Journal of
Cybersecurity and Privacy

MDPI

Review

Automotive Vulnerability Disclosure: Stakeholders, Opportunities, Challenges

Robin Bolz * and Reiner Kriesten

Institute of Energy Efficient Mobility, Karlsruhe University of Applied Sciences, 76133 Karlsruhe, Germany; reiner.kriesten@hs-karlsruhe.de
* Correspondence: robin.bolz@h-ka.de

Abstract: Since several years, the overall awareness for the necessity to consider a vehicle as a potentially vulnerable system is facing accelerated growth. In 2015, the safety relevant exploitability of vulnerabilities through cyber attacks was exposed to a broader public for the first time. Only a few months after this attack has reached public awareness, affected manufacturer implemented one of the first bug bounty programs within the automotive field. Since then, many others followed by adapting some of ITs good practices for handling and responsibly disclose found and reported vulnerabilities for the automotive field. Nevertheless, this work points out that much remains to be done concerning quantity and quality of these measures. In order to cope with this, this present paper deals with what can be learned from IT and which conclusions can be drawn from these findings in the light of special conditions in the automotive environment. Furthermore, current handling and challenges regarding the disclosure process of vulnerabilities in the automotive sector are presented. These challenges are addressed by discussing desirable conditions for a beneficial disclosure culture as well as requirements and responsibilities of all parties involved in the disclosure process.

Keywords: automotive security; vulnerability disclosure; threat intelligence

check for updates

Citation: Bolz, R.; Kriesten, R. Automotive Vulnerability Disclosure: Stakeholders, Opportunities, Challenges. *J. Cybersecur. Priv.* **2021**, *1*, 274–288. https://doi.org/10.3390/jcp1020015

Academic Editor: Dimitris A. Gritzalis

Received: 18 February 2021
Accepted: 25 April 2021
Published: 6 May 2021

1. Introduction

In industries like IT or sectors of critical infrastructure, which have had to deal with cybersecurity for a long time, the awareness of responsible handling of vulnerabilities found in the field has only grown over many years. According to a study from 2007 [1], vulnerability reports for software vendors correlated noticeably with their stock value and major incidents caused an average market value loss of approx. 0.6% in cases investigated. However, it should also be mentioned that the failure to fix a vulnerability within given time limit led to even higher losses. Compared to a decade earlier, there is a high degree of transparency in the IT industry, for example through publicly accessible databases of fixed and disclosed vulnerabilities (e.g., National Vulnerability Database- NVD [2]) and, last but not least, bug bounty programs. In contrast to the general IT landscape, automotive industry is still in the early stages of this transformation. However, some automobile manufacturers take the lead and are, for example, already successfully represented on platforms such as HackerOne and Bugcrowd (see Section 2 Vulnerability Disclosure). In the first two years after starting a disclosure program, GM was able to eliminate 700 vulnerabilities and establish a network of 500 white-hat hackers [3]. Other manufacturers carry out vulnerability disclosure (VD) programs on their own account and independently of such platforms (BMW, Mercedes-Benz, Bosch, Continental, Siemens, etc.).

The automotive industry faces very special challenges due to the strict requirements of functional safety related subsystems like braking or advanced driver assistance systems, as well as extraordinarily long product lifetimes (in Germany as of 2014 18 years on average) [4]. This requires the continuous preservation of a high level of vehicle security in road traffic over decades of strong technological change. According to [5], about half of all newly delivered vehicles are equipped with external connectivity capabilities. Modern cars contain two to five times as many lines of code as a standard PC operating system, and up to seven times as much as many passenger aircrafts (100 million) and, thus, provide ample opportunity for security gaps. With development towards a higher degree of connectivity (e.g., fleet management, update-over-the-air, V2X, cloud services), exploitation of a local vulnerability in a single vehicle or backend server can quickly scale to a global fleet. In addition, there is a particular complexity, especially in the vertical supply chain, which makes rapid vulnerability management considerably more difficult compared to many general IT products. Due to great potential threat to drivers or even public safety, handling of vulnerabilities in connected vehicles is even more challenging [6].

Regulatory authorities around the world have recognized these ever-increasing challenges. In January 2021, the two UN regulations on Cybersecurity and Cyber Security Management Systems [7] and on Software Updates and Software Updates Management Systems [8] entered into force. They are the first ever internationally harmonized and binding norms in the area of cyber security and the broad adoption of these regulations across the world is expected [9]. The upcoming ISO/SAE 21434 standard [10] is intended to support the implementation of measures to comply with the UNECE regulation [7]. It is already in the status of formal approval since March 2021. Since the two regulations are also highly relevant with regard to the Coordinated Vulnerability Disclosure, they will be dealt with specifically in the following.

In order to obtain type approval according to UN regulation, vehicle manufacturers must prove by means of document checks that they have appropriate measures in place with regard to cyber security for all phases of the product life cycle. The proof obligation on the one hand covers processes, responsibilities and governance to treat cyber risks (e.g., Cyber Security Management System (CSMS)). On the other hand, it covers the implementation of security measures in the vehicle. An essential component of the CSMS is risk management, which means coordinated activities to direct and control an organization with regard to cyber risk. This contains processes to manage vulnerabilities, which need a response of the manufacturer in a reasonable timeframe. Furthermore, it contains obligation for vehicle manufacturers to manage dependencies with regard to vulnerabilities, which may exist with their sub-organizations, service providers or contracted suppliers. A VD program can meet these requirements and can therefore be an important part of a mature vulnerability management system in the post-production phase. Furthermore, a VD Program can help create a supportive environment for benign hackers (e.g., research) and motivate them to find and submit vulnerabilities to industry. This contributes to an up-to-date and comprehensive threat intelligence and thus serves the risk management also in the development phase. According to the other previously mentioned UN regulation on software updates [8], manufacturers must demonstrate that they are able to assess the potential impact of a software update on type approvals or legally defined parameters. Patches developed to address vulnerabilities during the post-production phase may potentially require type approval renewal or confirmation.

The vehicle is often not yet perceived by the public as a cyber-physical system. Customers are often not aware of the danger of potential attacks. However, according to a study, the proportion of black hat hackers with targets in the automotive sector has risen steadily and amounted to 57% in 2019 [11]. A sudden change in customer awareness can happen as soon as a major security incident with serious damage occurs and receives media attention. This could considerably increase the customer's demand for cybersecurity in a vehicle. A cooperative handling of security incidents by manufacturers can then be perceived by potential customers as a sign of quality and may become a decisive criterion for buyer decisions or the estimation of value of a car (see NCAP crash test [12] or ADAC breakdown statistics [13]).

