨大な数の IoT デバイスを扱う必要があります。確かにスケールの課題は存在します。IoT デバイスの POC ではよくこの課題にぶつかります。インフラレベルでの IoT デバイスの規模は、企業 IT レベルのスケールとは大きく異なります。データセンターでは数十万から数百万の IoT デバイスが相互に通信することになります。IOT のスケールはチャレンジングですが、ただ参入の障壁ではありません。

運用コストは企業 IoT ビジネスにも影響します

～運用コストは IoT のセキュリティにも直結します～
インターネットに接続されている**モノ**はすべて、悪用される可能性があります。接続される IoT デバイスのセキュリティの観点で見る限りでは、保護コストが高くなることを意味します。ネットワークの多くは、重要な情報を送信している数百万規模のデバイスには対応しますが、小型軽量 IoT デバイスの**モノ**を処理するようには設計されていません。攻撃対象範囲は広がっています。ファイアウォールとか VPN は、大量の IoT デバイスを稼働させたり管理するには高価なリソースを必要とします。ただ、ネットワーク上に接続されている IoT デバイスの数が急激に増加しても、それらのデバイスをセキュアにするために必要な運用コストは、飛躍的に増加するというわけではありません。
ただし、これらのデバイスをセキュアにしないままにするとリスクは大きくなります。企業 IoT でセキュアに保護されていないデバイスは、ハッカーによってアクセスされると、大混乱を招く可能性があります。医療機器に接続されたセンサーを使用して鎮痛薬やインシュリンを制御したり、患者のバイタルサインを監視したり、医師に異常を知らせたり、透析などの救命処置を制御するような医療環境を想像してください。ハッカーたちは、これらの保護されていない医療記録データを盗むために病院のサーバをターゲット

にして侵入します。これらのサーバをハッキングすると、大量のデータ盗難の扉が開き、患者の安全を危険にさらす可能性が出てきます。過剰服用や呼吸器系の鎮痛薬の投与量を強制的に増やすために、患者が自ら注入ポンプをハッキングした実例もあります。

運用コストを大幅に増やすことなく、これらのすべてをセキュアに保護するためにネットワークをどのように改革しますか？

大規模な DDoS 攻撃に対して IoT デバイスが無防備に使用されているという米国調査会社からの報告でもわかるように、IoT を保護するのに IP プロトコルに頼ることはできません。産業界では IP アドレスを使用してネットワークデバイスを識別しますが、IP プロトコルは安全なプロトコルとして設計されていません。IP アドレスは簡単に偽装されます。今日のネットワークのデフォルトは、IoT のセキュリティの複雑さに加えて、すべてのデバイスがネットワーク上に完全に見えてしまいます。

企業が必要とするのは、IoT デバイスの爆発的な普及でセキュリティ対策を講ずるために、アイデンティティと可視性の問題に対処する持続可能な方法が必要です。 このフレームワークは、信頼できるデバイス同士だけがエンタープライズインフラと通信できるように、デバイスとサーバー間、および 1 つのデバイスと別のデバイス間の強力な認証を促進する必要があります。

良いニュースとして、現在、ホスト識別プロトコル（HIP）と呼ばれる業界標準プロトコルのソリューションが存在することです。HIP は IETF HIP ワーキンググループで承認され、過去 15 年間で改善され実用化レベルに達しました。HIP を使用すると、ID は、一意でスプーフィング不可能なアイデンティティベースのアドレスとして認証されたユーザ以外にはまったく見えません。

これは、Tempered Networks がアイデンティティデファインドネットワーク（IDN）を採用するアプローチです。彼らの HIP ベースのソリューションは、既存のネットワークレイヤーへのオーバーレイです。HIP は、新しい識別子ベースによる認証ネットワーキングのパラダイムを実現しました。ここでは、信頼できる ID がすべての接続するための認証として効果的にセキュリティを担保します。HIP サービスと集中型オーケストレーションを組み合わせることで、顧客はどこでも IoT デバイスを安全に接続、セグメント化、クローク、移動、フェイルオーバー、または取り消すことができます。HIP は安全でモバイルでのインターネット接続を実現するために、ネットワーク化されたすべてのクライアント、デバイス、センサー、システム、またはアプリケーションにインストールする必要があります。