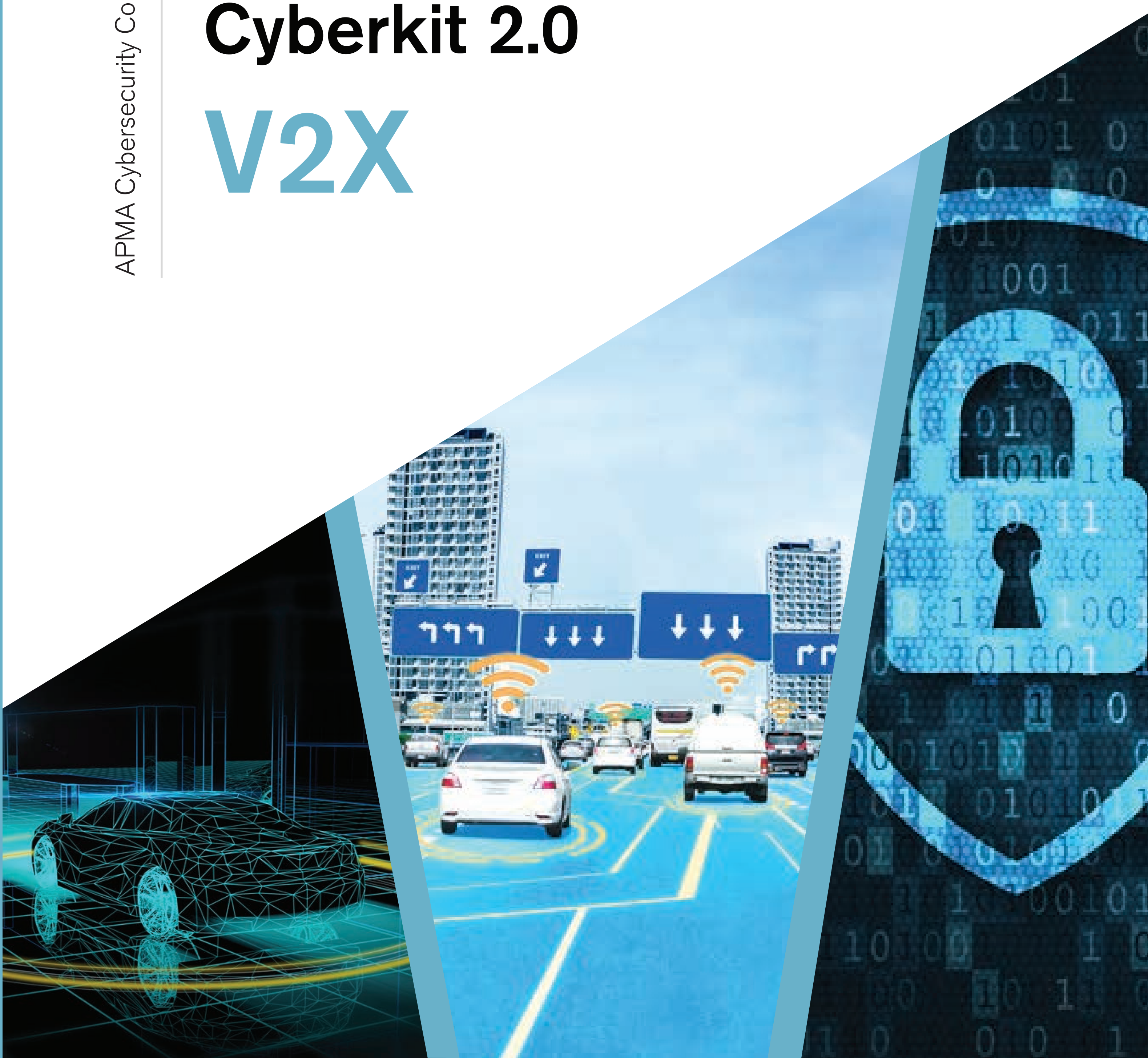
LEAD. REACH. CONNECT.

March 2021

APMA Cybersecurity Committee

Cyberkit 2.0

V2X



CONTENTS

Introduction

Vehicle-to-Everything (V2X) technology is the foundation of tomorrow's connected mobility ecosystem.

Since this technology has a promising and foreseen impact on both public safety and the economic growth of the transportation sector, industry and research communities have shown significant interest in recent years by investing and developing resources in it.

With the emergence of autonomous vehicles, wireless connectivity will become a critical aspect that will enable real-time, reliable communication. To enable this ubiquitous connectivity, a myriad of technology components will be required: roadside infrastructure, dedicated hardware and software on vehicles, all communicating wirelessly and securely, leveraging network and backend services.

All this technology will revolutionize transportation systems and bring a safer experience for the drivers on the road. When fully implemented, it promises to enable sharing a broad spectrum of information, ranging from the direction, speed, and turning status to weather and traffic. The key players in this new mobility ecosystem are the automotive, telecommunication and transport industries.

