Automotive Innovation
https://doi.org/10.1007/s42154-022-00203-2

ORIGINAL ARTICLE

# A Double Assessment of Privacy Risks Aboard Top-Selling Cars

**Giampaolo Bella**[1] · **Pietro Biondi**[1] · **Giuseppe Tudisco**[2]

Received: 9 March 2022 / Accepted: 6 November 2022


**Abstract**
The advanced and personalised experience that modern cars offer makes them more and more data-hungry. For example, the cabin preferences of the possible drivers must be recorded and associated to some identity, while such data could be exploited to deduce sensitive information about the driver's health. Therefore, drivers' privacy must be taken seriously, requiring a dedicated risk assessment framework, as presented in this paper through a double assessment combining the asset-oriented ISO approach with the threat-oriented STRIDE approach. The framework is tailored to the level of specific car brand and demonstrated on the ten top-selling brands as well as, due to its innovative character, Tesla. The two approaches yield different, but complementary findings, demonstrating the additional insights gained through their parallel adoption.

**Keywords** Automotive · Cyber physical systems · Risk management · ISO 27005 · STRIDE

## 1 Introduction

Safety, cyber-security and privacy intertwine aboard modern cars. While safety is always the primary objective, security comes close and intertwines safety, because modern cars are more and more intensively computerised. For example, no driver would like her cabin preferences to be altered remotely by someone else and, worse still, her lane assistance system to be hijacked. These are the reasons why cyber-security expertise and related socio-technical measures have been ported, since the beginning of the last decade especially, to the automotive world. As a result, a simple car repair session may occur solely logical today, for example to review and reset an error message that got triggered sporadically.

Cyber-security is known to be a circular process that sees the perennial addition of security measures, which may eventually get broken by upcoming attack techniques calling, in turn, for yet more measures. This implies that some cyber-security risk always exists, and notable works have been advanced to asses that risk specifically in the automotive domain, as noted below. The motivating observation of the present article is that comparatively less attention has been paid to the privacy risks in the same domain.

Modern cars acquire a variety of data, including music preferences, payment information and environmental information such as temperature, GPS coordinates and camera streams. Some cars explicitly collect the driver's personally identifiable information (PII), hence the mass of data that a car treats is personal data because it can be easily referred to a natural person. When PII is not treated, it could be inferred with high approximation in various ways, including by querying the Public Vehicle Register, in particular by an attacker with data exfiltration aims.

Despite the tight relationship between cyber-security and privacy, which recognises the role of cyber-security measures to protect personal data, we contend that privacy requires a separate argument from cyber-security, particularly in terms of risk assessment, for various reasons. One is that the existing risk assessment frameworks, recalled below, do not appear to revolve around personal data. Another one is the plethora of personal data that is involved, which may even include sensitive data, for example about the driver's

Academic Editor: Zhongxu Hu

✉ Giampaolo Bella
giamp@dmi.unict.it

✉ Pietro Biondi
pietro.biondi@phd.unict.it

✉ Giuseppe Tudisco
giuseppe.tudisco@inaf.it

[1] Dipartimento di Matematica e Informatica, Università degli Studi di Catania, Catania, Italy

[2] Osservatorio Astrofisico di Catania, Istituto Nazionale di Astrofisica, Catania, Italy

Published online: 06 January 2023

health and religion [1]. Moreover, there is evidence that drivers' understanding of the implications on their privacy deriving from their use of a car is somewhat ill-understood [2]. Privacy concerns rise particularly in Europe, where EU Regulation 2016/679, the "General Data Protection Regulation" (GDPR) addresses privacy as highly as an element of "protection of natural persons" [3]. Here comes the full motivation for the work presented in this article.

There are two best-known approaches to conduct risk assessment. One is oriented to assets, as pioneered by ISO 27005 [4] and its ancestors. This approach pursues a discourse that is clearly pivoted around the value of assets. When privacy is the overall objective of the risk assessment, as in our case, all assets are types of personal data. When the domain is automotive, such data is of various types, as outlined above, and refers to the driver (and more sporadically to passengers). The other notable risk assessment approach is oriented to threats and is termed STRIDE [5]. It prescribes a process resting on 6 threat categories and produces insights on how threats and threat categories affect a target system such as a car brand, namely all cars of that brand.

### 1.1 Related Work

The ISO 26262 international standard [6] is among the best known standards for the automotive domain, hence must be recalled here. It concerns functional safety in the overall domain and, in particular, for electrical and electronic systems employed aboard modern cars [7]. That standard is not directly related to our work, which specifically targets a different property, privacy.

Risk assessment has been framed quite a few times in the context of modern vehicles, in the last decade especially. The work by Wolf and Scheibel [8] can be considered a milestone in its pioneering contextualisation in automobiles. However, the framework used is rather basic, and the demonstrating example only concerns attacks to ECU firmware. The need to source information to support the assessment is acknowledged through the definition of a questionnaire to collect information.

Macher et al. [9] instrument risk assessment over safety and security by advancing the so called "Safety-Aware Hazard Analysis and Risk Assessment" (SAHARA) Approach. It combines the "Hazard Analysis and Risk Assessment" (HARA) approach to safety risk assessment with STRIDE in a rather intuitive way but is only demonstrated on a very small example. A sibling contribution by Monteuuis et al. [10] is the "Security Automotive Risk Analysis Method" (SARA) approach, which considers attacker's features such as knowledge, expertise and equipment as explicit parameters of the assessment. This may be useful when a characterisation of a threat with respect to the specificity of the attacker is requested, whereas this is normally captured implicitly through the threat likelihood. The approach is exemplified on two specific threats independently of a specific brand.

It is worth mentioning here that the Forbes magazine [11] recently published an additional argument for investments in cybersecurity risk assessment. More or less at the same time, Wang et al. [12] advanced an abstract framework for automotive cybersecurity risk assessment. Notably, the claimed advantages of the approach include applicability during the vehicle lifecycle as well as support for quantitative risk metrics. However, the manuscript lacks a convincing running application to demonstrate the benefits and overall strengths of the framework. Applicability to privacy is mentioned but scantly accounted for.

While all these works were inspirational for ours, none of them explicitly target privacy or treat it extensively. By contrast, this work distilled out both assets and threats that are relevant to privacy in the automotive domain using a novel, double approach, which is then demonstrated in practice by offering ways to compare the top car brands. Such a treatment at the specific level of car brand also seems a distinctive feature with respect to the existing literature.

### 1.2 Contributions

This article contributes a novel framework for a double assessment of privacy risks affecting car brands. The framework adopts both the ISO 27005 and the STRIDE

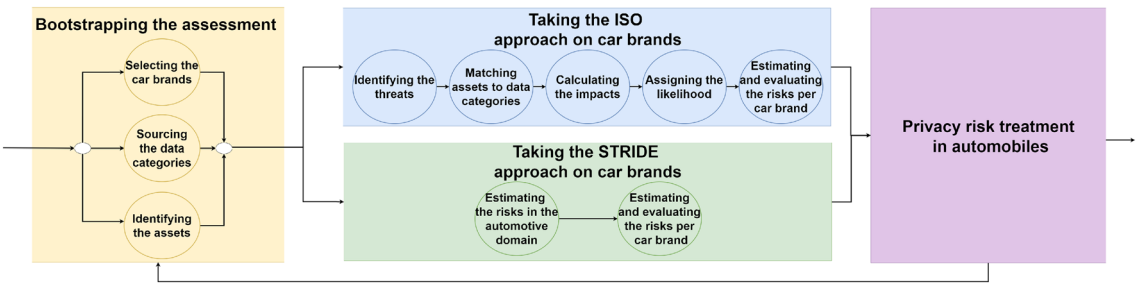



**Fig. 1** Flowchart of the framework for the double assessment of privacy risks aboard top-selling cars

approaches and applies them in synergy. It is summarised through the flowchart in Fig. 1, which is described in the sequel of this article. The underlying approach is general, hence the double assessment can be tailored to virtually any application scenarios beyond the automotive domain.

The framework is demonstrated on the car brands that are most common upon the basis of sales data. Such a practical application highlights the main advantages of the proposed framework because it finds the brands whose assets are most at risk by the ISO approach and, at the same time, also the brands suffering highest threats by the STRIDE approach. The asset-oriented findings are that the top data breach risks affect Tesla, Volkswagen and Audi, while the threat-oriented outcomes highlight that the top risks affect Mercedes on 4 threat categories and Ford, Tesla and Toyota on 2 threat categories. These findings confirm that, by looking at risk from different angles, the two approaches enrich the insights with a complementarity that was not available before.

This is the first large-scale privacy risk assessment exercise concerning specific representatives of the automotive domain, culminating with a discussion on possible additional measures to mitigate the estimated risks. It must be recalled that risk assessment is inherently subjective and affected by the assessor's bias, limitations that are typically thwarted by focus groups and by relying on existing evidence in support of the assessment, as shall be seen below. This in turn calls for a need of relevant information, which may be problematic in general. This article sources the relevant information from the web by means of structured queries. Should other sources of information become available, the assessment could be easily reviewed, while our framework would not change.

### 1.3 Article Structure

Section 2 recalls the basics of risk assessment, and Sect. 3 sets the essentials for a privacy risk assessment in the automotive domain. Then, Sects. 4 and 5 demonstrate, respectively, the asset-oriented and the threat-oriented findings. Section 6 introduces possible risk treatment measures. Finally, Sect. 7 concludes, and Appendix A complements the presentation with the details of the domain-level STRIDE findings in support of Sect. 5.

