ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 3, No. 6, 105-110 (2018)

www.astesj.com

First International Virtual Conference on Multidisciplinary Research 2018

ASTESJ

ISSN: 2415-6698

Analysis and Methods on The Framework and Security Issues for Connected Vehicle Cloud

Lin Dong[1,2], Akira Rinoshika[2,*]

[1]*Mechanical and Automotive Engineering School, Shanghai University of Engineering Science, 201620, China*

[2]*Department of Mechanical Systems Engineering, Yamagata University, 992-8510, Japan*

ARTICLE INFO

Article history:
Received: 07 June, 2018
Accepted: 09 July, 2018
Online: 14 November, 2018

Keywords:
Internet of Things (IoT)
Connected Vehicle Cloud (CVC)
Security of Vehicle Cloud

ABSTRACT

In the world today, the rapid development of the Internet of Things (IoT) and the application of the Connected Vehicle Cloud (CVC) as the Internet of Things in the intelligent transportation are becoming widespread. They can improve people's safety, vehicle security as well as reduce the cost of ownership of an automobile. At the same time the security of the Internet is a non-negligible factor in the development of the Internet of Vehicles. Therefore, the security of vehicle networking is of great concern. This article starts with the network architecture of vehicle networking and combines the examples of vehicle networking security issues, which analyzes and researches the security problems of vehicle networking, and proposes solutions to the security problems faced.

1. Introduction

Connected Vehicle Cloud (CVC) increases the core business value of automotive OEMs by providing a platform for creating, managing, and deploying connected vehicle services as shown in Figure1. It creates a direct channel to the driver and gives the possibility to introduce new partners to participate in the value network of the automotive industry. CVC enables OEMs to engage with different players in the automotive eco-system to deliver services while remaining in control and keeping the costs of deploying and managing the services to a minimum, as shown in fig 1.

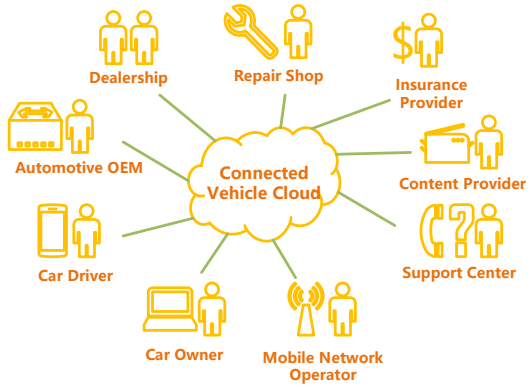

Figure 1. Connected Vehicle Cloud powering the Automotive Ecosystem.

*Akira Rinoshika, Email: rinosika@yz.yamagata-u.ac.jp

CVC is a common service delivery platform for infotainment, telematics, and other services related to connected vehicles. It is completely independent of connectivity solutions and can be deployed without any integration with a mobile network. CVC is based on the Service Enablement Platform (SEP). SEP combines functional components from Multiservice Delivery Platform (MSDP), General Composition Engine (GCE), M2M Data Management (M2M DM) and Dispatcher.

Cloud Computing is the basis of CVC [1]. Cloud Computing is the internet based new computing system which is distributing services for the interest of clients such as shared network resources, software, and platform computing infrastructure [2]. Therefore, the CVC is an open platform that supports flexible deployment and realization of services. The flexibility of the Service Enablement Platform (SEP) allows the CVC to be continuously adapted to changing business and technical requirements. SEP has functionalities needed to support creation and deployment of connected vehicle services. Each connected vehicle service is developed according to the customer needs with the support of the SEP functionality and sometimes with the support of additional third-party components (3PPs). Through these components, vehicles can access the cloud and obtain, at the right time and the right place, all the needed resources and applications that they need or want [3].

Connected Vehicle Cloud provides functionality to connect vehicles and other devices to the cloud. Vehicles are securely

connected through a bidirectional communication link supporting multiple protocols and notification mechanisms such as SMS Shoulder Tap, HTTP, and MQTT. Status information and data are collected and sent to CVC, where it is normalized, stored, aggregated and combined with data from other systems and sensors.

