Adaptive Data Security for Autonomous Driving Vehicles

David Yu
Hillstone Networks Inc. Santa Clara California U.S.A.

Keywords: Autonomous Driving, ADAS, AD, Adaptive Data Security, Intelligent Connected Vehicle.

Abstract: With the rapid technological advancement of automotive EE architecture, modern autonomous driving (ADAS/AD) vehicles have become high performance computer system on the wheels. There is huge amount of data constantly being generated on an autonomous vehicle. These data can originate from different sources, including vehicle platform, ECUs, sensors, cockpit, connected vehicle networks (V2X). These data are significant heterogenous in nature and can have quite different processing and security requirements. A large amount of the data can be sensitive under certain circumstances, attackers can conduct malicious attacks from vehicle sensor jamming to user data breaches which can compromise driving safety and even cause national security risks. It is vital to ensure data security and control on autonomous vehicles and vehicle networks and protect data from cyberattacks.

This paper presents an adaptive data security solution for autonomous driving vehicles, focusing on ADAS/AD domain. The solution aims to provide the end-to-end data security solution during its entire lifecycle. It is based on Service Oriented Architecture (SOA) design methodology and expand legacy cyber security techniques on the autonomous vehicles. It also aims to provide flexibility for future upgrade on its data classifications and data security policies.

1 INTRODUCTION

Automotive E/E architecture (Andreas, 2021) has evolved from its original form that has large number of distributed, dedicated ECUs, each performing a specific task to today's fewer numbers, more centralized high-performance functional domain control units where much more complicated functionalities can be developed on these domain control units. Looking into the future, through V2X and vehicle cloud collaborations, more functions can be done on vehicles as well as in the cloud. This collaboration helps to further improve autonomous driving safety as well as user experiences.

The centralized Domain Control Unit (DCU) on modern autonomous vehicle is essentially a high-performance computer (HPC) system with powerful parallel computing capabilities using multiple CPUs and GPUs. Driven by modern Software Defined

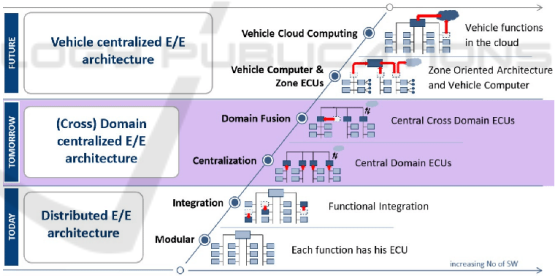

Figure 1: Example of E/E Architecture Evolution. Source: Bosch.

Vehicle (SDV), more complex deep learning and other AI algorithms for autonomous driving applications and services are developed on this computing system using modern software engineering design to support L3+ level automation. This makes the modern autonomous vehicle essentially "A High-Performance Computer on the Wheel".

Modern autonomous driving vehicle is built upon heterogeneous hardware platform, including multiple sensors, vehicle control units, AI hardware engines and other platform hardware. ADAS/AD functional software pipeline typically consists of perception,

Yu, D.
Adaptive Data Security for Autonomous Driving Vehicles.
DOI: 10.5220/0012010900003612
In *Proceedings of the 3rd International Symposium on Automation, Information and Computing (ISAIC 2022)*, pages 658-663
ISBN: 978-989-758-622-4; ISSN: 2975-9463

fusion, localization, planning and control, utilizing deep learning and other AI based algorithms. The software architecture typically based on Service Oriented Architecture (SOA) (Rumez, 2020) to provide layered, modular, scalable support for higher level ADAS/AD functions and applications development. This is also critical to develop large scale software engineering project, especially to support L3+ level automations.

The other significant characteristics of modern autonomous vehicles is that huge amount of data is constantly generated and collected from the vehicles, usually in the level of terabytes per hour. These data are generated from multiple sources, such as from vehicle powertrains, from ADAS/AD sensors, from deep learning algorithms, from applications as well as from the cockpit where driver related data are generated. These data are highly heterogeneous in nature, they can be structured or un-structured, they also have different processing and performance requirements. For example, the data collected by cameras, radar, lidar and other sensors are upload to cloud platforms where they are used for continuous deep learning model training and optimization; vehicle runtime data collected are used by OEMs in their vehicle network operational centers.

2 SECURITY RISKS ON AUTONUMOS DRIVING VEHICLE

The complexity of modern autonomous driving vehicles has increased dramatically in both hardware and software architectures, the amount of heterogeneous data generated, complexity of ADAS algorithms and applications, the data processing pipeline, V2X networking and vehicle cloud collaborations etc. The amount of software codes also increased dramatically, this complexity in software can introduce more vulnerabilities and security risks.

