Title

How Risky Are Cyber Security Threats Against Autonomous Vehicles?

Permalink

https://escholarship.org/uc/item/4qv7r7xf

Authors

Chakraborty, Trishna
Chen, Qi Alfred

Publication Date

2024-04-01

DOI

10.7922/G29P3004

POLICY BRIEF

Institute of Transportation Studies
UNIVERSITY OF CALIFORNIA

How Risky Are Cyber Security Threats Against Autonomous Vehicles?

Trishna Chakraborty and Qi Alfred Chen
Department of Computer Science, University of California, Irvine

April 2024

Issue

To operate safely, autonomous vehicles (AVs) rely on external sensors such as cameras, light detection and ranging (LiDAR) technology, and radar. These sensors pair with machine learning-based *perception modules* that interpret the surrounding environment and enable the AV to act accordingly. Perception modules are the "eyes and ears" of the vehicle and are vulnerable to cybersecurity attacks. The most critical and practical threats, however, arise from physical attacks that do not require access to the AV's internal systems. The risks of these types of attacks are still unknown.

To advance the field in this area, we conducted the first ever quantitative risk assessment for physical adversarial attacks on AVs. First, we identified relevant *attack vectors*, or types of cyber security attacks, targeting AV perception modules. Next, we conducted an in-depth analysis of the stages of an attack. Finally, we used these exercises to identify risk metrics and perform a subsequent computation of risk scores for different attack vectors. Through this process, we were able to quantitatively rank the real-life risks posed by different attack vectors identified in existing research. This analysis provides a framework for comprehensive risk analysis to ensure the safety of AVs on our roadways.

Key Research Findings

Existing research identifies eight types of AV cyberattack vectors. These are summarized in the table below.

Risk Level	AV Attack Vector	Description
Highest Risk	2D Printed Images	Uses road object images (e.g., pedestrians, cars) printed on paper and/or poster to confuse sensors
	2D Patches	Deploys papers and/or stickers to existing road objects to affect their perception
	Coated Camoflague	Adds camouflage imagery stickers to mask objects and/or vehicles
Lower Overall Risk	Light Projection	Uses visible light projections on the AV or on a road object
	Laser/IR Light	Uses invisible laser or infrared (IR) light projection to the AV or to a road object.
	Acoustic Signals	Uses sounds (or acoustic signals) to attack AV sensors.
	Electromagnetic Interference (EMI)	Uses EMI signals to attack AV sensing and perception pipeline.

California Resilient and Innovative Mobility Initiative

Three risk categories enable initial risk ranking and interpretation of attack vectors. The following three risk metrics can be used to calculate an overall risk score:

- Deployability —how much time, effort, and resources are required to set up and carry out an attack in real-world situations.
- Stealthiness —how easily-detectable are the attack setup and the attack behavior itself to system operators and potential nearby observers.
- Attacker's Cost —how much will it cost to plan and execute the attack (e.g., acquiring necessary tools, resources, or personnel).

These risk categories were used to identify the top three attack vector types with the highest risk profiles, among the eight listed above (2D printed images, 2D patches, and coated camouflage stickers). These three deserve more focused attention for developing potential future mitigation strategies and policy making.

While other attack vector types may present serious risks, they are less likely to occur. For example, the very dangerous, laser IR/Light attack has demonstrated a high attack success rate. However, it requires a costly physical setup: a function generator, oscilloscope, amplifier, photodiode, laser diode, lenses, camera-tracking system, and a pan-tilt system. Together this would cost an attacker about $10,000. In addition, while the equipment is being set up it will be visible to anyone on the street. For these reasons, it less likely for an attacker to engage in this type of attack in the real world due to a lack of concealability, cost-effectiveness, and ease of deployment, resulting in a lower daily-life risk. This example points to how technical attributes of such attacks alone may not predict the level of risk these attacks may pose to our daily lives.

More Information

This policy brief is drawn from the report "Risk Assessment for Security Threats and Vulnerabilities of Autonomous Vehicles" prepared by Trishna Chakraborty and Professor Qi Alfred Chen with the University of California, Irvine. The report can be found here: www.ucits.org/research-project/rimi-5b-03. For more information about findings presented in this brief, please contact Professor Qi Alfred Chen at alfchen@uci.edu.

[1] Shen, J., Wang, N., Wan, Z., Luo, Y., Sato, T., Hu, Z., Zhang, X., Guo, S., Zhong, Z., Li, K. and Zhao, Z., 2022. Sok: On the Semantic AI Security in Autonomous Driving. arXiv preprint arXiv:2203.05314.

[2] Cao, Y., Bhupathiraju, S. H., Naghavi, P., Sugawara, T., Mao, Z. M., & Rampazzi, S. (2023). You Can't See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 2993-3010).

Research presented in this policy brief was made possible through the Resilient and Innovative Mobility Initiative (RIMI) led by the UC Institute of Transportation Studies (UC ITS). RIMI is supported by the State of California through a one-time allocation in the 2021 State Budget Act. The UC ITS created RIMI as a living laboratory – bringing together university experts, policymakers, public agencies, industry stakeholders, and community leaders – to inform the state transportation system's immediate COVID-19 response and recovery needs, while establishing a long-term vision and pathway for directing innovative mobility to develop sustainable and resilient transportation in California. Established by the California Legislature in 1947, the UC ITS has branches at UC Berkeley, UC Davis, UC Irvine, and UCLA.

Project ID UC-ITS-RIMI-5B-03 | DOI: 10.7922/G29P3004