Uptane：
地上車両を対象とするソフトウェア アップデート配信のセキュリティ対策

Uptane ホワイトペーパー　《シリーズ 第一弾》

危殆化は、"IF" ではなく "WHEN" の問題

（翻訳：蓼原祥太郎）

作家アイザック・アシモフが 1953 年に著した *"Sally"* [1]という短編小説があります。その舞台である 2057 年の未来世界で描かれた自動車は、自律走行はもちろん、自動車自体が知覚能力を持つまでに進化しています。同作品では、20 世紀半ばの SF 小説らしく、便利で魅力的に見えるテクノロジーにはある程度のリスクが伴うという教訓が示されています。

アシモフがこの小説を出版してから 68 年が経った現在、自動車はまだ知覚能力を持つに至っていません。しかし、知覚能力こそありませんが、自動車に使われる電子部品の数は劇的に多くなりました。今日の自動車に搭載される、ECU と呼ばれるプログラム可能なスマートユニットの数は増え続けており、そこには大規模で複雑なプログラミングコードが含まれています。現代の平均的な自動車に搭載される ECU に含まれるコードの行数は 1 億にも及びます [2]。これは、現代における他のどのオペレーティングシステムも凌駕する規模です。しかし、これらのコードには、今後何年間も発見されないかもしれないプログラミングエラーがいくつも含まれている可能性が高いのです。今日の自動車が数多くの無線通信インターフェースに対応していることもあり、遠隔操作による脆弱性を狙った攻撃の脅威は、さらに差し迫ったものになりました。さらに、複雑なサプライチェーンの中でたくさんのサプライヤが関わっている自動車業界では、ソフ

トウェアが分散して開発されるため、マルウェアを忍び込ませるなど、ハッカーが多種多様な攻撃を企む機会はいくらでもあります。

このような脆弱性を狙った攻撃の結果は、ホワイトハットハッカー [3] によるシミュレーションと、偶発的な事故 [4] の両方によって既に実証済みです。国家主導とみられる実行犯グループや大規模な犯罪組織が関与する車両へのハッキングが多くなった現在、かつてのハッカーたちには持ちえなかった潤沢なリソースを後ろ盾に、ハッカー集団は暗躍しています。これは、悪意のある危殆化がより一般的かつ、潜在的にさらに危険なものになることを意味します。UpStream Security 社が 2020 年 12 月に発行した 2020 年グローバルオートモーティブサイバーセキュリティレポート [5] によると、自動車のエコシステムに対するサイバー攻撃は、2018 年から 2019 年の間に 99%、2016 年を起点とすると 700%も増加しました。サイバー攻撃によって ECU が危殆化されると、警察署にあるパトカー全車両のブレーキの改ざん、事業用車両フリートへのランサムウェアによる攻撃、車両盗難の増加、その他の深刻な事態など、最悪のシナリオにおちいる可能性があります。

20 世紀の SF 作品に描かれた悪夢が、現実的な課題となって 21 世紀の現在に戻ってきたのだと認めることが必要です。現在、「高信頼性」、「高適応性」、「高回復力」といった特性を持つ、乗用車や小型トラックのための防御システムの開発および実装の重要性は、これまでに無かったほど増しています。

このホワイトペーパーでは、国家レベルの実行犯グループによる攻撃にも耐えることを目的に開発された自動車業界初のソフトウェア更新セキュリティシステムである "Uptane" について説明します。 Uptane が採用するマルチレイヤーの防御機構では、車両や自動車メーカーのインフラへアクセスするためには各階層で異なるレベルのアクセス許可を得なければならないとすることで、自動車用ソフトウェアアップデートのセキュリティ全体が一度に低下するのを防ぎます。このように、複数の階層を組み込んだセキュリティシステムを構築することで、たとえ攻撃者が、サーバーを危殆化したり、

運用担当者を賄賂で買収したり、車両ネットワークへのアクセス権を奪ったりしても、侵入による損害範囲を限定的に抑え込むことができるでしょう。

ソフトウェアアップデートは諸刃の剣…その対応と、自動車のセキュリティ確保の難しさについて

自動車が直接の攻撃対象ではなかったものの、最近あった SolarWinds 製品に対するハッキングでは、システム管理ソフトウェアの更新プログラムにマルウェアを忍び込ませることで、一般企業・政府機関・学術機関などが甚大なデータ侵害を受けました。これは、ソフトウェアは更新する必要があるものの、そこには常にリスクが伴う、ということを再認識させられたインシデントでした。今回の SolarWinds 製品への攻撃は、米国国防総省、国務省、国土安全保障省、財務省、商務省、エネルギー省のコンピュータシステムにも被害を与えたと報じられており、その影響範囲の全体像は未だに明らかになっていません。