## 2 A Primer on Risk Assessment

Risk assessment is a process to describe risks and enable organisations to prioritise risks according to their established criteria. The core sub-processes of risk assessment are risk estimation and risk evaluation. Risk assessment determines the relevant assets, identifies the threats and vulnerabilities that exist or could exist, determines the potential impacts, prioritises the derived risks and ranks them against the risk criteria set in a preliminary context establishment. The overall process is often conducted over several iterations. An overall assessment may be carried out over the risks that generally affect the application domain. Then, using the output of the previous analysis, a further vertical assessment may be carried out over the specific representatives of the domain. This article concentrates on the second level of assessment, hence it derives general privacy risk assessment findings about the automotive domain and tailors them to specific car brands.

### 2.1 Asset Identification

One of the essential tasks through risk assessment is to create a comprehensive list of assets. An asset is anything that has value to the organisation and therefore requires protection. The definition of assets is not limited to hardware or software. The set of assets includes services, communications, data and infrastructure. The level of detail used through asset identification can be refined in further iterations of the risk assessment. Although each asset needs to be protected, some assets are more critical than others, that is, damage to these assets causes greater damage to the organisation. Each asset is then subject to a valuation process, that is, it is assigned a value determined by the replacement value of the asset and the business consequences of loss or compromise of the asset. These include legal consequences from the disclosure, modification, non-availability and destruction of information. Intuitively, the higher the value, the more important is the asset.

### 2.2 Threat Identification

The organisation should identify the general sources of risk, areas of impacts, relevant events and their possible consequences. The aim of this step is to determine what could happen to cause a potential loss and to gain insights into how, where and why the loss might happen. Relevant and up-to-date information is important in identifying risk sources. This is a critical step because a source that is not identified here will not be processed along the subsequent steps. Sources should be considered whether or not they lie under the control of the organisation.

Risk sources help identify threats. While a source of risk is where a risk originates and where it comes from, a threat is any event that may potentially occur from the risk source and would harm assets hence organisations. Threats include both accidental and voluntary events, which may arise from within or from outside the organisation. Some threats may affect more than one asset.

## 2.3 Risk Estimation

Risk estimation involves developing an understanding of the risk. It makes it possible to assess the danger of an undesirable event, that is, a threat, in order to define the priority and the urgency of the measures necessary to control the odds that the event occurs.

Risk estimation is commonly qualitative and involves an assignment, typically on a small interval of numbers such as 1 through to 4, on the likelihood that a threat materialises. It also involves an understanding of the impacts that would derive, also in this case to be expressed within some interval of numbers. Impacts normally depend on asset values, as we shall see in the following. When the estimation is quantitative, the interval numbers are replaced with actual quantities, for example of money or time.

The assessment of threat likelihood is notoriously affected by the human assessor's bias. While some level of subjectivity is unavoidable, bias is routinely thwarted by considering previous pertaining events, such as how often a threat occurred in the past — assuming that the future will not deviate significantly from the past. The likelihood assignment process also depends on how easily a threat can be exploited by skilled and motivated attackers.

A third factor influencing the likelihood assignment comes from the existing controls, precisely from whether they work well against the threats. This is why the existing controls should be identified and their functioning checked. An incorrectly implemented or malfunctioning control could itself be a vulnerability and represent a threat.

Typical likelihood values can be interpreted as follows:

- 1, or *rare:* there are valid countermeasures or, alternatively, the motivation for an attacker is very low;
- 2, or *unlikely:* a possible attacker needs to address strong technical difficulties to pose the threat or, alternatively, the efforts are not worth the impacts;
- 3, or *possible:* the technical requirements necessary to pose this threat are not high and could be solved without significant effort, furthermore there is a reasonable motivation for an attacker to perform the threat;
- 4, or *likely:* there are no sufficient mechanisms installed to counteract this threat and the motivation for an attacker is quite high.

Risk estimation may take an *asset-oriented* approach or *threat-oriented* approach or both. Asset-oriented estimation revolves around asset values and aims to describe the impacts and their likelihood to produce a risk level. Threat-oriented estimation is somewhat complementary to the previous approach and develops in the opposite direction, being pivoted on threats. Impact and likelihood values may be combined differently, according to various categories of threats as well as to scope and objectives of the overall management process. Taking both approaches in parallel may offer deeper insights, as this article demonstrates below.

Independently of the approach taken, the outcome of the assessment is a description of the estimated risks in the form of prose, numbers, colours, or a combination of these. However, these may not be meaningful for the organisation until they undergo evaluation, which is the next step.

### 2.3.1 The ISO Approach

The best-known asset-oriented risk estimation process comes from the ISO 27005, a de-facto standard framework for risk assessment.

The evaluation of impact is based on the typical parameters that characterise the overall objective of the risk assessment process. For example, a privacy objective implies that impact refers to type and volume of personal data as well as to the level of identifiability of data subjects. For example, because (PII) has a high value, any threats to it get a correspondingly high impact.

If the impact values are given on the same interval as that for the likelihood values, than a popular approach to estimate the risk level is through a *risk matrix*. Each cell of a risk matrix expresses a specific pair of likelihood and impact values. It must be remarked that ISO 27005 [4] does not prescribe a standard risk matrix, hence organisations may create their own, depending on the specific features of their activities and business sector.

If likelihood or impact values are decimal numbers, they could still be mapped through a risk matrix, but we find a purely numerical treatment to be more effective in this case. In consequence, risk can be estimated by a standard formula:

$$\text{Risk}(\mathit{threat}, \mathit{asset}) = \text{Likelihood}(\mathit{threat}, \mathit{asset}) \times \text{Impact}(\mathit{threat}, \mathit{asset}) \quad (1)$$

Lifting this formula at the level of the organisation to produce the organisation's privacy risk can be done in various ways, but could get complicated because of the necessary generalisation on both parameters. For example, fixing a threat, its likelihood for the organisation could be derived as the maximum or the average of the threat likelihood on all assets. Such outcomes for all threats could then be combined, by a similar function, as the overall privacy risk likelihood for the organisation. However, the lifting to brand level is simple in the sequel of this manuscript (Sect. 4.4) because of the underlying privacy objective: all threats reduce to the threat of personal data breach, and its likelihood is constant over the various assets because these ultimately are types of data.

A similar lifting process should occur for the impact. The overall privacy risk impact could be derived as a generalised sum of the impacts of all threats on all assets. This gets both

simpler and more complicated in our specific application to car brands (Sect. 4.3). If, on one hand, only personal data breach applies, on the other hand, the impact on each asset shall be a weighted version of the asset value.

#### 2.3.2 The STRIDE Approach

The best-known threat-oriented risk estimation process is STRIDE [5], developed by Microsoft and relying on 6 categories of threats: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege. The name is the simple acronym of the category names.

The focus on threats implies that threat identification may have to be reiterated to recognise all possible threats per category. It is also convenient to highlight which assets would be affected (by non-negligible impact). The general considerations about subjectivity through likelihood assignment, and about impact of a threat on an asset as bound to the asset value, continue to apply here. However, the risk level is assessed for the given threat in the domain, independently from a specific asset because the threat impact is considered holistically on all assets, as the formula shows:

$$\text{Risk}(\textit{threat}) = \text{Likelihood}(\textit{threat}) \times \sum_{\textit{asset}} \text{Impact}(\textit{threat}, \textit{asset}) \tag{2}$$

Therefore, such threats refer to the application domain in general. Lifting this formula at the level of the organisation may only require a verification of which risks specifically apply to the organisation and then add up their levels. However, this could be complicated by the number of threats, as shall be seen below (Sect. 5.2) over car brands.

### 2.4 Risk Evaluation

Risk estimation provides the necessary input to the risk evaluation process. The purpose of risk evaluation is to assist in making decisions about which risks need treatment and their implementation priority.

To evaluate risks, the organisation compares the risk levels with a set of criteria defined during the initial context establishment and possibly reviewed through the various steps of the assessment. The aim of the evaluation is to match the risk levels to the criteria to decide whether the levels meet the criteria. For example, a risk level of 50 meets criteria stating a minimum level of 40. In turn, criteria, which should also comply with legal and regulatory requirements, could derive from an *absolute* or a *relative* approach. An absolute approach yields firm criteria such as "the minimum level is 40". Alternatively, a relative approach sees a prioritisation of the risks by ordering the risk levels, grouping them coherently and assigning them some urgency for some treatment. Relative evaluation approaches shall be applied below.

For example, a relative approach relying on a chromatic scale red-orange-yellow-green may group the risk levels into a colour depending on how many non-zero risk levels are available, as represented in Table 1. Clearly, at least 4 risk levels are needed for the 4 groups to become meaningful.

Then, either approach may assign an urgency for a treatment to the various groups of risk levels by leveraging the chromatic scale as follows:

- *Green* or *low risks*: risk may be treated by acceptance;
- *Yellow* or *modest risks*: risk must be treated only if additional cost-benefit analysis is carried out; treatment by acceptance is possible;
- *Orange* or *tangible risks*: risk must be treated soon; treatment by acceptance is prohibited;
- *Red* or *high risks*: risk must be treated as a matter of urgency; treatment by acceptance is prohibited.

### 2.5 Risk Treatment

Risk evaluation inspires risk treatment, more precisely, the applicable decisions on the risk treatment strategies and methods to take.

The treatment involves selecting one or more options to face the evaluated risk levels. Typical options are the application of new controls that reduce the likelihood or the impacts, the transfer of risks to other parties or the acceptance of risks.

