Report from Dagstuhl Seminar 22042

Privacy Protection of Automated and Self-Driving Vehicles

Frank Kargl[*1], **Ioannis Krontiris**[*2], **André Weimerskirch**[*3], **Ian Williams**[*4], and **Nataša Trkulja**[†5]

1 **Universität Ulm – Ulm, DE.** frank.kargl@uni-ulm.de
2 **Huawei Technologies – München, DE.** ioannis.krontiris@huawei.com
3 **Lear Corporation and University of Michigan Transportation Research Institute – Ann Arbor, US.** aweimerskirch@lear.com
4 **University of Michigan – Ann Arbor, US.** ianwill@umich.edu
5 **Universität Ulm – Ulm, DE.** natasa.trkulja@uni-ulm.de

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 22042 "Privacy Protection of Automated and Self-Driving Vehicles". The Seminar reviewed existing privacy-enhancing technologies, standards, tools, and frameworks for protecting personal information in the context of automated and self-driving vehicles (AVs). We specifically focused on where such existing techniques clash with requirements of an AV and its data processing and identified the major road blockers on the way to deployment of privacy protection in AVs from a legal, technical, business and ethical perspective. Therefore, the seminar took an interdisciplinary approach involving autonomous and connected driving, privacy protection, and legal data protection experts. This report summarizes the discussions and findings during the seminar, includes the abstracts of talks, and includes a report from the working groups.

Seminar January 23–28, 2022 – http://www.dagstuhl.de/22042
2012 ACM Subject Classification Security and privacy → Human and societal aspects of security and privacy; Security and privacy → Privacy protections; Security and privacy → Privacy-preserving protocols
Keywords and phrases automotive security and privacy, privacy and data protection
Digital Object Identifier 10.4230/DagRep.12.1.83

1 Executive Summary

Frank Kargl (Universität Ulm – Ulm, DE)
Ioannis Krontiris (Huawei Technologies – München, DE)
Nataša Trkulja (Universität Ulm – Ulm, DE)
André Weimerskirch (Lear Corporation – Ann Arbor, US)
Ian Williams (University of Michigan – Ann Arbor, US)

Cooperative, connected and automated mobility (CCAM) has the potential to drastically reduce accidents, travel time, and the environmental impact of road travel. To achieve their goals, connected and automated vehicles (AVs) require extensive data and machine learning algorithms for processing data received from local sensors, other cars, and road-side infrastructure. This immediately raises the question of privacy and data protection. While privacy for connected vehicles has been considered for many years, AV technology is still

[*] Editor / Organizer
[†] Editorial Assistant / Collector

in its infancy and the privacy and data protection aspects for AVs are not well addressed. The capabilities of AVs pose new challenges to privacy protection, given that AVs have large sensor arrays that collect data in public spaces. Additionally, AVs capture data not only from other vehicles, but also from many other parties (i.e. pedestrians walking along a street) with very limited possibilities to offer notice and choice about data processing policies. Additionally, the driver will not necessarily be the owner of the vehicle and it may be the case that the majority of AVs are owned by fleets.

Our seminar reviewed existing technologies, standards, tools, and frameworks for protecting personal information in CCAM, investigated where such existing techniques clash with the requirements of an AV and its data processing, and identified gaps and road-blockers that need to be addressed on the way to deployment of privacy protection in AVs from a legal, technical, and ethical perspective. While we ran only a shortened online version of the originally planned seminar due to COVID pandemic limitations, we made very good progress, in particular towards identifying and structuring the challenges. Future meetings will build on the results and will discuss the different challenges in more depth, prioritize the corresponding road blockers, and push for research to overcome them.

Discussions during the seminar were organized in seven sessions with presentations from renowned experts from industry and academia, and a final discussion that collected and structured outcomes. In the concluding session, we identified four main challenges that we present in this report alongside the talk abstracts.

- The first challenge is **ethics** and responsible behavior of companies and other actors that collect and process personal data in such systems. This goes beyond mere regulatory compliance but was seen as a promising path to complement this minimal baseline. Further discussions are required to identify ways to encourage such practices.
- Second, we discussed how **regulation** needs to evolve for future CCAM systems in order to establish a stable baseline. A challenge here will be to identify to what extent sector-specific regulation will be needed to address specifics of CCAM and if regulation of future systems is reasonable and possible.
- A third challenge is the **commercial** environment. Industry has to meet regulations and financial expectations and sometimes even conflicting goals like privacy and safety. Understanding and narrowing these trade-offs while acknowledging that industry has many such constraints that limit its flexibility requires further investigation.
- Last but not least, we see a strong progress in the privacy-enhancing **technology** (PET) as a promising path towards resolving many of the above mentioned problems. At the same time, many PETs have not been designed for the CCAM domain and might not meet its demands in data quality or latency. For this reason, we see the need to further investigate how existing PETs meet CCAM requirements or how they can be developed further to do so.

Generally speaking, there is a lack of incentives for enterprises like original equipment manufacturers (OEMs) to go beyond the legal minimum requirements to manage personal data in a privacy-respecting manner, to design privacy-preserving products, or to make the use of personal data transparent to the data subject. During our discussions one question became prominent: What could be the motivation for OEMs to do more in the field of data protection that goes beyond the bare minimum of legal compliance? Ethical and trustworthy aspects, as well as reputation and brand image could be worth investigating in answering this question. However, the field is massively interdisciplinary making it necessary to convince other involved disciplines of the value of data protection for the automotive sector.