All this technology will revolutionize transportation systems and bring a safer experience for the drivers on the road.

Advanced Driver-Assistance Systems (ADAS) is part of Autonomous Driving, and there are five levels based on the degree of automation. ADAS is positioned at level 2 of Autonomous Driving, and the driver is responsible for the driving tasks. At level 2, ADAS provides the functions to assist the driver in avoiding accidents, and the drivers make the decision based on these assist functions.

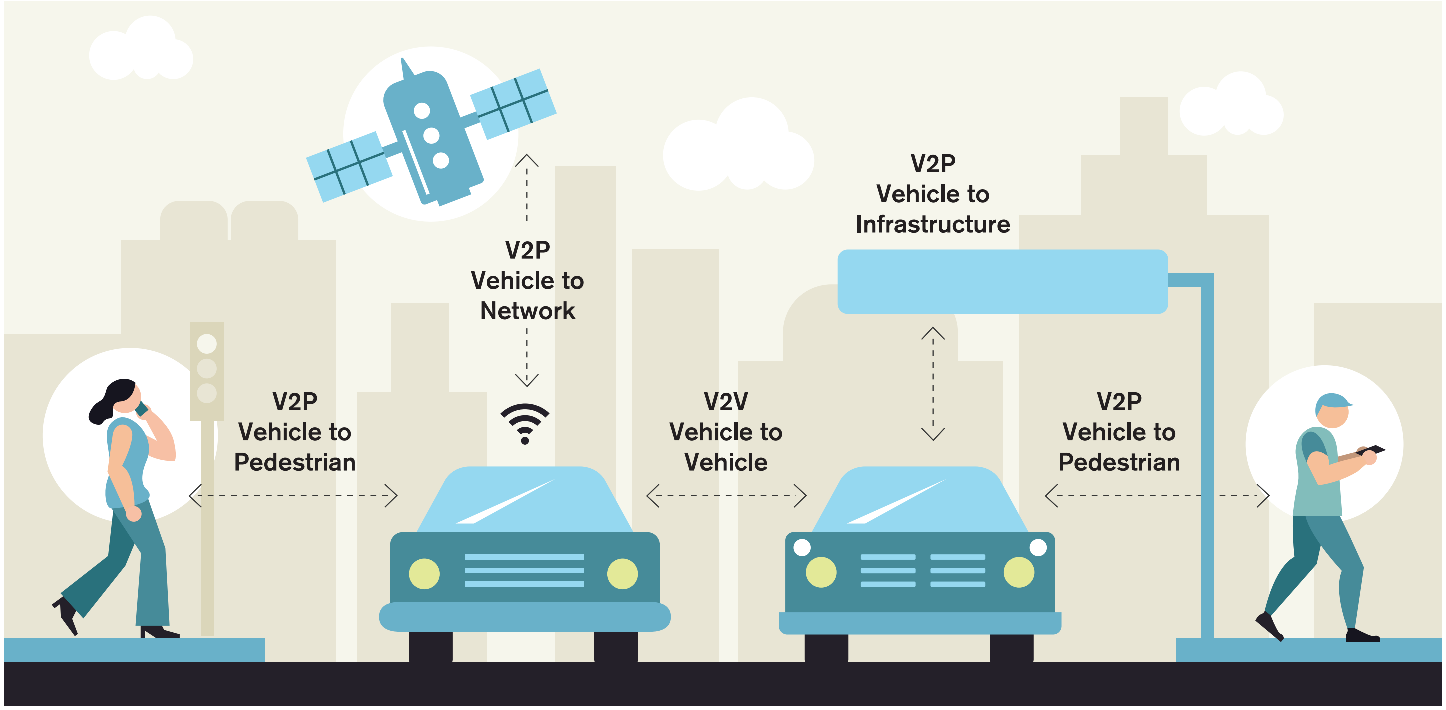
At level 3, the system is responsible for carrying out the driving tasks, and the driver will only take charge when the operation cannot be continued without the driver. At this transitioning level 3, for vehicle safety, V2X will increase the system's capability to process not only the information from the vehicle's sensors but also from its surroundings.

With this amplified situation awareness, the decision making of the system improves for level 3 automated vehicles. This forms the base for fully automated vehicles. For level 4, automated driving systems performs all the driving tasks; however, the driver may still control the vehicle if needed.

Ultimately, at level 5, the system will be fully responsible for making all the decisions, and there would be no need for the driver. The role of the V2X at level 3 and higher levels will be to provide connectivity to the vehicles on the road to the surrounding vehicles and infrastructure. For safety purposes, active safety alerts like Forward Collision Warning, Left Turn Assist, Blind Spot Warning etc., are critical.

On the other hand, the informational alerts to provide the advisories for speed, queue, situation, or lane would significantly help traffic management. Level 2 may not need V2X, but autonomy levels 3, 4 and 5 absolutely need V2X.

The recent advancements in autonomous vehicles have demonstrated the need for sufficiently robust control to eliminate human involvement in driving. This can be accomplished with a complete suite of sensors and communications fused to create complete situational awareness.



