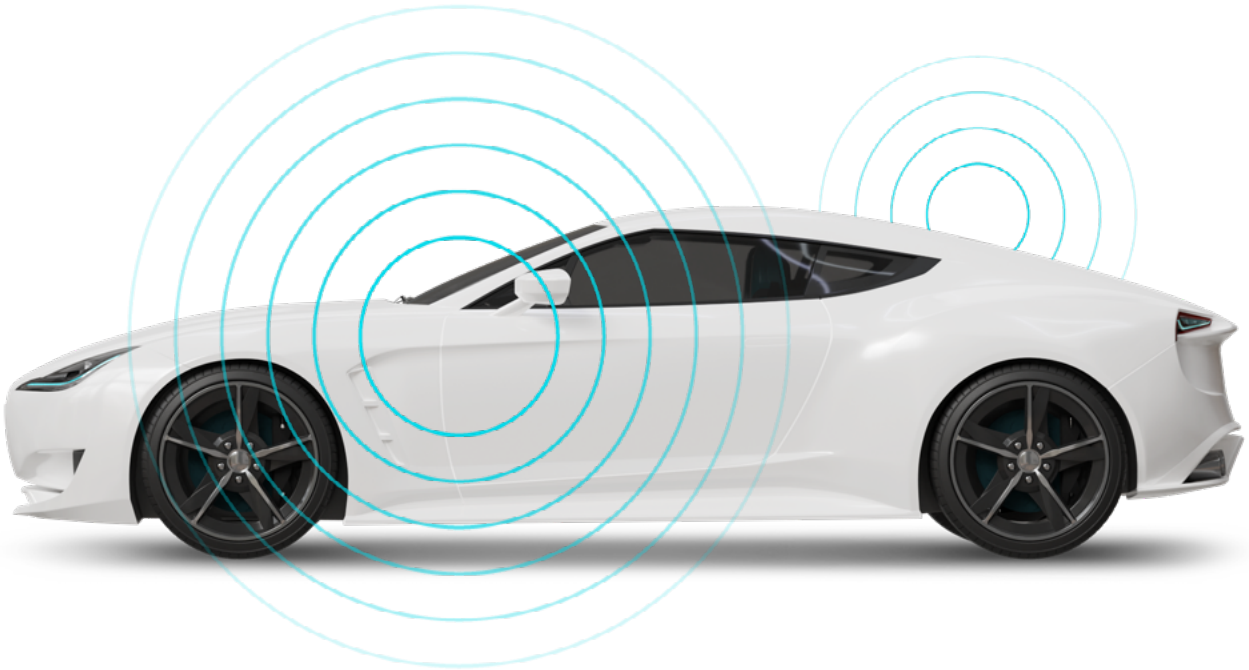
PLAXIDITYX

GO EVERYWHERE

信頼性の確保: V2X通信におけるセキュリティの課題



執筆:

Shahar Shechter、セキュリティリサーチャー

Itay Lidovski、セキュリティリサーチャー

David Lazar、組み込みセキュリティリサーチチームリード

目次

はじめに

V2X(Vehicle-to-Everything)通信は、車両が他の車両、道路インフラ、歩行者、ネットワークといった様々な対象と通信することを可能にする画期的な技術です。この双方向通信技術は、道路の安全性を向上させ、渋滞を緩和し、自動運転の開発を支えます。

本書ではV2X エコシステムの中に実装されている公開鍵基盤(PKI)に焦点を当て、関連する脅威と攻撃領域を検証して、V2Xのセキュリティ上の課題を詳細に分析します。この分野においては、不正なノードを検知してV2Xエコシステム内での信頼性を確立することが重要です。悪意のある行為を検出し、新たなタイプの潜在的攻撃を防ぐには、PKIに加え、新しいセキュリティツールや機能が求められます。

V2Xとは?

