ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE CYBER DOMAIN

Issue 11/24 (November)

Securing the Future: Cybersecurity Challenges and Solutions in Autonomous Vehicles

INTRODUCTION

1. Autonomous vehicles (AVs) are vehicles that are capable of sensing their external environment and operating without human control or involvement. As such, a human driver is not needed on the vehicle, neither is a human passenger required to be present in the vehicle. The definition of AVs is itself wide-ranging, encompassing a range of modes of transport from cars, public transit and shuttles, to drones, aerial vehicles and maritime vessels.

2. AVs heavily rely on technology for their operations, with millions of codes involved in ensuring that they run essential functions such as navigation, object detection and collision avoidance. This heavy reliance on technology opens up a range of cybersecurity threats, from remote hacking and hijacking, to vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) attacks and system malfunctions. These threats in turn have severe impacts. For example, a cyberattack can hamper an AV's braking and acceleration functions, causing road accidents that lead to casualties or even loss of life. Hence, it is important to understand the cybersecurity threats that AVs face and to mitigate the risks of cyberattacks on AVs.

OVERVIEW OF AVS AND THEIR CYBERSECURITY THREATS

3. AVs encompass a wide range of modes of transport. These are some examples of AVs, categorised by the various modes of transport:

a. Cars. Tesla autopilot and full self-driving (FSD) models such as Model S and Model X.

b. Public transit and shuttles. The Robobus that shuttles passengers around Resorts World Sentosa in Singapore, launched in Jul 2024; the driverless shuttle bus service at Singapore's Nanyang Technological University (NTU), which is the world's first full size, autonomous electric bus, launched in Oct 2020; trials for AV buses to shuttle airside workers in Singapore's Changi Airport, starting in 3rd quarter of 2024; the driverless trains that ply many of Singapore's newer Mass Rapid Transit (MRT) lines, starting with the North East Line that was first opened in 2003.[1]

c. Drones and aerial vehicles. Amazon Prime Air, which is Amazon's package delivery service that utilises autonomous drones.

d. Maritime vessels. Rolls-Royce's Ship Intelligence which is being developed for autonomous cargo ships and semi-autonomous ferries.

4. AVs are particularly susceptible to cyber threats due to their reliance on interconnected systems, vast amounts of data and external networks for operation. Key attack vectors include:

a. High levels of connectivity (required for an AV's operations). AVs rely on a vast network of communication systems, known as vehicle-to-everything (V2X) communication. V2X communication encompasses V2V, V2I, vehicle-to-cloud (V2C), vehicle-to-network (V2N) and vehicle-to-pedestrian (V2P) connections. The interactions of these connections are illustrated in Figure 1, which shows how these interactions collectively allow an AV to operate smoothly. The large volumes of consistent data flows in the operations of AVs make their operations vulnerable to cyberattacks. Additionally, many AVs can be monitored and updated remotely, introducing many entry points for attackers who can gain control over vehicle systems.

[1] Today, 60% of Singapore's MRT network operates using driverless trains.

Figure 1: V2X communications that allow an AV to operate safely. (Source: Automotive Technology)

b. Complex software systems and third-party code dependencies. AVs require millions of lines of code to run essential functions like navigation, object detection and collision avoidance. The massive nature of their software architecture raises their vulnerabilities to bugs. Furthermore, the supply chain of AVs may also rely on third-party components and libraries which may not be as rigorously tested for bugs and security measures, making them a vulnerable vector for attack on the entire AV operating system.

c. Dependencies on cloud and edge computing. AVs use cloud services for navigation updates, data processing and software updates. If cloud security is compromised, it can lead to data theft, system manipulation and service disruption. Additionally, edge computing nodes can provide additional attack points for hackers to manipulate or inject data into AV systems if they are not securely managed.