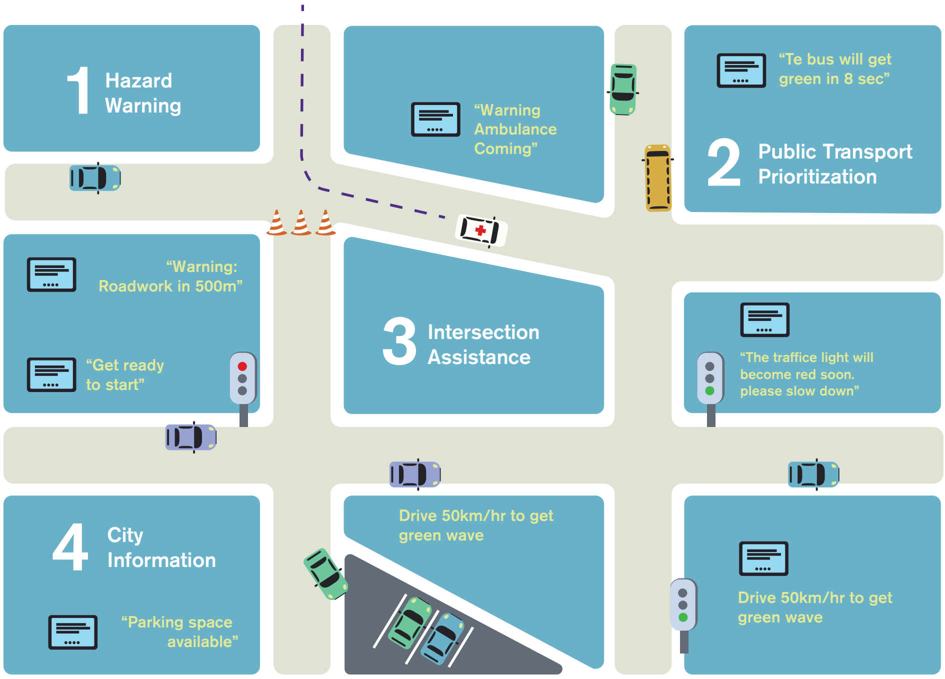
Why V2X is important

Today, many vehicles are equipped with Advanced Driver-Assistance Systems (ADAS), which help the driver by providing safety warnings and alerts.

The extent of ADAS's situational awareness is limited since it senses the immediate environment of the vehicle without direct communication with neighbouring vehicles. In the last two decades, wireless technology has revolutionized various sectors through pervasive connectivity.

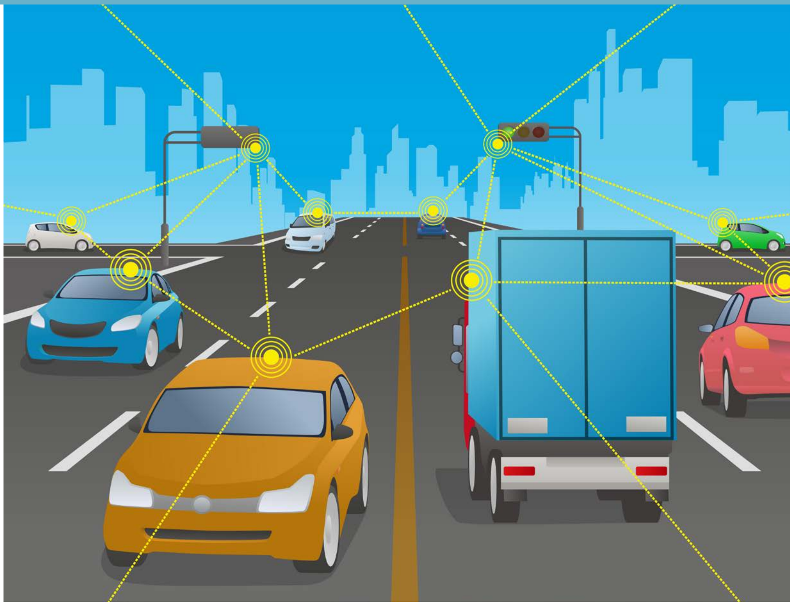
Vehicles are becoming ever more connected to other vehicles on the road to stay informed about the latest information for safe navigation. Vehicle-to-Everything (V2X) communication enables connectivity among the vehicles and nearby infrastructure, which improves the accuracy of safety-related alerts and introduces a new set of safety warnings that were not previously possible with ADAS.

It will also communicate to nearby transportation infrastructure to receive current traffic updates and download the latest maps. These communication services will increase road safety by preventing accidents using alerts and warnings for drivers. Also, V2X will significantly improve traffic management by introducing real-time traffic updates. Vehicle Safety Communication (VSC) technologies are built on IEEE 802.11p and IEEE 1609 standards.