Options should be selected considering not only the outcomes of the estimation phase but, if possible, also the expected cost to implement those options and the expected benefits stemming from those options. Risk treatment

**Table 1** Example application of relative criteria to group risk levels for risk evaluation

| Risk levels | Green values | Yellow values | Orange values | Red values |
|---|---|---|---|---|
| 1 | | | | 1 |
| 2 | | | 1 | 1 |
| 3 | | 1 | 1 | 1 |
| 4 | 1 | 1 | 1 | 1 |
| 5 | 1 | 1 | 1 | 2 |
| 6 | 1 | 1 | 2 | 2 |
| 7 | 1 | 2 | 2 | 2 |
| 8 | 2 | 2 | 2 | 2 |
| 9 | 2 | 2 | 2 | 3 |
| 10 | 2 | 2 | 3 | 3 |
| . | | | | |

options are not necessarily mutually exclusive or appropriate in all circumstances. Organisations can benefit from a combination of options, also taking into due account the applicable legal and regulatory requirements.

## 3 Bootstrapping the Privacy Risk Assessment

This Section instantiates the risk assessment over 11 real-world car brands, thus taking both approaches discussed above. Precisely, it refers to the yellow, leftmost box of the framework flowchart as represented in Fig. 1.

### 3.1 Selecting the Car Brands

The target car brands are chosen in terms of market shares. The top ten best-selling car manufacturers during the first quarter of 2019, according to "Car Sales Statistics" [13] are: Volkswagen, Renault, Peugeot, Ford, Opel, Mercedes, BMW, Audi, Skoda, Toyota. Somewhat arbitrarily, this article adds a specific brand that is widely acknowledged as a pioneer of electrification, Tesla.

### 3.2 Sourcing the Data Categories

Costantino, De Vincenzi and Matteucci studied the policies of the to car brands and pinpointed the data categories that each brand declares to collect [14]. Table 2 summarises them. This information is very relevant to bootstrap both flavours of our risk assessment process, as shall be seen below.

### 3.3 Identifying the Assets

The various types of data treated by modern cars are the privacy-relevant assets. We independently analyse the current technological landscape in the automotive domain by scrutinising the relevant state of the art and identified the following assets:

- **Personally Identifiable Information** any data that could potentially be used to identify a particular individual (such as full name, date and place of birth, driver's license number, phone number, mailing and email address).
- **Special categories of personal data** about the driver, e.g. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning sex life or sexual orientation (GDPR art. 9).
- **Driver's behaviour** driver's driving style, e.g. the way the driver accelerates, speeds up, turns, brakes.

**Table 2** Data categories that each car brand declares to collect [14]

| Manufacturer | DC1 Personal | DC2 Geolocation | DC3 Driver's phone | DC4 Purchase | DC5 Offences and violations | DC6 Driver's behaviour | DC7 Vehicle status | DC8 Surrounding vehicle environment | DC9 Voice and messages | DC10 App usage |
|---|---|---|---|---|---|---|---|---|---|---|
| Volkswagen | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| Renault | ✓ | ✓ | | ✓ | | | ✓ | | ✓ | |
| Peugeot | ✓ | ✓ | ✓ | ✓ | | | ✓ | | ✓ | |
| Ford | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| Opel | ✓ | ✓ | ✓ | ✓ | | | ✓ | | | ✓ |
| Mercedes | ✓ | ✓ | ✓ | | | | ✓ | | ✓ | ✓ |
| BMW | ✓ | ✓ | | | | | ✓ | ✓ | | ✓ |
| Audi | ✓ | ✓ | ✓ | ✓ | | | ✓ | | ✓ | ✓ |
| Skoda | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Toyota | ✓ | ✓ | ✓ | ✓ | | | | | ✓ | |
| Tesla | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |

- **User preferences** data regarding cabin preferences, e.g. seating, music, windows, heating, ventilation and air conditioning (HVAC).
- **Purchase information** financial information of the users such as credit card numbers and bank accounts.
- **Smartphone data** data that the vehicle and user's smartphone exchange with each other via the mobile application and short-range wireless connections such as WiFi and Bluetooth (contact book, phone calls, text messages).
- **GPS data** vehicle geo-location history and route tracking.
- **Vehicle information** vehicle information such as car maker, model, vehicle identification number (VIN), license plate and registration.
- **Vehicle maintenance data** data on the maintenance and status of vehicle components such as kilometres travelled, tyre pressure, oil life, brake, suspension and engine status.
- **Vehicle sensor data** data analysed and calculated by car sensors such as distance sensors, crash sensors, biometric sensors, temperature sensors and internal and external cameras.

To reduce bias, we completed the asset identification job prior to learning the categories identified by our colleagues [14]. We then continued by valuating the assets on a scale from 1 to 5 upon the basis of the sensitiveness of data—the top value in fact was only assigned to the special categories of personal data. The outcome is in Table 3.

## 4 Taking the ISO Approach On Car Brands

This Section discusses the blue, top-central box of the framework flowchart as represented in Fig. 1. The goal of the present exercise is to compare the various car brands with each other in terms of the overall privacy risk affecting a brand. It could be seen above that the ISO approach is based on assets, therefore this effort rests on the relevant assets and their values to calculate impact and likelihood that threats materialise.

**Table 3** List of privacy-related assets and their valuation

| ID | Name | Value |
|---|---|---|
| A1 | Personally Identifiable Information | 4 |
| A2 | Special categories of personal data | 5 |
| A3 | Driver's behaviour | 2 |
| A4 | User preferences | 2 |
| A5 | Purchase information | 3 |
| A6 | Smartphone data | 4 |
| A7 | GPS data | 3 |
| A8 | Vehicle information | 2 |
| A9 | Vehicle maintenance data | 3 |
| A10 | Vehicle sensor data | 4 |

### 4.1 Identifying the Threats

A number of threats exist for the privacy of (the data of) people. For example, personal data could be illicitly disclosed to anyone that the data owner did not intend as a recipient of the data; similarly, data could be altered or destroyed. Similar scenarios are instances of the overarching applicable threat: a *personal data breach*. This is precisely defined by GDPR art. 4.12 as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Therefore, also in the interest of brevity, the sequel of this section refers to a data breach as the only outstanding threat.

### 4.2 Matching Assets To Data Categories

Prior to calculating the impacts of a data breach in the various cases, the identified assets need to be matched with the data categories recalled above. Three matches are obvious, quite a few need some grouping before a matching can be drawn, and no matching is possible in one case.

- Obvious matches. PII, Purchase information and GPS data have an obvious one-to-one correspondence with the data categories as follows:
  - A1 to DC1
  - A5 to DC4
  - A7 to DC2
- Non-obvious matches. These do not have an obvious one-to-one correspondence, e.g. "Smartphone data" includes the categories of data relevant to the driver's smartphone, i.e. "Driver's phone", "App usage" and "Voice and messages". Another example is the declared data type "driver's behaviour", which is associated with the assets "Driver's behaviour & user preferences". The other matches are shown here:
  - A3 to DC6
  - A4 to DC6
  - A6 to DC3, DC9 and DC10
  - A8 to DC7
  - A9 to DC7
  - A10 to DC5 and DC8
- Impossible matches. It turns out that no car brand declares to collect special categories of personal data, hence the asset A2 cannot be matched to any data category.

### 4.3 Calculating The Impacts

The next step is to assign a weight to each asset depending on whether it appears in the policy of a car brand, represented as a data category. A weight allows us to scale down the value of an asset when that asset matches more than one data category among those mentioned in the policy. Therefore, the associations between assets and data categories discussed above play a crucial role here. For example, asset A6, smartphone data, relates to the three data categories DC3, DC9 and DC10 (that is, driver's phone, voice and messages and, finally, app usage). Therefore, if a given policy only treats one of those three data categories, then the asset value would be scaled down to a third. The precise assignments of weights are shown in Table 4.

For each car brand, upon the basis of the data categories it claims to collect, we calculate a numerical value representing the impact that a data breach would have on each asset by weighting its value as explained above:

$$\text{Impact}(asset) = \text{Value}(asset) \times \text{Weight}(asset) \tag{3}$$

Clearly, applying this formula to all assets of all brands required deriving the right weights, hence tight consideration of all information given in the tables above, particularly in Table 2. Impact at asset level could then be lifted at brand level by adding it up over all assets:

$$\text{Impact}(brand) = \sum_{asset} \text{Impact}(asset) \tag{4}$$

We obtain values that fall within a range from 11.3 to 21.6, meaning that the higher the value, the higher the impact that a data breach would have on the car brand. Notably, the top impact of 21.6 concerns Tesla, which collects all data categories discussed above with the only exception of "Voice and message". The impact on Tesla, represents well the large amount of data about both the vehicle and its driver their cars collect.

**Table 4** Assigning weights to data categories

| Asset ID | Matching data category | Asset value | Asset weight if data c. is declared | Asset weight if data c. is undeclared |
|---|---|---|---|---|
| A1 | DC1 | 4 | 1 | 0 |
| A2 | - | 5 | - | 0 |
| A3 | DC6 | 2 | 1 | 0 |
| A4 | DC6 | 2 | 1 | 0 |
| A5 | DC4 | 3 | 1 | 0 |
| A6 | DC3 | 4 | 0.33 | 0 |
| A6 | DC9 | 4 | 0.33 | 0 |
| A6 | DC10 | 4 | 0.33 | 0 |
| A7 | DC2 | 3 | 1 | 0 |
| A8 | DC7 | 2 | 1 | 0 |
| A9 | DC7 | 3 | 1 | 0 |
| A10 | DC5 | 4 | 0.5 | 0 |
| A10 | DC8 | 4 | 0.5 | 0 |

### 4.4 Assigning the Likelihood

As already noted, establishing the likelihood of the manifestation of a threat generally is a subjective process. Bias is normally reduced by focus groups and, most importantly, by bringing existing evidence of prior manifestations of the same threat. We employ classical web searches as a source of relevant information by building query pairs as "brand name, keyword", with "brand name" ranging over 11 car brands and "keyword" ranging over the set *breach*, *vulnerability*, *exploit* and *attack*. Therefore, we conduct a total of 44 web searches and studied the hits. Those that are deemed relevant are reported in Table 5.

