one standard CAN node and one where CANflict is implemented, showing that our techniques heavily reduce the computational requirements for link-layer attacks, enabling such attacks from remote on low-end microcontrollers. Moreover, we proved the effectiveness of CANflict even with partial conflicting peripherals by implementing a targeted denial of service attack that uses SPI and I2C to respectively read and write on the bus. Finally, we evaluated the compatibility of polyglot frames between real-world CAN traffic and the UART and I2C protocols. We provide the community the CANflict framework to enable the implementation of our approach on different platforms and peripherals through an easy-to-use and expandable interface. Future works will focus on extending the framework with new platforms and new peripherals, evaluating the feasibility of applying our intuitions on other protocols aside CAN, and in the design of data-link layer countermeasures to detect CAN attacks through the use of CANflict.

## ACKNOWLEDGEMENTS

This work was supported by the Dutch Science Organization NWO through project Intersect.

## REFERENCES


[1] Omar Y. Al-Jarrah, Carsten Maple, Mehrdad Dianati, David Oxtoby, and Alex Mouzakitis. 2019. Intrusion Detection Systems for Intra-Vehicle Networks: A Review. *IEEE Access* 7 (2019), 21266–21289. https://doi.org/10.1109/ACCESS.2019.2894183

[2] Ange Albertini. 2014. This PDF is a JPEG; or, This Proof of Concept is a Picture of Cats. *PoC or GTFO 0x03* (2014).

[3] Gedare Bloom. 2021. WeepingCAN: A Stealthy CAN Bus-off Attack. *Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021* 2021 (02 2021). https://doi.org/10.14722/autosec.2021.23002

[4] Mehmet Bozdal, Mohammad Samie, Sohaib Aslam, and Ian Jennions. 2020. Evaluation of CAN Bus Security Challenges. *Sensors* 20, 8 (2020). https://doi.org/10.3390/s20082364

[5] Mehmet Bozdal, Mohammad Samie, and Ian Jennions. 2018. A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions. In *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*. 201–205. https://doi.org/10.1109/iCCECOME.2018.8658720

[6] Sergey Bratus, Travis Goodspeed, Ange Albertini, and Debanjum S. Solanky. 2016. Fillory of PHY: Toward a Periodic Table of Signal Corruption Exploits and Polyglots in Digital Radio. In *10th USENIX Workshop on Offensive Technologies, WOOT 16, Austin, TX, USA, August 8-9, 2016.*

[7] Tim Brom. 2018. *CANT.* https://github.com/bitbane/CANT

[8] 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 *Proceedings of the 20th USENIX Conference on Security* (San Francisco, CA) *(SEC'11)*. USA, 6.

[9] Kyong-Tak Cho and Kang G. Shin. 2016. Error Handling of In-Vehicle Networks Makes Them Vulnerable. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (Vienna, Austria) *(CCS '16)*. 1044–1055. https://doi.org/10.1145/2976749.2978302

[10] Kyong-Tak Cho and Kang G. Shin. 2017. Viden: Attacker Identification on In-Vehicle Networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (Dallas, Texas, USA) *(CCS '17)*. 1109–1123. https://doi.org/10.1145/3133956.3134001

[11] Wonsuk Choi, Kyungho Joo, Hyo Jin Jo, Moon Chan Park, and Dong Hoon Lee. 2018. VoltageIDS: Low-Level Communication Characteristics for Automotive Intrusion Detection System. *IEEE Transactions on Information Forensics and Security* 13, 8 (2018), 2114–2129. https://doi.org/10.1109/TIFS.2018.2812149

[12] John Donovan. 2014. What Engineers Need to Know When Selecting an Automotive-Qualified MCU for Vehicle Applications. https://www.digikey.com/en/articles/what-engineers-need-to-know-when-selecting-an-automotive-qualified-mcu-for-vehicle-applications

[13] Bernd Elend and Tony Adamson. 2017. Cyber security enhancing CAN transceivers. In *Proceedings of the 16th International CAN Conference.*

[14] Markus Hanselmann, Thilo Strauss, Katharina Dormann, and Holger Ulmer. 2020. CANet: An Unsupervised Intrusion Detection System for High Dimensional CAN Bus Data. *IEEE Access* 8 (2020), 58194–58205.

[15] Infineon. 2022. SAK-TC399XP MCU. https://www.infineon.com/cms/en/product/microcontroller/32-bit-tricore-microcontroller/32-bit-tricore-aurix-tc3xx/aurix-family-tc39xxx/sak-tc399xp-256f300s-bd/

[16] ISO Central Secretary. 2003. *Road vehicles — Controller area network (CAN) — Part 2: High-speed medium access unit.* Standard ISO 11898-2:2003. International Organization for Standardization, Geneva, CH. https://www.iso.org/standard/33423.html

[17] KeenLab Security. 2018. Experimental Security Assessment of BMW Cars.

[18] Kaveh Bakhsh Kelarestaghi, Mahsa Foruhandeh, Kevin Heaslip, and Ryan Gerdes. 2021. Intelligent Transportation System Security: Impact-Oriented Risk Assessment of in-Vehicle Networks. *IEEE Intelligent Transportation Systems Magazine* 13, 2 (2021), 91–104. https://doi.org/10.1109/MITS.2018.2889714

[19] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. 2010. Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy*. IEEE, 447–462.

