AUTOMATED VEHICLES

Cybersecurity & Automated Vehicles

In the past decade, significant advances in vehicle technology and safety features have been achieved, although, the types of technologies used in vehicles today, like many other electronic devices, possess cybersecurity vulnerabilities. The development of automated vehicle (AV) technology poses a new challenge to data security as automated vehicles are likely to integrate connected vehicle (CV) technology to enable external communication between vehicles, and between vehicles and the environment. This connectivity may create more routes for hackers to potentially gain remote access and execute cyberattacks. It is important to ensure that the appropriate safeguards are in place to mitigate cyber threats and maintain public trust and perceptions of safety. As such, cybersecurity must be effectively addressed before large-scale implementation of these technologies on public roads.

This fact sheet addresses key questions and issues related to cybersecurity of automated and connected vehicle technology. It includes an overview of potential cybersecurity risks and vulnerabilities, and describes ways governments and industry can work collaboratively to ensure the highest level of cybersecurity is achieved to safely deploy vehicles on public roads.

Questions & Answers

What is the difference between automated and connected vehicle technology?

AV technology relies on sensors, computer analytics and technology systems to perform certain functions without human input.

CV technology uses wireless networks to communicate with other vehicles and the surrounding environment but does not involve any automation of the driving task. Although automated vehicles do not require CV technology to operate, this technology can facilitate certain automated features and is likely to be integrated into vehicles with conditional automation (level 3) and higher.[1] For example, connectivity can provide access to the latest maps for navigation or allow vehicles to receive operational updates to their software. CV technology also contributes to the safety of AVs as collected sensor data could be shared with other nearby AVs to inform them of an issue ahead.[2]

Your brain is your vehicle's most important safety feature.

Will AVs be vulnerable to cyberattacks?

Likely. Vehicles with conditional automation (level 3) or higher will likely have some degree of connectivity and require access to data networks.[3] Although connectivity allows for desired functionality, it also increases physical access points for potential cyber-attacks, similar to risks associated with other devices connected to external networks (e.g., phones, tablets or smart appliances). The risk of malicious attacks is heightened because these vehicles will be able to perform certain driving functions without human input. If a hacker gained control of critical driving functions, this could result in potential safety and operational consequences to vehicle occupants and other road users.[4] A national survey about automated vehicles suggests perceptions of cybersecurity vulnerabilities are a concern, with results demonstrating only 21% of drivers strongly agreed the technology would be safe from cyberattacks. Moreover, a survey by Transport Canada found similar results, and also demonstrated that concerns over the cybersecurity of AV's was related to reported levels of comfort with automated vehicles.[5]

What are some ways AVs could be hacked?

As it is likely that AV technology will eventually incorporate some degree of connectivity, there would be a possibility for remote attacks, where hackers could obtain remote access by connecting to data networks. In theory, hackers could gain access to large amounts of data, such as personal and financial information. They could also gain access to trip data, such as frequent driving destinations, trip length, and number of trips per day.

Hackers could theoretically interfere with certain vehicle components, such as sensors, radar, and GPS navigation. These attacks are know as jamming or spoofing. A jamming attack occurs when signals from a vehicle component are interrupted and the vehicle cannot receive or transmit essential information.

A spoofing attack occurs when false information is injected, overriding the functioning of a vehicle component. For example, attackers could jam GPS signals necessary for safe navigation of the vehicle or inject false information to direct the vehicle off course or to a new destination.[6] Hackers may also be able to gain access to the internal vehicle network[7] which is responsible for multiple critical vehicle control functions (e.g., braking, steering and acceleration). Once internal access is achieved, hackers could theoretically control all vehicle functions.[8]

Although remote attacks are a major concern due to external connectivity, hackers could also execute an attack through direct physical access to the vehicle. If an infected device were plugged in a port (e.g., USB port), hackers could inject false messages, subverting automated functions and instructing the vehicle to perform dangerous actions.[9]

The Federal government, vehicle manufacturers and other industry stakeholders have identified cybersecurity as a top priority to ensure the safety and security of automated vehicle technology. Guidelines have been established by Transport Canada in collaboration with national stakeholders to help strengthen vehicle cyber resilience.[10] Read more below about how stakeholders are preparing AVs against cybersecurity attacks.