しかし、ソフトウェア更新を無視するのも現実的な選択肢とは言えません。ニューヨーク大学タンドン工科校コンピュータサイエンスおよび工学の准教授であり、Uptane 運営委員会のメンバーでもあるジャスティン・カポス氏 (Dr. Justin Cappos) は、「システム保守運用担当者にとってソフトウェアのアップデートは実施するのが当然のことですが、国家レベルの実行犯の攻撃を引き寄せる結果となってしまいました。」と説明しています (2020 年 12 月 20 日 Yahoo Finance) 。ある意味、OEM やサプライヤは八方塞がりだと感じていることでしょう。しかしカポス氏は、「ソフトウェア更新にはリスクが伴うものの、ソフトウェアアップデートを適用しなければ、システムは確実に、間違いなく脆弱化します。古いソフトウェアは脆弱なソフトウェアですから。」と注意を促しています。

自動車メーカーにとって、ソフトウェアアップデートにおけるセキュリティ確保は、従来のサーバーベースの企業向けシステムよりもずっと複雑です。ECU には、限られた

実行メモリ、小容量のストレージ (場合による) 、インターネットに直接接続できない、といった制約があります。さらにソフトウェアアップデートは、多様なサプライヤによって設計および保守運用されている、自動車用デバイスの分散型システム全体に適用させる必要があり、車両を「文鎮」化し、走行不能にしてしまうような不具合が発生する確率を、無視できるほど低いレベルまで下げる必要があります。

どのような脅威があり、なぜセキュアトランスポートとコード署名だけでは不十分なのか?

車載 ECU のソフトウェア更新では、「SOTA (software over the air: ソフトウェア・オーバー・ジ・エア)」 戦略 [8] によって、改訂版のソフトウェアプログラムがインターネット経由で車両に送信されます。この戦略は、従来の「USB フラッシュドライブを配る」、「顧客に整備サービスのために販売店へ車を持ち込むよう依頼する」といった方法よりも、はるかに迅速かつ費用対効果が高い導入の仕組みであり、人気が高まっています。さらに、SOTA 戦略を採用すると、「必須」アップデートの普及率を大幅に向上させることができます。既存の OEM は、この戦略の持つ高いポテンシャルを認識しています。2019 年 5 月、GM は、2020 年型『キャデラック CT5 セダン』に「OTA (over the air: オーバー・ジ・エア)」 ソフトウェア更新機構を採用し、今後 4 年間でこの更新機構を同社の全車種の標準装備にしていくと発表しました [9]。同年フォードも、同社のウェブサイトにて、フル EV の『マスタング・マッハ E 』を皮切りに、米国内で 2020 年以降モデルチェンジする多くの車種に高度な OTA ソフトウェア更新機構を順次搭載していくことを発表しました。また 2021 年、トヨタと日産も、OTA ソフトウェア更新機能を展開開始し、トヨタは『Lexus LS』に搭載予定の新規「Teammate」ドライバーアシスタンスシステムで高速道路でのハンズオフ (手放し) 運転を実現、日産は、2021 年型『アリア』で、ステアリングの応答性を向上させたり、消費電力を低減させたりする走行モードの追加・調整を実施する予定です [11]。

その反面、ECU をインターネットに直接接続するということは、同時に様々な攻撃にさらされること意味します。その中には、SolarWinds の例のように、正規のソフトウェアアップデートを装ってマルウェアを導入するものもあります。このような攻撃を受けた場合の損害は、リコールや売上減など経済的損失だけでなく、人命の損失につながる可能性があります。

ここでは、自動車用ソフトウェアセキュリティシステムが防御の対象とすべき攻撃の種類を以下の 4 つのカテゴリに分類します (後ほど深刻度が高い) 。

アップデートの読み取り: ここでの目的は知的財産を盗むことであり、攻撃者はソフトウェアアップデートの内容を読み取ろうとします。一般的にこれは、リポジトリ (またはソフトウェアイメージに関連するメタデータが格納されたサーバー、時にはソフトウェアイメージそのもの) から車両に送信された暗号化されていないソフトウェアアップデートを読み取る、盗聴攻撃 (Eavesdropping attack) によって達成されます。

