Research on Multi Domain Based Access Control in Intelligent Connected Vehicle

Kaiyu Wang(✉), Nan Liu, Jiapeng Xiu, and Zhengqiu Yang

Software Engineering School, Beijing University of Posts and Telecommunications, No.10 Xitucheng Road, Haidian District, Beijing, China
{wangkaiyu, nanliu, xiujiapeng, zqyang}@bupt.edu.cn

Abstract. With the development of Intelligent Connected Vehicle (ICV), the information security problems it faces are becoming more and more important. Authentication and access control is an important part of ensuring the security of intelligent connected vehicles' information. In this paper, we have proposed a multi-domain based access control model (MDBA) based on the attribute-based access control model. The model proposes access control from the aspects of intelligent connected vehicles' multi-domain, thus ensuring the information security of intelligent connected vehicles.

Keywords: Intelligent connected vehicle · Access control · Multi domain · Information security

1 Introduction

1.1 ICV Background

In recent years, with the increasing number of private vehicles, the road carrying capacity of many cities have reached saturation. Traffic safety, travel efficiency, environmental protection and other issues have become increasingly prominent, and hinder the development of society. In this case, more and more public and vehicle manufacturers are turning their attention to intelligent connected vehicles. In order to solve the problems faced by current vehicles, various manufacturers are committed to developing intelligent vehicles with "pre-judgment" functions.

The intelligent connected vehicles contain many devices such as on-board sensors, controllers, actuators, etc., which combines modern communication and network technologies. This will enable intelligent information exchange and sharing between vehicles and X(vehicles, rode-side unit, people, clouds, etc.) through perception. Intelligent decision-making in the surrounding complex environment helps drivers to achieve coordinated control of the connected vehicle itself, and ultimately replaces people with "safe, efficient, comfortable, energy-saving" automated driving.

The information security of intelligent connected vehicles is getting more and more attention. The traditional information security problems in the Internet also appear in the vehicle. Information tampering and virus intrusion have been successfully applied in car attacks. For example, In January 2015, BMW's intelligent driving system Connected Drive had security vulnerabilities, and millions of vehicles were exposed to

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 401–407, 2019.
https://doi.org/10.1007/978-3-030-21373-2_31

hackers. In February 2015, the On-star vehicle system installed by General Motors had a loophole, and the vehicle could be controlled at will after hacking. In July 2015, the White Hat hacker demonstrated the invasion of the Unconnect in-vehicle system and controlled the vehicle via remote commands. In September 2016, the Keen Security Lab of Tencent conducted a remote attack on the Tesla Model S in parking and driving mode, successfully invading and controlling the vehicle. Due to the frequent occurrence of vehicle safety problems in recent years, the information security crisis of intelligent connected vehicles can not only cause losses to individuals and enterprises, but also even rise to national public security issues.

1.2 Security Problems

Due to its intelligent and connected features, ICV need to interact with other entity like other ICVs, manufacture cloud platform and public service platform. Potential threats will also enter the vehicles network. We group the security threats on ICV as cloud layer, telecommunication layer and vehicle layer. All these threats can potentially impact the safety and privacy of the ICV.

The security threats faced by ICV are shown in the following Fig. 1:

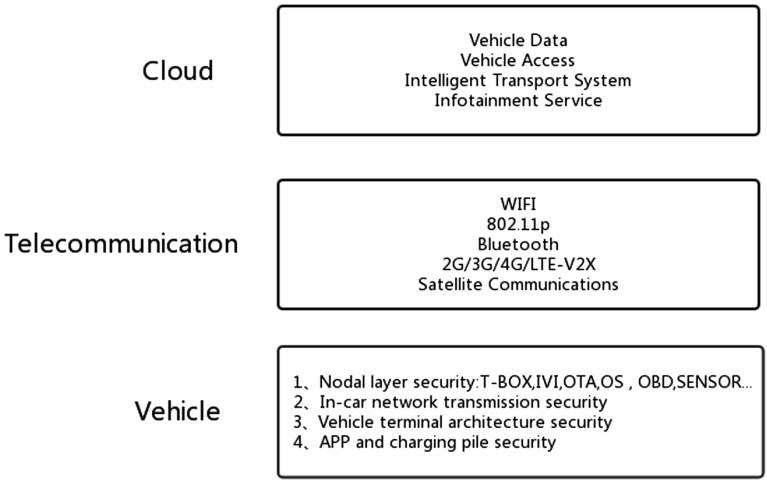

Fig. 1. The security threats faced by ICV

Vehicle layer's threats mainly involves vehicle system, car's CAN bus, Electronic Control Unit (ECU), On Board Diagnostic (OBD), T-Box and Infotainment (IVI) etc. Once crack the T-Box, hackers can send command through the CAN bus. The ECU connected to CAN bus will execute the command, which will impact the safety of the ICV.

