DRIVE-BY-WIRE IMPLEMENTATION OF FORD ESCAPE

DATA ACQUISITION OF AUTONOMOUS VEHICLES AND IMPLICATIONS ON CYBER SECURITY

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Mechanical Engineering

By
Jacob E. Deane

November 1, 2021

Technical Project Team Members
Matt Deaton
Henry Goodman
Logan Montgomery
Alex Pascocello
Vishal Singh

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Catherine Baritaud, Department of Engineering and Society

Tomonari Furukawa, Director of VICTOR Lab

Privacy has always been a bartering chip in American politics. In 2001 the American people gave up part of their privacy for freedom when the Patriot Act increased the government's power to spy into citizens' lives (American Civil Liberties Union, n.d, sect. 3). Recently, teenagers give up part of their privacy to social media or search engine companies like Instagram or Google to connect with other people. Now, a new form of privacy breach is being integrated into society; an invention with the best intentions to improve safety and convenience, but behind the wheel are unregulated corporations.

Autonomous vehicles are the next step in mobility, being the first to transition the common era into the future of artificial intelligence. Electric vehicles, the first step to self-driving cars, are rising in popularity and it is estimated that "by 2040, 58% of global passenger vehicle sales will come from electric vehicles" (Kopestinsky, 2021, "Electric Car Statistics Worldwide" section). In the technical project the team will be replacing a stand-alone mechanical driving system in a Ford Escape with an electromechanical drive-by-wire system. The intent is to control the vehicle through a practical controller connected to the wiring of the car, just a step in the process to autonomous driving. The team, consisting of fourth-year mechanical engineering students Jacob Deane, Henry Goodman, Logan Montgomery, Alex Pascocello, Vishal Singh, and Matthew Deaton, is led by Professor Tomonari Furukawa, a highly respected and published researcher in the fields of robotics and computational mechanics. Having already completed the review of existing technologies, customer data, and technology specifications, the team is ready to begin concept generation and will hopefully start work on the vehicle within the next week.

The loosely coupled STS research paper through the Social Construction of Technology lense developed by Trevor J. Pinch and Wiebe E. Bijker will aim to discuss and clarify the

consequences of data collection by autonomous vehicles. Having little legal regulation of data collected by car manufacturers and a relatively easy hackability of these vehicles, the wide array of data collected could be stolen or used against the user. There are currently researchers debating safety regulations that could decrease the threat of privacy to future users such as new firewalls or algorithms to find cracks in the system. Autonomous vehicles can create safer roads and give great freedom to those unable to drive, but there must be precautions set forth before their adoption to ensure users' privacy remains safe.

DRIVE-BY-WIRE IMPLEMENTATION OF FORD ESCAPE

Drive-by-wire was developed following the success of fly-by-wire, a process used by NASA in the 1970s to control the Apollo Lunar Module (National Museum of American History, 2018, para. 1). It is comprised of a series of sensors and actuators connected to the control area network (CAN) bus matrix. The CAN bus to a car is like "the nervous system in the human body," (Autopi, 2021, "CAN Bus Easily Explained" section) as it enables communication between the sensors within the system. This allows information collected by sensors such as LiDar and Radar to communicate with the system through a central core processing station. It will be integral for the technical project to successfully communicate with the already existing CAN bus within the Ford Escape.

Integrating an electromechanical drive-by-wire system is difficult to implement on an already functioning vehicle. This is due to the fact that the mechanical gas pedals and steering wheel are already installed and will have to be removed or adjusted to allow for the motors and actuators. It is also important to note that "introducing changes into the most critical subsystems in the car may be very dangerous" (Belcarz, 2018, "Car Choice and Modification" section)

because systems could fail at high speeds. The steer-by-wire portion will be less strenuous a task as the Ford Escape has power-steering. This is useful because power steering “uses an electric motor that draws energy from the vehicle's electrical system to provide the steering assistance” (Vanderwerp, 2019, para. 7) which can be rewired to the new steer-by-wire system. The current vehicle delivered to the team has already been used in a similar drive-by-wire experiment. This is helpful as many of the wires have already been pulled out of the interior, however it will be a feat of reverse engineering to unscramble and assign the massive mess of wires present to the correct portions of the vehicle and CAN bus. The team will be working on the vehicle in the Observatory Mountain Engineering Research Facility in the old nuclear reactor space.

Another difficulty the team will have to face is the creation of a practical controller for the system. In recent years control theory has been implemented through practical controllers, most commonly as partial, derivative, integral (PID) controllers. There have been several difficulties converting closed loop control theory to a fully functioning plant system, specifically in creating a controller that is low complexity, operates in discrete-time, and is free of numerical problems (Anderson, 1993, p. 17). A controller will be a requirement for the project as it is relevant to the customer needs set forth. The controller will connect to the system computer on board placed in the trunk of the car. A system diagram of how the computer will then connect to the rest of the electromechanical system is presented in Figure 1 (p. 4).

