[10] 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 USENIX Security Symposium, Vol. 4. San Francisco, 2021.

[3] Aiman Al-Sabaawi, Khamael Al-Dulaimi, Ernest Foo, and Mamoun Alazab. 2021. Addressing malware attacks on

connected and autonomous vehicles: Recent techniques and challenges. Malware Analysis using Artificial Intelligence

and Deep Learning (2021), 97–119.

[23] Shah Khalid Khan, Nirajan Shiwakoti, Peter Stasinopoulos, and Yilun Chen. 2020. Cyber-attacks in the next-generation

cars, mitigation techniques, anticipated readiness and future directions. Accident Analysis & Prevention 148 (2020),

105837.

[14] Zeinab El-Rewini, Karthikeyan Sadatsharan, Niroop Sugunaraj, Daisy Flora Selvaraj, Siby Jose Plathottam, and

Prakash Ranganathan. 2020. Cybersecurity attacks in vehicular sensors. IEEE Sensors Journal 20, 22 (2020), 13752–

13767.

[45] Bas G. B. Stottelaar. 2015. Practical Cyber-Attacks on Autonomous Vehicles. Master’s thesis. University of Twente.

[12] Ludvig Christensen and Daniel Dannberg. 2019. Ethical hacking of IoT devices: OBD-II dongles.

[8] Yulong Cao, Chaowei Xiao, Dawei Yang, Jing Fang, Ruigang Yang, Mingyan Liu, and Bo Li. 2019. Adversarial objects

against LiDAR-based autonomous driving systems. arXiv preprint arXiv:1907.05418 (2019).

[31] Athanasios Moschos, Kevin Valakuzhy, and Angelos D. Keromytis. 2022. On the feasibility of remotely triggered auto-

motive hardware trojans. In 2022 International Conference on Electrical, Computer, Communications and Mechatronics

Engineering (ICECCME). IEEE, 1–6.

[13] Riccardo Coppola and Maurizio Morisio. 2016. Connected car: Technologies, issues, future trends. ACM Comput. Surv.

49, 3, Article 46 (Oct. 2016), 36 pages. https://doi.org/10.1145/2971482