This data (in whole or in part) is distributed to CVC applications and participants who gained the relevant access rights. With granular access control, you can publish only the precise information necessary to subscribe to services such as analysis systems. Events are defined for notification when a particular set of conditions is applied.

Firmware update function allows the OEM to wirelessly update software and firmware of onboard units in the vehicle. CVC acts as a cache and provides software updates for many vehicles. In addition, because business rules and scheduling functions are also provided, OEM can control which software file is provided to which vehicle when and when. Many industry standard protocols for software and firmware updates are provided by the standard, and additional protocols are being added using the open SDK.

This paper firstly presents the main actors of the Connected Vehicle Cloud solution. Then the analysis of security problems are caused by CVC. Finally a solution of CVC security issues is provided.

2. Framework of connected vehicle cloud

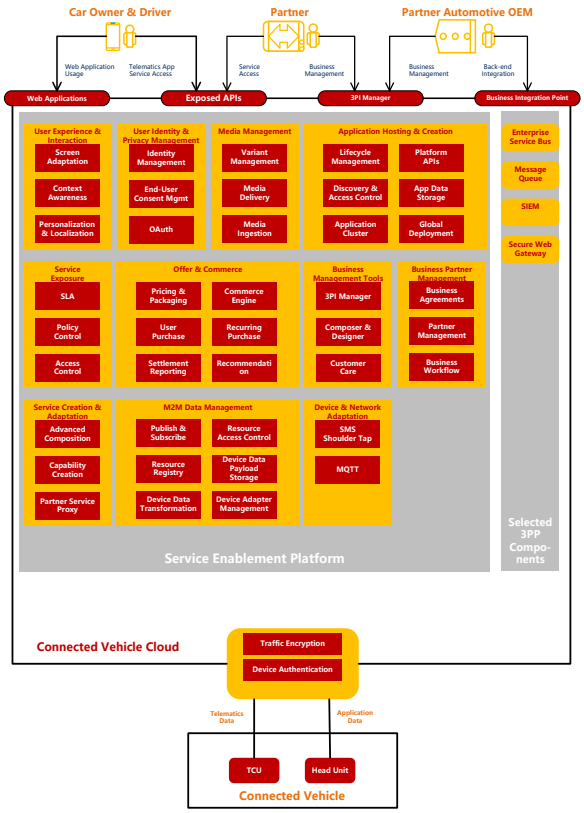

Figure 2. Connected Vehicle Cloud Functional Overview.

CVC is a comprehensive platform for creating, deploying, and managing all types of services related to connected vehicles.

CVC is an open platform that supports flexible deployment and realization of services. The flexibility of the Service Enablement Platform (SEP) allows the CVC to be continuously adapted to changing business and technical requirements. SEP has functionalities needed to support creation and deployment of connected vehicle services. Each connected vehicle service is developed according to the customer needs with the support of the SEP functionality and sometimes with the support of additional third-party components (3PPs).

An overview of the main functional areas of SEP that are used in CVC as well as some of 3PP components that typically make the foundation of a customer solution is shown in the above fig 2.. The fig 2. also shows some examples of how the main actors in the automotive ecosystem interact with the CVC.

2.1. The main actors of the Connected Vehicle Cloud framework

- Car Driver and Owner:

  The primary end-user of CVC is a person driving a car connected to the cloud. The driver or owner accesses the services of CVC through one or more devices types connected to the cloud. For example, a built-in head unit in a car, a smartphone application, or a web portal offering services related to the vehicle. CVC separates the Driver and Owners from the Connected Vehicle; they are the end users of most of the services deployed in CVC, and they may be using services related to one or more vehicles. In some cases, an end user may be someone who is not the driver or owner of the vehicle that he is accessing services from.

