Carjacking Goes Digital: A Survey of Proven & Potential Network Security Threats in Modern Automobiles

Katie Kennedy, College of Science & Engineering,
San Francisco State University

Abstract

To remain competitive in the new car market, vehicle manufacturers face constant pressure to roll out cutting-edge tech features at warp speed. The culture of the auto industry incentivizes manufacturers to prioritize novelty and market-delivery speed, which often comes at the expense of necessary cybersecurity implementation. But as network capabilities continue to expand in both conventional and autonomous vehicles (AVs), so does the potential for devastating vehicle hackings. Unsurprisingly, consumers are far more concerned with novelty than network security, leading manufacturers to cut corners with regard to necessary cybersecurity implementation. The advent of self-driving capabilities has immense potential increase quality of life, save lives, and revolutionize mobility for those who cannot drive or do not own a car. However, if manufacturers and regulators do not drastically increase their concern for vehicle systems security, the eminent industry shift to AVs risks devaluing human safety instead of improving it.

Keywords: Vehicle cybersecurity, Autonomous vehicle security, Sensor attacks, Jamming, Spoofing, ECU security, OBD security, CAN buses, LiDAR, Infotainment systems, In-vehicle networks

Introduction

Though the vast majority of consumers don't acknowledge their cars as computers, modern vehicles employ some of the most intricate embedded computer networking systems available on the global market. The automobile manufacturing industry is a stanchly competitive one, requiring constant innovation to maintain consumer demand for new vehicles in a market saturated with better priced used options. As evidenced by Tesla's recent dethroning of Toyota as the world's most valuable car company, the customer base for new vehicles is a reliably technophilic one (Nusca & Morris, 2020).

However, the nature of the modern auto industry has proven to incentivize premature rollout of brand-new vehicle features, often at the expense of adequate network security measures and penetration testing. Both conventional and autonomous vehicles (AVs) are subject to similar vulnerabilities, though the latter is considered far more vulnerable due to its novelty, additional sensors, and drastically increased network reliance. This paper aims to predict the future landscape of vehicle cybersecurity threats via a survey of past intrusions on a variety of vehicle-related systems.

Method

Research for this survey was primarily conducted via keyword searches on article archive databases and on Google Scholar. All resources referred to and cited in this paper are either peer-reviewed academic research publications or news articles from media outlets, namely Wired and Fortune. Additionally, all resources cited are either free to view on Google Scholar or available for free to San Francisco State University (SFSU) students through the school library's OneSearch tool, an aggregated search engine that allows for keyword searches over multiple databases at once. Database websites used include Jstor, ScienceDirect Journals, ProQuest, and Arxiv. OneSearch did not function properly with content from EBSCO. SFSU does not have a subscription to IEEE Xplore, but limited content is available. IEEE Spectrum publications are available to view without a paid subscription.

Original search keywords used were: “car cybersecurity,” “vehicles,” “lidar security,” and “networked vehicle cybersecurity.” However, as early research for this study confirmed, the most appropriate way to predict future threats is to analyze past events of vehicle cybersecurity failure. As a result, the objective of this study pivoted to survey events that have previously occurred as a result of cybersecurity lapses by manufacturers. After this pivot, search keywords used in addition to those listed above expanded to include “auto industry,” “vehicle ransomware,” “sensor spoofing,” “Uconnect by Chrysler,” “hacked Tesla,” and “in-vehicle network.”

The events surveyed in this report are primarily sourced from the bulleted list included in the introduction of Mahmoud Hashem Eiza and Quang Ni’s publication “Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security” (2017, p. 2).

Basic System Architecture of Modern Vehicles

To understand vehicle cybersecurity intrusion methods, it is necessary to understand the infrastructure of a vehicle’s internal systems. Both conventional and semi-autonomous vehicles principally operate through the facilitation of the in-vehicle network, which is responsible for communicating necessary data between different components of the car. The in-vehicle network made up of many individual specialized controllers known as electronic control units (ECUs). On a basic level, this network of ECUs is responsible for accepting inputs, communicating them between necessary components, then responding or performing accordingly. The in-vehicle network must also alert the driver or mechanic when the vehicle needs attention to remain operating safely.

