2.1 Introduction and Definition of Terminology

Since the early 1920s, people have envisioned cars 1 day driving them, free of human intervention. We have now reached a point where the technology exists to make this a reality. In less than 10 years, we can expect to see autonomous vehicles on our roads, fundamentally changing what it means to drive. While the technical challenges of getting a car to navigate on its own have been largely addressed, that is not the only criteria required for success.

No autonomous driving program will ever make it out of trial phase unless issues surrounding privacy, safety, and security have been addressed. In this chapter, we use the term “safety” for the correct system functioning of the car and the protection of the people in the car, mainly to ensure avoidance of car and/or traffic accidents. The term “privacy” is about the protection of a person and his/her behavior, meaning that he/she is able to control the risks for his or her rights to privacy, freedom, or equality caused by the processing of data related to him or her. The term “security” defines a situation where the integrity, confidentiality, and availability of data are guaranteed. Security particularly serves here, referring to the sum of measures taken, to ensure safety and privacy in its meaning described before. Therefore, a holistic development view on security, safety, and privacy is required, as they are all interacting, and cannot be seen completely independent.
Consumers, governments, and businesses need to be assured that autonomous vehicles are safe from hacks, viruses, and other malicious elements that could cause widespread damage. Just a serious incident with one vehicle may be enough to ensure that autonomous vehicles never make it to our roads, so technologists must be sure that what they have created is safe and secure.

Privacy is also front of mind for consumers. Concern about what data is being collected on individuals and how it is being used, is widespread, particularly relating to new technology. The autonomous cars of tomorrow will have to take these serious concerns into account and use data in a way that is useful, but not damaging to individuals. Guardedness will be even more a strong differentiator for OEMs to get a competitive advantage in the sharing economies of the future.

2.2 Principles of Autonomous Driving

2.2.1 Technological Principles

From a technological perspective, driverless cars will be enabled by connectivity, raising the necessity to achieve the next level of performance and reliability in security, safety, privacy protection, and traffic efficiency.

This will be achieved through the design and development of next-generation automotive components, subsystems, and connected platform architectures. All of these must be based on the following critical-trust principles:

1. Secure maintenance of safety, comfort, productivity, and mobility services in a privacy conserving way.
2. Health management (monitoring and upgrading).
3. Open platform principles and architectures utilizing trusted components and trusted intra and extra vehicular networks, including seamless cooperation of different communication paradigms and high data rate sensor networking, e.g., using Automotive Ethernet.
4. Trusted cloud services for diagnostics, prognostics, and the monitoring and upgrading of security, functionality, and reliability.
5. All highlighting the need for security, privacy frameworks, and implementations on the basis of security and privacy by design, as well as “need to know” principles.

This is illustrated in Fig. 2.1, where security is seen to be a system-property spanning from components to cloud solutions. It is to be noted that for some of the components physical security is essential (so protection to side-channel attacks and physical reverse engineering), since trustworthiness of the services and information provided by complete infrastructure solutions can be at stake. This is for example the case with the V2X communication subsystems which are based on public key security infrastructures.
2.2.2 Data Principles

Legal uncertainty with regard to security and privacy currently disadvantages Europe’s ability to take the lead for intelligent, connected, or autonomous driving solutions. Therefore, Europe should take a proactive role in defining and implementing a strategy how to create impetus for a secure and privacy respecting Internet of Things (IoT), supporting this with leading state-of-the-art technology solutions.

The aim is to facilitate automotive IoT components and subsystems to seamlessly work together across the various connectivity standards and compiling big data on their operations, including:

- Vehicle-to-Anything (V2X)/802.11p Wireless
- Radar
- Radio and Satellite Broadcast
- Automotive Telematics Onboard Unit Platforms

This also applies the concept of data governance, referring to the needs of private companies for immaterial property rights and business secrets as well as of citizens for privacy and safety, providing a best rule of access to data. In doing so, we must focus on three data principles:

- **Security by Design**—All devices connected to the IoT shall be protected via ensuring the devices and communication are intrinsically secure, achieved through a.o. incorporating secure coding and encrypted communications.
- **Privacy by Design**—Privacy is safeguarded not only by normative expectations such as by law but already on the infrastructural technological level.
• **Need to Know Principle**—Each connected entity can only communicate data to the IoT that is absolutely relevant for its core application. Further to the privacy-by-design principle, the access is granted by the entities, be it a person or a company, having the corresponding access rights.

