Poster: Efficient Exploration of Automotive Ranging Sensor Attacks

Jack Carter
University of Southern California
Los Angeles, CA, USA
jackcart@usc.edu

Bhagawat Baanav Yedla Ravi
University of Florida
Gainesville, FL, USA
b.yedlaravi@ufl.edu

Md Rafiul Kabir
University of Florida
Gainesville, FL, USA
kabirm@ufl.edu

Sandip Ray
University of Florida
Gainesville, FL, USA
sandip@ece.ufl.edu

ABSTRACT

Security is a critical challenge in emergent autonomous vehicles. However, the security challenges in automotive systems are not widely understood even in the cybersecurity community. To address this problem, we develop an adaptable exploration platform for automotive security. This platform enables users to gain hands-on experience and insights into security vulnerabilities. We discuss specific challenges and prerequisites involved in designing such an exploration tool. We demonstrate the platform's capabilities by exploring automotive ranging sensor attacks.

CCS CONCEPTS

• **Hardware → Communication hardware, interfaces and storage**; **Sensors and actuators**;

KEYWORDS

Exploration Platform, Automotive Security

ACM Reference Format:
Jack Carter, Bhagawat Baanav Yedla Ravi, Md Rafiul Kabir, and Sandip Ray. 2023. Poster: Efficient Exploration of Automotive Ranging Sensor Attacks. In *The Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '23), October 23–26, 2023, Washington, DC, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3565287.3617986

1 INTRODUCTION

In recent years, vehicular systems have undergone a rapid and remarkable transformation, witnessing a surge in autonomous features. A modern automobile is equipped with a multitude of Electronic Control Units (ECUs), interconnected with various sensors, actuators, in-vehicle networks, interfaces, and wireless protocols. This amalgamation results in a complex network, supported by several hundred megabytes of software. The autonomous features hold out the promise to substantially enhance safety, comfort, and infrastructure utilization by reducing human errors and improving reaction time to external stimuli. However, a crucial downside that comes along with these benefits is the heightened vulnerability of these systems to cyber-attacks. Unfortunately, recent research demonstrates that malicious entities can easily compromise vehicular systems, leading to catastrophic accidents and even posing a threat to the entire transportation infrastructure [6]. However, despite its undeniable importance, an understanding of the pivotal role that security plays in vehicular systems is lacking even among automotive designers or cybersecurity experts. A key challenge is that there is no infrastructure for users to "play with" various scenarios and attack attempts and realize what is actually involved in exploiting a vulnerability in a vehicle. It is consequently critical to develop intuitive, effective exploration platforms to plug this crucial gap.

In previous research [9], we developed a platform called AutoHaL to facilitate the exploration of ultrasonic ranging sensor attacks in automotive systems. This platform enabled users the ability to delve into diverse attack scenarios targeting ultrasonic sensors in automobiles. However, while this platform served as a proof-of-concept demonstration, it fell short of being a fully practical exploration platform suitable for learning purposes. We explain the deficiencies in more detail in Section 3, but some of the key challenges included bulk, cost, and lack of modularity and interoperability.

In this paper, we explain how to enhance the foundation of AutoHaL, transforming it into a viable and effective learning platform. We systematically deconstruct the platform needs to achieve the needs of viability. We discuss the challenges involved in developing such a platform, and our approach in addressing these challenges. To our knowledge, our work represents the first viable learning platform for exploring automotive sensor attacks.

2 RELATED WORK

Considerable research has been done on the exploration of ranging sensor attacks within vehicular systems. Yan *et al.* [10] showed the compromise of sensors within actual vehicles, employing techniques such as jamming and spoofing. Lim *et al.* [5] constructed an experimental environment that serves as a proving ground for an attack capable of compromising the accuracy of ultrasound sensors, thereby inducing object detection failures. Petit *et al.* [7] offers a comprehensive display of remote attacks encompassing jamming,

MobiHoc '23, October 23–26, 2023, Washington, DC, USA
© 2023 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9926-5/23/10.
https://doi.org/10.1145/3565287.3617986

spoofing, replay, and blinding on Lidar and camera-based systems utilizing readily available commercial hardware.

