AFFECTED VEHICLE POPULATION IN AUTOMOTIVE CYBER RISK ASSESSMENTS

Daniel S Fowler, Carsten Maple*

WMG, University of Warwick, Coventry, UK
**dan.fowler@warwick.ac.uk*

Keywords: CONNECTED VEHICLES, CYBERSECURITY, RISK ASSESSMENT, ISO/SAE 21434, TRUST

Abstract

The computerised and connected car brings with it the possibility of cyber-attacks. The automotive industry is addressing the cyber threat with new regulations and standards. As a result, cyber risk assessments will become part of the systems engineering process as vehicle manufacturers build cyber resilience and trust into their products. This work examines an overlooked aspect of automotive cyber threats, that of the affected vehicle population as a risk rating impact factor. It examines real-world attacks for a qualitatively affected population and then uses UK vehicle statistics to see if the qualitative population can be related to physical quantities. A vehicle population risk rating impact factor was derived from the real-world UK vehicle data; however, limitations exist, and further work is required to quantify other vehicle risk assessment impact and likelihood factors.

1. Introduction and purpose

The connected car incorporates multiple technologies to allow it to interact with the world. It senses and responds to the environment, interacts with smartphones and apps, provides Internet-based services, communicates directly with the manufacturer for servicing information and software updates, and engages in vehicle-to-vehicle and vehicle-to-infrastructure communications [1]. Vehicle manufacturers present vehicle connectivity as being beneficial to vehicle users. However, the benefits of the connected car come with a downside, the potential for threat agents to perform a vehicle cyber-attack.

The regular media reports of computer hacking, ransomware, and data leaks demonstrate the ongoing cybersecurity issues with connected systems. The purpose of this study is to examine demonstrated cyber-attacks against vehicles and investigate the potential scale of those attacks as an aid to vehicular cyber risk assessments. I.e., does a cyber-attack only apply to a single vehicle, or can it be scaled across a fleet of vehicles or other vehicle populations? The potential target population of a cyber-attack will impact a vehicles risk assessment. Results from risk assessments will influence cyber-attack mitigation engineering requirements and the cyber resilience and trust of a deployed vehicle.

In section 2 the background to vehicular cybersecurity is briefly examined, followed by a summary of the new international initiatives requiring manufacturers to address cyber issues throughout a vehicle's lifecycle, including the role of cyber risk assessments. Section 3 examines the methodology used, with the findings in section 4 and discussion in section 5, before the conclusion in section 6.

2. Background

Research interest in vehicular cybersecurity issues began in earnest in the early 2000s. The Embedded Security in Cars (escar) conferences started in Germany in 2003 [2]. The European E-safety vehicle intrusion protected applications (EVITA) project, 2008 to 2011, investigated the protection of vehicle systems, categorising attack aims and motivations [3]. In 2015, security researchers demonstrated taking control of an unaltered vehicle from a remote location via a cellular data connection [4], requiring a recall of 1.4 million vehicles for software updates. Continuing research and reported issues [5] on vehicular cybersecurity, including the data collated here, demonstrate that the attack surface of the computerised vehicle provides multiple attack points for threat agents. The automotive industry has responded, measures include:

- addressing issues found by security researchers [6];
- bug bounty programs [7];
- international regulations on a Software Update Management System (SUMS) [8], and a Cyber Security Management System (CSMS) [9] for manufactured vehicles from the World Forum for the Harmonization of Vehicle Regulations at the United Nations Economic Commission for Europe (UNECE);
- international standard (ISO/SAE 21434) for cybersecurity engineering over the lifecycle of a vehicle [10], developed by the International Organization for Standardization (ISO) and SAE International (SAE), previously known as the Society of Automotive Engineers.

In the UNECE CSMS regulation and ISO/SAE 21434 standard, the management of cybersecurity risks requires a documented and systematic risk-based approach, aimed at addressing the cyber threats to vehicles and used to tackle the presence of potential vulnerabilities. The regulation and standard recognise that cybersecurity is not a point in time issue but requires ongoing vigilance, requiring processes to handle the response to cyber-attacks and new threats. These processes update risk assessments and ensure threat mitigating actions are performed.