In recent years, hacking and malicious attacks toward autonomous vehicles and vehicle networks rose dramatically. In one report by Automotive Management Online, attacks on connected cars rose by a staggering 99% (lhpes, 2022). In another report by China Software Testing Centre, 60% of the vehicles have various security risks, from physical interfaces to web browsers that could allow hackers or malicious attacks to infiltrate and install malwares or viruses to steal sensitive data. Today information security on autonomous vehicles including network security, data security has become the must-have requirements for auto manufacturers and their suppliers imposed by government and industry regulations (Data Security Law, 2021) (Data Security WP, 2020) (am-online, 2020). There are several major industry standards and regulations focusing on automotive functional and information security. For example, ISO/SAE 21434, a drafted standard on engineering requirements for cybersecurity risk management. On the other hand, common automotive operating system software or middleware like ROS2, AUTOSAR have also added stronger security implementations in their newer releases (AUTOSAR,2020) (ROS2, 2019).

In summary, the complexity of hardware and software of modern autonomous vehicles introduce more security vulnerabilities, exposing more attacking points and larger attacking surface. Information and data security are critical for autonomous vehicles and vehicle networks to be widely adopted.

2.1 Data Security Risks

On average, a self-driving car can generate 100GB of data per second, with L4-L5 of autonomous level and with more cars are connected, that amount will go even higher. These data are generated and collected from within different vehicle domains including vehicle platform control, ADAS/AD, and cockpit domains. These data are valuable assets for automakers, service providers, and consumers.

Here we focus on the data generated and collected from ADAS/AD domain. For higher level of automation support, multiple cameras, radars, lidar, IMU, GNSS, HDMap and other sensors collect large amount of raw data constantly. These raw data are stored in the memory and feed into deep learning algorithms for object detection, traffic sign detection, lane detection and other AI based perception algorithms. During perception, fusion, localization and planning stages, intermediate results are produced and used as inputs for computations of next stage in the pipeline.

Hackers or attackers can infiltrate into these data processing stages and conduct malicious activities. This not only can potentially cause driving safety issues, but it can also impose state security issues as the external environmental data, geographic location data, landmark data as well as vehicle runtime data are constantly collected, processed, and uploaded to the cloud platform in real time, the data collected and uploaded could include sensitive information under certain circumstances. To be able to control and

protect ADAS/AD and other vehicle runtime data is critical on autonomous vehicles.

3 ADAPTIVE DATA SECURITY ON AUTONOMOUS VEHICLE

Data security on the autonomous vehicle has become a must have requirements for automobile manufacturers. While many enterprises level or cloud-based data security techniques and solutions are available, given the specific operational environment and limits in computing power and storage resources, data security solutions on an autonomous vehicle have their unique requirements.

3.1 Requirements

A data security solution on an autonomous vehicle should meet these requirements.

3.1.1 End-to-End Security

From the time data is generated and collected, for example, the raw data from the camera, lidar, radar and other sensors, or the intermittent results from the AI driven perception or fusion algorithms, throughout their lifecycle, these data are subjected to hacker attacks or other malicious infiltrations, data security should be able to track, control and secure every stage from the beginning to the end of data lifecycle including data collection, storage, consumption, uploading, transport etc. centering around the each stage in ADAS/AD data processing pipeline, applying different security mechanisms during each different phase.

3.1.2 Automotive Grade

Any data security solution on the autonomous vehicles needs to meet the automotive grade level of system and functional safety requirements. The data plane of the data security services is part of the overall ADAS/AD data processing pipeline, it also needs to meet the real time performance and reliability requirements. The data security service design and implementation usually need to be implemented inside the functional or middleware of ADAS/AD operating system software, but at the same time, it need to be decoupled from the main data processing pipeline to minimize any performance impacts as well as to provide flexible upgrade path. The data security modules also need to meet both the software engineering process and product functions that required by corresponding standards such as ISO 26262, ASPICE and ISO 21434 etc.

3.1.3 Lightweight

Even with today's high performance domain controller, usually hundreds of TOPS to support L3+ level of autonomous driving applications, computing resources are still relatively scarce on the vehicle. On the other hand, auto OEMs are often very cost sensitive in their mass production products, any additional add-on services that potentially have cost impact will face adoption challenges. Therefore, data security solution needs to be light-weighted, easy to deploy, minimizing the performance and cost impacts.

3.1.4 Flexible and Upgradable

Information security and data security for autonomous driving and intelligent connected vehicles are very active areas in the industry. A lot of government lead, industry driven standards, guidelines and regulations are in the making. They are constantly evolving, enhancing towards completions. Today's data security solutions on autonomous vehicles also need to be able to provide flexible design to migrate in sync with the latest development of related standards and regulations through OTA upgrade.

3.2 Adaptive Data Security on Autonomous Vehicles

This section discusses the overall design principles of the adaptive data security solution on the autonomous vehicle.