The field of exploration platforms for effective comprehension of automotive security is in its infancy. However, studies have considered modeling attacks and comprehending their ramifications on system functionality [8]. Liang [4] pioneered a web-based educational platform that harnessed network connections alongside computer-aided design (CAD), open-source software, and virtual reality technology to facilitate circuit design within automotive electrical systems. Englisch *et al.* [1] took a different route by developing an educational platform that concentrated on software development. This platform interlinked the various phases of automotive system development through custom-built tools, thereby augmenting the learning journey of participants. In a similar manner, Kabir *et al.* [3] conceptualized a software-based exploration platform tailored for automotive electronics targeting functional simulation and optimization. Gireesh *et al.* [2] created a mixed reality platform that focused on machine learning attacks on DNNs deployed in computer vision modules. However, it's worth noting that none of these platforms have thus far offered a hands-on learning experience specifically focused on automotive security.

3 NEEDS FOR EXPLORATION PLATFORM, AutoHaL APPROACH, AND LIMITATIONS

Ranging sensors enable a vehicle to detect objects in its environment. Attacks on ranging sensors attempt to distort this detection. Clearly, a hardware exploration platform that enables the exploration of these attacks would need two entities: an attacker and a proxy vehicle. In AutoHaL, a vehicle based on Raspberry Pi is used as a proxy vehicle. The setup is controlled by a GUI that has a section for each hardware entity. The attacker has the parameters: angle, height, trigger frequency, number, and type of the attacking sensor. The user can play with various parameters on the attacker section to generate interfering signals that subvert the vehicle from functioning normally. The behavior can be observed for various values and selections of parameters in both sections. In a benign scenario, the proxy car stops at a user-defined distance from an obstacle obstructing its path. This stopping distance can be adjusted within the graphical user interface (GUI).

Given the above organization, an exploration platform should ideally satisfy the following four objectives.

- The platform should enable a wide range of sensor attacks, not limited to those previously explored.
- The platform is user-friendly and versatile, capable of accommodating various microcontroller breakout boards.
- The platform must be compact, to enable effective usage in traditional classroom or lab, and portability.
- The platform needs to be cost-effective for widespread use in academic and research laboratories.
- The platform must produce consistent results, *i.e.*, if given the exact same attack stimuli multiple times, the behavior of the platform should be the same each time.

Unfortunately, AutoHaL as originally designed did not satisfy many of the above. It lacked the required level of flexibility to execute potential attacks, *e.g.*, it only supported ultrasonic sensors with two frequencies. It had a rudimentary frontend that enabled the user to configure some attack parameters, but only the height of the attacking platform was effusively configurable. It involved bulky power supplies and a complex network of wires connecting various electronic components, actuators, and sensors, all of which operated on different voltage levels. It had a heavier attacker gantry that needed medium-sized stepper motors such as the NEMA 11 and NEMA 14, which drew large currents to prevent skipping steps. This demanded stepper motor drivers like TB6600 and DM566 which were heavy and occupied a larger volume. Furthermore, identifying the root cause of any faults was challenging due to the sheer number of components and sub-assemblies involved.

