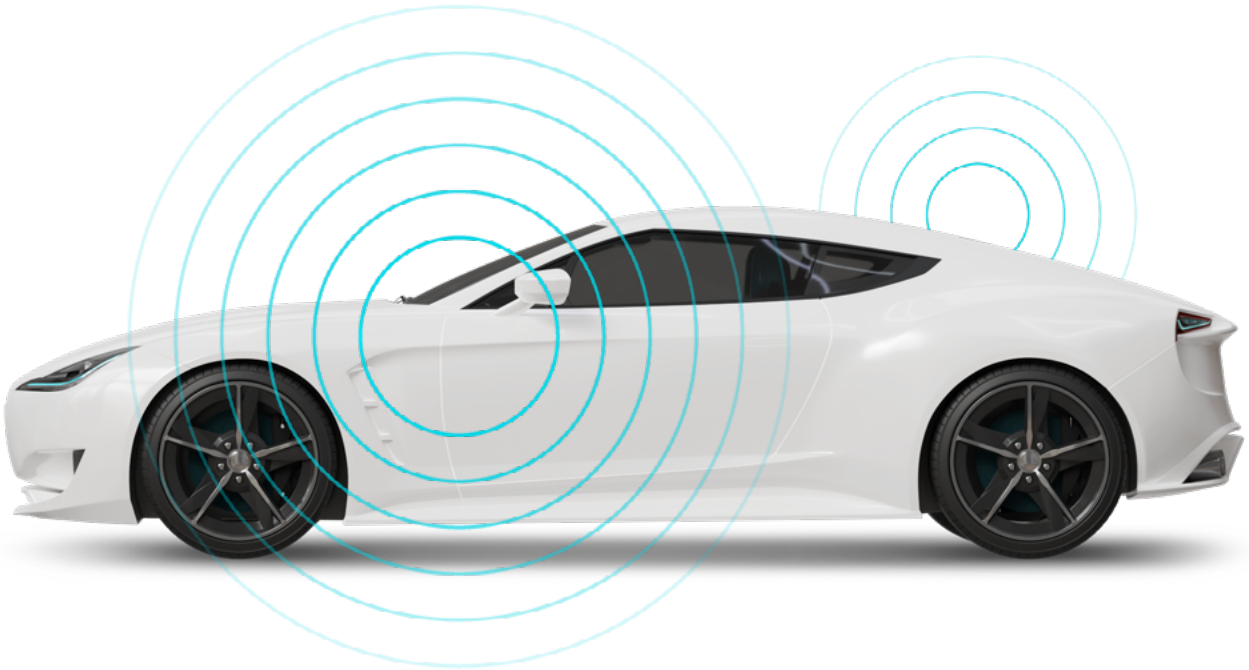
PLAXIDITYX

GO EVERYWHERE

Navigating Trust: Security Challenges in V2X Communications



Authors:

Shahar Shechter, Security Researcher

Itay Lidovski, Security Researcher

David Lazar, Embedded Security Research Team Lead

Table of Content

Introduction

Vehicle-to-Everything (V2X) communication is an innovative technology that enables vehicles to interact with various entities, including other vehicles, road infrastructure, pedestrians, and networks. This interaction enhances road safety, reduces traffic congestion, and supports the development of autonomous driving.

This paper provides an in-depth analysis of V2X security challenges, highlighting the Public Key Infrastructure (PKI) implemented in the V2X ecosystem and examining the associated threats and attack surfaces. In this context, the ability to identify rogue nodes and establish trust within the V2X ecosystem is crucial. New security tools and capabilities, in addition to PKI, are required to detect malicious behavior and prevent new types of potential attacks.

What is V2X?

V2X, or Vehicle-to-Everything, refers to the communication system that enables vehicles to interact with their environment. This encompasses various forms of communication, including:

1. **Vehicle-to-Vehicle (V2V):** Direct communication between vehicles to share information such as speed, position, and road conditions. This helps in collision avoidance and coordinated driving.
2. **Vehicle-to-Infrastructure (V2I):** Interaction between vehicles and road infrastructure like traffic lights, road signs, and toll booths. This can optimize traffic flow and reduce congestion.
3. **Vehicle-to-Pedestrian (V2P):** Communication between vehicles and pedestrians or cyclists, enhancing safety for vulnerable road users through alerts and warnings.

