ATIS-I-0000059

Improving Vehicle Cybersecurity

ICT Industry Experience & Perspectives

Abstract

This whitepaper addresses how the Information and Communication Technology (ICT) industry can share lessons learned to assist the vehicle Original Equipment Manufacturers (OEMs) with improving vehicle cyber security, and how the ICT industry and vehicle OEMs can benefit from working together.

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-Internet Protocol (IP) transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user’s attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Contents

1. Introduction

The age of connected and self-driving vehicles is bringing unprecedented new innovations and options to transportation and to other sectors. The greatest risks to this exciting future are those posed by cyber intrusion to the vehicle, and if left unaddressed, these threats have the potential to eclipse the bright future inherent in these innovations. The dangers range from access to the owner's, driver's, or passenger's personal and financial information to outright loss of physical control of the connected vehicle.

The Information and Communication Technology (ICT) industry has extensive experience with cybersecurity and is actively working to continually enhance security in its networks and devices. And because of how central the ICT industry is to the "connected world," it is able to offer cyber intrusion detection and prevention functionality to and across many industries and sectors. With the advent of the connected vehicle, the network reaches into new frontiers as it provides the connectivity for advanced applications and data collection. Yet, until now, the ICT industry and automobile original equipment manufacturers (OEMs) have engaged in limited industry-to-industry dialog regarding how to best address and plan for connected vehicle cybersecurity.

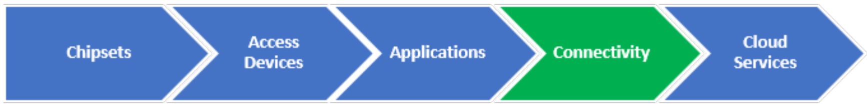
The Alliance for Telecommunications Industry Solutions (ATIS) believes that through collaboration, including the sharing of best practices and lessons learned, that the ICT and vehicle OEMs will be able to mitigate the risk of cyber intrusion in the connected vehicle. This is why ATIS identified the need for and began working toward the opportunity of a consistent and coordinated approach to most effectively share the ICT industry's technical knowledge, experience, and perspectives with the automobile OEMs. This dialog and collaborative work will contribute to increased road safety, improved reliability of connected vehicles, enhanced customer experience, and many other benefits to both industries.

ATIS' diverse membership represents the ICT ecosystem – from telecommunications network providers, to equipment and software suppliers, to device manufacturers, to Internet Service Providers and more. In this white paper, ATIS, on behalf of its members, describes approaches that the ICT industry is currently taking to mitigate the risk of connected vehicle cyber intrusion. The paper also outlines the next steps to advance this critical work. The ICT industry and the vehicle OEMs can collaboratively and cooperatively be successful in improving the cybersecurity of the connected vehicle. This white paper is intended as a starting point and invitation to open the dialog in support of this imperative. As new technology developments, knowledge, and experience emerge in this constantly unfolding area, the opportunity of ongoing dialog will be important to this ever-changing and expanding challenge.

2. ICT Industry

The ICT industry represents a broad and diverse set of companies, functionalities, and capabilities from core chip manufacturers, to communication devices, to telecommunications networks, and cloud services. This white paper concentrates on the functionality and security provided by the **"connectivity"** layer of the ICT industry's value chain, that is by the **telecommunications network carriers** (often referred to herein as telecommunications carriers or networks). These networks deliver connectivity to vehicles and to their drivers and passengers. As a result, vehicles, just like smartphones, can be viewed as end-points or access devices. Outlined below in Figure 1 are the five functions that make up the Basic ICT Value Chain. Subsequent white papers and dialog may address the other elements of the ICT industry value chain as the dialog between the two industries expands.

Figure 1 – Types of Cyber Threats to Vehicles and Their Occupants



3. Alliance for Telecommunication Industry Solutions (ATIS) Representing the ICT Industry

ATIS is a member-driven industry organization representing all aspects of the ICT ecosystem. Members convene to find solutions to their most pressing shared business and technical challenges. ATIS takes a comprehensive approach regarding technical, market, and regulatory impacts to assist its 150 member companies in achieving their business objectives. ATIS also provides its members with a strategic view of the future of technology through access to the Chief Technology Officers (CTOs) of the leading ICT companies.

ATIS is accredited by the American National Standards Institute (ANSI). It is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP) – which is developing 5G standards, a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunications Union (ITU), as well as a member of the Inter-American Telecommunications Commission (CITEL), focused on central and South America.

4. ICT and Vehicle OEMs – Two Platforms Inextricably Linked

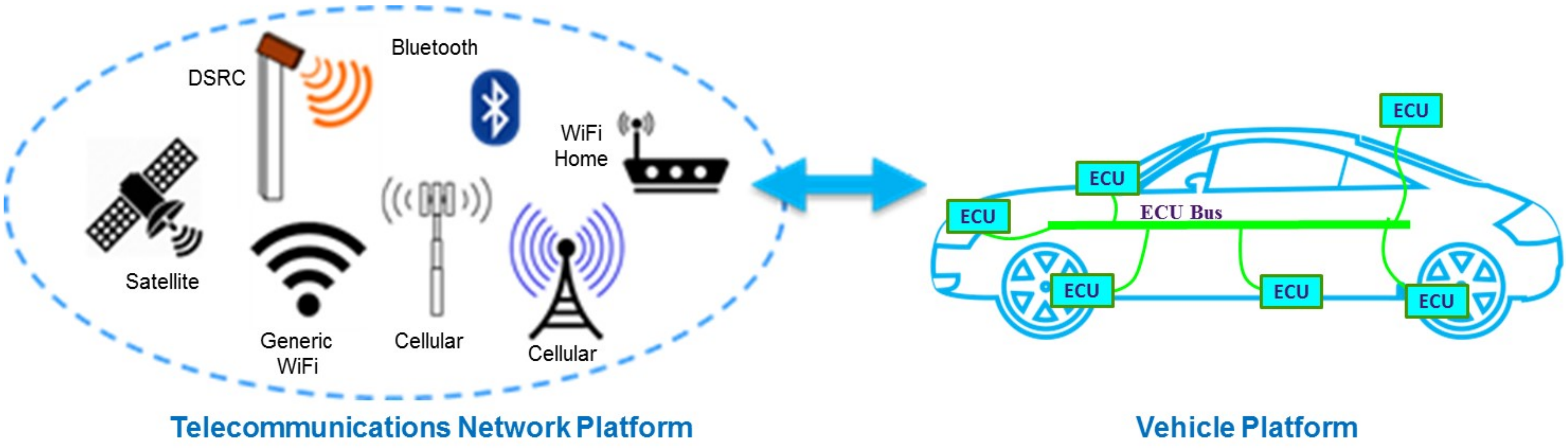
The ICT industry and advanced vehicles are inextricably linked. The ICT industry companies already supply many key technology components to vehicle OEMs, such as chipsets, access devices, telecommunications radios, and applications to enable the development of advanced vehicles. This white paper focuses on the telecommunications network aspect of ICT, which is one of the platforms referred to throughout this document. The other platform is the vehicle platform.

Outlined in Figure 2 in this section, the telecommunications network platform includes Dedicated Short-Range Communication (DSRC), Bluetooth, Wi-Fi, and Cellular connectivity. Also outlined in Figure 2 is the vehicle platform, which consists of computers, busses, Electronic Control Units (ECUs), and sensors. This vehicle platform can also be viewed as an endpoint connected to various networks to receive and send communication, infotainment, and control data.

As vehicle functionality becomes more network connected for automated vehicle control, and as software updates and downloads become more prevalent and dependent on network connectivity, the interrelationship of these two platforms will only increase in importance for all aspects of automated vehicle functionality. As the relationship grows, so should the collaboration between the ICT and automotive industries, which can deliver greater platform-to-platform security, greater end-to-end security, and most importantly, increased safety and privacy for the vehicle's occupants and surrounding environment such as pedestrians and cyclists.

The ICT industry, particularly the telecommunications carriers, are already protecting end-point customers in enterprises, residences, mobile handsets, and vehicles by securing their networks, and in many cases the end device itself. Network security is a core area of expertise for telecommunications network providers. Multiple security features are designed into the basic fabric of the communications infrastructure, allowing telecommunications network providers to offer secure connections to the end user device, often done transparently without any end user-initiated action such as downloading a security application. In addition, carriers leverage the basic security capabilities of the network to offer services to specific market segments. For example, Virtual Private Networks (VPNs) can offer secure dedicated transmission capabilities to enterprise customers, ensuring that all traffic is encrypted end-to-end and receives enhanced security treatment (e.g., firewalls, intrusion detection, or application layer firewalls) as required.

Figure 2 – Industry Platform-to-Platform Collaboration



5. Types of Cybersecurity Risks and Threats

The National Highway Traffic Safety Administration (NHTSA) previously identified direct cyber threats to four types of data or control (see Figure 3). Each of these threat types has the potential to cause disruption to the vehicles and impact drivers, passengers, and the surrounding environment including pedestrians and cyclists. Of the four cyber threats listed in Figure 3, the threat to operational control (which could affect safety such as taking control or compromising steering, braking, acceleration, or sensors that provide vital inputs to these functions) appears to present the highest risk.

Further, cyber intrusion could affect a single vehicle or, far more dangerous, a group of vehicles of a certain make and/or model or having certain parts or software of the same type from the same supplier(s) or using a common communication path. These multiple risk points call for **end-to-end** security between the two platforms – vehicles and telecommunications network as described in Section 4. This entails not only securing the communication paths **outside** of the vehicle but also securing the environment that makes up the **internal** vehicle platform. Providing end-to-end security across these two platforms can be further described as:

1. End-to-end security from outside the vehicle as it communicates with the cloud, with specific servers or with individuals.
2. End-to-end security internal to the vehicle platform. (This includes OEMs and their suppliers, including software and hardware suppliers along the critical data and communication paths within the vehicle.)

Even further risk is presented because vehicles are likely to be connected to more than one telecommunications network using different access devices. It is easy to imagine a scenario in which: the driver has a subscription to Provider A; the vehicle's control radio is subscribed to Provider B; a passenger is subscribed to Provider C; another passenger is connected to Provider D; and the driver’s home Wi-Fi connection is through Provider E and is unmanaged and not secure. These multiple access paths and multiple access networks are a source of serious concern. The ICT industry, especially the network carriers, and the vehicle industry should collaborate to ensure that all communication and connectivity paths are secure from cyber intrusion.

Figure 3 – Types of Cyber Threats to Vehicles and Their Occupants

Privacy/Security	Commercial Transactions (Unwanted/ Unauthorized)	Operational Interference (Non-safety)	Operational Interference (Safety)
Examples			
• Data on the vehicle equipment, systems, suppliers • Data on the vehicle performance location, route • Data on the driver	• Toll pass charges • VIN or other vehicle ID used as payment method • Transceiver linked to payment method	• Control or compromising of vehicle systems (e.g., heater, electronic seat control	• Control or compromising of vehicle systems (e.g., brakes, steering, ADAS equipment, ECUs)

