

Forensische Untersuchung autonomer Fahrzeuge

Gleumes, Folke Henning
Hochschule Mannheim
Fakultät für Informatik
Paul-Wittsack-Str. 10, 68163 Mannheim

Zusammenfassung—

Inhaltsverzeichnis

1	Einleitung	1
2	Angriffe auf Autonome Fahrzeuge	1
2.1	Physish	1
2.2	Intern Digital	1
2.3	Extern Digital	1
3	Übersicht bisheriger forensischer Methoden	1
4	Ansätze für zukünftige forensischer Methoden	1
5	Fazit	1
	Abkürzungen	1
	Literatur	1
1.	Einleitung	
2.	Angriffe auf Autonome Fahrzeuge	
2.1.	Physish	
2.2.	Intern Digital	
2.3.	Extern Digital	
3.	Übersicht bisheriger forensischer Methoden	
4.	Ansätze für zukünftige forensischer Methoden	
5.	Fazit	
	Abkürzungen	

Literatur

- [1] C. Lauterwasser, M. Kreutner und O. Braxmeier, „Unfallaufklärung als Grundlage für sichere Fahrzeugautomatisierung“, *ATZextra*, Jg. 26, Nr. 1, S. 32–35, 2021. DOI: 10.1007/s35778-021-0473-4. Adresse: <https://doi.org/10.1007/s35778-021-0473-4>.
- [2] Z. A. Baig et al., „Future challenges for smart cities: Cyber-security and digital forensics“, *Digital Investigation*, Jg. 22, S. 3–13, 2017. DOI: 10.1016/j.diin.2017.06.015. Adresse: <https://www.sciencedirect.com/science/article/pii/S1742287617300579>.
- [3] K. K. Gomez Buquerin, C. Corbett und H.-J. Hof, „A generalized approach to automotive forensics“, *Forensic Science International: Digital Investigation*, Jg. 36, S. 301 111, 2021. DOI: 10.1016/j.fsidi.2021.301111. Adresse: <https://www.sciencedirect.com/science/article/pii/S2666281721000056>.
- [4] F. Akowuah und F. Kong, „Physical Invariant Based Attack Detection for Autonomous Vehicles: Survey, Vision, and Challenges“, in *2021 Fourth International Conference on Connected and Autonomous Driving (MetroCAD)*, 2021, S. 31–40. DOI: 10.1109/MetroCAD51599.2021.00014.
- [5] C. Gao, G. Wang, W. Shi, Z. Wang und Y. Chen, „Autonomous Driving Security: State of the Art and Challenges“, *IEEE Internet of Things Journal*, S. 1–1, 2021. DOI: 10.1109/JIOT.2021.3130054.
- [6] M. A. Hoque und R. Hasan, „AVGuard: A Forensic Investigation Framework for Autonomous Vehicles“, in *ICC 2021 - IEEE International Conference on Communications*, IEEE, Juni 2021. DOI: 10.1109/icc42927.2021.9500652.
- [7] S. Lee, W. Choi, H. J. Jo und D. H. Lee, „T-Box: A Forensics-Enabled Trusted Automotive Data Recording Method“, *IEEE Access*, Jg. 7, S. 49 738–49 755, 2019. DOI: 10.1109/ACCESS.2019.2910865.
- [8] S. Kim und R. Shrestha, *Automotive Cyber Security*. Springer Singapore, 2020. DOI: 10.1007/978-981-15-8053-6.
- [9] K. Kim, J. S. Kim, S. Jeong, J.-H. Park und H. K. Kim, „Cybersecurity for autonomous vehicles: Review of attacks and defense“, *Computers and Security*, Jg. 103, S. 102 150, 2021. DOI: 10.1016/j.cose.2020.102150. Adresse: <https://www.sciencedirect.com/science/article/pii/S0167404820304235>.

- [10] C. Yan, „Can You Trust Autonomous Vehicles : Contactless Attacks against Sensors of Self-driving Vehicle“, 2016.
- [11] J. Botaschanjan, L. Kof, C. Kühnel und M. Spichkova, „Towards Verified Automotive Software“, *SIGSOFT Softw. Eng. Notes*, Jg. 30, Nr. 4, S. 1–6, Mai 2005. DOI: 10.1145/1082983.1083199. Adresse: <https://doi.org/10.1145/1082983.1083199>.
- [12] D. Kopencova und R. Rak, „Issues of Vehicle Digital Forensics“, in *2020 XII International Science-Technical Conference AUTOMOTIVE SAFETY*, 2020, S. 1–6. DOI: 10.1109 / AUTOMOTIVESAFETY47494.2020.9293516.