A typical V2X ecosystem begins with an On-Board Unit (OBU) that facilitates communication between the vehicle and other entities. The OBU can either be integrated into the vehicle's connectivity unit (such as Telematics) or function as a standalone unit. These OBUs enable communication between vehicles and roadside units (RSUs) positioned along the road. RSUs, in turn, interact with vehicles, infrastructure (e.g., traffic lights and road signs), and the cloud, enabling seamless data exchange from the road to the cloud.

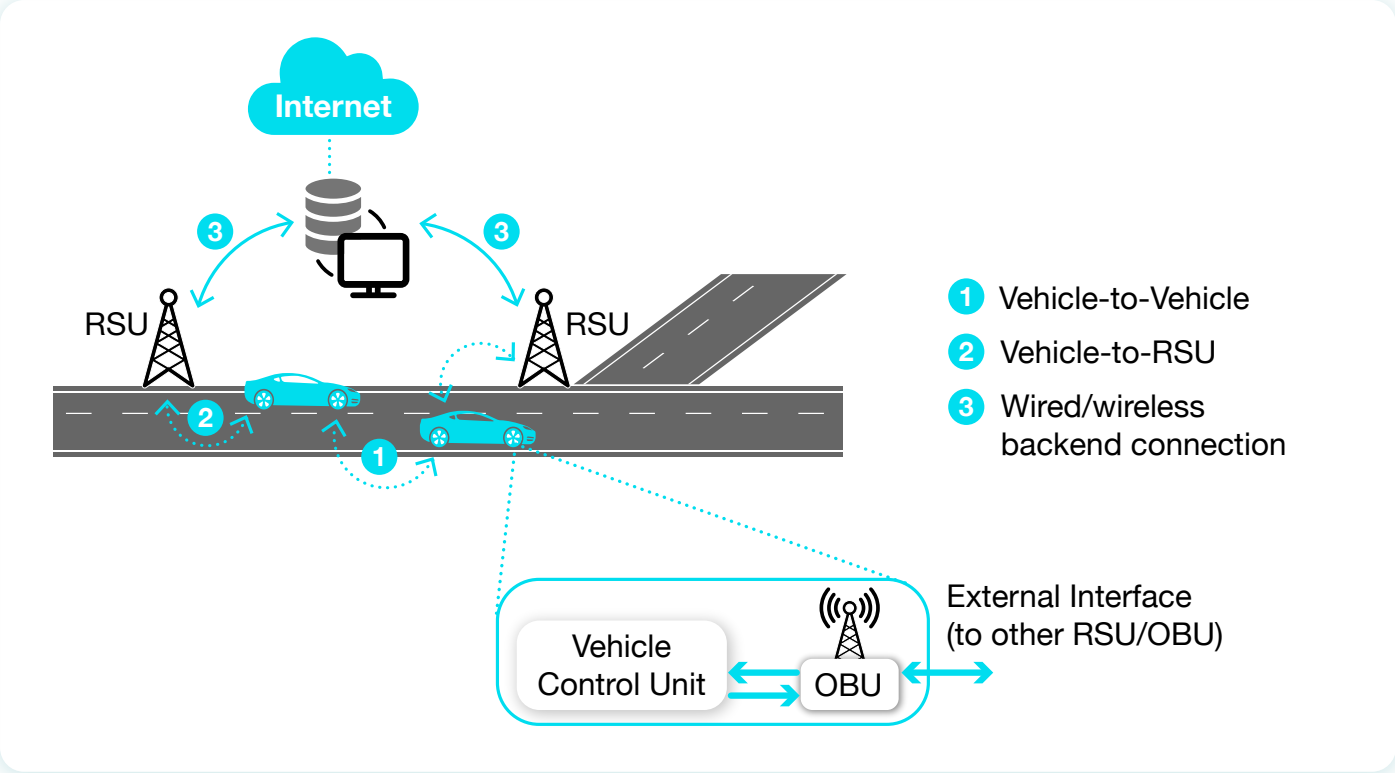


Figure 1. V2X communication ecosystem[1]

In the short term, V2X will be used to support applications that provide warnings and information to the driver to improve road safety. In the long term, V2X could be integrated into autonomous driving systems, allowing these systems to detect hazards in blind spots that are beyond the reach of traditional sensors like cameras, radar, or LiDAR.