- Connected Vehicle

  A vehicle connects to CVC through one or more mobile network connections. CVC Services are delivered to one or more of the vehicle's built-in or aftermarket devices such as an infotainment head unit or a telematics control unit (TCU). The vehicles connect to CVC using one or more components in the vehicle that is capable of sending and receiving data to and from the cloud, execute service logic, display information to the drivers and passengers, collect data from the vehicle, and interact with other micro-controllers and software components in the vehicle. The capabilities of the components in the Connected Vehicle can vary greatly depending on the vehicle platform, and the functionality can be separated into a variety of different components. In this document, we refer to these type of components as being either a component that is primarily focused on telematics services, a Telematics Control Unit (TCU), or a component responsible for infotainment services, a Head Unit.

- Automotive OEM

  An enterprise that manufactures the vehicles connected to the CVC is the Automotive OEM (OEM). The OEM uses the services delivered through CVC to build and improve the customer relationship with car owners, capture aftermarket sales, collect vehicle information to improve quality control, and earn additional revenues from partners accessing or providing services through the platform. The OEM will typically integrate CVC with existing business support systems.

1) Partners
CVC enables any of the players in the automotive eco-system to become a partner of the Automotive OEM. The partner will provide services through CVC or access services provided by the platform.
a) An Insurance Company that gains access to the platform to enable a Pay-as-You-Drive program.
b) A Telematics Service Provider the uses the platform communication channels to deliver Tele Guard services to assist drivers in the case of a breakdown.
c) A Live Traffic Information Provider that provides real-time traffic information content to multiple Intelligent Navigation services deployed on the platform.
d) A Fleet Management Company that buys access to the platform APIs to develop its own Fleet Management Applications.
2) Service Provider
CVC service provider is responsible for operating CVC and delivering services to the connected vehicles. The service provider can be an Automotive OEM, a mobile operator, or any other party willing to take this role.

2.2. Component architecture of the Connected Vehicle Cloud framework

The CVC solution is comprised of MSDP, GCE, M2M DM, and the Dispatcher components which provide the different functionalities of the solution. This chapter gives a high-level overview of the functionalities of the different components and how they interact with each other.

This chapter describes how the different components in CVC are used together to realize and expose the functionality of collecting data and sending message to in-vehicle devices. This functionality provides a foundation for implementing any type of telematics service. Depending on the business needs and customer requirements the solution can be implemented with or without using the Service Exposure and User Identity Privacy Management functionality.

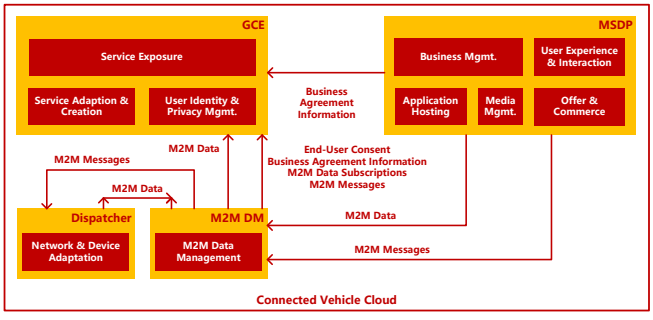

Figure 3. Overview of Components of CVC and How They Interact with Each Other.

Fig 3. provides an overview of the components, the functionalities they provide, and the primary information flows between the different components. Chapter III gives a detailed description of the different functionalities of CVC. For detailed instructions on how to install and configure MSDP, GCE, M2M DM, and the Dispatcher components, refer to Installation and Initial Configuration Guide for CVC 1.3 [4].

The following is a short description of how the components interact with each other.

MSDP: The MSDP realizes the business management related functionality of CVC. The 3PI Manager tool is used to configure business agreements which define the SLAs and terms of the services that are made available to the business partners of the OEM through the Service Exposure Functionality. Once the agreements have been signed and activated in MSDP the information is provisioned to GCE. This information contains information about throttling and quota rules for exposed services registered OAuth applications, and M2M data resource information. MSDP is also used to host services (for example telematics services) that directly access M2M DM to request M2M data reported from vehicles or to send M2M messages to vehicles, Services that make use of the M2M Data Management functionality may be hosted web applications making use of the Application Hosting functionality or may be services directly made available to external end-user services through the User Experience & Interaction functionality.

