# **REFERENCES**

4g.com. (2022). *How fast is 4g and 5g?* <https://www.4g.co.uk.> Retrieved May 5, 2022, from <https://www.4g.co.uk/how-fast-is-4g/>

40 CFR 86.1806-05, Federal U.S.C. (1994). <https://www.law.cornell.edu/cfr/text/40/86.1806-05>

AAMCO. (2017). *What’s an engine control module?* [www.aamcocolorado.com.](https://refworks.proquest.com/www.aamcocolorado.com.) Retrieved May 5, 2022, from <https://www.aamcocolorado.com/how-to-tell-if-your-engine-control-module-ecm-is-failing/>

Abdul Rehman Javed, Saif ur Rehman, Khan, M. U., Alazab, M., & Thippa, R. G. (2021). CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network Using CNN and Attention-Based GRU. *IEEE Transactions on Network Science and Engineering, 8*(2), 1456-1466. <http://dx.doi.org.proxymu.wrlc.org/10.1109/TNSE.2021.3059881>

ARILOU, & NNG. (2018). *Understanding automotive cyber security – The in-vehicle network.* Retrieved July 10, 2022, from <https://ariloutech.com/news/understanding-automotive-cyber-security-the-in-vehicle-network/>

Autoconnectedcar.com. (2014). *Definition of connected car. What is the connected car? Defined.* Retrieved May 5, 2022, from <https://www.autoconnectedcar.com/definition-of-connected-car-what-is-the-connected-car-defined/>

Axelrod, C. W. (2017). Cybersecurity challenges of systems-of-systems for fully-autonomous road vehicles. Paper presented at the *13th International Conference and Expo on Emerging Technologies for a Smarter World,* 1-6. 10.1109/CEWIT.2017.8263141 <http://proxymu.wrlc.org/login?url=https://www-proquest-com.proxymu.wrlc.org/conference-papers-proceedings/cybersecurity-challenges-systems-fully-autonomous/docview/1989750855/se-2?accountid=27975>

Barry, K. (2011). Hack to the future. *Car & Driver, 57*, 21-22. <http://proxymu.wrlc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=62856278&site=ehost-live>

Becker, R. (2021). *What does computer-aided design (CAD) mean?* Retrieved May 5, 2022, from <https://www.techopedia.com/definition/2063/computer-aided-design-cad>

Beyeler, B. D. (2000). *Communication framework for remote vehicle access.* Society of Automotive Engineers. <http://www.sae.org/servlets/productDetail?PROD_TYP=PAPER&PROD_CD=2000-01-0150>. <https://doi.org/10.4271/2000-01-0150.>

Bose, A., Gilpin, L., Agosti, J., & Quinn Dang. (2017). The vehicle act: Safety and security for modern vehicles. *Willamette Law Review, 53*(2), 137–159. <http://proxymu.wrlc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=125932678&site=ehost-live>

Bozdal, M., Samie, M., Aslam, S., & Jennions, I. (2020). Evaluation of CAN bus security challenges. *Sensors, 20*(8), 2364. <http://dx.doi.org.proxymu.wrlc.org/10.3390/s20082364>

CAN-CIA.org. (2022). *History of CAN technology.* Retrieved May 20, 2022, from <https://www.can-cia.org/can-knowledge/can/can-history/>

Careless, J. (2019, October). Connectivity providers explain how they’re cyber-protecting business jets.<https://interactive.aviationtoday.com/avionicsmagazine/october-2019/connectivity-providers-explain-how-theyre-cyber-protecting-business-jets/>

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. Paper presented at *Usenix* *San Francisco, CA,* 1-16. <https://www.usenix.org/conference/usenix-security-11/comprehensive-experimental-analyses-automotive-attack-surfaces>

Chen, C., Hsu, C., Juang, R. & Wang, T. (n.d.) *The Development of Remote Diagnostic System for Internet-connected Vehicles.* Retrieved June18, 2022, from <https://www.artc.org.tw/upfiles/ADUpload/knowledge/tw_knowledge_492798821.pdf>

