References

[1]

[2] amcl - ROS Wiki. https:/wiki.ros.org/amcl.

[3] Tesla Autopilot. https://www.tesla.com/autopilot.

[4] Uber Advanced Technologies Group. https://www.uber.com/info/atg.

[5] Waymo. https://www.waymo.com.

[6] Zipline. https://www.flyzipline.com.

[7] H. Choi, Z. Cheng, and X. Zhang. Rvplayer: Robotic vehicle forensics by replay with what-if reasoning. In *2022 Network and Distributed System Security (NDSS) Symposium 2022*, 2022.

[8] D. Fox. Adapting the sample size in particle filters through KLD-sampling. *The International Journal of Robotics Research*, 22(12):985–1003, 2003.

[9] A. Garg and N. Karimian. Leveraging deep cnn and transfer learning for side-channel attack. In *2021 22nd International Symposium on Quality Electronic Design (ISQED)*, pages 91–96. IEEE, 2021.

[10] L. He and K. G. Shin. Battery-enabled anti-theft vehicle immobilizer. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services*, pages 142–154, 2022.

[11] M. A. Hoque and R. Hasan. Avguard: A forensic investigation framework for autonomous vehicles. In *ICC 2021-IEEE International Conference on Communications*, pages 1–6. IEEE, 2021.

[12] A. Li, J. Wang, and N. Zhang. Chronos: Timing interference as a new attack vector on autonomous cyber-physical systems. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 2426–2428, 2021.

[13] D. A. Osvik, A. Shamir, and E. Tromer. Cache attacks and countermeasures: the case of AES. In *Cryptographers' Track at the RSA Conference*, pages 1–20. Springer, 2006.

[14] M. Song, J. Lee, T. Suh, and G. Koo. Rt-sniper: A low-overhead defense mechanism pinpointing cache side-channel attacks. *Electronics*, 10(22):2748, 2021.

[15] D. Stabili, L. Ferretti, M. Andreolini, and M. Marchetti. Daga: Detecting attacks to in-vehicle networks via n-gram analysis. *IEEE Transactions on Vehicular Technology*, 2022.

[16] J. Sun, Y. Cao, Q. A. Chen, and Z. M. Mao. Towards robust {LiDAR-based} perception in autonomous driving: General black-box adversarial sensor attack and countermeasures. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 877–894, 2020.

[17] H. Wang. *Applied Machine Learning for Analyzing and Defending against Side Channel Threats*. PhD thesis, UNIVERSITY OF CALIFORNIA DAVIS, 2022.

[18] H. Wang, S. M. Hafiz, K. Patwari, C.-N. Chuah, Z. Shafiq, and H. Homayoun. Stealthy inference attack on dnn via cache-based side-channel attacks. In *2022 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1515–1520. IEEE, 2022.

[19] H. Wang, S. Salehi, H. Sayadi, A. Sasan, T. Mohsenin, P. S. Manoj, S. Rafatirad, and H. Homayoun. Evaluation of machine learning-based detection against side-channel attacks on autonomous vehicle. In *2021 IEEE 3rd International Conference on Artificial Intelligence Circuits and Systems (AICAS)*, pages 1–4. IEEE, 2021.