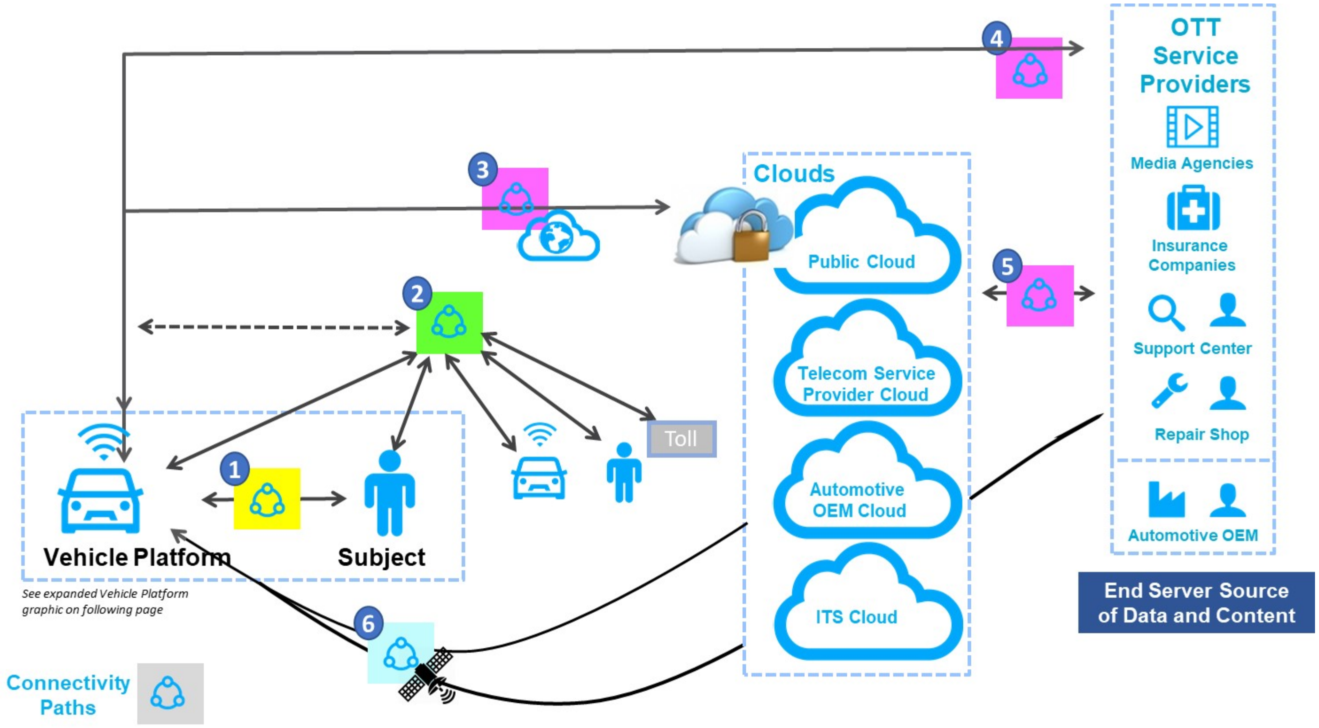
Source: NHTSA

In addition to cyber attacks directed against the vehicle, it is also possible for attacks to be directed against the cloud-based platforms that offer connected vehicle services. If these services are compromised, the attacker could exploit the interfaces to connected vehicle fleets as well as to external-facing commercial and business interfaces to partner organizations. The cloud-based connected vehicle services are likely to be attractive targets since they could contain financial data on many users. In addition, malware planted in these systems could propagate to the vehicles that use the service, leading to widespread infections. With that in mind, the telecommunications network carriers have an important role to play in securing connecitivity to/from cloud services, remote servers and individuals. One way in which the telecommunications carrriers can play this very important role is defined as the Cloud Access Security Broker (CASB) model and is described in detail in Section 9 of this white paper.

6. Telecommunications Network Connectivity Paths

An effective cybersecurity strategy must recognize the many possible communications paths to the connected vehicle. Each of these paths is likely to be provided by a telecommunications network operator which can offer numerous security features to reduce the risk of cyber intrusion. This white paper has identified six primary connectivity paths as illustrated in Figure 4.

Figure 4 – Six Connectivity Paths to Vehicles



See expanded Vehicle Platform graphic on following page

🟨 Path 1: Internal and very short range connectivity to people

🟩 Path 2: External and longer range connectivity to other vehicles or people outside the vehicle

🟪 Path 3, 4 & 5: External, longer range and Telco managed connectivity to applications

🟦 Path 6: Satellite connectivity to the vehicle

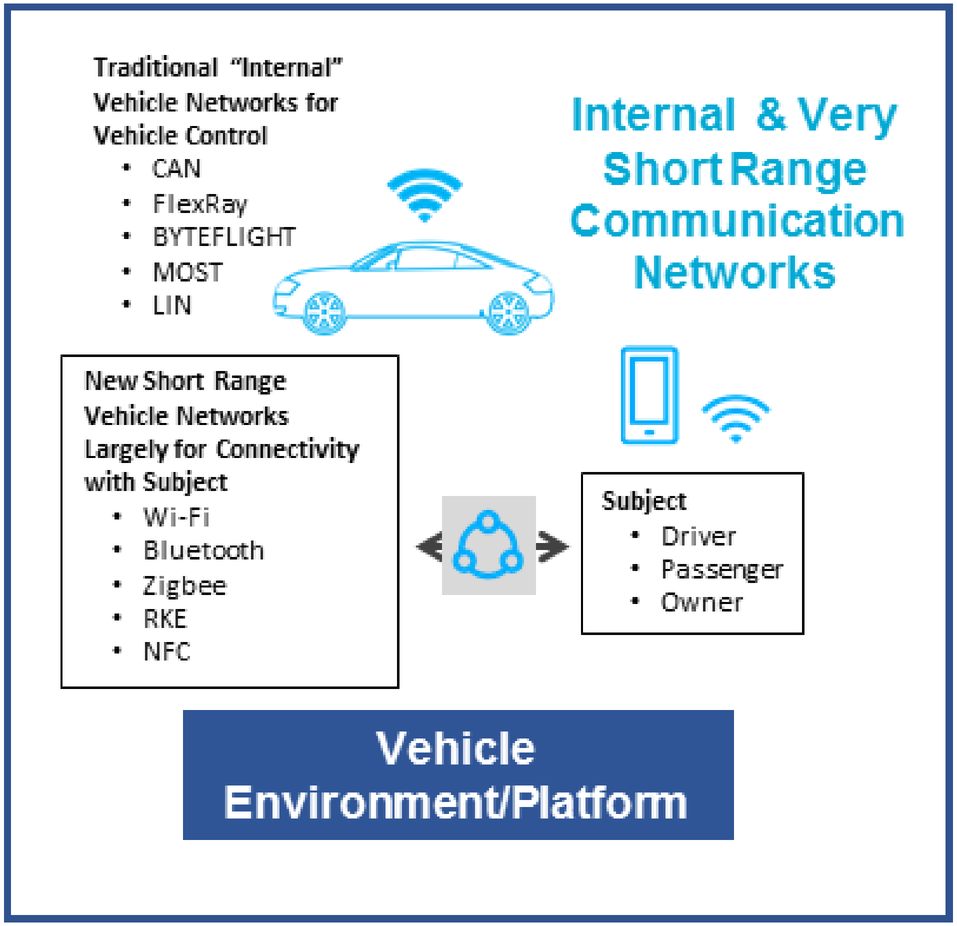
Cloud Access Security Broker

PATH 1 – Internal and very short-range connectivity: This path recognizes that subjects (drivers, passengers, and others) will connect to the vehicle through a variety of communication technologies. This connectivity is primarily short range over un-managed connections such as Bluetooth, Zigbee, and Near Field Communication (NFC), to a device such as a handset or tablet. These devices in turn are likely to be further connected to a cellular or Wi-Fi network and therefore susceptible to cyber intrusion from the broader network to which the device is connected.

Telecommunications carriers can secure the managed networks that provide communication to the connected vehicle using the tools described in Section 8. This path can be used as a direct attack vector (e.g., key fob attacks or Bluetooth attacks against the entertainment system), completely bypassing the telecommunications network. This is one of many reasons of the need for end-to-end security, including network and end-point security and each layer in between. This end-to-end approach is described in Section 8.

Figure 5 illustrates the short-range communication paths that are most prevalent for Path 1.

Figure 5 – Internal and Very Short-Range Connectivity


Traditional "Internal" Vehicle Networks for Vehicle Control
• CAN
• FlexRay
• BYTEFLIGHT
• MOST
• LIN
Internal & Very Short Range Communication Networks
New Short Range Vehicle Networks Largely for Connectivity with Subject
• Wi-Fi
• Bluetooth
• Zigbee
• RKE
• NFC
Subject
• Driver
• Passenger
• Owner
Vehicle Environment/Platform

PATH 2 – External and longer-range connectivity: This path is slightly longer range than Path 1, connecting the vehicle to other vehicles, or to subjects that are not inside or adjacent to the vehicle (e.g., toll booths or other vehicles). Communication technologies that can be used for this type of connectivity include Wi-Fi and DSRC (see Appendix A for more detail on DSRC).

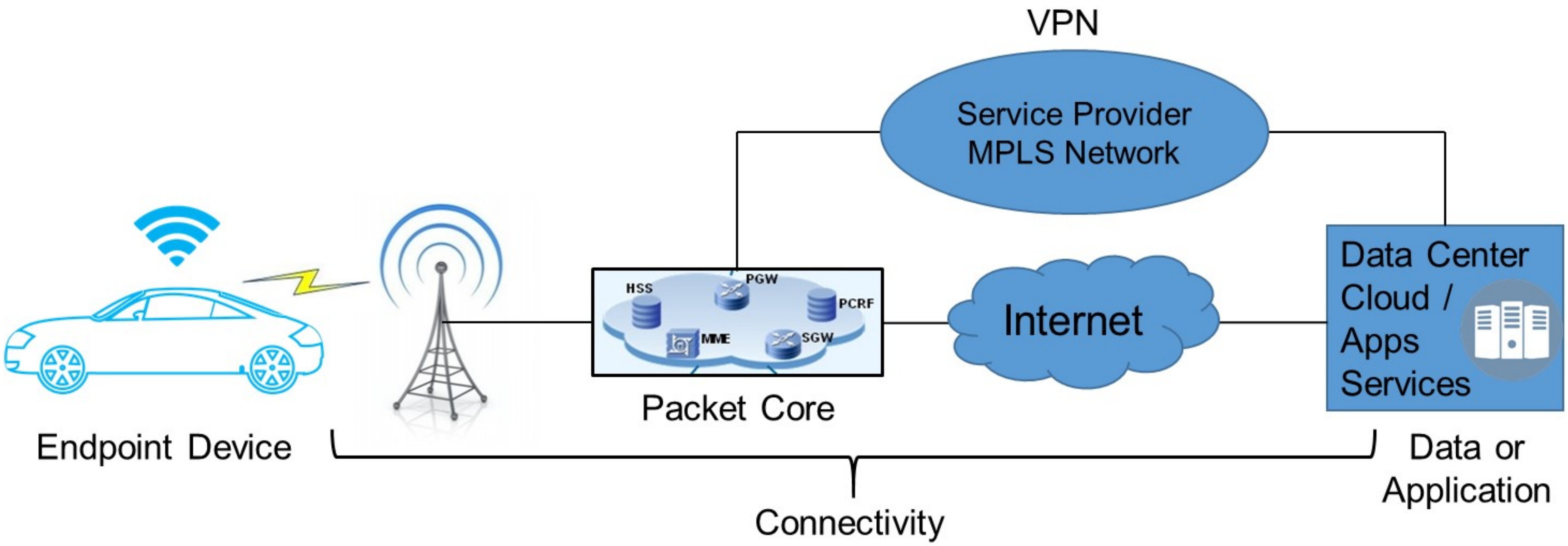
As in Path 1, the telecommunications network providers can secure the broader networks using the tools described in Section 7 and 8 below. But again, additional securing of the connected vehicles with end-point security solutions will be needed especially for communication technologies such as Radio Frequency Identification (RFID), NFC, and un-managed Wi-Fi. This is further described in Section 8.

PATHS 3, 4, and 5 – Telco-managed connectivity:

- **PATH 3** involves connectivity to the open Internet and cloud services, including search and clouds for specific applications such as Intelligent Transportation Systems.
- **PATH 4** involves direct connectivity to end servers for specific applications.
- **PATH 5** involves connectivity that connects back and forth between clouds and specific servers.

These three paths depend on connectivity provided by the telecommunications carriers and function in a substantially similar manner (i.e., cellular/mobile and secure Internet Protocol [IP]/ Multiprotocol Label Switching [MPLS] transport over optical networks), connecting the endpoint device to a variety of applications, services, and data. These paths can be simplified to the following diagram (Figure 6) showing the endpoint device, cloud applications or data, and connectivity linking the two.

Figure 6 – Telecommunication Network Carrier Architectures



PATH 6 – Satellite connectivity: This path provides a direct download link to the connected vehicle. It is included for completeness, and is not further analyzed in this white paper.

7. Overview of Which Network Types Telecommunications Carriers Can Control and Secure Today

Telecommunications carriers operate wireless and wired networks to deliver communication, information, and entertainment to their customers in the form of voice, text messages, data, and video. These networks employ the types of cybersecurity methodologies outlined in Section 8. Not all electronic access points into vehicles (or to other network end-points) are operated by telecommunications carriers. Those that are not will require other cybersecurity methods to ensure safety and security.

Figure 7 is an adaptation of previous work by NHTSA that outlines the types of electronic connections which currently have or have the potential to provide access to vehicles.