GCE: The Service Exposure functionality of GCE ensures that the SLAs and terms of services provisioned from MSDP are enforced on all exposed services. It also ensures that end-user consents are obtained before any M2M data can be accessed by a partner application by implementing the OAuth request flow. GCE exposes all the functionalities of the M2M Data Management component through the M2M Data Exposure and M2M Messaging Exposure services. Additionally GCE provisions information about created end-user consents as well as new OAuth applications to M2M DM in order for M2M DM to enforce the m2m data access control based on this information

M2M DM: The M2M DM component realizes the M2M Data Management functionality to store, transform, and provide access control for all data reported by vehicles as well as messages being sent from applications to vehicles. M2M DM provides interfaces for applications and services to access the data and messaging services either directly or through the services exposed through the GCE and the Service Exposure functionality M2M Messages that should be forwarded to vehicles are transformed into the correct format by M2M DM and forwarded to the Dispatcher component to be delivered to the vehicle.

Dispatcher: The Dispatcher provides a common interface for M2M devices (for example Telematics Control Units) to communicate with the different services enabled by the CVC using different communication protocols and message delivery mechanisms. The Dispatcher forwards data and messages to and from the M2M DM component from and to devices using either the MQTT protocol or an SMS Shoulder Tap mechanism.

2.3. Case study

One of the more common applications for connected vehicles are In-Car Navigation applications that help the driver navigate to the right destination and provides information about points of interests (POIs) along the planned route.

In this example, as shown in fig 4.,the In-Car Navigation application has been developed as a native application for the head unit operating system. The application accesses one of the API

services that has been developed and deployed on the platform to send and retrieve data.

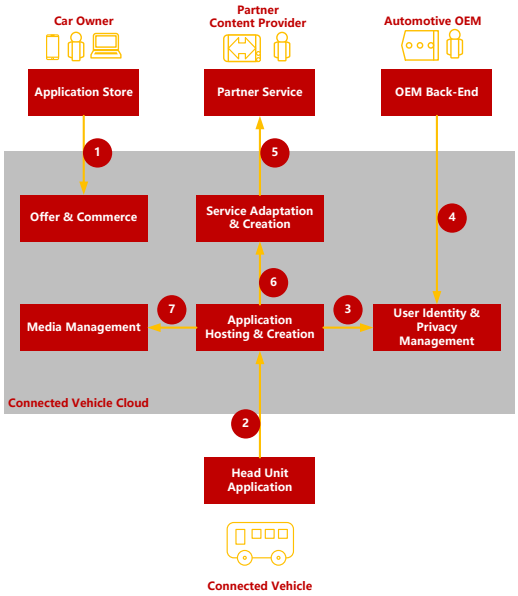

Figure 4. Overview of the CVC Functional Areas involved in Enabling an in-car Navigation Application Running in the Vehicle Head Unit.

This example describes how the CVC functionality is used to enable the In-Car Navigation application.

The following steps describe the main interactions between systems and functional components:

- The car owner uses the CVC Application Store to discover and purchase the In-Car Navigation Application. After the application is installed in the head unit of the car, it is available for the driver to use.
- When car driver uses the In-Car Navigation application, the application connects to the application back-end to download additional content. The application back-end is hosted in the CVC application hosting environment and exposes application features through REST APIs that are accessed by the application client in the head unit.
- The back-end application uses the CVC User Profile APIs to ensure that the user is authorized to use the application and retrieve the user profile.
- The automotive OEM integrates with CVC to provide user profile information from a central CRM database as well as retrieve information about user application usage from CVC.
- The automotive OEM integrates with Partner Service that provides additional content to navigation applications. To integrate external services with the hosted back-end applications the Advanced Composition can be used to create new APIs that access and retrieve content provided by partners.
- The back-end application uses the integration with a navigation information Content Provider Partner service to retrieve information about relevant POIs to display to the driver.
- The hosted back-end applications accesses the CVC Media Management functionality to retrieve the correct variants of image and video content to display in the application based on the information received from the partner service and head unit device capabilities.

