AUTOHAL: An Exploration Platform for Ranging Sensor Attacks on Automotive Systems

Bhagawat Baanav Yedla Ravi, Md Rafiul Kabir, Neha Mishra, Srivalli Boddupalli, and Sandip Ray
Department of ECE, University of Florida, Gainesville, FL 32611. USA.

***Abstract*—Security is a critical concern in the emergent era of autonomous vehicles. Nevertheless, security challenges in automotive systems are not well-understood except by a small set of selected experts. In this paper, we address this problem by developing a novel, flexible exploration platform for automotive security. Our framework, AUTOHAL, enables the user to get a hands-on understanding of security compromises. We discuss the unique challenges and requirements in the design of such an exploration platform. We discuss the use of the platform in exploring automotive ranging sensor attacks.**

I. INTRODUCTION

Vehicular systems have seen a rapid transformation in recent years, with an explosive infusion of autonomous features. A modern automobile includes hundreds of Electronic Control Units (ECU) each attached to a variety of sensors and actuators, a number of in-vehicle networks, interfaces, and wireless protocols for communicating with several external entities, and several hundred megabytes of software. However, an obvious upshot of autonomy is the increased susceptibility of these systems to cyber-attacks. Recent research has shown that it is surprisingly easy for a malicious entity to subvert a vehicular system, causing catastrophic accidents and possibly bringing down the transportation infrastructure [1]. Unfortunately, despite its critical need, awareness of the role of security in vehicular systems remains limited across the spectrum of stakeholders, including designers, parts suppliers, platform integrators, policy enforcement authorities, and even the cybersecurity community. While several high-profile papers have been published demonstrating compromises to transportation systems, these works remain perceived as niche topics. Unsurprisingly, in a recent survey by the world's second-largest reinsurer Munich Re, 55% of the surveyed corporate risk managers named vehicular security as their top concern for autonomous vehicles [2].

We address this problem by developing an exploration platform that enables users with he limited domain expertise to get a sense of security challenges in modern vehicles. Our platform, AUTOHAL (**Auto**motive **Ha**nds-on **L**earning Platform), enables the user to "play with" a variety of automotive security compromises. The focus of this paper is on ranging sensors that are used by an autonomous vehicle to develop an internal perception model of its environment. An adversary providing wrong or misleading sensor values to the vehicle can coerce it into unsafe or inefficient driving maneuvers, *e.g.*, by distorting the distance of a vehicle from a pedestrian or obstacle, leading to accidents. We discuss some interesting research challenges in developing such an exploration platform, and our approaches to address them.

II. AUTOMOTIVE RANGING SENSOR ATTACKS

Ranging sensors are used by autonomous vehicles to detect a variety of features in their environment, *e.g.*, signs, pedestrians, obstacles, etc. An adversarial action entails interfering with the sensory data either to prevent delivery of information through a specific sensory channel (*e.g.*, jamming attacks) or to create incorrect sensory data (*e.g.*, spoofing attacks). In this paper, we consider ultrasonic sensors, *i.e.*, sensors that operate primarily by emitting ultrasounds. Spoofing attack involves emitting ultrasound pulses identical to the victim ultrasonic sensor [3]; the victim vehicle will interpret the spoofing signals the same way as the reflected signals resulting in false detection of obstacles. Jamming involves producing an external interference signal capable of overpowering the actual ones; if the jamming signal is stronger than the victim sensor, the echo will be unable to overcome the high threshold, and the victim sensor will not receive any echo.

There has been significant research on ranging sensor attacks in vehicular systems. Yan *et al.* [4] shows how to compromise sensors in actual vehicles through jamming and spoofing. Lim *et al.* [5] develop an experimental environment where they demonstrate an attack that jeopardizes the accuracy of the ultrasound sensor leading to object detection failure. Petit *et al.* [6] show jamming, spoofing, blinding, and replay attacks remotely on Lidar and camera-based systems using commodity hardware.

III. REQUIREMENTS AND CHALLENGES IN EXPLORATION PLATFORMS

In spite of significant literature on sensor attacks, we have not found a platform that can be used as a hands-on exploration platform to learn how to conduct such attacks. Note that developing a useful pedagogical experimental platform that lets a new user get an overall sense of the attack and its impact is different from a demonstration of an attack by an expert. Obviously, unlike many real attacks, it is not possible to use actual vehicles. Apart from being economically infeasible, it is ineffective for learning: a modern vehicle includes the interplay of a variety of safety guard-bands to ensure that a compromise of a component does not render the entire system vulnerable; this makes it non-trivial for someone unfamiliar

*This research has been supported in part by the National Science Foundation under Grant No. CNS-1908549.