Figure 7 – Electronic Access Points to Vehicles

Network Type	Examples	Comments
Short Range Wireless Access Networks	- **Wi-Fi**	Many short-range wireless networks are "access" networks connected to long range wireless or wired networks. Some access networks are operated by telecommunications carriers, some are not.
Short Range Wireless – Peer-to-Peer	- Short range radiotire pressure, remote key entry (RKE), other). Most RKEs operate at 315 MHz in NA vehicles and at 433.92 MHz in European, Japanese and Asian vehicles - NFC - Bluetooth - DSRC (In the U.S., 75 MHz licensed spectrum around 5.9 GHz)	A number of short range wireless technologies are emerging for peer-to-peer communications within a localize environment, such as an automated home or vehicle. These peer-to-peer networks may also have connectivity to the Internet or to other networks managed by telecommunications carriers.
Long Range Wireless	- **Wi-Fi Mobile radio (GSM/CDMA and 2G, 3G, 4G, and 5G)** - **Satellite (GPS, Sirius/XM, DirecTV, other)**	These networks are operated by telecommunications carriers.
Wired	- **Twisted pair telephone** - **Broadband/fiber** - **Cable TV**	Since wired (fixed) networks provide the backbone for all wireless networks, their security is vital as they connect to wireless networks. Today, most wired networks are a hybrid of technologies including fiber, coaxial cable and telephone twisted pair.

NOTE: Telecommunication carrier networks are shown in blue text.

Source: NHTSA, Marconi Pacific

Telecommunications carriers provide services to their customers through managed connections. Managed connections are those in which the carrier is able to control the end-to-end delivery of the communications in order to deliver Quality of Service (QoS), provide additional security features, authorize access to the network, authenticate (verify) that the user is the registered user, and bill for the services. Managed connections almost always require a subscription to the network either directly or through roaming agreements such that the user can be authenticated, authorized, and billed. Managed connections provide the types of security described in Sections 8 and 9.

By contrast, unmanaged connections are those which are not under the end-to-end control of the telecommunications carriers and therefore do not have the full end-to-end security discussed in Sections 8 and 9. Unmanaged connections may be between the vehicle and a user device such as a smartphone to enable local features or may provide temporary Internet access (e.g., unmanaged Wi-Fi) for data downloading. In some cases, the smartphone may utilize managed mobile broadband services to connect with external services or backend-servers, but the connection to the vehicle or other device will still be unmanaged (i.e., a Bluetooth connection).

Some technologies are generally associated with unmanaged connectivity. Examples of technologies that are almost always unmanaged include: USB, Bluetooth, NFC, and private or public Wi-Fi connections. Wireless unmanaged connections typically use unlicensed radio spectrum, and the end user must configure the service rather than it being automatically available. In the case of Wi-Fi, the unmanaged connectivity may be provided by a third party as a free or paid Internet access, but without service guarantees or security functions. Unmanaged connections are often used to access services such as:

- Infotainment.
- Tethered communication, e.g., via a smartphone.
- Tire pressure monitoring.

- CarPlay and Android Auto.
- Diagnostics from aftermarket OBD-II connectors.

Unmanaged connections represent a risk regarding cyber intrusion because the telecommunications carrier has secured its network and the vehicle OEM likely has secured its internal network. However, the vehicle short range communication technologies are not secure because they are not managed by either party (e.g., Bluetooth, unmanaged Wi-Fi, Zigbee, and others).

8. Current Telecommunications Carrier Initiatives in Cyber Security – The Layered Approach

Telecommunications network providers have extensive experience addressing cybersecurity threats to network infrastructure and to connected end-point devices, including handsets, applications, enterprise gateways, and cloud servers. Today's threats include Distributed Denial of Service (DDoS) attacks, malicious hacks, and malware, as well as threats against the ICT infrastructure itself. For example, in the fourth quarter of 2016, on the quietest day of the year, 90 DDoS attacks were identified, with attacks frequently exceeding 500 per day[1].

These threats are aimed at the Public Switched Telephone Network (PSTN) and at the IP networks. Threats to the latter are the focus of this section since the traffic destined for and originating from vehicles relies on IP networks. These IP networks are an open

[1] Khalimonenko, A., Strohschneider, J., Kupreev, O. (2017, February 2). *DDoS attacks in Q4 2016*. Available at: < https://securelist.com/analysis/quarterly-malware-reports/77412/ddos-attacks-in-q4-2016/ >.

technology designed to inter-connect people, Internet-driven services, private, government, and public IP networks on a global scale, and are much more susceptible to cyber intrusion. This is due to the plethora of devices, network equipment, laptops, desktop computers, servers, tablets, smartphones, and now Internet of Things (IoT) devices that make up the IP network ecosystem, each offering a potential access point for cyber attacks and the distribution of malware. As a result, the telecommunications carriers have developed significant expertise and deployed sophisticated tools in the quest to constantly monitor and secure IP networks. For example, critical infrastructure services such as Government Emergency Telecommunications Service (GETS) and 9-1-1, which at one time totally depended on the PSTN environment of telecommunications carriers, are increasingly carried over IP networks and require IP techniques to secure these critical services.

To secure these IP networks and the customers' traffic, telecommunications carriers use a Layered Approach relying on a number of primary security methods. Applying this strategy allows the carriers to deliver a high level of security and meet specific security metrics. Listed below, and followed by a visual representation in Figure 8, are the nine primary security methods widely used in telecommunications networks for IP traffic. Additional detail and descriptions for each security method listed below can be found in Appendix B.

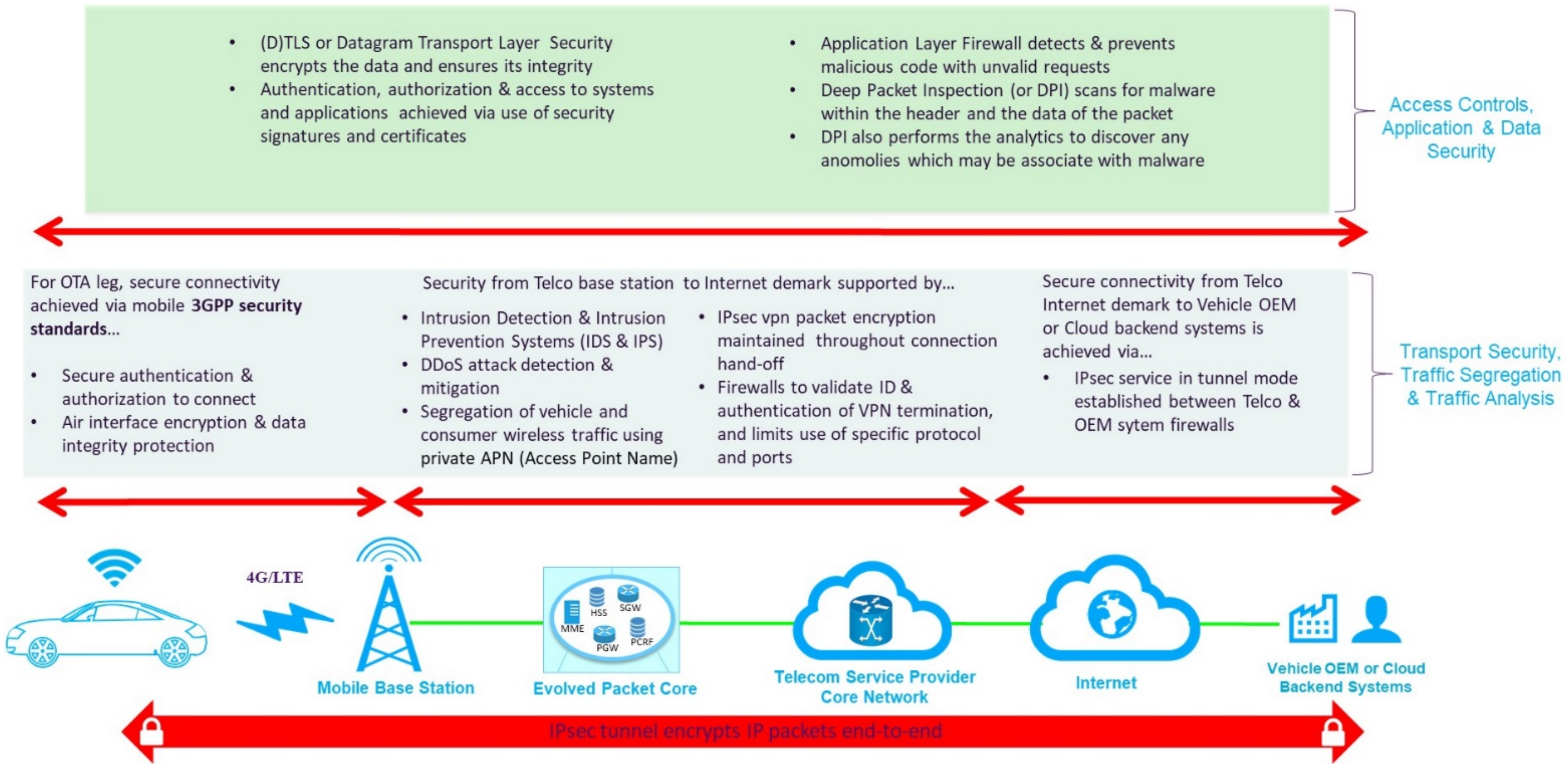
First Layer: Transport Security, Traffic Segregation and Traffic Analysis

1. Secure mobile network connectivity (from the vehicle to the base station) based on 3GPP Security Standards.
2. Secure wireline network connectivity.
3. Network Layer Firewalls.
4. DDOS Mitigation and Prevention.

Second Layer: Access Controls, Application and Data Security

1. Application Layer Firewall.
2. Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs).
3. Authentication and Authorization.
4. Identity and Access Control.
5. Deep Packet Inspection (DPI).

Figure 8 – Layered Security Model: End-to-End Security



- (D)TLS or Datagram Transport Layer Security encrypts the data and ensures its integrity
- Authentication, authorization & access to systems and applications achieved via use of security signatures and certificates

- Application Layer Firewall detects & prevents malicious code with unvalid requests
- Deep Packet Inspection (or DPI) scans for malware within the header and the data of the packet
- DPI also performs the analytics to discover any anomolies which may be associate with malware

For OTA leg, secure connectivity achieved via mobile **3GPP security standards**...

- Secure authentication & authorization to connect
- Air interface encryption & data integrity protection

Security from Telco base station to Internet demark supported by...

- Intrusion Detection & Intrusion Prevention Systems (IDS & IPS)
- DDoS attack detection & mitigation
- Segregation of vehicle and consumer wireless traffic using private APN (Access Point Name)
- IPsec vpn packet encryption maintained throughout connection hand-off
- Firewalls to validate ID & authentication of VPN termination, and limits use of specific protocol and ports

Secure connectivity from Telco Internet demark to Vehicle OEM or Cloud backend systems is achieved via...