3. Analysis of Security Problems Caused by CVC

While car networking brings convenience to people, safety issues also follow. Like other information systems, the security threats of the Vehicular Network also include denial of service, information leakage, tampering, replay attacks, counterfeit identities, and denial of operations. These attacks cannot be mitigated by means of traditional security techniques, as in the case of network attacks [5]. To achieve a higher level of security for sensitive messages, one can apply active security mechanisms [6] at the cost of losing a certain amount of efficiency.

3.1. Case of vulnerability in remote Control key system

Dutch electronics industry designer Tom Wimmenhove found a serious safety design flaw in the key systems of various Subaru cars, as shown in fig 5.. The manufacturer has not yet fixed the loophole and the loophole will lead to the hijacking of Subaru cars.

Figure 5. Case of vulnerability in remote Control key system.

By receiving a data packet sent by the key system (for example, the attacker only needs to capture the packet within the signal range after pressing any key of the key system), the attacker will be able to use the data packet. To guess the rolling code generated by the vehicle key system for the next time, he can then use this prediction code or direct replay to lock and unlock the vehicle. The use of this vulnerability is not difficult, attacking devices can be made using off-the-shelf electronic components, and do not require attackers with high-end programming skills. There are many hardware hackers in underground cybercriminals and things that can be done by designers in the electronics industry. These people can easily do the same. The car thief only needs to make a simple device that collects radio signals from the car key system, calculates the next scrolling code, and then sends a similar radio signal back to the target car after the target Subaru car owner leaves, and they can hijack the car.

3.2. An attack case of Tesla vehicle networking system

Tesla has built a WIFI Tesla Service into every Tesla car. Its password is a clear text stored in QtCarNetManager and will not be automatically connected in normal mode, as is shown in fig 6..

Tesla-Guest is a WIFI hot spot provided by Tesla 4S store and charging station. This information is stored in Tesla for automatic connection in the future. Researchers can create a fishing hotspot, Tesla, where users can redirect QtCarBrowser traffic to their domain names when they use CID to search for charging piles, which can be used for remote attacks.

In addition to WIFI technology, in cellular networks, if an attacker builds enough websites, phishing techniques or user errors can also be used to achieve the purpose of the intrusion. Because it is a browser-based attack, it can be done remotely without physical contact.

Figure 6. An attack case of Tesla vehicle networking system.

3.3. Solutions to security problems

- SIEM

  A Security Information and Event Management (SIEM) system is a system that enables real-time analysis of security-related information and event logs. It also provides automation of security-related tasks, and production of alarms and reports. SIEM system can be used to collect log and status information from many different subcomponents from the system, and it is based on a set of pre-defined rules take action when a security risk has been detected.

  It can be used to detect vehicles that quickly connect from different geographical locations that are far away from each other. This situation can indicate that a SIM card or vehicle identity has potentially been compromised, and the SIEM system can then instruct the Cloud Entry Point or other authentication systems to temporarily block access for this vehicle and raise an alarm for system administrators to investigate.

- Boundary Defenses & Secure Gateway

  On top of boundary defenses like encryption, CVC comes with an additional level of security based on a Security Incident and Event Monitoring (SIEM) system that is used to detect suspicious communication patterns and anomalies, sometimes also referred to as an Anomaly Detection system, as shown in fig 7..

  Anomaly detection systems help to protect against malicious attempts to hack the vehicles. Events outside of the normal pattern will be detected and the reputation level of the device will change. CVC controls the policy for how a device is using services. For example, if the Anomaly detection system lowers reputation the CVC may enforce read access only.

  Additionally the CVC includes a Secure Gateway. An automotive OEM may want to let the Car Drivers or Vehicle Passengers browse the web using the connectivity of the CVC and the in-vehicle infotainment unit or let a user connect using a mobile device that connects through the vehicle access point. To protect both the end-users and the CVC system from harmful or malicious content or software the CVC can be integrated with Secure Web Gateway 3PP that filters the web traffic of the user and ensures that no unwanted content or malicious web sites are accessed.