1 Hazard Warning
"Warning Ambulance Coming"
"Te bus will get green in 8 sec"
2 Public Transport Prioritization
"Warning: Roadwork in 500m"
"Get ready to start"
3 Intersection Assistance
"The traffice light will become red soon. please slow down"
4 City Information
"Parking space available"
Drive 50km/hr to get green wave
Drive 50km/hr to get green wave

Vehicles are becoming ever more connected to other vehicles on the road to stay informed about the latest information for safe navigation.

V2X Communication Types and Applications



V2X-capable vehicles have an On-Board Unit (OBU), which enables wireless communication with other vehicles and the Roadside Units (RSUs) that constitute the infrastructure, including traffic signal controllers, roadside signage systems, cameras, and parking meters. These RSUs are directly connected to the back-end service providers such as the Certificate Authority (which deals with short-term certificate provisioning), Location Authority and Law Enforcement Authority.

The primary aim of V2X communication is to reduce the number of fatalities and casualties in road accidents. The secondary goal is to address the problem of traffic jams in cities that contribute to increased air pollution and fuel consumption. Trends indicate that the growing number of vehicles on the road will escalate the latter problem in the coming years.

To address these problems, automotive and telecommunication companies are closely working with Government and Science Institutions to develop various communication networks to enable connectivity among the entities on the road. With such smart technology, the information exchange among pedestrians, vehicles and roadside infrastructure will revolutionize the mobility ecosystem.

The moving vehicles exchange safety information to provide Vehicle-to-Vehicle (V2V) communication by forming ad hoc networks. Vehicle-to-Infrastructure (V2I) communication allows disseminating the information to the vehicles regarding the traffic in the region by collecting the data from these vehicles and providing autonomous vehicles with the same environmental context that drivers absorb by sight and sound. Vehicle-to-Pedestrians (V2P) networks communicate with pedestrians through their smartphones to provide auditory and visual warnings.

When the vehicle communicates with the IT network or data centres, it forms Vehicle-to-Network (V2N) connections. The increasing cloud-based integrations and applications will drive Vehicle-to-Cloud as one of the largest markets in the coming years. These communication types are collectively known as Vehicle-to-Everything (V2X) since they provide the vehicle links with a broad array of recipients.

V2X solves various issues and offer a better driving experience by providing safety warnings, complete route guidance and navigation, and optimal speed recommendations. It introduces efficient logistics solutions, efficient transportation infrastructure, high-quality transportation services and avenues for innovative solutions and services. Some of the additional applications of V2X are Automatic Parking, Emergency Vehicles Coordination, Fleet and Asset Management, Passenger Information System.

V2X Connectivity type: DSRC and Cellular

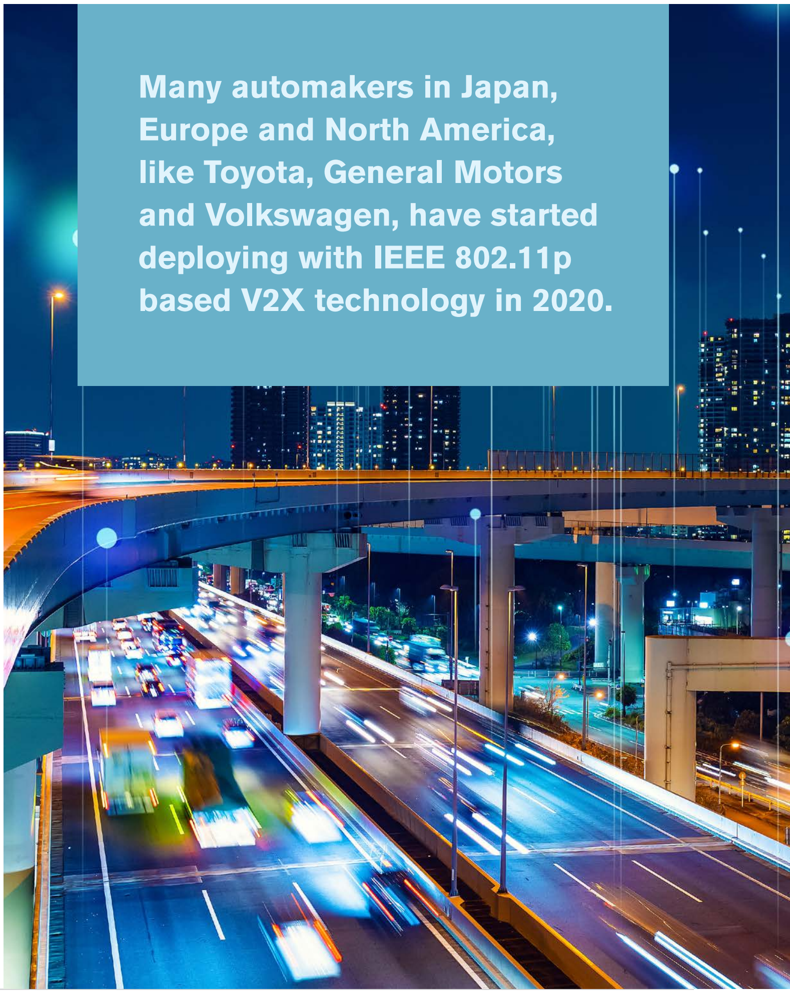
✓ Dedicated Short Range Communication (DSRC) is an IEEE 802.11p based wireless communication technology that enables cooperative awareness. It provides high-speed direct communication for safety among vehicles and nearby infrastructure. DSRC is non-interoperable with cellular networks and uses the Wi-fi standards' variants as the physical and medium access layers of its protocol stack. For the communication among the vehicles, a radio frequency band of 75 MHz on 5.9 GHz of the radio spectrum was reserved for the Intelligent Transportation System (ITS) usage.