Through the process of assigning likelihood values for a data breach on each asset, it became apparent that each asset gets the same value because all assets are data that the vehicle collects and treats. Therefore, the process produced one likelihood value per brand, precisely derived by counting the number of relevant hits for the brand and then augmenting it by one. In consequence, brands that produced no relevant hits get a unit likelihood, hence the impact gets preserved as is in the estimated risk level. The full list of likelihood values is given in Table 6.

### 4.5 Estimating and Evaluating the Risks Per Car Brand

Once the likelihood and the impact of a personal data breach are available for each brand, the risk that the breach materialises can be customarily estimated by multiplying likelihood and impact. Table 6 shows the complete findings for all car brands. The risk levels are calculated using Formula 1 from Sect. 2.3.1, and span over 10 non-zero values. By taking a

**Table 5** Relevant web search hits

| Brand | Relevant hits |
|---|---|
| Volkswagen | Breach [15], Vulnerability [16, 17] |
| Renault | Breach [18] |
| Peugeot | *none* |
| Ford | Breach [19], Vulnerability [16] |
| Opel | *none* |
| Mercedes | Breach [20], Vulnerability [21] |
| BMW | Breach [22, 23], Vulnerability [24], Exploit [25] |
| Audi | Breach [15], Vulnerability [17], Exploit [26] |
| Skoda | *none* |
| Toyota | Breach [27], Attack [28], Vulnerability [29] |
| Tesla | Breach [30, 31], Attack [32], Vulnerability [33] |

**Table 6** Privacy risk levels per car brand—ISO approach

| Manufacturer | Impact | Likelihood | Risk |
|---|---|---|---|
| Tesla | 21.6 | 5 | 108.0 |
| Volkswagen | 19.0 | 4 | 76.0 |
| Audi | 17.0 | 4 | 68.0 |
| BMW | 13.3 | 5 | 66.5 |
| Ford | 19.0 | 3 | 57.0 |
| Toyota | 12.6 | 4 | 50.4 |
| Mercedes | 14.0 | 3 | 42.0 |
| Renault | 11.3 | 2 | 22.6 |
| Skoda | 17.3 | 1 | 17.3 |
| Peugeot | 15.6 | 1 | 15.6 |
| Opel | 15.6 | 1 | 15.6 |

relative evaluation approach as discussed in Sect. 2.4, risk levels are evaluated through a chromatic scale of 3 red values, indicating a high risk, 3 orange values, meaning a tangible risk, 2 yellow values, signifying a modest risk, and 2 green values, for a low risk.

It is apparent that a high risk affects, in order, Tesla, Volkswagen and Audi; a tangible risk affects BMW, Ford and Toyota; a modest risk affects Mercedes, Renault and Skoda; finally, a low risk affects Peugeot and Opel.

## 5 Taking the STRIDE Approach on Car Brands

It could be seen above that the STRIDE approach is based on threats. This section takes that approach to assess the privacy risks of the 11 car brands. It describes the green, bottom-central box of the framework flowchart as represented in Fig. 1.

Section 2.3.2 outlines the approach, in particular promoting the 6 threat categories of Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege. The current technological landscape in the automotive domain does not raise significant repudiation threats, hence the sequel of this section only treats 5 threat categories.

### 5.1 Estimating the Risks in the Automotive Domain

Considering the state of the art in the automotive domain, we tailor STRIDE to identify the relevant threats in each category. This takes considerable effort, and a justification on each threat and its likelihood can be found in Appendix A. We then estimate the corresponding risks [34] by systematically applying Formula 2 given in Sect. 2.3.2. The findings are summarised in Table 7, where each threat in each category comes with the relevant likelihood, an indication of the assets (from Sect. 3.3) that are non-negligibly affected and, ultimately, the estimated risk level.

Table 7 confirms that the top spoofing risk derives from the companion mobile app and that the top tampering risk from infotainment malware. Both risks concern a rather high architectural level, thereby calling for attention at a software middleware level. The top disclosure risk is CAN eavesdropping and the top denial-of-service risk is CAN Bus flooding. Both concern a rather low architectural level, hence calling for additional scrutiny of bus security and internal network separation. The top escalation risk derives from insider threats, coherently with other application domains.

### 5.2 Estimating and Evaluating the Risks Per Car Brand

Once the privacy risk levels in the application domain are estimated, the next step is to specify such estimations over the individual representatives in the domain, which in this case are the car brands. Following the general approach explained above, we take that step by deciding which of the domain threats applies to which car brand. For example, we need to verify whether the smart key cloning threat applies to Peugeot, as well as all other possible pairs of threat and car brand. When a threat were found to apply to a car brand, we would then burden the car brand with the risk level for that threat.

To verify such matches, we leverage classical web searches as a source of relevant information, as done above, precisely by building query pairs as "brand name, keyword". While "brand name" continued to range over the 11 car brands, this time "keyword" ranged over the 5 threat categories. Therefore, we conduct a total of 55 web searches and study the hits, which only partially overlap with those found before through the ISO approach.

A number of hits are relevant, and we study them to decide what threats applied to what car brands. Opel is found to be vulnerable to attacks of smart key bruteforcing and cloning [35]. Other car manufacturers, including Audi, Skoda, Ford and Volkswagen, also suffer similar attacks [36].

Both Ford and Peugeot are affected by a data breach [37, 38]. In addition, Volkswagen has been hit by multiple types of attacks of smart key cloning, data breach and at infotainment level [39, 40]. Audi, BMW and Toyota brands share a similar fate, in fact they receive attacks of smart key cloning and data breach [22, 27, 41]. Renault appears to have received reverse engineering attacks and ransomware [18, 42].

Multiple attacks targeting Tesla vehicles have been documented in recent years [43–45]. Mercedes, which also turn

**Table 7** Application of STRIDE to automotive domain

| Threat | Likelihood | Assets affected | Risk level |
|---|---|---|---|
| **Spoofing** | | | |
| Mobile App | 3 | A1, A3, A4, A5, A6 | 45 |
| Smart key bruteforcing | 1 | A8, A10 | 6 |
| Smart key cloning | 2 | A8, A10 | 12 |
| GPS spoofing | 2 | A7, A10 | 14 |
| V2X Message replay | 1 | A8, A10 | 6 |
| **Tampering** | | | |
| Infotainment malware | 3 | A1, A3, A4, A5, A6, A7 | 54 |
| Mobile App malware | 3 | A1, A3, A4, A7, A8 | 39 |
| ECU reflash | 2 | A9, A10 | 14 |
| CAN frame injection | 3 | A9, A10 | 21 |
| CAN frame tampering | 1 | A9, A10 | 7 |
| V2X data tampering | 1 | A7, A8, A10 | 9 |
| **Information disclosure** | | | |
| CAN eavesdropping | 4 | A3, A4, A8, A9, A10 | 52 |
| Unauthorised diagnostic access | 4 | A3, A4, A8, A9, A10 | 52 |
| Infotainment reverse engineering | 2 | A1, A3, A4, A5, A7 | 28 |
| Insecure API endpoint | 2 | A1, A8, A9, A10 | 24 |
| ECU firmware dump | 1 | A8, A9, A10 | 9 |
| Server violation | 3 | A1, A3, A5, A8 | 33 |
| V2X eavesdropping | 3 | A1, A3, A10 | 30 |
| **Denial of service** | | | |
| CAN bus flooding | 4 | A9, A10 | 28 |
| Smart key jamming | 3 | A8, A10 | 18 |
| Data loss | 2 | A1, A5, A8 | 18 |
| V2X doS | 2 | A7, A10 | 14 |
| **Privilege escalation** | | | |
| Infotainment Alteration | 1 | A1, A3, A4, A5, A6, A7 | 18 |
| Rogue OBD-II Device | 3 | A9, A10 | 21 |
| Insider Threat | 3 | A1, A3, A5, A7, A8 | 42 |

out rather data hungry (Table 2), seems to have been struck by serious attacks — mobile app [46] and data breach [47].

The information outlined here is represented in detail through the ticks in Table 8, where all threat (categories) are scaled up to the car brands; the table features a sub-table per threat category. The impact that each threat causes is indicated in brackets. Each tick signifies a threat that is confirmed, through the web search hits, to concern a car brand. The rest of the table can be easily understood. The rightmost columns add up the risk levels per car brand; for example, because Volkswagen is only concerned by two spoofing threats, of risk level 6 and 12, respectively, the brand's total spoofing risk is 18. The bottom line of each sub-table adds up the number of occurrences of each threat; for example, smart key bruteforcing is a spoofing threat that affects 9 brands.

Each sub-table also evaluates the total risk levels in a relative way and represents them through a chromatic scale. However, the number of non-zero different values varies across the tables:

- 5 for the total spoofing risk levels;
- 6 for the total tampering risk levels;
- 4 for the total information disclosure risk levels;
- 2 for the total denial of service risk levels;
- 3 for the total privilege escalation risk levels.

Therefore, the number of values per colour must be reviewed as discussed in Sect. 2.4.