3.2.1 Adaptive Data Security Based on Service Oriented Architecture (SOA)

The overall design of data security solution on autonomous vehicles uses Service Oriented Architecture (SOA) principles. It mainly focuses on data security and control within ADAS/AD domain. It consists of two main parts: the management plane and the security service data plane. Security protection for each phase of data lifecycle is designed as software service module. These software service modules are installed on the main ADAS data flow pipeline as pluggable services and integrated with data processing pipeline using data interfaces APIs.

The management plane includes configuration and security policy modules. Initial configuration and security policies are loaded into the operating system software from manufactures. They can be upgraded via OTA later, through well-defined data interface and APIs, providing flexible configuration or security policy upgrades to each service module.

The data plane consists of several major service modules running in real time, including Data Collection, Data Classification, Data Storage, Data Upload etc. Each of these service modules interacts with the management plane at north-bound interface, it also has south-bound interfaces to interact with the run time data processing pipeline.

The overall components are shown in the following figure 2.

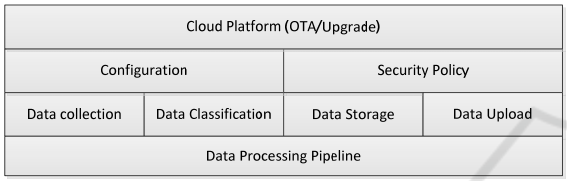

Figure 2: Adaptive Data Security Components

The adaptive nature of this data security solution for ADAS/AD domain refers to the following functions and capabilities:

- Adaptive SOA based Framework: Management plane and data plane are separated. Each real time data plane service module is essentially a light-weighted software module and can be installed into overall data processing pipeline. The north-south bound data interfaces are well defined APIs. These services can be executed in both mirroring mode and inline mode depending on requirements. The management plan modules can be updated using OTA. This makes overall framework elastic and dynamic.

- Adaptive data classification: Data can be tagged or labelled according to the classification rules defined in configuration policy. These rules can be statically configured and loaded during system initialization time. They can also be updated at later time through configuration policy module using OTA. This way the security control of data can be adaptive to different use cases and runtime environments.

- Adaptive data security control: Security control over the classified data can also be adaptive to the real runtime operational environment and circumstances. For example, security policies can be enforced based on geographic locations, coordinate positions, based on different data labels, perceptive environment, object detection results etc. Security actions can include those such as data masking, data upload disabling, data encryption for storage and transmission etc. These security criteria and actions, defined in security policies, can also be updated using OTA, providing effective control during runtime.

3.2.2 Data Collection

Autonomous vehicles collect data from driving environment through multiple sensors like camera, radar, lidar etc., simultaneous vehicle data are collected from IMU, location data are collected from GNSS or HDMap. Raw data are stored in the on-board memory and are feed into deep learning perception and other AI algorithms for fusion, localization, and planning. Intermediate data are the outputs of deep learning and other AI algorithms and are used as the inputs for the next stage in data processing pipeline. As raw or intermediate data are collected, data tags or labels, together with other context information are built as meta descriptors according to the configuration policies and set in meta data descriptor buffers to represent the priority, security, and other control characteristics for different classes of data.

3.2.3 Data Storage

Raw data, intermediate results data from algorithms and computing are stored in different on-board memory areas. Metadata descriptors are associated together with these classified data buffers throughout their lifecycles. Different classes of data in different storage have different security and control mechanisms according to the configuration policies, including access control, secure storage etc.

3.2.4 Data Classification

Data generated on the autonomous vehicles are heterogenous in nature. They can be structured or un-structured, each has its own different processing or performance requirement. To classify the data properly is vital for proper data security control throughout their lifecycles.

There can be different ways to classify data. It is important to adhere and follow data classification methodology and guidelines defined by the industry standards or government regulations.

Data classifications can have different levels, data security and control policies can apply to each of

these levels, providing better security and control granularities.

The following is an example of data classification with three levels.

Table 1: Data classification with three levels

Level 1	Level 2	Level 3
	vehicle ID	
Vehicle Data	vehicle	license, model, OEM
	ECU	
	camera	road, human, env
	lidar	coordinates
	radar	env measure
	IMU	
Perception Data	HDMap	coordinates
	GNSS	coordinates, trajectory
	V2X	
	object	object classification
	system	steering angle, speed, acc..
Decision Data	driver operation	
	vehicle state	
	vehicle perf	speed, acc, angel
Runtime Data	module runtime	GNSS, IMU, ADAS, OBU, cameras
	runtime logs	

Associated with each classified data category is a set of security and control attributes or requirements, covering each stage during the data lifecycle such as data collection, storage, usage, and transmission. The definitions of these requirements are usually drawn from industry standards or government regulations. For example, for collection, whether needs legal qualification or authorization; for storage, whether needs encryption, minimal storage timeout; for usage, whether needs access control or privileges; for transmission, whether needs to use private line, whether needs encryptions etc.