アップデートの妨害: このクラスの攻撃では、車両が新たに発見された脆弱性を含むソフトウェアの欠陥を修正できないように、車両のソフトウェアアップデートへのアクセスを妨げることが目的です。これらの攻撃には以下が含まれます:

- ドロップリクエスト攻撃 *(drop-request attack):* 車外または車内のネットワークトラフィックを遮断し、ECU がソフトウェアアップデートを全く受け取れないようにします。
- スローリトリーバル攻撃 *(slow retrieval attack):* ECU へのソフトウェアアップデート配信時間を遅らせて、ECU に修正パッチが届く前に既知のセキュリティ脆弱性を狙って攻撃します。
- フリーズ攻撃 *(freeze attack):* もっと新しいソフトウェアアップデートが存在するにもかかわらず、ECU に 1 バージョン古いアップデートを送信し続けます。

- パーシャルバンドルインストレーション攻撃 *(partial bundle installation attack):* 選択した ECU へのトラフィックを消失させることで、ECU にソフトウェアアップデートの一部のみがインストールされるようにします。

機能の妨害: 以下のいずれかの方法で車両の機能を停止させるこのクラスの攻撃は、脅威度がさらに一段高くなります。

- ロールバック攻撃 *(rollback attack):* ECU を騙して、既知の脆弱性を持つ古いソフトウェアをインストールさせます。
- エンドレスデータ攻撃 *(endless data attack):* ECU の保存領域が無くなるまで無限にデータを送り続けることで、ECU をクラッシュさせます。
- ミックスバンドル攻撃 *(mixed-bundles attack):* 同時にインストールしてはいけない非互換バージョンのソフトウェアアップデートを複数のインストールして、ある ECU をシャットダウンさせます。これは攻撃者が、様々な ECU に対して異なるソフトウェアバンドルを同時に見せることで実現可能になります。
- ミックスアンドマッチ攻撃 *(mix-and-match attack):* 前述の「ミックスバンドル攻撃」と同様、この攻撃も任意の組み合わせの新バージョンソフトウェアアップデートを ECU 群に使用させます。しかしこれは、攻撃者がリポジトリキーを悪用してこのソフトウェアバンドルに署名したことを証明するものであり、より深刻な脅威と言えます。したがって、提供されるソフトウェアアップデートは完全に任意のものである可能性があります。

コントロール:最後に、最も深刻な種類の攻撃は、ECU に攻撃者が選んだソフトウェアが強制的にインストールされ、ECU のコントロール (制御能力) を完全に失うことです。 これは攻撃者が、ECU 内の既存ソフトウェアを悪意のあるソフトウェアプログラムで上書きすることにより、車両のふるまいを任意に変更できることを意味します。

この攻撃に対する最も一般的な防御策は、HyperText Transport Protocol Security (HTTPS) などのセキュアトランスポート通信プロトコル と、ベーシックなコード署名 (例: 単一の鍵を使ってコードを署名する) を利用することです。しかしそれだけでは、セキュアな OTA ソフトウェア更新システムとして十分ではありません。単一の暗号署名は、任意のソフトウェア攻撃に対してある程度の防御効果を発揮しますが、これだけでは前述したような多様な攻撃に対する防御策としては不十分です。さらに単一の署名鍵は、それ自体がシステムの単一障害点となります。攻撃者が、共通署名鍵のコントロールを手に入れるということは、更新可能なすべての ECU の制御能力も手に入れることを意味します。

信頼性の高い OTA ソフトウェアアップデートの実施には、上記のすべての攻撃に対応し、かつ危殆化に対する耐性を持つソリューションが必要です。危殆化に対する耐性を持つシステムでは、リポジトリや署名鍵の制御能力をハッカーに乗っ取られても、システム全体のセキュリティが壊滅的に低下することはありません。さらに、Uptane のように危殆化に対する耐性を持つシステムには、このような攻撃を受けても比較的迅速に回復するための機構が組み込まれています。