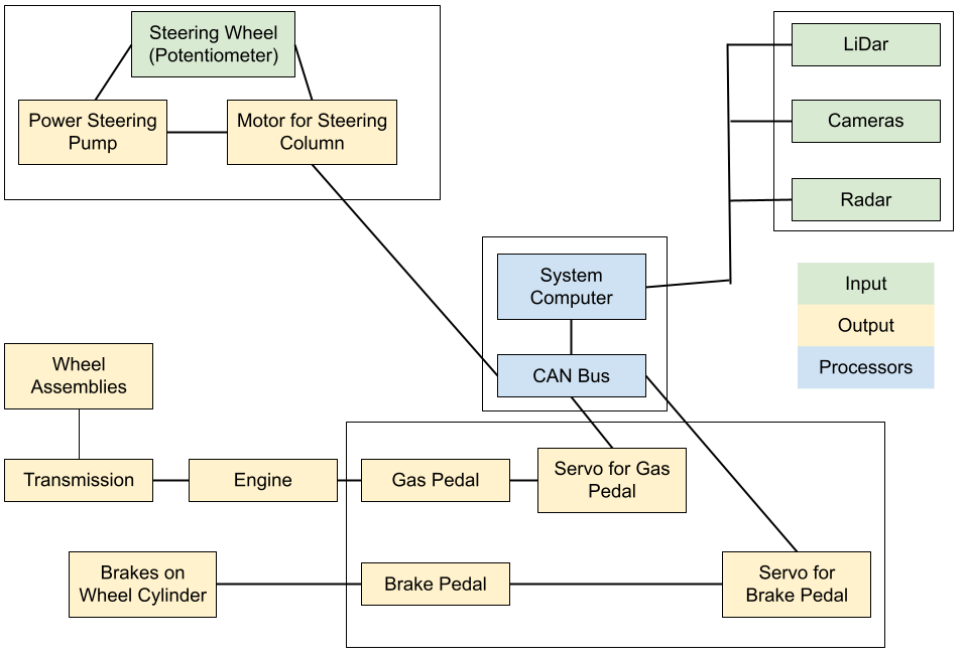

Figure 1

System diagram of drive-by-wire implementation including sensors and actuators connected to appropriate outputs. A key is included to describe the inputs, outputs, and processors of the system. (Deane, 2021)

Drive-by-wire vehicles are integral to the progress of autonomous cars in the near future. They provide more freedom of driving to those disabled and can allow for safer roads. In addition, this approach to car manufacturing results in:

(1) enhanced safety and comfort,

(2) reduced cost associated with manufacturing and maintenance, and

(3) elimination of environmental concerns caused by hydraulic systems. (Xiang, 2008, p.138)

The technical report will aim to adhere to these advantages while still allowing for user input through mechanical leverage. This is another customer need presented in response to the lack of

faith in electric systems. It represents general skepticism against electric control of vehicles instead of physically steering and driving the car. With this in mind it is the aim of the technical project to completely control the Ford Escape using an external practical controller connected to a drive-by-wire electromechanical system while still allowing for the mechanical control of the vehicle.

DATA ACQUISITION OF AUTONOMOUS VEHICLES AND IMPLICATIONS ON CYBER PRIVACY

It is required for autonomous vehicles to collect mass amounts of data of the environment to respond appropriately and safely on the roads. The CAN bus collects location, speed, addresses, and, if there is a listen-response AI in the car, your conversations as well. If the car was a closed loop system that only uses this information as a feedback input to improve driving, then the only network with access to that data would be the car manufacturers. In fact, Jim Farley, Chief Executive Officer of Ford, said in a statement in 2014 at the Consumer Electronics Show:

"We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing. By the way, we don't supply that data to anyone."

Though Farley later retracted the statement, his "quote highlights the privacy implications of data collection and use in vehicles." (Riontino, 2021, "Addressing Privacy Concerns" section). There are few legal regulations on car manufacturers as to the power they have over the data accumulated by their vehicles.

The General Data Protection Regulation (GDPR) has been hindering the progress of self-driving vehicles precisely due to this dilemma. Countries without the GDPR have been more successful in their advancements of autonomous vehicles because they have not had to "navigate between privacy and data protection on the one side, and the need for vast amounts of processing data for SDVs to function, on the other" (Ryan, 2020, p. 1194). In the United States this mass amount of data is privy only to the car manufacturers, which gives them an unprecedented amount of power over traffic, urban planning, home addresses, and private affairs. All of "that information is currently housed in technological and corporate black boxes" (Self-driving cars, 2019, para. 1) which is not transparent even to the user. This creates a lopsided power dynamic between car companies and users, stripping the users of essential privacies. This STS research paper aims to use the Actor-Network theory to examine the dangers and security of the mass data collected by autonomous vehicles.

