Research Report on Security Issues faced by Autonomous Vehicles (AV)

S M RAGIB REZWAN
School of Science, Computing and Engineering Technologies
Swinburne University of Technology
Melbourne, VIC, Australia
103172423@student.swin.edu.au

***Abstract*---The increase in technology and innovation has brought about the rise in automation, leading to the creation of Autonomous Vehicle (AV) technology and its benefits. But even so, the technology is still at its initial stage and thus is plagued with various security issues and challenges. Thus, this report focuses on the security aspects of AV technologies. This is done by first explaining about AV in brief, before discussing about the security frameworks that are currently being utilized for it. After this, the report delves into the various issues that these frameworks address and resolve. This is then used to list out the issues that have yet to be fully resolved, before discussing about some new approaches that are being considered for them. In the end, the report is concluded with a brief summary, along with a suggestion towards the direction for future research on security for AV.**

***Keywords*---AV, SAEJ3016, GPS, Security by Design, Collaborative analysis, ISO26262, ISO PAS 21448, AVES, ISO21434, TR 68, S&CS, SCSD, DOS, ECU, LiDAR, Radar, CAN bus, Wi-Fi, HMI, V2X, MITM, DDOS, Block chain, MA-AIM, semi-decentralized security, CP-ABE**

I. INTRODUCTION

In the current world, there has been a huge boom in technology and innovation, leading to automation of various tasks that were previously performed by people. One such example is Autonomous Vehicle (AV), also known as "the self-driving car"

AV is basically a vehicle that can operate itself without any human intervention [1], through the use of driver assistance technologies [2]. Currently, following the definition provided by SAE's (Society of Automotive Engineers) J3016 standard [3, 4] there are 6 types of it depending on the level of autonomy that is has (see Fig. 1). But in this report, only those at and beyond level 3 (i.e. Conditional automation), will be considered as AV as in those cases, the majority of the control (i.e. Steering, surrounding monitoring, etc.) is performed by the system, rather than a human.

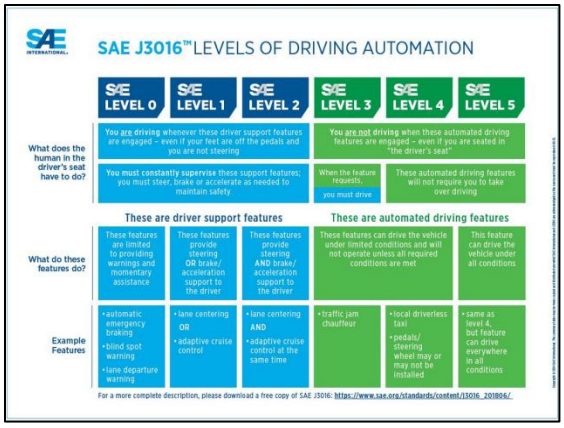

Fig.1. Autonomous vehicle: Levels of driving automation [3]

Note: Several attempts had been made to convert the pictures into SVG format. But it kept displaying the pictures as blobs of colors which couldn't be read. Thus, it had been decided to keep them as PNG.

Although AV technology brings various benefits to the table (i.e. reduced chances of accidents due to human error like distracted driver, increase in convenience and efficiency in transport of goods and people, etc.), it is still an emerging technology with various safety and security challenges (i.e. faulty GPS system in AV, hacking of on-board computer in AV, etc. causing disastrous accidents). This, in turn has led to various research articles focusing on that matter.

Hence, in this report, those articles will be summarized and organized in the following sections:

a) Section II will focus the security frameworks and protocols that have been developed for AV,

b) Section III will focus on the problems these frameworks attempt to resolve and their way of resolution,

c) Section IV will focus on the issues that remain unresolved,

d) Section V will focus on the new approaches that are being considered for AV,

e) Section VI will conclude the report with overall findings and future thoughts.