Federal Communications Commission (FCC) approved a rule change in Nov 2020, and the new band plan designates the lower 45-megahertz (5.850-5.895 GHz) for unlicensed uses and the upper 30-megahertz (5.895-5.925 GHz) for enhanced automobile safety using Cellular Vehicle-to-Everything (C-V2X) technology.

✓ C-V2X is a 3GPP standard that is the alternative to IEEE 802.11p for V2X communication that uses cellular protocols to provide direct communications between vehicles and obstacles, and it has an evolutionary path towards 5G. Many automakers in Japan, Europe and North America, like Toyota, General Motors and Volkswagen, have started deploying with IEEE 802.11p based V2X technology in 2020.

While the Commission designated DSRC services as the technology standard for ITS services over twenty years ago, DSRC has not been meaningfully deployed, and this critical mid-band spectrum has mostly been unused for decades. This rule change initiates the transition away from DSRC services to hasten ITS services automotive safety improvements. The C-V2X and DSRC technologies have similar capabilities, but C-V2X is relatively untested, and these two technologies are not compatible.

Ultimately, DSRC will fade out, and there will be knowledge transfer to enable C-V2X. Since C-V2X is relatively untested, for the safety concerns, there is a requirement for new technology to go through a whole new round of testing before deployment.



Many automakers in Japan, Europe and North America, like Toyota, General Motors and Volkswagen, have started deploying with IEEE 802.11p based V2X technology in 2020.

V2X Cybersecurity and Privacy

The DSRC have used, and C-V2X is now using the IEEE 1609.2 standard to provide authentication based on digital signatures and certificates for their security layer. To protect privacy, the certificates do not include the driver's information, and the system changes the certificates frequently to make it challenging to track individual vehicles on the road.

The Security Credential Management System (SCMS) for V2X communications has been developed by the Crash Avoidance Metrics Partners LLC (CAMP) under a Cooperative Agreement with the USDOT. Currently, this system design is transitioning from research to Proof-of-Concept and will be used for establishing Public Key Infrastructure (PKI) for V2X security in the United States. It is distinguished from a traditional PKI in various respects. The Cooperative ITS Credentials Management System (CCMS) in Europe is a similar system to SCMS in the US. There are some differences in these two systems based on the intrinsic components and their operations. Security and privacy attacks in V2X communication networks can comprise different threats and roles of adversaries.

Following is a brief introduction to some of the leading security attacks:

- ✓ Bogus Information Attack: The adversary may send fake messages to achieve a specific goal and disrupt communication.
- ✓ Unauthorized Pre-emption Attack: The adversary may illegally request green traffic light.
- ✓ Spoofing Attack: The adversary may illegally access restricted area(s).
- ✓ Message Replay Time-based Attack: The adversary may replay the valid messages previously sent by a valid source to disturb the road traffic.
- ✓ Message Replay Location-based Attack: The adversary may replay the valid messages immediately sent by a valid source at another location to disturb the road traffic.
- ✓ Message Manipulation Attack: The adversary may change the content or source of the message during or after the transmission, including altering the message content.
- ✓ Impersonation Attack: The adversary can pretend to be another entity in the network for its benefit.
- ✓ Denial-of-Service (DoS) Attack: A malicious actor can send a large volume of bogus messages to overwhelm the network capacity that eventually would consume all its resources like network jamming.
- ✓ Sybil Attack: The adversary generates several vehicles on the road with multiple identities, which makes the other vehicles send the messages to false recipients resulting in the benefit of the attacker.
- ✓ Malicious Code attack: The malicious actor injects malicious information in codes such as a virus or worm intending to attack the vehicle system or infrastructure units.
- ✓ Personal Information Leakage: V2X communication network is an openly shared medium, and unprotected information transmission would allow the adversary to intercept the messages within a region. Personal information leakage could result in traceability and identifying mobility patterns.

Cybersecurity is an increasingly urgent issue for the automotive industry as the systems are getting complex with technological advancements such as high-automated & autonomous driving and V2X communications. A rational approach to cybersecurity would be based on understanding risk, which is the combination of the severity and likelihood of successful attacks.