Choi, W., Lee, S., Joo, K., Hyo Jin Jo, & Lee, D. H. (2021). An enhanced method for reverse engineering CAN data payload. *IEEE Transactions on Vehicular Technology, 70*(4), 3371-3381. <http://dx.doi.org.proxymu.wrlc.org/10.1109/TVT.2021.3063261>

CISA. (2017). *ICS alert (ICS-ALERT-17-209-01)CAN bus standard vulnerability.* CISA. <https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-17-209-01>

CISA, Rapid, 7., & Kiley, P. (2019). *CAN bus network implementation in avionics.* CISA. [https://us-cert.cisa.gov/ics/alerts/ics-alert-19-211-01](https://us-cert.cisa.gov/ics/alerts/ics-alert-19-211-01" \t "_blank)

Continental Automotive Global. (2017). *Cybersecurity @ automotive connectivity by Continental.* YouTube. <https://www.youtube.com/watch?v=WEq6SC0Rcb0>

CSS Electronics, & Falch Martin. (2022). *CAN FD explained.* Retrieved December 4, 2022, from <https://www.csselectronics.com/pages/can-fd-flexible-data-rate-intro?_pos=2&_sid=5581e96c7&_ss=r>

CSS Electronics, & Falch Martin. (2022). *CANopen explained - A simple intro.* Retrieved June 18, 2022, from <https://www.csselectronics.com/pages/canopen-tutorial-simple-intro>

CSS Electronics, & Falch Martin. (2022). *LIN bus explained – A simple intro*. Retrieved May 5, 2022, from <https://www.csselectronics.com/pages/lin-bus-protocol-intro-basics>

CSS Electronics, & Falch Martin. (2022). *OBD2 explained – A simple intro.* Retrieved May 5, 2022, from <https://www.csselectronics.com/pages/obd2-explained-simple-intro>

Cuéllar, M. (2019). A common law for the age of artificial intelligence: Incremental adjudication, institutions, and relational non-arbitrariness. *Columbia Law Review, 119*(7), 1773–1792. <http://proxymu.wrlc.org/login?url=https://www-proquest-com.proxymu.wrlc.org/scholarly-journals/common-law-age-artificial-intelligence/docview/2330576418/se-2?accountid=27975>

Currie, R., & Northcutt, S. (2017). *SANS Institute* Retrieved May 20, 2022, from <https://www.giac.org/paper/gcia/9927/hacking-bus-basic-manipulation-modern-automobile-bus-reverse-engineering/133228>

De Faveri Tron, A., Longari, S., Carminati, M., Polino, M., & Zanero, S. (2022). CANflict: Exploiting Peripheral Conflicts for Data-Link Layer Attacks on Automotive Networks. Paper presented at the *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security,* 711-723. <https://doi.org/10.1145/3548606.3560618>

EETimes. (2013). *How hackers can take control of your car.* Retrieved June18, 2022, from <https://www.eetimes.com/how-hackers-can-take-control-of-your-car/>

Eftekhari, S. A., Nikooghadam, M., & Rafighi, M. (2020). Robust session key generation protocol for social internet of vehicles with enhanced security provision. *The Journal of Supercomputing, 77*(77), 2511–2544. <https://doi.org/10.1007/s11227-020-03363-2>

ENISA. (2021). *How to Secure the connected & automated mobility (CAM) ecosystem.* Retrieved June18, 2022, from <https://www.enisa.europa.eu/news/enisa-news/how-to-secure-the-connected-automated-mobility-cam-ecosystem>

Evenchick, & Eric. (2016). *Hopping on the CAN bus  
.* BlackHat. <https://www.youtube.com/watch?v=U1yecKUmnFo&t=432s>

EVTV, & Kidder, C. E. A. (2022). *SavvyCan.* Retrieved June 18, 2022, from <https://github.com/collin80/SavvyCAN>