### 2.3 Status of What Exists Today

Different systems and networks within the car have different vulnerabilities and attack points. They therefore require different levels of security. In some cases, software security may be sufficient, but other cases require much stronger tamper proof security solutions. Similarly, solutions like intrusion detection systems and authentication of messages and secure firmware over-the-air updates can provide a comprehensive protection system. Physical security at component level is needed in order to protect against advanced side-channel attacks and physical reverse engineering.

As more vehicles leverage V2X to eliminate accidents, ease congestion, and reduce emissions, they are creating new challenges for the industry. With more cars communicating wirelessly, vehicles are now opening up gateways for car systems to be accessed and manipulated.

Hackers are able to use these communications channels to gain direct control of cars and as a result wreak potential havoc on the roadways and even create mass accidents. For example, causing multiple cars to brake suddenly can cause a mass accident. It is therefore critical that vehicles are able to detect malicious data such as viruses or intrusions and authenticate incoming messages.

In the past year, several leading automotive manufacturers have fallen victim to connected car hacks. In summer 2015, two security experts hacked into a Jeep Cherokee via its internet-connected entertainment system. As a result, they were able to cut the vehicle’s transmission, bringing it to a grinding halt on a busy American highway—all from the comfort of their sofa. A month later, researchers at the Usenix security conference demonstrated how they could access critical functions of a Corvette through a wirelessly connected device commonly used for tracking by insurers and trucking fleets.

Despite these risks, vulnerability to hacking is not sufficiently covered in the main automotive industry standards. ISO26262, for example, only determines Automotive Safety Integrity levels for passenger cars and light utility vehicles based on the reduction of systematic failures caused by human error and random failures caused by factors such as aging or thermal wear-out.

Leading automotive manufacturers such as Ford, GM, Nissan, Mazda, Honda, VW, Audi, Daimler, Hyundai Motor, and Kia are now cooperating to drive common security approaches and standards. For example, the CAMP consortium (Crash Avoidance Metrics Partnership consortium) in America has been set up to build a secure system in cooperation with the U.S. Department of Transportation. CAMP has already spent several years researching and testing a variety of security
solutions. Similar initiatives are the Car 2 Car Communication Consortium (C2CC) and the C-ITS Advisory Group in Europe and the ITS Connect Promotion Consortium in Japan. Regarding privacy requirements, there are similar initiatives. For example, members of the German Union of Automobile Industry (VDA) provided for data protection principles for connected cars. These privacy-by-design principles shall ensure safe and transparent processing of personal data in order to meet legal responsibility and the customers’ trust.

Though connected vehicles are still a long way from mass adoption, the recent hacking incidents are an important lesson for the automotive industry. They highlight that there needs to be a solid foundation of security, privacy, and trust to fully take advantage of innovations in connected and self-driving vehicles. A large part of this relies on the entire ecosystem coming together, manufacturers, technology suppliers, regulators, etc., to make sure that the physical and digital safety of drivers is prioritized, so vehicles will be robust enough to stand up to hacking attempts and any further abuse of data.

### 2.4 Future Expectations for Autonomous Driving

The transformation towards autonomous driving is already well underway, thanks to several features of automated driving (adaptive cruise control, lane-warning, etc.). Over the next few years, the car as we know will transform from a simple mode of transport to a personalized mobile information hub—fully connected to the outside world.