V2X(Vehicle-to-Everything)とは、車両とその周囲の環境との情報のやり取りを可能にする通信システムです。これには以下のような様々な形態の通信が含まれます。

1. **車両対車両(Vehicle-to-Vehicle: V2V):** 車両間で速度、位置、道路の状況などを伝え合う、直接的な通信を指します。これにより、衝突事故を防ぎ、周囲と協調した走行が可能になります。
2. **車両対インフラストラクチャ(Vehicle-to-Infrastructure: V2I):** 車両と、信号機、道路標識、料金所といった交通インフラとの通信を指します。これにより、交通の流れが最適化され、渋滞緩和につながります。
3. **車両対歩行者(Vehicle-to-Pedestrian: V2P):** 車両と歩行者や自転車との通信を指し、注意喚起や警告によって道路利用者の安全性が高まります。

一般的なV2Xエコシステムは、車両と他の対象物との間の通信を促進する車載ユニット(OBU)から始まります。OBUは車両のコネクティビティユニット(テレマティクスなど)に統合することも、スタンドアロンユニットとして機能することもできます。これらのOBUは車両と、道路脇に配置されたロードサイドユニット(RSU)との間の通信を可能にします。RSUは車両、インフラ(信号機、道路標識)、クラウドとやり取りを行い、道路からクラウドへのシームレスなデータ交換を実現します。

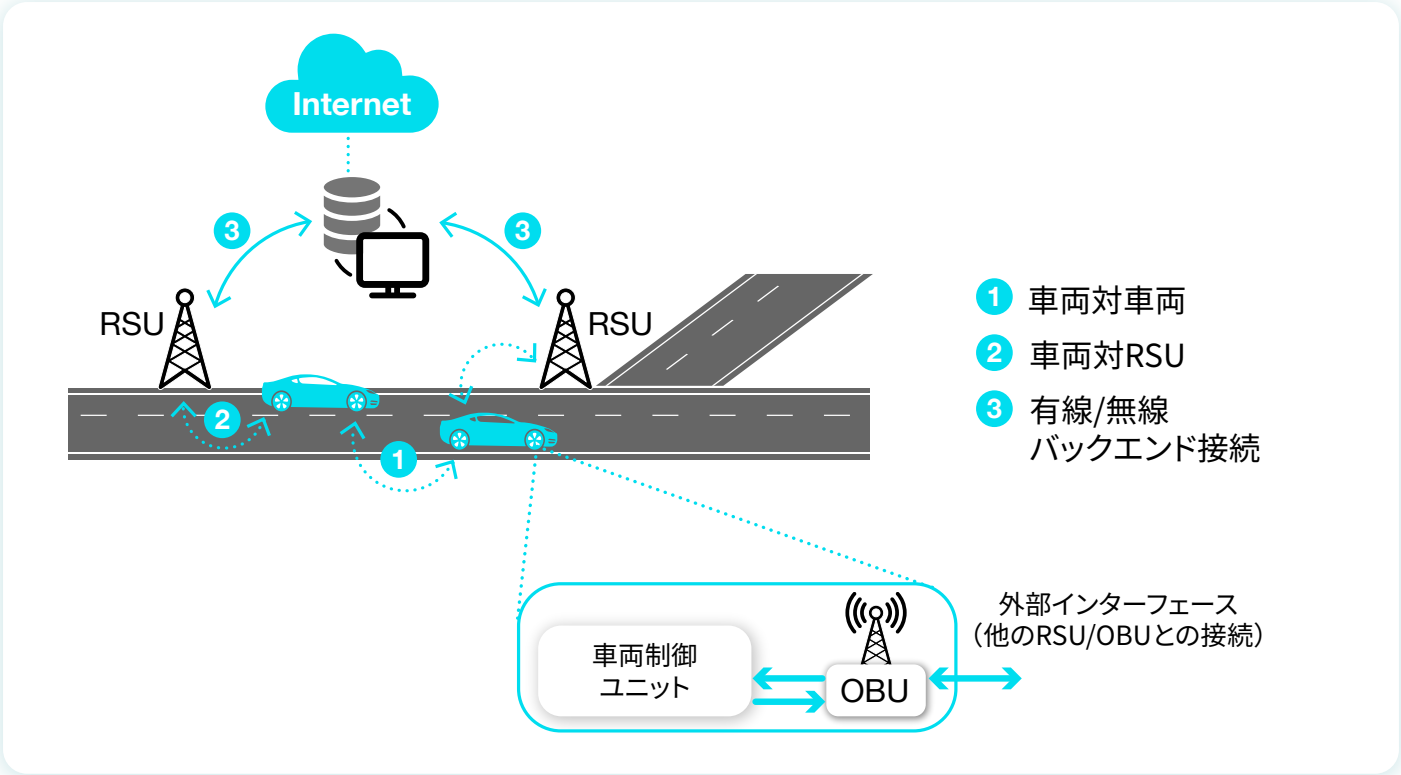


図1. V2X通信エコシステム[1]