5. AVs are also at risk of a plethora of cybersecurity risks. Examples of such cybersecurity-related risks include:

a. Remote hacking and hijacking. AVs are susceptible to remote hacking, allowing attackers to take control of the vehicle and manipulate the vehicle's steering, braking or acceleration. Consequently, it can cause crashes or lead to other hazardous situations, thereby risking the safety of passengers and other road users.

b. Misuse of Data. AVs collect vast amounts of data, including location, audio, video and user information. Malicious actors can target such data to engage in identity theft, track individuals or commit other cybercrimes, such as targeted attacks, surveillance and financial fraud.

c. Attacks on V2X. AVs use V2V and V2I to interact with other vehicles, traffic systems and road infrastructures. Cyberattacks on V2V and V2I systems can disrupt traffic flows, cause accidents or lead to system-wide failures in transportation networks. Furthermore, attacks on V2X can result in large-scale traffic chaos or result in the weaponisation of the AV network against critical infrastructure, leading to widespread disruptions.

d. Sensor system malfunctions. AVs rely on a plethora of real-time sensors, such as cameras, light detection and ranging (LiDAR), radar and global positioning systems (GPS), to understand their surroundings and operate. If these sensors are tampered with, such as with GPS spoofing, the vehicle's perception to its surroundings are compromised. Therefore, cyberattacks could lead to software malfunctions, causing vehicles to perform unpredictably. For example, software malfunctions can disable vehicle functions like navigation, collision avoidance or emergency braking, jeopardising the safety of occupants and other road users.

6. Cyberattacks on AVs can lead to wide-ranging consequences and impacts. Examples of such impacts include:

a. Economic impacts of AV disruptions. Cyberattacks on certain types of AVs have widespread economic impact, particularly with AVs involved in the public transport of people and goods. For instance, AV disruptions on mass commuter transport systems, like driverless subways, during morning rush hours on a weekday can lead to widespread commuting chaos, preventing people from getting to work or schools with subsequent impacts on their productivity and economic output. For industries dependent on just-in-time supply chains, AV disruptions can threaten the operational continuity of their operations, having adverse

impacts on subsequent stages down the supply chain and therefore more broadly, on economic activity.

b. Public trust in autonomous technology. If AVs were to be widely adopted, the public needs to be reassured of their safety and reliability. Cyber breaches threaten to erode public confidence in such technology, especially if such attacks are high profile like in the case of widespread traffic disruption or incidents leading to mass casualties. Therefore, cybersecurity measures are essential to maintain public trust in AV systems and prevent setbacks in technological progress.

Case Study: Uber Self-Driving Car Incident in 2018

An autonomous Uber vehicle struck and killed Elaine Herzberg, 49, a pedestrian in Tempe, Arizona, whilst operating in self-driving mode. The car's safety driver, Rafael Vasquez, had been streaming on her mobile device whilst sat on the driver's seat at the time of the accident. The incident was not classified as a cyberattack, with the US National Transportation Safety Board (NTSB) concluding that the accident was the result of human error, as Ms Vasquez had the ability to take control of the vehicle in the event of an emergency since she was sat at the driver's seat. Nonetheless, NTSB also found "inadequate safety risk assessment procedures" at Uber, since the vehicle's automatic systems failed to detect Ms Herzberg as an imminent collision danger.

At the point of the accident, confidence in AV technology was at an all-time high. However, the accident in Arizona dealt a huge blow to that confidence, with Uber forced to halt its testing programme for AVs. Rivals like Google's Waymo also had to be more cautious in their trials.

Therefore, the incident highlights the importance of robust and secure software for AVs given the fallout that can occur after any incidents. It also underscores how software vulnerabilities can lead to real-world harm if not properly addressed, with consequences on public confidence and trust in AV technology.

ENHANCING CYBERSECURITY FOR AVS

7. In light of the vulnerability of AVs to cybersecurity incidents, as well as the consequences of cyberattacks, it is paramount that the cybersecurity of AVs

is enhanced. Enhancing cybersecurity of AVs is more effective when a multi-stakeholder approach is adopted, involving standards and guidelines set by the government and international organisations, and adoption of defensive strategies and best practices by AV manufacturers.