New vehicles today typically ship with anywhere from 30 to 70 ECUs, though some publications report this number to be as high as 100 or more (Hashem Eiza & Ni, 2017, p. 2).

Each ECU is an embedded computer that controls one or more subsystems of the in-vehicle network. Though luxury vehicles employ a greater number of ECUs than their economy-friendly counterparts, all vehicles require a few mission-critical types of ECUs, including controllers for the powertrain, transmission, brake control, timing control, and general electricity control (Takefuji, 2018, p. 16). Semi-autonomous vehicles include extra ECUs to handle additional sensors and operations required for self-driving functions, like LiDAR and additional camera integration.

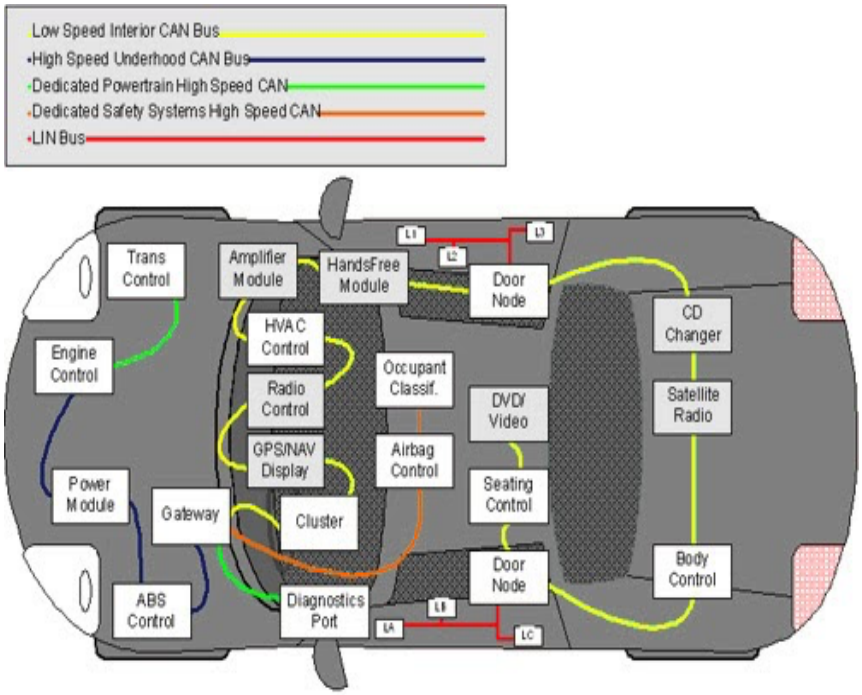

Figure 1: *A simplified diagram of subsystems that comprise the in-vehicle network. The colored connecting lines represent different bus types used to communicate data throughout the vehicle. Graphic provided by FEV, a European powertrain development firm.*

In-vehicle networks require minimal latency and maximum reliability due to the inherent danger involved in operating heavy machinery at high speeds. Data is sent between system modules via a variety of controller area network (CAN) and local interconnect network (LIN) buses. As shown in Figure 1, the high-speed interior CAN bus is reserved for engine control and brake functionality, as these components are the most critical to human safety. The low-speed interior CAN bus services noncritical features, namely the infotainment and temperature systems. LIN buses are also low speed, servicing other noncritical components like door locks and window controls. Data from a LIN bus is often then placed on a CAN bus and sent to other subsystems (Al-Jarrah et al., 2019, p. 21268).

Virtually all cars manufactured for the American market today include features for networking with external devices like smartphones and on-board diagnostics (OBD) devices. Any networking done between a vehicle and an external device provides an additional gateway to a potential cybersecurity intrusion. One pair of researchers suggest the word "connected" can be considered synonymous with "exposed" in the context of computer networking (Hasham Eiza & Ni, 2017, p. 1).