For instance, consider a situation where an attacker hacks into the traffic light infrastructure, turning all traffic lights green simultaneously to cause accidents. Such a malicious act might go undetected by conventional sensors, but V2X can identify and alert vehicles to the anomaly, preventing potential collisions.

The adoption of V2X technology is growing globally. In Europe, for example, the European New Car Assessment Programme (Euro NCAP) has integrated V2X features into its safety rating system. Since 2023, V2X capabilities have been considered in the assessment.
In the United States, the Department of Transportation (USDOT) has recently released a comprehensive plan to accelerate the deployment of V2X technologies.

[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

Common Messages and Standards Comparison

There are two transmission technologies for V2X communication:

1. **IEEE 802.11p** - a WLAN-based in the 5.9GHz frequency band (also referred to as DSRC in the U.S. and ITS-G5 in Europe). Mainly relevant to Europe..
2. **4G/5G based** - Also referred to as C-V2X, this standard also allows the integration of other types of road users since it may be easily integrated into cell phones. Mainly relevant for the U.S. and China.

In addition, Europe, the U.S. and China each have its own standards:

3. **Europe** - ETSI and ISO standards are used.
4. **U.S.** - IEEE and SAE standards are used.
5. **China** - GB/T and C-SAE standards are used.

This paper focuses on the ETSI and ISO standards which are relevant for Europe. The European standard defines a set of messages that broadcast and share information between vehicles' OBUs and RSUs. These message types include the following:

6. **Cooperative Awareness Message (CAM):** The CAM message is periodically transmitted to inform other vehicles and roadside units about the vehicle's position dynamics and attributes (e.g., speed, heading, vehicle width, etc.).
7. **Decentralized Environmental Notification Message (DENM):** Provides a way to send alerts to other road users on various detected events (e.g., car accidents, weather events, road hazards, etc.).
8. **Collective Perception Message (CPM):** Offers the possibility to share information about objects in the surroundings, which have been detected by sensors, cameras or other information sources.
9. **Signal Phase And Timing Extended Message (SPATEM):** Used by traffic lights to share traffic signal information to vehicles.

Those messages are defined using ASN 1 Packed Encoding Rules (PER), while the upper layers are the Basic Transport Protocol (BTP) and the GeoNetworking protocols.

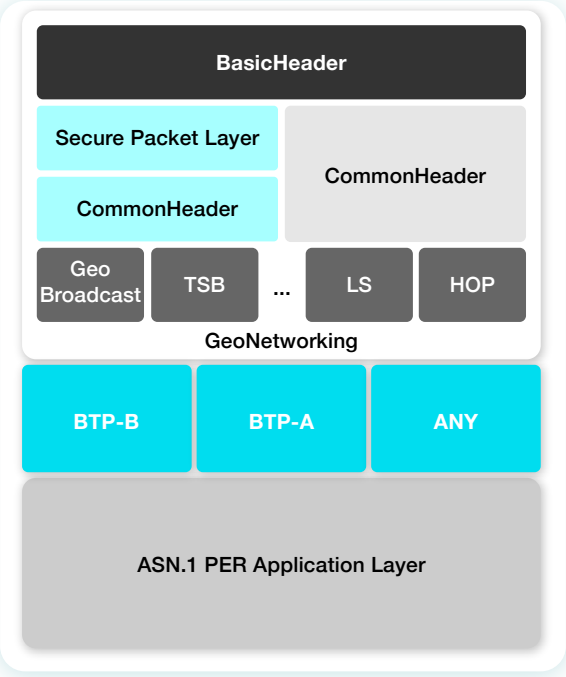


Figure 2. Structure of V2X message (Europe standard)

The BTP layer defines the end-to-end connectionless transport service, while the GeoNetworking layer defines the routing of the packets. Routing is defined from the following options:

- **Single Hop:** Direct communication between sender and receiver within range.
- **Multi Hop:** Relayed communication through intermediate nodes for longer distances.
- **GeoBroadcast:** Broadcasting messages to all nodes within a specified geographical area.