There does exist a variety of Threat Analysis and Risk Assessment (TARA) techniques [11], [12] that can be deployed to record and rank cybersecurity threats, i.e., vulnerabilities, and provide the evidence to enable a manufacturer to address vehicle cybersecurity. This is done by applying targeted mitigation to reduce the risk of the identified threats. The CSMS regulation has an appendix listing some examples of threats with mitigation, but no example of a TARA process. Section 15 in ISO/SAE 21434 covers a generic TARA process, which is performed "from the viewpoint of affected road users" [10]. Additionally, Annex H provides a worked example on calculating a risk value.

The impact (a.k.a. severity) of a threat and the likelihood of its occurrence are factors in determining the level of risk [13]:

Risk rating = Likelihood x Impact

A threat that is unlikely to occur and unlikely to have much of an impact is of low risk. A higher risk threat will be due to a higher likelihood of occurring, and/or the possibility of having a bigger impact, giving a larger risk rating. In [14] the risk rating is called *Aggregate Risk Score* (AGR) and is calculated from impact and likelihood which are both ranked from 1 to 5, from *informational*, through *low*, *medium*, *high*, to *critical*, see Table 1. This provides a simple risk score between 1 and 25.

Table 1. A risk rating called an Aggregate Risk Score

Level	Impact Score	Likelihood Score	AGR range
Critical	5	5	20-25
High	4	4	12-19
Medium	3	3	6-11
Low	2	2	2-5
Informational	1	1	1

Compared to AGR, ISO/SAE 21434 has one less level. The four levels are *negligible*, *moderate*, *major*, and *severe*. However, the methodology is more complex. The levels can be applied to the four impact categories of *safety*, *financial*, *operational*, and *privacy* (S, F, O, P). These are combined with *attack feasibility* ratings (from *very low*, through *low*, *medium*, to *high*) to produce a *risk value* (i.e., a risk rating) using matrices and/or formulas. Adherence to the ISO/SAE 21434 standard is likely to cover the CSMS requirements. However, the specific TARA process to use by vehicle manufacturers is not prescribed in either the regulation or the standard. Therefore, it is likely a TARA will vary between manufacturers and their supply chains. Yet, they will need to meet the requirements of the standard, likely via a mapping to the ISO/SAE methodology.

The risk ratings used to rank issues can be qualitative [15] or quantitative [14], [16], provided they can help determine how seriously and quickly a manufacturer needs to address vulnerabilities. Ideally, a quantitative assessment can provide data points for analysis and reduce subjectivity. However, knowledge on vehicular risk assessments is still in the process of maturing, and more quantitative evidence needs to be established to aid a reliable quantitative vehicular TARA. In this work, the affected vehicle population from a cyber incident is investigated as a possible contributory impact factor to cyber risk ratings. Modelling shows that population is important during malware propagation [17], furthermore, vehicle mobility may aid propagation [18] in a future incident. Fortunately, despite an established concept of a vehicle virus [19], debilitating vehicle malware has not (yet) been seen. If such malware comes into existence understanding the affected population could aid risk ranking calculations.

3. Methodology

Cybersecurity issues related to deployed vehicles were examined. The sources include reports of events by online media and published research. The incident year, reference, and brief description were recorded. Details of a published cyber incident do not always address the affected population, therefore a qualitative judgement on the population was made, and engineering knowledge provides confidence in that assessment. Table 2 describes the qualitative populations used.

