

Connected Car Architecture and Virtualization

Husein Dakroub
Visteon Corporation

Adnan Shaout
Univ. of Michigan

Arafat Awajan
Princess Sumaya University of Technology

ABSTRACT

Connectivity has become an essential need for daily device users. With the car projected to be the “ultimate mobile device”, connectivity modules will eventually be mainstream in every car. Network providers are expanding their infrastructure and technology to accommodate the connected cars. Besides making voice and emergency calls the connected car will be sharing data with telematics service providers, back end systems and other vehicles. This trend will increase vehicle modules, complexity, entry points and vulnerabilities. This paper will present the current connected car architectures. The paper will present current architectural issues of the connected car and its vulnerabilities. The paper will present a new proposed architecture for the future connected car that enhances efficiency and security.

Keywords: Connectivity, Architecture, Autonomous Cars, Efficiency, Security, Virtualization

CITATION: Dakroub, H., Shaout, A., and Awajan, A., "Connected Car Architecture and Virtualization," *SAE Int. J. Passeng. Cars – Electron. Electr. Syst.* 9(1):2016, doi:10.4271/2016-01-0081.

I. INTRODUCTION

The future of the automotive industry is to turn the vehicle into a valuable partner in the Internet-of-Things (IoT), where every device is connected to the Internet. The practical way in generating data was usually through human generated data, but going forward we will see data generated by devices. This trend will increase the amount of modules and software in the vehicle. Sensors will eventually be placed throughout the body of the vehicle. The automotive industry is heading to self-driving autonomous cars. A recent technology and product line driven by this is Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure which is generally referred to as Vehicle-to-Everything (V2X). Dedicated Short Range Communication (DSRC) is a standardized short-range communication between “things” and the vehicle. One can see the architecture of the connected car as the vehicle connected to anything with an electronic device. With a focus on connectivity between the car and everything, V2X, vehicle, cloud, smartphone, servers and infrastructure can replace X. The process of exchanging data is relatively straightforward for many manufacturers and automotive suppliers, but the competitive piece of the architecture is consolidation, security and consumer privacy. With these connected features, the modules open many entry points to potential hackers. Hackers can potentially cause accidents and remotely control vehicles [1].

There can be multiple vulnerabilities for the vehicle, but some of the physically achievable threats are access to electronic control units (ECU's), a driver's mobile device that is connected to the vehicle and the cloud infrastructure. To achieve great security, the protocol, authentication, authorization, encryption and data protection have to be bulletproof. The ECU can be reverse engineered. Hardware altered or probed to potentially identify how to hack other components in the vehicle [1]. In general, production systems usually have diagnostic access which potentially can be a threat, but that is out of the scope of this paper.

Over-the-Air updates (OTA) can alter code in vehicle modules that updates their software to do new things. Moreover, the vehicular network can easily be reversed engineered, that's why it's essential to protect diagnostic data, firmware update, or critical commands [1]. For connected devices to the infotainment or connectivity system, the ability to get into the software of the systems through the kernel can lead to the exchange of deception techniques with malware.

Moreover, as vehicle functionality is growing, so is the amount of hardware modules and software within the vehicle. This trend increases the complexity of software, cost and weight of the vehicle. Automakers will need to reduce somewhere to accommodate for this new drift of events to sustain the same bill of material cost. Also, as

government mandates an improvement in fuel efficiency year over year, OEMs will have to reduce weight to improve their fuel efficiency. This paper will present a solution that will benefit automakers by reducing cost, creating a consistent environment and increase security.

The paper is organized as follows: section II presents the current connected car architecture, section III presents the current connected car architecture issues, section IV presents a new proposed architecture that would achieve efficiency and security and finally section V will present the conclusion.

II. CONNECTED CAR ARCHITECTURES

What defines a connected car? Connected car is a car equipped with Internet access. It allows the car to be made available to the Internet for shared data. The connection to the Internet is typically done by a built-in embedded modem on-board the car called a Telematics Control Module (TCU) and a Wi-Fi connection available within a module inside the car [2]. Some of the functions of a connected car include the following:

- Automatic roadside assistance in case of crashes
- Information calls to Telematics Service Providers (TSP)
- Stolen Vehicle Tracking (SVT)
- Remote Service (Vehicle on/off, vehicle lock/unlock)
- Vehicle Updates
- Video streaming / Web browsing