In this paper, we introduce the topic of vulnerability disclosure by talking about the benefit it can provide for manufacturers, benign hackers and end users. Furthermore, hackers' incentives, the corresponding legal challenges and the state of the art for implementing such a program within the classic IT environment is discussed. In the third section, the current practice within the automotive environment is illustrated. The objective is to learn from the implementation and insights within the classical IT processes and adapt the VD process appropriately for the automotive field. In the last section, we discuss the requirements and responsibilities of the various stakeholders and make a proposal as to what might be an appropriate strategy for the usage and disclosure of information on vulnerabilities in the automotive sector.

2. Vulnerability Disclosure

A VD program is an application security methodology, which can help to continuously maintain or enhance the cybersecurity of a product during its lifetime. Various strategies have been established in practice for the disclosure of vulnerabilities [14]. Full disclosure, limited disclosure, which includes responsible disclosure and coordinated disclosure.

2.1. The Protection of the User as the Main Objective of Standardized Processes

Before standardized processes were recognized, vulnerabilities found were often published anonymously in public due to fear of legal prosecution or a lack of appropriate reporting contacts (known as zero-day disclosure, full disclosure). The problem for manufacturers and users is not only the risk of the vulnerability being maliciously exploited, but also the lack of access to valuable detailed knowledge about the existing vulnerability. Full Disclosure is not the preferred solution, as it ultimately serves the interests of none of the parties involved. Both manufacturers and users are directly exposed to enormous risks and the finder usually achieves the opposite of what he or she wanted to achieve. Namely, reputation or money and closed security gaps before any harm is done. Two standards have been developed for the disclosure of vulnerabilities, which on the one hand define a responsible publication process (ISO/IEC 29147 [15]) and on the other hand define the internal company handling of reported vulnerabilities (ISO/IEC 30111 [16]). In particular, ISO/IEC 29147 propagates limited disclosure, i.e., the publication of only selected information at specific points in time. This strategy places the protection of the user and the cooperation of all parties involved in the foreground (responsible disclosure). In 2010, the Google Security Team criticized in an article [17] the way in which responsible disclosure is implemented in some companies, as it sees the propagated responsible behavior as often not being treated seriously by vendors ("...responsible disclosure is a two-way street..."). It is probably for this reason that Microsoft in particular has contrasted responsible disclosure with the concept of coordinated disclosure [18]. The distinction is marginal and consists in the fact that the finder of a vulnerability is not only seen as a valuable provider of information, but as an equal partner in the process. The harmonious relationship between interests of all parties involved is even more in focus here and should ultimately serve the main goal of protecting users. The finder thus has even more transparency regarding implementation, progress, and time management of patch development and release. He in particular discusses appropriate patching times with the manufacturer and possibly third parties on an equal footing. The goal is to avoid conflicts and to ensure that vulnerability information is only made public after a patch or at least a mitigation of the given vulnerability problem has been made available.

2.2. The Implementation—Learning from Classical IT

2.2.1. Appropriate Grace Periods for Patching

In IT industry, non-profit and profit organizations have established themselves as recipients of vulnerability reports and as intermediaries between the finder and the affected manufacturer (e.g., Zero Day Initiative (ZDI), since 2005 [19], CERT/CC [20]). It is quite common for the vendor to be given fixed deadlines, so-called grace periods, to fix or mitigate vulnerabilities before (partial) information is published, regardless of existing patches or mitigations (ZDI, today: 120 days [21], Rapid7: 60 days [22], Google Security Team (2010)/Project Zero (2020): 60 days/90 days [17,23], CERT/CC: 45 days [24]). In a worst-case scenario, details may then be published even before a mitigation or fix is available. The question of the ideal grace periods for IT products and services has been subject of research (e.g., [25,26]). This has led to a wealth of experience in the IT sector and to adjustments to the grace periods (e.g., in the case of ZDI, see [21,25]). Nevertheless, the considerable deviation between 45 and 120 days shows the difficulty of implementing a widely applicable and yet adequate timing. In large part, this is because the complexity of vulnerabilities and their resolution can vary widely. According to McQueen et al. [25], there is no clear evidence for or against some of the established grace periods. Although it could be shown that the introduction of a grace period leads to an accelerated patch creation regarding the examined ZDI data set from about august 2010, when the given ZDI period was 182 days. But even after this period no patches were provided by vendors for about a quarter of the vulnerabilities.

2.2.2. Exact Specifications for Valid Vulnerability Reports Are Important

As mentioned before, platforms like HackerOne or Bugcrowd are established not only within the IT but also within the automotive security environment. They provide their customers with a framework for the launch of a VD program as a service. Apart from ready-made policies, the greatest value for customers of these organizations is probably the direct access to the expertise of the hacker community. In addition, the costs of implementing and running such a program can quickly become a significant burden on companies. In addition, according to a study by Zhao, M. et al. [27] from 2017, up to 50% of vulnerability reports for desktop and mobile computing software are about vulnerabilities which are either not valid, insufficiently described, or do not meet the vendor's specifications for the type of vulnerability. These reports put an enormous load on involved parties without providing any benefit. In order to work as efficiently as possible, a thorough, early validation and prioritization of the reports and especially a precise formulation of conditions such as out-of-scope vulnerabilities is crucial for the profitability of a VD program.

2.3. In the Mind of a Hacker

If a manufacturer wants to benefit from the contact to the hacker community by implementing a VD program, it is essential to know what motivates the community to report vulnerabilities and to design the program accordingly. According to the Hacker Report 2020 by HackerOne [28], the five most important reasons for hackers to enter into such a process are the associated challenge, monetary incentives, learning effects, fun and improved career opportunities. The most important criteria according to which "ethical" hackers choose their targets are the amount of rewards, competition, loyalty to the products or the manufacturer, and a private invitation. Among the most common reasons stated for starting their activities are media coverage and another previously discovered vulnerability. Only 9% state that they hack for professional reasons. However, this distribution is likely to be somewhat different in the automotive sector, as instructions and discussions about hacking a vehicle in online forums or literature should be much less widespread and there are fewer opportunities for learning vehicle-specific hacking in a playful way with limited access and resources. These findings should be used by manufacturers to tailor their VD program accordingly and to attract the attention of hackers. Essential to attract the attention of the community seems to be an open and publicly communicated handling of security issues as well as an adequate reward in form of money, reputation or lucrative job opportunities. Incentives for academic researchers, on the other hand, can be an active willingness to cooperate, dealing at eye level, transparent, coordinated and adequate disclosure and patching processes, as well as legal security and the opportunity to publish about the vulnerability and gain reputation.