Table 2. Cyber-attack qualitative vehicle populations

Qualitative population	Description
Single component	The attack could only target a single component in a single vehicle
Single vehicle	The attack targets a single vehicle
Single vehicle model	The attack could be targeted at any vehicle of the same make and model
Vehicle fleet	The attack targets vehicles used for specific purposes
A vehicle manufacturer	The attack could target several vehicle models from a single manufacturer
Multiple vehicle manufacturers	The attack could target several vehicle models from several manufacturers

The collated data was then used to assess a possible effect the vehicle population would have on a risk rating impact factor. This is achieved by examining publicly available UK registered vehicle statistics for June 2021 [20] and using the obtained figures to derive a vehicle population impact factor. This allowed for a mapping from the qualitative vehicle population to the ISO/SAE 21434 impact level.

4. Findings

The 27 real-world cyber-related incidents collated in Table 3 are against vehicles that have been manufactured and sold. It spans a 25-year period, corresponding to the increasing use of technology and connectivity within vehicle systems. Column 1 is the year of the event/publication. Column 2 is a reference for the issue, and column 3 has a brief description. column 4 is the judged qualitative vehicle population. A full TARA for the incidents listed in Table 3 is out of scope for this work. The primary objective is to determine how the affected vehicle population of future incidents could be an impact factor in risk rating assessments. Plus, access to primary data would be required for a full TARA analysis.

Table 3. A summary of vehicle cyber incidents and a qualitative estimate of the affected vehicle population

Year	Ref.	Description	Qualitative population
1996	[21]	Criminals use laptops to lower the mileage displayed single component on a vehicle's digital odometer, known as clocking.	single component
1998	[22]	Spoofing tachograph data in goods vehicles.	single component
2002	[23]	Altering engine ECU code.	single component
2003	[24]	Privacy issues via eavesdropping (sniffing) on vehicle occupants.	a vehicle manufacturer
2005	[25]	Vehicle operating system infected with a virus via Bluetooth.	a vehicle manufacturer
2005	[26]	Weak Bluetooth security allows for audio sniffing and injection.	multiple vehicle manufacturers
2005	[27]	Aftermarket vehicle systems modification.	multiple vehicle manufacturers
2005	[28]	RFID hacking allows for vehicle and petrol theft.	multiple vehicle manufacturers
2007	[29]	Injecting false navigation information via RDS-TMC.	multiple vehicle manufacturers
2010	[30]	An ex-employee was able to disable multiple vehicle's or sound the horn remotely.	vehicle fleet
2010	[31]	Wirelessly control vehicle functionality via the OBD port.	single vehicle model
2010	[32]	Track and spoof data for a Tire Pressure Monitoring System.	multiple vehicle manufacturers
2011	[14]	Compromised vehicle systems, including remote compromise over a cellular connection.	single vehicle model
2011	[35]	Vehicle keyless entry relay attack allows for vehicle theft.	single vehicle
2013	[36]	Alleged driver death because of vehicle compromise.	single vehicle model
2015	[4]	A researcher takes control of an unmolested vehicle from a driver remotely over a cellular connection.	single vehicle model
2015	[33]	Researchers control a vehicle using an OBD plug-in telematics device.	multiple vehicle manufacturers
2015	[37]	The US Environmental Protection Agency issues a notice of Violation to the Volkswagon Group over the use of a software defeat device for emissions testing. The manufacturer's hack affects vehicle models from 2009.	vehicle manufacturer
2016	[38]	Researchers crack a vehicle's WiFi interface to control functions, disable the car and track vehicles.	single vehicle model
2016	[39]	Security researchers can control vehicle functions remotely.	single vehicle model
2018	[40]	Researchers find vulnerabilities in BMW head units and telematics ECUs using fake GSM base stations.	vehicle manufacturer
2018	[41]	Bluetooth vehicle connections leak personal data.	multiple vehicle manufacturers
2019	[42]	A stalker used a manufacturer's app to track a victim and control the victim's vehicle.	single vehicle
2019	[43]	A vehicle emits a Bluetooth identifier beacon that allows the vehicle to be tracked.	single vehicle model
2019	[44]	Cracked fleet management apps give access to thousands of accounts allowing data to be obtained and the potential immobilization of thousands of vehicles.	vehicle fleet
2020	[45]	Ghost image projections cause vehicle systems to react.	multiple vehicle manufacturers
2021	[46]	Researchers reverse engineer a luxury car's security system to enable additional key fob provisioning and vehicle theft.	single vehicle model