8. The National Highway Traffic Safety Administration (NHTSA) of the US has released guidelines, which was updated in 2022, to enhance cybersecurity in AVs. Key aspects of the guidelines are:

a. Adopting a multi-layered approach to cybersecurity, that addresses both wireless and physical entry points to minimise vulnerabilities. This includes developing secure software architecture, intrusion detection systems and regular monitoring of cybersecurity threats.

b. Encouraging manufacturers to conduct robust risk assessments, so as to identify potential cybersecurity threats that can jeopardise safety. Thereafter, manufacturers can more effectively design protections that eliminate or mitigate such risks.

c. Requiring that manufacturers ensure sensor and communication integrity, so as to allow for accurate vehicle operation. This is important given the vulnerability of AV sensors and V2V communications, such as with GPS spoofing, LiDAR jamming and camera tampering.

d. Promoting information sharing and collaboration amongst AV manufacturers with entities such as the US Cybersecurity and Infrastructure Security Agency (CISA), so as to facilitate faster response to emerging threats across the industry. This builds on the US Department of Transportation's Automated Vehicles 4.0 report, which encourages AV manufacturers to share cyber threat intelligence and vulnerabilities with CISA as part of CISA's threat-sharing programmes. This therefore promotes a unified approach for protecting AV systems and infrastructure, enhancing industry-wide resilience and enabling timely responses to cybersecurity threats in AVs.

9. International organisations, such as the International Organization for Standardization (ISO), have themselves set international standards that guide

cybersecurity for AVs, such as ISO/SAE 21434. This is a comprehensive framework that guides the automotive industry to identify and mitigate cybersecurity risks in the lifecycle of a vehicle. Key aspects of ISO/SAE 21434 include:

a. Requiring manufacturers to engage in systematic threat analysis and risk assessments, so as to identify and evaluate cybersecurity threats and vulnerabilities. Therefore, manufacturers can prioritise high-risk areas and implement countermeasures to curb cybersecurity threats.

b. Promoting cybersecurity by design. This emphasises embedding cybersecurity measures from the earliest stages of a vehicle's life cycle, including in its conceptualisation, design and development. Hence, cybersecurity becomes integral to the AV's architecture and functions.

c. Ensuring supply chain security. This standard highlights the importance of securing the entire supply chain, including third-party suppliers and software providers. Manufacturers are therefore required to collaborate closely with their suppliers to ensure that each component meets cybersecurity requirements, therefore reducing risk exposure from external sources.

d. Securing updates and patching. In order to effectively address new vulnerabilities, the ISO/SAE 21434 mandates secure update mechanisms, such as over-the-air updates, so as to keep vehicle systems current. This includes validating updates to ensure that they do not introduce new vulnerabilities and securely delivering patches to protect against cyber threats.

Case Study: Singapore's Land Transport Authority (LTA)

Singapore LTA's revised Technical Reference (TR) 68 incorporates principles inspired by ISO/SAE 21434. It introduced new guidelines to promote cybersecurity principles to ensure the safety of AVs and keep pace with recent technology advancements. These enhanced cybersecurity requirements are based on principles such as security-by-design that ensures cybersecurity is considered even at early stages of an AV's development. Consequently, cybersecurity considerations are built into the design of AVs and they become more resilient to cybersecurity attacks.

10. Additionally, AV manufacturers themselves can adopt defensive strategies and best practices that enhance the cybersecurity of AVs and mitigate the impact of cyberattacks and breaches. These include:

a. Enhancing V2X security. V2X strategies seek to ensure the security of V2X interactions and communications, therefore safeguarding them against cyberattacks. This can be done through public key infrastructure (PKI), which ensures that V2X communications, such as those between AVs and infrastructure, are authenticated and encrypted. Therefore, it prevents man-in-the-middle attacks, where malicious actors can intercept and alter communication data. V2X security can also be promoted through the use of intrusion detection systems that are tailored for V2X data flows, which can flag unusual patterns of potential tampering in real time.

