Poster: Scenario Creation for Immersive Automotive Security Exploration

Aidan Kwok
Colby College
Waterville, Maine, USA
adkwok26@colby.edu

Richard Owoputi
University of Florida
Gainesville, Florida, USA
rowoputi@ufl.edu

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

ABSTRACT

Modern autonomous vehicles are increasingly infused with sensors, electronics, and software software. One consequence is that they are getting increasingly susceptible to cyber-attacks. However, awareness of cybersecurity challenges for automotive systems remains low. In this paper, we consider the problem of developing a virtual reality (VR) infrastructure that can enable users who are not necessarily experts in automotive security to explore vulnerabilities arising from compromised ranging sensors. A key requirement for such platforms is to develop natural, intuitive scenarios that enable the user to experience security challenges and impact. We discuss the challenges in developing such scenarios, and develop a solution that enables exploration of jamming and spoofing attacks. Our solution is integrated into a VR platform for automotive security exploration called IVE (Immersive Virtual Environment). It combines realistic driving with a first-person view, user interaction, and sound effects to provide all the benefits of a real-life simulation without the consequences.

CCS CONCEPTS

• **Security and privacy → Denial-of-service attacks**; **Usability in security and privacy**.

KEYWORDS

Virtual reality, Cybersecurity, Immersive learning, Autonomous vehicles

ACM Reference Format:
Aidan Kwok, Richard Owoputi, and Sandip Ray. 2023. Poster: Scenario Creation for Immersive Automotive Security Exploration. 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/10.1145/3565287.3617978

1 INTRODUCTION

Modern automotive systems have been infused with electronics, software, and sensors over the recent years, targeted to improve autonomy, increase road safety, and better utilize the transportation infrastructure. However, one unfortunate upshot of this phenomenon is the significant increase in the vulnerability of these systems to cyber-attacks. Recent research has shown that it is possible, — even easy in many cases, — to compromise a vehicular system and cause catastrophic accidents [1, 6, 8].

However, despite such demonstrations, the understanding of the scope of vehicular security remains limited, even among researchers in security and researchers and practitioners in automotive system design. A critical bottleneck for the community to comprehend cybersecurity challenges in automotive systems is the need for a platform that enables hands-on exploration of automotive security vulnerabilities.

Previous work introduced an exploration platform called IVE, which used Virtual Reality (VR) to enable hands-on exploration of attacks on ranging sensors in automotive systems [9]. It introduced a dual-view environment to capture both the victim's and hacker's perspectives and incorporated intuitive environment designs to provide an immersive experience for the user. However, in spite of these features, the evaluation of the approach was reported to be lukewarm. A key problem with IVE, as pointed to by user feedback, was the limited diversity in attack scenarios and limited set of options provided to the user to tweak and configure the system.

This paper addresses this problem by creating rich, immersive environments that enable users to comprehend sensory attacks in vehicle-to-vehicle interactions. We discuss challenges and approaches for introducing diverse environmental scenarios and interactive elements in such platforms, as well as potential pitfalls involved in the process.

2 OVERVIEW OF IVE

IVE stands for "Immersive Virtual Environment". It is a platform designed to familiarize users with jamming attacks on autonomous automotive systems, with a special emphasis on ultrasonic sensors. These sensors assist vehicles in creating an accurate perception of their surroundings. An attacker can drive the vehicle into dangerous or ineffective maneuvers by feeding misleading or incorrect sensor values. The uniqueness of IVE lies in its incorporation of VR infrastructure, offering users a hands-on experience with diverse automotive security breaches. This simulates real-world operational processes, and to our awareness, IVE stands as the first platform leveraging VR for automotive security education. Following is a summary of key features of IVE.

(1) **User Experience**: Users step into the shoes of an attacker inside a virtual autonomous vehicle. This unique perspective allows them to both initiate and witness the consequences of their attacks.

MobiHoc '23, October 23–26, 2023, Washington, DC, USA

ACM ISBN 978-1-4503-9926-5/23/10…$15.00
https://doi.org/10.1145/3565287.3617978

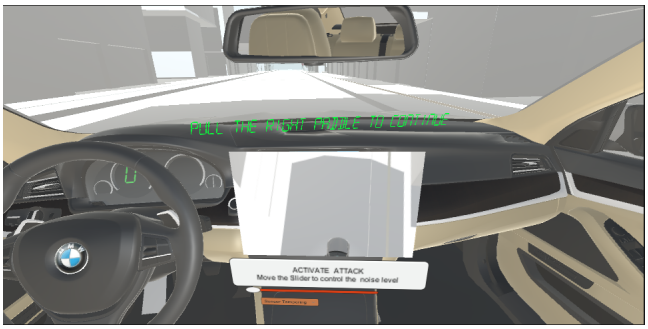

Figure 1: The Dashboard and Windshield View with IVE

(2) **Dual Views**: IVE enables the user to distinguish ground truth from the perception of vehicles under attack through two views:
- *Dashboard View*: Shows the vehicle's understanding (the car TV screen as shown in Fig. 1).
- *Windshield View*: Gives a first-person perspective, showcasing the real-world scenario (as shown in Fig. 1).