Having examined the reported cyber issues, the next stage was analysing the UK Government statistics to investigate real-world vehicle populations of car models. The total UK population of licensed road vehicles in June 2021 was 39.2 million. Most vehicles are cars, 33 million, comprising of 2320 car models, from which 210 models, i.e., 9.1%, make up 90% of the cars on UK roads. To get a car model into the 90% bracket a manufacturer needs to sell over 24,832 vehicles. However, road vehicles are dominated by a few car models, as shown by the skewed chart in Figure 1.

Around a third of licensed cars (36.5%) are dominated by the top 20 models. Furthermore, ten car models dominate the top 25.2%, see Table 4, with four models above 1 million vehicles. Therefore, a cyber-attack against a popular vehicle model may have a bigger impact than an attack against a car model that does not have as many vehicles on the road. For example, hacking a Tesla Model X [46] affects a population of 6104 vehicles, a tiny proportion, 0.02%, of all road cars. An inconvenience to Model X owners, but potentially less impactful than if a Ford Fiesta was attacked, which covers 4.6% of all road cars.

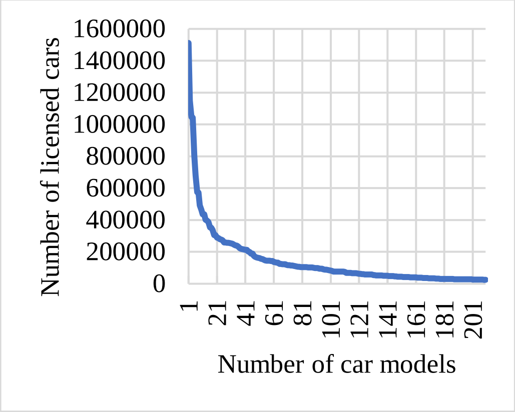

Figure 1. UK road cars distribution

The analysis of the UK road car statistics is used to inform an example mapping of vehicle population to the four levels of the ISO/SAE 21434 impact factor. This is in Table 5. It is an example mapping because it would likely be different for other countries, or different at a global level.

Table 4. 25% of UK cars come from 10 car models

Rank	Car	Count
1	Ford Fiesta	1511485
2	Ford Focus	1149721
3	Volkswagon Golf	1046563
4	Vauxhall Corsa	1042273
5	Vauxhall Astra	800962
6	Volkswagon Polo	678179
7	Nissan Qashqai	574302
8	BMW 3 Series	572089
9	Toyota Yaris	491416
10	Mini Cooper	464433

The skewed nature of the UK car model populations is reflected in the selected impact factor. The two highest impact factors represent 20 car models but 36.5% of the total UK licensed car models. Row three represents 53.5% of UK road cars, but only 189 of the UK's 2320 models. The lowest impact factor is 10% of UK cars but represents 2,110 car models (and 1,429 of those models have 1,000 or fewer vehicles on the UK roads, representing old and vintage vehicles, or exotic cars). Many luxury cars, often with advanced technology, would fall into the bottom 10%.

Table 5. Assigning an impact factor to vehicle population

ISO/SAE	UK Rank	Vehicle population, x
Severe	Top 4 (14.4%)	x >= 1 million
Major	20 to 5 (22.1%)	300,000 <= x < 1m
Moderate	210 to 21 (53.5%)	25,000 <= x < 300,000
Negligible	Last to 209 (10 %)	x < 25,000

Vehicle manufacturers performing a TARA would likely have access to vehicle model production figures, unlike the examination of real-world cyber-attacks against vehicles in Table 3, where six types of qualitative vehicle population were identified. However, the qualitative population can aid an estimated mapping to a quantitative impact factor. This is discussed in the next section.