HACKING OF AUTONOMOUS VEHICLES

While there is a debate on the legal ownership of data collected by autonomous vehicles, there is also the possibly greater threat of the illegal obtaining of this data. Hacking is as old as technology itself, and new technologies create new weaknesses. The reality of autonomous vehicles is that they will not be closed loop systems, but will use the cloud and its connection to other vehicles in the process of collecting data. This opens the car and its data up to threats from hackers.

Autonomous vehicles not confined to closed loop systems can communicate with other autonomous vehicles on the road or use GPS systems to create safer environments and shorter

drive times. However, this opens up the vehicle to several different types of attacks shown in Figure 2.

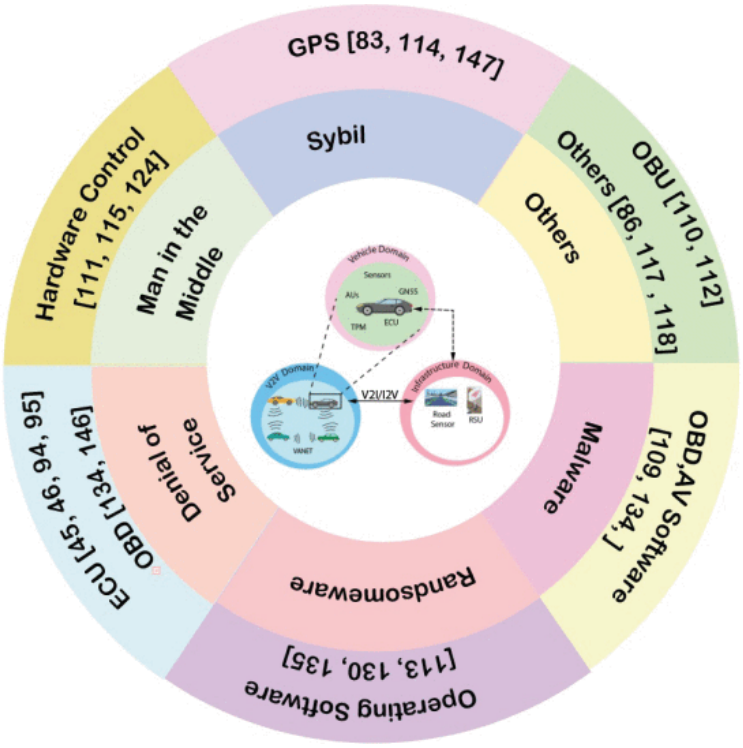

Figure 2

Classification of attacks on autonomous vehicles by type of attack and piece of software or hardware that is hacked by the attack. The diagrams in the middle are explanatory images of the connections created between the vehicle and different environments. (Crowdhurry, 2020, sect. V)

These attacks all involve an individual either intercepting, spoofing, or manipulating data messages sent from the autonomous vehicle through different weaknesses in the car (Crowdhurry, 2020, sect. V).

There is also the threat coming from mobile applications connecting to vehicles. Most cars today can communicate and connect to mobile devices, but these devices can be used to "[configure] a backdoor by activating the service port to allow the attacker to reenter the device and elevate the privileges of available accounts" shown in Figure 3 (Park, 2020, sect. 2.2).

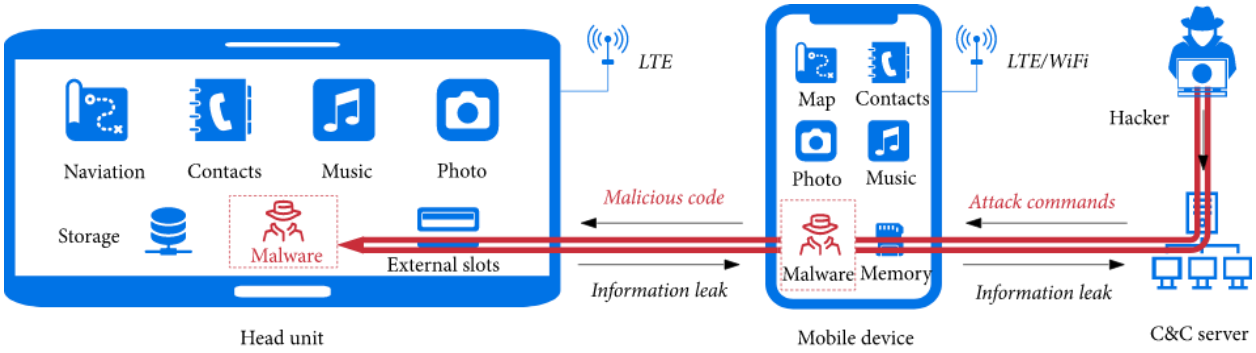

Figure 3

Infographic of malware inserted into autonomous vehicle software through android connection. It shows the hackability of autonomous vehicles through the placement of malware in an android device before connecting to the vehicle. (Park, 2020, sect. 3.1)

All of these attacks have been successful at one point on different autonomous cars and are still relevant threats to users' privacy today.