2.4. Facing Legal Challenges

Finding vulnerabilities can easily become legally relevant. Then the intention of the finder is often decisive. But even if the finder is in good-faith, he can easily operate in a legal grey area. The legal situation is global and even within the EU very heterogeneous. With regard to the EU there are efforts to homogenize the national laws, but the implementation varies from country to country. In order to provide the necessary security for ethical hackers, companies should take a clear position on their ideas and requirements regarding the finder himself, vulnerabilities and a disclosure policy in general. In this way, the risk of misunderstandings regarding the question of which actions are still in the interest of involved parties can be minimized. This provides the hacker with a safe harbor and, to the greatest possible extent, legal certainty and increases incentive, in addition to monetary reasons, to enter into an orderly, coordinated disclosure process with the manufacturer. In their 2018 report [29] the CEPS Working Group examined the overall situation and the implementation status of VD programs at government and economic level in the EU area. Areas of law which may be relevant in the context of VD processes are identified as criminal law, data protection law, intellectual property, trade secrets and dual-use regulations. Persons who want to implement a VD program should keep these areas of law in mind when developing a disclosure policy.

3. Current Practice within the Automotive Environment

In its "Best Practices on Incident Response" [30], AUTO-ISAC (with members like Volkswagen, GM, or Toyota) recommends that a manufacturer should integrate official third parties on a voluntary basis if the incident makes this seem appropriate. The early entry into force of the new UNECE regulation [7,8] in conjunction with ISO/SAE 21434 [10] will significantly increase the pressure on the automotive industry to innovate on their security approach and to address all of the challenges mentioned above. The important role which access to the knowledge of the hacker community through VD can play in this context is highlighted by the work of Bolz et al. [31]. This work classifies such programs into the entire product life cycle and outlines their potential for optimization in the various phases of the product development process (e.g., threat and risk analyses, testing, access management). Kurachi et al. [32] also highlight the benefit of a vulnerability database to extend the coverage of existing automotive coding rules by the automated migration.

Several cases have been reported in recent years in which the discovery of critical vulnerabilities led to legal disputes between researchers and the manufacturers concerned. For example, the intention to publish a scientific paper by Verdult et al. [33] on the exploitation of a vulnerability in an immobilizer of several popular car brands in 2013 led to a two-year legal dispute with media impact [34]. While Volkswagen succeeded in a British court, this also meant a potential threat of vehicle theft for thousands of car owners for years. In another case from 2015, researchers revealed partial information about a critical vulnerability in the media after the manufacturer concerned failed to respond to their report. The researchers succeeded in gaining remote access to a number of critical functions of the vehicle via the built-in WIFI access point [35]. The result was an openly published vulnerability for which no patch was available. While we do not judge the legal assessment of such cases in this paper, these events are undesirable because they delay and hinder the elimination of vulnerabilities and can cause lasting damage to trust between the community of ethical hackers, the automotive industry and their customers. These cases once again demonstrate the need for strengthening responsible and coordinated disclosure processes in the automotive sector. However, there are also success stories in which disclosure of vulnerabilities by researchers in the automotive environment was carried out responsibly and fairly without any danger to users. In May 2018, researchers published their work in which they described the discovery of 14 vulnerabilities in BMW cars [36]. A total of seven CVE (Common Vulnerabilities and Exposures [37]) entries were assigned to this work. Between the vulnerability report to BMW and their report confirmation, only ten working days passed. Another nine days later BMW provided the planned technical mitigation measures for the reported vulnerabilities to the finder. Within a few weeks, security enhancements were distributed via over-the-air updates to the affected vehicles. Furthermore, BMW provided improvements in form of optional software updates, which were available through the BMW dealer network. In total, it took less than four months from the discovery of the vulnerabilities to the deployment of first countermeasures by BMW, so that the researchers could afterwards publish their work without endangering the public. In 2015, Tesla and a research team in the USA provided another positive example [38]. With physical access, the researcher gained root access to the infotainment systems of a Model S and conducted a multi-stage attack leveraging multiple vulnerabilities, which e.g., allowed them to start and stop the car. In their publication, the researchers attest Tesla a positive and productive working relationship and state that it is clear that Tesla is taking the security of their cars very seriously. The dissemination of a corresponding over-the-air update took only about 1–2 weeks. An even more recent example of a successful disclosure process was provided in February 2020 by the Sky-Go Team in cooperation with Mercedes-Benz (MB) [39]. The responsible handling of 19 vulnerabilities found in the Daimler back end and in the Telematics Control Unit (TCU), which is included in all MB connected cars was presented at the RSA Conference. The researchers were able to remotely unlock the door and start the engine. This attack potentially affected all MB connected cars in China (estimated over 2 million). Within two days after the report to Daimler AG, MB reacted with a mitigation. Vulnerable services were shut down to prevent damage. Already five days after the report MB provided a first fix, so that after three weeks, all access vulnerabilities were fixed and there was no longer any threat to the end customers. Due to the appropriate acting of the parties involved, coordinated, limited information about the vulnerabilities could be published and discussed about six months after the first report.

4. Disclosure and Usage of Automotive Vulnerability Information

4.1. Joint Schemes for Description and Sharing of Vulnerabilities and Their Information

The first automotive vulnerabilities have been already included in the CVE list for previously classic IT vulnerabilities some years ago and thus in publicly accessible databases worldwide. The CVE is a centralized point for automated synchronization of vulnerability databases worldwide. In classical IT, it not only represents an important part of the global dissemination of vulnerability information, but also creates a uniform naming and description system for vulnerabilities which is understood globally. An approach how to adapt this for better addressing automotive needs is discussed in Section 6. The first publicly disclosed attack on a vehicle led to an entry in the NVD in 2015 [40]. To provide an overview, Sommer et al. [41] collected exhaustive data on automotive attacks in their Automotive Attack Database-AAD [42]. This database contains attacks found and published by researchers between 2010 and 2018. It contains over 400 entries on exploited vulnerabilities, which are linked to 162 attacks. This practice of uniquely and quickly identify, track, and eliminate automotive security issues should be intensified within the automotive sector. The basis for this practice is the willingness to deal with weaknesses and incidents in a transparent manner. This requires confidential handling when exchanging sensitive vulnerability information within the disclosure process. A trustworthy communication infrastructure, which is widely accepted within the industry, standardizes and automates the transfer of information across companies in order to achieve time efficiency can help to meet this need (see MISP [43], OASIS-STIX/TAXII [44], FIRST-TLP [45], FIRST-IEP [46], ICASI-CVRF [47]). In order to meet the challenges of the special automotive supplier structures with increasing cross-industry networking and to promote the exchange of information, an information security certification based on the TISAX [48] could also increase mutual trust. Trust and transparency is essential between OEMs and their suppliers. An exchange of vulnerability information helps all affected parties to handle incidents more efficiently, reduce their costs and achieve higher product quality.