Uptane の特徴とは？

Uptane は、ベストプラクティスと競合するものでは無く、むしろ障害耐性が高いソフトウェアのためのベストプラクティスを拡張・改善します。また Uptane は、既存のソフトウェア管理システムを置き換えるものではなく、既存のソフトウェア更新戦略により現実的なアプローチを追加することで、既存のソフトウェア管理システムと連携して動作するように設計されています。先に述べたとおり、Uptane では、危殆化は "If" ではなく "When" の問題であると考えます。つまり、攻撃は**遅かれ早かれ**発生するものなので、最善の防御戦略は、攻撃の被害範囲を限定的に抑え、漏洩被害を最小限にすることができる戦略です。このアプローチを構成する要素は、4 つの設計原則に基づいています。

- 信頼の分離 *(separation of trust):* メタデータの署名に関する責任を分散させることで、1 つの署名鍵が漏洩してもシステムの他の部分に影響を与えないようにします。
- 署名数閾値 *(threshold signatures):* ファイルの真正性を証明するために、ソフトウェアアップデートをダウンロードする前に、少なくとも最低限の数の署名を集めることを要件とします。
- 鍵の明示的・非明示的な失効 *(explicit and implicit revocation of keys):* 悪意を持つ者がマルウェアの認証のためにメタデータを署名し続けることができないように、危殆化された鍵を交換する機構を提供するとともに、鍵に妥当な有効期間を設定します (すなわち、同じ鍵が永続的に使われないようにする)。
- 最も脆弱な鍵のオフライン保持 *(keeping the most vulnerable keys offline):* 特定の署名鍵が、オンラインサービスからいかなる時も利用不可能であることを義務付け、それら署名鍵の盗難や危殆化を困難にします。

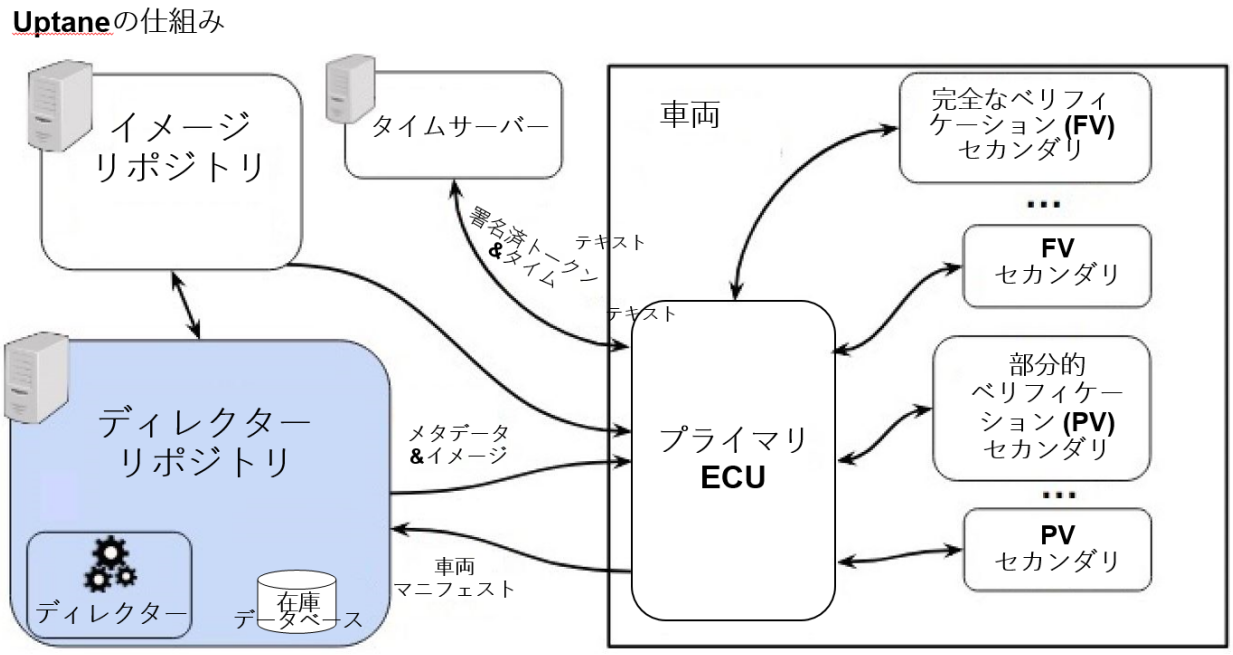
これらの原則は、The Update Framework (TUF) [12] と呼ばれる、ソフトウェア更新システムやソフトウェアリポジトリのセキュリティ確保で実績がある柔軟なフレームワーク・仕様である、既存の標準規格から抜粋されたものです。しかし研究者らは、これらの原則を車載 ECU に適用するにはいくつかの変更が必要だと考えました。