短期的には、V2Xはドライバーに警告や情報を提供するアプリをサポートするのに使用され、道路の安全性の向上に寄与します。長期的には、自動運転システムに組み込まれ、カメラ、レーダー、LiDARといった従来のセンサーでは検知できないブラインドスポットにある危険を自動運転システムが検出できるようにします。

例えば、攻撃者が信号機のインフラをハッキングし、すべての信号機を同時に青に変え、事故を引き起こそうとしている状況を検討してみましょう。このような悪意のある行為は従来のセンサーでは検出できない恐れがありますが、V2Xなら異常を検知して車両に警告を発し、衝突事故を防ぐことができます。
V2X技術の採用は、世界中で拡大しています。例えばヨーロッパでは、欧州新車アセスメントプログラム(Euro NCAP)がその安全性評価システムに V2X 機能を組み込んでいます。2023年以降、V2X機能はアセスメントの対象となっています[2]。
米国においては、運輸省(USDOT)がV2X技術の導入を促進する包括的な計画を発表しています[3]。

[1] https://www.semanticscholar.org/paper/Securing-Vehicle-to-Everything-(V2X)-Communication-Hasan-Mohan/e348120357b6f3ff9955c031c7f3d5b91ffea5d7
[2] https://www.eetimes.eu/v2x-communication-paves-pathway-toward-zero-accident-future/
[3] https://www.transportation.gov/briefing-room/usdot-releases-national-deployment-plan-vehicle-everything-v2x-technologies-reduce

共通メッセージと標準の比較

V2X通信には2つの伝送技術があります。

1. **IEEE 802.11p** - 5.9GHz周波数帯域のWLANベース(米国ではDSRC、ヨーロッパではITS-G5とも呼ばれます)。主にヨーロッパで使用されています。
2. **4G/5Gベース**- C-V2Xとも呼ばれます。この標準は携帯電話に容易に統合できることから、他の種類の道路利用者の統合も可能になります。主に米国と中国で使用されています。

その他、ヨーロッパ、米国、中国はそれぞれ独自の規格を持っています。

3. **ヨーロッパ** – ETSIおよびISO規格が使用されています。
4. **米国** – IEEEおよびSAE規格が使用されています。
5. **中国** - GB/TおよびC-SAE規格が使用されています。

本書は、ヨーロッパに関連するETSIおよびISO規格に焦点を当てています。ヨーロッパで使用されているこれらの標準は、車両のOBUとRSUの間で情報を送信し共有する一連のメッセージを定義します。これらのメッセージのタイプには、以下が含まれます:

6. **協調型認識メッセージ(Cooperative Awareness Message: CAM):** CAMメッセージは定期的に送信され、他の車両やロードサイドユニットに車両の位置関係や属性(速度、進行方向、車両の幅など)を伝えます。
7. **分散型環境通知メッセージ(Decentralized Environmental Notification Message: DENM):** 他の道路の使用者に対し、検知されたさまざまなイベント(自動車事故、気象イベント、路上の危険など)について警告を送信します。
8. **集団認知メッセージ (Collective Perception Message: CPM):** センサー、カメラ、その他の情報元によって検知された周囲の物体についての情報を提供します。
9. **信号フェーズおよびタイミング拡張メッセージ (Signal Phase And Timing Extended Message: SPATEM):** 交通信号機により使用され、車両に交通信号の情報を伝えます。

これらのメッセージはASN 1圧縮符号化規則(PER)を使用して定義され、上位レイヤーにはベーシックトランスポートプロトコル (BTP) とGeoNetworking（位置情報利用）プロトコルがあります。