- IPsec service in tunnel mode established between Telco & OEM sytem firewalls

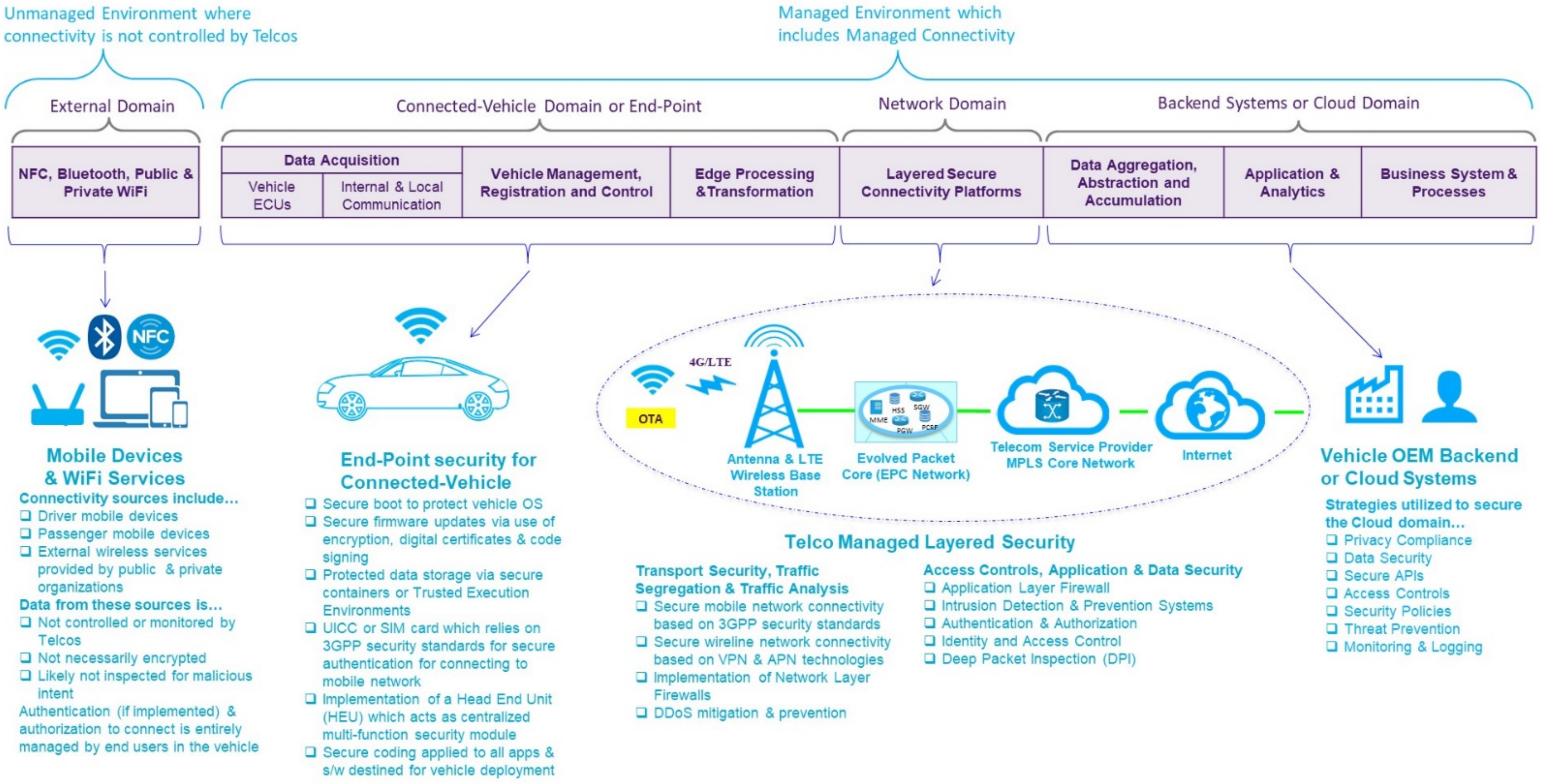
Access Controls, Application & Data Security
Transport Security, Traffic Segregation & Traffic Analysis
4G/LTE
Mobile Base Station
HSS
SGW
MME
PGW
PCRF
Evolved Packet Core
Telecom Service Provider Core Network
Internet
Vehicle OEM or Cloud Backend Systems
IPsec tunnel encrypts IP packets end-to-end

9. Comprehensive Connected Vehicle Security Framework

As the ICT industry and the telecommunications carriers in particular work with the vehicle OEMs to deliver secure vehicle strategies, a comprehensive end-to-end security framework can assist in ensuring that all the links and parts of the value chain are secure.

A “Connected Vehicle Security Framework” detailed in Figure 9 below illustrates this end-to-end approach. The framework can also place a further spotlight on the “Managed versus Unmanaged” networks discussed in Section 5 above. As addressed in Section 5, **unmanaged networks**, referenced as the External Domain in Figure 9, represent an area of very high cyber vulnerability and therefore require special attention.

Figure 9 – Connected Vehicle Security Framework


Unmanaged Environment where connectivity is not controlled by Telcos
Managed Environment which includes Managed Connectivity
External Domain
Connected-Vehicle Domain or End-Point
Network Domain
Backend Systems or Cloud Domain
NFC, Bluetooth, Public & Private WiFi
Data Acquisition
Vehicle ECUs
Internal & Local Communication
Vehicle Management, Registration and Control
Edge Processing & Transformation
Layered Secure Connectivity Platforms
Data Aggregation, Abstraction and Accumulation
Application & Analytics
Business System & Processes
NFC
4G/LTE
OTA
HSS
SGW
MME
PGW
PCRF
Antenna & LTE Wireless Base Station
Evolved Packet Core (EPC Network)
Telecom Service Provider MPLS Core Network
Internet

Mobile Devices & WiFi Services

Connectivity sources include…

❑ Driver mobile devices
❑ Passenger mobile devices
❑ External wireless services provided by public & private organizations

Data from these sources is…

❑ Not controlled or monitored by Telcos
❑ Not necessarily encrypted
❑ Likely not inspected for malicious intent

Authentication (if implemented) & authorization to connect is entirely managed by end users in the vehicle

End-Point security for Connected-Vehicle

❑ Secure boot to protect vehicle OS
❑ Secure firmware updates via use of encryption, digital certificates & code signing
❑ Protected data storage via secure containers or Trusted Execution Environments
❑ UICC or SIM card which relies on 3GPP security standards for secure authentication for connecting to mobile network
❑ Implementation of a Head End Unit (HEU) which acts as centralized multi-function security module
❑ Secure coding applied to all apps & s/w destined for vehicle deployment

Telco Managed Layered Security

Transport Security, Traffic Segregation & Traffic Analysis

❑ Secure mobile network connectivity based on 3GPP security standards
❑ Secure wireline network connectivity based on VPN & APN technologies
❑ Implementation of Network Layer Firewalls
❑ DDoS mitigation & prevention

Access Controls, Application & Data Security

❑ Application Layer Firewall
❑ Intrusion Detection & Prevention Systems
❑ Authentication & Authorization
❑ Identity and Access Control
❑ Deep Packet Inspection (DPI)

Vehicle OEM Backend or Cloud Systems

Strategies utilized to secure the Cloud domain…

❑ Privacy Compliance
❑ Data Security
❑ Secure APIs
❑ Access Controls
❑ Security Policies
❑ Threat Prevention
❑ Monitoring & Logging

In the framework, the **managed environment** is comprised of three distinct domains: (1) the Connected Vehicle Domain (or End-Point); (2) the Network Domain (or Connectivity); and (3) the Cloud Domain (or Backend Systems).

The telecommunications carriers can enhance the connected vehicle's security chain by providing additional security technology services within each domain. But the telecommunications carriers cannot do this alone. Effective security must be provided at all "layers" (as outlined in Section 8) and within/between each domain – a holistic approach. This includes technologies to connect various subsystems inside the automobile, as well as technologies that allow subsystems to communicate with entities outside the vehicle. Using the Connected Vehicle Security Framework coupled with the layered security approach identified in Section 8 assists in identifying the security requirements for each domain.

Further, the security models must be able to be updated and flexible. One key example of this is the need to be able to provide secure Firmware Over-the-Air (FOTA) updates to address any newly discovered security vulnerabilities.

What follows are more in-depth descriptions for each of the domains as outlined previously in this section and depicted in Figure 9.

Endpoint Security for Connected Vehicle Domain

Endpoint security refers to securing the overall vehicle, (i.e., the vehicle platform as described in Section 4), as well as securing each component inside the vehicle to protect it from cyber attacks. There are several ways network service providers can contribute to securing the connected vehicle "endpoint", as outlined in this section.

For cellular network access to the connected vehicle, telecommunication providers utilize the Universal Integrated Circuit

Card (UICC) for endpoint security. The UICC allows for bi-directional authentication between the device (endpoint) and the network. This functionality is critical to ensure that the vehicle does not connect to a "rogue" network and risk exposure to malware or hacking. Security mechanisms implemented inside the vehicle can also be reinforced by network-based firewalls, intrusion detection, and intrusion prevention systems that can be implemented to detect and prevent cyber attacks before they access the vehicle.

The connected vehicle can also leverage service provider expertise with mobile devices to implement the trusted computing base that is critical to enforce security policies to protect the vehicle. Important security capabilities include:

- Securing the boot capabilities so that malware cannot corrupt the operating system. This can ensure the device is running authorized code from the device manufacturer to effectively drive security up the stack.
- Evaluating update paths to ensure that any new firmware is verified by the bootloader before installation. Firmware updates can also be secured with strong encryption to protect the firmware source code against unauthorized access by hackers.
- Following the "rule of least privilege" which ensures that each person or entity connected to the endpoint has access only to the minimum information and resources needed to perform its function.
- Securing storage in the vehicle components to protect keys, certificates, firmware updates, and other sensitive information.

There are several ways the capabilities discussed above can be implemented. One approach is to implement an in-vehicle security model as shown in Figure 12 (in Section 11 below). Most vehicle infrastructures include a common bus (i.e., controller area network bus) to allow intercommunication between the various components within the vehicle. This architecture opens multiple avenues of attack and increases the importance of detecting and blocking attacks at the vehicle boundary. The in-vehicle security architecture can reduce risk by implementing intrusion detection and prevention mechanisms within the vehicle or by allowing the network to help protect the connected vehicle as shown in Figure 11. This could be strengthened by coupling it with telecommunications providers' network policies to allow or deny network access based on the source of the traffic.

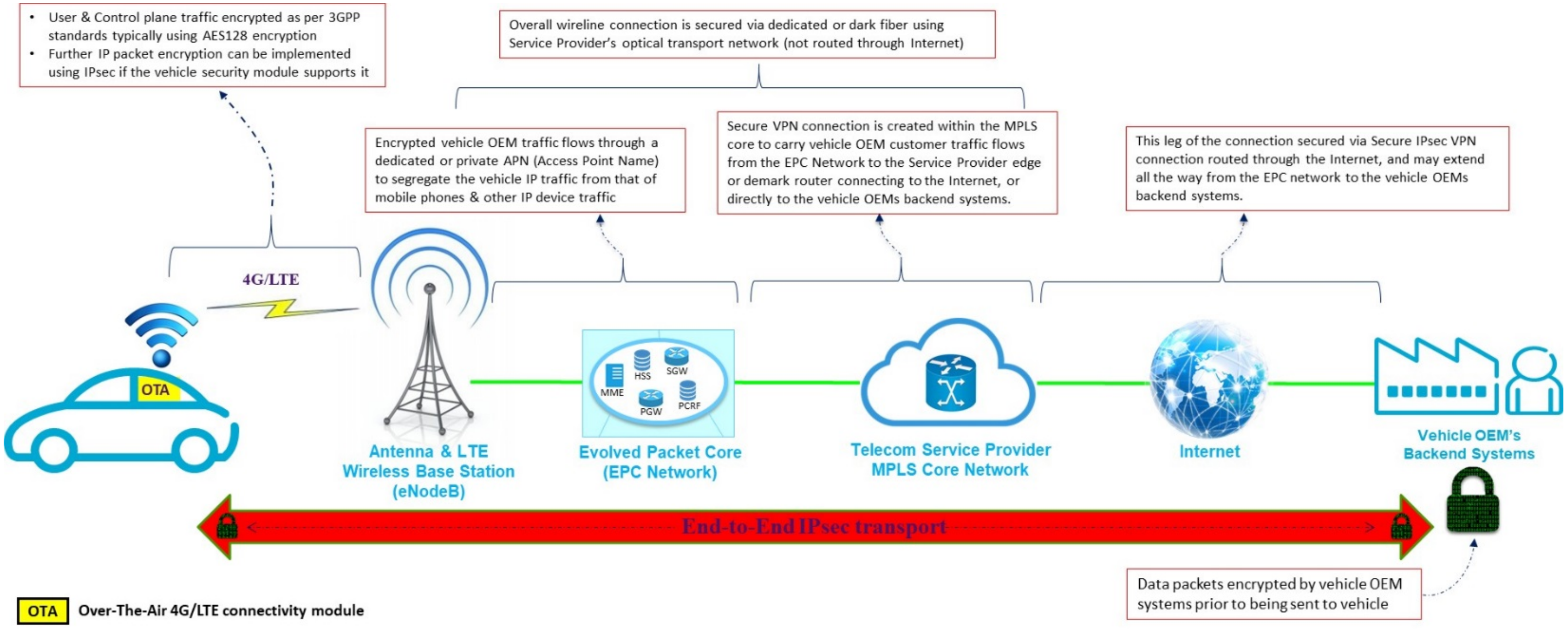
Secure coding practices and languages can also help secure vehicles. Since open source libraries are well documented and scrutinized by many users, they often receive more updates to patch code. Open source libraries that are well-documented and continuously monitored for updates and potential vulnerabilities improve security. Telecommunications network providers have extensive experience in this area, and could be a useful partner to the vehicle OEMs. These practices could be further strengthened through a Connected Vehicle App Store that would ensure connected vehicle apps received wide scrutiny, and that security vulnerabilities could be rapidly identified. Telecommunications network providers could act as valuable partners in this respect, ensuring that threat information was shared across the vehicle industry and provided to intrusion detection systems. This is shown in Figure 14 as part of Section 11.