Fakhfakh, F., Tounsi, M., & Mosbah, M. (2021). Cybersecurity attacks on CAN bus based vehicles: A review and open challenges. *Library Hi Tech, 40*(5), 1179–1203. <https://doi.org/10.1108/LHT-01-2021-0013>

FCC. (2021). *FCC 4G LTE coverage tool ARCGIS.* fcc.gov. <https://fcc.maps.arcgis.com/apps/webappviewer/index.html?id=6c1b2e73d9d749cdb7bc88a0d1bdd25b>

FREECADS. (2022). *Car top view.* Retrieved June 20, 2022, from <https://www.freecads.com/en/transportation/car-top-view-00000990>

Greenberg, A., & WIRED. (2015). *Hackers remotely kill a Jeep on a highway. Wired.* YouTube. <https://www.youtube.com/watch?v=MK0SrxBC1xs>

Griffith, D. S. (1990). The computer fraud and abuse act of 1986: A measured response to a growing problem. *Vand.L.Rev., 43*, 453. <https://scholarship.law.vanderbilt.edu/vlr/vol43/iss2/4/>

Haking, & Stark, A. (2022 ). Car hacking. *Hakin9, 17*, NO 02. <https://hakin9.org/product/car-hacking/>

Helligrath, E. (2017). In Honda Motor Co. Ltd. (Ed.), *Honda Motor granted patent for remote vehicle access system.* <https://patents.google.com/patent/US10055916B1/en?oq=15%2f420%2c732>

Hu, Q., & Luo, F. (2018). Review of secure communication approaches   
for in-vehicle network. *International Journal of Automotive Technology, 19*(5), 879–894. DOI: 10.1007/s12239−018−0085−1

ISO/SAE. (2021). Road vehicles — Cybersecurity engineering. *Technical Committee: Electrical and Electronic Components and General System Aspects,* (1) 81. <https://www.iso.org/standard/70918.html>

Jämsä, J., & Kaartinen, H. (2016). Enhancing traffic safety with mobile applications. *ActaTechnica Jaurinensis, 9*(3), 216-236. <https://doi.org/10.14513/actatechjaur.v9.n3.419>

Jo, H. J., Choi, W., Na, S. Y., Woo, S., & Lee, D. H. (2016). Vulnerabilities of Android OS-based telematics system. *Wireless Personal Communications, 92*(4), 1511–1530. <https://doi.org/10.1007/s11277-016-3618-9>

Jo, H. J., Kim, J. H., Choi, H., Choi, W., Lee, D. H., & Lee, I. (2020). MAuth-CAN: Masquerade-attack-proof authentication for in-vehicle networks. *IEEE Transactions on Vehicular Technology, 69*(2), 2204–2218. DOI: [10.1109/TVT.2019.2961765](https://doi.org/10.1109/TVT.2019.2961765)

Kang, M., & Kang, J. (2016). Intrusion detection system using deep neural network for in-Vehicle network security. *PLoS One, 11*(6), 1–17. DOI [10.1109/VTCSpring.2016.7504089](https://doi.org/10.1109/VTCSpring.2016.7504089)

KDE. (2022). *Using Ark.* Retrieved June 18, 2022, from <https://docs.kde.org/trunk5/en/ark/ark/ark-extract.html>

Kernel.org. (2022). *SocketCAN – Controller area network.* Retrieved June 18, 2022, from <https://docs.kernel.org/networking/can.html>

Khatri, N., Shrestha, R., & Nam, S. Y. (2021). Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain. *Electronics, 10*(8), 893. <http://dx.doi.org.proxymu.wrlc.org/10.3390/electronics10080893>

Kiley, P. (2019). *CAN bus in aviation*. Retrieved May 20, 2022, from Rapid 7 and Defcon <https://www.youtube.com/watch?v=bydy7lbFyFU>

Knight, A. (2020). *Hacking connected cars: Tactics, techniques, and procedures.* Wiley. <https://doi.org/10.1016/S1353-4858(20)30090-8>