There are several technical solutions available for protecting privacy and facilitating the privacy-by-design approach. However, the up-scaling of these solutions to larger systems and their integration with existing systems often fails because systems aspects and the related interdisciplinary issues are not taken into account. So, further progress is needed in promoting privacy-friendly system engineering, as well as integrating PETs into complete systems, taking into consideration the special requirements of safety and trust in the automotive domain. Overall, there should be a push for joint efforts to define and deploy technologies that are superior to today's solutions and that are commercially feasible since cost and effort are split amongst many participants.

Further progress is also required for the development of best practices, methodologies, and a requirements standard similar to ISO 21434 that supports the engineering of practical privacy solutions in complex systems. This will give OEMs a proper threshold target and allow for efficient solution finding and re-use. That guidance or standard could be a layer on top of regulation, similar to how the UN ECE R155 regulation requires a Cybersecurity Management System (CSMS) for which the ISO 21434 standard defines process requirements.

2 Table of Contents

Executive Summary

Overview of Talks

Working groups

3 Overview of Talks

3.1 Introduction to Privacy Protection of Automated and Self-Driving Vehicles

Frank Kargl (Universität Ulm, DE)

This talk opened the seminar with an overview over the field of automotive privacy and how it developed over the years. We started from early works on Car-to-Everything (C2X) and discussed how privacy was considered an important requirement from day one. From this perspective, C2X is an excellent example of privacy-by-design and privacy-by-default. We introduced how changing pseudonyms were designed as a mechanism to protect privacy and prevent location tracking, also highlighting its limitations and the need to balance and trade-off technical privacy against effort and efficiency of applications. As an example, we looked into tracking attacks that can easily reconstruct a vehicle's path from anonymous position samples (if they are available with sufficiently high resolution).

We then continued with the observation that just providing technical solutions is not enough. We also need to consider the field of privacy engineering and the challenges that integrating privacy engineering with the overall engineering process implies. This includes a number of observations. First, system engineering for automotive E/E systems is already a highly complex process that needs to consider many aspects, like safety, real-time requirements, security, and now also privacy. Simplifying and streamlining these processes is important. Second, we need to educate experts for privacy engineering and privacy-enhancing technologies (PETs), while at the same time providing the tools and skills to ordinary developers to enable privacy-by-design in their projects. And third, as automotive industry builds products for world-wide markets, considering all the different privacy regulations is a special challenge.

We then looked into a case study that Prof. Kargl's research group conducted on privacy of electric vehicle charging in 2010 [1]. In the POPCORN protocol [2], they re-engineered the ISO/SAE 15118 protocol towards better technical privacy protection. This research highlighted that with proper privacy engineering, we can build systems that are highly privacy-preserving that at the same time provide rich and personalized functionality. In its conclusion, the talk discussed challenges and questions specific to autonomous vehicles and future cooperative intelligent transportation system (cITS) architectures including:

- Privacy of automotive AI and machine learning mechanisms
- Increased complexity and data flows in cooperative ITS and CCAM
- The conflict between privacy and functional and safety requirements, and whether PETs could help to resolve it
- Challenges to policy-making and law-making

Many of these challenges were in the focus of the talks and discussions throughout the remainder of the seminar week.

References

1 Fazouane, Marouane, Henning Kopp, Rens W. Heijden, Daniel Le Métayer, and Frank Kargl. "Formal verification of privacy properties in electric vehicle charging." In International Symposium on Engineering Secure Software and Systems, pp. 17-33. Springer, Cham, 2015.

2 Christina Höfer, Jonathan Petit, Robert Schmidt, and Frank Kargl. "POPCORN: privacy-preserving charging for eMobility." In Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles, pp. 37-48. 2013.

3.2 The Role of Information in Autonomy and Community

Bryant Walker Smith (University of South Carolina, US)

Issues of privacy and data protection implicate the role of information in the larger goals of autonomy and community. These issues are exacerbated by the combination of increasingly powerful perception, processing, and transmission by advanced motor vehicles. In an analysis of these issues, some common distinctions among advanced vehicles matter, while others probably do not. This is evident in three threshold questions. First, (how) are mobile phones and other connected devices different than vehicles? Second, (how) are V2V-capable vehicles different than conventional vehicles? Third, (how) are automated vehicles different than conventional vehicles?

Connectivity and automation are orthogonal concepts. Connectivity in a narrow sense typically refers to the vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication that involves low latency, high reliability, direct(ish) transmission between road users. Connectivity in a broad sense refers to all manner of digital and wireless communication technologies and applications, including telematics, infotainment, over-the-air updates, remote assistance, mobile vehicle apps, and others. Automation typically involves distinctions between assisted driving and automated driving and among trips, vehicles, and features, but for the purposes here the distinction between safety and convenience features may be more significant.

Current and future technologies can monitor inside the vehicle, the vehicle itself, and outside the vehicle. This monitoring is accomplished with a large number and variety of internal-facing and external-facing sensors. Indeed, Congress recently directed NHTSA to soon mandate impaired driver detection systems in new vehicles. Data can be collected by these sensors for multiple overlapping purposes: To operate the system (implicit collection), to develop the system (implicit or intended), to document performance of the system (intended), or merely during operation of the system (incidental). It is also helpful to distinguish among data that are generated, processed, used, stored, and transmitted–on-board or off-board the vehicle.