5. Discussion

The published automotive attacks (Table 3) can describe how an attack is achieved, the effect on a car or vehicle system, and suggest or demonstrate mitigation action, though some do not discuss mitigation. However, whilst the practical attack effects are often demonstrated, the real-world impact sees little detailed analysis, hence the qualitative statement on the affected vehicle population. The analysis of UK road vehicle data can provide some quantitative data, see Table 5. This can aid risk impact analysis. In this case, for UK vehicles, it allows a mapping of the qualitative population to an ISO/SAE 21434 impact factor. For example, if production figures for a *single vehicle model* are known the mapping is straightforward, e.g., a top 4 vehicle could be rated as *Severe*, a specialist vehicle with very low sales as *Negligible*, as would a *single component* or *single vehicle* attack. Likewise, a cyber incident that affects *a vehicle manufacturer* or *multiple vehicle manufacturers* could be rated *Severe* due to the combined count of all the models affected, even if counts of individual model production figures would normally fall at the *Major* or *Moderate* impact factor level. In a multi-model *vehicle fleet*, total vehicle counts can be used to obtain the impact factor from Table 5.

Another use of the vehicle population analysis would be to support malware propagation modelling. Knowing the number of specific vehicles allows for improved models and scenarios, e.g., malware propagation via a popular car model compared to a less popular car, or through all cars from a certain manufacturer. However, car model density, e.g. in an urban area, would need to be determined.

There are limitations in this study, it did not address data from other countries or globally. Furthermore, future work needs to examine how vehicle population affects risk rankings in a full TARA analysis. In addition, more research into moving from qualitative to quantitative assessments of vehicle technologies would aid accuracy in risk ratings.

6. Conclusion

The new challenge for vehicle manufacturers is supporting the CSMS regulation and ISO/SAE 21434 standard for the execution of TARA processes for connected vehicle systems engineering. These vehicular cyber risk assessments are currently qualitatively focused, likely due to the lack of access to real-world data and the reliance on cybersecurity experience. Transforming qualitative rankings to quantitative values allows a vulnerability risk ranking to be performed. Any real-world data-based factor that improves the trust of the cyber risk assessment process is beneficial. This work examined vehicle populations as a potential contributory impact factor in an automotive TARA. The examination of UK road vehicle data suggests the current diversity of vehicle populations is likely to suppress higher risk ratings for automotive cyber-attacks. Only a few car models are sold in large enough quantities to cause a higher rank in impact factors unless a cyber incident affects multiple car models and manufacturers. Targeting exotic and luxury cars, which often carry the latest technology, is not likely to lead to high-level risk ratings due to their low sales volumes unless other ISO/SAE TARA factors (i.e., safety, financial, operational, and privacy) increase the risk rating.

The affected vehicle population has had little if any, quantification in the literature. This work begins to address that shortcoming; however, further research is required to provide a firmer foundation for the use of other quantitative impact and likelihood factors within an automotive TARA.

7. Acknowledgements

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) through the Trustworthy Autonomous Systems Hub (EP/V00784X/1), the platform grant entitled "AutoTrust: Designing a Human-Centred Trusted, Secure, Intelligent and Usable Internet of Vehicles" (EP/R029563/1).

8. References

[1] M. K. Svangren, M. B. Skov, and J. Kjeldskov, "The Connected Car: An Empirical Study of Electric Cars as Mobile Digital Devices," 2017. doi: 10.1145/3098279.3098535

[2] isits AG International School of IT Security, "escar: Embedded Security in Cars," 2021, https://www.escar.info/escar-europe/history.html (accessed May 17, 2021)

[3] A. Ruddle *et al.*, "Security requirements for automotive on-board networks based on dark-side scenarios," 2009

[4] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," in *Black Hat USA*, 2015, vol. 2015, pp. 1–91. [Online]. Available: https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf

[5] D. S. Fowler, "Automotive Cyber Security Timeline," *Tek Eye*, 2020. https://tekeye.uk/automotive/cyber-security/timeline (accessed May 24, 2021)