These security risks may seem intimidating when addressed in isolation without using prior knowledge. Therefore, the open professional discussion of needs and approaches with the other industries can benefit the automotive industry in understanding cybersecurity risks based on their lessons learned. The security risks are manageable when handled with appropriate expert attention.

Privacy

Privacy in the Connected Vehicle ecosystem is becoming a big concern because, as connectivity increases, the threat to private information increases along with it. It is vital to consider Privacy Enhancing Technologies (PETs) while developing these systems. Knowledge about a vehicle's actions can reveal a lot about the person driving that vehicle, most obviously location and travel history, but worst-case, it can lead to profiling of individuals.

ITS aims to enable efficient traffic management and a safer driving experience. ITS applications rely on the real-time information of the vehicles on the road. Therefore, a wireless communication network is an essential requirement for data collection. The information associated with a car can infer the driving behaviour when the vehicular sensor information is collected over time. It is predicted that future technologies will equip vehicles with advanced navigation systems and will gather data from more than 200 sensors in a vehicle.

A rational approach to cybersecurity would be based on understanding risk, which is the combination of the severity and likelihood of successful attacks.

This information is primarily intended for communicating road conditions and driving preferences to manage traffic congestion and prevent collisions. However, high precision and sensitive information -- such as location, timestamps and vehicle identifiers -- introduce a privacy threat. With this set of data, precise movement patterns can be inferred along with driving behaviour, leading to long-term driver profiling and vehicle tracking.

Many people are legitimately concerned about their privacy, and automobile manufacturers need to pay attention to the "Privacy by Design" starting at the system design and development phases. The easiest way to ensure privacy is to avoid sharing any driving information and operate as an isolated system, which is the case for most vehicles on the road today. However, this approach will fail to take advantage of the tremendous benefits achieved in a connected vehicular environment. Therefore, a balance is required to optimize what information can be shared and with whom.

Challenges and Opportunities

CHALLENGES

- Vehicles travel long distances cutting across local and international boundaries. To keep the V2X promises, communications must function without interruptions when vehicles cross these borders.
- One of the challenges is the sheer complexity of V2X technology, which encompasses a tremendous amount of information to make safety-related decisions. Therefore, there must be simple wireless mechanisms for deploying, evolving and updating the technology, in which reconfiguration can take place remotely.
- The urban scenario with V2X connectivity would look different than the rural communities. Often, the metropolitan locations are focussed on leveraging such technologies first; however, it is important to notice that, to realize the full potential of V2X, vehicles should have continuous connectivity with other vehicles and the infrastructure. Therefore, widespread roadside infrastructure is necessary for road networks from urban, suburban to rural areas, residential to city centres, and highways to county roads.
- The challenges indicated by the automotive supply chain are the lack of transparency, communication, and collaboration for vehicle cybersecurity.
- The ultimate challenge is to enable this comprehensive operating environment. The technology needs to perform in a robust, reliable, and secure manner in an ever-changing environment with high-speed vehicles while providing low latency safety-related information across this dynamic network. The complex ecosystem with multiple stakeholders is the primary restraint in the market dynamics. This complexity necessitates a bold vision among automotive supply chain contributors, along with a commitment to standards and healthy competition. Creative partnerships will quite likely to create market advantages.

OPPORTUNITIES

- The large volume of data generated by vehicles offers opportunities for Big Data Analytics that would aid traffic management systems.
- The growing Global Automotive V2X market needs to keep up with the continuous evolutions in the V2X ecosystem and Tier 1 Automotive Suppliers should be investing in the continuous R&D of V2X solutions.
- The skyrocketing demand for electric vehicles and shared mobility opens the doors to innovative solutions based on connectivity.
- With cyberattacks in V2X networks, ‘Security’ can be translated as ‘Safety’. With human lives at stake, it is critical to monitor and address the cyberattacks which require skilled and talented personnel with a security mindset and motivation to contribute to societal good.
- Reinforcement of mandates by regulatory bodies for vehicle data protection creates the opportunity for involved stakeholders to collaborate to ensure privacy protection throughout the lifecycle of the vehicle.
- Revenue opportunity associated with applications: civil (first responder traffic light preference), industry (fleet optimization), the consumer (fuel-saving, real-time navigation around nearby impediments), and other innovative value-add capabilities.

EXIT
EXIT
EXIT

V2X Security Standards Landscape

Secure, privacy-preserving, interoperable V2X communication is enabled by several families of standards, many of which have been harmonized across significant regions.

A common approach to security has been adopted to be used over multiple communication mediums, such as Dedicated Short Range Communication (DSRC), ITS-G5, or Cellular-V2X (C-V2X).

The IEEE 1609 family of standards defines Wireless Access in Vehicular Environments (WAVE), built upon the IEEE 802.11p wireless standard [1]. The combination of IEEE 802.11p, IEEE 1609.3, and IEEE 1609.4 make up the DSRC communication protocol. Additionally, IEEE 1609.2 [2] defines a purpose-built, compact certificate format and security services for WAVE messaging. Although defined as part of the IEEE 1609 family, the IEEE 1609.2 certificate format has been harmonized and adopted in Europe, China, and other major regions. The security services defined in IEEE 1609.2 are independent of the underlying communication layer, and the standard is flexible and extensible enough to accommodate a variety of applications.

