Associate Professorship of Embedded Systems and Internet of Things
Department of Electrical and Computer Engineering
Technical University of Munich

Security Evaluation of Autonomous Vehicle Software Frameworks

Supervisor: Andrew Roberts and Dr.-Ing. Mohammad Hamad
Period: 24 Weeks
Start Date: ASAP
Type: Master's Thesis

Context

Autonomous Vehicle open-source software frameworks, such as Autoware, are widely used to support algorithm development for Autonomous Driving (AD). Existing security evaluation studies are focussed on testing unsanitised input on the cyber-physical features of the AD control algorithm [2]. Examples include, adversarial robust invariants for object-detection to manipulate the computer vision of the camera and distributed-denial-of-service attacks on LiDAR sensors. Yet, there is lack of evaluation of the security of the underlying code base which supports autonomous driving and an understanding of how vulnerabilities at the "cyber-layer" of the AD system can cause physical effects [3]. The study by Garcia et al. [1] is the closest to this topic, however, since this work was published, there have been numerous updates to autonomous vehicle software frameworks and a wider usage of diverse software frameworks. The aim of this study is to evaluate vulnerabilities in diverse autonomous vehicle software ecosystems through experimentation with diverse fuzzing tools and strategies. The overall aim is to assess the validity of Garcia et al. [1] in existing systems and to enhance it by developing efficient software security evaluation methods and tools.

Requirements

- **High motivation** for exploring Autonomous Driving security
- **Very good** programming skills: Python or C++
- a **Good** understanding of security (in general) and automotive security
- Knowledge of popular fuzzing tools, such as AFL, is a **plus**
- Experience in penetration testing is a **plus**

Are you Interested?

please send your full application (CV, current transcript of records) to (mohammad.hamad@tum.de).

References

[1] J. Garcia, Y. Feng, J. Shen, S. Almanee, Y. Xia, Chen, and Q. Alfred. A comprehensive study of autonomous vehicle bugs. In *Proceedings of the ACM/IEEE 42nd international conference on software engineering*, pages 385–396, 2020.

[2] S. Kim, M. Liu, J. J. Rhee, Y. Jeon, Y. Kwon, and C. H. Kim. Drivefuzz: Discovering autonomous driving bugs through driving quality-guided fuzzing. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 1753–1767, 2022.

[3] J. Shen, N. Wang, Z. Wan, Y. Luo, T. Sato, Z. Hu, X. Zhang, S. Guo, Z. Zhong, K. Li, et al. Sok: On the semantic ai security in autonomous driving. *arXiv preprint arXiv:2203.05314*, 2022.