[6] Tencent Keen Security Lab, "Experimental Security Assessment of BMW Cars: A Summary Report," 2018. Accessed: May 25, 2018. [Online]. Available: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf

[7] A. Magazinius, N. Niklas Mellegård, and L. Olsson, "Bug Bounty Programs – A Mapping Study," in *2019 45th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, 2019, pp. 412–415. doi: 10.1109/SEAA.2019.00070

[8] UNECE World Forum for Harmonization of Vehicle Regulations (WP.29), "Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system," 2020. [Online]. Available: https://undocs.org/ECE/TRANS/WP.29/2020/80

[9] UNECE World Forum for Harmonization of Vehicle Regulations (WP.29), "Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system," Geneva, 2020. [Online]. Available: http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

[10] ISO and SAE International, "Road vehicles – Cybersecurity engineering (ISO/SAE 21434)." ISO, Geneva, 2021

[11] D. J. Bodeau, C. D. McCollum, and D. B. Fox, "Cyber threat modeling: survey, assessment, and representative framework," McLean, 2018

[12] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, "A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context," in *Computer Safety, Reliability, and Security*, 2016, pp. 130–141

[13] NIST, "FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems," 2006

[14] J. Hammond and J. Culliss, "Commonalities in Vehicle Vulnerabilities 2018 Remix," 2018

[15] E. Wheeler, "Chapter 6 - Risk Exposure Factors," in *Security Risk Management*, E. Wheeler, Ed. Boston: Syngress, 2011, pp. 105–125. doi: 10.1016/B978-1-59749-615-5.00006-2

[16] L. ben Othmane, R. Ranchal, R. Fernando, B. Bhargava, and E. Bodden, "Incorporating attacker capabilities in risk estimation and mitigation," *Computers & Security*, vol. 51, pp. 41–61, 2015, doi: 10.1016/j.cose.2015.03.001

[17] A. M. del Rey, "Mathematical modeling of the propagation of malware: a review," *Security and Communication Networks*, vol. 8, no. 15, pp. 2561–2579, 2015, doi: https://doi.org/10.1002/sec.1186

[18] B. Liu, W. Zhou, L. Gao, H. Zhou, T. H. Luan, and S. Wen, "Malware Propagations in Wireless Ad Hoc Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 6, pp. 1016–1026, Nov. 2018, doi: 10.1109/TDSC.2016.2642191

[19] D. K. Nilsson and U. E. Larson, "Simulated attacks on CAN buses: vehicle virus," *Fifth IASTED International Conference on Communication Systems and Networks (AsiaCSN 2008)*, pp. 66–72, 2008

[20] Department for Transport and Driver and Vehicle Licensing Agency, "Statistical data set, All vehicles,"

GOV.UK, 2021. https://www.gov.uk/government/statistical-data-sets/all-vehicles-veh01 (accessed Dec. 01, 2021)

[21] J. Ruppert, “Only done 30,000. Honest, guv,” *The Independent*, London, p. 1, May 1996. [Online]. Available: http://www.independent.co.uk/life-style/motoring/only-done-30000-honest-guv-1345479.html

[22] R. Anderson, “On the security of digital tachographs,” in *Computer Security --- ESORICS 98: 5th European Symposium on Research in Computer Security Louvain-la-Neuve, Belgium September 16--18, 1998 Proceedings*, J.-J. Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 111–125. doi: 10.1007/BFb0055859

[23] J. Fahey, “How to Hack Your Car.” 2002. [Online]. Available: https://www.forbes.com/forbes/2002/0708/148.html

[24] K. Poulsen, “Court limits in-car FBI spying.” 2003. [Online]. Available: https://www.theregister.co.uk/2003/11/20/court_limits_incar_fbi_spying/

[25] D. Quainton, “Mobile virus infects Lexus cars.” 2005. [Online]. Available: https://www.scmagazine.com/home/security-news/mobile-virus-infects-lexus-cars/