Proven Vulnerabilities in Vehicle Cybersecurity

Wireless Carjacking

Among the most unnerving forms of known vehicle cyberattacks is wireless carjacking, a nightmarish event where hackers assume control of a vehicle while its unsuspecting driver is actively traveling on the road. These hackers can be miles away from their victim without ever having physical access to the targeted car. As of 2015, wireless carjacking of commercially available vehicles is no longer science fiction, but a reality. In the first successful hack of its kind, two white-hat security experts sent a Jeep Cherokee and its driver off a highway and into a ditch using a laptop ten miles away (Hashem Eiza & Ni, 2017). The pair of researchers, Charlie Miller and Chris Valasek, thus proved they could wirelessly override the driver's control of the Cherokee's braking system via its vehicle-to-smartphone infotainment system, Uconnect. A hole in the vehicle's built-in 3G network capabilities, provided by Sprint's cellular network, allowed Miller and Valasek the potential to take remote control of any car released between 2013 and 2015 with Uconnect software (Greenberg, 2015).

As a result, parent company Fiat Chrysler was forced to recall 1.4 million cars with Uconnect software, including models by its Chrysler, Jeep and Dodge subdivisions (Jabs, 2018). Uconnect isn't the only system found to be released with serious shortcomings in security, though it is the most egregious of its kind. Nissan was forced to scrap their vehicle-to-smartphone app for electric vehicles, NissanConnect, after one white-hat hacker located in the U.K. managed to drain the battery of a random Nissan Leaf in Australia with only the car's VIN (Buser, 2019, p. 16). Infotainment systems appear to be a common attack surface for wireless intrusions.

GPS Jamming & Spoofing

One of the easiest and cheapest ways to interfere with both conventional and semi-autonomous vehicles is GPS jamming. Using inexpensive and readily available devices, a vehicle's built in GPS can be disabled by blocking its communication with satellites. Jamming devices bombard the target vehicle's GPS receiver with "white noise" using the same radio frequency as used by GNSS satellites, which are responsible for returning signals to the car's GPS receiver. Because GNSS satellite signals are weak compared to those emitted by the jamming device, the vehicle's GPS receiver becomes too overwhelmed to receive signals from satellites, in turn disabling the vehicle's location services completely. Typical jamming devices for sale on Amazon can interrupt signals within a radius of ten meters, and, as of December 2020, can be purchased for less than $40. However, jamming is a well-studied attack type for which solutions exist. One effective countermeasure involves detecting unusual bandwidth activity, then re-routing bogus signal traffic and switching communication frequencies (Grover et al., 2014).

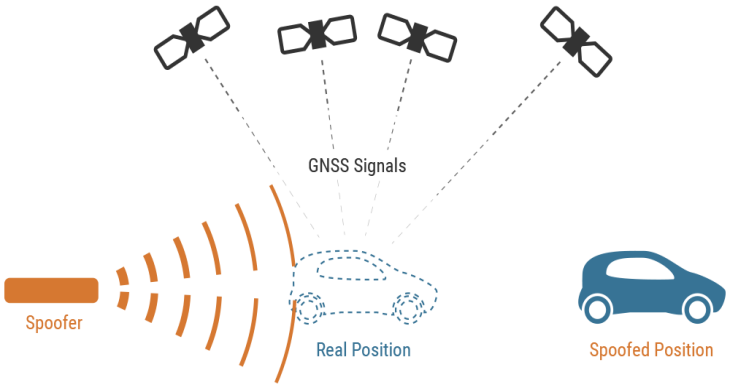

Figure 2: *A spoofing device intercepts GNSS signals from satellites, manipulates them, then transmits a false location to the vehicle's GPS receiver. Graphic provided by Orolia, a cybersecurity consulting firm.*

However, a newer GPS-based attack, known as spoofing, is becoming an increasing threat. Though it requires more expertise and specialized equipment, GPS spoofing is far more dangerous than a jamming attack. Instead of simply disabling the system, GPS spoofing fools a vehicle into believing that it is in an entirely different location than where it actually located. Because it is a relatively novel attack method, anti-spoofing and spoofing-detection methods are extremely underdeveloped, leading to a largely unmitigated risk for functions that rely on GPS and GNSS communications (Cuntz et al., 2012). Though conventional vehicles can operate safely without GPS services, AVs

rely on extensive GPS use for critical functioning. A successful spoofing attack on a self-driving vehicle traveling at highway speeds could be catastrophic.

