Human Factors in Design, Engineering, and Computing, Vol. 159, 2024, 287–293
https://doi.org/10.54941/ahfe1005593

Threat Analysis for Autonomous Vehicle Systems

Markus Sihvonen and Reijo Savola

University of Jyväskylä, Jyväskylä, Finland

ABSTRACT

Connected Automated Vehicles (CAVs) have significant role for enhancing logistics operations by providing improved efficiency, cost savings, traffic safety and to diminish environmental foot print. These are all major features of a competitive logistic operations of a modern company that seeks business advantage via its logistic operations. Already multiple types of CAVs are supporting logistic operations in warehouses, mines and generally in restricted areas in factory type environments. Reliability and safety of automated vehicle systems (AVS) can be realized in restricted environment for CAVs that operate on predetermined fixed routes relatively easy since these restricted environments have usually dedicated communication network that is not open to the Internet. This is not the case when CAVs start operating on public roads, in air space or at sea. There are already pilots in place that are using level 5 CAVs for delivering packages for a first/last mile logistic service on public roads and to provide taxi services for public with in a city. These CAVs require full support from AVS and they rely fully on public communication infrastructure to provide safe and secure services. Vehicles that require AVS services are in all practical means computers with full of multiple sensors and software that can and must utilize variable communication solutions in order to function as intended. Therefore, this paper's research problem and focus is to analyse potential threats scenarios of a CAV and to find vulnerabilities of an AVS. The problem is analysed via general AVS use case and focus is on level 5 fully autonomous system when a vehicle can perform all driving tasks under all conditions without human intervention. Some of the very same vulnerabilities already exists today even for level 2 vehicles that have advanced driver assistance system (ADAS) since they regularly use public communication infrastructure to access service providers data platform. The vulnerability analysis mainly focuses on vehicle to everything communication cases, vehicle to vehicle communication cases and analyses potential risks for intra-vehicle operations if cyber security protection fails. This will provide better understanding for logistic operators how to prevent AVS's complete, disastrous shut down by an external threat.

Keywords: Cyber-security, Connected automated vehicle, Threat path, Intelligent traffic system

INTRODUCTION

Autonomous vehicles provide a major advancement in transportation and mobility by reducing traffic accidents, improve mobility, and increased efficiency of transportation services. Global trend of urbanization is leading to increased traffic congestion and pollution in cities. Electric powered CAVs enable smart mobility solutions in public transportation optimizing and

© 2024. Published by AHFE Open Access. All rights reserved.

first/last mile logistics has major role when cities are transforming towards zero emission mobility solutions. This transition is partly enabled by very latest digital technological innovations in AI, IoT, and big data analytics. They are, together with fast and robust communication infrastructure, key enablers in development of smart mobility systems, autonomous vehicles, and smart infrastructure that enhance the efficiency and safety of urban transportation networks. Furthermore, they are main drivers to clean cities from many problems caused by overcrowded combustion engine-based traffic. Therefore, in many countries governments drive sustainable smart mobility system development by environmental legislations. Also, consumers are preferring convenient, cost-effective, and flexible mobility options and companies are looking for modern logistic solutions to enhance their competitive edge. The global smart mobility market was valued at approximately USD 38 billion in 2022 and is projected to reach over USD 70 billion by 2030, by growing at a CAGR (Compound Annual Growth Rate) of around 8-10% during the forecast period. Today, North America and Europe are leading in the adoption of smart mobility solutions due to their robust infrastructure, technological advancements, and supportive government policies.

VULNERABILITIES OF A CONNECTED AUTOMATED VEHICLE

A state-of-the-art CAV can have over 100 million lines of code in its operating system that controls autonomous driving and more than 70 ECUs (Electronic Control Unit) (Charette, 2009) (Glancy, 2012) (Klinedinst and King, 2016). Windows Vista operating system had 40 million lines of code and 905 known vulnerabilities according by the National Vulnerability Database (NVD) at 2017. This weakness of Vista was attacked by the widescale WannaCry and NotPeyta ransomware that year of 2017 (Perlroth et al., 2017). The NVD is open data base for vulnerabilities reported by researchers operated by the U.S. National Institute of Standards and Technology (NIST).