Connectivity to and from the Vehicle

Connectivity is the key component that telecommunication providers can offer in the end-to-end connected vehicle ecosystem. Nevertheless, the details of how data packets flow through an IP network are valuable for understanding how the data is secured to and from the endpoint device, either through the Radio Access Network (RAN), or, in the case of wireless networks, back through the packet core and to the customer's cloud or data application.

Data to and from the RAN is encrypted using 3GPP standards. The packet then traverses the telecommunication carrier's network and ends at the Packet Gateway (P-GW), the last network element that IP packets touch before being routed through the Internet. When packets are routed through the Internet to the customers back-end or cloud application, telecommunications network providers can offer secure connectivity mechanisms (e.g., VPNs, tunneling, and encryption) to prevent potential man-in-the-middle attacks or compromising of data. OEMs (and other end customers) have the option of securely tunneling their data through the network carrier's MPLS backbone to their data center or cloud application, avoiding the Internet all together. Figure 10 below illustrates how these end-to-end connectivity paths and the various technologies are utilized to secure data moving through the network.

Figure 10– End-to-End Network Security



- User & Control plane traffic encrypted as per 3GPP standards typically using AES128 encryption
- Further IP packet encryption can be implemented using IPsec if the vehicle security module supports it

Overall wireline connection is secured via dedicated or dark fiber using Service Provider's optical transport network (not routed through Internet)

Encrypted vehicle OEM traffic flows through a dedicated or private APN (Access Point Name) to segregate the vehicle IP traffic from that of mobile phones & other IP device traffic

Secure VPN connection is created within the MPLS core to carry vehicle OEM customer traffic flows from the EPC Network to the Service Provider edge or demark router connecting to the Internet, or directly to the vehicle OEMs backend systems.

This leg of the connection secured via Secure IPsec VPN connection routed through the Internet, and may extend all the way from the EPC network to the vehicle OEMs backend systems.

Data packets encrypted by vehicle OEM systems prior to being sent to vehicle

4G/LTE
OTA
Antenna & LTE Wireless Base Station (eNodeB)
MME
HSS
SGW
PGW
PCRF
Evolved Packet Core (EPC Network)
Telecom Service Provider MPLS Core Network
Internet
Vehicle OEM's Backend Systems
End-to-End IPsec transport
OTA Over-The-Air 4G/LTE connectivity module

Cloud Domain to Secure Backend Applications or Data

The third domain making up the Connected Vehicle Security Framework is the Cloud Domain. This is where data is processed or analyzed.

This also where data is stored such that:

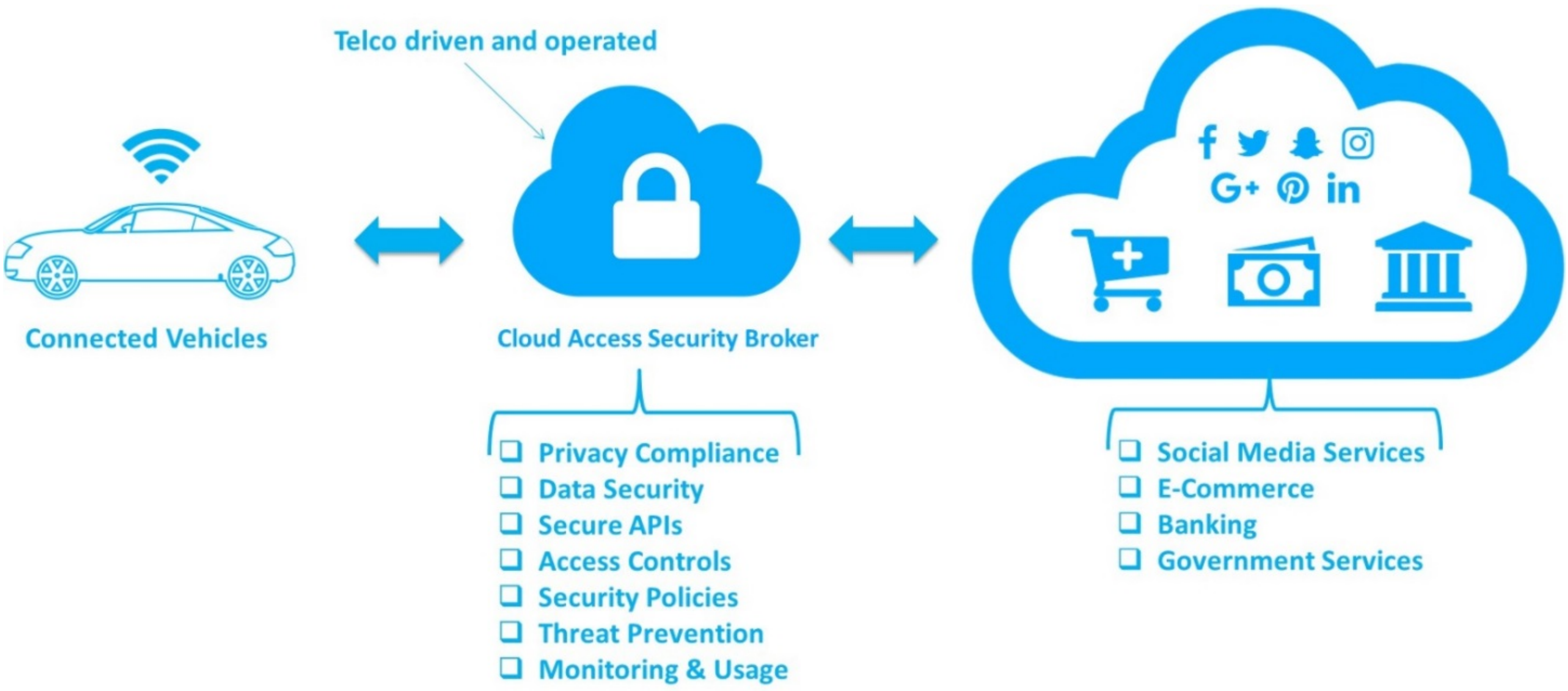
- Access is limited.
- Data is encrypted.
- Data integrity is validated and verified.
- Raw sensor data is secured.
- Data is anonymized for privacy concerns.

Telecommunications carriers can, and in many customer implementations do, offer added security to back-end applications by providing a Cloud Access Security Broker (CASB). This is an additional layer of security that is focused on all aspects of connection requests aimed at protecting the customer (Vehicle OEM's) backend system or Cloud system. By implementing the CASB model, telecommunication carriers can offer the following security services for the OEM's Cloud Domain:

- Privacy Compliance.
- Data Security.
- Secure APIs.
- Access Controls.
- Security Policies.
- Threat Detection and Prevention.
- Monitoring and Usage.

Figure 11 is a high-level diagram outlining the implementation of the CASB model for vehicle OEMs.

Figure 11 – Cloud Access Security Broker (CASB)



Even when data is secured from the vehicle to the cloud application, other paths that allow access from the Internet to that cloud application can offer a backdoor, potentially giving a bad actor access to the vehicle.

10. Telecommunications Carriers and Vehicle OEMs – Potential Engagement Model

The telecommunications carriers and the vehicle OEMs can enhance vehicle cybersecurity and passenger safety, independently and together. Numerous company-to-company initiatives have already begun and many more are in the development stage or will be in the coming months and years. In conjunction with these bi-lateral initiatives, there is an opportunity for the two industries together to pursue greater cooperation and explore best practices and optimum safety initiatives. Cyber intrusion that negatively affects vehicle safety/performance and results in injuries affects those injured as well as tarnishes the image of all the companies, governmental entities and organizations in the ecosystem. An incident or series of incidents that affects one or two OEMs, or one or two telecommunications carriers, will create suspicion as to the cyber prevention capability of all OEMs and all telecommunications carriers.

With this backdrop in mind, ATIS proposes three steps:

1. A sub-committee of the Automotive Information Sharing and Analysis Center (Auto-ISAC) could be formed with members of ATIS’ telecommunications carrier group, vehicle OEM member companies, and other vehicle ecosystem suppliers as appropriate. We envision this white paper as a starting point for discussions and the sub-committee’s work.

   One initiative that may be of value by working together would be to identify “use case categories” that identify common characteristics shared by a range of individual use cases for the connected vehicle. The intent would be to capture the essence of the overall connected vehicle use cases while keeping the overall number manageable. This will provide context for a systems perspective on how the ICT industry could potentially provide capabilities that would bring value to the important use cases in the connected vehicle space.

2. ATIS could expand the working group that generated this white paper to further explore how the ICT industry can best participate and enhance cybersecurity as well as work with vehicle OEMs. The ICT industry would provide additional detail on how it is working on cybersecurity with emphasis on best practices that ICT is adopting, and how those practices could contribute to cooperation with the automotive OEMs. This work could provide a systems view of the cybersecurity role that the ICT industry can play for the connected vehicle. Viewing the "network as a platform," and taking a "systems" view (architecture, interface, and implementation), including the connected vehicle as an entity accessing that system, could improve the telecommunications networks understanding of how to provide enhanced security to connected vehicle applications. Examples of functions that could be valuable to the connected vehicle include:

    a. Standard of care: Providing a fully managed connection to the vehicle, with guaranteed levels of service and cybersecurity monitoring would contribute to proving the required standard of care is being offered for the connected vehicle user.

    b. ICT network's on-going monitoring of connectivity to the vehicle: This could include a wide range of functions, based on services that are already offered to enterprises and individual mobile network users.

    c. Secure, guaranteed delivery of content to the vehicle: Provides for regular software updates, critical safety recalls, or even regular service reminders.

    The cybersecurity expertise of the ICT industry could be applicable to any communications path to the connected vehicle, but it is expected that the most value would come from primarily focusing on managed wireless connections over the public mobile network, and the potential cybersecurity value that could be provided through these networks.

3. Both ATIS and the Auto-ISAC could reach out to other industry groups to determine how industry best practices can be shared and implementation accelerated. Groups such as 5GAA (5G Automotive Association), ENISA (European Union Agency for Network and Information Security), and Global Automakers could be contacted to explore greater industry wide participation, education and identification of threats and prevention and remediation measures.

11. Telecommunications Carriers and Vehicle OEMs – Potential Discussion Topics

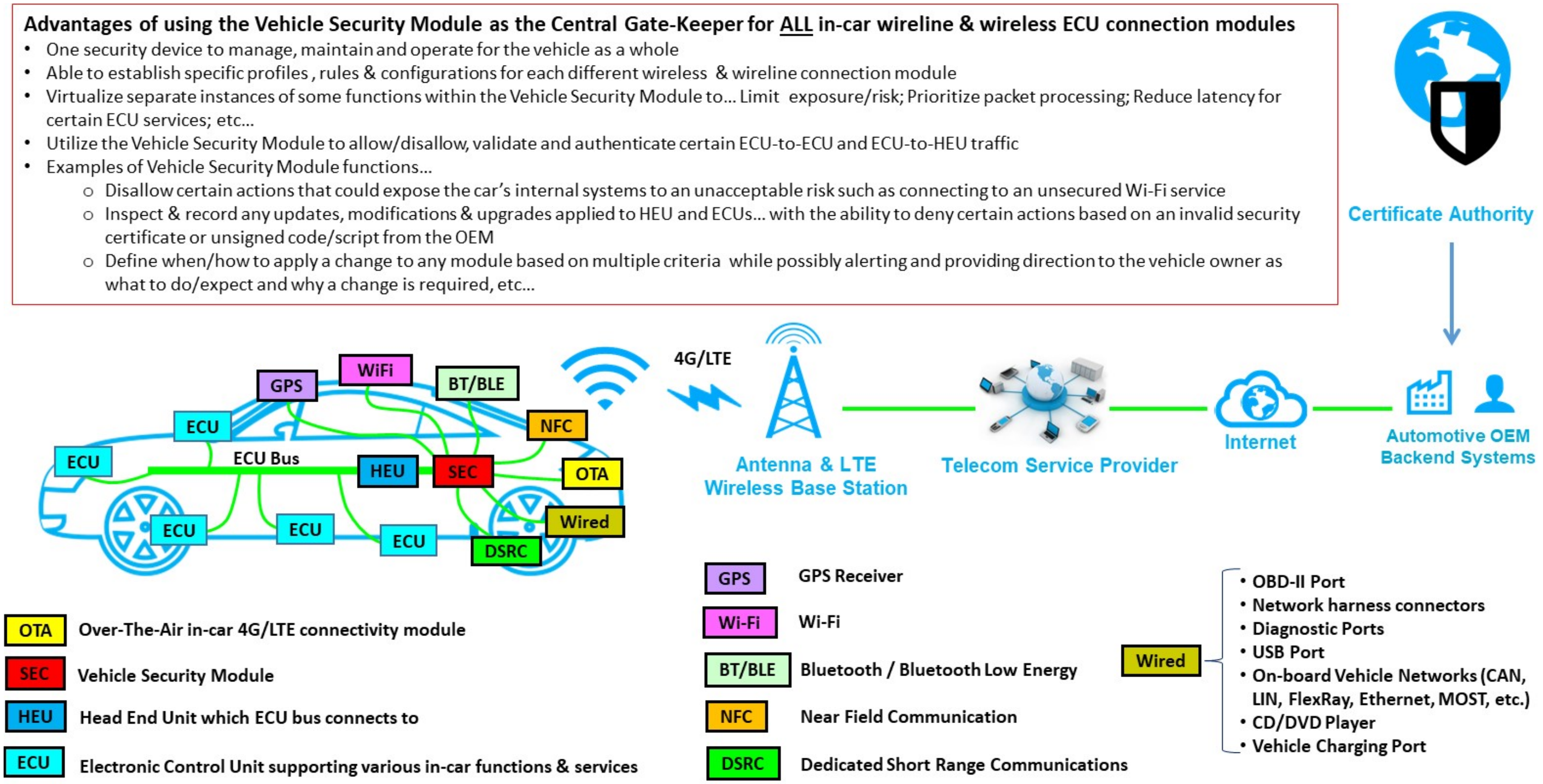
The topics for a collaborative engagement between the ICT industry and the connected vehicle industry will emerge from a discussion between the two industries, but this section outlines potential topics that could be considered. This is not intended to provide a definitive proposal, but rather is intended to provide a starting point for further dialog, a sense of the technical details and to illustrate the potential value that could result from the two industries bringing their respective expertise to the discussion. This section has detailed four "ideas/topic areas" for further discussion:

1. Centralized In-Vehicle Security Model.
2. DPI Security.
3. Applications Store Concept.
4. Connected Vehicle Bug Bounty Program.

Centralized In-Vehicle Security Model

This section provides a high-level overview of a centralized security module in the vehicle that would contribute to enhanced security for connected vehicles. It would bring many aspects of security to the "end-point" within the vehicle, which is an important principle for securing any environment. Bringing security as close as possible to the "network edge" or to the end-point device itself will enhance the security of the solution. Additionally, if telecommunications carriers, hardware manufacturers, software development companies, and vehicle OEMs work together in a collaborative effort, it would be possible to develop approaches that place functions in the vehicle or in the network depending on where they will be most effective. One potential view of this approach is illustrated in Figure 12.

Figure 12 – Centralized In-Vehicle Security Model



Advantages of using the Vehicle Security Module as the Central Gate-Keeper for ALL in-car wireline & wireless ECU connection modules

- One security device to manage, maintain and operate for the vehicle as a whole
- Able to establish specific profiles , rules & configurations for each different wireless & wireline connection module
- Virtualize separate instances of some functions within the Vehicle Security Module to... Limit exposure/risk; Prioritize packet processing; Reduce latency for certain ECU services; etc...
- Utilize the Vehicle Security Module to allow/disallow, validate and authenticate certain ECU-to-ECU and ECU-to-HEU traffic
- Examples of Vehicle Security Module functions...
  - Disallow certain actions that could expose the car's internal systems to an unacceptable risk such as connecting to an unsecured Wi-Fi service
  - Inspect & record any updates, modifications & upgrades applied to HEU and ECUs... with the ability to deny certain actions based on an invalid security certificate or unsigned code/script from the OEM
  - Define when/how to apply a change to any module based on multiple criteria while possibly alerting and providing direction to the vehicle owner as what to do/expect and why a change is required, etc...

OTA Over-The-Air in-car 4G/LTE connectivity module

SEC Vehicle Security Module

HEU Head End Unit which ECU bus connects to

ECU Electronic Control Unit supporting various in-car functions & services

GPS GPS Receiver

Wi-Fi Wi-Fi

BT/BLE Bluetooth / Bluetooth Low Energy

NFC Near Field Communication

DSRC Dedicated Short Range Communications

Wired
- OBD-II Port
- Network harness connectors
- Diagnostic Ports
- USB Port
- On-board Vehicle Networks (CAN, LIN, FlexRay, Ethernet, MOST, etc.)
- CD/DVD Player
- Vehicle Charging Port

A more detailed study of options for a Centralized In-Vehicle security model has been developed and can be shared with interested parties.

DPI Security

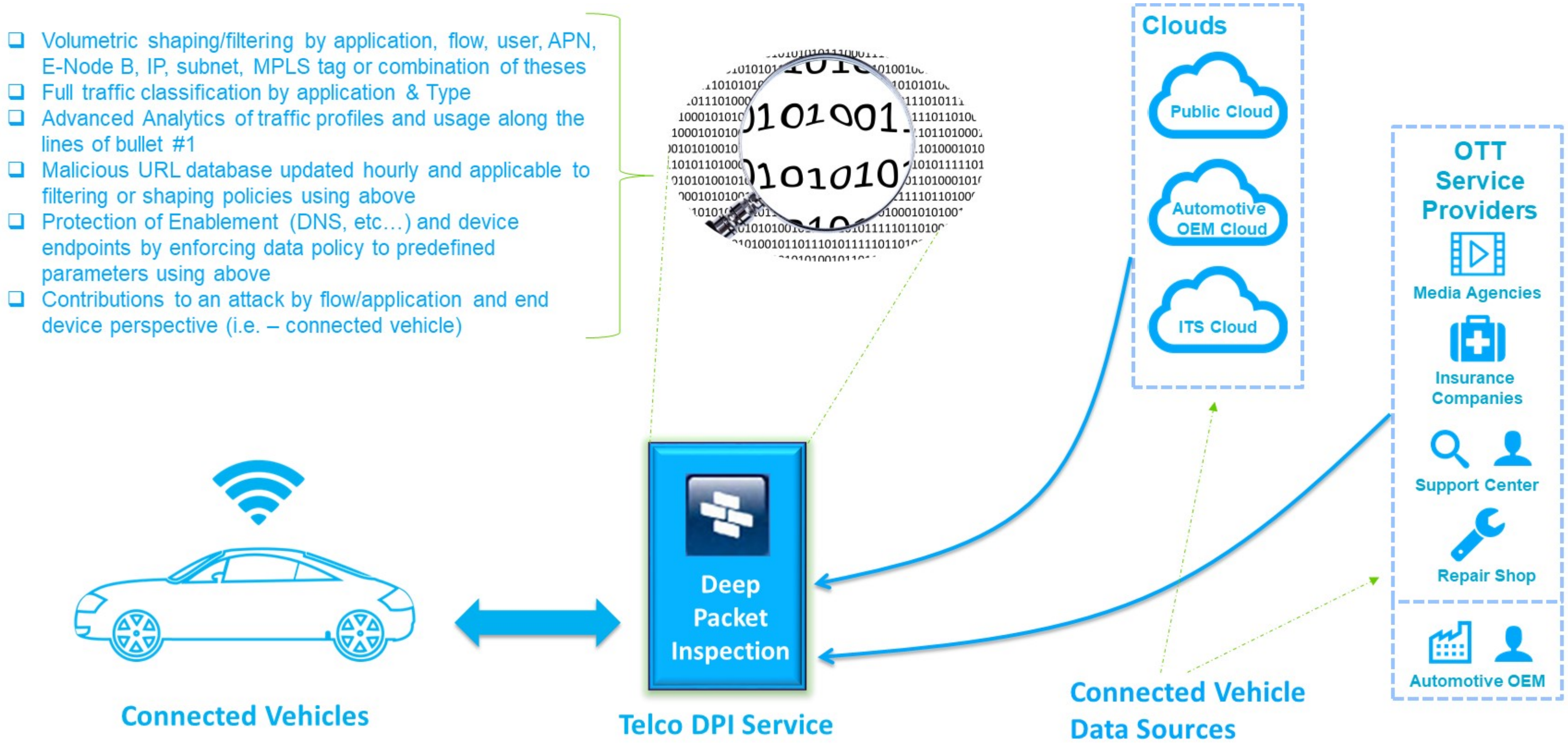
Deep Packet Inspection (DPI) could be an invaluable security tool for vehicle OEMs. DPI allows malicious content to be identified and stopped before it even reaches the vehicle. An often-expressed objection to DPI is that it enables network "snooping" into the user's data. This does not have to be the case, especially if the telecommunications network providers and vehicle OEMs work cooperatively to define the solution. Below are potential mechanisms that could address privacy concerns, while still offering enhanced security:

- In some implementations, DPI boxes have the ability to decrypt data packets, which could raise privacy concerns. However, DPI boxes could be deployed with split access controls such that no one person from one organization could access the box and independently implement a change. This configuration could ensure the vehicle OEMs retain control of their data while working with telecommunications carriers to block malicious content. It also possible to only allow one admin console, located on the vehicle OEM's premise. This would ensure that only the vehicle OEM could view the data in its decrypted form. DPI alerts and logging could still go to the telecommunications carriers for monitoring and analysis to identify malware and conduct trend analysis without compromising the vehicle OEM's encrypted data.
- Vehicle OEMs may not want data related to safety decrypted or accessed via DPI while still allowing DPI for all other (non-safety related) traffic destined for vehicles. This could be achieved by appropriately tagging the specific data before it leaves the vehicle OEM's backend systems.

- DPI technology could be deployed purely to inspect data from third party application developers who want to deploy vehicle OEM apps to the vehicle’s internal systems and/or to mobile devices that would interface with the vehicle via Wi-Fi or Bluetooth.
- DPI technology could be deployed without any ability to decrypt the data. In this configuration, the DPI would only have access to IP header information containing transport information (source/destination/protocol data) and metadata related to applications name, website, etc. Even this limited information can provide telecommunications carriers with important insight allowing them to identify attacks and malware without viewing any of the actual payload data.

Figure 13 illustrates how DPI could be deployed to provide enhanced protection to connected vehicles.

Figure 13 – Deep Packet Inspection (DPI)