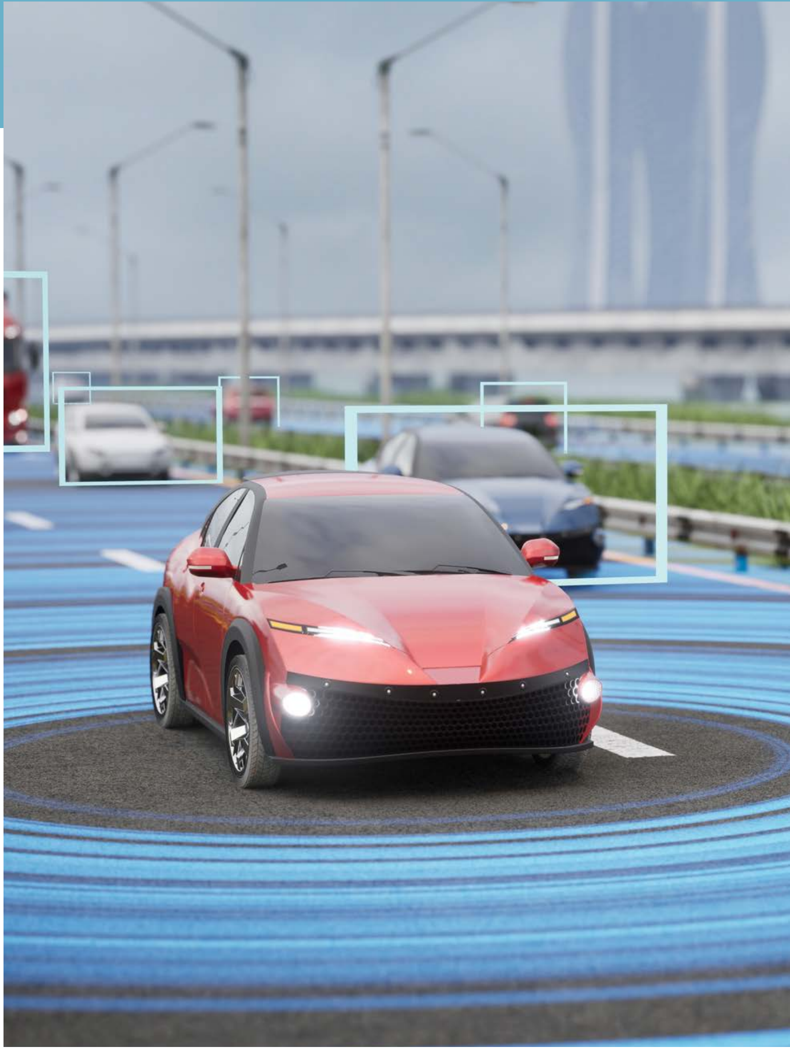
While IEEE 1609.2 defines the underlying security services that enable V2X communication, it does not specify how security credentials should be issued and managed. As of 2021, IEEE 1609.2.1 defines an end entity (device/end-user) interface for issuing and managing private and non-private credentials. This standard is built off earlier work of the Crash Avoidance Metrics Partners LLC (CAMP), an automotive consortium that defined the requirements for the Security Credential Management System (SCMS) to support credential issuing for CV-Pilots in the United States [3]. CAMP's SCMS was cited in a 2016 USDOT notice of proposed rulemaking as the proposed system to secure V2X communication in the United States.

Building upon the IEEE communication and security protocols, the Society of Automotive Engineers (SAE) has defined several standards to guide the deployment of V2X applications, including SAE J2735 [4], which defines a message dictionary of V2X messages for uses cases such as Basic Safety Message (BSM), Signal Phase and Timing (SPaT), Signal Request Messages (SRM), Roadside Alerts (RSA), and Traveller Information

IEEE 1609.2 certificate format has been harmonized and adopted in Europe, China, and other major regions.

Messages (TIM). The SAE J2945 family of standards [5] also defines several requirements relating to the security of devices, specific applications, and behaviours that must be in place to ensure privacy is protected.

The ITS ecosystem is much larger than just the vehicle itself, including infrastructure, traffic management centres, manufacturing and service facilities. The industry has recognized that security spans all areas of the automotive and ITS ecosystem and needs an overarching approach to managing the ecosystem's security. To this end, security frameworks such as the NIST Cybersecurity Framework and SAE J3061 have led to SAE/ISO 21434 [6]: Road Vehicle Cybersecurity Engineering, as an organized approach to cybersecurity in the automotive sector. On the ITS side, frameworks such as the US National ITS Architecture have been developed, which proactively incorporate security and provide guidance on building and deploying secure ITS applications.