Because modern CAVs have vast amount of software and use the very latest digital technologies, they also have numerous security threats that need to be considered to ensure their safe and reliable operations. Primary security concerns associated with autonomous vehicles are cybersecurity threats, such as hacking, malicious software, integrity of communication and unauthorized access. CAVs are very much depended on communication systems and sensors that provide data for Artificial Intelligent (AI) solutions that actually controls CAV's operations. AI based system are particularly fully dependent on timely available reliable data. CAVs use usually machine learning (ML) algorithms for decision-making, which can be susceptible to adversarial attacks where manipulated data inputs cause the system to make incorrect decisions. A hacker could potentially gain control of a CAV's all vital systems and therefore cause accidents and steal sensitive data. A malicious software or virus can penetrate CAV's operating system and disrupt its functionality and safety features. The AI models used in CAVs can be stolen or tampered with, leading to unauthorized replication or altered behaviour. Since CAV is depended on much of its operations of timely reliable data

provided its sensor, physical tampering with the sensors could cause an CAV's ability to perceive its environment accurately. High-value CAV can also be potential target for theft and vandalism.

CYBER-ATTACK PATHS

This chapter discusses on relevant attack paths and types for CAVs. Cyberattacks cause major concerns about safety, connectivity, privacy, and performance risks of CAVs (Khan et al., 2024). They need to be fully addressed prior to people acceptance of fully autonomous level 5 CAVs on public roads. Successful cyberattacks on CAVs can be executed on six various avenues. They are 1) attack on CAV's communication framework, 2) break CAV's secure physical access, 3) human factors, 4) CAV penetration, 5) regulations and policy framework, and 6) trust in CAVs-industry and the public (Khan et al., 2021b). CAV's cyber security attacks can be classified into nine types based on their influence on target vehicle's behaviour and damages (Wang et al., 2020). They can be grouped in two categories due to a target of the cyber-attack: 1) attack on CAV's on board devices by transmitting malicious data to CAV's on board system, and 2) prevent vehicle's communication with other CAVs or infrastructure e.g., by jamming used communication frequencies (Parkinson et al., 2017). Because CAVs usually utilize low-latency communication channels for transferring remote-control commands and monitoring information, the connectivity risks are similar to the risks for the Internet and wireless networks in general. Therefore, very common risks are vulnerabilities related to availability of an available communication network for CAVs, which is in main focus of this paper.

A typical and relatively easy cyber-attack is denial of remote control. This is done by jamming frequencies that CAV uses for communication or to impair the latency of used communication channel. In general, CAVs should use communication technologies that can provide guaranteed quality of service (QoS) level and have capability to deploy alternative communication channels when eventually need arises. A very good alternatives for a CAV's reliable communication technologies in cities and areas with good telecommunication infrastructure are 4G and 5G networks supported by satellite communication technologies. A CAV should have a capability to analyse the QoS of multiple communication channels at any given moment and utilise the best available channel or communication. However, attacker may be able to get target CAVs to use a particular network. Therefore, in some circumstances it could be feasible for a CAV to use two or more available communication channels simultaneously in all circumstances. A distributed denial of service attack can also target multiple CAVs or whole communication infrastructure that is supporting CAVs operations. This can be executed very efficiently e.g. by preventing handover signalling in 4G and 5G networks. Usually in handover from one base station to another, communication is required with the core network components. Absence of it probably disconnects the communication. A CAV's control messages can be forged by bogus remote operator or Man-In-The-Middle adversary. This can

be avoided by utilising security protocols and, e.g., VPN tunnelling. Since the weak links are endpoints in VPN tunnelling, security solutions for the end-points need to be addressed.

RELIABILITY OF DATA

A typical CAV has, in addition to communication devices, multiple onboard sensors. Numerous cameras provide 360-degree view of the CAV's present environment. They provide detailed information on objects around the vehicle for data analysis. LiDAR sensor is used to measure object's speed and position in three-dimensional space around a CAV. Radar sensor is used to determine objects' speed and position on greater distances that camera or lidar can detect. Global Positioning System (GPS) is today commonly used navigation system for CAVs.

Machine learning (ML) is key technology in developing autonomous driving systems and it's used to analyse all collected sensor data, particularly CAV's situational awareness data. The most challenging in autonomous driving classification of objects around vehicle (Feng et al., 2022). This is mainly done by camera and LiDAR sensor of which later technology has taken notable leap forward in recent years (Bilik, 2023). Still, in certain challenging cases a CAV may erroneously perceive e.g. traffic signs incorrect or a stop sign as a less consequential traffic sign, such as a speed limit indicator. Even when a CAV system is operating correctly, it is possible for a pedestrian to be misidentified as a stationary object. The most challenging for a CAV's on board system is to predict movements of traffic around the vehicle (Taminul et al., 2023).