The following is an example of data control for each data service module.

Table 2: Data control example for each data services.

Collection	Storage	Usage	Transport
Legal Authorization	Storage Timeout	Access Privilege	Encryption Methods
User Consent	Encryption Methods	Auditing	Private Network
User Notification	Access Control	Monitoring	Public Network

3.2.5 Data Security Policy

Security policies in traditional firewall, IPS, IDS products usually consist of three types of elements: scope definition, condition matching and actions.

For example, a typical firewall policy usually has schema like:

```
   FROM entity-1 TO entity-2 IF criteria-matching
THEN action
```

Next generation firewall further enriches the security policies to incorporate more powerful and flexible elements such as applications, users or user groups, behaviours, and other contexts in each of these building blocks.

In data security solution design, traditional network or application security policies will be further expanded in these categories to incorporate those elements that are unique in autonomous driving circumstances.

- Scope: Besides legacy security scope entities like security zone, user, or applications etc., data that labelled with proper classifications can also be included in the scope according to data source types such as camera, radar, GPS, IMU etc. Scope can further include each level defined in data classifications or combinations of them.

- Criteria: Criteria matching can be expanded to include geographic location or coordinate position-based criteria or other normalized schema that can be used to describe the location, coordinate positions or areas that the vehicle is currently located in. It can also use results classifications from ADAS/AD algorithms such as object type, traffic sign, landmarks and other normalized entities defined in the autonomous driving environmental model.

- Action: Besides action in traditional network security policies such as DENY, PASS, LOG etc., data security actions can also include NO_COLLECT, NO_UPLOAD, DO_MASK, DO_ENCRYPT and others. These actions can be done for each level in data classification to provide better granularities of security control.

A simplified data security rule example can have following contents:

```
IF
   data_source == CAMERA_DATA &&
   data_class_prio == HIGH_PRIO &&
   data_class_sec == HIGH_SEC &&
   object_type == RESTRICTED_ZONE
THEN
   # Stop upload if in restricted zone
   data_upload = NO_UPLOAD
END

IF
   data_source == CAMERA_DATA &&
   data_class_prio == HIGH_PRIO &&
   data_class_sec == HIGH_SEC &&
   object_type == RESTRICTED_ZONE
THEN
```

```
    # Stop data upload in restricted
    # Zone and mask LV license plate
    data_upload = NO_UPLOAD
    data_sec_proc = DO_MASK
END
```

Data security policies need to be standardized. The rule schemas need to be defined in a normalized way. Security policies can be described using XML or YAML files in which more complex security rules and logical relationships can be defined.

In traditional network, security policies are installed on device or in the cloud and apply to each packet received on the wire. In case of autonomous vehicle computing environment, various computing tasks are usually running in a timer based executing loop controlled by OS kernel task scheduler, usually every 10ms in SOC. Data security services are also executed in a timer-based loop as separate tasks.

4 CONCLUSIONS

In this paper, we presented an adaptive data security framework on the autonomous driving vehicles. It aims to provide end to end data security controls throughout the lifecycle of the heterogeneous data on the autonomous vehicles. From the time they are generated, collected, stored, transmitted, and uploaded, adaptive to the different scenarios on how data are classified, prioritized, protected, and transmitted. It also aims to provide agility and flexibility in term of future upgrade through OTA so the existing design and implementation can be leveraged. It should be noted that there are future work needs to be done including the completion of each level of data classification, standardization and normalization security policy and control rules.

REFERENCES

Andreas Lock, “Trends of Future E/E-Architectures”, Accessed: Oct. 18, 2021. https://www.gsaglobal.org/wp-content/uploads/2019/05/Trends-of-Future-EE-Architectures.pdf

Rumez, Marcel & Grimm, Daniel & Kriesten, Reiner & Sax, Eric, “An Overview of Automotive Service-Oriented Architectures and Implications for Security Countermeasures”. IEEE Access. 8. 10.1109/ACCESS, 2020.

Data Security Law of the People's Republic of China http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml

Requirements on Security Management for Adaptive Platform https://www.autosar.org/fileadmin/user_upload/standards/adaptive/201/AUTOSAR_RS_SecurityManagement.pdf

ROS2 DDS-Security Integration https://design.ros2.org/articles/ros2_dds_security.html

https://www.lhpes.com/blog/why-is-cybersecurity-important-for-autonomous-vehicles

Data Security for Autonomous Driving – Whitepaper http://www.impcia.net/Uploads/report/2020-04-28/5ea7dba33e4e7.pdf

https://www.amonline.com/news/manufacturer/2020/06/04/cyberattacks-on-connected-cars-rise-by-99

Connected Vehicles – Whitepaper https://www.amonline.com/news/manufacturer/2020/06/04/cyberattacks-on-connected-cars-rise-by-99