Kris8. (2020). *I’m using a Rock64 with armbian but it should be similar/identical. Here are my notes:* Retrieved 6/18/2022, from <https://community.teamviewer.com/English/discussion/101071/how-to-install-teamviewer-on-raspberry-pi-4-running-ubuntu-mate-20-04-64bit-armv8>

LDRA. (2022). *SAE J3061 and ISO 26262? They 're Made for Each Other.* <https://resources.ldra.com.> Retrieved 6/18/2022, from <https://resources.ldra.com/resources/sae-j3061-and-iso26262theyre-made-for-each-other/>

Li, X., Yu, Y., Sun, G., & Chen, K. (2018). Connected vehicles’ security from the perspective of the in-vehicle network. *IEEE Network, 32*(3), 58-63. <http://dx.doi.org.proxymu.wrlc.org/10.1109/MNET.2018.1700319>

Linke, R. (2017). *Additive manufacturing explained*. Retrieved May 5, 2022, from <https://mitsloan.mit.edu/ideas-made-to-matter/additive-manufacturing-explained>

Luo, X., Liu, Y., Chen, H., & Guo, Q. (2020). Physical layer security in intelligently connected vehicle networks. *IEEE, 34*(5), 232–239. <https://doi-org.proxymu.wrlc.org/10.1109/MNET.011.1900628>

Lynch, K., Marchuk, N., & Elwin, M. (2016). *Embedded computing and mechatronics with the PIC32 microcontroller CAN.* Elsevier.

Marcinek, M. (2020). Cybercrime in automotive security in the 21th century. *Internal Security, 12*(2), 191–200. <http://dx.doi.org.proxymu.wrlc.org/10.5604/01.3001.0014.6694>

Markham, T. R., & Chernoguzov, A. (2017). A balanced approach for securing the OBD-II port. *SAE International Journal of Passenger Cars: Electronic & Electrical Systems, 10*(2), 390–399.<https://link.gale.com/apps/doc/A531111147/AONE?u=anon~d98dd8d9&sid=googleScholar&xid=0ae67cfd> DOI 10.4271/2017-01-1662

Matterhackers. (2022). *Nylon X.* Retrieved May 5, 2022, from <https://www.matterhackers.com/store/c/NylonX>

Mayilsamy, K., Ramachandran, N., & Sunder Raj, V. (2018). *An integrated approach for data security in vehicle diagnostics over internet protocol and software update over the air*. Elsevier. <https://doi.org/10.1016/j.compeleceng.2018.08.002>

Miller, C. (2019). Lessons learned from hacking a car. *IEEE Design & Test, 36*(6), 7–9. <http://dx.doi.org.proxymu.wrlc.org/10.1109/MDAT.2018.2863106>

Moguen-Toursel, M. (2007/2008). Emergence and transfer of vehicle safety standards: Why we still do not have global standards. Paper presented at the *Business History Conference. Business and Economic History: Papers Presented at the BHC Annual Meeting, 5,* 88–102. <https://doi.org/10.3917/eh.051.0088>

Moreau, P. (2001). In Valeo Electronique SA Valeo Securite Habitacle SAS (Ed.), *Valeo Securite Habitacle’s European patent for anti-theft control procedure and device therefor, for vehicles with remote control access systems expires.*

Mühlbach, S., & Wallner, S. (2008). Secure communication in microcomputer bus systems for embedded devices. *Journal of Systems Architecture, 54*(11), 1065–1076. DOI: 10.1016/j.sysarc.2008.04.003

NIST, & SP800-12REV1. (n.d.). *Commercial-off-the-shelf (COTS).* Retrieved May 5, 2022, from <https://csrc.nist.gov/glossary/term/commercial_off_the_shelf>

Oconnor, T. J. (2013). *WNIC wireless mayhem with Python/violent Python.* Elsevier Science Inc. . Elsevier Science Inc. <https://doi.org/10.1016/C2011-0-07761-X>

Offensive Security. (2022). *Kali Linux ARM V1.2.* Retrieved June 18, 2022, from <https://www.kali.org/get-kali/#kali-arm>