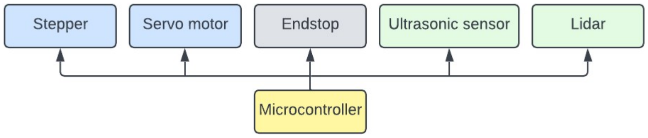

Figure 1: Attacker: microcontroller and peripherals

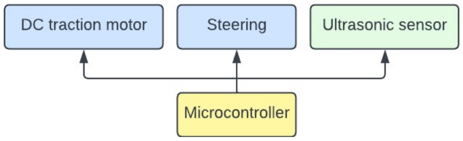

Figure 2: Proxy vehicle: microcontroller and peripherals

4 A VERSATILE, COST-EFFECTIVE, COMPACT EXPLORATION PARADIGM

Figs. 1 and 2 show the overall organization of our exploration paradigm and approach to address the deficiencies above. We introduce modularity to the platform, allowing both software and hardware modules to be added and upgraded. This facilitates the exploration and execution of advanced attacks that demand specialized knowledge. As an example, the chassis is designed to include a steering mechanism as an attachment if the user decides to work on advanced attacks *e.g.*, Auto-park features, which essentially require path planning in 2D. The platform also enables configurability and can accommodate microcontroller breakout boards such as the Arduino Nano 33 BLE, Raspberry Pi Pico W, ESP32, etc. Each microcontroller is equipped with its respective adapter to facilitate necessary hardware connections within the attacker. To address the issue of bulk and achieve interoperability, the platform standardizes two voltage levels. Furthermore, instead of employing individual power supplies for each component, we utilize a microcontroller capable of supplying the range of voltage, allowing us to power low-voltage components such as the attacking transducer and end stops with a low voltage (*e.g.*, 3V), while using higher voltage (*e.g.*, 5V) for the LiDAR sensor, servo, and stepper motor. To enable compactness, a NEMA stepper motor is used instead of medium-sized motors. An onboard rechargeable battery is employed in lieu of lengthy wires connected to external power supplies. Furthermore, our platform successfully cuts down on unit cost by replacing the original Raspberry Pi with a microcontroller and making use of off-the-shelf components while improving robustness, modularity,

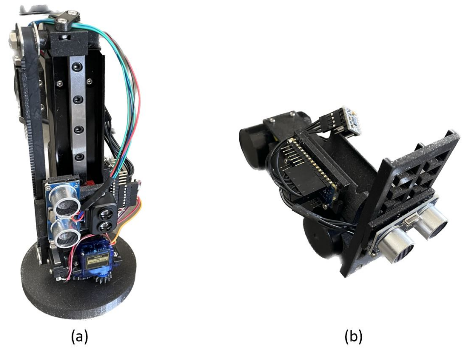
(a) (b)

Figure 3: (a) Attacker module and (b) Proxy vehicle

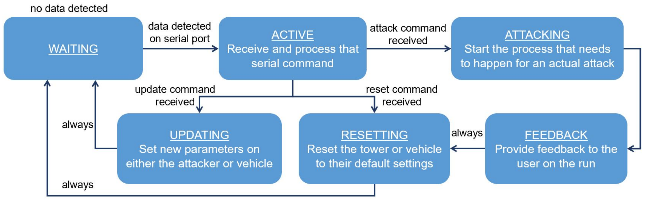
no data detected
WAITING
data detected on serial port
ACTIVE
Receive and process that serial command
attack command received
ATTACKING
Start the process that needs to happen for an actual attack
update command received
reset command received
always
UPDATING
Set new parameters on either the attacker or vehicle
RESETTING
Reset the tower or vehicle to their default settings
always
FEEDBACK
Provide feedback to the user on the run
always

Figure 4: Arduino Workflow

and functionality. Finally, consistency is addressed by carefully going through the design strategy and eliminating designs that could potentially alter experimental outcomes during usage. Fig. 3 shows the attacker module and proxy vehicle hardware.

Finally, we comment a bit on the software design for the platform. The software functionality is divided into separate states that the controller would move through as incoming commands are parsed and executed (see Fig. 4). This structure allows for the versatility and modularity of the code when future features are added or removed, enabling easier identification of code segments that are not functioning correctly. In addition, these states are moved through automatically, meaning the seemingly more complex inner workings of the Arduino code can be ignored by the user who is interacting with a simplified, intuitive GUI.