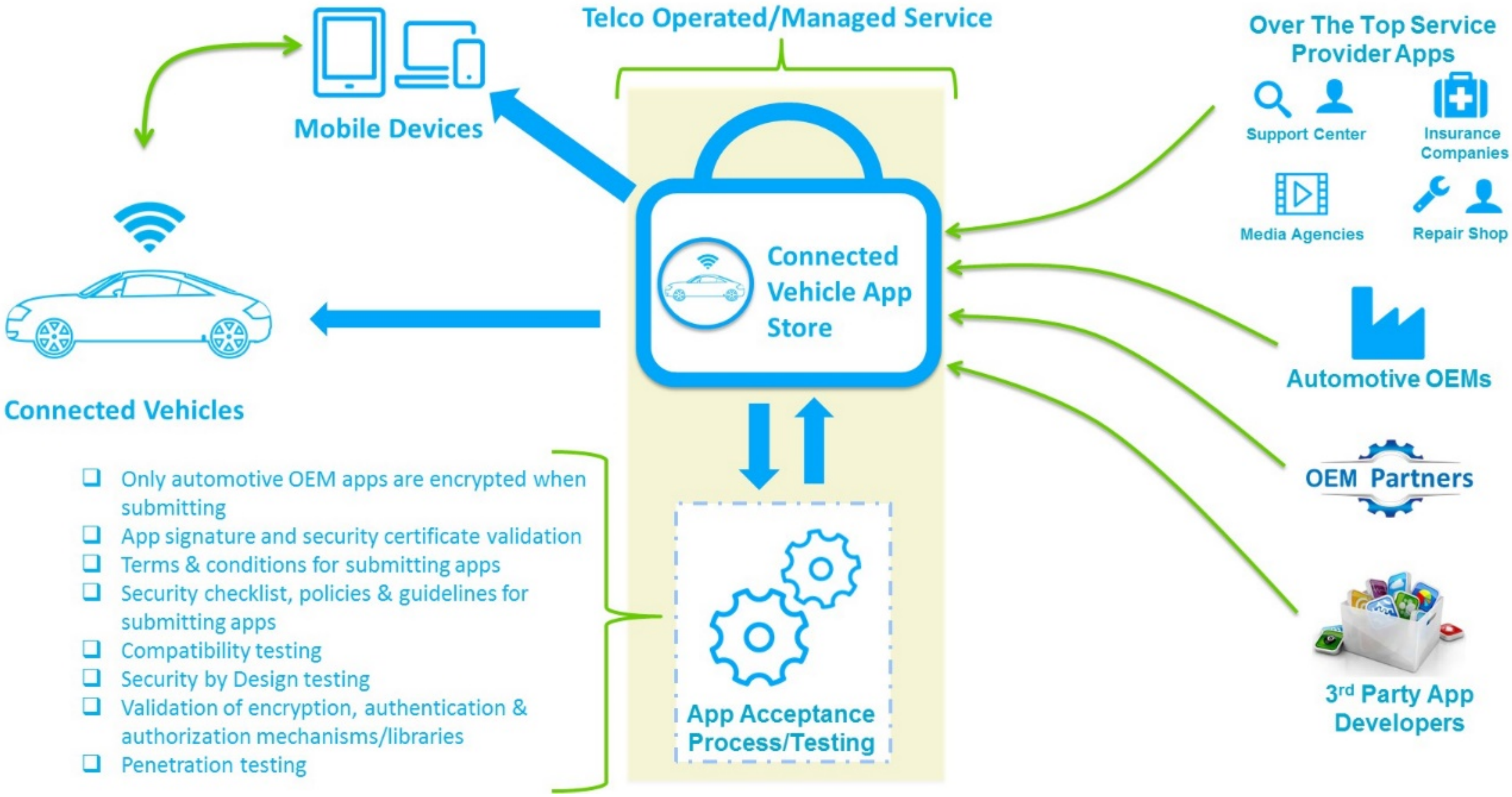


- ❑ Volumetric shaping/filtering by application, flow, user, APN, E-Node B, IP, subnet, MPLS tag or combination of theses
- ❑ Full traffic classification by application & Type
- ❑ Advanced Analytics of traffic profiles and usage along the lines of bullet #1
- ❑ Malicious URL database updated hourly and applicable to filtering or shaping policies using above
- ❑ Protection of Enablement (DNS, etc…) and device endpoints by enforcing data policy to predefined parameters using above
- ❑ Contributions to an attack by flow/application and end device perspective (i.e. – connected vehicle)

Applications Store Concept

By working together, telecommunications carriers and vehicle OEMs could create an environment where vehicle OEM-destined apps could be loaded in a secure environment prior to publishing to screen for application violation policy and malware content review. This vehicle OEM Secure Store could be managed by a telco team or co-managed with vehicle OEM employees with processes to keep all application testing and reviews unbiased and without influence. All applications destined for in-vehicle deployment or destined for mobile devices that interface with internal vehicle systems, whether developed by the vehicle OEMs, their partners, or third parties, could be distributed through the vehicle OEM's Secure Store to test/verify/validate secure/safe functionality on the vehicle's platform before being accepted/published as legitimate. This is illustrated in the following diagram.

Figure 14 – Applications Store Concept

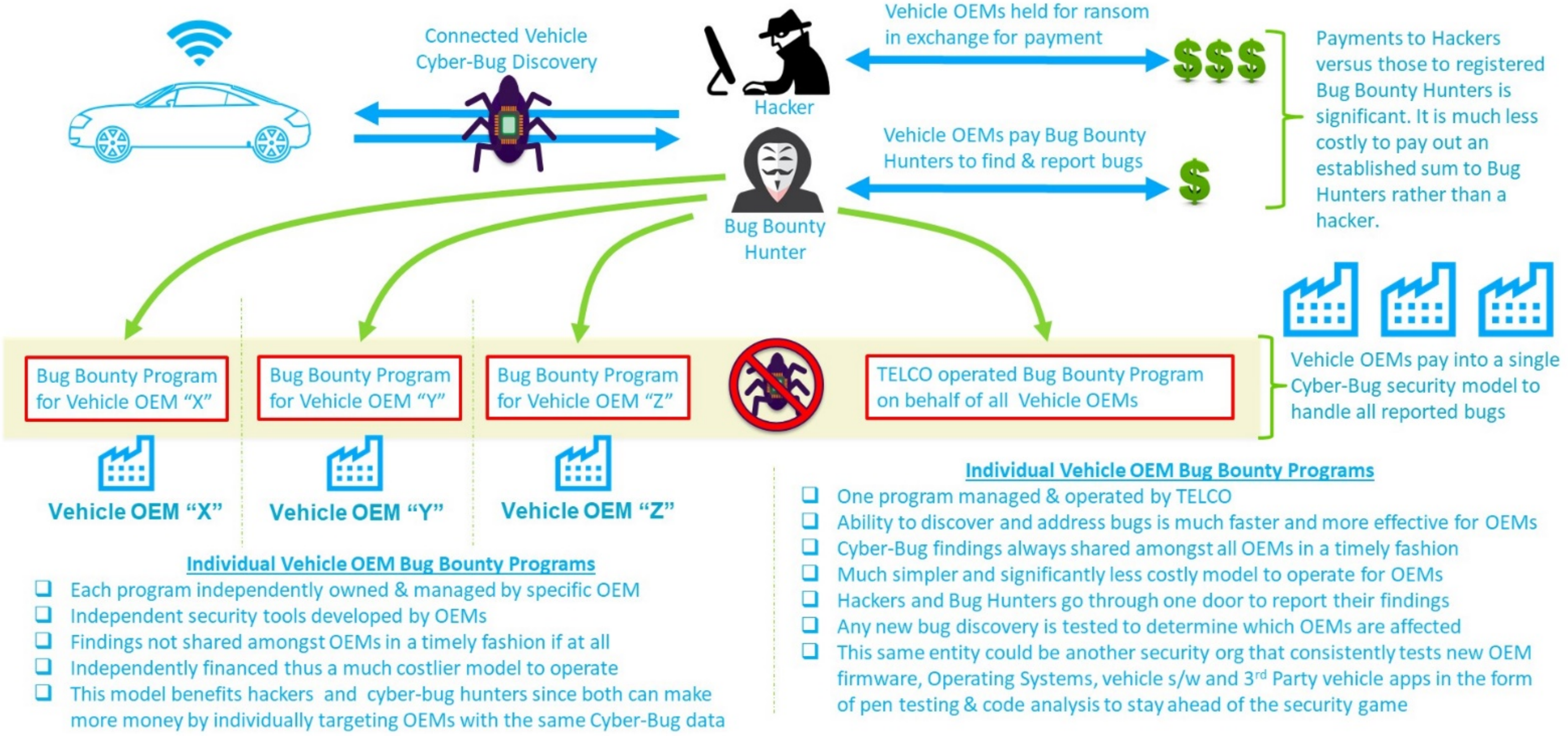

Telco Operated/Managed Service
Mobile Devices
Connected Vehicles
Connected Vehicle App Store
App Acceptance Process/Testing
Over The Top Service Provider Apps
Support Center
Insurance Companies
Media Agencies
Repair Shop
Automotive OEMs
OEM Partners
3rd Party App Developers
❑ Only automotive OEM apps are encrypted when submitting
❑ App signature and security certificate validation
❑ Terms & conditions for submitting apps
❑ Security checklist, policies & guidelines for submitting apps
❑ Compatibility testing
❑ Security by Design testing
❑ Validation of encryption, authentication & authorization mechanisms/libraries
❑ Penetration testing

The topics discussed in this section are not intended to be a definitive list of areas for collaboration. They are only examples, but do illustrate areas where the joint expertise of the telecommunications network providers and the vehicle OEMs could contribute to greatly enhanced cybersecurity for connected vehicles.

Connected Vehicle Bug Bounty Program

Vehicle OEMs have in some cases initiated “bug bounty” programs, offering a payout for new security bugs that are reported. Telecommunication carriers or another third party could enhance the effectiveness of these programs by acting as a front end for these services. This would enable all vehicle OEMs and all telecommunications carriers to have the same view of the bugs and risks. The more data on potential exploits and vulnerabilities that is available, the better and more accurate the analysis would be to mitigate against these vulnerabilities for all members of the connected vehicle ecosystem. When an attack is discovered on one vehicle, a federated security bug bounty program would allow telecommunications carriers to identify similar issues for code on other vehicle manufacturers *before* they are impacted. Over time, all vehicle OEMs could benefit from this program. This is another example of the potential for telecommunications carriers working together for the benefit of the full connected vehicle industry.

Figure 15 – Connected Vehicle Bug Bounty Program



Payments to Hackers versus those to registered Bug Bounty Hunters is significant. It is much less costly to pay out an established sum to Bug Hunters rather than a hacker.

Vehicle OEMs pay into a single Cyber-Bug security model to handle all reported bugs

Individual Vehicle OEM Bug Bounty Programs

□ Each program independently owned & managed by specific OEM

□ Independent security tools developed by OEMs

□ Findings not shared amongst OEMs in a timely fashion if at all

□ Independently financed thus a much costlier model to operate

□ This model benefits hackers and cyber-bug hunters since both can make more money by individually targeting OEMs with the same Cyber-Bug data

Individual Vehicle OEM Bug Bounty Programs

□ One program managed & operated by TELCO

□ Ability to discover and address bugs is much faster and more effective for OEMs

□ Cyber-Bug findings always shared amongst all OEMs in a timely fashion

□ Much simpler and significantly less costly model to operate for OEMs

□ Hackers and Bug Hunters go through one door to report their findings

□ Any new bug discovery is tested to determine which OEMs are affected

□ This same entity could be another security org that consistently tests new OEM firmware, Operating Systems, vehicle s/w and 3rd Party vehicle apps in the form of pen testing & code analysis to stay ahead of the security game

12. Conclusion: Working Together (ICT and OEMs) – What Can We Achieve?

This white paper has provided an overview of the cybersecurity expertise of the ICT industry and shown how this could be applied to the connected vehicle. This material is intended to provide a starting point for an industry-to-industry discussion to jointly identify next steps that the ICT and vehicle OEM industries can take together and independently to advance cybersecurity efforts. The ICT industry has developed many use cases that provide the basis for active cybersecurity offerings and many of them apply to vehicles. The potential benefits from a joint cybersecurity program include:

- Improved confidence in the safety of connected vehicles.
- Higher level of cyber detection and threat prevention.
- Risk reduction initiatives and a shared risk model that recognizes "we're all in this together."
- A huge win from a marketing perspective for all partners involved in propelling this technology forward and encouraging governments to further invest in smart cities to maximize the connected vehicle's potential. When governments see multiple partners working closely together toward a common goal, support is more likely for the initiative.
- Reduce overlap in security R&D aimed exclusively at connected vehicles.
- Reduced costs by having all partners sharing responsibility and accountability to define, design, and deploy new connected vehicle security measures.
- Improve information sharing and cooperation among all partners, thereby reducing each company's individual risk.
- Decreased time-to-market with new security initiatives for connected vehicles.
- Potential to develop new services for the connected vehicle market; without cooperation between the partners many of these services might never emerge.

- Improve the time-to-market for new security standards for the connected vehicle since the partners would already be working together on multiple fronts and in agreement to promote recommendations and designs.

Appendix A: A Dedicated Short-Range Communication

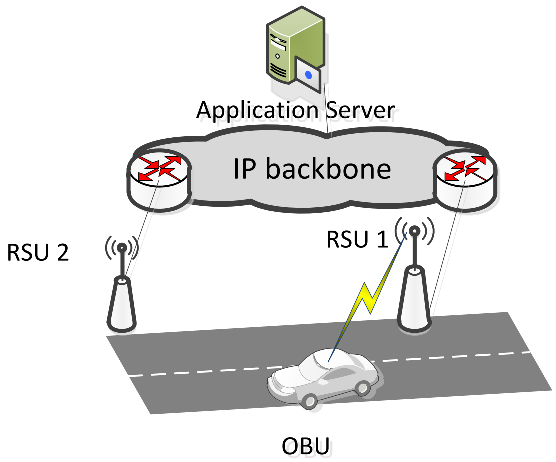
Significant efforts to standardize vehicular communications technology have been made by major contributors in industry, academia, and the public sector. In North America, the U.S. Department of Transportation is accelerating the regulation of Dedicated Short-Range Communications (DSRC) for Intelligent Transportation Systems ITS initiatives [1]. The connected vehicle standardization is expected to be fully tested and deployed in the near future [2].

The main objective of DSRC is to enable the transmission of safety messages among vehicles in order to reduce the number of accidents on the road. This wireless technology is based on the IEEE 802.11p standard which defines the medium access control specifications for nodes in highly mobile environments. The main network elements are briefly described below.