Ookla, L., & Speedtest. (2022). *Speedtest-CLI.* Retrieved June 18, 2022, from <https://www.speedtest.net/>

Palanca, A., Evenchick, E., Maggi, F., & Zanero, S. (2017). A stealth, selective, link-layer denial-of-service attack against automotive networks. Paper presented at the *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment,* 185–206. <https://link.springer.com/chapter/10.1007/978-3-319-60876-1_9>

PRNewswire, & USNewswire. (2016, July 21,). Automotive industry collaborates in developing vehicle cybersecurity best practices to address cybersecurity challenges. *India Automobile News*. <http://proxymu.wrlc.org/login?url=https://www-proquest-com.proxymu.wrlc.org/magazines/automotive-industry-collaborates-developing/docview/1805815465/se-2?accountid=27975>

Raspberrypi. (2022). *Raspberrypi.* Retrieved June 18, 2022, from <https://www.raspberrypi.org/help/what-%20is-a-raspberry-pi/#:~:text=The%20Raspberry%20Pi%20is%20a,languages%20like%20Scratch%20and%20Python.>

Raz, I. (2018). *Automotive security.* YouTube. <https://www.youtube.com/watch?v=YO_52KFMJsU>

Regulation (EU) 2015/758, Regulation U.S.C. (2015). <https://www.legislation.gov.uk/eur/2015/758/introduction>

Sahoo, B. P., Chou, C., Weng, C., & Wei, H. (2018). Enabling millimeter-wave 5G networks for massive IoT applications: A closer look at the issues impacting millimeter-waves in consumer devices under the 5G framework. *IEEE Consumer Electronics Magazine, 8*(1), 49–54. 0.1109/MCE.2018.2868111

Sanal, J. (2020). *Kali Linux Auto Login: How to enable autologin Kali Linux Raspberry Pi.* Retrieved June 18, 2022, from <https://hackersgrid.com/2020/03/raspberry-pi-autologin-kali.html>

Sbdautomotive. (2015). *TSP.* Retrieved May 5, 2022, from <https://www.sbdautomotive.com/files/sbd/pdfs/612sample.pdf>

Scribendi (2023). ***Professional dissertation copy editing.***

<https://www.scribendi.com/service/academic_proofreading>

Serviejs. (2021). *Popsicle.* Retrieved June 18, 2022, from <https://github.com/pop-os/popsicle>

Shishodia, M. (2017). *Kaspersky Lab, AVL software and functions join hands on development for automotive cybersecurity.* ProQuest. <http://proxymu.wrlc.org/login?url=https://www-proquest-com.proxymu.wrlc.org/magazines/kaspersky-lab-avl-software-functions-join-hands/docview/1905179708/se-2?accountid=27975>

Smith, C. (2016, March/April). The car hacker's handbook. *Network Security, 278*(4), 4. DOI: 10.1016/S1353-4858(16)30034-4 <http://proxymu.wrlc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=114675600&site=ehost-live>

Sun X, Yu FR, Zhang P, Xie W, Peng X. (July 30, 2020) A Survey on Secure Computation Based on Homomorphic Encryption in Vehicular Ad Hoc Networks. *Sensors (Basel)*. 20(15):4253. DOI: 10.3390/s20154253

<https://pubmed.ncbi.nlm.nih.gov/32751627/>

Driving In the Cloud & Software World (2017, January). Driving in the cloud. *48*(1), 21. [*http://Search.Ebscohost.Com/Login.Aspx?direct=true&db=iih&AN=121220076&site=ehost-Live,*](http://Search.Ebscohost.Com/Login.Aspx?direct=true&db=iih&AN=121220076&site=ehost-Live,)

Spiegel, R., & Murray, C. J. (2015). What can be done about car hacking? *Design News*. <http://proxymu.wrlc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=109450993&site=ehost-live>

System76. (2022). *Pop\_OS.* Retrieved June 18, 2022, from <https://pop.system76.com/>