The findings can be interpreted in many ways. Intra-category considerations highlight the most common risks: smart key issues in spoofing, infotainment malware and CAN injection in tampering, CAN eavesdropping in information disclosure, CAN flooding in denial of service and, finally, rogue OBD-II devices in privilege escalation. Also,

**Table 8** Privacy risk levels per car brand—STRIDE approach

| **SPOOFING** | Mobile App (45) | Smart Key Bruteforcing (6) | Smart Key Cloning (12) | GPS Spoofing (14) | V2X Message Replay (14) | **TOTAL RISK** |
|---|---|---|---|---|---|---|
| MERCEDES | ✓ | ✓ | ✓ | | | 63 |
| FORD | ✓ | | | ✓ | | 59 |
| PEUGEOT | ✓ | | | | | 45 |
| SKODA | | ✓ | ✓ | ✓ | | 32 |
| OPEL | | ✓ | ✓ | ✓ | | 32 |
| AUDI | | ✓ | ✓ | ✓ | | 32 |
| BMW | | ✓ | ✓ | ✓ | | 32 |
| TESLA | | ✓ | ✓ | ✓ | | 32 |
| TOYOTA | | ✓ | ✓ | ✓ | | 32 |
| RENAULT | | ✓ | ✓ | ✓ | | 32 |
| VOLKSWAGEN | | ✓ | ✓ | | | 18 |
| Number of affected brands | 3 | 9 | 9 | 8 | 0 | 29 |

| **TAMPERING** | Infotainment Malware (54) | Mobile App Malware (39) | ECU Reflash (14) | CAN Frame Injection (21) | CAN Frame Tampering (7) | V2X Data Tampering (9) | **TOTAL RISK** |
|---|---|---|---|---|---|---|---|
| MERCEDES | ✓ | ✓ | | | | | 93 |
| AUDI | ✓ | | | ✓ | | | 75 |
| BMW | ✓ | | | ✓ | | | 75 |
| TESLA | ✓ | | | ✓ | | | 75 |
| VOLKSWAGEN | ✓ | | | ✓ | | | 75 |
| TOYOTA | ✓ | | | ✓ | | | 75 |
| SKODA | | ✓ | | ✓ | ✓ | | 67 |
| RENAULT | ✓ | | | | | | 54 |
| FORD | | ✓ | | | | | 39 |
| PEUGEOT | | | | ✓ | ✓ | | 28 |
| OPEL | | | | | | | 0 |
| Number of affected brands | 7 | 3 | 0 | 7 | 2 | 0 | 19 |

| **INFORMATION DISCLOSURE** | CAN Eavesdropping (52) | Unautho-rised Diagnostic Access (52) | Infotainment Reverse Engineering (28) | Insecure API Endpoint (24) | ECU Firmware Dump (9) | Server Violation (33) | V2X Eavesdropping (30) | **TOTAL RISK** |
|---|---|---|---|---|---|---|---|---|
| MERCEDES | ✓ | | | ✓ | ✓ | ✓ | | 118 |
| FORD | ✓ | | ✓ | | | ✓ | | 113 |
| TESLA | ✓ | | ✓ | | | ✓ | | 113 |
| AUDI | ✓ | | ✓ | | | ✓ | | 113 |
| VOLKSWAGEN | ✓ | | ✓ | | | ✓ | | 113 |
| TOYOTA | ✓ | | ✓ | | | ✓ | | 113 |
| BMW | ✓ | | ✓ | | | ✓ | | 113 |
| PEUGEOT | ✓ | | | | | ✓ | | 85 |
| SKODA | ✓ | | | ✓ | | | | 76 |
| OPEL | | | | | | | | 0 |
| RENAULT | | | | | | | | 0 |
| Number of affected brands | 9 | 0 | 6 | 2 | 1 | 8 | 0 | 26 |

| **DENIAL OF SERVICE** | CAN Bus Flooding (28) | Smart Key Jamming (18) | Data Loss (18) | V2X DoS (14) | **TOTAL RISK** |
|---|---|---|---|---|---|
| FORD | ✓ | | ✓ | | 46 |
| RENAULT | ✓ | | ✓ | | 46 |
| TOYOTA | ✓ | | ✓ | | 46 |
| MERCEDES | ✓ | | ✓ | | 46 |
| PEUGEOT | ✓ | | | | 28 |
| AUDI | ✓ | | | | 28 |
| BMW | ✓ | | | | 28 |
| TESLA | ✓ | | | | 28 |
| VOLKSWAGEN | ✓ | | | | 28 |
| SKODA | | | | | 0 |
| OPEL | | | | | 0 |
| Number of affected brands | 9 | 0 | 4 | 0 | 13 |

| **PRIVILEGE ESCALATION** | Infotainment Alteration (18) | Rogue OBD-II Device (21) | Insider Threat (42) | **TOTAL RISK** |
|---|---|---|---|---|
| MERCEDES | | | ✓ | 42 |
| TESLA | | | ✓ | 42 |
| RENAULT | ✓ | ✓ | | 39 |
| FORD | | ✓ | | 21 |
| PEUGEOT | | ✓ | | 21 |
| BMW | | ✓ | | 21 |
| SKODA | | | | 0 |
| OPEL | | | | 0 |
| AUDI | | | | 0 |
| VOLKSWAGEN | | | | 0 |
| TOYOTA | | | | 0 |
| Number of affected brands | 1 | 4 | 2 | 7 |

the brands that get the top risk levels per threat category are apparent.

Inter-category analyses report spoofing threats are most common, with 29 occurrences, followed by information disclosure ones, with 26 events. Out of 5 threat categories, Mercedes is the brand that gets top risk level most of the times, that is, 4, followed by Ford, Tesla and Toyota, with 2 top places each, and Audi, BMW, Peugeot, Renault and Volkswagen, with 1 red risk level.

Moreover, it can be seen that the most frequent threats that ever materialise, with 9 occurrences reported so far, have got to do with smart keys and the CAN Bus. By contrast, there are 7 threats that have never materialised through events, often involving V2X communications.

## 6 Privacy Risk Treatment In Automobiles

As explained above, a typical risk treatment option is to apply measures that limit risks by reducing impact or likelihood of threats. This section considers the most common threats per category, based upon Table 8, and selects the technical components that are found to be most at risk: smart keys, infotainment systems, CAN Bus and OBD-II. It then outlines technical measures that could be applied to reduce the associated risk levels stemming from either of the approaches taken above. This corresponds with the rightmost, purple box in the framework flowchart as represented in Fig. 1.

### 6.1 Smart Keys

Smart keys are convenient, allowing one to easily open their car and turn on the engine even from a distance. However, they may pose relevant threats. For example, if the range of action is too wide and the signal is not protected, it is possible to capture and replay the signal at a later time, allowing a thief to steal the vehicle effortlessly.

Signals could be encrypted by one-time passwords so as to thwart replay attacks. A trade-off with usability would be the use of multi-factor authentication, which could thwart scenarios of loss or theft of keys. Smart keys could be hardened by reducing the range of action to a few centimetres, so that a vehicle should not start when the key is not inside it. This could be combined with seat sensors for weight so as to prevent ignition when no driver is inside. The key could be equipped with motion sensors to shut it down after a long lapse of time.

### 6.2 Infotainment Systems

There are several countermeasures to reduce the likelihood of threats deriving from the infotainment. Over-the-air updates should be deployed as soon as possible to fix discovered vulnerabilities. In order to prevent malicious code execution from USB drives, the system must check the file system of USB devices and mount only supported file systems. Infotainment firmware should make sure that only necessary USB device classes are enabled, specifically with read-only and no-exec mount options.

Moving on to infotainment applications, the system should allow the installation of software only from official and specific sources. To prevent malware injection, it should deny the installation or the update of software downloaded from unofficial online stores or from users' devices. The system should be able to isolate high risk applications into containers or VMs because software isolation adds an additional security layer.

Update mechanisms should be used in order to deploy security updates and fix discovered vulnerabilities. If the infotainment system provides multi-user support, it should implement access control to separate privileges of different users and should require multi factor authentication at least for administrator login.

### 6.3 CAN Bus

The CAN Bus is one of the main targets during car hacking operations, likely due to its broadcast nature, fragility to Denial of Service attacks, lack of source fields and lack of authentication. Once access to the CAN Bus has been obtained, vehicle control is available as the various components communicate with each other using this communication channel. Most critical attacks concern the injection of artificial messages to trigger unwanted actions or the bus saturation with messages (fuzzing) aimed at predicting the behaviour of the ECUs. Any treatment measure that is conceived should also consider the limited resources that vehicles have with respect to computers, such as low bandwidth, memory, computational power and time constraints, although we can expect that such limitations will fade away in the near future.

Eavesdropping can be prevented by encrypting messages before transmission over the bus, making it impossible for an attacker to understand the messages sent by the legitimate vehicle components. Intra-vehicular communication must be protected using both message encryption (for confidentiality) and cryptographic hashing (for authentication and integrity). The CIA triad might be achieved by a single software module [48, 49]. Unfortunately, cryptographic key management is not easily applicable on a large scale in the automotive field. Also, considering the lifetime of an average vehicle, any cryptographic key should be strong enough against brute force attacks. Frames that are not authenticated or come from an undefined source should be dropped by the receiver.

In addition, intrusion detection systems (IDS) and intrusion prevention systems (IPS) could help identify and prevent most of the known attacks. Anomalies such as bus load, messages with illegal ID, and high number of dropper frames may indicate a potential attack in place. If any anomaly is detected, such systems should quickly warn the driver and the car maker. Another possible measure is network segregation, i.e. separate critical and non-safety-critical ECU connections and use gateways to communicate with each other. This measure, however, requires a modification of the network topology.