4.2. Conditions for a Beneficial Disclosure Culture

In addition to building a trustworthy infrastructure for the exchange between companies, each company should have sufficient internal resources and structures to be able to react appropriately to all reports and not provoke conflicts with finders. This also includes a concept for report prioritization, as well as the definition of common criteria for the vulnerability specific evaluation of appropriate grace periods for the communication of vulnerability information, the development of mitigations or patches, and for their implementation in the target system. In this way, industry-wide recognized guidelines can be created for the definition of contractual agreements on the disclosure process. In the event of uncoordinated public disclosure, each manufacturer and a potential coordinator should have defined and agreed escalation or emergency plans. A sound understanding of the incentives for action of the free hacker community and security research are helpful here. In the automotive sector, there is currently a lack of parties who can accompany a disclosure process as a mediating coordination and arbitration body if required (see CERT/CC [24] for IT). The essential requirements for such a body are its independence (non-profit), expertise and broad recognition, integrity and networking within the industry. An active role, particularly on the part of public authorities, but also of other non-profit organizations, would be desirable. The ENISA Cars and Roads SECurity (CaRSEC) Expert Group [49] could embody these attributes. To address potential finders and encourage them to get in touch with the manufacturer concerned, a precisely formulated disclosure policy has to be publicly available. Such a policy should address all issues discussed to achieve a high rate of valid reports (scope), build trust (transparency, safe harbor) and create incentives for cooperation (rewarding, Hall of Fame). A reporting form can enable an automated processing of the transmitted data and give the finder orientation for essential information. This can help to speed up the assessment of the reporting process and save resources.

4.3. Multiplying Benefits Through Sharing of Informaton

Not only for the continuous improvement of the security of the vehicle during its operating phase, the benefit for all parties involved can be multiplied by an intensive exchange of information on vulnerabilities. Also during the product development phase, manufacturers can increase their benefit from the vulnerability data obtained by merging their data pools with industry partners and, for example, improve the precision of automated threat and risk analyses and penetration testing by using a database which is as broad as possible (Dürrwang et al. [50]). This aspect should be taken into account for a cost-benefit calculation for a VD program.

4.4. The Automotive Strategy for Vulnerability Disclosure

The benefits of a vulnerability disclosure program, as well as its special role with regard to the automotive-specific challenges, have already been discussed in Sections 2 and 3. The orientation towards standard patching times from IT is not recommended for the automotive sector, nor is the application of strict deadlines for the patching process (grace periods). A major uncertainty factor for the definition of generally valid grace periods is the complex horizontal and vertical supplier structure within the automotive industry and occasionally long communication channels. The enormous safety criticality as well as a lack of empirical values for appropriate patching times for vulnerabilities in vehicles require a more careful handling of disclosure. In addition, careful security tests or type approval renewals may be necessary for patches. The time required for such a renewal can neither be estimated in advance nor directly influenced by the manufacturer. Also a time estimate of patch distribution is still problematic today (over-the-air-update technology is hardly widespread), as is the reliable implementation of patches in the target system. Instead of providing a finder concrete information on the patching time in the disclosure policy, transparency should be better achieved by specifically pointing out special challenges in the automotive sector. Broadly recognized and comprehensible criteria for the initial assessment of patching and grace periods in relation to vulnerabilities and their event-triggered adjustment in the course of the disclosure process must be defined jointly (see Section 7). Furthermore, predefined plans for escalation management (e.g., involvement of an independent coordinator) and criteria for triggering them should be agreed. For type approval for their cars, OEMs must prove the existence and suitability of processes, which serve to detect vulnerabilities and attacks and react appropriately. In addition, OEMs have to prove processes, which serve to provide relevant data to support the analysis of attacks. OEMs not only have a special role in the disclosure of reported vulnerabilities. It is also up to them to identify risks (e.g., non-existent processes) from suppliers and service providers and to prove their compliance with existing regulation.

The disclosure strategy the ISO/IEC 29147 [15] proposes is shown in Figure 1. It shows the dependencies of all parties involved in the process. The finder remains passive and outside after the report has been submitted. A continuous communication in the sense of coordinated disclosure and the associated transparency cannot take place. A process as it is propagated for the automotive sector is hinted by the three thickly drawn bidirectional arrows, which are added to the original image. Thus, this adapted approach is qualitatively in alignment with the FIRST approach for multi-party coordinated disclosure [51], which focuses on the well-being of the customer as the highest good to be protected.

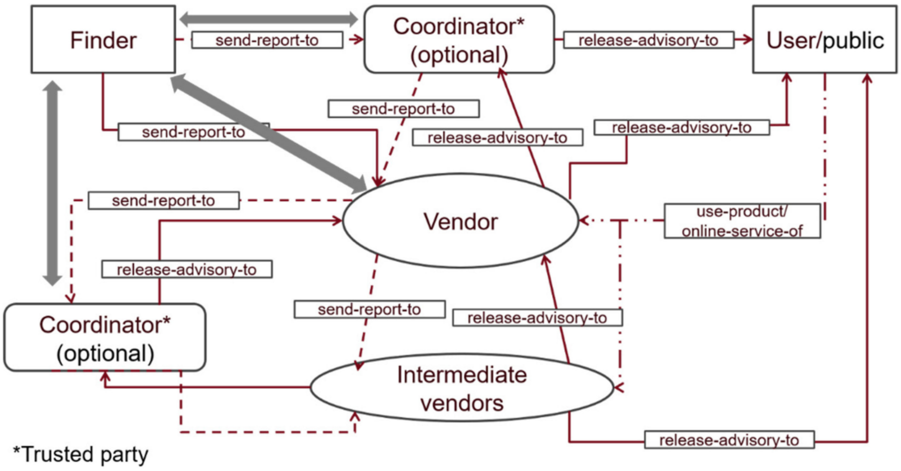

Figure 1. Approach of ISO/ICE 29147 and modification proposal for application in the automotive field indicated by bold arrows.

4.5. Process Description, Requirements and Responsibilities

With the exception of the adaptation outlined in Figure 1, a VD process for the automotive sector is not basically different to the procedures described in the established standards [15] and [16] already discussed and in the work of FIRST [51]. For this reason, not the disclosure process itself is discussed here. Instead, all parties are addressed which are actively involved in the process and those who work in the automotive environment and indirectly place requirements on the disclosure of vulnerabilities. Special attention is given to requirements specific to the automotive sector or to the scope, which, in the author's view, still needs to be established in the automotive sector.

In the following, the requirements, roles and responsibilities which all parties involved in the process have to meet will be discussed. These are (i) manufacturer, (ii) finder, (iii) coordinator, (iv) public and user, (v) governmental organizations, (vi) testing organizations and independent workshops. The consideration includes the phase of preparation, implementation—including patch approval and dissemination—as well as the follow-up of the disclosure process.

4.5.1. Manufacturer

This includes all producers of hardware, software and other vehicle components, which are connected along the vertical and horizontal supply chain. These are OEMs, suppliers and sub-suppliers. For an efficient disclosure process, intensive networking is just as important as contractual agreements for dealing with vulnerabilities such as grace periods for their mitigation and patching. OEMs, in particular, have special obligations in relation to the UNECE regulations already discussed in ensuring cyber security along the entire supply chain.