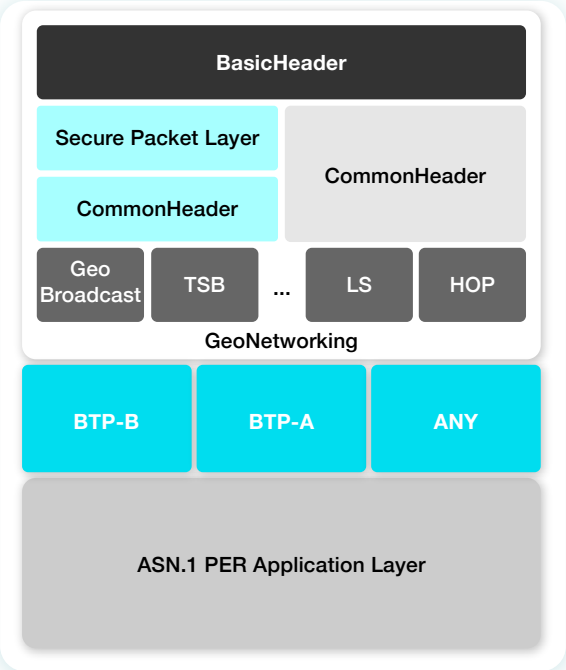


図2. V2Xメッセージの構造（ヨーロッパ標準）

BTPレイヤーがエンドツーエンドの無接続方式のトランスポートサービスを定義するのに対し、GeoNetworkingレイヤーはパケットのルーティングを定義します。ルーティングは次のオプションから定義されます:

- **シングルホップ**: 範囲内にいる送信者と受信者間の直接的通信。
- **マルチホップ**: より遠方にメッセージを送るための中間ノードを通したリレー式通信。
- **GeoBroadcast**: 指定された地理的範囲内のすべてのノードにメッセージを送信。

ヨーロッパと米国の標準でメッセージの名称が異なることがありますが、その機能は類似しています。たとえば、ベーシックセーフティメッセージ(BSM)にはCAMメッセージと同様の情報が含まれています。ヨーロッパ標準のSPATEMの機能は、米国標準のSPATメッセージとよく似ています。

プロトコルスタックにもこうした類似点を見出だすことができます:

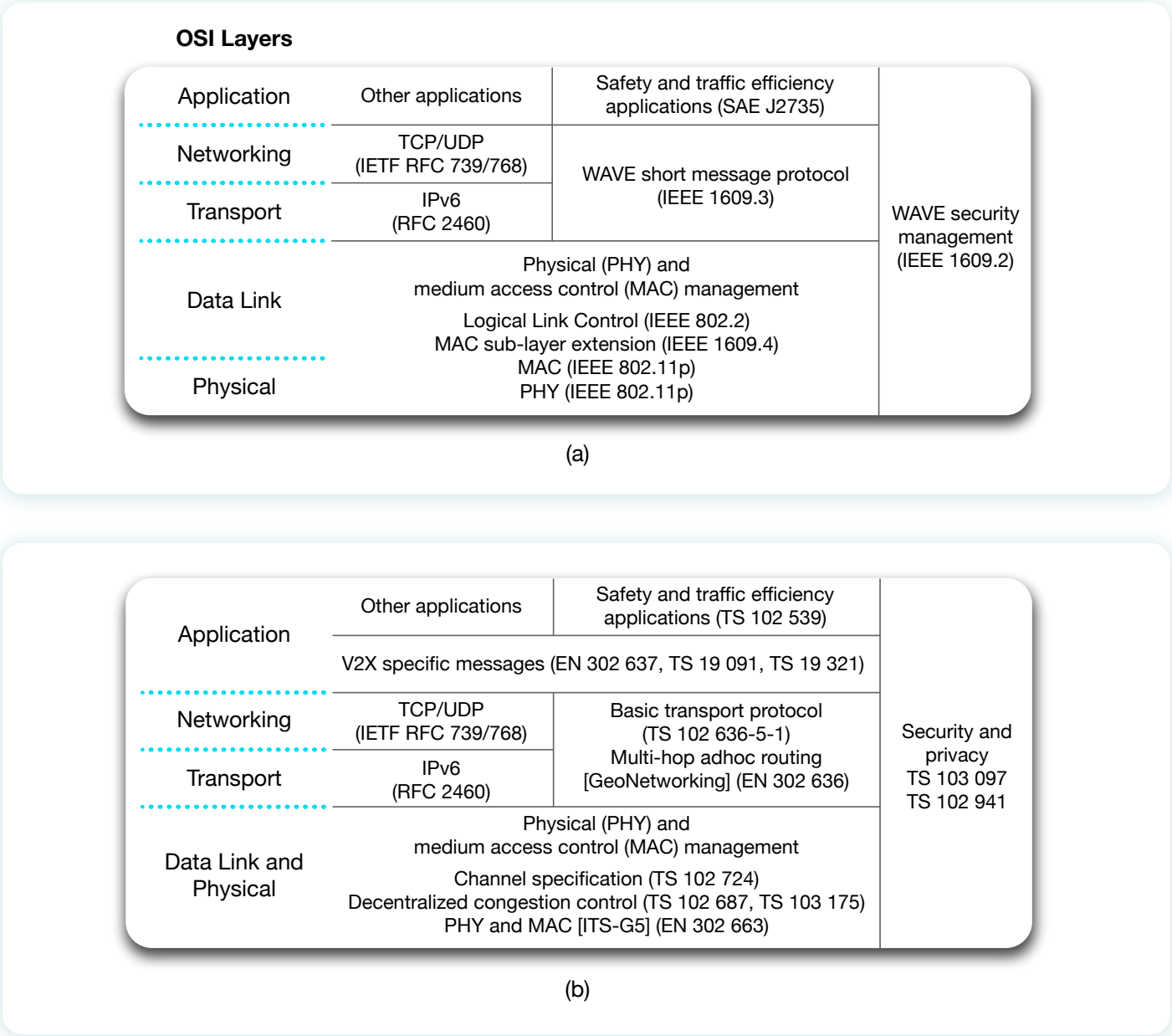


図3. V2X通信のプロトコルスタックと関連する主要標準: (a) 米国(SAE 2945/1)、(b) ヨーロッパ(ETSI-ITS)[4]

[4] Securing Vehicle-to-everything (V2X) communication platforms

V2Xのセキュリティ機能

V2X通信が車両の安全に重要な役割を果たしていることを踏まえると、V2Xネットワーク内に間違った情報や悪意のある情報が混入した場合、渋滞、安全性の低下、そして場合によっては交通事故など、深刻な結果につながる恐れがあります。このため、V2X通信システムには、車両とインフラとの間の通信が安全性と信頼性を保った状態で行えるようにするためのさまざまなセキュリティ機能が組み込まれています。この機能の1つが、メッセージにデジタル署名を行い、送信者を認証しデータの整合性を確保する機能です。リプレイ保護機能ももう1つの重要な機能です。これは、タイムスタンプや、場合によってはシークエンス番号を用いて、攻撃者が古いメッセージを再利用してシステムを欺くことを防止するものです。また、妥当性検証機能は、メッセージの地理的な位置または有効期間を検証し、その情報が正確かつコンテクストに照らして妥当であるかを確認するために用いられます。これらのセキュリティ機能は、全体としてV2Xネットワークの堅牢性を強化し、潜在的な脅威からネットワークを保護し、信頼性の高い通信を確保する役割を果たしています。

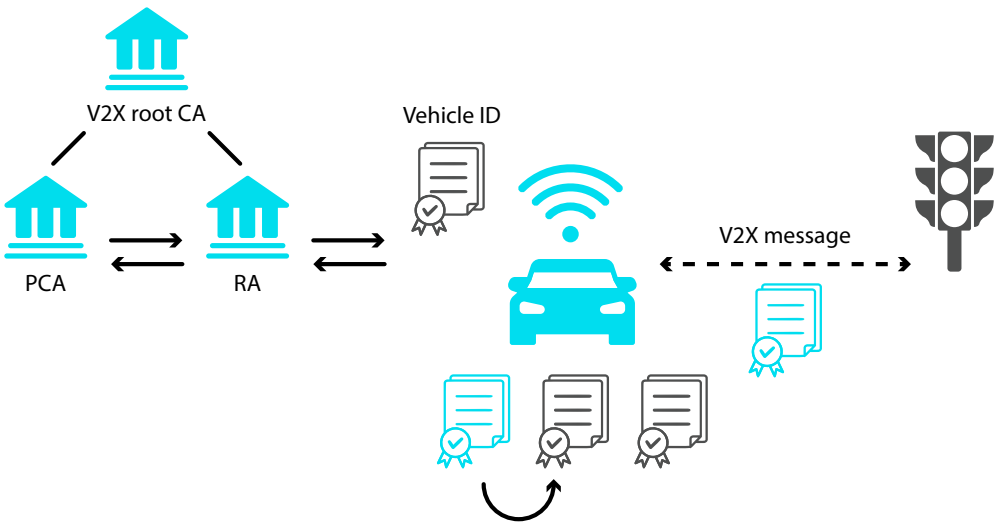
V2X PKI

V2X通信の信頼性とプライバシーを確保するために、堅牢な公開鍵基盤(PKI)が使用されています[5]。

V2Xが搭載された各車両またはデバイスには、車両IDとして知られる、一意の長期にわたり使用される識別子が割り当てられます。車両はこのIDを使用して、登録局(RA)に短期通信証明書をリクエストします。リクエストはRAの公開鍵を使用して暗号化されます。次にRAはこのリクエストを認証局(PCA)へ転送し、PCAは車両に対して短期間のみ有効な複数の仮名証明書を発行します。