Innovations are already helping to create a more enjoyable, customized driving experience for consumers as well as making driving safer and more enjoyable. But this is just the beginning. Let’s take a glimpse of what the future of driving looks like and how privacy and security will work in the age of the autonomous car.

One of the biggest changes brought on by autonomous driving will be the shift from car ownership to a share/rental model. Already car sharing schemes like DriveNow, Car2Go, or ZipCar are changing urban driving habits to a more pay-by-use model. This trend will accelerate as autonomous driving becomes more commonplace. Cars will be able to be booked in advance from a provider or available on demand via smartphone (or wearable) apps. The autonomous car will drive directly to the customer’s house and wait outside. One can think about “uber taxis” without driver. It will be important to ensure that only the approved driver has access to the autonomous vehicle. Solutions in place today, like RFID tags for example, will be able to securely identify users via their smartphone.
With the advent of mass car sharing comes enhanced risk of data being mistakenly shared between users. The autonomous car sharing schemes of tomorrow will use data collected about users to enhance their experience. Data will be stored on:

- Recent or favorite destinations
- Personal details on the user, including payment details
- Preferences relating to seating, temperature, music, etc.

This data also awakens the interests of many further parties such as insurance companies or providers of commercial products and services. Insurance companies are able, for example, to adapt the insurance policies to the personal driving behavior of drivers. Providers of commercial products and services will increasingly seek to advertise their offers based on the location and personal preferences of the drivers.

Securing and protecting this personal data will be vital to maintaining consumer trust, as proven by several high profile incidents of data theft/loss. UK Internet provider TalkTalk, for example, suffered huge reputational and financial damage following a cyber attack in which customers personal details were stolen.

Autonomous vehicles will travel on the roads using a complex system of radar and V2X technologies which gather information about its surroundings, providing the onboard computers with an image of obstacles or dangers the driverless system must avoid.

The cars will know the route and automatically stream onto the motorway to “platoon”—hooking themselves to another group of cars heading in the same direction. Safe speed and distance is maintained via the onboard V2X technology. As well as communicating with vehicles around it, the device also speaks to other connected infrastructure.

These “communications” are enabled by V2X resulting in ad hoc data exchange networks between the vehicle and environment—in other words, independent, self-organizing networks of mobile users.

As with any other wireless network, communication is exposed to security risks that must be guarded against in order to prevent access from hackers and other potential threats. To do this, firstly the quality and integrity of data has to be ensured. Intelligent vehicles must be able to detect whether data has been altered and falsified for any reason when collected or transmitted. Wrong or defective data can block the applications on which they are based or render them ineffective—in the worst case becoming a genuine safety risk.

For instance, if inaccurate data misleads a vehicle into incorrectly recognizing the speed of the vehicle driving ahead of it, there could be fatal consequences. So mechanisms need to be integrated that can detect bad data, remove it from the communication circuit, or destroy it entirely. Automotive solutions will encrypt, authenticate, and secure data at a chip level. Using a set of security keys, the car can determine if the data really originates from a specific, trustworthy vehicle.

The same principle applies to other devices and services, which the vehicle may interact with. For example, there is no reason why the autonomous cars should not be able to interact with a café en route, making orders and sending payments in advance. Maintaining a secure connection will be essential to safeguard the
reputations of both the vendor and the car manufacturer. Service providers as well as consumers will not buy into a system unless they are confident it is secure and privacy preserving.

## 2.5 Building Social Trust

We have already mentioned the importance of consumer trust, but it is worth looking at in greater depth as it is vital to the future of autonomous vehicles. The world is becoming an increasingly networked place. From billboards to bus stops, lamppost to cars and roads, infrastructure is becoming smarter and more connected. Many people feel scared or at least insecure about the consequences. Is the technology reliable? What happens with my data? Companies and legislators have to face up to these concerns.

According to the latest surveys, half of all Internet users do not regard their data as secure on the Internet. For businesses, customer trust and revocation of trust are important elements of business models.