II. SECURITY FRAMEWORKS AND PROTOCOLS

Considering the dangers of out-of-control vehicles on the road (along with the current increase in devices being hacked), it's not too surprising to see the numerous security frameworks (based on various Security Standards) that has been designed to protect AV. Amongst them, the most prominent ones include:

A. Security by Design Framework:

This is the approach used in hardware and software development where the vulnerabilities of a system is removed with the help of testing, authentication setup, etc. and ensures that security is built into the product from the start [5]. In the case of AV, this is done by modeling it as a socio-technical system (systems that incorporate human and technology [6]) and ensuring that its basic areas of operation (i.e. sensing of its environment, communication between it and service workshops or manufacturer, decisions made by it in updating of routes or braking of vehicle, etc.) are not hampered by any external influence [7]. This is done by dividing the system in the AV into Core (physical enclosure of AV), AV Gateway (interfaces that connect AV and external work) and infrastructure layers (infrastructure and backend modules that are trusted and connected to AV), as seen in Fig. 2, and setting up protection feature for each. Furthermore, it had also been developed keeping ISO26262, ISO PAS 21448 and SAEJ3061 safety standards in mind to ensure both safety and security for AV.

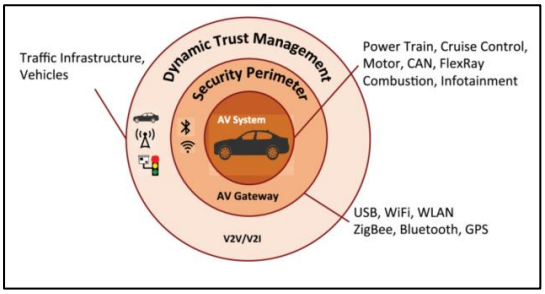

Fig. 2: Security by Design's layered architecture [7]

B. Collaborative Analysis Framework:

This is the approach where a given data is analyzed by multiple people (from different teams or companies) in order to develop an agreed upon analysis (and also report) [8]. In case of AV, the data being analyzed in depth (and on regular basis) is basically the artifacts produced in the S&S (safety and security integration) methodology (i.e. functions, structures, failures, attacks, safety and security counter measures) which links the security and safety aspects of AV together (as seen in Fig. 3) by using relational matrices. This ensures seamless linking between SAEJ3061 and ISO26262, ensuring that all aspects of safety and security of AV are considered (i.e. protection against software failure, weather impact, malicious attacks, etc.) [9].

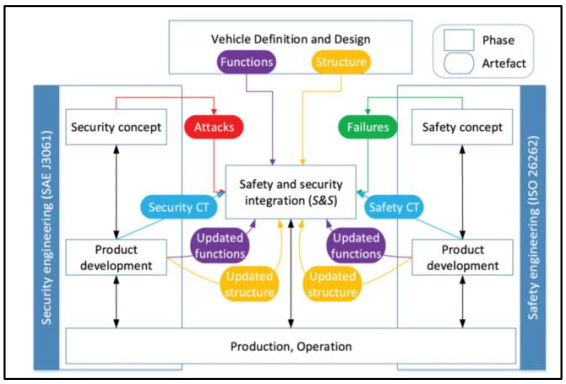

Fig. 3: Collaborative analysis framework [9]

Note: In fig. 3 CT is abbreviation for Countermeasure

C. AVES (Automated Vehicle Safety and Security Analysis) Framework:

This is basically a framework that has been developed solely focusing on the AV lifecycle (including its conception, development, production, operation, service and decommissioning stages, which can be seen in Fig. 4) and ensuring that they are both compliant with standards (like SAE J3061, ISO26262, ISO21434, TR 68) and also enable integrated Safety and Cyber Security analysis [10]. This ensures that security aspects are analyzed and satisfied at all stages before, during and after development of AV and hence reduces the chance of hazard and security threats.