[20] Sekar Kulandaivel, Tushar Goyal, Arnav Kumar Agrawal, and Vyas Sekar. 2019. CANvas: Fast and Inexpensive Automotive Network Mapping. In *28th USENIX Security Symposium, USENIX Security 2019, Santa Clara, CA, USA, August 14-16, 2019*. 389–405.

[21] Sekar Kulandaivel, Shalabh Jain, Jorge Guajardo, and Vyas Sekar. 2021. CANNON: Reliable and Stealthy Remote Shutdown Attacks via Unaltered Automotive Microcontrollers. In *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, 195–210. https://doi.org/10.1109/SP40001.2021.00122

[22] Stefano Longari, Andrea Cannizzo, Michele Carminati, and Stefano Zanero. 2019. A secure-by-design framework for automotive on-board network risk analysis. In *2019 IEEE Vehicular Networking Conference (VNC)*. IEEE, 1–8.

[23] Stefano Longari, Matteo Penco, Michele Carminati, and Stefano Zanero. 2019. CopyCAN: An Error-Handling Protocol based Intrusion Detection System for Controller Area Network. In *Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy*. 39–50.

[24] Stefano Longari, Daniel Humberto Nova Valcarcel, Mattia Zago, Michele Carminati, and Stefano Zanero. 2020. CANnolo: An Anomaly Detection System based on LSTM Autoencoders for Controller Area Network. *IEEE Transactions on Network and Service Management* (2020).

[25] ST Microelectronics. 2022. STM32L5x2. https://www.st.com/en/microcontrollers-microprocessors/stm32l5x2.html

[26] Charlie Miller and Chris Valasek. 2013. Adventures in automotive networks and control units. *DEF CON* 21 (2013), 260–264.

[27] Charlie Miller and Chris Valasek. 2014. A survey of remote automotive attack surfaces. *Black Hat USA 2014* (2014).

[28] Charlie Miller and Chris Valasek. 2015. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA 2015* (2015).

[29] Pal-Stefan Murvay and Bogdan Groza. 2017. DoS Attacks on Controller Area Networks by Fault Injections from the Software Layer. In *Proceedings of the 12th International Conference on Availability, Reliability and Security* (Reggio Calabria, Italy) *(ARES '17)*. Article 71, 10 pages. https://doi.org/10.1145/3098954.3103174

[30] NXP. 2016. LPC11C00 microcontroller family. https://www.nxp.com/products/processors-and-microcontrollers/arm-microcontrollers/general-purpose-mcus/lpc1100-cortex-m0-plus-m0/scalable-entry-level-32-bit-microcontroller-mcu-based-on-arm-cortex-m0-cores:LPC11C00

[31] oshaw 2022. A Resolution to Redefine SPI Signal Names. https://www.oshwa.org/a-resolution-to-redefine-spi-signal-names/.

[32] Andrea Palanca, Eric Evenchick, Federico Maggi, and Stefano Zanero. 2017. A Stealth, Selective, Link-Layer Denial-of-Service Attack Against Automotive Networks. In *Detection of Intrusions and Malware, and Vulnerability Assessment - 14th International Conference, DIMVA 2017 (Lecture Notes in Computer Science, Vol. 10327)*. Springer, 185–206. https://doi.org/10.1007/978-3-319-60876-1_9

[33] polyglots 2013. Polyglots PoCs. https://github.com/corkami/pocs.

[34] NXP Semiconductors. 2019. NXP TJA115x Secure CAN Transceiver Family. https://www.nxp.com/docs/en/fact-sheet/SECURCANTRLFUS.pdf

[35] Yuefend Du Sen Nie, Ling Lie. 2017. Free-Fall: Hacking Tesla from Wireless to CAN Bus. In *Black Hat USA 2017.*

[36] IEEE Spectrum. 2020. How Software Is Eating the Car. https://spectrum.ieee.org/software-eating-car

[37] Ken Tindell. 2020. CANhack. https://github.com/kentindell/canhack

[38] Ken Tindell. 2021. The Janus Attack. https://kentindell.github.io/2021/07/15/janus-attack/

[39] Li Yue, Zheming Li, Tingting Yin, and Chao Zhang. 2021. CANCloak: Deceiving Two ECUs with One Frame. *Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021* 2021 (02 2021). https://doi.org/10.14722/autosec.2021.23024

[40] Mattia Zago, Stefano Longari, Andrea Tricarico, Michele Carminati, Manuel Gil Pérez, Gregorio Martínez Pérez, and Stefano Zanero. 2020. ReCAN–Dataset for reverse engineering of Controller Area Networks. *Data in brief* 29 (2020), 105149.

[41] Haichun Zhang, Xu Meng, Xiong Zhang, and Zhenglin Liu. 2020. CANsec: A Practical in-Vehicle Controller Area Network Security Evaluation Tool. *Sensors* 20, 17 (2020). https://doi.org/10.3390/s20174900