### 6.4 OBD-II

The OBD-II port is a powerful entry point to a car. Therefore, it should be secured in such a way that only authorised personnel such as car dealers and mechanics may use this port successfully. Therefore, connecting personnel should be authenticated. Also, diagnostic features should be limited as much as possible to a specific mode of vehicle operation.

Operations that are to be executed via OBD-II must be secure by default, namely they should provide the most secure configuration by default. Connecting devices should be simplified to only connect to a car and execute its diagnostic features. Another countermeasure is a firewall (usually referred to as "secure gateway" in this domain) on the OBD-II to prevent malicious command injection to the Bus.

Aftermarket components change the security boundary of the vehicle. Segmentation and isolation from the other components should limit the damage a potential attacker can cause, for example separate CAN communications from the network stack and allow applications to send a request only from a list of pre-defined chosen OBD-II commands.

## 7 Conclusions

Modern cars expose a variety of digital services and process a variety of personal data, at least of the driver's, hence the motivation for the privacy risk assessment framework is discussed and demonstrated in this article. By taking both the asset-oriented ISO approach and the threat-oriented STRIDE approach in parallel, and by specifying the details to instantiate them to the automotive domain first and to specific car brands later, we built a privacy risk assessment framework that can be easily applied by anyone to any automotive-based scope.

Executing the framework by sourcing the relevant information through structured web searches produces the following findings. The asset-oriented outcomes call for attention on Tesla, Volkswagen and Audi for the risk of a data breach, while the threat-oriented outcomes are that the top risks affect Mercedes on 4 threat categories and Ford, Tesla and Toyota on 2 threat categories. Additionally, the most common threat per category becomes apparent. It can be appreciated that the parallel approach offers different, complementary standpoints to the assessment, hence augments the understanding of the privacy risk.

While the framework for the double assessment of privacy risks is general, a limitation of the findings derives from the quality of the information that is leveraged. In particular, web searches are employed here as a (public) source of relevant information, but it is impossible to fully verify the reliability of the returned entries.

In the future, other sources of information may become available, for example of classified type, and may be leveraged to review the assigned values and the corresponding findings described in the present article — yet without a need to change the general framework. Additional future work may tailor techniques of natural language processing and data mining to automate the extraction of relevant information from a large body. Also, the possible inter-relations between drivers' privacy and safety are worth of further investigation both at the technical level and at the broader, socio-technical level.

While technology in general is notoriously data-driven today, so is the specific technology that modern cars progressively embody. This study laid the foundations to risk-assess the privacy objective of such common yet complex cyber-physical systems as the latest cars are, ultimately extending, to recall the GDPR, the "protection of natural persons" to those who drive them.

## Appendix A Tailoring STRIDE to the Automotive Domain

This section summarises the findings of a privacy risk assessment exercise conducted over the automotive domain by taking the STRIDE approach [34].

### A.1 Spoofing

An example of identity spoofing is to illegally access and then use another user's authentication information, such as username and password.

Similarly to traditional websites, mobile apps can also be targets for spoofing attacks [50]. The likelihood of this threat is possible.

As for smart keys, a possible spoofing attack is related to brute forcing techniques, that is, to try every possible signal combination to unlock the victim's vehicle. The likelihood of success of the attack is rare. Smart keys are also subject to cloning attacks. The signal may be amplified and intercepted for later use [51, 52]. The likelihood of attack is unlikely

because the attacker needs to be nearby the victim's key fob to clone the signal.

Modern infotainment systems have a built-in navigation system that can be the target for GPS spoofing attacks [53]. The likelihood of this threat is unlikely because a potential attacker needs to be near the victim's car to perform the attack.

V2X communications are based on wireless connections. VANET (Vehicle Ad-hoc Network) connections use both long-range (3 G, LTE) and short-range (Bluetooth and WiFi) connections. Since they are wireless communications, everyone can receive the signals and messages that are sent by the vehicles. The likelihood of this threat is rare.

### A.2 Data Tampering

Data tampering involves the malicious modification of data. Examples include unauthorised changes made to persistent data, such as that held in a database, and the alteration of data as it flows over a network.

The infotainment systems may be subject to malware designed to damage the system by compromising the data it contains. Both input peripherals and applications provide a possible attack surface for injecting malware into the software system. Automatic execution of scripts on USB devices [54], malware hidden inside audio tracks on CDs [55] and even integrated browser navigation [44, 45, 56, 57] can be exploited as transmission media for malicious software. Considering the numerous access points available for spreading malware and the experience of successful exploits, the likelihood of this threat is possible.

Malware can also affect mobile applications that are vulnerable to code injection. In fact, mobile applications that are not obfuscated, in particular Android applications, can be decompiled and recompiled. Once the application is decompiled, it may be possible to edit and add arbitrary code to the source before recompiling everything into a new APK file. The likelihood of this attack is possible, considering that many official applications do not implement security measures [58, 59].

The OBD-II standard specifies the possibility to reprogram ECUs through the connector. The firmware image can then be retrieved through the update channels, which are mainly two: Over the Air update and offline update through OBD-II port. These images can be analysed to find possible vulnerabilities or change the behaviour of the ECU in certain situations. A malicious reflash of ECU firmware can compromise the integrity of vehicle data (maintenance and sensors). The likelihood of attack of this threat is unlikely because the upgrade packages are likely to be encrypted, and the ECU performs an integrity check before proceeding with the upgrade.

The CAN bus is very vulnerable to data tampering. Considering the broadcast nature of communications and the lack of integrity checks, it is possible that a malicious node may modify the content in transit in the communication channel by altering the frame bits. Considering the broadcast nature of communications and the lack of integrity checks, it is possible that a malicious node disrupts or causes interference that would prevent a specific message from being received correctly. The likelihood of this threat is rare as it is not easy to alter a data frame without anyone noticing.

Another problem for the CAN Bus is frame injection. Considering the absence of the authentication field, a malicious node could forge and send frames to trigger actions by other ECUs. Compared to other CAN related attacks, for this type of threat an attacker needs some more knowledge about the frames that the target vehicle uses. The likelihood of this threat is possible.

V2X communications have threats related to data tampering. In vehicle-to-vehicle messages, a malicious intermediate node might modify the message, thus vehicles may receive forged information. But, as mentioned above, there are security measures applied by the transmission protocols that make the threat difficult to occur. Therefore, the likelihood is rare.

### A.3 Information Conflict of interest

Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it, for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

The CAN Bus can be a target for this kind of threats because the frames travel in the clear. This means that any message sent by an ECU is readable from any other node connected to the CAN Bus [60]. This threat is likely once the attacker gets access to the CAN Bus, also considering that all vehicle information (including maintenance and sensor data) travels on the CAN Bus without any security measures.

Vehicle's data can also be obtained from the on-board diagnostic (OBD) component. Through the OBD protocol, it is possible to obtain the diagnostic information of the vehicle and the status of its components such as tyre pressure, brake status, suspension status, oil life, etc. Computers can also be connected to a vehicle's OBD-II port using USB-to-OBD adapters. The ease of obtaining this information increases the likelihood that is likely.

A possible source of risk associated with the infotainment system is the installed firmware. There are several methods to retrieve the firmware image of the infotainment system: debug interfaces, memory dump or download from official websites and specialised forums on the Internet [61–63]. Compared to malware injection, reverse engineering requires

higher and more targeted skills, so the likelihood of success of such an attack is lower, thus the likelihood of this threat is unlikely.

Mobile applications interface with the vehicle via exposed API endpoints. These APIs allow one to receive information such as tyre pressure status and vehicle status, but also to locate the vehicle in real time [64, 65]. The likelihood of success of this attack is unlikely, the automatic controls of online stores (Google Play, Apple Store) are able to detect unsafe connections and refuse to load the application on the store [66].

Unlike the infotainment system, dumping the firmware from an ECU is more difficult since the attacker does not have direct read access to the ECUs. ECUs can implement flash read commands from the CAN Bus, therefore, the attacker would need to know the CAN frame to perform this operation. The only way to find out these commands is by analysing the firmware, thus going back to the starting point, so the likelihood is rare.

The security of the manufacturer's server is also very important. The organisation may expose poorly protected databases due to incorrectly configured Intranet settings and lack of reliable authorisation methods. An attacker may obtain the database endpoint through traffic analysis [23, 27, 67]. Therefore, the likelihood of this threat is possible.

### A.4 Denial of Service

Denial of service (DoS) attacks deny service to valid users, for example by making a web server temporarily unavailable or unusable.

It is easy to cause a denial of service on the CAN Bus thanks to the frame priority given by its identifier. In fact, flooding the communication channel with high priority frames, possibly with an ID as low as possible, prevents access and sending by the other nodes, causing a denial of service. This threat also has a possible likelihood of happening once a potential attacker gains access to the CAN Bus.

A potential attacker might also aim to block the owner's smart key signal by preventing the expected operation. There are many devices, even low cost ones, that act on a wide range of frequencies in order to increase the likelihood of successful attack. The likelihood of attack is possible, especially when a careless driver does not verify the actual locking of the doors.

A data loss on automaker's cloud servers could also cause a denial of service. When there are no data backup mechanisms, it is possible for an organisation to experience loss of information when their data is object of targeted attacks. The likelihood of attack is unlikely.

V2X communications can also be subject to jamming attacks and denial of service. The DoS attacks comprise a group of attacks that target the network service availability. In a possible scenario, an attacker with physical access to the vehicle could install a device connected to the OBD or USB connector that, once powered, disturbs all wireless signals and interrupts all non-wired vehicle communications. The likelihood of this threat is unlikely as the attacker needs to be near the targets to cause damage.