Although the names of the messages sometimes differ in the European and U.S. standards, their functionality is similar. For example, Basic Safety Message (BSM) contains similar information to the CAM message. The SPATEM in the European standard provides similar functionality to the SPAT message in the U.S. standard.

It is also possible to see the similarity in the protocol stack:

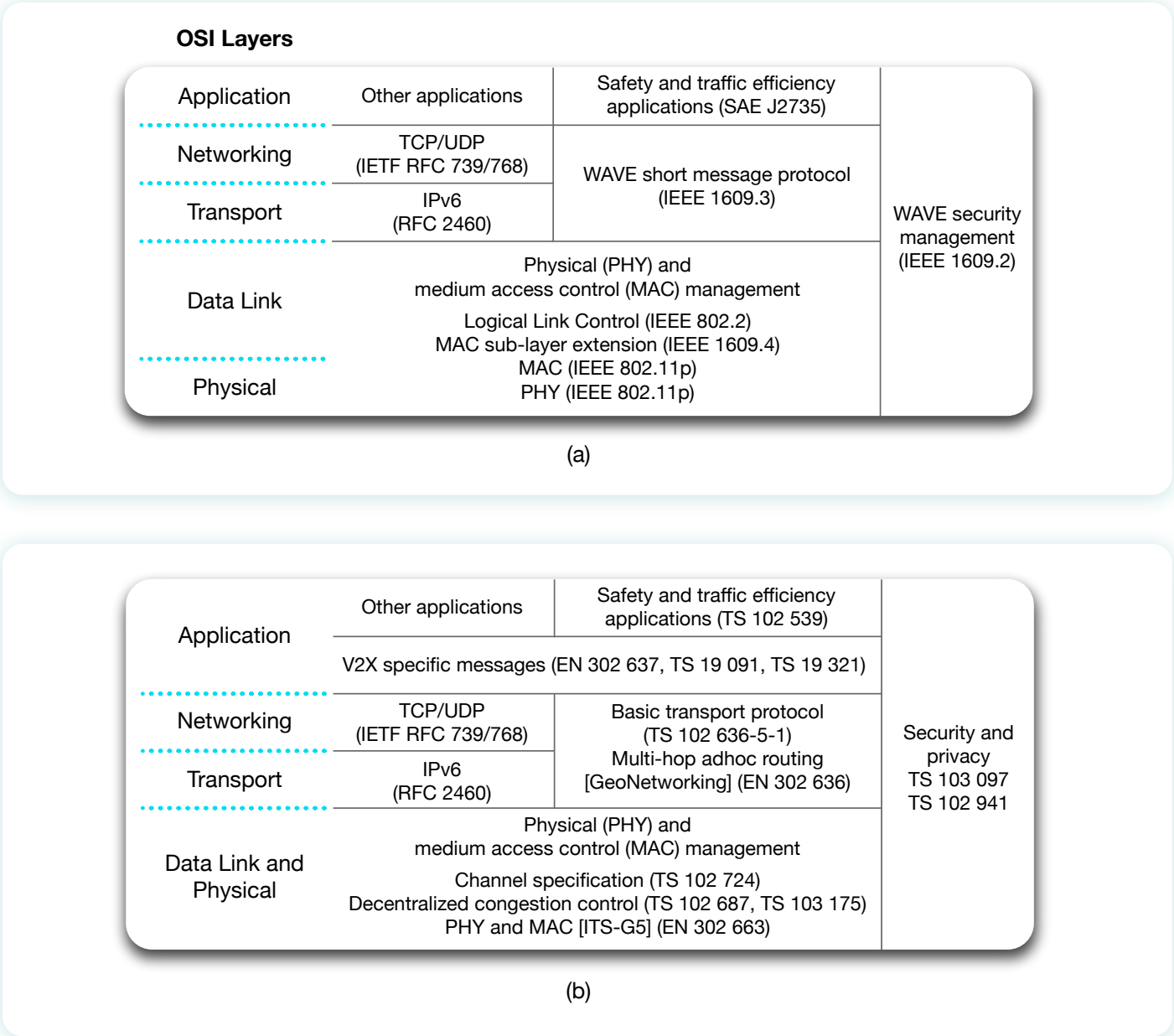


Figure 3. Protocol stack and related core standards for V2X communications: (a) in United States (SAE 2945/1); (b) in Europe (ETSI-ITS)[4]

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

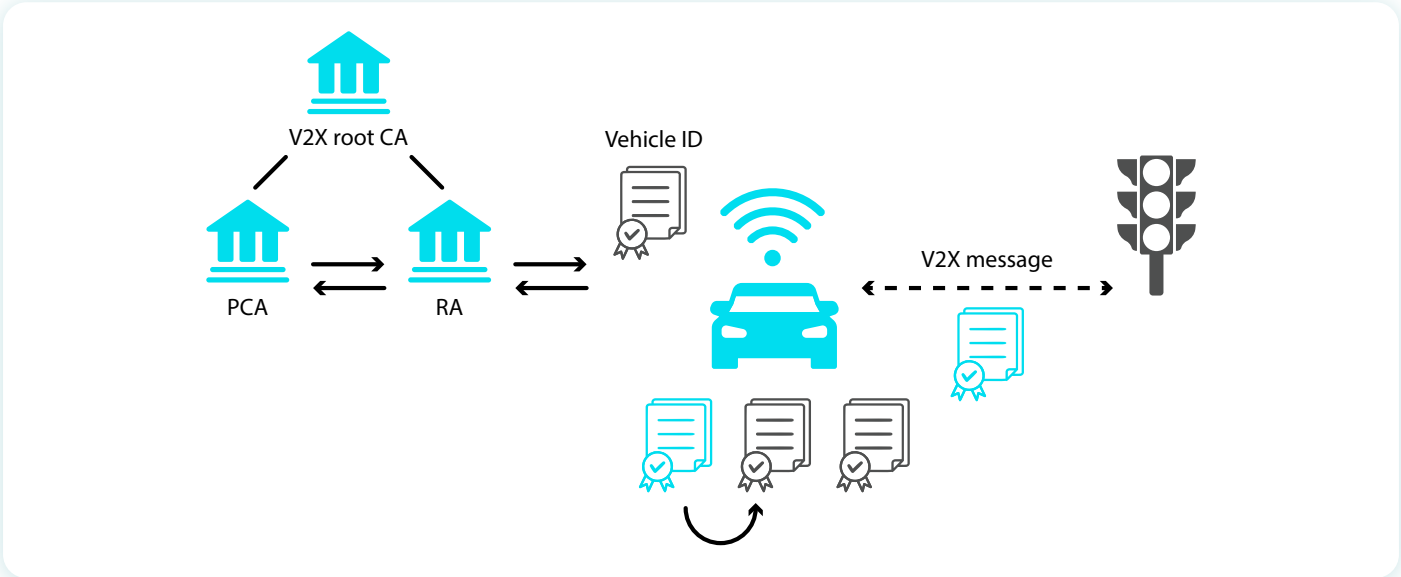
V2X Security Features

Given the critical role of V2X communication in vehicle safety, faulty or malicious information within a V2X network can result in severe consequences, including congestion, compromised safety - and in some cases - even traffic accidents. Therefore, V2X communication systems incorporate various security features to ensure safe and reliable interactions between vehicles and infrastructure. Among these features is digitally signing the message to authenticate the sender and ensure data integrity. Replay protection is another crucial feature, utilizing timestamps and in some cases sequence numbers to prevent attackers from reusing old messages to deceive the system. Additionally, plausibility validation is employed to verify the geographic location or expiration time of messages, ensuring that the information is both accurate and contextually relevant. These security measures collectively enhance the robustness of V2X networks, safeguarding against potential threats and ensuring trustworthy communication.