b. Sensor security and spoofing protection. By using multiple sensor types, such as LiDAR, radar and cameras, cross-verification is enabled, making it harder for attackers to spoof sensor data by introducing false signals. AV manufacturers should also work towards signal authentication and verification, where incoming sensor data is verified to detect spoofed signals. This can be done using machine learning-based algorithms that can flag anomalies or inconsistencies in data input.

c. Data encryption of sensitive data. Sensitive data that is stored on the AV or transmitted to external systems should be encrypted and protected against interception or unauthorised access. Additionally, AV manufacturers should limit and anonymise data collected by AVs, as this reduces privacy risks and the attractiveness of the data to attackers.

d. Implementing an incident response and recovery mechanism. As much as AV manufacturers seek to avoid cybersecurity breaches of AVs, contingency measures should still be put in place to respond to any cybersecurity incidents that might happen. Manufacturers should therefore design systems with fail-safe mechanisms and redundancies that ensure that the vehicle can continue to operate or safely shut down in case of a cyberattack. Such pre-defined response protocols enable rapid containment and recovery, helping to mitigate the effects of a cybersecurity breach.

Case Study: Cybersecurity Implementation at Waymo, Alphabet Group's AV Division

Waymo released a report in 2021 that included points that the Alphabet Group was adopting to enhance cybersecurity measures in its AV sector. The report emphasises Waymo's adoption of a six-pronged approach, as illustrated in Figure 2, to deal with cybersecurity threats to its AVs.

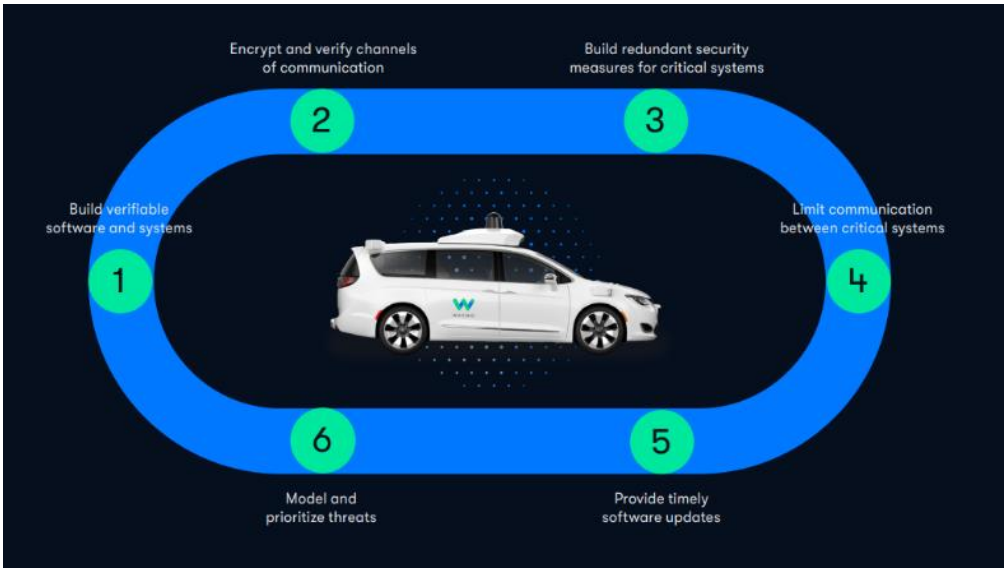

Figure 2: Waymo's six-pronged approach to enhancing cybersecurity of its AVs. (Source: Waymo Safety Report)

This approach to cybersecurity allows multiple layers of security that can more thoroughly protect Waymo's autonomous driving systems from unauthorised communications, with a keen focus on safety-critical functions like steering and braking. Collectively, they prevent anyone with limited physical access to Waymo's AVs from impairing or altering their security. If Waymo were to detect malicious activity, such as attempts to impair their vehicle's security, Waymo will trigger their company-wide incident response procedure, which involves impact assessment, containment, recovery and remediation.