(3) **Interactive Controls**: The virtual dashboard of IVE is equipped with a slider, enabling users to tweak the noise of the attack and see the effects.

(4) **Real-world Simulation**: The virtual scenarios closely match real-world outcomes. For instance, if a user alters a sensor's frequency in a non-standard way, IVE will still realistically depict the outcome on the targeted vehicle. To achieve this accuracy, we model the effects of hardware sensors into the virtual environment.

Shortcomings. In spite of its success as the first platform for enabling automotive security exploration through a VR environment, IVE had several shortcomings which became apparent from user feedback. One critical feedback was that since the user was provided a single slider to choose the intensity and noise level of attack, the environment was too simplistic from the perspective of the user gaining knowledge regarding the practical intricacies of the attacks and parameters controlled by a hacker attempting to compromise an actual vehicle. Thus, the scenario was deemed too simplistic and did not necessarily capture the nuances of the real-world experience. Furthermore, if an attack was successful, its impact was not immediately evident on the platform. The oncoming car, positioned to the player's right, was only visible if the player happened to glance that way upon entering the intersection. Players often remained unaware of an imminent collision until it was too late. This design failed to replicate the genuine anxiety a driver would experience, seeing a potential crash but being powerless to prevent it.

3 RESEARCH CHALLENGES AND APPROACH TO SCENARIO DESIGN

The above discussion on the limitation of IVE also points to a key challenge in the design of an immersive virtual environment for automotive security exploration: how to ensure that the user gets an intuitive experience of security compromises and their impact in a way that reflects what they would experience in the real world while not getting overwhelmed by the high complexity of vehicular design and the sheer number of sensory and environmental parameters that the hacker needs to configure and control to generate a successful attack.

To enable effective navigation of this question, we systematically deconstruct what a user may reasonably expect to achieve through the usage of a platform like IVE. Roughly, the expectations can be classified into the following categories.

- **Knowledge:** The platform should enable the user to get knowledge and understanding of the domain. For IVE, the platform should help the user understand the purpose of a ranging sensor in an autonomous vehicle, provide insights into how attackers can manipulate sensor values to mislead/compromise autonomous vehicles, and highlight the potential consequences of a successful attack on a ranging sensor.
- **Usability:** The platform should be easy to use, and the notifications and feedback provided by the system should accurately convey the progress of the attack. More importantly, the user should be able to freely navigate and explore the virtual environment, experiencing a sense of agency and control over actions and movements.
- **Engagement:** It should maintain a balanced level of challenge and difficulty in the attack scenario, ensuring engagement without becoming excessively frustrating or overwhelming.

4 SCENARIO DESIGN

We have extended IVE with scenarios to systematically address the constraints mentioned above. This ensures that the appropriate knowledge is incorporated while also fulfilling the engagement requirement by decoupling the views of the victim and the attacker. In particular, recall that IVE included one unified view for the attacker and the victim, where the role of the user is as an attacker sitting in the vehicle and experiencing the effect. This requires the user to have limited attack reconfigurability since only a limited set of vehicle-to-infrastructure attacks are consistent with this scenario. By separating the attacker role from the victim role, we can introduce different knowledge components in different roles while not worrying about the user being overwhelmed with too many parameter settings in one role.

Note that it is still critical that the scenarios are reflective of the experience the user has in practice. We achieve this by permitting attacks via parameter settings that have resulted in successful attacks in real life, e.g., we use attack parameters that correspond to actual attacks on Tesla (see below).

In more detail, the following is a summary of the scenarios created for the VR environment.

Environmental Setup. The two cars travel along a city street to maintain the required 10-meter distance for a successful attack. In the hacker's view, the jammer is strategically aligned with the victim vehicle's ultrasonic sensor to facilitate the attack.

Scenario 1: The Victim's Perspective. In this scenario, the user plays the victim role and receives no indication that their vehicle

will be hacked. When the vehicle's sensors jam, its display screen turns white, as seen in Fig 2a, alerting the player of an attack and symbolizing the vehicle's inability to detect its surroundings. This captures the actual behavior of the ultrasonic sensors under an attack, where they perceive no objects in the vicinity. To improve user interaction, users can press "A" on the Oculus controller to switch the car to manual mode and then "B" to stop their vehicle to avoid collision.

(a) Victim's Perspective **(b) Attacker's Perspective**

Figure 2: Two Perspectives for Attack.

Scenario 2: The Attacker's Perspective. Here, the user takes control of a jammer. Following are the requirements for the attacker to perform a successful jamming attack.

