



Chapter 13

Driving Into Cybersecurity Trouble With Autonomous Vehicles


Calvin Nobles

 <https://orcid.org/0000-0003-4002-1108>
Illinois Institute of Technology, USA

Darrell Norman Burrell

 <https://orcid.org/0000-0002-4675-9544>
Marymount University, USA

Sharon Burton

 <https://orcid.org/0000-0003-1653-9783>
Capitol Technology University, USA

Tyrone Waller

Capitol Technology University, USA

ABSTRACT

Researchers forecast that autonomous vehicles will reduce accidents by 90%. The ethical interplay of autonomous vehicles, cybersecurity vulnerabilities, and societal demands further complicates the governments' decisions on self-driving cars. Autonomous vehicles have safety, economic, and societal benefactors; however, offsetting the unintended consequences of technologies requires governance initiatives to address cybersecurity threats and vulnerabilities. At issue is the lack of ethical consideration for autonomous vehicles from a cybersecurity perspective, given the amount of personal and sensitive data created, used, and stored by autonomous vehicles. The advancement of autonomous cars is increasingly reliant on software, consequently making them vulnerable to cyber-attacks. Software vulnerabilities remain a top cyber-attack vector in all industries. The deliberation concerning ethics for autonomous cars is ebb and flow, especially as opposing sides increase arguments as self-driving vehicles reach a reality.

DOI: 10.4018/978-1-6684-7207-1.ch013

INTRODUCTION

Recent developments in autonomous vehicles proliferate cybersecurity concerns with self-driving technologies. The advancement of self-driving vehicles stems from researchers seeking initiatives to improve highway safety (Page & Krayem, 2017). Vehicle accidents account for 35,000 fatalities, 2.4M injuries, and 10M crashes annually, in which human-enabled errors are the contributing factors (Boeglin, 2015; Page & Krayem, 2017). Fleetwood (2017) contended that autonomous vehicles could save 10 million lives within a decade due to the cars' crash-avoidance capability. Although in 2016, Singapore received praise for its autonomous vehicle breakthroughs with nuTonomy, a self-driving taxi, which included a human operator to control the take control, if necessary, Uber, Telsa, Volkswagon, Audi, Ford, and Google all joined the autonomous vehicles arms race (Fleetwood, 2017).

To leverage the economic and safety aspects of autonomous vehicles, California, Nevada, Florida, and Michigan have existing legislation that supports the testing of self-driving vehicles; however, Nevada and California mandate that self-driving cars relinquish control to a human operator when requested (Boeglin, 2015). Researchers forecast that autonomous vehicles will reduce accidents by 90%; nonetheless, a salient concern of autonomous vehicles is cybersecurity risk. The current cybersecurity threat landscape is hyperactive, chaotic, and troublesome due to the threat actors' unrelenting quest to access sensitive data, intellectual property, and critical systems, including autonomous vehicles. This paper critically highlights the cybersecurity risks and threats associated with autonomous vehicles from an ethical lens. The ethical interplay of autonomous vehicles, cybersecurity vulnerabilities, and societal demands further complicates the governments' decisions on self-driving cars.

Autonomous vehicles have safety, economic, and societal benefactors; however, offsetting the unintended consequences of technologies requires governance initiatives to address cybersecurity threats and vulnerabilities (Taeihagh & Lim, 2019). Researchers contend that autonomous vehicle manufacturers are rapidly developing technologies (Taeihagh & Lim, 2019). At issue is the lack of ethical consideration for autonomous vehicles from a cybersecurity perspective, given the amount of personal and sensitive data created, used, and stored by autonomous vehicles. As a result, data protection and privacy come to the forefront of security requirements to protect the owners of autonomous vehicles. Given the safety concerns of autonomous vehicles, cybersecurity threats, risks, and vulnerabilities require an assertive and comprehensive approach to ensure that information security remains a salient priority.

AUTONOMOUS VEHICLES

Autonomous cars are computer-manipulated entities with the sensory and actuator capacities to detect and identify their location and surroundings, plan actions, and execute in accordance with regulatory and safety standards (Hussain & Zeadally, 2019; Winkelman et al., 2019). This paper uses autonomous vehicles, self-driving cars, and autonomous cars interchangeably. Of note, autonomous cars are categorized by levels of autonomy, as depicted in Figure 1. Heineke et al. (2021) indicated that level 4 autonomy is attainable by 2022, while level 5 is forecasted for 2030. Figure 1 depicts the progressive autonomous levels.

Even with the technological advancements of autonomous cars, the biggest bottleneck impeding the adoption is the regulation quandary (Heineke et al., 2021). Level 5 is the most advanced autonomous capacity; given this stage's lack of human engagement in the vehicle's execution and manipulation, it

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/driving-into-cybersecurity-trouble-with-autonomous-vehicles/321022

Related Content

Tripartition of Knowledge in Knowledge-Intensive Services

Tytti Kurtti, Samppa Määttä, Jukka Aaltonen, Annamari Turunenand Sari Riipi (2013). *Business Innovation, Development, and Advancement in the Digital Economy* (pp. 117-125).

www.irma-international.org/chapter/tripartition-knowledge-knowledge-intensive-services/74140

The Effects of Online Consumer Reviews on Fashion Clothing Purchase Intention: Peripheral Cues and the Moderating Role of Involvement

Julie A. Dennisonand Matteo Montecchi (2017). *Advanced Fashion Technology and Operations Management* (pp. 318-347).

www.irma-international.org/chapter/the-effects-of-online-consumer-reviews-on-fashion-clothing-purchase-intention/178837

Big Data and Machine Learning: A Way to Improve Outcomes in Population Health Management

Fernando Enrique Lopez Martinezand Edward Rolando Núñez-Valdez (2018). *Protocols and Applications for the Industrial Internet of Things* (pp. 225-239).

www.irma-international.org/chapter/big-data-and-machine-learning/202569

The Value of Sociotechnical Theories for Implementation of Clinical Information Systems

Joanne Callen, Andrew Georgiou, Julie Liand Johanna Westbrook (2012). *Inter-Organizational Information Systems and Business Management: Theories for Researchers* (pp. 192-208).

www.irma-international.org/chapter/value-sociotechnical-theories-implementation-clinical/61613

An Integrated Vendor-Buyer Model with Uncertain Lead Time, Life Time under Inflation and Variable Holding Cost

S. R. Singhand Diksha Bhatia (2013). *Optimizing, Innovating, and Capitalizing on Information Systems for Operations* (pp. 371-380).

www.irma-international.org/chapter/integrated-vendor-buyer-model-uncertain/74027