この証明書は「認証チケット」として機能し、これには個人情報や車両IDが含まれていないため、プライバシーを保護することができます。

車両はこれらの仮名証明書の1つをアクティベイトし、またセキュリティを強化するために、有効な証明書を頻繁に入れ替えながら使用します。強調型認識メッセージ(CAM)や分散環境通知メッセージ(DENM)といったV2Xメッセージの送受信の際に、この有効な証明書が認証に使用されます。車両は、通信の安全性を確保するために、定期的にRAに対して新しい短期証明書をリクエストします。



[5] ETSI TS 102 941

V2Xのセキュリティ脅威と予想される攻撃シナリオ

上記のセキュリティ機能が組み込まれているにも関わらず、V2X通信システムは、さまざまなセキュリティ脅威にさらされています。

重大な脆弱性の1つは、署名検証が行われる前のネットワークスタック内に存在します。ここでは、攻撃者は、メモリ破損による脆弱性を悪用して、有害なデータやコマンドを送り込むことができます。これにより、最悪の場合、デバイスが完全に侵害される可能性があります。ジャミングやフラッディングなどのサービス拒否(DoS)攻撃は、過剰なトラフィックや信号でネットワークに処理能力以上の負荷をかけ、ネットワークを使用不能にすることで、V2X通信を妨害する恐れがあります。虚偽データが送り込まれると、特に証明書が適切に機能していない場合や、暗号に欠陥がある場合に、別の重大な脅威が引き起こされます。攻撃者は紛らわしい情報を送り込むことができ、車両は虚偽のデータに基づいて危険な判断を下してしまう原因となります。

登録手続きも、攻撃対象領域となり得ます。攻撃者は正当な車両として、または権限を不当に昇格させ、そのような権限を持つ主体として自身を登録し、ネットワークへの不正なアクセス権を獲得することができます。

また、仮名証明書の生成や選択に欠陥があると、車両の匿名性が失われる可能性があります。攻撃者は認証サーバーとの通信を傍受して(特に、データが暗号化されていない場合)車両のIDを明らかにし、プライバシーやセキュリティを侵害します。

V2Xの信頼性における課題

V2Xは新たなアプリケーションやメリットをもたらしますが、それには、ネットワーク内のすべてのノードが信頼できるものでなければならないというコストが伴います。不正なノードが1つあり、それが間違った情報や警告を他のノードに送信すると、路上での行動に影響を及ぼし、安全の問題または事故につながる恐れがあります。

そのため、V2Xのキーポイントの1つは、ネットワークの信頼性を確保することです。これは、先に述べたように、PKIインフラストラクチャを導入することで達成されます。このようなインフラストラクチャにおいては、攻撃者はネットワーク内の他の車両に影響を及ぼすには、メッセージに署名する必要があります。つまり、攻撃者は、取得したOBUの有効な秘密鍵にアクセスしたり、車載ネットワークを経由してOBUに虚偽の車両情報を流したりするために、リソースに投資しなければなりません。こうした防御策は重要ですが、これで十分だとはとても言えません。

セキュリティの世界では、システムの強さはその最も弱い部分で決まります。これはV2Xにも当てはまります。車両ネットワーク内のECUの1つに脆弱性があれば、攻撃者が秘密鍵を抜き取り、コードを実行したり、メッセージに署名したりすることができ、攻撃者がネットワークに侵入し、悪意のあるメッセージを近くの車両に送信するには十分です。
一台の車両に何百ものECUが搭載されている現在、こうしたシナリオが実際に起きる可能性があり、V2Xノードはこの点を考慮に入れる必要があります。