最初の変更点は、ソフトウェア更新のベリフィケーション (検証) プロセスにおける別の側面を分担させるための、第 2 のリポジトリを追加することです。 「イメージ」リポジトリは、OEM が管理する全車両のすべての ECU 内に現時点で存在するすべてのソフトウェアイメージの正確な在庫情報と、対応するメタデータを保持します。 この「イメージ」リポジトリは、オフライン鍵を使って独自のメタデータに署名するので、攻撃者が危殆化したソフトウェアイメージに置き換えることは非常に困難となります。「ディレクター」リポジトリは、次にどのソフトウェアアップデートをインストールすべきかを車両に指示しますが、オンライン鍵を使ってそれ自身のメタデータに署名し、ソフトウェア更新キャンペーンをより容易かつ高速化します。OEM は、これら 2 つの

リポジトリを組み合わせることで、車両に搭載された ECU のカスタマイズ性と強固なセキュリティを両立させることができます。

The Update Framework (TUF) の基本設計に加えられた第 2 の変更点は、Uptane によるソフトウェアアップデートの検証方法に関係しています。ベリフィケーション段階において、ファイルに付随するメタデータを確認することで、ECU はそれをダウンロードしても問題ないかどうかを判断します。ECU は、その処理能力や他のリソースに応じて、完全なベリフィケーション (FV: full verification) または部分的ベリフィケーション (PV: partial verification) の 2 種類の検証方法のいずれかを採用するように設計可能です。完全なベリフィケーション (FV) では、署名されたメタデータに含まれるソフトウェアアップデートのハッシュおよびサイズが、「イメージ」リポジトリに保存されているハッシュおよびサイズと一致していることを確認する必要があります。部分的ベリフィケーション (PV) では、「ディレクター」リポジトリから受け取ったメタデータのサブセットの署名確認だけが要求されます。

Uptane の基本設計



上の図は、Uptane システムの「チェック & バランス」の仕組みを示しています。図の右側は車両上のコネクテッド構成要素を、図の左側は各リポジトリを表します。「イメージ」リポジトリは、ソフトウェアイメージに関する「権威ある」情報源であり、OEM またはサプライヤが現在展開しているすべてのイメージを、その信頼性を証明するためのメタデータファイルと併せて保持していると考えることができます。「ディレクター」リポジトリは、各 ECU に配布するソフトウェアアップデートを決定します。

ソフトウェア更新プロセスにおける第 1 のステップとして、車両は、インストールされている全 ECU の車両バージョンマニフェストを「ディレクター」リポジトリに送信します。この車両バージョンマニフェストには、既存のインストール済ソフトウェアイメージに関する署名付き情報が含まれます。この入力に基づいてディレクターは、次にどのソフトウェアイメージをインストールすべきか選択します。メタデータとソフトウェアイメージが車両に配布され、ベリフィケーション (検証) プロセスが車両で実行されます。上の図は、プライマリ ECU が複数のセカンダリ ECU に接続されている様子を示しています。プライマリ ECU は、ディレクターレポジトリおよびイメージリポジトリからソフトウェアイメージとメタデータをダウンロードし、同じ車両に搭載されている 1 つまたは複数のセカンダリ ECU とそれらを共有します。ECU は、「ストレージ領域」、「メモリ」、「電源」、「インターネットへの直接接続 (オプション) 」へのアクセスを有するかどうかという観点から分類されます。また、完全なベリフィケーション (FV) と部分的ベリフィケーション (PV) のどちらのベリフィケーション形態を選択するかは、ECU 上で利用可能なリソースと、安全性および / またはセキュリティにおけるソフトウェアアップデートの重要性に基づいて決定されます。ベリフィケーションのプロセスで問題が見つからなければ、ソフトウェアイメージを ECU にフラッシュすることで車両のバージョンマニフェストが更新可能です。

完全なベリフィケーション (FV) は、比較的複雑な手順を実行するのに十分なメモリおよびストレージのリソースを有する ECU に、より優れた防御効果を提供します。一方どんなに性能が低い ECU であっても、リソースをあまり必要としない部分的ベリフィ