4.5.2. Finder

This group includes security experts who act on their own initiative, security researchers who are usually financed by public funds (academia), hobby hackers or professional hackers (private individuals). Security experts who work for a company, for example, are less likely to be addressed by a VD program, as they are already acting on behalf of another company or their own. In the automotive sector, the group of free, non-employed hackers is not yet very large, but it is growing steadily. Contests such as the regularly held Black Hat are increasingly addressing the automobile and its environment. In addition to academic research and commercial service providers, this group represents a valuable resource for OEMs and suppliers to expand their threat intelligence. Penetration tests can be supplemented cost-effectively and thus the product development process can be improved.

4.5.3. Coordinator

Coordinators are usually groups of experts organized by public, private or institutional bodies, such as Computer Emergency Response Teams (CERTs) or Computer Incident Response Teams (CSIRTs). These have their origins in IT, but can also serve as contact entities beyond that. During a disclosure process, they can act as moderators between parties with conflicting interests and points of view. In addition, they can also act as operators of a reporting office for vulnerabilities (e.g., U.S. CERT/CC) or cyberattacks on companies (CERT alliance of the BSI). Some also operate their own vulnerability databases or platforms where advisories are published. Intensifying the networking of CSIRTs in Europe is a defined goal in the EU (NIS Directive [52]). With the initialization of the CaRSEC Expert Group [49] in 2016, a first approach within the EU towards an independent entity specifically for the automotive sector already exists. It remains to be seen to what extent the CaRSEC Expert Group meets necessary qualities to act as a coordinating entity. We think that these qualities are independence, expert competence, an extensive global networking within the industry and, in particular, high acceptance by manufacturers and the hacker community.

4.5.4. Public and Users

One of the biggest weak points within the networked world (regardless of the sector) is the human being himself [53]. It is to protect health and personal data of the public and to raise awareness of cyber risks in the vehicle. The discussed UNECE regulation [7] explicitly refers to the human factor as a potential risk in Annex 5 List of threats and corresponding mitigations. It lists threats to vehicles due to unintended, legitimated human actions, facilitating a cyber attack (Innocent victims are tricked, security procedures are not followed). According to a report by Upstream Security [54], over 4% of known cyber incidents in 2020 were directly related to unintended human actions. Independent of mitigations recommended by the UNECE, public disclosure of fixed vulnerabilities can promote public awareness of the responsible use of the vehicle as a potentially threatened cyber physical system. When users start to see the security of a vehicle as a criterion for its quality, this can additionally strengthen the constructive, open handling of vulnerabilities and establish VD programs as proof of quality.

4.5.5. Governmental Organizations

The worldwide harmonization of legislation regarding ethical hacking is as necessary as it is impossible. Nevertheless, national authorities should lead by example. Instead, only 2 out of 27 EU member states have an official, legally recognized disclosure policy [29]. Only the Netherlands has specific exceptions for ethical hacking in its legislation. Official contact points for reporting could close the gap that the automotive industry still leaves open with regard to VD. Having a VD program should be an elementary means for manufacturers to prove compliance with upcoming regulations (Cybersecurity management system). Publicly accessible automotive vulnerability or attack databases could help to create transparency on fixed vulnerabilities, build up threat intelligence for governmental authorities and raise public awareness. Furthermore, in order to promote a fair market, framework conditions should be created so that independent workshops can also have access to patches from the manufacturer.

4.5.6. Testing Organizations and Independent Workshops

Testing organizations and independent workshops do not have an active part within the disclosure itself. However, as contractors of approval authorities, testing organizations are involved in the approval processes for developed patches for open vulnerabilities. Thus, they can become a critical time bottleneck within the disclosure process. Here it is important to build up the necessary awareness and expertise for automotive security, especially in the case of critical vulnerabilities. Both, independent workshops and testing organizations should have the possibility to get access to released patches and information about patch history to be able to provide or test the latest version of patches in the context of general inspections or services.

Finally, Figure 2 gives an overview of an automotive vulnerability disclosure process and assigns key elements and stakeholders to the individual phases from a process and technical perspective. Framed by dashed lines are those elements, which currently offer particular potential for improvement in the automotive sector.

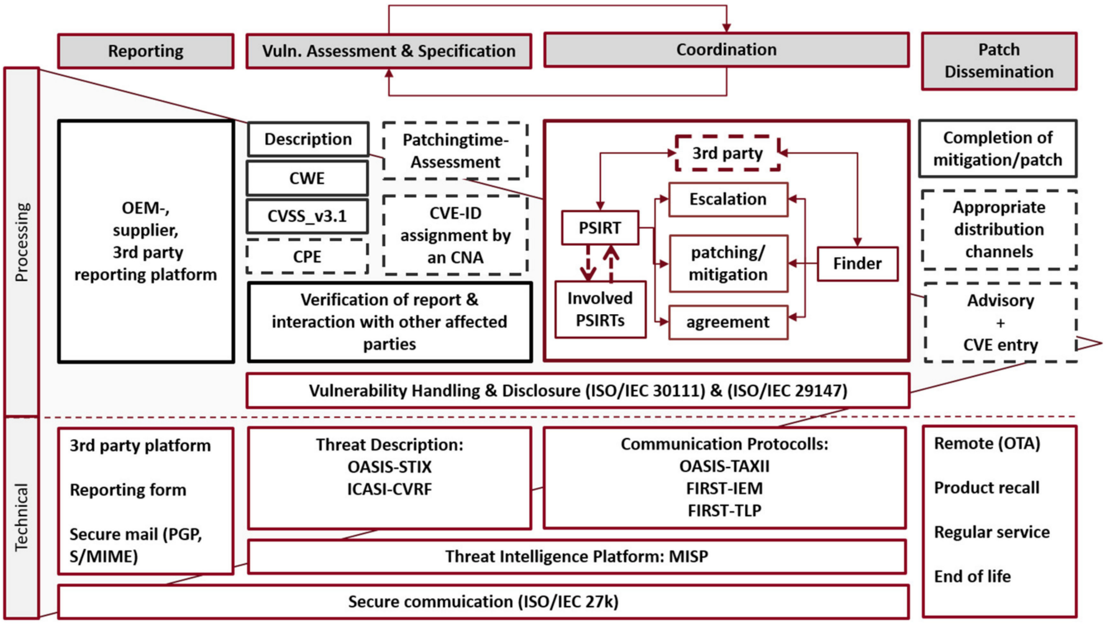
Reporting
Vuln. Assessment & Specification
Coordination
Patch Dissemination
Processing
OEM-, supplier, 3rd party reporting platform
Description
CWE
CVSS_v3.1
CPE
Patchingtime-Assessment
CVE-ID assignment by an CNA
Verification of report & interaction with other affected parties
3rd party
PSIRT
Escalation
patching/ mitigation
Finder
Involved PSIRTs
agreement
Completion of mitigation/patch
Appropriate distribution channels
Advisory + CVE entry
Vulnerability Handling & Disclosure (ISO/IEC 30111) & (ISO/IEC 29147)
Technical
3rd party platform
Reporting form
Secure mail (PGP, S/MIME)
Threat Description: OASIS-STIX ICASI-CVRF
Communication Protocolls: OASIS-TAXII FIRST-IEM FIRST-TLP
Threat Intelligence Platform: MISP
Remote (OTA)
Product recall
Regular service
End of life
Secure commuication (ISO/IEC 27k)

Figure 2. Overview of the phases of automotive vulnerability disclosure from a process and technical perspective.