Can I unknowingly download a virus to my AV?

Possibly. Automated vehicle technology requires frequent software updates to provide routine patches and improvements to programming, new functionality, and bug fixes. Although it is likely AVs will receive these updates at the dealership, it is possible some manufacturers may allow updates to be downloaded

Hackers could also interfere with certain vehicle components, such as sensors, radar, and GPS. These types of attacks are known as jamming or spoofing.

Downloading third-party applications not developed by the vehicle manufacturer could also create serious vulnerabilities.

remotely, using over-the-air updates.[11] However, if a vehicle manufacturer's database were compromised by hackers, this may enable hackers to place hijacked programming into regular system updates, infecting an entire fleet of vehicles.

Downloading third-party applications not developed by the vehicle manufacturer could also create serious vulnerabilities. Such vehicle applications could provide another route for hackers to gain remote access, and vehicle manufacturers will have to balance the consumer demand for increasing personalization and the end-to-end security of third-party applications. For example, the use of mobile applications, connecting to social media applications, and integrating payment systems can increases the cyber threats to these vehicles.[12]

Who would be responsible for damages in the event of a cyberattack?

Although it is likely the technology could identify an attack, there would be little evidence to identify and prosecute a hacker. It is also uncertain whether vehicle owners would be responsible for damages as a result of the attack (e.g., vehicle repairs, cleaning the vehicle of potential malware) or damage to other vehicles.[13]

What are some of the potential motivations behind a cyber attack?

Theoretically a hacker could execute a cyberattack to weaponize an AV, or a fleet of AVs. It could be possible to create large scale chaos and gridlock by disabling vehicles in a given radius. Hackers motivated by theft could theoretically steal personal or commercial vehicles for ransom. Luckily, current research and known hacking events on AV technology are from "white-hat" hackers. "White-hat" hackers are researchers that proactively hack vehicle systems to test for vulnerabilities to ensure the security of the vehicle.[14]

What is being done to prepare AVs against cybersecurity attacks?

Advanced cybersecurity must be developed in tandem with new automated technology. The Defense-in-Depth[15] is a leading approach, which could provide multiple layers of defence mechanisms. This means if one layer fails to thwart an attack, the next layer of defence mechanisms would take action. However, development of cybersecurity protocols should be based on a comprehensive and systematic approach involving stakeholders working collaboratively to develop standards and best practices to ensure the cybersecurity of all AVs. Collectively, all levels of government, as well as automotive stakeholders have a role to play in maximizing the potential safety benefits of this technology while minimizing the risks of technological disruption and negative consequences. Public Safety Canada developed a National Cyber Security Strategy,[16] which provides an overarching vision and direction for cybersecurity in Canada. Building on the Strategy, Transport Canada published Canada's Vehicle Cyber Security Guidance in May 2020.[17] These guidelines provide a set of technology-neutral guiding principles to support industry in incorporating vehicle cybersecurity best practices throughout the vehicle lifecycle. This approach aligns with the U.S. government, which has also developed non-mandatory guidelines on cybersecurity and best practices for the automotive industry.[18]

Conclusion

As automated vehicle technology continues to evolve, increasing levels of automation will bring about new cybersecurity vulnerabilities. Cybersecurity challenges will require government and industry stakeholders to work collaboratively to develop a comprehensive cybersecurity strategy. It must provide clear technology neutral standards and regulatory requirements

applicable across the ecosystem of suppliers and providers responsible for different aspects of the technology. The cybersecurity strategy must also be unified across jurisdictions so the industry can endeavour to attain universally-acknowledged certification. Therefore, despite technological advances, a sound cybersecurity strategy keeping pace with this progress is essential to aid the safe introduction of this technology on our roads.

References

Chong, J. (2016). Automated and Connected Vehicles: Status of the Technology and Key Policy Issues for Canadian Governments. Library of Parliament, Publication No. 2016-98-E

Cutean, A. (2017). Autonomous Vehicles and the Future of Work in Canada. Information and Communications Technology Council (ICTC). Ottawa, Canada.