This leads to three key questions: What can vehicle sensors perceive that humans cannot? What can computers do with that information that humans cannot? And what might companies, governments, and individuals do with these capabilities? This suggests immense possibilities both good and bad, for which canals, railroads, highways, and the Internet offer useful analogies from technologies of the past. Imagine a real-time version of Google's Street View or automated enforcement by private networks in which pedestrians who impede the movement of a company's vehicle are identified through facial recognition and then barred from that company's services as punishment.

This brings us to an antagonistic view of "privacy" as against a variety of actors, including domestic governments acting in their law enforcement or national security or administrative capacity or on behalf of companies, foreign governments acting in equivalent capacities, companies acting in a market, as employers, or on behalf of governments, individuals who are nosy, malicious, or controlling, and so forth.

The domain of safety offers lessons for privacy–since, indeed, both implicate autonomy and community. My argument is that automated vehicles are driven not by hardware or software or humans or nobody but by the companies that develop and deploy them. This is the position taken by the Uniform Law Commission's Automated Operation of Vehicles Act.

In other words, we should focus less on technologies and more on the companies behind those technologies. This means asking not "does the public trust this technology" but, rather, "is the company behind this technology worthy of our trust?" The former question is not useful because the public is fickle, words are not actions, marketing is still coming, and a lot can still change before we reach 100% adoption or acceptance (if ever). Similarly, asking "should the public trust this technology?" is not helpful because future technologies don't yet exist, these technologies will be diverse, and most won't be super dangerous. Indeed, the story of technology, society, law, and progress is about replacing one set of problems with a new set of problems and just hoping that the new set in aggregate is less than the old set–as illustrated by replacing the pollution of the horse with the pollution of the car.

"Is the company behind this technology worthy of our trust?" is an important question because companies act through their human and their machine agents, because technologies are only as safe (or privacy protecting) as the companies behind them, because safety (like privacy) is a marriage rather than a wedding, and because companies can do right even after their technologies fail. Similarly, regulation (whether of safety or privacy) needs the concept of trustworthiness because emerging technologies are complex, stochastic-ky, and dynamic; because developers have the expertise, information, and access to make lifecycle safety (or privacy) cases; because developers need space for technical innovation and regulators need space for regulatory innovation; and because even though regulators won't have all the answers, they can still ask better questions.

The question of how safe is safe enough has two answers: the retrospective (after a failure) and the prospective (before a deployment). Retrospective is more straightforward: a system must be at least as safe as a human in the maneuver and at least as safe as a comparative system, and (more controversially) safer than the last system to fail. Prospective safety is trickier, and my answer is that it means having reasonable confidence that the developer is worthy of our trust.

A trustworthy company, in turn, shares its safety philosophy (by saying what the company is doing, why it believes that to be reasonably safe, and why the public can believe the company), makes a promise to the public (by committing to market only what it believes to be safe, to being candid about its limits and failures, and by mitigating its failures), and then keeps that promise (by appropriately managing public expectations, supervising the entire product lifecycle, and mitigating harms promptly, fully, and publicly). The same approach might be applied to issues of privacy.

Looking for early breaches of trust is key to identifying untrustworthy actors. These breaches include making hyperbolic claims, misrepresenting evidence, failing to update technologies, exploiting the litigation process, and forcing confidential settlements. For example, if we cannot trust a company when it calls it system "full self driving," why should we trust that company when it calls its system safe or private? By analogy: Calling my umbrella a parachute doesn't make it true, but does make my umbrella more dangerous.

This approach also has implications for administrative regulation: Regulate the company rather than the technology; expect a company to vouch for its technologies through a public safety (or privacy) case; focus on processes and systems; identify assumptions and logical progressions; ask questions and challenge answers; and target breaches of public trust. In short (and to quote Voltaire or Spiderman): With great power comes great responsibility.

This detour into safety can also apply to privacy. In some ways, modern privacy law is something of a late 19th century invention. The foundational article, at least in the United States, may have been inspired by the fact that the paparazzi of the day used one technology–the camera–to take photos of a high-society wedding attended by one of the authors and then used another–the modern printing press–to distribute them widely in newspapers. But most people of the day did not enjoy privacy: They shared beds in tenements or other small homes, and they lived in communities of hundreds or thousands in full view of what Jane Jacobs approvingly called "eyes on the street." At the same time, they did have a form of escape that is largely unavailable today: They could physically run, or be chased, away from gossip and rumors and reputations. They could physically move to a new place without the kind of digital trail that would likely follow each of us today.

Privacy has since become a key aspect of the modern human rights doctrine. It can be embraced (or rejected) in ways that are revolutionary or evolutionary. It can be an end in itself or a means to an end. In particular, is may serve as a tool toward the goal of autonomy, where autonomy means the freedom to discover oneself, to be true to oneself, and to live one's own life. At the same time, society necessitates community, and every unit of governance other than the individual is a collective: governments, companies, religious institutions, families. And so both autonomy and community are part of happiness in the classic sense of leading a good life–that is, eudaimonia.

One of the key policy choices, to be determined by society much more than it is dictated by any existing law, is who or what will be empowered: individuals, governments, companies, or other collectives. Consider, very roughly, data protection. The approach in the EU has been to empower individuals through legal rights created by the General Data Protection Regulation (GDPR). The approach in the United States, at least prior to some recent state laws, has been to empower companies by generally enforcing the contracts of adhesion that we have all accepted in order to use many of the products and services essential to our modern lives. And the approach in the People's Republic of China has been to empower government in the storage and access expectations for companies operating in that country.