### A.5 Privilege Escalation

In this type of threat, an unprivileged user gains privileged access and thus has sufficient access to compromise or destroy the entire system. Privilege elevation threats include those situations in which an attacker has effectively penetrated all system defences and becomes part of the system itself. However, the likelihood of success is rare [68], requiring successful reverse engineering, advanced knowledge of low-level languages such as assembly language, and finally a way to redistribute and install the modified firmware without arousing suspicion. For these reasons, the likelihood of success of this threat is rare.

Another possible attack of privilege escalation concerns rogue devices connected to the OBD port. In fact, many external devices such as dashcams and anti-theft systems connect via OBD port to add functionalities that were not initially designed for the vehicle. However, such devices could potentially add and expose more vulnerabilities as they have access to the CAN Bus through the OBD-II port. The likelihood of this threat is possible due to the ease of access to the vehicle's network and trusting drivers.

The risk of insider threat should not be underestimated. An insider threat is a malicious activity against an organisation that comes from users with legitimate access to an organisation's network, applications or databases. The likelihood of this threat is possible.

**Funding** Open access funding provided by Università degli Studi di Catania within the CRUI-CARE Agreement.

## Declarations

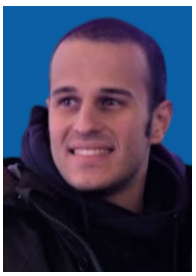
**Conflict of interest** On behalf of all authors, the corresponding author states that there is no conflict of interest. All authors contributed equally to the various steps underlying this work and to the writing of this manuscript. All authors read and approved the final manuscript.

## References

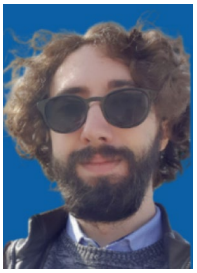

1. Bella, G., Biondi, P., Costantino, G., Matteucci, I., Marchetti, M.: Towards the COSCA framework for COnseptualing Secure CArs. In: Roßnagel, H., Schunck, C.H., Mödersheim, S. (eds.) Open Identity Summit 2021, pp. 37–46. Gesellschaft für Informatik e.V, Bonn (2021)
2. Bella, G., Biondi, P., Tudisco, G.: Car drivers' privacy concerns and trust perceptions. In: Fischer-Hübner, S., Lambrinoudakis, C., Kotsis, G., Tjoa, A.M., Khalil, I. (eds.) Trust, Privacy and Security in Digital Business, pp. 143–154. Springer, Cham (2021)
3. European Union: General Data Protection Regulation (EU Regulation 2016/679) (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL. Accessed 02 Nov 2022
4. International Organization for Standardization: ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management (2018). https://www.iso.org/standard/75281.html. Accessed 02 Nov 2022
5. Microsoft: The STRIDE Threat Model (2009). https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20). Accessed 02 Nov 2022
6. International Organization for Standardization: ISO 26262 - Road Vehicles - Functional Safety (2018). https://www.iso.org/standard/68383.html. Accessed 02 Nov 2022
7. Smishad, T.: Automotive Risk Assessment with ISO 26262 (2021). https://www.einfochips.com/blog/automotive-risk-assessment-with-iso-26262/. Accessed 02 Nov 2022
8. Wolf, M., Scheibel, M.: A systematic approach to a qualified security risk analysis for vehicular IT systems. In: Plödereder, E., Dencker, P., Klenk, H., Keller, H.B., Spitzer, S. (eds.) Automotive - Safety & Security 2012, pp. 195–210. Gesellschaft für Informatik e.V, Bonn (2012)
9. Macher, G., Armengaud, E., Brenner, E., Kreiner, C.: Threat and risk assessment methodologies in the automotive domain. Proc. Comput. Sci. **83**, 1288–1294 (2016). https://doi.org/10.1016/j.procs.2016.04.268
10. Monteuuis, J.P., Boudguiga, A., Zhang, J., Labiod, H., Servel, A., Urien, P.: Sara: Security automotive risk analysis method. In: Proceedings of the 4th ACM Workshop on Cyber-Physical System Security. CPSS '18, pp. 3–14. Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3198458.3198465
11. Forbes: Five Risk Assessments Where Automotive Giants Need To Improve To Compete With Startups (2021). https://www.forbes.com/sites/stevetengler/2021/07/08/five-risk-assessments-where-automotive-giants-need-to-improve-to-compete-with-startups/. Accessed 02 Nov 2022
12. Wang, Y., Wang, Y., Qin, H., Ji, H., Zhang, Y., Wang, J.: A systematic risk assessment framework of automotive cybersecurity. Automotive Innovation **4**(3), 253–261 (2021). https://doi.org/10.1007/s42154-021-00140-6
13. Bekker, H.: Q1/2019 Europe: Best-Selling Car Manufacturers and Brands (2019). https://www.best-selling-cars.com/europe/q1-2019-europe-best-selling-car-manufacturers-and-brands/. Accessed 02 Nov 2022
14. COSCA Team: Classifying data collected by cars (2020). https://cosca-project.dmi.unict.it/. Accessed 02 Nov 2022
15. Osborne, C.: Volkswagen, Audi disclose data breach impacting over 3.3 million customers, interested buyers (2021). https://www.zdnet.com/article/volkswagen-audi-disclose-data-breach-impacting-over-3-3-million-customers-interested-buyers/. Accessed 02 Nov 2022
16. Motorbiscuit: Major Software Flaw Leaves Ford and Volkswagen Cars Vulnerable to Hackers (2021). https://www.motorbiscuit.com/major-software-flaw-leaves-ford-volkswagen-cars-vulnerable-hackers/. Accessed 03 Nov 2022
17. O'Donnell, L.: Volkswagen Cars Open To Remote Hacking, Researchers Warn (2018). https://threatpost.com/volkswagen-cars-open-to-remote-hacking-researchers-warn/131571/. Accessed 03 Nov 2022
18. France24: France's Renault hit in worldwide 'ransomware' cyber attack (2017). https://www.france24.com/en/20170512-cyber attack-ransomware-renault-worldwide-british-hospitals. Accessed 03 Nov 2022
19. Sharma, A.: Ford bug exposed customer and employee records from internal systems (2021). https://www.bleepingcomputer.com/news/security/ford-bug-exposed-customer-and-employee-records-from-internal-systems/. Accessed 03 Nov 2022
20. Kass, H.: Mercedes-Benz hit by third-party data breach (2021). https://www.msspalert.com/cybersecurity-news/mercedes-benz-hit-by-third-party-data-breach/. Accessed 03 Nov 2022
21. Arghire, I.: Researchers Find Exploitable Bugs in Mercedes-Benz Cars (2021). https://www.securityweek.com/researchers-find-exploitable-bugs-mercedes-benz-cars. Accessed 03 Nov 2022
22. CISOMAG: Data Breach Affects 384,319 BMW Customers in the U.K. (2020). https://cisomag.eccouncil.org/bmw-data-breach/. Accessed 03 Nov 2022
23. Robinson, T.: BMW customer database for sale on dark web (2020). https://www.scmagazine.com/home/security-news/bmw-customer-database-for-sale-on-dark-web/. Accessed 03 Nov 2022
24. Osborne, C.: Over a dozen vulnerabilities uncovered in BMW vehicles (2018). https://www.zdnet.com/article/over-a-dozen-vulnerabilities-uncovered-in-bmw-vehicles/. Accessed 03 Nov 2022
25. Tencent Keen Security Lab: New Vehicle Security Research by KeenLab: Experimental Security Assessment of BMW Cars (2018). https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/. Accessed 03 Nov 2022
26. Abel, R.: Audi airbags disabled through software exploit (2015). https://www.crn.com.au/news/audi-airbags-disabled-through-software-exploit-410992. Accessed 03 Nov 2022
27. Cimpanu, C.: Toyota announces second security breach in the last five weeks (2019). https://www.zdnet.com/article/toyota-announces-second-security-breach-in-the-last-five-weeks/. Accessed 03 Nov 2022
28. Goud, N.: Cyber Attack on Toyota Car Maker (2019). https://www.cybersecurity-insiders.com/cyber-attack-on-toyota-car-maker/. Accessed 03 Nov 2022
29. Tencent Keen Security Lab: Experimental Security Assessment on Lexus Cars (2020). https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/. Accessed 03 Nov 2022
30. Brook, C.: Tesla Data Theft Case Illustrates the Danger of the Insider Threat (2021). https://digitalguardian.com/blog/tesla-data-theft-case-illustrates-danger-insider-threat. Accessed 03 Nov 2022
31. Houcheime, W.: Tesla Experiences Internal Breach, Leaking Valuable Company Data (2021). https://securityboulevard.com/2021/02/tesla-experiences-internal-breach-leaking-valuable-company-data/. Accessed 03 Nov 2022
32. Kovacs, E.: Tesla Car Hacked Remotely From Drone via Zero-Click Exploit (2021). https://www.securityweek.com/tesla-car-hacked-remotely-drone-zero-click-exploit. Accessed 03 Nov 2022
33. Whittaker, Z.: Flaws in third-party software exposed dozens of Teslas to remote access (2022). https://techcrunch.com/2022/01/24/teslamate-bug-teslas-exposed-remote/. Accessed 03 Nov 2022
34. COSCA Team: Assessment of car security risks and drivers' privacy risks (2020). https://cosca-project.dmi.unict.it/. Accessed 03 Nov 2022

