Poster: Access Control Needs in Smart Cars

Maanak Gupta and Ravi Sandhu
Institute for Cyber Security (ICS),
Center for Security and Privacy Enhanced Cloud Computing (C-SPECC),
Department of Computer Science, University of Texas at San Antonio
Email: gmaanakg@yahoo.com, ravi.sandhu@utsa.edu

***Abstract*—Smart Cars are the soul of intelligent transportation and smart cities of future world. As these entities get internet exposed and functionally complex they become vulnerable to cyber attacks, which in case of cars can shut down engine in the middle of road or freeze a car steering. This paper discusses security and privacy needs in smart cars and elaborates on access control requirements in dynamic and mobile ecosystem, which is often supported by cloud. We present an access control framework and also propose some cyber security focused research directions.**

I. Introduction

Internet of Things has proliferated itself to every domain from wearable devices, smart homes, manufacturing units, and power grids. Smart and Connected cars are imperative to envision smart cities and offer users convenient, safe and a royal driving experience. These cars are equipped with multitude of sensors, electronic control units (ECUs), softwares which range to almost 100 million lines of code and internet connectivity. This ecosystem allows interaction between vehicles (V2V), vehicles and infrastructure (V2I), vehicle to pedestrian (V2H) and ultimately between anything involved. The protocols to enable communications include dedicated short-range communications (DSRC), LTE, Bluetooth, and WiFi. Key distinguishing features of smart cars from other IoT domains include dynamic topology structures, random communication, time-sensitive, mobility, network scale, and non-uniform nodes distribution. Some applications envisioned by smart cars ecosystem include remote vehicle diagnostic and over the air updates (OTA), on-demand infotainment services, nearby parking notification, location based marketing, fleet management, and driving based insurance.

The amount of data generated by on-boards sensors in cars offer business opportunities, which are fully harnessed by boundless cloud services. The novel concept of vehicular cloud (VC) [1] was introduced where on-board resources (computation, storage, network etc.) are used to offer edge computing services to applications. VCs are more mobile, agile and autonomous since the nodes are random moving vehicles. The location and time-sensitive applications of smart cars require multiple cloud and edge computing infrastructures to enable real-time processing. Virtual objects [2] also also important to ensure communication between heterogenous physical objects and to resolve the issues of intermittent connectivity in dynamic and mobile smart car ecosystem.

An important concern in Smart cars is security and privacy. As these cars have broad attack surface (including TPMS, keyless entry, smartphone, engine ECU, OBD ports) and exposed external interfaces, attacks like false and unauthorized basic safety message (BSM) exchange, controlling ECU, stealing personal information, and spoofing sensors, can be easily orchestrated as discussed in several reports including [3], [4], [5]. An example scenario for a potential attack can include: finding a connected vehicle with vulnerable external interface, using external interface to gain access to in-vehicle network, and sending malicious spoofed message to critical systems to damage the car or issue commands.

Access Controls are important security mechanism to ensure authorized access to resources. Similar controls are also needed in smart cars to ensure trust among entities exchanging BSM messages and prevent unauthorized control of systems. We propose an extended access control oriented (E-ACO) [6] architecture which takes into consideration the access control requirements in smart cars ecosystem and helps to determine suitable access control models at different layers. Figure 1 shows our E-ACO architecture which has four layers: **Object Layer** has clustered objects (like cars, traffic lights) which have multiple individual objects as sensors and on-board in-vehicle applications. **Virtual Object Layer** resolves the issues of heterogeneity and connectivity by offering a cyber twin of all physical objects. In case of cars, where mobility and location cannot always ensure internet, it is needed to have virtual entity which keeps state information of physical object. **Cloud Services and Application Layer** provides cloud infrastructure for data processing and storage whereas application layer has the end-user applications which use data in cloud to provide services to user. It should be noted that entities within and across adjacent layers interact with each other, for example, a car can 'talk' to other cars and also with its virtual object. Further, users can issue commands to sensors inside car using smart phones or remote keys.

II. Access Control Framework

In this section we define our access control framework which reflects various interaction scenarios across E-ACO architecture layers and present some approaches to enforce access control in dynamic smart cars system. Most of these communications are supported by publish-subscribe protocols including MQTT, DDS or using HTTP and COAP. The framework, as shown in Figure 2, is categorised into three levels: Object level, Virtual Object level and Cloud Services level. Direct communication and indirect interactions (beyond