This is a crude model, and like everything else it is full of contradictions and unexpected consequences. For example, in the early 1900s, the US entered the "Lochner era" that empowered big business in the name of individual rights: Because the freedom to contract was paramount (indeed, the courts said, constitutionally protected), states could not enact rules for minimum wages or maximum hours worked. There are still echoes of this in so-called "right to work" states that restrict the power of unions. And in the European Union, there is concern that the GDPR could ultimately empower large companies vis-à-vis their smaller counterparts and ultimately vis-à-vis consumers.

One of my research interests is on using technologies and other tools to appropriately empower collectives. A key: Who inside the community, who is outside, and who decides?

These issues can be considered on the strategic, tactical, and operational levels. And here too there is much tension! It may be that governments should not necessarily adopt the policies that people think they want. For example, a world full of single-occupant vehicle trips on big, wide, fast roads is also a world of obesity and isolation and massive sea-level rise. In fact, there are benefits to "frictions" in life – what some incorrectly call inefficiencies. Sharing space with strangers, for example, can produce empathy and maybe even friendship–although it could also lead to harassment and assault. But it may be that policy should seek to accomplish what people say they want at a strategic level if not necessarily at an operational level. People say they want communities with fresh air and active mobility, for example. One answer is to set, regularly review, and as necessary revisit public policy goals so that changes are happen through deliberation rather than by default.

This presents a challenging strategic and even ethical question: Should innovation be understood primarily as a technical solution (to accomplish that which otherwise is technically impossible) or primarily as a policy solution (to accomplish that which is already technically feasible but not politically feasible)? For example, the public may be far more accepting of privacy and other risks inherent in the status quo than of equivalent risks inherent in new technologies. Similarly, economic interests may be far more entrenched for established technologies than for those that are merely emergent. This is one of the ethical issues explored in the "Ethics of AI in Transport" book chapter in the 2020 Oxford Handbook of Ethics in AI.

3.3 Ethics, Privacy, and Autonomous Vehicles

Adam Henschke (University of Twente, NL)

Main reference Adam Henschke: "Ethics in an Age of Surveillance: Personal Information and Virtual Identities", Cambridge University Press, 2017.
URL http://dx.doi.org/10.1017/9781316417249
Main reference Adam Henschke: "Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System", Moral Philosophy and Politics, Vol. 7(1), pp. 123–149, 2020.
URL http://dx.doi.org/doi:10.1515/mopp-2019-0056

In this talk, I covered a range of conceptual and ethical issues to do with privacy and autonomous vehicles. The talk started with a motivating problem, showing how potentially innocuous vehicle data can have social and political implications. The talk then gave an overview of the "swamp" of different ways that privacy can be conceptualised. When thinking of privacy in an interpersonal sense, it can be descriptive or normative. The talk then shows that we also need to think of privacy in a political sense, as the relationship between citizens and the state. The talk then suggested that technologies like autonomous vehicles may need us to add an international geopolitical sense of privacy, where what matters are the relationships between states. The talk next looked at how autonomous vehicles are different from traditional cars in terms of the capacity to aggregate, share, and use personal information. Finally, the talk offered a way out of the swamp of privacy concepts by suggesting that we ought to be concerned for privacy if and when autonomous vehicles gather, access, use, and/or communicate information that is revealing, powerful, or has a special meaning given a particular context.

3.4 CCAM Research: Experiences in Handling Data Protection Regulations @UULM-MRM

Michael Buchholz (Universität Ulm, DE)

Main reference Michael Buchholz, Johannes Muller, Martin Herrmann, Jan Strohbeck, Benjamin Volz, Matthias Maier, Jonas Paczia, Oliver Stein, Hubert Rehborn, Rudiger-Walter Henn: "Handling Occlusions in Automated Driving Using a Multiaccess Edge Computing Server-Based Environment Model From Infrastructure Sensors", IEEE Intelligent Transportation Systems Magazine, Vol. PP, pp. 2–16, 2021.
URL http://dx.doi.org/10.1109/MITS.2021.3089743

This talk starts with a short introduction of our cooperative, connected and automated mobility (CCAM) research at the Institute of Measurement, Control, and Microtechnology (MRM) at Ulm University (UULM). Besides several automated test vehicles with approval for public traffic, UULM-MRM operates a smart infrastructure installation at an intersection in Ulm-Lehr, a suburb of Ulm. Details can be found in this video: `https://www.youtube.com/watch?v=RFdIpi3buAg`.

For both, test vehicles and smart infrastructure, sensors such as cameras are used, which potentially capture personal data of (other) road users. The second part of this talk focuses on the experiences made with implementing data security concepts as required by GDPR and national laws, as well as the experiences that the research team had with the persons concerned, all from an engineering perspective. For UULM, the Data Protection Act of the State of Baden-Württemberg holds, whereas for companies, the federal law is applicable.

The talk highlights some specific experiences and solutions, such as storing video data in read-only mode to avoid logging of potential changes, or the use of pictograms and QR codes to inform the persons concerned. Additionally, it is reported that sharing the data with others, like companies, is also possible, e.g., by using subcontracting or joint controller contracts. One experience discussed in the talk is the fact that most people seem not to care about the cameras on the vehicles or in the infrastructure, since there have been almost no questions and objections from persons concerned. Finally, personal conclusions are drawn, which address also the requirement of a good communication between the responsible lawyers/data security officers and the engineers.