35. Greenberg, A.: A New Wireless Hack Can Unlock 100 Million Volkswagens (2016). https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/. Accessed 03 Nov 2022
36. Sajdak, M.: The new hack allows wireless opening of over 100 million cars: Audi, Skoda, various VW, Ford, Citroen (2016). https://research.securitum.com/the-new-hack-allows-wireless-opening-of-over-100-million-cars-audi-skoda-various-vw-ford-citroen/. Accessed 03 Nov 2022
37. McGlaun, S.: Ford Data Breach Not An Issue Says Automaker (2019). https://fordauthority.com/2019/06/ford-data-breach-not-an-issue-says-automaker/. Accessed 03 Nov 2022
38. Johnstone, L.: Peugeot Canada Hacked, Accounts and Data leaked by @Ag3nt47 (2013). https://www.databreaches.net/peugeot-canada-hacked-accounts-and-data-leaked-by-ag3nt47/. Accessed 03 Nov 2022
39. Winder, D.: Airbus, Porsche, Toshiba And Volkswagen Data Stolen In Massive Breach – What You Need To Know (2019). https://www.forbes.com/sites/daveywinder/2019/05/04/airbus-porsche-toshiba-and-volkswagen-data-stolen-in-massive-breach-what-you-need-to-know/. Accessed 03 Nov 2022
40. The Institution of Engineering and Technology: Serious cybersecurity flaws uncovered in Ford and Volkswagen cars (2020). https://eandt.theiet.org/content/articles/2020/04/serious-cybersecurity-flaws-uncovered-in-ford-and-volkswagen-cars-that-could-endanger-drivers/. Accessed 03 Nov 2022
41. Johnstone, L.: Automotive Giant Audi Hacked, 2000+ Account Credentials leaked by Xc0unt3r (2013). https://www.databreaches.net/automotive-giant-audi-hacked-2000-account-credentials-leaked-by-xc0unt3r/. Accessed 03 Nov 2022
42. Hackaday: Reverse engineering the Renault Update List display - Part 1 (2017). https://hackaday.io/project/27439-smart-car-radio/log/67874-reverse-engineering-the-renault-update-list-display-part-1. Accessed 03 Nov 2022
43. Constantin, L.: Researchers hack Tesla Model S with remote attack (2016). https://www.pcworld.com/article/3121999/researchers-demonstrate-remote-attack-against-tesla-model-s.html. Accessed 03 Nov 2022
44. Cimpanu, C.: Tesla car hacked at Pwn2Own contest (2019). https://www.zdnet.com/article/tesla-car-hacked-at-pwn2own-contest/. Accessed 03 Nov 2022
45. Bizga, A.: Tesla Data Leak: Pre-Owned Vehicle Infotainment Components Store Owners' Personal Details and Passwords (2020). https://securityboulevard.com/2020/05/tesla-data-leak-pre-owned-vehicle-infotainment-components-store-owners-personal-details-and-passwords/. Accessed 03 Nov 2022
46. Whittaker, Z.: Mercedes-Benz app glitch exposed car owners' information to other users (2019). https://techcrunch.com/2019/10/19/mercedes-benz-app-glitch-exposed/. Accessed 03 Nov 2022
47. Kirk, J.: Mercedes-Benz Data Leak Lesson: Lock Down Code Repositories (2020). https://www.bankinfosecurity.com/blogs/mercedes-benz-data-leak-embarrassing-but-endurable-p-2903. Accessed 03 Nov 2022
48. Bella, G., Biondi, P., Costantino, G., Matteucci, I.: CINNAMON: A Module for AUTOSAR Secure Onboard Communication. In: 2020 16th European Dependable Computing Conference (EDCC), pp. 103–110 (2020). https://doi.org/10.1109/EDCC51268.2020.00026
49. Bella, G., Biondi, P., Costantino, G., Matteucci, I.: Designing and implementing an AUTOSAR-based Basic Software Module for enhanced security. Computer Networks, 109377 (2022). https://doi.org/10.1016/j.comnet.2022.109377
50. Felt, A.P., Wagner, D.: Phishing on Mobile Devices (2011). https://people.eecs.berkeley.edu/%7Edaw/papers/mobphish-w2sp11.pdf. Accessed 03 Nov 2022
51. Francillon, A., Danev, B., Capkun, S.: Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars (2010). https://eprint.iacr.org/2010/332.pdf. Accessed 03 Nov 2022
52. Greenberg, A.: Hackers Could Steal a Tesla Model S by Cloning Its Key Fob-Again (2019). https://www.wired.com/story/hackers-steal-tesla-model-s-key-fob-encryption. Accessed 03 Nov 2022
53. Zeng, K., Liu, S., Shu, Y., Wang, D., Li, H., Dou, Y., Wang, G., Yang, Y.: All your gps are belong to us: Towards stealthy manipulation of road navigation systems. In: Proceedings of the 27th USENIX Conference on Security Symposium. SEC'18, pp. 1527–1544. USENIX Association, USA (2018)
54. Turla, J.: Mazda Infotainment USB Port PoC Attacks (2017). https://github.com/shipcod3/mazda_getInfo. Accessed 03 Nov 2022
55. Thomson, I.: Stop the music! Booby-trapped song carjacked vehicles - security prof (2016). https://www.theregister.com/2016/01/26/hackers_can_take_full_control_of_car_os/. Accessed 03 Nov 2022
56. Negru, S.: Connected cars and in-car payments: the road so far and the road ahead (2019). https://thepaypers.com/expert-opinion/connected-cars-and-in-car-payments-the-road-so-far-and-the-road-ahead. Accessed 03 Nov 2022
57. Constantin, L.: Researchers Hack Car Infotainment System and Find Sensitive User Data Inside (2017). https://www.vice.com/en/article/3kvw8y/researchers-hack-car-infotainment-system-and-find-sensitive-user-data-inside. Accessed 03 Nov 2022
58. Kuzin, M.: Mobile apps and stealing a connected car (2017). https://securelist.com/mobile-apps-and-stealing-a-connected-car/77576/. Accessed 03 Nov 2022
59. Costantino, G., La Marra, A., Martinelli, F., Matteucci, I.: CANDY: A Social Engineering Attack to Leak Information from Infotainment System. In: 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), pp. 1–5 (2018). https://doi.org/10.1109/VTCSpring.2018.8417879
60. Fugiglando U. et al.: Characterizing the "Driver DNA" Through CAN Bus Data Analysis. In: Proceedings of the 2nd ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services. CarSys '17, pp. 37–41. Association for Computing Machinery, New York, NY, USA (2017)
61. Vasile, S., Oswald, D., Chothia, T.: Breaking all the things–a systematic survey of firmware extraction techniques for iot devices. In: Bilgin, B., Fischer, J.-B. (eds.) Smart Card Research and Advanced Applications, pp. 171–185. Springer, Cham (2019)
62. Whittaker, Z.: Security flaws let anyone snoop on Guardzilla smart camera video recordings (2018). https://techcrunch.com/2018/12/27/guardzilla-security-camera-flaws/. Accessed 03 Nov 2022
63. Mimoso, M.: Unnamed, Popular ICS Firmware Contains Hard-Coded FTP Credential (2013). https://threatpost.com/unnamed-popular-ics-firmware-contains-hard-coded-ftp-credential/100941/. Accessed 03 Nov 2022
64. Hunt, T.: Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs (2016). https://www.troyhunt.com/controlling-vehicle-features-of-nissan/. Accessed 03 Nov 2022
65. Ruef, M.: Car Hacking - Analysis of the Mercedes Connected Vehicle API (2018). https://www.scip.ch/en/?labs.20180405. Accessed 03 Nov 2022
66. Conger, K.: Apple will require HTTPS connections for iOS apps by the end of 2016 (2015). https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/. Accessed 03 Nov 2022
67. Cyber Center of Excellence: Data Leak Hits Nissan North America (2021). https://sdccoe.org/breach/data-leak-hits-nissan-north-america/. Accessed 03 Nov 2022
68. Gayou, S.: Jailbreaking Subaru StarLink (2018). https://github.com/sgayou/subaru-starlink-research/blob/master/doc/README.md. Accessed 03 Nov 2022

**Giampaolo Bella** holds a Cambridge University Computer Laboratory Ph.D. and postdocs at Technische Universität München and Cambridge University. He has been with the University of Catania since 2001, seconded through the years with De Montfort University and SAP Research France. He is currently a visiting professor at the Royal Holloway University of London. His main research area is cybersecurity, data protection, and their socio-technical aspects, having conducted inter-disciplinary research with Social Scientists, Biologists, and Lawyers. He is the Chief Cyber Security Advisor for ICT Cyber Consulting and directs the Catania Site of CINI Cybersecurity Lab. He is a stable EU FP7/H2020 evaluator, rapporteur and reviewer.



**Pietro Biondi** is a Ph.D. student in Computer Science at the University of Catania. He obtained his Master's Degree in Computer Science (summa cum laude) in July 2019 at the University of Catania. His degree thesis concerns the study, design, and implementation of a security protocol on the CAN bus called TOUCAN. From 2018 he holds a position as a junior researcher with CNR, focusing on topics related to automotive security under the supervision of Dr. Gianpiero Costantino and Dr. Ilaria Matteucci. Pietro Biondi has produced a few scientific articles on this field. At the moment he teaches at the scientific high school in Sicily.



**Giuseppe Tudisco** graduated with a Master's degree in Computer Science (Network and Security Systems) in 2020 at the University of Catania. His master's thesis, under the supervision of professor Giampaolo Bella and Dr. Pietro Biondi, focused on cybersecurity risks in the modern automotive context. Currently, he is a research fellow at the Astrophysical Observatory of Catania (INAF-OACT). His research interest covers the field of scientific visualization. He is currently involved in the following projects: H2020 NEANIAS, ERC ECOGAL, INAF PRIN CIRASA, and SKA Regional Centres.