ケーション (PV)方式により、基礎的な防御を実現できます。このように、システム全体のセキュリティが向上します。

市場の変化に合わせて Uptane が進化し続けるために

Uptane は、常に進化しているテクノロジーです。Uptane コミュニティは過去 5 年間、同テクノロジーの標準化に向けて活動してきました。また、学術系、政府系、自動車業界からの多国籍の専門家が結集して、Uptane の仕様の継続的開発の指針となる主な原則を策定しました。Uptane コミュニティが採用している、今後の長期的なテクノロジーの進化を可能にする重要な原則は以下のとおりです。

アジリティ: ここで言うアジリティとは、自動車用ソフトウェア業界の最新トレンドを先取りし、それらに適宜対応していく敏捷性のことです。Uptane プロジェクトでは、このテクノロジーを規定する標準規格 [13] と、OEM や Tier 1 (ティアワン) サプライヤの現場での応用例をまとめたデプロイメントのベストプラクティスの両方に、さまざまな分野の専門家が継続的に貢献していることが大きな利点です [14]。 また、Uptane はオープンソースのプロジェクトですので、「標準規格」、「デプロイメントのベストプラクティス」や提案の変更点を、どなたでも閲覧することができます。 このように、Uptane テクノロジーでは、実際の現場での実装から得られる継続的なフィードバックが役立てられています。

採用の容易さ: 前述のとおり、Uptane はデプロイメントのベストプラクティスと矛盾することがありませんし、ここでのコミットメントの 1 つは、「Uptane フレームワークを統合するだけの目的で、導入企業がソフトウェア更新システムの再構成をする必要が無い」ということです。そのため、Uptane コミュニティは早い段階に、データバインディングのフォーマットまたはその他のプロトコル・操作・使用方法・フォーマットなどを規定しないことを決定しました。代わりに、Uptane 規格チームが Uptane のスペックを詰める際に、「後方互換性・ローカリゼーション・デプロイメントなど相互運

用性に関する側面」と、「信頼性・セキュリティ・機能性のために必須の側面」の 2 つに分ける新しい手法が開発されました。まず、「信頼性・セキュリティ・機能性のために必須の側面」がインストラクションの基礎となる第 1 層として、実際の Uptane 標準規格を構成します。次に第 2 層として、「後方互換性・ローカリゼーション・デプロイメントなど相互運用性に関する側面」のすべての要素の仕様が、Uptane ”POUF" (Protocols, Operations, Usage, and Formats: プロトコル、運用、使用法、およびフォーマット) 文書として指定されています。Uptane 技術では、実装者側に"POUF" [15] を作成する選択肢を与えたことにより、大規模な変更を要求することなく既存の実装の制約条件に適合させることが可能になりました。また、"POUF" の概念により、サプライヤがプロプライエタリ (独自) な設計を共有することなく、必要に応じてサプライヤをソフトウェア更新エコシステムに加えることが容易になります。

進化し続ける規制と規格への対応: 政府と業界がオートモーティブ向けセキュリティ向上の必要性に取り組み始める中、Uptane プロジェクトでは、自動車分野で重要となる OTA ソフトウェア更新やサイバーセキュリティの他の側面を統括する規制および国際規格との整合性を維持することを目指しています。 これは、Uptane 標準規格の継続的な改訂を通じて業界の専門家の知見を活用し、オープンソースの Uptane フォーラムで自動車業界のすべてのステークホルダーからのフィードバックを継続的に提供するように呼びかけることで達成されます。

今後の課題に関する話し合いの開始

新しい自動車がさらに進化し、20 世紀半ばの小説や映画の中で思い描かれていたようなデザインに近づくにつれ、サイバーセキュリティ上の新たな問題が生まれてくることでしょう。現在、Uptane プロジェクトでは、以下の 3 つの課題について話し合いを始めています。現時点では、これらの問題に対する業界の対応は流動的なため、Uptane プロジェクトとして今すぐ解決策を提供する必要はないかもしれません。しかし、Uptane ホワイトペーパーを通じて、私たちの活動を進める上で解決していく必要があ

