Information Security Thought Paper
Autonomous Vehicles

Introduction

Autonomous (self-driving) vehicles are a transformative technology that will greatly impact public convenience and safety while improving the efficiency of modern transportation. With new opportunities come additional considerations from a privacy and security perspective. Organizations are urged to consider the impacts to confidentiality, integrity, and availability to networks, systems, data, and personal safety.

Defining Autonomous Vehicles and Driving

Autonomous vehicles are those that are capable of sensing their environment and operating without human interaction. The SAE (Society of Automotive Engineers) International has defined a six-point scale to define levels of autonomous driving. These have been widely accepted and are considered the standard throughout the industry.

Non-autonomous Driving	Autonomous Driving
Level 0: Driver only: human driver controls everything (steering, throttle, brakes, etc.)	**Level 3:** Conditional automation: the operator monitors the system and can intervene.
Level 1: Assisted driving: assistance systems help during vehicle operation (cruise control, etc.).	**Level 4:** High automation: there is no monitoring by the driver required.
Level 2: Partial automation: the operator must monitor the system at all times. At least one system, such as lane centering, is fully automated.	**Level 5:** Full automation, no driver required.

How Do Autonomous Vehicles Work?

Cameras and radar systems collect data about the environment such as traffic, speed and distance (from one centimeter to a few hundred meters). Advanced Driver Assistance Systems (ADAS) require several radar sensors that can 'cocoon' the vehicle for highly automated driving. Light Detection and Ranging (LIDAR) sends out millions of laser beams every second to build a detailed 3-D map of the surrounding area (this may be seen as a bubble with a spinning mirror on the top of the vehicle).

This sensor data is fed into specialized deep neural networks that run algorithms for detecting patterns and converting them into usable insights.[1] The software can recognize objects, people, cars, road markings, signs and traffic lights; obeying the rules of the road and allowing for multiple unpredictable hazards while emulating only the 'most polite' driving behaviours.

Security and Public Safety

A current modern vehicle has over 100 million lines of code; that's 25 times the amount required for the Space Shuttle (4 million lines). Autonomous vehicles will harness the most complex software ever deployed, estimated to contain half a billion lines of code.[2] With the creation of the astounding amount of program logic, how will they adhere to software engineering standards or ensure writing and testing with secure code? With automotive cyberattacks on the rise and the enormous attack surface of the autonomous landscape, lawmakers, manufacturers and the public are concerned.

It's not just autonomous vehicles that are concerning, it is the wireless communication systems involved with connected autonomous vehicles that pose the greatest vulnerability. Connected Autonomous Vehicles (CAVs) will be wireless-enabled to communicate with smart infrastructures such as connected road panels, traffic signals, rail crossings and road conditions as well as others traveling on the roads (motorcyclists, trucks, trains, etc.). This offers an opportunity to intercept, disrupt and inject malicious code affecting the entire infrastructure. Privacy is also a concern as autonomous data will be packed with personal information and may not benefit from data masking techniques.

More convenience for the public also means more convenience for criminals. Authorities will need to find novel ways to monitor autonomous delivery vehicles as the 'packages' they carry may not be common commerdial goods but narcotics, weapons or explosives. Autonomous vehicles may change the way smugglers operate or terrorists plan their attacks.

Conclusion

Organizations must perform due diligence to ensure the safety and security of those who will use autonomous vehicles. They should review, consider adopting, and benefit from relevant regulations set forth by other countries. Organizations should be prepared for the flood of enormous data volumes (equivalent to 10,000 internet users every second)[2] and ensure they have a plan to ensure adequate protections from a privacy and security perspective.

It is clear that the benefits of autonomous vehicles will eventually outweigh the challenges. Over 90% of all traffic accidents are caused by human error with 1.2 million global fatalities every year.[3] Even without mature systems, introducing Highly Automated Vehicles (HAVs) is likely to save hundreds of thousands of lives.[4]

Resources

[1] https://blackberry.qnx.com/en/ces-2018
[2] https://p.blg.com/the-sensor-the-legal-crystal-ball?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original
[3] https://www.morganstanley.com/im/publication/insights/investment-insights/ii_edge_autonomousvehicles_us.pdf
[4] https://www.rand.org/pubs/research_reports/RR2150.html