- On-Board Unit (OBU). This communication equipment is expected to be installed inside the vehicle by the vehicle OEM. The OBU is a tamper-resistant device that consists of a wireless transceiver of 5.9 GHz, a GPS location system, a processor for application services, and Human Machine Interface (HMI).
- Roadside Unit (RSU). This communication equipment is expected to be deployed along the road network by municipalities. The RSU is the gateway between the fixed infrastructure and the vehicle. The RSU comprises a wireless transceiver of 5.9 GHz, and a GPS location system.
- Message Switch (MSW). The MSW handles and parses all data intended to reach any network element within the fixed infrastructure.

Figure A.1 illustrates the communications between a vehicle and the roadside infrastructure.

Figure A.1 – Communication between the OBU and RSU



In order to support the transmission of expedited messages, the communication protocol stack defines a new layer called Wireless Access in Vehicular Environments (WAVE) (Figure A.2). WAVE describes the methods to exchange different types of messages depending on the intent of the application (See Table A.1). There are two communication modes: the first one is Vehicular-to-Vehicular (V2V) where high speed vehicles exchange messages. The second one is Vehicular-to-Infrastructure (V2I) where high speed vehicles exchange messages with the roadside infrastructure.

Figure A.2 – DSRC WAVE protocol stack

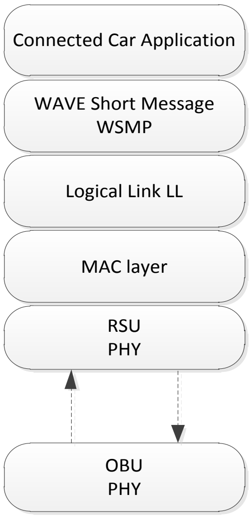


Table A.1 – Channel Allocation for WAVE Applications

Frequency (MHZ)	Channels	Applications
5860	172	Control channel
5870	174	Public safety/Private
5875	175	Public safety/V2V
5880	176	Control channel
5890	178	Public safety/Private
5900	180	Public safety/Private
5905	181	Public safety/Private
5920	184	Public safety intersections

Security Considerations for DSRC

The security requirements for DSRC are addressed on WAVE P1609.2 [3], which describes different security services for WAVE applications. Moreover, this standard defines the methods to secure message formats and their processing along the communicating elements [4]. The main security considerations are as follows:

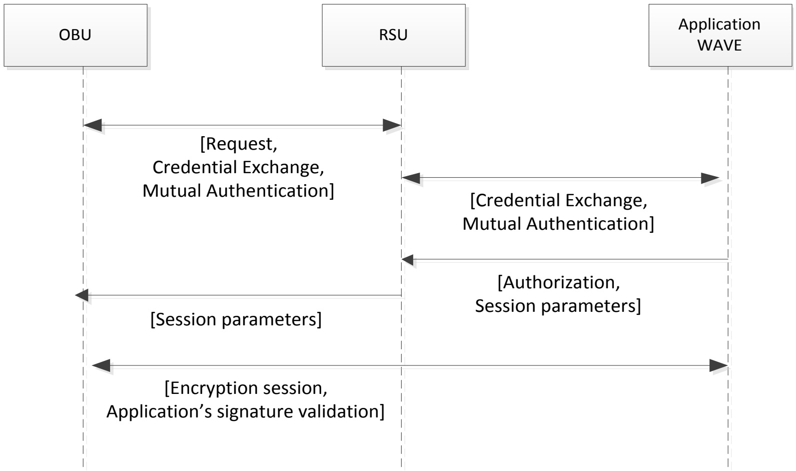
- Support of mutual authentication between the network elements through Public Key Infrastructure (PKI). Vehicles are given a set of cryptographic keys by a Certificate Authority (CA) managed by official transit authorities. Government CAs are considered to be trusted network elements.
- Support of encryption between the OBU and the roadside infrastructure is done at the link level when a service session is established. End-to-end encryption is achieved by the use of short-term session keys.
- Application messages transmitted by the roadside infrastructure are authenticated by the OBU nodes through the validation of the sender's signatures.
- Support of privacy by randomizing OBUs' addresses.
- Validation of high-priority messages with another set of special cryptographic keys.

The main requirements for certificates are as follows:

- Certificates for OBUs will be provided by vehicle (OEMs) and can also be provisioned by official transit authorities.
- Transit authorities are considered to be trusted entities and these are responsible for the generation of root certificates.
- Root certificates are based on a hierarchical architecture providing separation of duties and anonymity to OBU certificates.
- OBUs and RSUs certificate model follows a hierarchical architecture.
- For certificate revocation, OBUs will require to be updated with a certificate revocation list from official authorities. It is worth noting that the set of OBUs' certificates have identifiers derived from a single secret for a unique OBU.

Figure A.3 illustrates the secure interaction between the network elements.

Figure A.3 – Service Enablement Interaction


OBU
RSU
Application WAVE
[Request, Credential Exchange, Mutual Authentication]
[Credential Exchange, Mutual Authentication]
[Authorization, Session parameters]
[Session parameters]
[Encryption session, Application's signature validation]

Even though vehicles are considered non-Trusted network elements by nature, the security considerations listed above need to address the security pillars for vehicular communications, i.e., Confidentiality, Integrity, and Availability.

References

1. Intelligent Transportation Systems Joint Program Office, U.S. Department of Transportation. "Connected Vehicle Basics." < http://www.its.dot.gov/cv_basics/cv_basics_how.htm >.
2. Hill, K. "What is DSRC for the connected car?". RCR Wireless News. < http://www.rcrwireless.com/20151020/featured/what-is-dsrc-for-the-connected-car-tag6 >.
3. Ahmed, S. A. M., Ariffin, S. H. S., Fisal, N. "Overview of Wireless Access in Vehicular Environment (WAVE) Protocols and Standards". Indian Journal of Science and Technology. <http://www.indjst.org/index.php/indjst/article/viewFile/34355/27974 >.
4. Weigle, M. "Standards: WAVE / DSRC / 802.11p". Old Dominion University. < http://www.cvt-project.ir/Admin/Files/eventAttachments/109.pdf >.

Appendix B: Current Telecommunications Carrier Initiatives in Cybersecurity

This Appendix adds detail to Section 8 of the main body of this white paper.

First Layer: Transport Security, Traffic Segregation and Traffic Analysis

Secure Mobile Network Connectivity (from the Vehicle to the Wireless Network)

Secure network connectivity is designed into today's mobile network based on a wide range of 3GPP security standards. In addition, the telecommunications industry has developed robust mechanisms for provisioning, connecting, authenticating, managing, and securing devices accessing the network. This knowledge has been incorporated into the underlying 3GPP standards, the chipsets, and the software in mobile devices. A key component of this security is the UICC (Universal Integrated Circuit Card) that contains the USIM (UMTS Subscriber Identity Module), which is the 3G+ application for securing mobile devices. It includes the private keys and network parameters that carriers use to manage and secure the device, and allows 3G+ devices to mutually authenticate with the network. A UICC can also hold certificates that allow the network to authenticate applications.

Secure Wireline Network Connectivity

Telecommunications carriers use various techniques to ensure a customer's traffic is secure and isolated from other customers' (Internet) traffic. These can include:

- Virtual Private Network (VPN) sends traffic from a customer over public access connections, but establishes a virtual point-to-point connection through the use of MPLS, virtual tunneling protocols, or encryption. This approach provides performance and security approaching the level provided by a private network.

- Dedicated Access Point Name (APN) can be used for wireless traffic that requires priority treatment or additional security features. This allows specific traffic (e.g., for a connected vehicle) to be routed separately from general Internet traffic and to receive enhanced security treatment. This traffic could also be routed to additional security systems, such as malware scanning to monitor traffic on a specific APN or to/from a set of devices. These malware scans can identify malware, notify users, and if required, pre-emptively block the malware.
- Encryption is applied at several points in today's networks, including the air interface, backhaul, and transport networks. This provides additional security for traffic.
- Integrity Protection is used to mitigate against injections and replay attacks. Some encryption algorithms also contain integrity protection.

Network Layer Firewalls

Firewalls are systems that prevent access to or from a network and therefore control the flow of traffic. Telecommunications carriers employ firewalls throughout their networks. Firewalls generally work via one of five mechanisms:

1. Packet Filtering.
2. Proxy.
3. Stateful inspection.
4. Dynamic packet filtering.
5. Kernel proxy.

DDoS Mitigation and Prevention

Distributed Denial of Service (DDoS) attacks generally employ bots to take over computers and servers and generate attacks aimed at a host server, thereby overwhelming the host server's ability to function, slowing processing or stopping it entirely. Telecommunications carriers take many steps to reduce DDoS attacks, including:

1. Rate limiting techniques that limit the maximum traffic to the server to ensure the server can withstand peak traffic volume.
2. Access Control Lists that limit access from certain servers or telecommunication paths to ensure that traffic is from legitimate sources.
3. Deployment of attack countermeasures such as traffic scrubbing to block or limit traffic based on the "attack signature".
4. Blocking DDoS traffic at the source or as close to the originating network connection as possible.

Second Layer: Access Controls, Application and Data Security

Application Layer Firewall

Many threat vectors in the vehicular environment target the upper layers (i.e., the applications) within the connected vehicle. Application firewalls are an important tool to secure applications and prevent malicious agents from compromising their availability and integrity. Telecommunications carriers work with device and applications providers to enforce applications security controls to mitigate the risks as much as possible. Some common controls are:

1. Web application firewalls provide protection for web services, and the security controls at this level can prevent

attacks such as cross-scripting sites, data injection, phishing, intrusion, and DDoS attacks.

2. Scrubbing centers where data is filtered and analyzed for malicious content. Also, this may include Deep Packet Inspection (DPI) tools to filter payload from in-line traffic.
3. Threat intelligence platforms, which provide information on discovered malware to support defensive actions. Threat detection techniques become essential at the application layer.
4. Scanning tools such as Static Application Security Testing (SATS) and Dynamic Application Security Testing (DAST) assessments perform vulnerability scans on the source code and data flows on web applications. Many of these scanning tools run different security tests that stress applications under certain attack scenarios to discover security issues.

Intrusion Detection and Prevention Systems (IDS/IPS)

Intrusion Detection Systems (IDSs) detect and log inappropriate, incorrect, or anomalous activity. IDS can be located in the telecommunications networks and/or within the host server or computer. Telecommunications carriers build intrusion detection capability in all network connections to routers and servers, as well as offering it as a service to enterprise customers. IDS typically functions via one or more of three systems:

1. Pattern matching.
2. Anomaly detection.
3. Protocol behavior.

Once IDS systems have identified an attack, Intrusion Prevention Systems (IPSs) ensure that malicious packets are blocked before they cause any harm to backend systems and networks.

Authentication and Authorization

Because telecommunications carriers allow access to their networks by their customers (subscribers), provide different levels of service and bill those customers for service, AA security is a common baseline security layer for subscribers.

Authentication is the security process that validates the claimed identity of a device, entity or person, relying on one or more characteristics bound to that device, entity or person. Authentication can be ascertained via human input (such as inputting a passcode, fingerprint, voiceprint or IRIS scan) or automatically via machine to machine (M2M) authentication using digital certificates or digital credentials. Common digital authentication methods include:

- Raw Public Keys (RPK).
- Public Key Infrastructure (PKI) used to managed X.509 SSL Certificates.
- Pre-Shared Keys (PSK) such as employed SIM/AKA.

Mobile networks extend this to support mutual authentication between device and network (i.e., the device authenticates with the network to prove it is a legitimate device, and the network authenticates with the device to prove it is a legitimate network) allowing devices to identify rogue cell sites or other rogue or spoofed origination points and then not attach or allow traffic to be transported.

Authorization parses the network to allow access to some or all network functionality by providing rules and allowing access or denying access based on a subscriber’s profile and services purchased.

Identity and Access Control

Identity management (ID management) is a broad administrative area that deals with identifying entities in a system (such as a country, a network, an enterprise or an individual, or a device) and controlling access to resources within that system by associating user rights and restrictions with the established identity. Identity management is related to authentication, authorization, and accounting, but provides a broader set of capabilities for flexibly managing access to information and resources.

Deep Packet Inspection (DPI)

DPI provides techniques to analyze the payload of each packet, adding an extra layer of security. DPI can detect and neutralize attacks that would be missed by other security mechanisms.