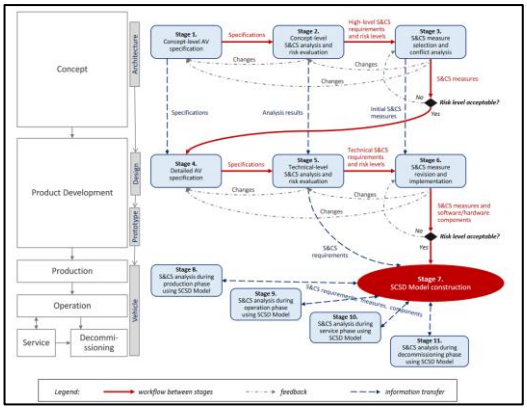

Fig. 4: Stages of AVES Framework [10]

Note: In fig.4 S&CS is abbreviation for Safety and Cyber Security, SCSD is abbreviation for Safety and Cyber Security Deployment model.

Note: Alongside these frameworks, there are also various standards that have been developed for AV security like SAE J3061, ISO26262, ISO21434, TR68, etc. But these haven't been separately elaborated here as most of the aforementioned frameworks already utilize them to various degrees.

III. PROBLEMS ADDRESSED BY FRAMEWORKS

Although these frameworks are quite similar, they tend to prioritize on different security problems and solve them in different ways:

A. Security by Design Framework:

a) It provides a Security perimeter to divide the AV into various security domains to differentiate between cyber-attacks and physical tampering and set up the controls in a holistic manner [7] (like AV Gateway level will focus on ensuring two factor authentication for remote control and not the core level). This isolated and simplified the threat environments, ensuring proper detection and analysis of threats against AV. This will prevent issues such as:

- Attackers forcing AV into collision with dynamic (other AV, pedestrians, etc.) or static object (road signs) by messing with the location and surrounding identification aspects [7],
- Attackers performing Denial of service (DOS) attack onto AV through its Electronic Controlled Units (ECU) [7], etc.

b) It provides trusted communication between devices internal and external to AV by establishing roots of trust (using Third party cryptographic key exchange and entity authentication) and using tamper resistant hardware [7]. This would prevent issues such as:

- Attackers providing false updates to the system (like changing the information in its GPS) [7],
- Attackers gaining control of the vehicle (like brake control, speed, etc.) through the remote control component and changing travel route or causing accidents [7], etc.

Note: Although it suggests various Threat analysis and testing methods that addresses more problems, it still leaves the final decision to the manufacturer's hands and doesn't enforce it.

B. Collaborative Analysis Framework:

a) It can identify and prevent various forms of hardware, software, communication system or road related failures (like preventing failure in Light Detection and Ranging (LiDAR) system by use of Radar, ensuring sensors work in all conditions through rigorous and regular testing, etc.), some of which have been listed below [9]:

- Platform hardware failure [9],
- Internal sensor (like LiDAR, GPS, Camera, etc.) failure [9],
- Software failure [9],
- Communication system failure [9],
- Failure in detection of other road users (like cyclist, pedestrian, vehicles, etc.) [9],
- Poor weather impact [9],
- Poor road condition (like improper marking, pavement condition, etc.) [9],
- Traffic signal failure (i.e. traffic signal not working properly) [9], etc.

b) It can identify and prevent attacks on AV (like spoofing attacks on sensors, physical attacks using brought-in devices, etc.) [9] which have been listed below:

- Dos, spoofing or physical type attacks on internal and externals sensors (and also actuators) [9],
- Dos, spoofing or physical type attacks on the ECU or inter-ECU communication [9],
- Dos, spoofing or physical type attacks on CAN bus (the in-vehicle controller area network), in communication between ECU and CAN bus, and in communication between CAN bus and on-board computer [9],
- Physical, Wi-Fi and Ethernet based attacks to on-board computer [9],
- Physical type attacks on the Human Machine Interface (HMI) [9],
- Physical type attacks on V2X (vehicle to everything) networks, its supporting infrastructure and on surrounding AVs [9], etc.

Note: It mainly focuses on identification of various issues and leaves the resolution of those issues to existing technologies (instead of enforcing any specific technology by itself).