5. Conclusions

In this paper, the implementation of VD in the automotive environment is discussed. Potentials and challenges for their implementation are specified. In Sections 1 and 2, the development of VD and the resulting findings from the IT environment are highlighted. Based on decades of experience and further development in IT, conclusions can be drawn for the automotive sector. The special conditions and challenges in this environment, which are also named and discussed are taken into account. In Section 3, pleasant and unpleasant practical examples from the automotive environment are considered and existing opportunities and challenges are reflected. In Section 4, the authors discuss the key areas of activity within the industry regarding vulnerability management and especially vulnerability disclosure. Furthermore, roles and requirements of various potential stakeholders in the automotive environment are discussed and potentials for improvement are identified. The responsible disclosure, as well as the public handling of vulnerabilities in IT (NVD, CVE, etc.) gained importance in the last 8 years. Such a development is also to be expected for the automotive industry and has already begun. A growing public awareness of the vehicle as a potentially vulnerable target will reinforce this development. A study from 2007 suggests that an open approach to vulnerabilities and their announcing but also their fixing has an impact on the monetary value of companies. In addition, current regulations, as well as government and industry associations (e.g., EU, UN, AUTO-ISAC) are increasing the pressure on manufacturers to implement measures to maintain security in the post-production phase. Vulnerability management measures and, in particular, VD processes are essential components for meeting the given challenges. In recent years, the public visibility of vulnerabilities, as measured by reserved CVEs, is also increasing. VD programs are now widespread among OEMs, but they still can learn from IT in designing a VD process, draw on mature technical protocols and platforms for information exchange (vulnerability description, sharing platforms, public databases), vulnerability assessment schemes, and mature processes for responsible disclosure. However, adaptions are needed due to specifics of their industry. This is the enormous relation to the safety of their products, the advancing autonomization and connectivity, significantly longer product life cycles, complex supplier structures, as well as a more difficult patch dissemination according to today's state. The timing of processes should therefore take particular account of potentially highly sensitive, life-threatening vulnerability information (grace periods). In addition, the will and capability of manufacturers for joint efficient vulnerability management, both internally and externally, should be built. Efforts should be intensified to exploit the hacker scene and its noteworthy value in maintaining security in the post-production phase. Essential to this is the benefit of an appropriate disclosure policy to eliminate existing legal uncertainty and create transparent disclosure processes. Different concepts of handling VD were discussed and finally Coordinated Disclosure was identified as the most target-oriented for the automotive environment. To achieve sufficient patch dissemination, OTA updates are important.

6. Related Discussion

Questions as to whether networked, autonomous vehicles of the future could potentially one day meet the criteria for critical infrastructure could become ever louder (EU Directives 2016/1148 [52] and 2008/114/EC [55]). A vehicle itself is not an infrastructure by definition. But the question, in which extent highly networked fleets interacting with each other and with the infrastructure constitute a "traffic control and guidance system". However, with regard to the disclosure of vulnerabilities and security incidents, this would have the consequence of legal reporting and handling obligations for the manufacturers.

The CVE list as a centralized point for automated synchronization of vulnerability databases and the CVE scheme to uniquely identify, track, and eliminate security issues was introduced in Section 4.1. An increasing number of vulnerabilities are being added to the CVE list (Total: 110 entries, in 2020 33 entries, in 2019 24 entries, by 11/25/20 [54]). These vulnerabilities are thus available to the global automotive environment in a syncronizable form to improve threat intelligence. In their 2020 paper, Bajpai et al. even propagate the introduction of a special naming system (Common Vehicle Vulnerabilities-CVV), especially for automotive vulnerabilities with its own CVV-ID [56]. The authors see the AUTO-ISAC as a possible central body for maintaining the CVV system. Furthermore, the continous expansion of the Common Platform Enumeration (CPE) [57] with automotive related components should be focused.

Bajpai et al. also demonstrate that the Common Vulnerability Scoring Systems (CVSS) [58] from classical IT can easily be adapted for the severity evaluation of automotive vulnerabilities. Other works by FFRI Inc. [59] and Ando et al. [60] reach similar conclusions. In addition, the new ISO/IEC 21434 recommends the CVSS Exploitability metric for the evaluation of automotive attack feasibility.

Already in the introduction, bug bounty programs were described as common and highly efficient in regular IT. In addition to a VD program, benign hackers can be motivated to stress specifically certain subsystems, or to seek out specific vulnerability types. With this incentive system, manufacturers can take an active role in attracting the world's most skilled hackers. Also for the automotive environment, this can be an important part of a VD strategy. Since 2016, the spread of bug bounty programs has been increasing when FCA established the first automotive OEMs bug bounty program [7,61]. Since such programs can mean a high investment of time and money, a manufacturer should weight up to what extent such a program is appropriate.

Effective disclosure and remediation of discovered vulnerabilities in the post-production phase is important for continuous preservation of cyber security. However, patches can only protect against risks once they have been installed in the vehicle. Therefore, the effective dissemination of the developed patches has a key role. To achieve this, over-the-air (OTA) updates are essential. While OTA updates become more frequent in recent years, for today's vehicles software updates can in many cases only be implemented via physical access, which leads to a greatly delayed or uneconomical elimination of potentially dangerous vulnerabilities in post-production phase. Further dissemination of OTA technology is desirable. The world's second-largest passenger car manufacturer, Volkswagen, made the first step in this direction by announcing to offer OTA for their ID.3 and ID.4 models across Europe starting in summer 2021 [62].

7. Further Work

The necessity to evaluate appropriate vulnerability related patching times was identified beforehand since there is a lack of experience for this issue within the automotive domain. Moreover, the specification of blanket and inflexible grace periods is negligent and not responsible in the automotive environment. This is currently being addressed in the project SecForCARs. A metric to assess the reasonable grace periods for reported vulnerabilities is under development. The applicability of this metric focuses on report prioritization and the finding of criterias for appropriate interface agreements. Moreover, a concept for describing and storing information from reported automotive vulnerabilities in a vulnerability database is under development. Such a database can deal manufacturers to enhance their product development process by making threat analysis more comprehensive. In addition, it can serve manufacturers or authorities to improve their threat intelligence abilities.