No matter how well the technology works, without consumer trust it will never achieve widespread adoption. This is especially true in case of autonomous cars. The technical challenges of driving will eventually be solved but the much harder task of convincing drivers to let go of the wheel will take longer. Without trust, there is no or very slow market uptake.

Figure 2.2 shows the concerns of new-car buyers regarding data privacy and hacking.

To build trust, customers need to be actively kept in the loop. They have to be able to understand the potential security vulnerabilities in the car and also understand how they are protected. This approach also benefits companies because strong security is a real cost factor. People will not be willing to pay for good security if they don’t understand how it is benefiting them. But if the awareness is raised, they will appreciate activities ensuring strong security even at higher costs.

Another important element to build trust is ensuring people and companies have complete sovereignty over their risks resulting from the processing of personal data. Connected cars and the entire Internet of Things will only be trusted if the data involved is solely used for the value added purposes offered to the consumer in a most transparent way. Furthermore, applying data minimization, i.e., by only collecting data that is really needed for the application, and nothing else, may increase people’s trust.

This requires absolute certainty in knowing which other devices have access to data and transparency about what they are using it for. They also need to be reassured that data is only accessed when necessary. For example, health records may be kept in autonomous cars in case of an accident but only emergency services should have access to these, not any other non-medical party.
New-car buyers are broadly concerned about data privacy and the possibility of hacking when it comes to car connectivity.

% of new-car buyers that (strongly) agree with the statement

| Statement                                                                 | Germany | US    | Brazil | China |
|---------------------------------------------------------------------------|---------|-------|--------|-------|
| I am reluctant to use car-related connected services because I want to keep my privacy | 51      | 45    | 37     | 21    |
| I am afraid that people can hack into my car and manipulate it (e.g., the braking system) if the car is connected to the Internet | 59      | 59    | 53     | 54    |

Source: McKinsey’s Connected Car Consumer Survey, 2014

Fig. 2.2 Concerns of new-car buyers regarding data privacy and hacking

In a sharing economy consumers eventually acting as “prosumers,” who are offering mobility services themselves, hold even more influence and power. So companies will very quickly learn that they can only be successful with a new deal approach based on cooperation. Ultimately consumers will decide more freely and volatile which trusted company they give their money to. In the end, only ethical and secure companies will survive.

When it comes to improving security, cross-industry and international collaboration is essential, all involved players need to be engaged for best-in-class solutions. By adhering to the aforementioned autonomous driving principles many of these issues can be overcome and trust can be built and maintained.

2.6 Impact on Industry

Maintaining privacy and security in autonomous vehicles is a complex issue that requires the support and cooperation of several industries in the complete value chain from semiconductor companies to TIER1’s and OEMs. When considering the implications of onboard connectivity, the need for security, and the possibility of cars driving themselves, it becomes clear that a cooperation is needed comprising the industry in the value chain, universities and research institutes. NXP Semiconductors and the Alexander von Humboldt Institute have started initiatives in this
field and are engaging with other partners to work towards complete solutions. In addition, other interest groups need to be actively involved, as, e.g., governments, insurance companies, and consumer groups (as, e.g., ADAC, ANWB, Touring, etc.).

Currently, a gap exists between governments and technology companies. This stems from a fundamental difference in how they traditionally operate. Governments are used to sharing information with the general public and being collaborative and open when it comes to new projects that have the potential to affect the lives of city residents. For democratic governments transparency is vital and they are very used to being held to account.

On the other hand, technology companies have a much more guarded approach to working. They come from a background where secrecy is essential to protecting risky R&D investments, valuable know-how, and sensitive intellectual property. They only unveil their solutions—even only partially—when they are ready to bring them to the market, as opposed to government projects which are generally transparent from the start and invite for active participation and feedback.

These systemic and cultural differences can cause friction between the two parties, and this slows down the development of a potentially joint innovation project like autonomous vehicles, which is reliant on the two working together. Ultimately without the government collaboration, autonomous vehicles can’t be approved for use on the road so a new way of working needs to be established that suits both parties. They must enter into a deliberative process where the outcomes are joint strategies and memorandums, which include both, the technological and social aspects of autonomous driving.

