**Thesis Project Portfolio**

# IMPE: Intelligence Malware Processing Engine

(Technical Report)

# Obstacles and Setbacks in the Development and Adoption of Autonomous Vehicles

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

**Dennis Tian**

Spring, 2024

Department of Computer Science

# Table of Contents

## Sociotechnical Synthesis

Artificial intelligence has become an increasingly-popular topic in the present day, especially in the automotive industry. Recent technology has emerged that allows vehicles to operate without a driver under limited circumstances, but integration of this technology into society is still very much in the distant future.

My STS topic explores the seemingly-endless setbacks that vehicle manufacturers have encountered throughout the push toward full vehicular autonomy. Combining case studies of prominent companies like Tesla and Cruise with an in-depth Actor-Network Theory analysis, I find that among the main areas of concern are 1) the lack of development of autonomous vehicle infrastructure alongside the vehicles themselves and 2) the conflict of interest between systems developers, who strive to produce the highest-quality and most rigorously-tested systems, and the businesses they work for, which prioritize speed above all else to outpace their competitors. I argue that trying to integrate autonomous vehicles directly into society is simply too lofty a goal for the state of the technology and the lack of supporting infrastructure. I propose one intermediate step that can be taken: public transportation. Autonomous public transportation can serve as an effective testing ground because it is easier to implement, as both the operating times and locations are restricted. If and only if it proves to be successful, the technology can be considered to expand to private vehicles.

My technical project focuses on a summer internship experience where I was in charge of the development of an internal web application, the Intelligence Malware Processing Engine (IMPE), that enables submission of a piece of suspected malware and returns valuable metadata and behavioral information obtained from various static and dynamic analysis tools. The project

was divided into two main teams: those in charge of the web application itself and those overseeing the reverse engineering (RE) tools that the application uses to process samples.

The web application side of IMPE was written using mostly Python 3 and JavaScript and had extended support for API integrators, people who interact with the application through the REST API rather than the UI. We implemented IMPE's backend using a combination of Celery, RabbitMQ, and Redis for parallelized worker/queue management, and we wrote the frontend using the React framework. The RE tools were written in a variety of languages, including Python, YARA, and Rust. They encompass both static and dynamic analysis and include both third-party programs and ones written in-house.

The tools I worked on mostly focused on static file analysis, where the goal was to glean information from a file without actually running it. For example, I helped design and write parsers to extract keywords and strings that could provide insight on the behavior of a malicious file. As another example, I wrote malware signatures using YARA; these signatures each correspond to a malware family and are run against files to potentially determine what family they belong to. IMPE has gradually become the go-to resource for analysts whenever they need information about a sample that would otherwise take hours or days to compile by hand, and the end goal is to have everything polished and tested to be ready for commercial distribution.

In the intersection of my STS and technical projects, I realized that the technology behind autonomous vehicles must place an extreme emphasis on security, as lives are immediately at stake in the event of a breach. This is different from typical incidents, where money or sensitive data is at risk; if the correct course of action is not taken, a fatal accident may occur within seconds. Working on IMPE and exploring the nuances of the societal impact of autonomous vehicles showed me that we are still a long way from this long-coveted dream.