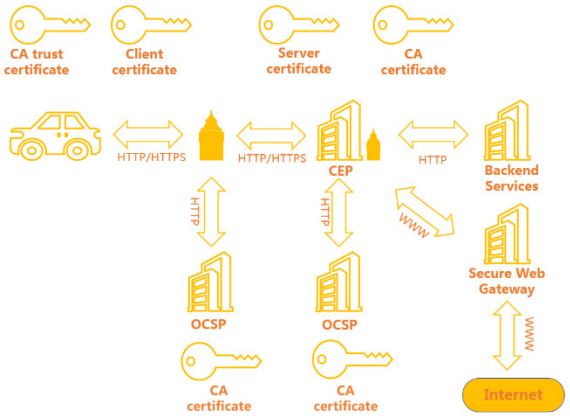

Figure 7. Certificates handling.

- Certificate Validation

  To ensure that all communication with the Connected Vehicle Cloud is secure, the automotive OEM will often have an existing Public Key Infrastructure (PKI). Public Key Infrastructure (PKI) and digital signature-based methods have been well explored in VANETs [7]. It requires that all vehicles authenticate with a pre-provisioned certificate for all communication with the cloud. This is the process of the mutual authentication. Mutual authentication ensures that both device and cloud (i.e. server side) can verify authenticity of each other. Access can be revoked or suspended through OCSP standards, this puts the OEM in control over which devices have access. All of this can ensure that all vehicles are securely authenticated when accessing the services of the cloud and that all communication is secure and encrypted [8].

  When the OEM uses a PKI, the CVC needs to implement the necessary components to validate the certificates of all vehicles and secure the communication between vehicle and cloud. This is typically achieved using Transport Layer Security (TLS) protocol to secure all communication and a CVC communication end-point (for example, a load balancer) that is capable of validating the vehicles' certificates and terminate the TLS traffic.

4. Conclusion

This paper exhibits that the Internet, Internet of Things and car networking become another major symbol in the future smart city. For improving the people's lives and increasing the convenience of travel, the car networking brings many security threats and seriously affects personal and information security. It is necessary to grasp the current development trend of the Internet of Everything, and while studying the development trend and core

technologies of the car networking. We must pay attention to the construction of safety protection under the environment of car networking and ensure the healthy and orderly development of car networking in the future.

Acknowledgment

This work is partially supported by the visiting foreign scholarship of 8th "Teacher Professional Development Project" fund by Shanghai Municipal Education Commission (No.2017 32), and Teaching construction project of Shanghai University of Engineering and Technology (No.P201701001).References

References

[1] Madhusudan Singh, Dhananjay Singh and Antonio Jara. "Secure cloud networks for connected & automated vehicles," 2015 International Conference on Connected Vehicles and Expo (ICCVE), pp.330 – 335, 2015.

[2] B. Hayes, Cloud computing, Commun. ACM 51(7) (July 2008) 9–11.

[3] Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C. Weigle, Security Challenges in Vehicular Cloud Computing, IEEE transactions on intelligent transportation systems, vol. 14, no. 1, march 2013

[4] Tao Zhang, Fellow, IEEE, Helder Antunes, and Siddhartha Aggarwal, Defending Connected Vehicles Against Malware: Challenges and a Solution Framework, IEEE internet of things journal, vol. 1, no. 1, February 2014.

[5] AlJahdali H, Albatli A, Garraghan P, Townend P, Lau L, Xu J. Multi-tenancy in cloud computing. In: Service Oriented System Engineering (SOSE). 2014 IEEE 8th international symposium on, Oxford; 2014. p. 344–51. doi: 10.1109/SOSE.2014. 50.

[6] G. Yan, S. Olariu, and M. C.Weigle, "Providing VANET security through active position detection," Comput. Commun., vol. 31, no. 12, pp. 2883–2897, Jul. 2008, Special Issue on Mobility Protocols for ITS/VANET.

[7] J. Sun, C. Zhang, Y. Zhang, and Y. M. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 9, pp. 1227–1239, Sep. 2010.

[8] S. Almulla, Y-Y Chon, "Cloud Computing Security management", 2nd International Conference On Engineering Systems Management and Its Applications, pp.1-7, March 2010.