The car can be connected in several ways. Depending on what it is being connected, the car has a different form of technology associated with that respective connection. The following is a list of several nodes that the car is typically connected to [3]:

- *Car-to-Network:* In this form of connection, the car is connected to the cellular network (2G, 3G or 4G), and is the medium to where SMS, Data and Voice Calls are transmitted.
- *Car-to-TSP:* This form of communication utilizes the network but is connected to a backend vehicle service provider. The Telematics Service Provider (TSP) has the ability to share data with the car,
- *Car-to-Cloud:* The cloud can store data and be accessed by the car via the network.
- *Car-to-Car:* In this form, cars communicate wirelessly among each other over short-range communication with safety related alerts.
- *Car-to-Infrastructure:* In this form of communication, the car is connected to the surrounding environment and engaged in exchange of data such as traffic lights, stop or speed limit signs.

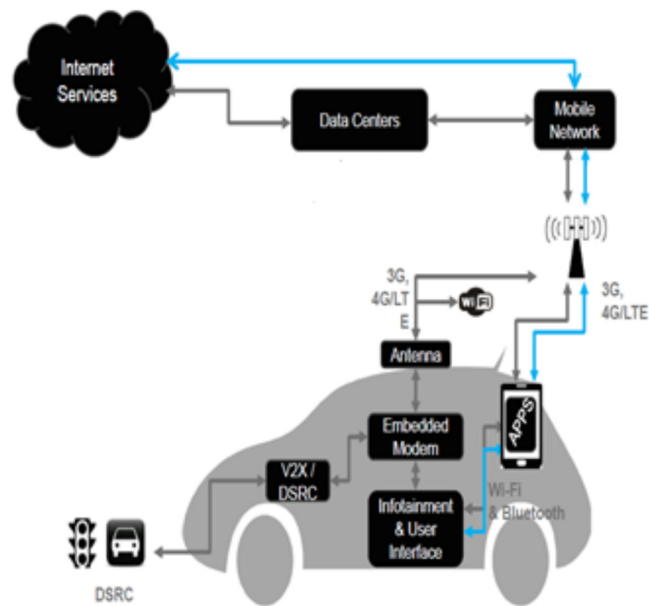


Figure 1. Connected Car (source Visteon [20])

Figure 1 displays a typical architecture for a connected car, with many hardware modules that can interact with the outside world. The following are the hardware modules that enable connectivity to anything outside the vehicle [3] [4]:

- *V2X/DSRC:* Vehicle-to-X (V2X) is a term used to describe the connection of a vehicle to anything such as a vehicle or infrastructure. V2X standards are currently being defined and are expected to operate using DSRC technology.
- *TCU/Embedded Modem:* The TCU, which typically houses the embedded modem, provides an Internet connection to the car based on a Cellular connection using 2G, 3G or 4G.
- *Infotainment:* Infotainment system provides the car with User Interface (UI) and radio/entertainment/media functionality, giving the driver the ability to connect over Wi-Fi or Bluetooth.

Vehicle Module	Technology	External to the Vehicle
V2X	DSRC	Vehicle/Infrastructure
TCU	2G/3G/4G	Telematics Services
Infotainment	Bluetooth/Wi-Fi	Smartphone/Home

Figure 2. Technology Chart

The previous paragraph discusses the hardware that enables the connected car features. The following paragraph will depict the wireless technology that enables the connectivity between the modules inside and outside the vehicle as shown in Figure 2:

- *Dedicated Short Range Communication (DSRC):* is a short-range wireless communication channel designed for automotive use. It utilizes the 5.9 GHz band [3].

- *Cellular Network (3G, 4G)*: 3G and 4G are mobile telecommunication technologies. They are based on a set of standards used for mobile communication that you must comply with for using the services and networks [4].
- *Wi-Fi*: A local area wireless communicating technology which uses the 2.4 GHz and 5 GHz band. It is defined by the Wi-Fi Alliance and is based on the IEEE 802.11 standards [5].
- *Bluetooth*: Short ranged, low powered radio waves. It communicates on the 2.4-2.48 GHz band [5].
- *NFC*: Near Field Communication (NFC), operates at 13.56 MHz and transfers wireless data up to 424 Kbits/s over a range of 4-10cm [6].