Author Contributions: Conceptualization, R.B.; methodology, R.B.; formal analysis, R.B.; investigation, R.B.; writing—original draft preparation, R.B.; writing—review and editing, R.K.; supervision, R.K.; project administration, R.K.; funding acquisition, R.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the German Federal Ministry of Education and Research (BMBF) in the context of the project SecForCARs under grant number 01KIS079.

Acknowledgments: Thanks to all project members who have contributed with their review. Special thanks to the project members Karsten Schmidt, Frank Kargl and Bastian Könings.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

VD	Vulnerability Disclosure
CPE	Common Platform Enumeration
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
CERT	Computer Emergency Response Team

CSIRT	Computer Security Incident Response Team
CSMS	Cyber Security Management System
NVD	National Vulnerability Database
MB	Mercedes-Benz
OTA	Over-the-Air
TCU	Telematic Control Unit

References

1. Telang, R.; Wattal, S. An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price. *IEEE Trans. Softw. Eng.* **2007**, *33*, 544–557. [CrossRef]
2. NIST, NVD—National Vulnerability Database. Available online: https://nvd.nist.gov/vuln/full-listing (accessed on 20 April 2020).
3. Hackerone, General Motors Celebrates Second Anniversary with Hackers Customer Stories. 2018. Available online: https://www.hackerone.com/blog/General-Motors-Celebrates-Second-Anniversary-Hackers (accessed on 20 April 2020).
4. Statista GmbH. Lebensdauer von Autos in Deutschland Nach Automarken. Available online: https://de.statista.com/statistik/daten/studie/316498/umfrage/lebensdauer-von-autos-deutschland/ (accessed on 10 April 2020).
5. Krempl, F. Security by Design im Auto: Neue UN-Vorgaben Für Cybersicherheit von Fahrzeugen. Available online: https://www.heise.de/news/Security-by-Design-Neue-UN-Vorgaben-fuer-Cybersicherheit-im-Auto-4767180.html?seite=all (accessed on 28 May 2020).
6. McKinsey & Company, GSA. Cybersecurity in Automotive—Mastering the Challenge. Available online: https://www.gsaglobal.org/resources/cybersecurity-in-automotive-mastering-the-challenge/ (accessed on 10 April 2020).
7. UNECE/TRANS/WP.29/GRVA. Proposal for a New UN Regulation on Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System. Available online: https://unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf (accessed on 23 July 2020).
8. UNECE/TRANS/WP.29/GRVA. Proposal for a New UN Regulation on Uniform Provisions Concerning the Approval of Vehicles with Regards to Software Update and Software Updates Management System. Available online: https://undocs.org/ECE/TRANS/WP.29/2020/80 (accessed on 25 March 2021).
9. UNECE Press Releases. UN Regulations on Cybersecurity and Software Updates to Pave the Way for Mass Roll Out of Connected Vehicles. Available online: https://unece.org/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll-out-connected-vehicles (accessed on 23 March 2021).
10. ISO/SAE FDIS 21434, Road vehicles—Cybersecurity Engineering. 2020. Available online: https://www.iso.org/standard/70918.html (accessed on 29 April 2020).
11. Upstream Security. Global Automotive Cybersecurity Report. Available online: https://www.upstream.auto/research/automotive-cybersecurity/?id=null (accessed on 5 April 2020).
12. Euro NCAP Crashtest. Available online: https://www.euroncap.com/en/ratings-rewards/latest-safety-ratings/ (accessed on 10 April 2020).
13. ADAC Pannenstatistik. Available online: https://www.adac.de/rund-ums-fahrzeug/unfall-schaden-panne/adac-pannenstatistik/ (accessed on 5 April 2020).
14. CERT/CC Computer Emergency Response Team/Coordination Center. What is Vulnerability Coordination? Available online: https://vuls.cert.org/confluence/pages/viewpage.action?pageId=4718642 (accessed on 28 May 2020).
15. ISO/IEC 29147:2014 Information technology—Security techniques—Vulnerability Disclosure. 2014. Available online: https://www.iso.org/standard/45170.html (accessed on 29 April 2021).
16. ISO/IEC 30111:2019, Information technology—Security techniques—Vulnerability Handling, amended in 2019. Available online: https://www.iso.org/standard/69725.html (accessed on 29 April 2021).
17. Google Security Team. Rebooting Responsible Disclosure: A focus on Protecting End Users. Available online: https://security.googleblog.com/2010/07/rebooting-responsible-disclosure-focus.html (accessed on 28 May 2020).
18. Jan Neutze (Microsoft), Coordinated Vulnerability Disclosure (CVD), CEPS Event: Software Vulnerabilities Disclosure: The European Landscape, Brussels. 23 June 2017. Available online: https://www.ceps.eu/wp-content/uploads/2017/05/Jan%20Neutze%20Microfsoft%20-%20CVD.pdf (accessed on 29 April 2021).
19. About the Zero Day Initiative. Available online: https://www.zerodayinitiative.com/about/ (accessed on 20 April 2020).
20. CERT/CC Computer Emergency Response Team/Coordination Center. Vulnerability Reporting Form. Available online: https://www.kb.cert.org/vuls/vulcoordrequest/ (accessed on 28 May 2020).
21. Zero Day Initiative. The Zero Day Initiative Disclosure Policy. Available online: https://www.zerodayinitiative.com/advisories/disclosure_policy/ (accessed on 20 April 2020).
22. Rapid7. The Rapid7 Disclosure Policy. Available online: https://www.rapid7.com/security/disclosure/ (accessed on 20 April 2020).
23. Project Zero. Policy and Disclosure: 2020 Edition. Available online: https://googleprojectzero.blogspot.com/2020/01/policy-and-disclosure-2020-edition.html (accessed on 8 March 2020).