C. AVES Framework:

It performs in-depth identification and analysis of all possible threats and hazards (including their risk levels, counter measures, etc.) even before the construction of AV. This not only ensures proper identification of any threats towards the AV system, but also ensures the selection and integration of appropriate counter measures (in terms of cost, coverage, least conflict with other devices, etc.) in the AV that will be developed.

Note: It uses a feedback loop between the development phases. So, if proper safety and security measure haven't been satisfied in any later stages, the development will be rolled back to previous stage to perform the identify modifications (even to the very initial stage of the AV design).

IV. ISSUES STILL UNRESOLVED

Although the aforementioned frameworks cover almost all of the areas of concerns regarding security aspect for AV, they mostly focus on identification of issues and leave their resolution to existing technologies.

But, even when they are utilized in conjunction with existing technologies, if the current technologies can't fully resolve those issues, then the problem still remains. This can be seen in the following cases:

a) In-vehicle security still being easily compromised through remote access, allowing malicious actors to randomly change vehicle direction, limit speed, etc. [11],

b) V2X communication being manipulated to perform Man-in-the-middle (MITM) or distributed-denial-of-service (DDOS) type attacks to AV [12],

c) Security model should be robust but lightweight and thus there is trade-off between security and power consumption of device [13],

d) Whilst driving, AV needs to be able to tackle a constantly changing risk environment in real time [13, 14],

e) Lack of a Unified Testing Standard to test all AV, instead of leaving it to choice of manufacturer [13],

f) Lack of proper Block chain (or equivalent) technologies that can support data transaction validation and management for large amount of devices whilst being computationally efficient [13, 14], etc.

V. NEW APPROACHES

Since existing technologies can't fully overcome the previous mentioned issues, the following approaches are also being considered:

a) Using an efficient Block Chain model to manage connectivity between AVs by providing better reduction in energy consumption (by 40.16%) through the optimization of transactions via distributed clustering (reducing number of transactions needed to share block chain data by 82.06%). This avoids the tradeoff between security and power in AV [15],

b) Leveraging of Block chain and smart contract technologies (alongside Vehicle-to-vehicle and vehicle-to-intersection communication) to create a multi-agent Autonomous Intersection Management system (MA-AIM) to securely manage vehicles crossing through intersections in real time and prevent collisions (by cryptographically securing AV data, use

of smart contract for non-repudiation of message exchanged amongst various AVs on the road, smart devices on the road, etc.) [16],

c) Using a Semi-decentralized Security framework, based on Ciphertext-policy Attribute-based encryption (CP-ABE) , which focuses on securing the communication between in-vehicle network to the external connected devices (i.e. connection between vehicles, Base stations, intelligent transport systems, and other external devices) without relying on any third party access policies. This ensures that the communication between the devices in the AV are not impacted by any external influences (i.e. from malicious actors) and also to reduce the reliance on third parties for AV security [17].

VI. CONCLUSION

Overall, the AV technology (especially for those including and beyond level 3 in terms of automation) is quite beneficial in reducing accidents due to human error, whilst providing convenience in transport of materials and people. But**,** through this report, it can be seen that the technology is still not fully ready in terms of security aspect as its current security frameworks (i.e. Security by design, Collaborative analysis, AVES), alongside the new emerging approaches (i.e. efficient block-chain technology, MA-AIM, Semi-decentralized security framework) are not adequate to resolve all of its issues.

Furthermore, there is also a lack of a unified global framework that can be used to enforce the organizations to ensure proper integration of all security features into AV. Hence, it will be better to further continue the research and development in AV technology's security aspects, so as to resolve all of these issues and fully embrace the benefits brought about by AV.

REFERENCES

[1] TWI Global, “What is an Autonomous Vehicle?,” *Twi-global.com*, 2019. https://www.twi-global.com/technical-knowledge/faqs/what-is-an-autonomous-vehicle (accessed Jun. 05, 2023).