These primary sensors and the system that analyses collected data fast and reliably is essential for a CAV to operate at all. If you remove just on a single sensor's data from the system, replace correct data with falsified data or just delay CAV's data analysis process in any way, the vehicle does not function safe and reliable way anymore. There are many types of potential cyber-attacks against CAV's sensor collection and analysis system: 1) Denial-of-Service (DoS); 2) black-hole; 3) replay; and 4) pseudospoofing (Changyin et al., 2023). In a DoS attack, a sensor's ability to deliver data for processing is simply prevented. CAV's sensor data is rerouted in black-hole attack to prevent data analysis by the system. When a reply cyber-attack is carried out, malicious data is delivered for analysis instead of real CAV's sensor data. In pseudospoofing attack, some of the data provided by CAV's sensors are manipulated.

When CAV's sensor systems are targeted by cyber attackers, the purpose is to prevent traffic flow and to cause logistics problems. This is achieved by sudden acceleration and deceleration a vehicle or selected vehicles in traffic flow. Similarly sudden and aggressive continuous lane changes cause problems in heavy traffic. An attacker can cause a greater damage when hundreds or thousands CAVs' share malicious sensor data (Changyin et al., 2023). Practically, a single malicious sensor or small piece of wrong data can cause numerous collisions and even loss of life in heavily congested traffic.

DISCUSSION

Determining a liability in the event of a CAV's security breach or accident because of cyber-attack is complex. The necessary legislation does not exist yet. A legal framework and liability mechanisms are needed before CAVs are in everyday use to address these issues. The main challenges are preventing criminal activities in both digital and physical domains in AVS, requires utilizing cybersecurity protocols and implementing the Cybersecurity Regulatory Framework (CRF) to ensure adequate cybersecurity measures in place to protect the system. The CRF aim would be to document the intelligent transport system's (ITS's) objectives, principles, and best practices to manage cybersecurity risks effectively and efficiently. The regulatory challenges are entangled with CAV's product liability, identity characteristics, real-time data flow, access constraints, ethical considerations governing CAV operation, travel behaviour, vehicle ownership, driver licensing, penalty regimes, ITS architecture, and the nature of vehicle-related crimes (Dukarski, 2021).

Current legal framework is good enough to address challenges caused by disruptive CAV technology. However, a product liability is not clear, especially in malfunctions caused by cyber-attack at CAV Levels 4 or 5 where on-vehicle computer is operating a vehicle (SAE-International, 2018). The responsibility for civil liability claims in such instances remains uncertain. Would liable party be the Original Equipment Manufacturer (OEM), the ITS/AVS service provider, or a consumer? (Ryan, 2020; Hussain et al., 2021).

Also, thorough data collection conducted by multiple sensors in a CAV, such as cameras, lasers, radars, and lidars, introduce right to privacy concerns for bystanders and nearby properties. A person can be recognized by monitoring its behaviour and actions, such as body movement data (Miller et al., 2020). Currently, the legal framework is not concerned for monitoring, analysing or sharing bystanders' data. There are many CAV's data-related issues that needs to solved such as the location, duration, access rights to the data. It is also unclear how consumer data is treated after the vehicle is sold (Khan et al., 2021a).

CONCLUSION

Today's CAV collect a vast amount of data about their passengers, load and surrounding environment. This collected data must be protected from unauthorized access to protect AVS operations and private data. The legislation of CAVs, ITS operations and data ownership should be brought to meet requirements of level 5 AVS operations.

Since CAVs communicate with each other, other road users and vehicles and smart infrastructure by using wireless networks and utilizing many wireless communication technologies, these communication channels are obvious attack paths and therefor particular attention should be given to them ensure reliable operations. Particularly regular Over-the-Air (OTA) updates for CAVs' operating system (OS), which are often executed to fix known bugs in the OS, need to executed in safe communication environment.

AVSs' operations are heavily depended on the accuracy of the data available. They must have adequate level of correctness, timeliness and uniformity. Correctness of data means that it is free from errors and accurately represents real-world values. Timeliness refers to that data is up-to-date, including dynamically changing data. It is important that the shared data among CAVs remain consistent, uniform, across AVS. Because of the importance of accurate data to the AVS, data in the system should have well-structured format and should comply to relevant standards. It should be ensured that the data is dependable and can be confidently used for decision-making by CAVs. Attack-path by weaponizing the data used by AVS must be prevented by the system design.

Security concerns surrounding autonomous vehicles are multi-faceted and require a comprehensive approach to address. Manufacturers, regulators, and other stakeholders must collaborate to develop robust security measures that protect against cyber threats, ensure data privacy, maintain software integrity, and safeguard physical assets. As the technology evolves, ongoing research and adaptation of security practices will be essential to keep pace with emerging threats and ensure the safe and reliable operation of autonomous vehicles.