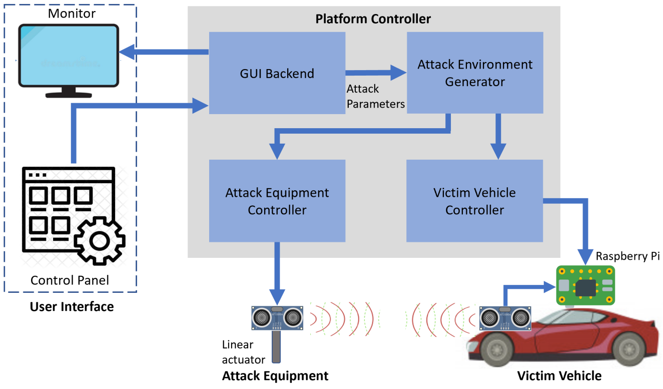

Figure 1. AutoHaL high-level architecture

without deep insight into the complete functionality get an intuitive understanding of an attack. Second, a platform must provide *controlled guidance* to the user. A sensor attack involves tweaking multiple parameters including sensor frequency, position, distance from the user, etc. A user attempting an attack would likely not be successful on the first try; even experts typically have to perform several trials before successfully compromising a sensor. When an attempt fails, the platform must provide effective feedback while letting the user continue to play with the attack. In particular, the platform must allow the user to tweak a broad (and sometimes unanticipated) range of parameter values, even those that do not result in any security compromise or even a well-defined behavior of the victim vehicle. Finally, the platform must provide configurability and extensibility so that the platform is reusable for a variety of attacks.

IV. AutoHaL Design

Fig. 1 shows the high-level architecture of AutoHaL. It includes (1) *User Interface Panel* that enables the user to tweak the various attack parameters and obtain feedback, *e.g.*, observe interference patterns created by programming the sensor position and frequency for specific values; (2) *Physical Attack Environment* that comprises of the attacker sensor to perform jamming or spoofing and a victim vehicle proxy that includes a mobile agent with a ranging sensor attached that is the target of the attack; and (3) *Platform Controller* that provides the coordination between the user interface and the physical attack environment, *e.g.*, translates user directives on sensor frequencies to program the physical sensors, propagates the impacted interference patterns to the user interface panel, and identifies how the deviations between the parameters provided by the user from the ones required for an actual compromise (if the attack fails). The AutoHaL implementation realizes the victim proxy through a PiCar-V, an open-source robot learning platform based on Raspberry Pi. It runs a dual-motor propulsion system on the rear wheels and has a four-bar steering mechanism that is actuated by a servo motor. These mechanical features are sufficient for the vehicle to follow the kinematics of a real vehicle. The distance sensor used is a commercially available ultrasonic sensor HC-SR04 with a range capability of 2cm to 4m [7]. ***The system can permit effective exploration of a spectrum of jamming and spoofing attacks through the configuration of sensor parameters as well as the position of the attacker relative to the victim vehicle.*** The user can explore these attacks by tweaking parameters through the interface panel without requiring the expertise of sensor technology.

We conclude the description of the AutoHaL setup with one representative design challenge, *viz.*, inconsistencies in the underlying computing system technologies, to illustrate the complexities involved in developing such exploration platforms. The victim proxy vehicle in AutoHaL uses a Raspberry Pi supporting on-board sensors that are built with an Arduino microcontroller. The attacker equipment also has used a heterogeneous combination of components. The heterogeneity is critical to AutoHaL's flexibility in developing a multitude of exploration scenarios. However, this leads to mismatched clock frequencies and inconsistent program execution time as a result of interpreter/compiler differences. A naive implementation that does not account for synchronization among these components would result in highly non-deterministic behavior in the platform. AutoHaL manages these inconsistencies by carefully controlling the throughput of high-frequency components to achieve system-level synchronization.

V. Conclusion

Ranging sensors are used by vehicles to detect a variety of features in their environment. In this paper, we have described a platform, AutoHaL, that enables the user to explore and comprehend attacks on ranging sensors, including spoofing and jamming attacks. AutoHaL can be used for teaching automotive security to students new to automotive, and also to train industry professionals familiar with automotive system functionality but unfamiliar with security.

In future work, we plan to extend AutoHaL to handle exploration of more sophisticated sensor attacks and extend the platform to automotive-grade sensors to enable exploration of vulnerabilities in current on-road automobiles.

References

[1] C. H. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, p. 91, 2015.

[2] C. Hempfield, "Why a Cybersecurity Solution for Driverless Cars May be Found Under the Hood," 2017, https://techcrunch.com/2017/02/18/why-a-cybersecurity-solution-for-driverless-cars-may-be-found-under-the-hood.

[3] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu, "Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5015–5029, 2018.

[4] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *Def Con*, vol. 24, no. 8, p. 109, 2016.

[5] B. S. Lim, S. L. Keoh, and V. L. Thing, "Autonomous vehicle ultrasonic sensor vulnerability and impact assessment," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. IEEE, 2018, pp. 231–236.

[6] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," *Black Hat Europe*, vol. 11, no. 2015, p. 995, 2015.

[7] "Ultrasonic ranging module hc - sr04." [Online]. Available: https://cdn.sparkfun.com/datasheets/Sensors/Proximity/HCSR04.pdf