This comprehensive cybersecurity management framework not only allows Waymo to prevent cyberattacks, but to also minimise the damage and impacts should its AVs nonetheless encounter a cyberattack.

11. Yet, there are ethical considerations that must be accounted for when enhancing the cybersecurity of AVs. Notably, safeguards must be put in place to ensure privacy protection, since AVs collect sensitive data including location and personal details. Additionally, AV manufacturers should be transparent in their

operations, including adopting clear communication about data collection and response protocols, as this fosters user trust. Furthermore, there must be a system of accountability that can determine responsibility for cybersecurity breaches and failures, especially if they concern shared data from multiple stakeholders. Failing which, AV manufacturers become at risk of legal challenges and liability issues should cybersecurity breaches occur.

CONCLUSION

12. In conclusion, the high levels of V2X connectivity and complex software systems make AVs a vulnerable target to cyberattacks by malicious actors. The impacts of cyberattacks on AVs in turn are wide-ranging.

13. Given the possibility of severe and multi-faceted disruptions that can occur when AVs are subjected to cyberattacks, it is of paramount importance that appropriate cybersecurity enhancement measures are put in place. These measures are more comprehensive when a multi-stakeholder approach is adopted, involving guidelines put forth by governments and international organisations, and defensive strategies and best practices adopted by AV manufacturers. Consequently, they foster an ecosystem that not only promotes higher levels of cybersecurity and safety for AVs, but also promotes greater public trust in AV technology. By extension, this further enables greater technological progress more generally.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • • •

REFERENCES

1. Singapore Launches Autonomous Shuttle Service, WeRide Robobus Becomes a New Attraction at Resorts World Sentosa – WeRide
https://www.weride.ai/posts/155

2. Resorts World Sentosa welcomes autonomous shuttle service to the island – TTG Asia
https://www.ttgasia.com/2024/07/08/autonomous-shuttle-service-becomes-latest-attraction-at-resorts-world-sentosa/

3. Self-driving bus for airport workers to be trialled at Changi Airport – Straits Times
https://www.straitstimes.com/singapore/transport/self-driving-bus-for-airport-workers-to-be-trialled-at-changi-airport

4. NTU Singapore and Volvo unveil world's first full size, autonomous electric bus – Nanyang Technological University
https://www.ntu.edu.sg/research/research-hub/ntu-singapore-and-volvo-unveil-world-s-first-full-size-autonomous-electric-bus

5. Alstom in Singapore – Alstom
https://www.alstom.com/alstom-singapore

6. Vehicle-to-Everything (V2X) Communication: Enhancing Road Safety and Traffic Management – Automotive Technology
https://www.automotive-technology.com/articles/vehicle-to-everything-v2x-communication-enhancing-road-safety-and-traffic-management

7. Uber's self-driving operator charged over fatal crash – BBC
https://www.bbc.com/news/technology-54175359

8. Automated Vehicles for Safety – NHTSA
https://www.nhtsa.gov/vehicle-safety/automated-vehicles-safety

9. Joint Factsheet by the Land Transport Authority (LTA) & SSC - Enhanced National Standards for the Safe Deployment of Autonomous Vehicles in Singapore – LTA
https://www.lta.gov.sg/content/ltagov/en/newsroom/2021/9/news-releases/enhanced-national-standards-for-the-safe-deployment-of-autonomou.html

10. Road vehicles: Cybersecurity engineering – ISO
https://www.iso.org/standard/70918.html

11. Waymo Safety Report: February 2021 – Waymo
https://downloads.ctfassets.net/sv23gofxcuiz/4gZ7ZUxd4SRj1D1W6z3rpR/2ea16814cdb42f9e8eb34cae4f30b35d/2021-03-waymo-safety-report.pdf

12. Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0 – National Science and Technology Council and US Department of Transportation

https://www.transportation.gov/sites/dot.gov/files/2020-02/EnsuringAmericanLeadershipAVTech4.pdf