Telecommunication layer's security threats mainly involves in telecommunication protocol itself. Once the telecommunication protocol cracked, the hackers can attempt a replay attack or Denial-of-Service (Dos) attack.

The cloud layer's security mainly includes the manufactures' platform and the public service platform. The cloud platform's threats Denial-of-Service, privacy data leak etc.

2 Related Work

Access control technology has been widely used to ensure system security, information confidentiality and integrity. Research on access control has become one of the research hotspots in computer security. With the continuous development of computing technology and network, the application of access control has also expanded to more fields, such as operating systems, databases, and wireless mobile networks, grid computing, cloud computing, and etc.

At present, the research on access control of intelligent connected vehicles mainly starts from two perspectives, one is access control based on identity authentication, and the other is access control through encryption mechanism.

The research on identity authentication has been widely used in traditional computer networks, these research results have laid a foundation for identity authentication in the intelligent connected vehicles environment. However, due to the complexity of the communication scenario of the intelligent connected vehicles and the low timeliness of information, thus increasing the difficulty of identity authentication. Sun etc. [1], proposed that the authentication method in the intelligent connected vehicles environment is constructed. The ID is used as the identity identifier of the vehicle node, which avoids the drawbacks caused by the certificate. Liu etc. [2] designed a dynamic trust model based on vehicle node messages and behaviors, providing strong real-time and high-accuracy trust evaluation, providing method support for actively sensing malicious nodes, and creatively considering future vehicles environments. It may run in the quantum communication environment and deduct the research direction of quantum threshold anonymous authentication and quantum trust evolution decision mechanism. Song etc. [3] proposed a lightweight uncertified and one round key agreement scheme without pairing, and further proved the security of the scheme in the random prediction model. This solution not only resists known attacks, but also has a small amount of computation. It is also an effective way to reduce vehicle-to-vehicle certification workloads, especially if there is no infrastructure available.

The research on encryption mechanism has been towards on attribute-based encryption. The key mechanism is that the holder of the subject encrypts the subject, and only the object that can be decrypted can access the subject data. This research idea is an access control strategy implemented by encrypting the attributes of the object by referring to the attribute-based access control idea in the traditional access control model. Huang etc. [4] proposed attribute-based encryption (ABE) to build an attribute-based security policy implementation framework. The framework treats various road conditions as attributes. These attributes are used as encryption keys to protect the transmitted data. At the same time, it is possible to naturally include a data access control policy on the transmitted data. Kang etc. [5] proposes an access control with an authentication scheme for propagating messages in VANET. In this scheme, the pseudonym is integrated with an identity-based signature (IBS), which not only verifies

the messages in the in-vehicle communication, but also protects the privacy of the message generator. Rao etc. [6] proposed a large cipher text size problem in the access control mechanism for vehicle communication based on attribute-based encryption (ABE). By using the access strategy in the Disjunction Paradigm (DNF), the length of the cipher text is linear in the number of conjunctions, not the number of attributes in the access policy. The communication overhead can be greatly reduced, and the scheme has the ability to resist collusion attacks under the damaged RSU.

3 Demand Analysis

3.1 Analysis of New Situation

The access control technology in ICV is quite different from the traditional cloud platform.

In the ICV background, the subject include other ICVs, roadside infrastructure (RSU), manufactures' cloud platform, public service cloud platform and people who can control the vehicle through the APP. We will pay attention to whether or not the subject have the access rights to the ICV, the access control process and granularity of Permissions.

Traditional access control models include autonomous access control (DAC) [7], mandatory access control (MAC) [8], and role-based access control (RBAC) [9, 10], which are static access control models. However, in the fast moving situation of the ICVs, the number of external subjects such diverse. Thus, this kind of dynamic authorization is quite different from the traditional access control models. The traditional access control model is difficult to adapt to such a large-scale and dynamic environment. The attribute-based access control (ABAC) [11] can better solve the access control problem in the intelligent connected vehicles environment, which is the main method of current research.