Autonomous Vehicle Sensor Attacks

In addition to heavy reliance on GPS, AVs employ light detection and ranging (LiDAR) sensors for principal operation. Using a cheap laser pointer and a Raspberry Pi, security expert Johnathan Petit proved just how simple and inexpensive it is to trick a vehicle's LiDAR unit into accepting malicious inputs. Petit cleverly found that by mimicking the same speed of light pulsation as emitted by an Ibeo LUX 3 LiDAR unit, it could be tricked by a simple laser into "seeing" pedestrians and other vehicles that do not actually exist (Takefuji, 2018, p. 17). As a result, the target AV will disable or move itself to avoid hitting what it believes to be an object in its path. Sensors for traditional radar and millimeter wave detection are also vulnerable to similar spoofing attacks. AV sensors can be improved by implementing support for alternative wavelength frequencies that can be used in the case of a spoofing attack. However, based on the success of laser attacks, manufacturers have not yet included such a feature. Petit concludes that misbehavior detection systems need to be prioritized in ongoing vehicle development (Harris, 2015).

OBD Attacks

Another notable gateway for a potential intrusion is via the onboard diagnostic (OBD) port, which provides direct access to the car's internal software systems by wire. This port allows manufacturers and mechanics to read the machine's log of data with a dedicated diagnostic device, which are available to anyone and relatively inexpensive. However, these devices are notoriously unsecured, with one survey reporting that as many as half of all diagnostic devices currently on the market are vulnerable to malicious exploits (Yan, 2015). The port also allows direct writing to ECUs and buses, typically with little or no authentication (Bielawski et al., 2020, p. 11). However, attacks via the OBD port require advanced skill. Previously, physical access to the target car was also required, but today, OBD ports can also be accessed wirelessly over a wi-fi network (Checkoway et al., 2011).

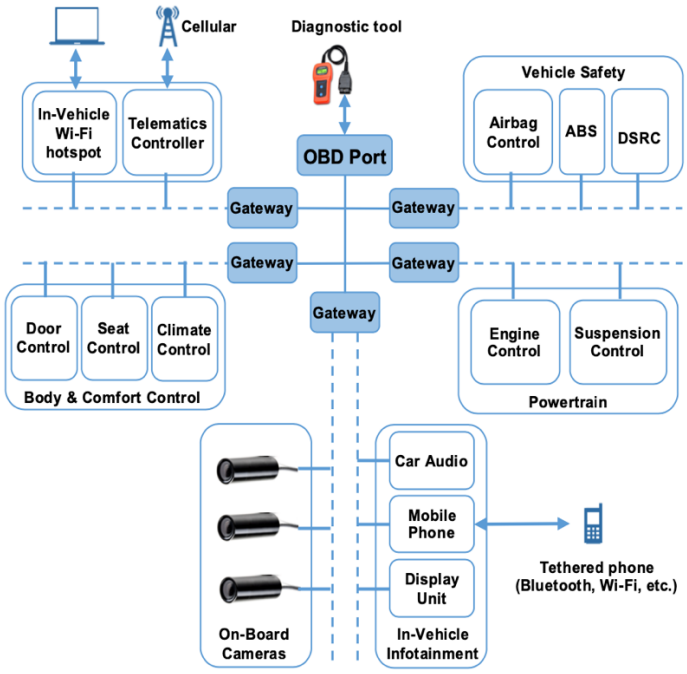

Figure 3: *An illustration of subsystems the OBD port allows access to. Graphic provided by Zhang, et al. (2014).*

Governance & Safety Regulation in the U.S.