[2] R. Cole, “Autonomous vehicle | Definition, History, & Facts | Britannica,” *www.britannica.com*, May 04, 2023. https://www.britannica.com/technology/autonomous-vehicle (accessed Jun. 05, 2023).

[3] SAE International, “SAE J3016 automated-driving graphic,” *sae.org*, 2019. https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic (accessed Jun. 05, 2023).

[4] SAE, “J3016C: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International,” *www.sae.org*, Apr. 30, 2021. https://www.sae.org/standards/content/j3016_202104/ (accessed Jun. 05, 2023).

[5] I. Wigmore, “What is security by design? - Definition from WhatIs.com,” *WhatIs.com*, Jul. 2015. https://www.techtarget.com/whatis/definition/security-by-design (accessed Jun. 05, 2023).

[6] SEBoK, “Sociotechnical System (glossary) - SEBoK,” *sebokwiki.org*, May 31, 2023. https://sebokwiki.org/wiki/Sociotechnical_System_(glossary) (accessed Jun. 05, 2023).

[7] A. Chattopadhyay, K. -Y. Lam and Y. Tavva, "Autonomous Vehicle: Security by Design," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 11, pp. 7015-7029, Nov. 2021, doi: 10.1109/TITS.2020.3000797.

[8] J. Daugherty, “Why Today’s Companies Need Collaborative Data Analysis | Mode,” *mode.com*, Dec. 15, 2022. https://mode.com/blog/collaborative-data-analytics/ (accessed Jun. 05, 2023).

[9] J. Cui, G. Sabaliauskaite, L. S. Liew, F. Zhou and B. Zhang, "Collaborative Analysis Framework of Safety and Security for Autonomous Vehicles," in *IEEE Access*, vol. 7, pp. 148672-148683, 2019, doi: 10.1109/ACCESS.2019.2946632.

[10] G. Sabaliauskaite, L. S. Liew, and F. Zhou, “AVES – Automated Vehicle Safety and Security Analysis Framework,” *ACM Computer Science in Cars Symposium*, Oct. 2019, doi: 10.1145/3359999.3360494.

[11] S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank and T. Engel, "A Car Hacking Experiment: When Connectivity Meets Vulnerability," *2015 IEEE Globecom Workshops (GC Wkshps)*, San Diego, CA, USA, 2015, pp. 1-6, doi: 10.1109/GLOCOMW.2015.7413993.

[12] V. T. Kilari, S. Misra and G. Xue, "Revocable anonymity based authentication for vehicle to grid (V2G) communications," *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Sydney, NSW, Australia, 2016, pp. 351-356, doi: 10.1109/SmartGridComm.2016.7778786.

[13] X. Sun, F. R. Yu and P. Zhang, "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 6240-6259, July 2022, doi: 10.1109/TITS.2021.3085297.

[14] A. Nanda, D. Puthal, J. J. P. C. Rodrigues and S. A. Kozlov, "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions," in *IEEE Wireless Communications*, vol. 26, no. 4, pp. 60-65, August 2019, doi: 10.1109/MWC.2019.1800503.

[15] V. Sharma, "An Energy-Efficient Transaction Model for the Blockchain-Enabled Internet of Vehicles (IoV)," in *IEEE Communications Letters*, vol. 23, no. 2, pp. 246-249, Feb. 2019, doi: 10.1109/LCOMM.2018.2883629.

[16] A. Buzachis, A. Celesti, A. Galletta, M. Fazio and M. Villari, "A Secure and Dependable Multi-Agent Autonomous Intersection Management (MA-AIM) System Leveraging Blockchain Facilities," *2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion)*, Zurich, Switzerland, 2018, pp. 226-231, doi: 10.1109/UCC-Companion.2018.00060.

[17] I. E. Carvajal-Roca and J. Wang, "A semi-decentralized security framework for Connected and Autonomous Vehicles," *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, Norman, OK, USA, 2021, pp. 1-6, doi: 10.1109/VTC2021-Fall52928.2021.9625336.