3.5 Privacy Challenges of Connected and Autonomous Vehicles

Benedikt Brecht (Volkswagen AG – Berlin, DE)

This talk is an opinion contributing to the discussion of the seminar rather than a scientific presentation. It focuses on vehicle data and the potential privacy issues that may arise when accessible via different means. It begins with showing and listing all known and specific privacy-relevant data that is available in modern cars [1]. The listing gives a first understanding as to why getting access to this data could be a privacy issue. Especially as it is relatively simple to access this data, given physical access to such a vehicle, the tools and the know-how that is available on the internet. The section ends with a discussion of potential reasons why this data is not better protected yet, and why this becomes a potential privacy problem when selling a car or parts of it. The next section is a digression to Car-to-Everything (C2X) communication. It lists which data is sent out when enabling

C2X in modern, European cars of a specific make. It also highlights the fact that this data is unencrypted as this is the only solution to solving the requirements of availability (even if not connected to the internet), as well as latency that is required by the safety functions; the overhead created by any key exchange for an effective encryption would not meet these requirements. This section ends with a discussion about whether legitimate interest following GDPR is a sufficient legal basis. The following section discusses why especially autonomous vehicles add massively to the privacy issue due to their extended sensors and the way data is collected in order to make machine learning work. The last section gives a glimpse to a developing effort of ETSI's Technical Committee (TC) Lawful Interception (LI) summarized in their Technical Report (TR) 103 854. They appear to be working on standardizing the access to in-vehicle data (e.g., live camera feeds, planning of routes, customer details etc.) for law enforcement agencies while linking their effort to the ongoing regulation effort of the European Union on Electronic Evidence (E-Evidence).

References

1 c't – *magazin für computertechnik* 2022, Heft 1, pages 20/21. Heise Medien GmbH & Co. KG, Hannover, GER, 2022

3.6 Technologies for Establishing and Managing Trust in CCAM

Thanassis Giannetsos (UBITECH Ltd. – Athens, GR)

Joint work of Thanassis Giannetsos, Ioannis Krontiris
Main reference Benjamin Larsen, Thanassis Giannetsos, Ioannis Krontiris, Kenneth A. Goldman: "Direct anonymous attestation on the road: efficient and privacy-preserving revocation in C-ITS", in Proc. of the WiSec '21: 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Abu Dhabi, United Arab Emirates, 28 June – 2 July, 2021, pp. 48–59, ACM, 2021.
URL http://dx.doi.org/10.1145/3448300.3467832

This talk focused on the security, privacy, and trustworthiness, which are key properties that need to be considered as we are moving towards the realization of the 5G C-V2X technology. In this context, converging all of these properties by assessing dynamic trust relationships and defining a trust model and a trust-reasoning framework is of paramount importance; based on which involved entities can establish trust for cooperatively executing safety-critical functions. This will enable both a) cybersecure data sharing between data sources in the cooperative, connected and automated mobility (CCAM) ecosystem that had no or insufficient pre-existing trust relationship, and b) outsource tasks to the MEC and the cloud in a trustworthy way. Beyond the needs of functional safety, trustworthiness management should be included in CCAM's security functionality solution for verifying trustworthiness of transmitting stations and infrastructure. Compounding this issue, new schemes need to be designed that build upon and expand the Zero Trust concept: how to bootstrap vertical trust from the application, the execution environment, and the device hardware from the vehicle up to MEC and cloud environments.

For the latter, a promising solution integrates the use of trusted computing technologies and attestation mechanisms to enable the establishment of such "strong" trust relationships. This includes the integration of TEE technologies that enable highly secure, trusted, and verifiable remote computing capabilities, which can offer guarantees and assurances for the establishment of trust through the required proofs/claims. Such proofs can provide verifiable evidence on their correctness and functional safety, from their trusted launch and configuration to the runtime attestation of both behavioral and low-level concrete execution properties.

On the privacy front, Direct Anonymous Attestation (DAA) offers a promising solution – to overcome the challenges of traditional Public Key Infrastructures (PKIs) – by shifting trust from the backend infrastructure to the edge vehicles. DAA is a cryptographic protocol designed primarily to enhance user privacy within the remote attestation process of computing platforms, which has been adopted by the Trusted Computing Group (TCG). Applying the DAA protocols for securing V2X communication results in the redundancy (and removal) of most of the PKI infrastructure entities, including the pseudonym certificate authority: vehicles can now create their own pseudonym certificates using an in-vehicle trusted computing component (TC), and DAA signatures are used to self-certify each such credential that is verifiable by all recipients. Furthermore, a DAA-based model supports a more efficient revocation of misbehaving vehicles that don't require the use of CRLs, therefore removing all of the computational and communication overhead that comes with it.

Based on the above, some final conclusions were reached as it pertains to the future of CCAM technologies: this new security paradigm is the key element for having certifiable, more agile levels of trustworthiness to automotive services and translates to long-term consumer confidence, which is a requirement for end-user adoption.