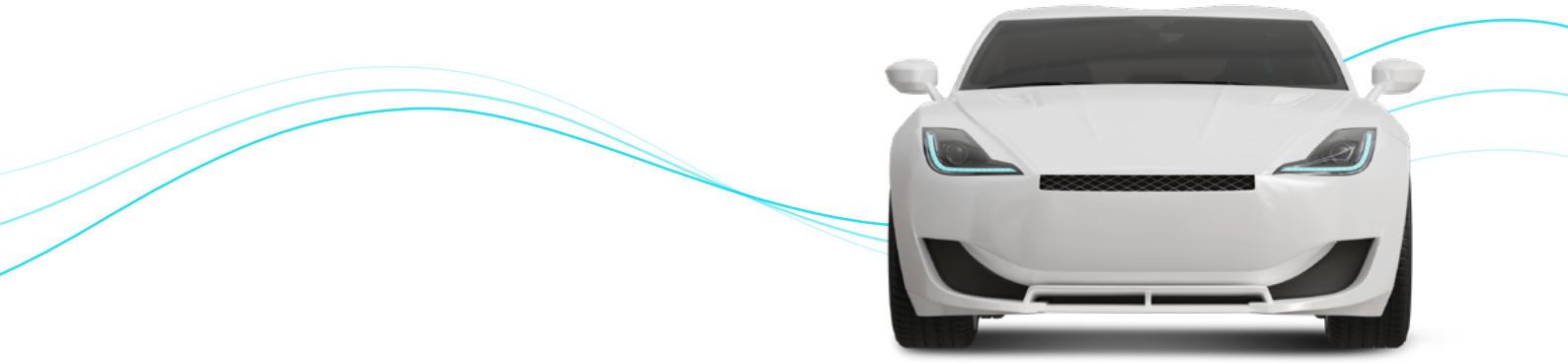
リソースの不足

V2X通信はステートレスであり、インフラ構成要素や他の車両などの相手とその都度信頼を確立する必要があります。信頼を築き、メッセージを認証するには、ノードは送信者の証明書を知っている必要があります。
2つのエンドポイント間のステートフル通信の場合は、証明書は通常初期化状態の一部として送信され、検証され、のちにメッセージを検証するのに使用されます。
しかし、ステートレス環境では、すべての車両の証明書をメモリに保存することはできません。
1つのアプローチは、送信されるすべてのメッセージに証明書を含めることですが、、この場合オーバーヘッドが大幅に増加します。車両と他のユーザーはすべてのメッセージごとに証明書を繰り返し再送信しなければならないため、帯域幅に影響を及ぼし、データスループットが低くなり、レイテンシが高まります。

IEEE 1609.2と**ETSI-103-097**は、このオーバーヘッドを低くする方法を示唆しています。どちらも、数回送信するごとに度証明書を送り、通常は証明書よりはるかにサイズの小さい証明書のハッシュダイジェストのみを送信することを提案しています。車両は実際の証明書とハッシュダイジェストの間のマッピングを保存します。このアプローチでは、帯域幅のオーバーヘッドを大幅に低減することができます。しかしこの方法では、関連する証明書を受信したダイジェストに基づき取得できるよう、車両がメモリに証明書を保存する必要があります。これにより、同時にサポートすべきノードの数に応じて、必要なメモリに制約が生じます。

セキュリティの観点から見ると、実装の仕方によっては、攻撃者は被害者の証明書ストレージをいっぱいにすることで、DoS(サービスの拒否)攻撃の実行を試みる可能性があります。これを行う方法には次のようなものがあります：

1. 攻撃者は公開鍵と秘密鍵のペアを複数取得し、それらを使って、実際の車両を装った有効なメッセージを作成します。
   - 鍵の取得は、PKIプロバイダーのハッキング、職員への賄賂、オンラインで購入された複数のECUのハッキングを通じて実行される可能性があります。
   - プライバシー保護の目的で、各OBUは通常、仮名化に対応できるように複数の証明書を備えています[6]。これは攻撃者が1つOBUを取得することで複数の証明書を手に入れることができる、ということを意味しています。
2. リレーアタック - 遠隔地の車両から被害者にメッセージを送信します。
3. 古いレコード済みのメッセージを再生する - 車両の実装方法に応じて行われます。



[6] ETSI TR 103 415

路上での信頼性の構築

以上、V2Xにおいて、セーフティクリティカルなアプリを保護するためには、ノードの信頼性を確認するだけでは不十分であることがわかりました。不正なノードを検出するメカニズムを追加で導入する必要があります。考えられるソリューションとしては、次のようなものがあります。