Remark 1. *While the improved hardware modularity and addition of front-end functionality improved the overall accessibility, the initial setup procedure for connecting the GUI to the attacker and vehicle requires a multi-step process which can easily be done incorrectly. In our testing using HC-06 Bluetooth modules, both the attacker and vehicle modules appear as "HC-06" upon Bluetooth connection and the front-end setup requires the user to correctly identify which HC-06 represents which module and assign their COM ports to the respective setup entry boxes. It is very easy for these to get switched around and such errors will prevent the system from functioning. This can be fixed by either (1) altering the broadcasting names for the vehicle and attacker to separately unique identifiers, or (2) moving the device identification to the software side with an identifying exchange upon establishing a connection between the devices and the GUI.*

Remark 2. *In our testing, an Arduino Nano 33 IoT did not provide support for the serial Bluetooth connection, so an additional HC-06 Bluetooth module was purchased to fulfill that need. This means the features of the Arduino Nano 33 IoT which add cost, were left unutilized. This can be remedied by making use of a microcontroller with more encompassing support for Bluetooth serial communication, such as an ESP32, or by using a non-Bluetooth microcontroller in conjunction with a Bluetooth module. These both could potentially be done and would further reduce the cost of the platform.*

5 CONCLUSION

The use of ranging sensors by vehicles to detect and respond to their environment is becoming increasingly relevant as autonomous vehicles start entering the public domain. In our work, we extended the AutoHaL educational exploration platform to create an accessible medium for a user to experience and grasp how an attack on these sensors might be done, and what an attack on these ranging sensors could result in. By drastically reducing cost, improving modularity, and improving functionality, this system is more apt than its predecessor to be used in an educational environment for those who may be a stakeholder in the automotive world, but lack the comprehension of automotive security.

In future work, we will explore further optimization of the platform to improve performance, usability, compactness, and cost. We will also extend it beyond ranging sensor attacks, including GPS and Lidar attacks and attacks on vehicular communications.

ACKNOWLEDGMENTS

This research has been partially supported by National Science Foundation under Grant No. REU-2150136.

REFERENCES

[1] Norbert Englisch, René Bergelt, and Wolfram Hardt. 2020. An Educational Platform for Automotive Software Development and Test. In *2020 IEEE 32nd Conference on Software Engineering Education and Training (CSEE&T)*. IEEE, 1–4.

[2] Venkata Sai Gireesh Chamarthi, Xiangru Chen, Bhagawat Baanav Yedla Ravi, and Sandip Ray. 2023. Exploration of Machine Learning Attacks in Automotive Systems Using Physical and Mixed Reality Platforms. In *2023 IEEE International Conference on Consumer Electronics (ICCE)*. 1–4. https://doi.org/10.1109/ICCE56470.2023.10043491

[3] Md Rafiul Kabir, Bhagawat Baanav Yedla Ravi, and Sandip Ray. 2023. A Virtual Prototyping Platform for Exploration of Vehicular Electronics. *IEEE Internet of Things Journal* (2023), 1–1. https://doi.org/10.1109/JIOT.2023.3267339

[4] Janus S Liang. 2007. A web-based learning platform for measuring and circuit practice in part design course of automotive electric. In *2007 11th International Conference on Computer Supported Cooperative Work in Design*. IEEE, 956–961.

[5] Bing Shun Lim, Sye Loong Keoh, and Vrizlynn LL Thing. 2018. Autonomous vehicle ultrasonic sensor vulnerability and impact assessment. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. IEEE, 231–236.

[6] C. H. Miller and C. Valasek. 2015. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA* 2015 (2015), 91.

[7] Jonathan Petit, Bas Stottelaar, Michael Feiri, and Frank Kargl. 2015. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Europe* 11, 2015 (2015), 995.

[8] Prabha R and Sriram Sankaran. 2019. An Experimental Platform for Security of Cyber Physical Systems. In *2019 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)*. 123–128. https://doi.org/10.1109/iSES47678.2019.00036

[9] Bhagawat Baanav Yedla Ravi, Md Rafiul Kabir, Neha Mishra, Srivalli Boddupalli, and Sandip Ray. 2022. Autohal: An Exploration Platform for Ranging Sensor Attacks on Automotive Systems. In *2022 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 1–2.

[10] Chen Yan, Wenyuan Xu, and Jianhao Liu. 2016. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *Def Con* 24, 8 (2016), 109.