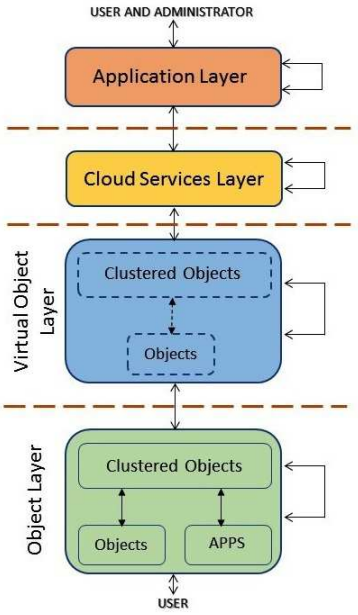

Fig. 1. Extended Access Control Oriented Architecture

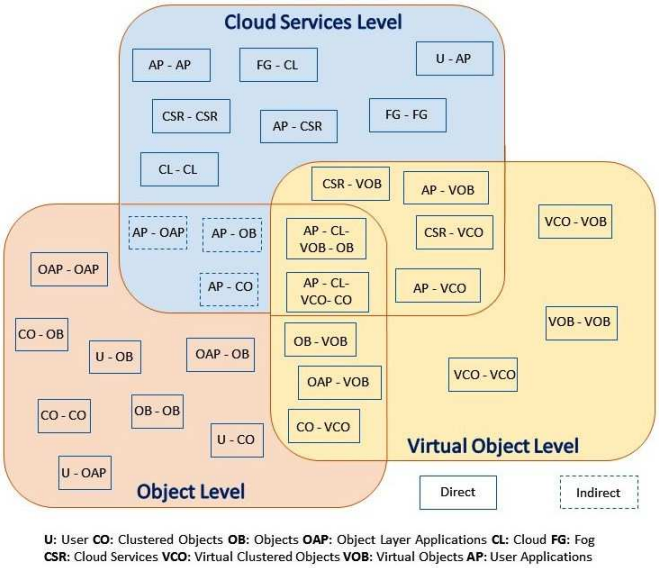

Fig. 2. Smart Cars Ecosystem Interaction Scenarios

adjacent layer communication) is specified using solid and dashed blocks respeectively in figure. Some interactions will exist in multiple layers because the entities involved like clustered object and its virtual entity (CO-VCO) belong to different layers. Object level category includes interaction between clustered objects (CO-CO), between individual objects (OB-OB), application on objects and sensors (OAP-OB) etc. At virtual object level, interaction will include between virtual objects (VCO-VCO, VOB-VOB) apart from indirect interaction with applications (AP-VOB) through cloud. Similarly, at cloud services level which involves single or multiple cloud instances, will require interaction between cloud (CL-CL), cloud and fog (CL-FG), applications and cloud services (AP-CL) etc. Access control models are needed in each category to authorize interactions and data exchange among entities.

An approach to establish trust among entities can be based on ownership, manufacturer or prior communication history. Since connected cars include random dynamic communication among moving entities on road, it is important to define the level of trust and what information to be exchanged among random or known entities. Attributes based access control will be required in such scenarios where attributes of cars like location, time, distance, road temperature will determine authorization decisions. Another approach may need multi-layered decision where type of operation will determine who can provide authorization. For example, a command to control the car will require authorization from car owner and police, whereas accessing sensor data may only need user approval.

III. Proposed Research Directions

It is well understood from above discussion that smart cars will require multi-layer access controls for both external and internal interface. Here we highlight some research directions:

- **External Interaction:** How to establish trust among entities is an important question to address here. Whether vehicles of same owner or at close location are more trusted?
- **Cross-Cloud Sharing:** Multi-cloud scenarios will be inevitable where entities in different clouds will communicate, which will require how to secure and trust cloud service providers. Can we exchange data among two clouds?
- **Data in Cloud:** Data lake in cloud will have user private information which needs to be protected and anonymization alone is not helping.

IV. Conclusion

In this paper, we discussed access control requirements in dynamic and mobile smart cars ecosystem. We presented brief summary about vehicular IoT ecosystem, its characteristic along with security and privacy requirements. We further discuss E-ACO architecture and discussed access control approaches along with some proposed research agenda.

Acknowledgment

This work is partially supported by NSF CREST Grant HRD-1736209, NSF grants CNS-1111925, CNS-1423481, CNS-1538418 and DoD ARL Grant W911NF-15-1-0518.

References

[1] M. Gerla and et al, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Proc. of WF-IoT*. IEEE, 2014, pp. 241–246.
[2] M. Nitti and et al, "The virtual object as a major element of the internet of things: a survey," *IEEE Comm. Surveys & Tutorials*, pp. 1228–1240, 2016.
[3] U. GAO, "Vehicle Cybersecurity ," *GAO-16-350*, 2016, March. [Online]. Available: https://www.gao.gov/assets/680/676064.pdf
[4] NHTSA, "NHTSA and Vehicle CyberSecurity," *NHTSA Report*, 2016.
[5] J. Barbaresso and et al, "USDOT's Intelligent Transportation Systems ITS Strategic Plan 2015- 2019," 2014.
[6] M. Gupta and R. Sandhu, "Authorization framework for secure cloud assisted connected cars and vehicular internet of things," in *Proc. of SACMAT'18 (To Appear)*. ACM, 2018, p. 12.