Therefore, we have proposed an access control strategy in a new situation, which can well solve our problems.

3.2 Multi-domain Based Access Control Model

In the intelligent connected vehicle environment, we have proposed a multi-domain based access control model. On the one hand, due to the intelligence of the intelligent connected vehicles and the characteristics of the network connection, the intelligent connected vehicles also have different functional components inside, and different functional components have different security levels. On the other hand, due to the complexity of the communication scenarios involved in the intelligent connected vehicle, the number of resources that the external subject accessing the vehicle and the vehicle object need to access is different from the level of access. Therefore, it is necessary for us to divide the domain of the resources inside the vehicle. At the same time, according to the behavior of the subject's access request, the subject is granted different level rights. Thus, a more granular access control is provided for the external subject to access the vehicle.

4 MDAC Model

Definition 1: subject
The subject refers to the entity that accesses the intelligent connected vehicles. Such as other connected vehicles, service cloud platforms, roadside communication infrastructure. Use S to represent the collection of subjects, S = {s1, s2 … sn}.

Definition 2: Object
The object that the subject is accessing. Use O to represent the resource object.
O = {o1, o2 … on}.

Definition 3: Domain
A unit that divides the internal resources of an object. Such as information domain, control domain, etc. D is used to represent the set of domains, D = {d1, d2 … dn}. The interdomain is divided into 4 parts shown in Fig. 2.

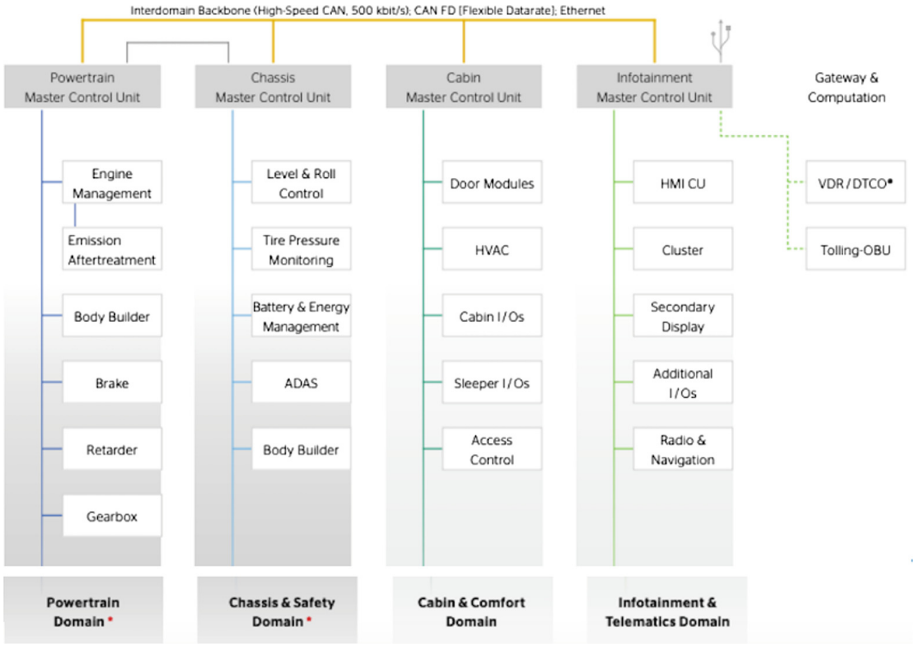

Fig. 2. Interdomain backbone

Definition 4: Permission
The specific access operation of the subject to the object resource. Such as creating, reading, copying, and etc. Use P to represent the set of permissions, P = {p1, p2 … pn}.

Definition 5: Action
The dynamic request operation of the subject's permission on the object resource, and the process of obtaining the dynamic permission. For example, the roadside infrastructure requests specific information of the vehicle, and the cloud service platform acquires real-time information of the vehicle. A is used to represent the set of requests, A = {a1, a2, … an}.
Definition 6: Risk
The threat index of the subject's access object's behavioral assessment, with a value of {–1, 1}. Where –1 means no risk and 1 means risky.