III. CONNECTED CAR ARCHITECTURE ISSUES

The current state of the art shown in section II consists of a distributed system. Many ECU's are dispersed around the vehicle's Controller Area Network (CAN) bus, communicating and triggering different commands, with some utilizing the same technology. Automakers usually source multiple Tier 1 suppliers to develop and manufacture the different ECUs in the vehicle. This has some political and manufacturing reasoning. To achieve better pricing, one would need multiple suppliers to bid on several products and leverage other ECUs currently in the vehicle in exchange for pricing on new ECUs. Moreover, in case of a Tier 1 supplier filing bankruptcy or having manufacturing constraints, automakers would need to have other Tier 1 suppliers already sourced on other projects to be educated enough about the automakers' logistics and manufacturing process to be competent enough to pick up added work, when needed.

The previous paragraph discusses some of the pros in a distributed and multi-sourced architecture. This paragraph discussed some of the cons. Typically, a standalone ECU consists of a printed circuit board (PCB) that is populated with discrete components, RAM and Flash memory, a processor that would handle the heavy processing and a Vehicle Interface Processor (VIP) that would handle the application logic and interfacing to the vehicular CAN bus. This redundancy of material and work is expensive and can cause latency, communication and upgrade capability issues, not including the hefty cost it takes to manufacture, validate and ship each ECU from the respective manufacturing plant. Furthermore, it takes companies' considerable amount of effort and resources to bring an Operating System (OS) up to the required automotive standards, fine-tuning and validating similar Board Support Packages (BSP) across multiple modules. This effort needs a great amount of capital investment made by OEMs to source multiple suppliers to develop something of this caliber.

In addition to some of the financial hurdles discussed, Firmware update Over-The-Air (FOTA) is an essential component of the connected car with ever changing protocols and features. The need to update software has become a priority, and as shown in [Figure 1](#), with multiple ECUs dispersed around the vehicle. FOTA updates become increasingly difficult to conduct with bottlenecks in entry points and vehicle network speeds.

Moreover, governments are frequently mandating automakers to improve their fuel efficiency. The US administration issued a statement on August 2012 that would require automakers to nearly double their average fuel economy of new vehicles by 2025 [16]. Transportation secretary said the new standards would save \$1.7 trillion in fuel costs. There are many ways to improve fuel efficiency, but the one method that correlates with the topic of this paper is weight. Reducing weight of the vehicle can drastically improve fuel efficiency. Weight reduction is increasing in the automotive world, for example, the 2015 Ford F150 redesigned to all aluminum helped achieve greater fuel efficiency. A research study conducted by Richard Broda and Anrico Casadei [17] has shown the impact of vehicle weight reduction on fuel economy. The author conducted different tests that correlated weight reduction with fuel consumption. Results concluded that reducing the vehicle weight resulted in less tractive effort required to accelerate the vehicle and less rolling resistance from the tires. Drive cycles showed greater fuel economy benefits from weight reduction [17]. To conclude, having many ECUs around for the connected car can increase the weight of the vehicle and can cause inefficiency with respect to fuel consumption for automakers.

To have a robust and efficient security solution, one has to understand the threats to the car. The following are some threats to the vehicle:

- *Software update*. Perform software update with altered unofficial re-flash image, which could include malicious code.
- *Antenna jamming*. Use RF signal generators to emit strong signal in the bands of interest to jam/interfere normal operation of a wireless module and/or a GPS module.
- *Wireless network spoof*. Use wireless network simulator or small cell to gain access to vehicle's OTA interface and accomplish intended tasks. This could be used as a method to facilitate other attack scenarios.
- *Manipulate wireless account settings*. Unauthorized manipulation of wireless account setting through the wireless carrier's control portal or similar interface.
- *Attack on WWAN*. The infected Device initiates attack on wireless wide area network (WWAN) by flooding spam voice calls, data calls or SMS. This is a scenario associated with other attack scenarios
- *Spoofing TSP with SMS*. Utilize WWAN interface to spoof as a valid TSP by sending legitimate SMS in right format. The attacker has proper knowledge of message definition and protocol used by TSP.
- *Hijack Data Communication with Server*. Intentionally send bad URL/spoof DNS system (man in the middle attack) to hijack data communication between Device and server.
- *Sniff SMS*. Use techniques to receive and decode SMS communications on interface between TCU and TSP.
- *Malicious Code Injection, Bluetooth*. Crash the product or inject malicious code by exploring the weaknesses in the Bluetooth communication stack or device software code, such as handling invalid or out-of-range input.