Both federal and state lawmakers continue to lag behind the speed of innovation in the auto industry. The National Highway Traffic Safety Administration (NHTSA) currently only requests voluntary updates from companies developing AVs (Taeihagh & Si Min Lim, 2019). Wenzel suggests that in contrast to aviation, vehicle oversight is extremely weak, citing that the FAA has 10,000 employees per 100 crashes, while the NHTSA has only 0.3 per 100, respectively (2017, p. 63).

In 2016, Michigan passed a state law punishing criminals who try to hack into cars for nefarious purposes, suggesting life in prison for serious offenses. However, car hacking quickly becomes a legal gray area when owners hack their own cars. Without permission of any kind, software engineer Jason Goeke hacked his Tesla to accommodate voice commands for the car's summoning system (Krok, 2016).

Going forward, if legislators are too aggressive with government regulation of AVs, the rate of development will surely slow. On the other hand, some form of development oversight is critical to assuring safety takes priority over company profits. The federal government holds a responsibility to make sure risk to human safety is preemptively mitigated. However, in practice, it has historically proven difficult for lawmakers to implement appropriate safety standards for cutting-edge technologies they don't fully understand.

Conclusions & Recommendations

This paper aimed to provide insight into the future plane of cybersecurity as both conventional and autonomous vehicles evolve to accommodate ever-increasing network reliance. Upgrades in vehicle networking technology provide drivers and riders with increased safety, convenience, comfort, and even social equity. But increased networking capabilities come at a considerable cost: increased vulnerabilities in vehicle software and firmware. Unsurprisingly, consumers are far more concerned with novel tech features than the strength of the car's network security. Instead, they seem to implicitly trust that car manufacturers would not sell a vehicle that capable of being hacked. Some might believe lawmakers would not allow the sale of a hackable car to the public. But as shown by the hacked Jeep Cherokee, cars with critical software vulnerabilities do make it to market.

For some attack types like LiDAR spoofing, countermeasures are still in their infancy, leading to largely unmitigated risk. However, for others, known solutions exist but are just not implemented by manufacturers. Interestingly, consumers and manufacturers behave similarly when faced with the choice between convenience and preventative security. No consumer wants to be the victim of a cyberattack, but many will choose a simpler, less secure password if it means they will not have to spend time resetting it in the future. Likewise, manufacturers have been shown to cut corners anti-hack prevention to save time.

But the swift adoption of AV technology should serve as a warning to carmakers that malware will too rapidly develop. As AV development matures, vehicle-to-vehicle and vehicle-to-infrastructure systems will introduce even more possible endpoints for potential intrusions. However, though AVs are likely to be the future of driving, manufacturers would be unwise to turn a blind eye to security improvement in conventional vehicles. As of 2018, Consumer Reports found that new car customers still reported a greater desire for features like reverse cameras and blind-spot detection, as opposed to semi-autonomous capabilities (Barry, 2018).

Further, the auto industry may want to reexamine its reliance on black box testing; vulnerabilities will surely be missed. However, open-source testing might not be a perfect solution either, as carmakers have a great incentive to keep their propriety designs a secret from competitors. At the very least, manufactures should improve the separation of the in-vehicle network's subsystems, possibly with the use of one-way CAN buses like used in avionics. There is no reason an infotainment system should be able to send commands to the braking system or engine control unit, even indirectly.

Increased concern for vehicle cybersecurity is not only in the best interest of the public, but beneficial for manufacturing companies' bottom line, as well. Recalls can inflict serious damage to a manufacturer's reputation for safety, in addition to extreme financial losses. To avoid recalls of entire models in the future, software updates and patches must be provided regularly to a massive fleet of individual vehicles. A global key-based update method could be potentially catastrophic should the key be compromised. On the other hand, individual mechanic-delivered updates would surely not reach all vehicles. Software delivery and authentication methods need extensive further research, as do intrusion detection methods.

Going forward, it will be increasingly imperative for consumers, manufacturers, and government bodies alike to increase their concern for vehicle cybersecurity. Otherwise, we continue to risk the prioritization of speed and profits over human lives.