Many of the standards presented thus far are focused on the North America market. While the underlying security services have been harmonized across regions, Europe has defined its C-ITS platform, backed by several standards developed under the European Telecommunications Standards Institute (ETSI). This includes an alternative to the SCMS defined in ETSI TS 103 097 [7], ETSI TS 102 940 [8] and ETSI TS 102 941 [9]. The EU also uses different application messages (e.g., Cooperative Awareness Message (CAM), Decentralized Environmental Notice Message (DENM)), though the message contents are similar to their NA counterparts, defined in ETSI TS 102 637, and application security in ETSI TS 102 942 and ETSI TS 102 943.

A final critical component that ensures the secure, long term operation of the V2X ecosystem is an effective governance structure to oversee and administer an ITS deployment. Such an organization assumes policy maintenance and operational oversight over the system and ensures that only trustworthy actors are granted privileges and that privileges are utilized as intended in support of the system's continued operation. Europe has a well-defined Certificate Policy and Security Policy, with the latter defining a governance structure for the C-ITS Platform. Similar initiatives are under development in North America and elsewhere.

On a global scale, the ISO technical committee TC 204 is responsible for ITS and has a comprehensive reaching family of standards governing the ITS ecosystem. While none of the core working groups is dedicated solely to security, it remains a critical consideration in every aspect of an ITS deployment.

Acknowledgements

V2X module:

Flavio Volpe

President, APMA

Colin Dhillon

Chief Technical Officer, APMA

The Automotive Parts Manufacturers' Association (APMA) of Canada President and CTO would like to thank the cybersecurity committee members for their continued efforts to provide leadership and a global voice on the topic of automotive cybersecurity, privacy and cyber safety. The work you have all undertaken is having a positive impact in the complete auto ecosystem.

Dr. Ikjot Saini

Assistant Professor, University of Windsor

We would like to acknowledge Dr. Ikjot Saini, Assistant Professor at the University of Windsor, for leading the development of the V2X module for Cyberkit 2.0.

The APMA would also like to thank the members of its cybersecurity committee for their continued support and ongoing efforts.

Catherine Bertheau - Cyber Solutions Business Dev Lead - Aon
Sumit Bhatia – Director, Communications & Knowledge Mobilization -– Ryerson Cybersecure Catalyst
Todd Bielarczyk - Intelligence Officer - CSIS
Olivier Charron – Microsoft Canada
Sarah Chippure – Senior Policy Analyst - Transport Canada
Ali Dehghantanha – Director – Cyber Science Lab – University of Guelph
Trish Dyl – Director of Partnerships – Ryerson Cybersecure Catalyst
Peter Elliot – Global Information Security Officer – Magna International
John Esvelt – Chief Risk Officer - Dentons
Sebastian Fischmeister – Professor – University of Waterloo
John Heaton – Partner, Cybersecurity - KPMG
Ganesh Iyer - CIO & VP of Eng. - Martinrea
Marc Kneppers - Chief Security Architect – Telus Communications
Philip Lafrance – Standards Manager - Isara
Kevin Magee – Chief Security and Compliance Officer - Microsoft Canada
Siddhartha Parti -Global Director IT, Infrastructure & Ops – Woodbridge
Ken Schultz – General Manager - Escrypt
Jazz Singh – Cybersecurity, IT & Risk – TD Bank
Cara Wolf – Founder & CEO – Ammolite Analytx
John Wright – Founder & Chairman - JPOM

References:

[1] IEEE Vehicular Technology Society, “IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture (IEEE 1609.0),” IEEE Standards Association, New York, 2013.

[2] IEEE Vehicular Technology Society, “IEEE Standard for Wireless Access in Vehicular Environments- Security Services for Applications and Management Messages (IEEE 1609.2),” IEEE Standards Association, New York, 2016.

[3] Crash Avoidance Metrics Partnership (CAMP), “Security Credential Management System Proof–of–Concept Implementation: EE Requirements and Specifications Supporting SCMS Software Release 1.2.2,” CAMP, 2016.

[4] Society of Automotive Engineers, “Dedicated Short Range Communications (DSRC) Message Set Dictionary (SAE J2735),” SAE International, 2016.

[5] Society of Automotive Engineers, “On-Board System Requirements for V2V Safety Communications (SAE J2945/1),” SAE International, 2016.

[6] Society of Automotive Engineers, “ Road Vehicles - Cybersecurity Engineering ISO/SAE DIS 21434,” SAE International, 2020.

[7] European Telecommunications Standards Institute, “TS 103 097: Intelligent Transport Systems (ITS); Security; Security header and certificate formats,” ETSI, Sophia Antipolis, France, 2017.

[8] European Telecommunications Standards Institute, “TS 102 940: Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management,” ETSI, Sophia Antipolis, France, 2018.

[9] European Telecommunications Standards Institute, “TS 102 941: Intelligent Transport System (ITS); Security; Trust and Privacy Management,” ETSI, Sophia Antipolis, France, 2019.

Module: V2X

APMA

LEAD. REACH. CONNECT.