Currently, researchers are working on combative efforts to the threat of hackers on self-driving vehicles. Some initial methods to secure the data of the user involves, but is not limited to, encrypting data, partial observation of secondary car's information, and context-based authentication. Even still, each of these methods has their own weaknesses that allow for manipulation of the users' vehicle (Karnouskos, 2018, p. 165). Park and Jin-Young, workers at the School of Information Security at Korea University studying cybersecurity and computer engineering, have been working on an algorithm as well to combat hacking through android systems. Their "algorithm is highly accurate (92.9%) and fast (0.049 s), making it suitable for real-time malware detection in a self-driving vehicle environment" (Park, 2020, "Conclusion" section). These efforts against malicious hacking of autonomous systems will hopefully enable a secure future for data in self-driving vehicles.

NEW TECH, NEW RULES

Technology is on an exponentially upward trajectory and its current advancements in autonomous vehicles is exhilarating and hopeful. As with all new technology, however, the security and privacy of its users must be put at the forefront of its innovation. Whether debating the legal ownership of the data collected by autonomous vehicles or examining the threats hackers pose to the new technology, safeguards must be present before any integration can succeed.

REFERENCES

American Civil Liberties Union. (n.d.). Surveillance under the USA/patriot act. *American Civil Liberties Union.* https://www.aclu.org/other/surveillance-under-usapatriot-act

Anderson, B. D. O. (1993). Controller design: Moving from theory to practice. *IEEE Control Systems, 13*(4), 16–25. https://doi.org/10.1109/37.229554

Autopi. (2021, March 18). CAN bus explained (2021). *AutoPi.Io.* https://www.autopi.io/blog/can-bus-explained/

Belcarz, K., Białek, T., Komorkiewicz, M., & Żołnierczyk, P. (2018). Developing autonomous vehicle research platform – a case study. *IOP Conference Series.Materials Science and Engineering, 421*(2) http://dx.doi.org/10.1088/1757-899X/421/2/022002

Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., & Das, R. (2020). Attacks on self-driving cars and their countermeasures: A survey. *IEEE Access, 8*, 207308-207342. http://dx.doi.org/10.1109/ACCESS.2020.3037705

Deane, J., Goodman, H., Montgomery, L., Pascocello, A., Singh, V., & Deaton, M., (2021). *Drive-by-Wire System Diagram*, [Figure 1]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Karnouskos, S., & Kerschbaum, F. (2018). Privacy and integrity considerations in hyperconnected autonomous vehicles. *IEEE Proceedings, 106*(1), 160-170. http://dx.doi.org/10.1109/JPROC.2017.2725339

Kopestinsky, A. (2021, August 12). Electric car statistics in the US and abroad. *PolicyAdvice.* https://policyadvice.net/insurance/insights/electric-car-statistics/

National Museum of American History. (2018, July 25). Driving by wire. *Smithsonian*. https://americanhistory.si.edu/america-on-the-move/driving-by-wire

Park, S., & Jin-Young, C. (2020). Malware detection in self-driving vehicles using machine learning algorithms. *Journal of Advanced Transportation, 2020*, 9. http://dx.doi.org/10.1155/2020/3035741

Riontino, M. S. (2021, January 15). Who will take care of data privacy on autonomous vehicles?. *Celantur*. https://www.celantur.com/blog/autonomous-vehicle-data-privacy/

Ryan, M. (2020). The future of transportation: Ethical, legal, social and economic impacts of self-driving vehicles in the year 2025. *Science and Engineering Ethics, 26*(3), 1185-1208. http://dx.doi.org/10.1007/s11948-019-00130-2

Self-driving cars and geospatial data: Who holds the keys? (2019). *Ecn*, http://proxy01.its.virginia.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Ftrade-journals%2Fself-driving-cars-geospatial-data-who-holds-keys%2Fdocview%2F2265708408%2Fse-2%3Faccountid%3D14678

Vanderwerp, D. (2019, June 11). What is power steering and how does it work? *Car and Driver.* https://www.caranddriver.com/features/a27888229/power-steering/

Xiang, W., Richardson, P. C., Zhao, C., & Mohammad, S. (2008). Automobile brake-by-wire control system design and analysis. *IEEE Transaction on Vehicular Technology*, *57*(1), 138-145. https://doi.org/10.1109/TVT.2007.901895