National Counterintelligence and Security Center

AUTONOMOUS AUTOMOTIVE VEHICLE SUPPLY CHAIN RISK

WHAT ARE AUTONOMOUS AUTOMOTIVE VEHICLES?

An autonomous automotive vehicle (AAV) incorporates its own ability to sense the surrounding environment and move safely with little or no human input. For simplicity, the U.S. adopted the Society of Automotive Engineers definition and classification for five levels of autonomy. Level 1 assists the driver with alerts and partial control on braking, throttle or steering. Level 2 is partial autonomy with drivers still monitoring actions but has automated brakes, steering and throttle. Level 3 assists human drivers in all activities but a driver is still required. Level 4 performs all driving functions but the driver can assume control if specific conditions require it. Level 5 is full automation where no driver is needed at all.

The AAV industry is still in its infancy but is projected to reach a market value of $61.9 billion globally by the mid-2020s. The key to this growth is the cheapening of critical advanced components such as the LIDAR sensors and incorporation of 5G assisted AI-processing power for driver assist Machine Learning software. North America is currently the largest market but the Asian market is expected to see the greatest growth of market share by 2026.

STRATEGIC RISKS

The AAV industry is heavily dependent on cheap semiconductor chips to function. The typical AAV has over 3,500 semiconductors installed. These serve the driver assist, safety, vehicle body monitor, powertrain, and sensor systems. As of 2019, U.S. based firms produced 47% of the required semiconductors but are subject to global supply chain disruptions. AAVs do not rely on the latest chip designs and instead bulk buys tried and true older, cheaper semiconductor chips.

Adversarial countries, such as China, could carry out strategic actions to disrupt or inhibit the supply of critical microchips imported into North America. Actions such as acquiring chip manufacturing companies, imposing legal restrictions, and disruption of shipping lanes could all increase supply risk.

Another risk is energy. AAVs require external support from 5G which depends on a reliable source of energy. Any disruption to the country's power grid could disrupt the 5G assisted Machine Learning software that aids the AAVs ability to function without human operators.

HARDWARE RISKS

AAVs rely on a wide variety of advanced components to function effectively. Remote sensing systems make up a large proportion of the vehicle hardware that could include LIDAR, visible HD and low light cameras, and automotive radars. U.S. automotive industry imports over 60% of its car sensors, mainly from Germany, Japan, and Canada.

Without supply chain integrity, quality assurance and tamper proofing verification becomes very difficult. Although not yet prevalent, white hat cybersecurity experts identified camera system exploits in an electric car at the Keen Security Labs in China that enabled the white hats to create a backdoor into the car system in 2019.

Besides the creation of cyber exploits, vulnerable hardware components could also be modified to transmit illegitimate signals to malicious actors, feed false stimuli to the sensors to impair function, and interfere with the Internet of Things (IoT) transmission signals to disrupt the Driver Assist Software.

SOFTWARE RISKS

AAVs rely on very advanced software designs that can parse, sort, and decide on actions from huge datasets. The more autonomy requires greater processing power which would add more weight to the vehicles. To make the vehicles viable, much of the software will rely on not just the vehicles' hardware but the additional computing power of the 5G IoT.

This means the vehicles will be continuously linked to the internet for assisting in machine learning, patching, and updates. AAVs will rely not only on its own software being reliable and properly configured but also third party software transmitted from 5G sensors and antennae.

Software-based threats to vehicles include attacks against the driver assist machine learning suite to implant malicious software, the sensor fusion processing software that could blind the vehicle, and the potential for a malicious actor to re-program the decision-processing software to take remote control of the vehicle.

References:

- Lou Frenzel, "Today's Advanced Driver Assistance Systems (ADAS) are Gradually Evolving into Full Autonomous Vehicle Systems," Innovation-Destination Automotive, 16 February, 2018. https://innovation-destination.com/2018/02/16/7-factors-critical-success-self-driving-cars/
- David Coffin et al, "Building Vehicle Autonomy: Sensors, Semiconductors, Software and US Competitvness," Office of Industries, US International Trade Commission, January 2020. https://www.usitc.gov/publications/332/working_papers/autonomous_vehicle_working_paper_01072020-_508_compliant.pdf
- Zeinab El-Rewini et al, "Cybersecurity Attacks in Vehicular Sensors," IEEE Sensors Journal, V. XX, N. XX, April 2020. https://ieeexplore.ieee.org/document/9122502
- James Andrew Lew, "National Security Implications of Leadership in Autonomous Vehicles," Center for Strategic and International Studies, June 28, 2021. https://www.csis.org/analysis/national-security-implications-leadership-autonomous-vehicles