The lack of standardized security protocols for autonomous vehicles makes it difficult to ensure consistent security practices across different manufacturers and models. Developing and enforcing industry-wide security standards is necessary for cohesive security measures.

REFERENCES

Bilik, I., 2023. Comparative analysis of radar and lidar technologies for automotive applications. IEEE Intell. Transp. Syst. Mag. 15 (1), 244–269. https://doi.org/10.1109/MITS.2022.3162886

Changyin Dong, Yujia Chen, Hao Wang, Leizhen Wang, Ye Li, Daiheng Ni, De Zhao, Xuedong Hua, Evaluating impact of remote-access cyber-attack on lane changes for connected automated vehicles, Digital Communications and Networks, 2023, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2023.06.004.

Charette, R. N., 2009. This car runs on code. IEEE Spectr. 46, 3.

Dukarski, J., 2021. Unsettled Legal Issues Facing Data in Autonomous, Connected, Electric, and Shared Vehicles. SAE Technical Paper.

Feng, D., Harakeh, A., Waslander, S. L., Dietmayer, K., 2022. A review and comparative study on probabilistic object detection in autonomous driving. IEEE Trans. Intell. Transp. Syst. 23 (8), 9961–9980. https://doi.org/10.1109/TITS.2021.3096854

Glancy, D. J., 2012. Privacy in autonomous vehicles. Santa Clara Law Rev. 52, 1171.

Hussain, Q., Alhajyaseen, W. K., Adnan, M., Almallah, M., Almukdad, A., Alqaradawi, M., 2021. Autonomous vehicles between anticipation and apprehension: investigations through safety and security perceptions. Transport Pol. 110, 440–451.

Khan S., Shiwakoti N., Stasinopoulos P., Chen Y., Warren M., The impact of perceived cyber-risks on automated vehicle acceptance: Insights from a survey of participants from the United States, the United Kingdom, New Zealand, and Australia, Transport

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., Matthew, W., 2021a. Dynamic assessment of regulation and policy framework in the cybersecurity of Connected and Autonomous Vehicles. In: In Australasian Transport Research Forum, ATRF 2021-Proceedings. https://australasiantransportresearchforum.org.au/wpcontent/uploads/2022/05/ATRF2021_Resubmission_124-1.pdf.

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., Matthew, W., 2021b. Dynamic assessment of regulation and policy framework in the cybersecurity of Connected and Autonomous Vehicles. In: In Australasian Transport Research Forum, ATRF 2021-Proceedings. https://australasiantransportresearchforum.org.au/wp-content/uploads/2022/05/AT RF2021_Resubmission_124-1.pdf.

Klinedinst, D., King, C., 2016. On board diagnostics: risks and vulnerabilities of the connected vehicle. Software Eng. Inst.-Carnegie Mellon Univ. 10.

Miller, M. R., Herrera, F., Jun, H., Landay, J. A., Bailenson, J. N., 2020. Personal identifiability of user tracking data during observation of 360-degree VR video. Sci. Rep. 10 (1), 1–10.

Perlroth, N., Scott, M., Frenkel, S., 2017. Cyberattack Hits Ukraine Then Spreads Internationally. The New York Times.

Parkinson S., Ward P., Wilson K., Miller J., Cyber threats facing autonomous and connected vehicles: Future challenges, IEEE Transactions on Intelligent Transportation Systems. 18 (11) (2017) 2898–2915.

Ryan, M., 2020. The future of transportation: ethical, legal. social and economic impacts of self-driving vehicles in the year 2025 26 (3), 1185–1208.

Khan S., Shiwakoti N., Stasinopoulos P., Chen Y., Warren M., The impact of perceived cyber-risks on automated vehicle acceptance: Insights from a survey of participants from the United States, the United Kingdom, New Zealand, and Australia, Transport Policy, Volume 152, 2024, Pages 87-101, ISSN 0967-070X, https://doi.org/10.1016/j.tranpol.2024.05.002.

Taminul Islam, Md. Alif Sheakh, Anjuman Naher Jui, Omar Sharif, Md Zobaer Hasan, A review of cyber attacks on sensors and perception systems in autonomous vehicle, Journal of Economy and Technology, Volume 1, 2023, Pages 242-258, ISSN 2949-9488, https://doi.org/10.1016/j.ject.2024.01.002.

Wang P., Wu X., He X., Modeling and analyzing cyberattack effects on connected automated vehicular platoons, Transportation Research Part C: Emerging Technologies. 115 (2020) 102625. doi: 10.1016/j.trc.2020.102625.