Deloitte (2019). Cybersecurity for Connected and Autonomous Vehicles. Retrieved from **https://www2.deloitte.com/ca/en/pages/risk/articles/cyber-connected-autonomous.html**

Deloitte (2017). Securing the future of mobility. Retrieved from: **https://www2.deloitte.com/content/dam/Deloitte/be/Documents/strategy/Securing%20The%20Future%20Of%20Mobility.pdf**

Georgia Institute of Technology (2019). "Hackers could use connected cars to gridlock whole cities." ScienceDaily. Retrieved from: **www.sciencedaily.com/releases/2019/07/190729111337.htm>**.

Kakareka, A. (2013). What Is Vulnerability Assessment?. In Managing Information Security (pp. 201-221). Syngress.

Meryem, S., & Mazri, T. (2019, October). Security study and challenges of connected autonomous vehicles. In Proceedings of the 4th International Conference on Smart City Applications (pp. 1-4).

Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015, 91.

National Highway Traffic Safety Administration (2016, October). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333). Washington, DC: Author.

National Highway Traffic Safety Administration (2013). Preliminary statement of policy concerning automated vehicles. U.S. Department of Transportation.

Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE transactions on intelligent transportation systems*, 18(11), 2898-2915.

Public Safety Canada (2018). National Cybersecurity Strategy. Cat. No.: PS4-239/2018E ISBN: 978-0-660-26553-7

RAND Corporation (2017). When Autonomous Vehicles Are Hacked, Who Is Liable? Retrieved from: **https://www.rand.org/pubs/research_reports/RR2654.html**

Robertson, R. D., Meister, S. R., & Vanlaar, W. G. (2016). Automated vehicles: driver knowledge, attitudes and practices. Ottawa, ON.

Transport Canada (2020) Canada's Vehicle Cyber Security Guidance. Retrieved from: **https://tc.canada.ca/sites/default/files/2020-05/cyber_guidance_en.pdf**

Transport Canada (2021) Public opinion research study: Consumer awareness of, and confidence in, automated vehicles (AVs) and advanced driver assistance systems (ADAS). #POR 046-20. Ottawa, ON.

Weimerskirch, A. (2016). Cybersecurity of Connected and Automated Vehicles. ATZelektronik worldwide, 11(3), 26-31.

Woo, S., Jo, H. J., & Lee, D. H. (2014). A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Transactions on intelligent transportation systems*, 16(2), 993-1006.

[1, 3] NHTSA 2013
[2] Chong 2016
[4, 9] Parkinson et al. 2017
[5] Robertson et al. 2016 ; Transport Canada 2021
[6] Meryem & Mazri 2019
[7] Woo et al. 2014; R
[8] Miller and Valasek (2015) executed a remote attack for research purposes on a vehicle through the multimedia system using the Wi-Fi connection. Ultimately, they gained access to the main internal network and were able to send commands to every component of the vehicle. This allowed them to remotely control components such as steering, engine, transmission, braking system, windshield wipers, air conditioner, and door locks (for more information, visit: **https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/)**.
[10, 17] Transport Canada 2020
[11] Weimerskirch 2016
[12] Cutean 2017; Deloitte 2017
[13] Parkinson et al. 2017; RAND Corporation 2017
[14] Georgia Institute of Technology 2019
[15] Kakareka 2013; Deloitte 2019
[16] Public Safety Canada 2018
[18] NHTSA 2016

TIRF

Want to learn more?

Visit **brainonboard.ca** to learn more about automated vehicles.

Traffic Injury Research Foundation

The vision of the Traffic Injury Research Foundation (TIRF) is to ensure people using roads make it home safely every day by eliminating road deaths, serious injuries and their social costs. TIRF's mission is to be the knowledge source for safer road users and a world leader in research, program and policy development, evaluation, and knowledge transfer. TIRF is a registered charity and depends on grants, awards, and donations to provide services for the public. Visit **www.tirf.ca**.

Traffic Injury Research Foundation (TIRF)
171 Nepean Street, Suite 200, Ottawa, ON K2P 0B4
Email: tirf@tirf.ca ISBN: 978-1-989766-22-4

Acknowledgements

Production of this fact sheet was made possible with sponsorship from Desjardins and technical expertise from Greg Overwater & Andrew McKinnon, Global Automakers of Canada.

Desjardins

Global Automakers of Canada

Your brain is your vehicle's most important safety feature.