侵入検知システム

V2Xプロトコル専用に設計された侵入検知システム(IDS)を導入することで、不正なノードを検出することができます。こうしたIDSは異常の検出に機械学習モデルを使用しています。また、こうした種類の検出にウォッチドッグを使用することについて書かれた論文があります。「Evaluating the Usefulness of Watchdogs for Intrusion Detection in VANETs(VANET での侵入検出におけるウォッチドッグの有用性の評価)」という論文では、侵入検知に対するウォッチドッグモジュールの有効性が評価されています。

コンセンサスアルゴリズム

この種のソリューションは、ネットワーク内のノードがネットワーク内で送信される情報やイベントに集合的に同意する必要があるアルゴリズムに基づいています。

1つの例が、「Proof-of-relevance: Filtering false data via authentic consensus in Vehicle Ad-hoc Networks(関連性の証明: 車両アドホックネットワークにおける本物の合意による偽データのフィルタリング)」という論文で説明されています。この論文では、目撃車両から協力的にイベントに関する本物のコンセンサスを収集することで達成される「関連性の証明 (Proof-Of-Relevance: PoR)」の概念が提示されています。追加のコンセンサスを提供できない攻撃者からのイベントレポートは破棄されます。

相互検証アルゴリズム

この種のソリューションは車両が他のOBUセンサー、RSUから得られた情報を集積し、すべてを相互検証するアルゴリズムに基づいています。

「VANET Alert Endorsement Using Multi-Source Filters(マルチソースフィルターを利用したVANETアラートの承認)」という論文では、車両が悪意のあるメッセージを除外できるようにするVANET環境で使用可能な情報について調査しています。また研究者たちは複数の補完的なソースを活用するメッセージフィルタリングモデルも紹介しています。

ハッカーたちの抱く夢

ワイヤレスインターフェイスは脆弱性を見つけるにはうってつけの場所であり、なによりもハッカーたちを幸せにするのは、リモート コード実行(RCE)の脆弱性です。V2Xは車両にアクセスするための新たな攻撃領域となっています。そのため、車両アーキテクチャプランでは、V2X通信を実行するOBUをその車両の他のECUとは分離しておくことが重要です。V2X がTCU機能の一部として実装されている場合、ハッカーはソフトウェアアップデート、診断、eCallなど、ドライバーの安全とプライバシーに影響を及ぼすその他の機能にアクセスする恐れがあります。

さらに、車両が相互に通信しあうという事実は、多くの車両をコントロールするためのワームを作成するのを容易にします。例えば、V2Xはマルチホップメッセージをサポートしており、車両は送信範囲外にある車両にメッセージを送信することができます。ある特定の種類のOBUに脆弱性を見出した攻撃者について考えてみましょう。マルチホップメッセージを通してその脆弱性を悪用することによって、攻撃者はより多くの車両に影響を及ぼすことができます。脆弱性のないOBUでも脆弱性のあるメッセージを他の車両に送信してしまうからです。

結論

理想的なシナリオにおいては、V2X通信の機能は他に比類がない優れたものです。V2Xは、他のセンサーでは不可能なインサイトをもたらし、命を救う可能性のある重要な安全情報を車両に提供します。

V2Xの要は信頼にあります。V2X通信を通して交換された情報はその正当性と信頼性を確保するために検証を受けることが重要です。これには、データのソースの検証、改ざんの様子がないかの確認、情報がタイムリーであり適切であることを1つ以上のデータソースを使用して検証することが含まれます。このようにすることにより、V2Xはセキュアで信頼性の高いネットワークを維持し、最終的には路上の安全性を高め、悪意のある活動を防止することができます。

PlaxidityXについて

PlaxidityX（プラクシディティ エックス）はArgus Cyber Security Ltd.（アルガスサイバーセキュリティ）として創業しており、モビリティ向けサイバーセキュリティのグローバルリーダーです。自動車メーカー、モビリティメーカー向けにDevSecOps、車両セキュリティ、フリートプロテクションのテクノロジーとサービスを提供しています。
PlaxidityXのソリューションは、自動車のコンポーネント、ネットワーク、フリートがそのライフサイクル全体を通じて安全で規制に適合できるよう支援しています。PlaxidityXのイノベーションとソリューションは、数十年にわたるサイバーセキュリティと自動車に関する研究に基づいており、取得済みと申請中を合わせて80件以上の特許を保有しています。2014年に設立され、PlaxidityXは本社をイスラエルに構え、米国、ドイツ、フランス、日本、韓国、ポーランド、インドに拠点を展開しています。

www.plaxidityx.com/ja