3.7 On Exploring the Use of Local Differential Privacy in ITS

Ines Ben Jemaa (IRT SystemX – Palaiseau, FR)

Joint work of Ines Ben Jemaa, Anis Bkakria, Cedric Adjih, Ala'a Almomani, Michael Wolf

In this talk, we focus on the vehicular kinematic data sharing with the edge servers scenarios. One of the main privacy threats of this data sharing is the ability of an attacker to reconstruct the vehicular trajectory and thus learn information about the user profile. Differential Privacy (DP) [1] seems to be a promising solution to protect such data. Compared to other privacy approaches based on anonymization, cryptography or obfuscation, DP offers strong theoretical guarantees of privacy by adding some noise on the data following a specific probabilistic distribution while keeping some desired utility. Thus, it is compatible with the low overhead and computation complexity requirements of embedded systems. While the centralized scheme of DP is based on the data noise addition by a trusted curator, the local scheme, which assumes an untrusted curator, seems more realistic and convenient for our data sharing model. In the local scheme, the noise addition operation is attributed to the end users (i.e. the data originators) before transmitting their data to the server. The Geo-indistinguishability [2] paradigm implements the local scheme of DP and provides interesting properties for location privacy protection. We focused on studying its feasibility in the context of continuous data sharing in the connected and automated driving context and realize that there are some remaining challenges that have to be addressed. One of these challenges is the periodic nature of data sharing which decreases the privacy level and raises the problem of privacy budget allocation. The privacy budget allocation strategy could also directly impact the trade-off between the privacy and the utility of the service. The second challenge is the location correlation risk created by continuous sharing, which is not solved by geo-indistinguishability designed originally for sporadic use.

References

1 C. Dwork. *Differential privacy*. Proceedings Of ICALP, volume 4052 of LNCS, pages 1–12. Springer, 2006

2 Andrés, M. E., Bordenabe, N. E., Chatzikokolakis, K., Palamidessi. *Geo-indistinguishability: Differentialprivacyfor location-basedsystems*. Proceedings of the ACM Conferenceon Computer and Communications Security, 901–914.

3.8 Automotive Privacy – The Good, The Bad, The Ugly

Mario Hoffmann (Continental Teves – Frankfurt-Sossenheim, DE)

Joint work of Mario Hoffmann, Sarah Syed-Winkler

The future of automotive products and mobility services is digital, autonomous, and personalized. Specifically, modern vehicles with dozens of assist systems, sensors and actuators, and autonomous driving capabilities will become a huge data source for a plethora of new individually tailored mobility services by the end of this decade. In this data industry, modern vehicles will become an important cornerstone for complex cross-domain scenarios with other road users, infrastructures, as well as mobile and back-end systems. One promising example are Smart Cities.

According to the "Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications" by the European Data Protection Board [1] these scenarios rely on the so-called Personally Identifiable Information (PII) and, therefore, are subject to special regulations and laws. One of the most prominent regulations is the European General Data Protection Regulation (EU GDPR, enforced May 2018). Here, a set of binding rules has been defined giving clear obligations for realizing – for instance – user consent, transparency, purpose binding, data minimization, data portability, and the right to be forgotten. Meanwhile, several regions around the globe took the EU GDPR as a blueprint for their own regulations.

The technical interpretation and implementation of these regulations in complex mobility scenarios, however, is a huge challenge. While Privacy Enhancing Technologies – such as Sticky Policies, Zero Knowledge Proofs, and Attribute Based Encryption, are well understood in the IT and Internet domain [2], there is still a technological gap in applying these techniques into the automotive domain. On the one hand, specifically, the PII life cycle in modern cars with its more than 100 Electronic Control Units (ECUs) lacks a consistent and interoperable data protection architecture which includes vehicles of different brands, mobile devices, infrastructures and back-end service environments. On the other hand, drivers and passengers, however, would like to be sure that the privacy settings defined in a car are enforced according to the regulation for each participant and stakeholder in any corresponding mobility scenario. Enjoying a particular personalized mobility service does not necessarily mean that the users' PII is free for any further usage.

In the publicly funded project "AUTOPSY – Automotive Data-Tainting for Privacy Assurance Systems", Continental investigates together with Fraunhofer AISEC and an equally small French consortium technical readiness and applicability of Privacy Enhancing Technologies for future automotive products and mobility services. From June 2021 to May 2024 the project will constantly update guidelines and learning material for the automotive domain regarding the impact of data protection regulations, applicable PETs for both embedded as well as end2end automotive architectures, and will demonstrate selected data tainting techniques. Future innovation projects need to investigate step by step more PETs in order to ensure cross-stakeholder inter-operability and policy enforcement as well as tackle all regulatory goals appropriately in order to fill the automotive privacy engineering toolbox.

References

1 European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*. Jan 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

2 ENISA, *Data Protection Engineering*. Jan 2022, https://www.enisa.europa.eu/publications/data-protection-engineering/@@download/fullReport

4 Working groups

4.1 Results of Concluding Discussions

Frank Kargl (Universität Ulm – Ulm, DE)
Ioannis Krontiris (Huawei Technologies – München, DE)
Nataša Trkulja (Universität Ulm – Ulm, DE)
André Weimerskirch (Lear Corporation – Ann Arbor, US)
Ian Williams (University of Michigan – Ann Arbor, US)

The seminar was organized in five 3-hour sessions with remote attendance due to the COVID pandemic. There was an introductory session and a concluding session, and the other time was spent on presentations and discussions around ethical, regulatory, legal, commercial, and technology aspects. The seminar sessions were loosely linked to those four topics with many cross-area considerations and discussions. The following summarizes the main results of the discussions.