Self-driving vehicles will also have big implications for the insurance industry. Today, car insurance is set up to protect drivers financially after an involvement in an accident, as a result of their own error or someone else’s. The advent of autonomous driving changes this model completely. Firstly, road traffic accidents should be almost eliminated completely so the risk of drivers and passengers will virtually nearly disappear. As the human element comes out of the equation, question marks also remain around liability.

Insurance companies will likely have to shift liability from consumers to manufacturers, which has already been seen considering Volvo saying that it will accept full responsibility for driverless car crashes. They will also have to look more into pay-as-you-drive models for insuring cars. Ultimately insurance companies will need to change their business model and in order to do this, they will need to work with the government and manufacturers to develop best practices. Without sufficient insurance measures in place, autonomous driving will falter.

There needs to be a change of thinking and a new coordinated approach between governments, technology companies, and insurers. If all three parties collaborate to create joint strategies, which encompass technological and social aspects, autonomous vehicles can be on the market in just few years.
2.7 Next Steps

Security, privacy, and issues around consumer trust are the biggest hurdles to overcome autonomous driving. Ultimately, consumers need to trust this technology with not only their lives but also the lives of their families.

In order for this trust to be built, the entire ecosystem must come together, manufacturers, technology suppliers, governments, and insurers to take the following steps.

1. **Multi-stakeholder dialogue**
   Establish a coherent multi-stakeholder dialogue including representatives of end-user interests (e.g., data protection authorities and/or consumer protection organizations) in order to develop solutions that respect societal needs and expectations regarding access to data.

   These groups should be used in order to gain broad acceptance for privacy and security by design measures, which fully addresses the concerns of the individuals with regard to privacy and security of data and assets, as well as the organizations.

2. **Establish global principles and standards**
   The second step is to build on the dialogue to establish a condensed set of implementable principles and standards of security and privacy by design.

   They need to be applied to all areas including design, organizational structures, and international legislative requirements. A global consensus will also need to be reached on reliable certification processes and trust providing privacy policies.

3. **Develop modular system solutions**
   Establish architectures and prototypes of system-within-systems solutions that address critical security and privacy by design with the following features:

   (a) User-selectable opt-in configuration modes
   (b) Based upon interoperable, modular principles (software/hardware) with standard interfaces
   (c) Automotive certified with built-in privacy-preserving features that restrict access to data
   (d) Allowing separation of systems for cost-effective multi-vendor component sourcing

   Separation of systems also protects against hacks that target different, less critical areas of the car in order to reach more essential components. E.g., targeting the digital radio to affect the highly safety critical braking system.

4. **Next Gen secure components**
   Develop next generation components with inherent privacy protection and secure authentication comparable to current banking standards.
These secure components will combine high performance with the latest security principles to maintain protection over its lifecycle, mitigating impact of software attacks, fault attacks side channel attacks, and physical attacks including physical reverse engineering. The components and software will be flexible and open, to an extent, to ensure that they can be easily updated and upgraded.

5. **Impactful applications**

Important to the entire process will be to demonstrate and communicate the capabilities of the system solutions and the security and privacy by design solution strategies through a number of societal and business use cases.

Through this process, seals of “quality and trust” can be developed for certified secure solutions.

**2.8 Conclusions**

Based on recent car hacking incidents, all stakeholders in the car industry have become aware that security and privacy protection become more and more important in cars, which are integrated in the Internet-of-Things and/or which are autonomously driving. This will require the inclusion of security elements and privacy protect features from components to electronic systems and the complete car architecture. Furthermore, a close cooperation between all stakeholders involved in the value chain must be strengthened, including the interaction with the citizens, through a multi-stakeholder dialogue. Finally, it is also of crucial importance for all parties to work together towards a social trust model in the evolution from communicating cars to fully autonomous cars.