References

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

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

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

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

[5] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *20th USENIX security symposium (USENIX Security 11)*, 2011.

[6] 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.

[7] M. Enev, A. Takakuwa, K. Koscher, and T. Kohno. Automobile driver fingerprinting. *Proc. Priv. Enhancing Technol.*, 2016(1):34–50, 2016.

[8] 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.

[9] 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.

[10] 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.

[11] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, et al. Experimental security analysis of a modern automobile. In *2010 IEEE symposium on security and privacy*, pages 447–462. IEEE, 2010.

[12] J. Liu, J. Corbett-Davies, A. Ferraiuolo, A. Ivanov, M. Luo, G. E. Suh, A. C. Myers, and M. Campbell. Secure autonomous cyber-physical systems through verifiable information flow control. In *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, pages 48–59, 2018.

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

[14] 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.

[15] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Europe*, 11(2015):995, 2015.

[16] G. Saileshwar and M. Qureshi. {MIRAGE}: Mitigating {Conflict-Based} cache attacks with a practical {Fully-Associative} design. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 1379–1396, 2021.

[17] T. Sato, J. Shen, N. Wang, Y. Jia, X. Lin, and Q. A. Chen. Dirty road can attack: Security of deep learning based automated lane centering under {Physical-World} attack. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3309–3326, 2021.

[18] 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.

[19] 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.

[20] N. Vasilakis, A. Benetopoulos, S. Handa, A. Schoen, J. Shen, and M. C. Rinard. Supply-chain vulnerability elimination via active learning and regeneration. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1755–1770, 2021.

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

[22] 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.

[23] 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.

[24] Y. Xun, J. Liu, N. Kato, Y. Fang, and Y. Zhang. Automobile driver fingerprinting: A new machine learning based authentication scheme. *IEEE Transactions on Industrial Informatics*, 16(2):1417–1426, 2019.

[25] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang. All your {GPS} are belong to us: Towards stealthy manipulation of road navigation systems. In *27th USENIX security symposium (USENIX security 18)*, pages 1527–1544, 2018.