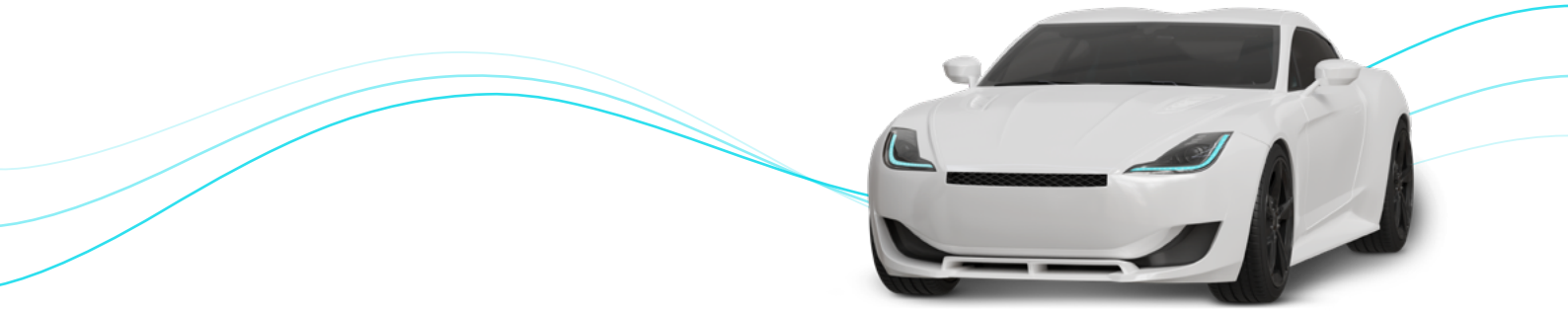
V2X PKI

To ensure authenticity and privacy in V2X communication, a robust Public Key Infrastructure (PKI) is employed[5]. Each V2X-equipped vehicle or device is provisioned with a unique long-term identifier, known as the vehicle ID. The vehicle uses this ID to request **short-lived communication certificates** from the **Registration Authority (RA)**, with the request encrypted using the RA's public key. The RA then forwards this request to the **Pseudonym Certificate Authority (PCA)**, which issues a set of short-lived pseudonym certificates to the vehicle. These certificates act as **'authorization tickets'** and do not contain any personal data or vehicle ID, thereby **preserving privacy**.

The vehicle activates one of these pseudonym certificates and frequently rotates the active certificate to enhance security. When a V2X message, such as a Cooperative Awareness Message (CAM) or Decentralized Environmental Notification Message (DENM), is sent or received, the active certificate is used for authorization. Periodically, the vehicle requests new short-term certificates from the RA to maintain secure communication.



[5] ETSI TS 102 941



V2X Security Threats and Possible Attack Scenarios

Even when the above security features are in place, V2X communication systems are susceptible to various security threats. One significant vulnerability may lie in the network stack before signature validation, where malicious actors can exploit memory corruption vulnerabilities to inject harmful data or commands, which in the worst case can lead to the full compromise of the device. **Denial of Service (DoS) attacks**, such as **jamming and flooding**, can disrupt V2X communications by overwhelming the network with excessive traffic or signals, rendering it unusable. **False data injection** poses another critical threat, especially if certificates are not properly implemented or if there are cryptographic flaws. Attackers can inject misleading information causing vehicles to make dangerous decisions based on false data.

The **registration procedure** is also a potential attack vector. Attackers can register as legitimate vehicles or identities with elevated permissions, gaining unauthorized access to the network. Additionally, **flaws in pseudonym certificate generation** or selection can lead to the **deanonymization** of vehicles. Attackers can sniff communications with the authorization server (particularly if the data is not encrypted) to uncover the true identities of vehicles, compromising privacy and security.

Trust Challenges in V2X

The new possible applications and benefits that V2X provides come with a price - all the nodes in the network must be trusted. One rogue node may transmit wrong information and warnings to other nodes, thus affecting their behavior on the road and potentially leading to safety concerns or even accidents.