4.1.1 Ethics

The ethical aspect considers the trustworthy and responsible use of personal data which is a matter of respect to other people including a company's customers. During discussions in the online seminar, we concluded that data protection regulation will not necessarily create ethical behavior but rather compliance. Compliance requires validation, which also creates cost and overhead. Furthermore, compliance does not rule out unethical behavior, e.g., today many terms of use and license agreements lure users to give their consent against their best interest. This observation led to a number of questions being raised and debated.

The working group discussed that stakeholders, in particular companies, might have an incentive to provide privacy protection that goes beyond minimal compliance and to establish a reputation of trustworthiness. There are examples available from the consumer electronics domain, even though only a few. For instance, the public opinion is that Apple is trustworthy in terms of privacy protection, but it is unclear if and how automotive stakeholders can follow Apple's role model.

It is also unclear what a company's incentive to act in a trustworthy way is and which regulatory steps can foster trustworthiness. Ideas include a regulatory requirement for transparency and demonstration of data protection practices. It is uncertain if a push for more trustworthiness as a concept replaces or extends data protection regulation. A concern raised is that perceived trustworthy behavior of a company might be created by clever marketing without the company providing actual trustworthiness. It is unclear how such practices can be stopped though. It appears this leads to a regulatory requirement for more transparency and for demonstrable privacy practices. At the same time, perceived trust and how technical safeguards to protect privacy are communicated to end-consumers is an important aspect that is built on trustworthiness and ethical behavior instead of strict compliance. We also discussed how this would evolve in a larger international setting. There is a strong overlap with the legal domain discussions presented in the next section.

The next discussion block was around the ethical goals of handling and processing personal data. It is unclear how to provide companies guidance on behaving ethically. We discussed that a reasonable expectation of privacy of a reasonable / average person could be a guiding principle where we would, e.g., ask whether such a person might expect to be unobserved by cameras when driving in an AV taxi.

We also identified that there is a lack of understanding of privacy expectations of people in traffic and mobility and this would require further research. For instance, it is necessary to understand under what circumstances end-consumers are willing to share information voluntarily for the greater or personal good, and what data they are willing to share. Experiences from some research projects show that people are usually willing to share data to contribute to research.

Overall, we think that this is an interesting concept to follow-up on and it would definitely help to explore the alternatives to the apparent trade-off between ever stricter regulation and abundant (ab-)use of personal data in cooperative, connected and automated mobility (CCAM) systems.

4.1.2 Regulation

The regulatory and the legal aspect of privacy are often termed data protection. Automated vehicles (AVs) face a number of legal and regulatory challenges that come from the complex intersection of data privacy law (often new and still developing) with a long-standing system of motor vehicle law and regulation. We discussed how we can ensure *compliance* and how we can encourage anything more than legally required compliance minimums. One train of thought is that heavy fines or significant potential legal liability are the only way to ensure even minimal compliance. An alternative argument is that potential reputational damage or the potential to use privacy protection as a marketing tool could be used to encourage compliance and even encourage privacy protection beyond minimum legal compliance. It is a challenge then for companies to prove compliance and for other stakeholders including end-consumers to check for compliance. Much of this discussion overlapped with a wider discussion on corporate trustworthiness, and what it means to be a "trustworthy" company.

A main question to answer is whether privacy issues around AVs (and connected vehicles) rise to a level that requires automotive-specific privacy laws and regulations, or whether privacy of AVs should be addressed through existing (or proposed) laws, regulation, and policy intended to govern privacy issues across a number of technologies.

The team discussed the effects of regulation on future technology and raised the concern that overly stringent privacy rules may lead manufacturers and developers to avoid new technologies or region-limit their deployments. Another challenge is how we communicate legal and regulatory requirements. In particular, how do we ensure that regulatory requirements are understood by engineers and developers in a way that assists the overall policy goal of a law/regulation, and how can we define threshold values around privacy for the average /

reasonable person, as this would also guide the courts in future disputes? The same holds for the communication with the end-consumers, e.g., how can we communicate a vehicle's level of privacy-friendliness or regulatory compliance to end-consumers similar to the idea of the NCAP 5-star safety rating.

A main challenge for industry are different regional data privacy regulations. For instance, the demands of the GDPR differ from those found in state privacy laws in the US, and from other countries' privacy regimes. Safety regulations also differ between countries and regions, so manufacturers may be more willing to deal with regional differences rather than try and apply standards more broadly. It is unclear if and how this will affect the deployment of AVs.

Finally, AVs could be used as a source of data for law enforcement – even as incidental surveillance (recording street activity as part of their regular activities). This might raise concerns both for industry stakeholders and end-consumers, and it is unclear how the stakeholders can balance privacy protection with cooperating with lawful data requests from law enforcement.

4.1.3 Commercial

The working group pointed out a few automotive specific challenges around privacy and self-driving vehicles that are described in the following. There seems to be a *trade-off between privacy and safety and efficiency* in that more detailed widely available data will enable more and better safety systems. In many applications and scenarios, it is unclear what this trade-off is though. It is also unclear who is supposed to decide about the trade-off. In fact, it is unclear if the automotive industry stakeholders should take the lead here or leave it to lawmakers to define regulation, and then the industry stakeholders only comply with said regulation. There are further trade-offs between privacy and traffic efficiency, pollution, and profits. There are also further trade-offs between physical safety such as emotional protection, pollution protection, etc. The same questions arise for these additional trade-off areas.