[26] M. Herfurt, “Introducing the Car Whisperer at What The Hack.” 2005. [Online]. Available: https://trifinite.org/blog/archives/2005/07/introducing_the.html

[27] J. Gartner, “Hacking the Hybrid Vehicle.” 2005. [Online]. Available: https://www.wired.com/2005/11/hacking-the-hybrid-vehicle/

[28] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, “Security Analysis of a Cryptographically-Enabled RFID Device,” in *14th USENIX Security Symposium*, 2005, p. 15

[29] D. Goodin, “Satnav hacking made simple.” 2007. [Online]. Available: https://www.theregister.co.uk/2007/04/20/satnav_hack/

[30] K. Poulsen, “Hacker Disables More Than 100 Cars Remotely.” 2010. [Online]. Available: https://www.wired.com/2010/03/hacker-bricks-cars/

[31] K. Koscher *et al.*, “Experimental Security Analysis of a Modern Automobile,” in *Security and Privacy (SP), 2010 IEEE Symposium on*, 2010, pp. 447–462

[32] I. Rouf *et al.*, “Security and Privacy Vulnerabilities of In-car Wireless Networks: A Tire Pressure Monitoring System Case Study,” 2010

[33] I. Foster, A. Prudhomme, K. Koscher, and S. Savage, “Fast and Vulnerable: A Story of Telematic Failures,” 2015.

[34] S. Checkoway *et al.*, “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” 2011

[35] A. Francillon, B. Danev, and S. Capkun, “Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars,” 2011. doi: 10.3929/ethz-a-006708714

[36] M. Hogan, “Was Michael Hastings’ Car Hacked? Richard Clarke Says It’s Possible.” 2013. [Online]. Available: https://www.huffingtonpost.co.uk/entry/michael-hastings-car-hacked_n_3492339

[37] EPA, “Learn About Volkswagen Violations.” 2019. [Online]. Available: https://www.epa.gov/vw/learn-about-volkswagen-violations

[38] D. Lodge, “Hacking the Mitsubishi Outlander PHEV hybrid.” 2016. [Online]. Available: https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/

[39] Tencent Keen Security Lab, “Car Hacking Research: Remote Attack Tesla Motors.” 2016. [Online]. Available: https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

[40] Z. Cai, A. Wang, W. Zhang, M. Gruffke, and H. Schweppe, “0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars,” *Black Hat USA*, vol. 2019, p. 39, 2019

[41] Privacy4Cars, “CarsBlues Vehicle Hack Exploits Vehicle Infotainment Systems Allowing Access to Call Logs, Text Messages and More.” 2018. [Online]. Available: https://www.privacy4cars.com/can-my-car-be-hacked/

[42] E. Bevin, “Man pleads guilty to stalking and controlling ex-girlfriend’s car with his computer.” 2019. [Online]. Available: https://www.abc.net.au/news/2019-11-06/ract-employee-pleads-guilty-to-using-app-to-stalk-ex-girlfriend/11678980

[43] S. Rosenblatt, “Have a Tesla Model 3? This app can track its location.” 2019. [Online]. Available: https://the-parallax.com/2019/11/14/tesla-radar-model-3-phone-key-ibeacon/

[44] L. Franceschi-Bicchierai, “Hacker Finds He Can Remotely Kill Car Engines After Breaking Into GPS Tracking Apps.” 2019. [Online]. Available: https://www.vice.com/en_us/article/zmpx4x/hacker-monitor-cars-kill-engine-gps-tracking-apps

[45] B. Nassi, D. Nassi, R. Ben-Netanel, Y. Mirsky, O. Drokin, and Y. Elovici, “Phantom of the ADAS: Phantom Attacks on Driver-Assistance Systems.” 2020. [Online]. Available: https://www.nassiben.com/phantoms

[46] L. Wouters, B. Gierlichs, and B. Preneel, “My other car is your car: compromising the Tesla Model X keyless entry system,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, no. 4, pp. 149–172, 2021, doi: 10.46586/tches.v2021.i4.149-172