る重要な問題点を整理することができます。以下に挙げる問題に対処するために、今後数ヶ月から数年かけて新しいホワイトペーパーを出版していく予定です。

連邦政府・州政府・地方自治体からの緊急アップデートを目的とする *ECU* へのアクセス許可

自動車のソフトウェアアップデートの SOTA 配信が高度化するにつれて、米国運輸省 (DOT: Department of Transportation) または州・地方自治体の運輸関連組織、国土安全保障省 (Department of Homeland Security) 、または連邦緊急事態管理庁 (FEMA: Federal Emergency Management Agency) などの政府機関や規制当局は、自動車メーカーに緊急事態における車両へのアクセスを要求する可能性があります。このようなアップデートの例には、交通規則の変更 (例: 国境や州境)、緊急時の経路情報 (US FEMA または US DOT から)、平常時の交通最新情報 (US DOT や他国のそれに相当する機関から)、信頼性の高い地図 (Google など以外) などが考えられます。現時点で、このようなアクセスを求める声は特にありませんが、他の規格のグループもこのような類のシナリオについて議論しています。さらに既に現時点で、携帯電話や、携帯電話に接続された車両のインフォテイメントユニットでは、このようなアップデートが実施されています。このような政府による車両へのアクセスに対応するためには、Uptane 実装の設定方法、特に委任の優先順位付けの方法や、おそらく「ディレクター」リポジトリのデュアル設定 (dual Director repository) への対応など、さらなる議論が必要でしょう。

アフターマーケット製品の使用に関連するセキュリティ上の問題

アフターマーケット自動車用パーツを取り扱う企業は、自動車に機能を追加するためのパーツを新たに作成したり、OEM のサポートが終了したパーツを再利用して再生品として扱ったりします。このようにして、OEM による制御・管理が全く及ばない ECU が、アフターマーケットパーツのサプライヤにより車両に導入されています。また一般的に、アフターマーケットパーツのサプライヤが OEM の設計資料を入手することはでき

ないため、部品の仕組みを調べるためにリバースエンジニアリングに頼らざるを得ない場合が多くなります。リバースエンジニアリングでは、アフターマーケットのサプライヤが ECU に関する設計情報をすべて把握するのはほぼ不可能でしょう。

このトピックは数多くの問題を内包するため、将来のホワイトペーパーの中で、現在可能性がある解決法について効果的に整理できるか試みる予定です。これらの疑問点には以下のようなものがあります:

- 独自のプライマリ ECU を持たないアフターマーケット ECU への対応はどうするか?
- これらのアフターマーケット ECU は、OEM の「ディレクター」リポジトリや「イメージ」リポジトリを利用できるか?
- アフターマーケット ECU が独自のプライマリ ECU を有する場合、それは相互に排他的な ECU の組み合わせを制御する能力を持つか?
- 「ディレクター」の所有権をサードパーティやオーナーに委譲可能か?

政府や業界の規制への対応

Uptane プロジェクトは、変化し続ける規制や規格を継続してモニタリングしています。我々の主な関心は、これらの要件および推奨内容が、「Uptane 規格」と「導入ベストプラクティス事例」に確実に反映されることですが、将来のホワイトペーパーでは、Uptane の設計・実装が以下のような関連規格にどのように適合するかを取り上げる予定です。

- Autosar Update Configuration Module (UCM)　Autosar 更新コンフィグモジュール (UCM)
- UNECEWP29R155&R156 cybersecurity and software update regulations UNECEWP29R155&R156 サイバーセキュリティとソフトウェア更新に関する規制

- ISO/SAE 21434 Road Vehicles: Cybersecurity Engineering　ISO/SAE 21434 公道を走行する車両: サイバーセキュリティエンジニアリング
- ISO 24089 Road Vehicles: Software Updates　ISO 24089 公道を走行する車両: ソフトウェアアップデート
- SAE J3101 Hardware Protected Security Environment　SAE J3101 ハードウェアで防御されているセキュリティ環境
- TCG (Trusted Computing Group) hardware security and remote attestation specs　TCG ハードウェアセキュリティとリモート認証の仕様
- IETF SUIT (Software Updates for IoT Devices) specs　IETF SUIT IoT デバイスのソフトウェアアップデート仕様

詳細情報

Uptane に関する詳細には、公式ウェブサイトを参照してください [16]。このウェブサイトでは、仕様に関する詳細、Uptane の設計と実装の標準規格最新版、デプロイメントのベストプラクティス) 、および過去と今後の会議プレゼンテーション、テスト情報、その他のデータを閲覧できます。これらの資料、ウェブサイト、または Uptane プロジェクトの他の側面に関する質問、フィードバック、提案などを受け付けております。GitHub 上で問題を提起していただくか、フィードバックの内容をメールにて jcappos@nyu.edu まで送ってください。