There are *commercial limitations* that limit the ability to go beyond the minimum legal requirements. OEMs and suppliers move in a highly regulated and competitive space, which limits flexibility of industry stakeholders. There might be other regulations that need to be considered for conflicts or contradiction in the context of privacy protection, such as right-to-repair law. Finally, it might be unclear who owns the data and hence how access to the data should be organized and controlled.

There are also challenges around the *technical solutions*. It is cumbersome to analyze each use-case/application and then design and implement a custom privacy solution. Maintenance and extensions are also rather cumbersome since each use-case that touches on the existing applications might alter the picture and require additional privacy solutions, and so do advances in privacy research and new attacks. Therefore, it appears there is a need for a framework, comprehensive technical guidance, and/or a standard to design, implement and audit privacy.

Companies might be able to utilize privacy for a *competitive advantage*. There are companies that implement privacy protection beyond legal compliance and that utilize their effort for a competitive advantage. It is unclear whether such an approach would be successful in the automotive sector, especially since the margins in the automotive industry are rather small compared to consumer electronics. Therefore, it is rather unclear whether any automotive stakeholder is willing to take the lead on privacy protection, especially since many tech companies don't appear to approach the topic beyond legal compliance.

4.1.4 Technology

The privacy-enhancing technologies (PETs) can be used to provide fundamental data protection principles to an AV system, e.g., minimizing personal data use, maximizing data security, and empowering individuals. Examples of such PETs include differential privacy, homomorphic encryption, secure multiparty computation, etc. The group particularly discussed the case of differential privacy that guarantees privacy protection in the presence of arbitrary auxiliary information. Differential privacy has been adapted to the context of location-based services to personalize the information provided to a user. In the context of the AV system, we can apply differential privacy to vehicle location data (often termed geo-indistinguishability). Notably, the system can add noise to vehicle location data to obfuscate the actual position of the driver or passengers. We identified two trade-offs:

- AVs count on an unprecedented amount of data to make decisions and usually it is a strict requirement that this data is accurate in order to allow the implementation of safety-critical services. This creates a tension with the fact that data needs to be handled in a secure and privacy preserving manner.
- The cryptography behind PETs can be computationally expensive like, for example, in privacy preserving machine learning. On the other hand, safety critical applications have such strict time constraints that makes it impossible to execute several cryptographic operations within these constraints.

A challenge is how to converge privacy protection with safety, based on the strict requirements of computational efficiency and time constraints. Emerging technologies that we can consider as solutions to overcoming this problem include Multi-access Edge Computing (MEC), which brings processing power near the vehicle to meet ultra-low latency requirements. With the help of MEC, massive computation and storage tasks need not be handled in the vehicle with its limited power and resources. Instead, these functionalities can be offloaded to the MEC which can handle it in a more cost-effective way in real-time. At the same time, 5G as the underlying communication paradigm can guarantee the strict service level agreements (bandwidth, zero latency, etc.).

Facilitating the secure and private collaboration between entities is a complex task, especially in the domain of CCAM that relies on cooperation and communication between vehicles and nodes. In this context, several entities that belong to different trust domains must interact with each other to exchange privacy sensitive data in order to enable safety-critical collaborative services. However, if these interactions are not properly managed, it can be the cause of privacy leaks. Therefore, there is a need to establish a high level of trust into received data and the functions that rely on this data. This in turn requires new trust assessment methods, in order to enable vehicles and nodes to assess the trust level of its neighbouring stations and received data and to take critical driving decisions.

A second challenge is how we can assess dynamic trust relationships and define appropriate trust models for involved entities. In this context the group investigated potential mechanisms. A promising approach is the employment of Trusted Computing and the enactment of remote attestation for producing verifiable claims on system properties and integrity.

Participants

- Ala’a Al-Momani
  Universität Ulm – Ulm, DE
- Ines Ben Jemaa
  IRT SystemX – Palaiseau, FR
- Benedikt Brecht
  Volkswagen AG – Berlin, DE
- Michael Buchholz
  Universität Ulm – Ulm, DE
- Thanassis Giannetsos
  UBITECH Ltd. – Athens, GR
- Adam Henschke
  University of Twente – Enschede, NL
- Mario Hoffmann
  Continental Teves – Frankfurt-Sossenheim, DE
- Frank Kargl
  Universität Ulm – Ulm, DE
- Alexander Kiening
  Denso Automotive – Eching, DE
- Ioannis Krontiris
  Huawei Technologies – München, DE
- Jason Millar
  University of Ottawa – . Ottawa, CA
- Kyriaki Noussia
  University of Reading – Reading, GB
- Christos Papadopoulos
  University of Memphis – Memphis, US
- Jonathan Petit
  Qualcomm – Boxborough, US
- Chrysi Sakellari
  Toyota Motor Europe – Brussels, BE
- Yu Shang
  Huawei Technologies – Shanghai, CN
- Lauren Smith
  Cruise – Washington, US
- Nataša Trkulja
  Universität Ulm – Ulm, DE
- Jessica Uguccioni
  Law Commission of England and Wales – London, GB
- Bryant Walker Smith
  University of South Carolina – Columbia, US
- André Weimerskirch
  Lear Corporation – Ann Arbor, US
- Ian Williams
  University of Michigan – Ann Arbor, US
- Harald Zwingelberg
  ULD SH – Kiel, DE