Takefuji, Y. (2018). Connected vehicle security vulnerabilities. *IEEE Technology & Society Magazine, 37*(1), 15–18. DOI 10.1109/MTS.2018.2795093

Team viewer. (2022). *Team viewer.* Retrieved June 18, 2022, from *r.* [https://www.teamviewer.com/.](https://www.teamviewer.com/) Retrieved 6/18/2022, from <https://www.teamviewer.com/en-us/#:~:text=TeamViewer%20is%20a%20comprehensive%20remote,as%20though%20you%20were%20there.>

UNECE. (1998). *UNECE Vehicle Regulations WP.29.* <https://unece.org/wp29-introduction.> Retrieved June 18, 2022, from <https://unece.org/wp29-introduction>

Urbina Coronado, P. D., Ahuett-Garza, H., Morales-Menendez, R., Orta Castañón, P., Dávila, L. D., & Flores Escalera, M. R. (2017). Connectivity of a modular electric vehicle by the use of a mobile device. *Advances in Mechanical Engineering, 9*(7). <http://dx.doi.org.proxymu.wrlc.org/10.1177/1687814017708087>

Vasileiadis, A. (2022). *Car hacking: The ultimate guide! - Part I*. <https://hakin9.org/car-hacking-the-ultimate-guide-part-i/>

Vasileiadis, A. (2022). *Car hacking: The ultimate guide! - Part II.* <https://hakin9.org/car-hacking-the-ultimate-guide-part-ii/>

Vasileiadis, A. (2022). *Car hacking: The ultimate guide! - Part III.* <https://hakin9.org/car-hacking-the-ultimate-guide-part-iii/>

Vector, & Mutter, A. (2022). *CAN XL – Enabler for future proof E/E architectures*.Retrieved December 6, 2022, from <https://www.vector.com.>

Vita, S. B., Caivano, D., Nannavecchia, A., & Scalera, M. (2020). A Kohonen SOM architecture for intrusion detection on in-vehicle communication networks. *Applied Sciences, 10*(15), 5062. <http://dx.doi.org.proxymu.wrlc.org/10.3390/app10155062>

Wang, Q. A. S., S. (2014). VeCure: A practical security framework to protect the CAN bus of vehicles. *International Conference on the Internet of Things, 9*(4), 13–18. DOI: 10.1109/IOT.2014.7030108

Wen, H., Chen, Q. A., & Lin, Z. (FEB (2019/2020)). Plug-N-owned: Comprehensive vulnerability analysis of OBD-II dongles as a new over-the-air attack surface in automotive IoT. Paper presented at the *Usenix August 12-14, 2020.*1-17. <https://www.usenix.org/system/files/sec20summer_wen_prepub.pdf>

Wu, W., Kurachi, R., Zeng, G., Matsubara, Y., Takada, H., Li, R., & Li, K. (2018). IDH-CAN: A hardware-based ID hopping CAN mechanism with enhanced security for automotive real-time applications. *IEEE Access, 6*, 54607–54623. <http://dx.doi.org.proxymu.wrlc.org/10.1109/ACCESS.2018.2870695>

Xiao, J., Wu, H., & Li, X. (2019). Internet of things meets vehicles: Sheltering in-vehicle network through lightweight machine learning. *Symmetry (20738994), 11*(11), 1388. DOI: 10.3390/sym11111388

Xun, Y., Liu, J., & Zhang, Y. (2020). Side-channel analysis for intelligent and connected vehicle security: A new perspective. *IEEE Network, 34*(2), 150–157. DOI: 10.1109/MNET.001.1900214

Yarkoni, O., & Attias, D. (2020). *Remotely hacking into a brand new car.* YouTube. <https://www.youtube.com/watch?v=fPQIWawXSRI>

Zhang, H., Meng, X., Zhang, X., & Liu, Z. (2020). CANsec: A practical in-vehicle controller area network security evaluation tool. *Sensors, 20*(20), 1–15. DOI 10.3390/s20174900