24. CERT/CC. The CERT/CC Disclosure Policy. Available online: https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy (accessed on 20 April 2020).
25. McQueen, M.; Wright, J.; Wellman, L. Are Vulnerability Disclosure Deadlines Justified? In Proceedings of the Third International Workshop on Security Measurements and Metrics, Banff, AB, Canada, 21 September 2011. [CrossRef]
26. Arora, A.; Telang, R.; Xu, H. Optimal Policy for Software Vulnerability Disclosure. *Manag. Sci.* **2008**, *54*, 642–656. [CrossRef]
27. Zhao, M.; Laszka, A.; Grossklags, J. Devising effective policies for bug-bounty platforms and security vulnerability discovery. *J. Inf. Policy* **2017**, *7*, 372–418. [CrossRef]
28. Hackerone. The 2020 Hacker Report. Available online: https://www.hackerone.com/resources/reporting/the-2020-hacker-report (accessed on 5 May 2020).
29. CEPS Working Group. Vulnerability Disclosure in Europe-Technology, Policies, Legal Challenges. Available online: https://www.ceps.eu/download/publication/?id=10636&pdf=CEPS%20TFRonSVD%20with%20cover_0.pdf. (accessed on 5 May 2020).
30. AUTO-ISAC. Best Practices-Incident Response v1.3, July 2019. Available online: https://automotiveisac.com/best-practices/.
31. Bolz, R.; Rumez, M.; Sommer, F.; Dürrwang, J.; Kriesten, R. Enhancement of Cyber Security for Cyber Physical Systems in the Automotive Field Through Attack Analysis. In Proceedings of the Embedded World Conference 2020, Nuremberg, Germany, 25–27 February 2020; Available online: https://www.researchgate.net/publication/339643941_Enhancement_of_Cyber_Security_for_Cyber_Physical_Systems_in_the_Automotive_Field_Through_Attack_Analysis (accessed on 29 April 2021).
32. Kurachi, R.; Takada, H. Improving secure coding rules for automotive software by using a vulnerability database. In Proceedings of the International Conference on Vehicular Electronics and Safety, Madrid, Spain, 12–14 September 2018. [CrossRef]
33. Verdult, R.; Garcia, F.; Ege, B. Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer. In Proceedings of the 22nd USENIX Security Symposium, Wahington, DC, USA, 14–16 August 2013.
34. The Guardian. Security Flaw Affecting More Than 100 Car Models Exposed by Scientists. Available online: https://www.theguardian.com/technology/2015/aug/18/security-flaw-100-car-models-exposed-scientists-volkswagen-suppressed-paper (accessed on 27 June 2020).
35. Pentest Partners Block-Automotive Security, Hacking the Mitsubishi Outlander PHEV Hybrid. Available online: https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/ (accessed on 27 June 2020).
36. Keen Security Lab. Experimental Security Assessment of BMW Cars: A Summary Report. Available online: https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/ (accessed on 27 June 2020).
37. MITRE Corporation. Common Vulnerabilities and Exposures (CVE) List. Available online: https://cve.mitre.org/ (accessed on 23 July 2020).
38. Mahaffey, K. Hacking a Tesla Model S: What We Found and What We Learned, Lookout Blog. Available online: https://blog.lookout.com/hacking-a-tesla (accessed on 12 November 2020).
39. The Sky-Go Team (360). Security Research Report on Mercedes-Benz Cars. Available online: https://skygo.360.cn/archive/Security-Research-Report-on-Mercedes-Benz-Cars-en.pdf (accessed on 12 October 2020).
40. National Institute for Standards and Technology (NIST), National Vulnerability Database; CVE-20155611. Available online: https://nvd.nist.gov/vuln/detail/CVE-2015-5611#VulnChangeHistorySection (accessed on 15 July 2020).
41. Sommer, F.; Duerrwang, J.; Kriesten, R. Survey and Classification of Automotive Security Attacks. *Information* **2019**, *10*, 148. [CrossRef]
42. Automotive Attack Database (AAD). Institute of Energy Efficient Mobility at Karlsruhe University of Applied Sciences. Available online: https://github.com/IEEM-HsKA/AAD (accessed on 7 October 2020).
43. Malware Information Sharing Platform (MISP). Available online: https://www.misp-project.org/ (accessed on 7 October 2020).
44. OASIS CTI, STIX/TAXII Threat Intelligence Sharing. Available online: https://oasis-open.github.io/cti-documentation/ (accessed on 7 October 2020).
45. FIRST, Traffic Light Protocol (TLP). Available online: https://www.first.org/tlp/ (accessed on 7 October 2020).
46. FIRST, Information Exchange Policy. Available online: https://www.first.org/iep/ (accessed on 7 October 2020).
47. ICASI, Common Vulnerability Reporting Framework (CVRF). Available online: https://www.icasi.org/cvrf/ (accessed on 7 October 2020).
48. VDA-ISA, TISAX 1–Model. Available online: https://www.vda.de/dam/vda/publications/Empfehlung%20Informationsschutz%202005/Beschreibung%20TISAX%20und%20VDA-ISA%20f%C3%BCr%20VDA%20Webseite-DE.PDF (accessed on 7 October 2020).
49. Terms of Reference for the ENISA Cars and Roads Security (CarSEC) Experts Group. Available online: https://www.enisa.europa.eu/media/news-items/terms-of-reference-for-the-enisa-cars-and-roads-security-carsec-experts-group (accessed on 23 July 2020).
50. Dürrwang, J.; Beckers, K.; Kriesten, R. A Lightweight Threat Analysis Approach Intertwining Safety and Security for the Automotive Domain. In Proceedings of the International Conference on Computer Safety, Reliability and Security, Trento, Italy, 13–15 September 2017.
51. FIRST Vulnerability Coordination SIG & NTIA. The Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure. Available online: https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1 (accessed on 23 July 2020).

52. EU Directive 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, July 2016. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148 (accessed on 29 April 2021).
53. Security Insider. Was Cyberkriminelle 2020 Bewegt. Available online: https://www.security-insider.de/was-cyberkriminelle-2020-bewegt-a-899804/?cmp=nl-4&uuid=93A2AF8C-BEE5-44A8-A609-ADCC489E9CF3 (accessed on 17 December 2020).
54. Upstream Security. Global Automotive Cybersecurity Report. Available online: https://upstream.auto/2021report/ (accessed on 17 December 2020).
55. EU Directive 2008/114/EG, Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, December 2008. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=DE (accessed on 29 April 2021).
56. Bajpai, P.; Enbody, R. Towards Effective Identification and Rating of Automotive Vulnerabilities. In Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security—AutoSec'20, New Orleans, LA, USA, 18 March 2020.
57. NIST-CSRC. Common Platform Enumeration (CPE) Method. Available online: https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe (accessed on 23 July 2020).
58. The FIRST CVSS-SIG. Common Vulnerability Scoring Systems (CVSS). Available online: https://www.first.org/cvss/ (accessed on 2 October 2020).
59. FFRI Inc. Latest Security Reports of Automobile and Vulnerability Assessment by CVSSv3. Available online: https://de.slideshare.net/ffri/latest-security-reports-of-automobile-and-vulnerability-assessment-by-cvss-v3-ffri-monthly-research-20159 (accessed on 2 October 2020).
60. Ando, E.; Kayashima, M.; Komoda, N. A Proposal of Security Requirements Definition Methodology in Connected Car Systems by CVSS v3. In Proceedings of the 5th IIAI International Congress on Advanced Applied Informatics, Kumamoto, Japan, 10–14 July 2016.
61. Cyberscoop. Automotive Companies Are Warming up to Vulnerability Disclosure Programs. Available online: www.cyberscoop.com/vulnerability-disclosure-programs-automotive-companies-general-motors-hackerone/ (accessed on 4 October 2020).
62. Volkswagen Press Release. Volkswagen Strives for Digital Leadership—the ID. Family Will Be Launched with Regular "Over-the-Air" Updates in 2021. Available online: https://www.volkswagenag.com/en/news/2021/03/volkswagen-strives-for-digital-leadership.html, (accessed on 23 March 2020).