References

Al-Jarrah, O.Y., Maple, C., Dianati, M., Oxtoby, D., & Mouzakitis, A. (2019, February). Intrusion detection systems for intra-vehicle networks: a review. *IEEE Access*. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8642311

Barry, K. (2018). Shoppers Want Car Tech That Helps Them Drive Better, Survey Shows. *Consumer Reports.* https://www.consumerreports.org/car-safety/car-safety-survey-new-car-buyers-want-advanced-safety-not-automation/

Bielawski, R., Gaynier, R., Ma, D., Lauzon, S., & Weimerskirch, A. (2020, October). *Cybersecurity of Firmware Updates* (Report No. DOT HS 812 807). National Highway Traffic Safety Administration. https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/cybersecurity_of_firmware_updates_oct2020.pdf

Buser, J. (2019). Cybersecurity Implications in Connected and Electronically Complex Commercial Vehicles. *ProQuest Dissertations Publishing*.

Cuntz, M., Konovaltsev, A., Dreher, A., Meurer, M. (2012). Jamming and spoofing in GPS/GNSS based applications and services – threats and countermeasures. *Communications in Computer and Information Science,* vol. 318.

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Sacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. *USENIX Security.* https://static.usenix.org/events/sec11/tech/full_papers/Checkoway.pdf

Durocher-Yvon, J.M., Tappin, B., Goolam Nabee, S., & Swanepoel, E. (2019). Relevance of supply chain dominance: A global perspective.

Greenburg, Andy. (2015, July) Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired*. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Grover, K., Lim, A. and Yang, Q. (2014). Jamming and Anti-jamming Techniques in Wireless Networks: A Survey. *International Journal of Ad Hoc and Ubiquitous Computing*. https://dl.acm.org/doi/10.1504/IJAHUC.2014.066419

Harris, M. (2015). Researcher hacks self-driving car Sensors. *IEEE Spectrum.*

Jabs, J. (2018). Tesla hack takeaways: 3 things auto suppliers, OEMs need to know. *Industry Week*.

Krok, A. (2016, April 29). Michigan lawmakers want to jail you for life for hacking cars. *Road Show by CNET.* https://www.cnet.com/roadshow/news/michigan-lawmakers-want-to-jail-you-for-life-for-hacking-cars/

Linkov, V., Zámecník, P., Havlícková, D. and Pai, C.W. (2019). Human factors in the cybersecurity of autonomous vehicles: trends in Current Research. *Frontiers in Psychology*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6509749/pdf/fpsyg-10-00995.pdf

Nusca, A & Morris, D. (2020). Teslanomics: How to justify being the most valuable car company on earth. *Fortune Magazine.* https://fortune.com/2020/08/10/tesla-most-valuable-car-company-in-the-world-electric-vehicles-evs/#:~:text=On%20July%201%2C%20after%20an,an%20eye%2Dwatering%20%24209%20billion

Orolia. *Spoofing a vehicle to introduce an erroneous result for position* [digital diagram]. Website. https://www.orolia.com/support/testing-simulation/skydel/vehicle-spoofing

Sheehan, B., Murphy, F. Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research. Part A, Policy and Practice*, *124*, 523–536. https://doi.org/10.1016/j.tra.2018.06.033

Taeihagh, A. & Si Min Lim, H. (2019). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews,* vol. 39 no.1, 103-128. https://doi.org/10.1080/01441647.2018.1494640

Wenzel, S.L. (2017). *Not even remotely liable: smart car hacking liability.* Pace School of Law. http://illinoisjltp.com/journal/wp-content/uploads/2017/05/Wenzel.pdf

Yan, W. (2015, October) A Two-year Survey on Security Challenges in Automotive Threat Landscape. *IEEE ICCVE*, 185-189.

Zhang, T., Antunes, H., & Aggarwal, S. (2014, February) Defending connected vehicles against malware: challenges and a solution framework," *IEEE Internet of Things*, vol. 1, no. 1, 10-21.