Therefore, one of the key points in V2X is to ensure the trustworthiness of the network. This is achieved by deploying a PKI infrastructure, as previously discussed. In such an infrastructure, an attacker would have to be able to sign messages to affect the other vehicles in the network. This means attackers would have to invest resources to access valid secret keys from an acquired OBU or feed false vehicle information to the OBU via the in-vehicle network. This protection is important but it is far from sufficient.

In the security world, a system is only as strong as its weakest link. This is true for V2X as well. One ECU in the vehicle network has a vulnerability that allows attackers to extract the private keys, execute code, or sign messages is enough for the attacker to infiltrate the network and send malicious messages to other vehicles nearby.
With hundreds of ECUs in a single vehicle, such a scenario is likely to occur and V2X nodes should take this into account.

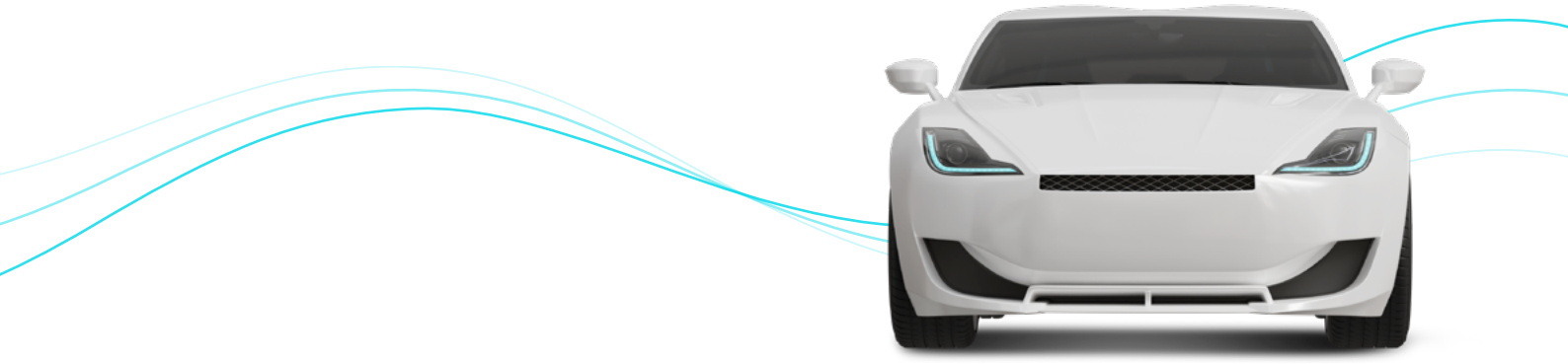
Resource Starvation

V2X communication is stateless and trust needs to be established under it with occasional parties such as infrastructure components and other vehicles. In order to do so and verify messages, the node must know the certificate of the sender.
In stateful communication between two endpoints, the certificate is usually transferred as part of the initialization state, verified, and later used to verify the messages.
However, in a stateless environment, it is not feasible to save the certificates of all the vehicles in memory. One approach is to include the certificate with each transmitted message, but this significantly increases overhead, affecting bandwidth and resulting in lower data throughput and higher latency, because vehicles and other users must repeatedly retransmit their certificates with every message.

The IEEE 1609.2 and the ETSI-103-097 suggest ways to lower this overhead. Both of them suggest sending the certificate once every couple of transmissions and most of the time only send a certificate hash digest, which is substantially smaller than the size of the certificate. The vehicle will store a mapping between the actual certificates and their hash digest. In this approach, the bandwidth overhead is significantly smaller. However, it requires the vehicles to save the certificates in memory to be able to fetch the relevant certificate based on its received digest. This, in turn, puts a constraint on the memory required depending on the number of nodes to support simultaneously.