The authorization group of the MDAC model can be represented by a 7-tuple MDAC = {S, S-A, P, S-P, D, P-D, O}. Among them, S is subject, S-A is the subject's behavior, P is the permission set of the operation resource, S-P is the permission set possessed by the subject, D is the fine-grained access control domain, P-D is the domain that the permission can access the operation, O is the A resource object that can be manipulated.

In the MDAC model, when the external subject s(s∈S) requests access to the resource object o(o∈O) in the intelligent connected vehicles, the identity of the subject is first authenticated, and then combined with risk assessment, wherein the risk assessment integrated entity and the interaction history of the object, request context, to determine the risk value (Risk) of the request behavior. If Risk > 0, the behavior permission is not granted. If Risk < 0, the request is granted access to the domain D. The object's resources are divided into several domains, each of which is isolated from each other. Assign the permissions on the corresponding domain d(d∈D) according to the permissions required by the subject's behavior. Therefore, the principle of minimizing the privilege is achieved when the subject accesses the object, and the high-risk authorization and the privilege entrustment behavior can be controlled to a large extent. The access flow chart is shown below (Fig. 3).

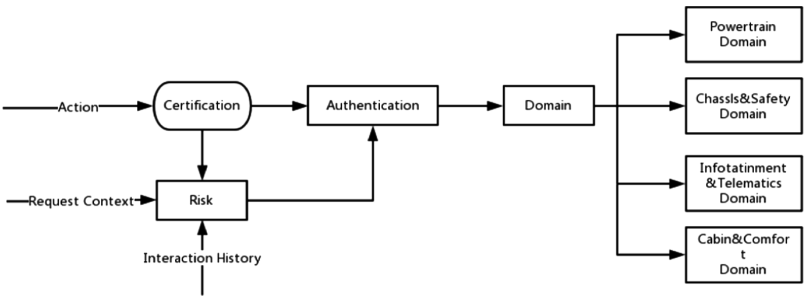

Fig. 3. The access flow chart.

5 Summary

By analyzing the development status of intelligent connected vehicles and the information security problems they face. This paper first analyzes the importance of information security, permission control and current permission control based on attributes, and deeply studies the current permission control technology, the mainstream permission control model and the characteristics of each model. A more efficient multi-domain based access control model (MDAC) is proposed through the abstraction of demand scenarios and the new attribute-based permission control model (ABAC). And the model is deeply explained from the aspects of the components, operation flow and working principle of the model, solving the problem of the authority control of the intelligent connected vehicle.

Acknowledgement. This work is supported by the subject (2017YFB0102502) of the National Key Research and Development Program of China.

References

1. Sun, J., Zhang, C., Zhang, Y., Fang, Y.: An identity-based security system for user privacy in vehicular Ad Hoc networks. IEEE Trans. Parallel Distrib. Syst. **21**(9), 1227–1239 (2010)
2. Liu, Y., Song, X., Xiao, Y.: Authentication mechanism and trust model for internet of vehicles paradigm. J. Beijing Univ. Posts Telecommun. **40**(3), 1–18 (2017)
3. Song, J., He, C., Zhang, L., Tang, S., Zhang, H.: Toward an RSU-unavailable lightweight certificateless key agreement scheme for VANETs. China Commun. **11**(9), 93–103 (2014)
4. Huang, D., Verma, M.: ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks. Ad Hoc Netw. **8**, 1526–1535 (2009)
5. Kang, Q., Liu, X., Yao, Y., Wang, Z., Li, Y.: Efficient authentication and access control of message dissemination over vehicular ad hoc network. Neurocomputing **181**, 132–138 (2016)
6. Rao, Y.S., Dutta, R.: Efficient attribute based access control mechanism for vehicular Ad Hoc network. In: Lopez, J., Huang, X., Sandhu, R. (eds.) NSS 2013. LNCS, vol. 7873, pp. 26–39. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38631-2_3
7. Vimercati, S.D.C.D.: Discretionary access control policies (DAC). Encycl. Crypt. Secur. 356–358 (2011)
8. Lawson, C., Wildy, H.: Mandatory access control (MAC) in virtual machines. Constr. Equipment (2014)
9. Ferraiolo, D.: Role-based access control (RBAC) (2004)
10. Ferraiolo, D., Cugini, J., Kuhn, D.R.: Role-based access control (RBAC): features and. motivations (1995)
11. Hu, V.C., Kuhn, D.R., Ferraiolo, D.F.: Attribute-based access control. Computer **48**(2), 85–88 (2015)