- The jammer's frequency needs to match that of the ultrasonic sensor, which operates between 40-50 kHZ [10].
- The jammer should be within 10 meters of the ultrasonic sensors [10], where they successfully attacked a Tesla from this range using a jammer with a voltage of 20 volts.
- The jammer must have a higher voltage power than the ultrasonic sensor since the amplitude (strength) of the waves is proportional to the voltage.
- The jammer should be aimed directly at the sensor to ensure its pulses reach and overpower the sensor's waves.

A side view is provided to assist users in aligning the jammer's frequency with the car's frequency, as seen in Fig. 2b. If the user succeeds in this hacking scenario, a collision occurs when the two vehicles reach a stop sign. This is due to the victim's vehicle being unable to detect the hacker's vehicle due to the jamming.

5 RELATED WORK

Recently, VR technologies have been leveraged to facilitate individuals in understanding models, systems, or scenarios by emulating authentic experiences in a more controlled, risk-free setting [2]. Immersive Virtual Reality (I-VR) has gained traction as an instructional tool in the educational sector. [4] analyzed 69 studies, focusing on their demographics, educational themes, benefits of VR in education, and software development traits. The standout observation was the emphasis on personalization in VR app development, particularly through gamification. Combining VR with gamified and adaptive design holds promise for impactful educational experiences. [5] looked into how different VR tools, like games, simulations, and virtual worlds, can be used in education. [3] developed an educational VR activity based on interactive molecular dynamics in virtual reality (iMD-VR), which allows for real-time, immersive interactions with a dynamic molecular world. These VR games let users step into and explore virtual places, making learning more interactive [7].

6 CONCLUSION AND FUTURE WORK

We have extended the IVE platform with scenarios to enable intuitive understanding and exploration of ranging sensor attacks. Developing scenarios for effective, immersive experiences through a VR platform requires balancing different factors targeting knowledge, usability, and engagement. We discuss the challenges involved in achieving this balance and discuss scenarios we created on IVE to enable exploration of the role of ranging sensors during vehicle-to-vehicle coordination together with corresponding cybersecurity implications and impact.

In future work, we plan to expand the platform's capabilities further. Potential enhancements include introducing scenarios where users must control their car's speed to maintain the 10-meter gap, dictate the sensor's voltage, or manually aim the jammer at the sensor. These additions will make the platform more immersive and provide users with a deeper understanding of the complexities involved in such attack scenarios.

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

REFERENCES

[1] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. Comprehensive experimental analyses of automotive attack surfaces. In *20th USENIX security symposium (USENIX Security 11)*.

[2] Yogesh K Dwivedi, Laurie Hughes, Abdullah M Baabdullah, Samuel Ribeiro-Navarrete, Mihalis Giannakis, Mutaz M Al-Debei, Denis Dennehy, Bhimaraya Metri, Dimitrios Buhalis, Christy MK Cheung, et al. 2022. Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management* 66 (2022), 102542.

[3] Jonathon B Ferrell, Joseph P Campbell, Dillon R McCarthy, Kyle T McKay, Magenta Hensinger, Ramya Srinivasan, Xiaochuan Zhao, Alexander Wurthmann, Jianing Li, and Severin T Schneebeli. 2019. Chemical exploration with virtual reality in organic teaching laboratories. *Journal of Chemical Education* 96, 9 (2019), 1961–1966.

[4] Andreas Marougkas, Christos Troussas, Akrivi Krouska, and Cleo Sgouropoulou. 2023. How personalized and effective is immersive virtual reality in education? A systematic literature review for the last decade. *Multimedia Tools and Applications* (2023), 1–49.

[5] Zahira Merchant, Ernest T Goetz, Lauren Cifuentes, Wendy Keeney-Kennicutt, and Trina J Davis. 2014. Effectiveness of virtual reality-based instruction on students' learning outcomes in K-12 and higher education: A meta-analysis. *Computers & Education* 70 (2014), 29–40.

[6] Charlie Miller. 2019. Lessons learned from hacking a car. *IEEE Design & Test* 36, 6 (2019), 7–9.

[7] Kylie Peppler and Yasmin Kafai. 2007. What videogame making can teach us about literacy and learning: Alternative pathways into participatory culture. (2007).

[8] Christian Plappert, Florian Fenzl, Roland Rieke, Ilaria Matteucci, Gianpiero Costantino, and Marco De Vincenzi. 2022. SECPAT: security patterns for resilient automotive E/E architectures. In *2022 30th Euromicro international conference on parallel, distributed and network-based processing (PDP)*. IEEE, 255–264.

[9] Owoputi Richard, Kabir Md Rafiul, and Ray Sandip. 2023. An Immersive Virtual Environment for Automotive Security Exploration. *9th International Conference of the Immersive Learning Research Network, iLRN 2023* 4 (2023). under submission.

[10] Wenyuan Xu, Chen Yan, Weibin Jia, Xiaoyu Ji, and Jianhao Liu. 2018. Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. *IEEE Internet of Things Journal* 5, 6 (2018), 5015–5029.