From a security perspective, depending on implementation, an attacker may attempt to carry out a DoS (Denial of Service) attack by filling up the certificate storage of the victim. There are a couple of ways to do this:

1. Adversary acquired multiple pairs of public-private keys and used them to construct valid messages mimicking real vehicles.
   - Acquiring keys may be performed by hacking a PKI provider, bribing an employee, or hacking multiple ECUs bought online.
   - For the sake of privacy, usually, each OBU will have multiple certificates to support pseudonymization, which means that an attacker may acquire multiple certificates from only one acquired OBU.
2. Relay attack - forwarding messages from remote vehicles to the victim
3. Replaying old recorded messages - depending on the vehicle implementation



Building Trust on the Road

We have seen that authenticating nodes is not enough for safety-critical applications in V2X. Additional mechanisms need to be integrated to detect rogue nodes. Some possible solutions include:

Intrusion Detection System

An Intrusion Detection System (IDS), specifically designed for V2X protocols, could be implemented to detect rogue nodes. Such an IDS uses machine learning models for anomaly detection. There are also articles about using watchdogs for this type of detection. The paper **Evaluating the Usefulness of Watchdogs for Intrusion Detection in VANETs** evaluates the usefulness of watchdog modules for intrusion detection.

Consensus Algorithms

This type of solution is based on algorithms where the nodes in the networks need to collectively agree on the information and events transmitted over the network.

One example is described in the **Proof-of-relevance: Filtering false data via authentic consensus in Vehicle Ad-hoc Networks** paper which presents the notion of Proof-Of-Relevance (PoR) which is accomplished by collecting authentic consensus on the event from witness vehicles in a cooperative way. Event reports from attackers who fail to provide additional consensus are discarded.

Cross Validation Algorithms

This type of solution is based on algorithms where the vehicles aggregate information from other OBUs, sensors, RSUs and cross-validate everything.

The paper **VANET Alert Endorsement Using Multi-Source Filters** explores the information available in a VANET environment to enable vehicles to filter out malicious messages. The researchers also introduce a message-filtering model that leverages multiple complementary sources.

[6] ETSI TR 103 415

Every Hacker's Dream

Wireless interfaces are always an interesting place to look for vulnerabilities. Nothing makes a hacker happier than a Remote Code Execution vulnerability (RCE). The V2X provides a new attack surface to gain access into vehicles. As such it is important to plan the vehicle architecture in a way that separates the OBU, which performs the V2X communication, from the rest of the car's ECUs. In a case where V2X is implemented as part of the TCU functionality, hackers may gain access to additional functionalities, such as Software Update, Diagnostics, or eCall, that may affect driver safety and privacy.

Moreover, the fact that vehicles communicate with each other may make it easier to write worms for taking control of a large number of vehicles. For example, V2X supports multi-hop messages, meaning that vehicles may transmit messages that reach vehicles outside of their transmission range. Consider an attacker who identified a vulnerability in a specific type of OBU. By exploiting the vulnerability through a multi-hop message, the attacker would be able to reach a lot more vehicles, since even non-vulnerable OBUs would forward the vulnerable message to other vehicles.

Conclusion

In an ideal scenario, the capabilities of Vehicle-to-Everything (V2X) communication are unmatched. V2X provides vehicles with critical safety information that can save lives, offering insights that other sensors cannot.

The essence of V2X lies in trust. It is crucial that the information exchanged through V2X communication undergoes validation to ensure its authenticity and reliability. This involves verifying the source of the data, checking for any signs of tampering, and ensuring that the information is timely and relevant using more than one data source. By doing so, V2X can maintain a secure and trustworthy network, ultimately enhancing road safety and preventing malicious activities.

About PlaxidityX

PlaxidityX (formerly named Argus Cyber Security Ltd.) is a global leader in mobility cyber security, providing DevSecOps, vehicle protection and fleet protection technologies and services for automotive and mobility manufacturers.

PlaxidityX's solutions ensure that vehicle components, networks, and fleets are secured and compliant throughout their life cycle. PlaxidityX's innovative methods and solutions are based on decades of cyber security and automotive research and have culminated in over 80 granted and pending patents. Founded in 2014, PlaxidityX is headquartered in Israel, with a global footprint in USA, Germany, France, Japan, Korea, Poland and India.

www.plaxidityx.com