自動車業界、オープンソースコミュニティ、セキュリティコミュニティに携わる方なら、誰でも Uptane フォーラムに参加いただけます。これは重大なニュース記事を展開したり、Uptane ワークショップ (オフライン) を計画するための小規模なメーリングリストです。Uptane 標準化へ向けた取り組みをコーディネートするため、Uptane 標準規格メーリングリストで Uptane 標準化のイニシアティブについて議論されています。

メーリングリストへの登録には、lad278@nyu.edu までメールにてお申込みください。

引用文献

1. “Sally (Short story),” *Wikipedia.* https://en.wikipedia.org/wiki/Sally_(short_story) .2/22/2021. アクセス日: 6/14/2021.
2. “How Much Code?Cars," *The Code Institute.* https://codeinstitute.net/blog/much-code-cars.アクセス日: 6/14/2021.
3. Greenberg, Andy.“Tesla Responds to Chinese Hack With a Major Security Upgrade,” *Wired.* https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/. 9/27/2016. アクセス日: 6/14/2021.
4. O’Kane, Sean.“Chrysler’s over-the-air update fiasco is limited to the Northeast, but customers are still waiting for a fix,” *The Verge.* https://www.theverge.com/2018/2/14/17013016/fiat-chrysler-ota-update-problem-jeep .2/14/2018. アクセス日: 6/14/2021.
5. Upstream Security.*2020 Global Automotive Cybersecurity Report.* https://upstream.auto/upstream-security-global-automotive-cybersecurity-report-2020/. アクセス日: 6/14/2021.
6. “2020 United States federal government data breach,” *Wikipedia.* https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach.6/12/2021. アクセス日: 6/14/2021.
7. Howley, Daniel.“Why Russia's massive cyberattack is especially insidious,” *Yahoo Finance.* https://au.finance.yahoo.com/news/why-

russias-massive-cyberattack-is-especially-insidious-222912267.html?__s=p54njaazgqic1gqfruk3.12/19/2020. アクセス日: 6/14/2021.

8. Juliussen, Egil.“Remote software update:Future growth business,” *IHS Markit.* https://ihsmarkit.com/research-analysis/remote-software-update-future-growth-business.html. 1/13/2015. アクセス日: 6/14/2021.
9. Hawkins, Andrew J."GM’s new ‘digital nerve system’ will enable over-the-air software updates on all vehicles,” *The Verge.* https://www.theverge.com/2019/5/21/18633000/gm-ota-software-updates-digital-platform-reuss. 5/21/2019. アクセス日: 6/14/2021.
10. “No more FOMO:New Ford over-the-air updates help Mustang Mach-E get even better with time--Without leaving home,” Ford Media Center. https://media.ford.com/content/fordmedia/fna/us/en/news/2020/05/12/new-ford-over-the-air-updates-mustang-mach-e.html. 5/12/2020. アクセス日: 6/14/2021.
11. Oshikiri, Tomoyoshi.“Toyota and Nissan to upgrade driving functions remotely,” *Nikkei Asia.* https://asia.nikkei.com/Business/Automobiles/Toyota-and-Nissan-to-upgrade-driving-functions-remotely. 2/9/2021. アクセス日: 6/14/2021.
12. *The Update Framework Website.* https://theupdateframework.io/. アクセス日: 6/14/2021.
13. *Uptane Standard for Design and Implementation.* https://uptane.github.io/papers/uptane-standard.1.1.0.html. 1/8/2021. アクセス日: 6/14/2021.

14. *Uptane Deployment Best Practices.* https://uptane.github.io/papers/uptane-deployment-best-practices-1.1.0.html. 1/8/2021. アクセス日: 6/14/2021.

15. Moore, Marina, McDonald, Ira, Weimerskirch, André, Awwad, Sebastien, DeLong, Lois Anne, and Cappos, Justin.“Using a Dual-Layer Specification to Offer Selective Interoperability for Uptane.”*ESCAR USA 2020 Special Issue, SAE Int.J. Transp.Cyber. & Privacy* 2(2):113-129, 2019. https://ssl.engineering.nyu.edu/papers/moore_pouf_2020.pdf.

16. *Uptane Website*. https://uptane.github.io/.アクセス日: 6/14/2021.