I am a researcher who studies automotive cybersecurity and privacy. My work is critical in understanding how existing and upcoming connected and autonomous vehicles can be protected against cyber risks. These issues are very important to address because the field of cybersecurity is getting increasingly important with rising cyber attacks against critical infrastructure as seen in recent years. New regulations [1, 7] underline the need to strengthen automotive cybersecurity which will trigger massive investments – increasing from 4.9 billion USD in 2020 to 9.7 billion USD in 2030 [4]. Since I first entered graduate school, my research interests have been continuously expanding. My primary research area is in-vehicle network — specifically CAN bus — security, and it is in this area that I focused most of my effort for my Ph.D. thesis. Towards the end of my Ph.D., however, I started shifting towards novel topics in connected vehicles, such as vehicle-to-vehicle and Android Automotive security.

The overarching goal of my research is to design practical, out-of-the-box solutions to defend against cyber-attacks in vehicles, specifically passenger cars. Thanks to the privilege of working closely with automotive companies in both Germany and the US before and during my Ph.D., I realized at an early stage that academia and industry are disconnected in the area of automotive security. This has lead to a lack of integration of academic advancements into real-world products. The main reason for this lack of adoption can be explained by the non-consideration of industry requirements — primarily cost — which affects functional requirements such as latency or computational capabilities. As a result, state-of-the-art defenses from other domains, such as computer networks, cannot be directly applied to vehicles to achieve security.

Finally, I also pioneered work in the field of vehicle data privacy, both on the offensive and defensive side. This diversified path has afforded me the luxury to not restrict myself to any particular area of automotive security and privacy research. As long as a problem is exciting and I have a reasonable way to attack it, I am willing to work on it.

Thesis Work: Bringing Practical Security to Vehicles

My thesis uniquely analyzes the trade-off between security and performance in passenger vehicles by proposing novel security solutions for CAN and V2V security that are feasible to be deployed in vehicles by car manufacturers. Each solution improves upon existing security countermeasures by drastically reducing the resource and implementation costs in vehicles. My thesis work was motivated by **LibreCAN** [CCS'19]. We demonstrated that the barrier for CAN injection attacks to cause vehicle malfunction can be significantly reduced by automated CAN bus reverse engineering. To mitigate this attack, I proposed **S2-CAN** [ACSAC'21] to bring confidentiality and authenticity to the CAN bus without the use of cryptography. To further mitigate CAN vulnerabilities, I designed **MichiCAN** that can also detect and prevent Denial-of-Service (DoS) attacks in a backwards-compatible and lightweight way. Finally, I applied the security-performance trade-off to V2V-enabled connected vehicles by proposing **CARdea** which is an intrusion detection system.

CAN Bus Security

Vehicles are comprised of numerous Electronic Control Units (ECUs). Data is exchanged between ECUs via an in-vehicle network (IVN), with the Controller Area Network (CAN) bus being the de-facto standard in contemporary vehicles. Since CAN has not been designed with security in mind, most of my Ph.D. thesis deals with enhancing it by the key cyber-security properties of *confidentiality*, *authenticity*, and *availability*. The main threat and key part of every cyber-attack against vehicles to date are CAN injection attacks, which can lead to serious malfunctioning of the vehicle [8, 5, 9]. CAN is also easily susceptible to DoS attacks [10].

LibreCAN [14]: CAN messages are unencrypted and any adversary with access to the CAN bus can sniff the plaintext data. Nevertheless, each make and model encodes the data differently, typically requiring an attacker to interpret data using a translation table (called DBC). Carmakers keep DBCs private in the hopes of hiding it them from attackers. This has failed to prevent attackers from conducting manual reverse engineering of the CAN bus, though this is a tedious and long process. I showed that by exploiting the security-by-obscurity principle of automotive carmakers in an automated fashion, an attacker can quickly and easily launch a CAN injection attack and cause the vehicle to malfunction. For this purpose, I designed an automated CAN message reverse engineering tool called LibreCAN that can reverse engineer most of the DBC in under two minutes with 82.6-95.1% accuracy, much higher than existing works. We have filed a patent application to the USPTO.

S2-CAN [13]: As my work demonstrated, automated CAN reverse engineering accelerates CAN injection attacks on unknown vehicles. Spoofing can be prevented by adding a Message Authentication Code using cryptographic means. However, this comes at the expense of latency and the need for more powerful ECUs. Since hard real-time deadlines and cost requirements make this form of authenticity and integrity protection infeasible, I developed a novel security solution called S2-CAN. It presents a trade-off between security and performance on the CAN bus. S2-CAN adds the security properties of confidentiality, authenticity, and freshness to CAN messages without using cryptography. By modifying

LibreCAN to attack S2-CAN, I show that a secure CAN is possible with minimal overhead on ECU resources and latency. We have filed a provisional patent application to the USPTO.

MichiCAN [in progress]: CAN is also susceptible to DoS attacks which have traditionally been a focus of CAN-based intrusion detection systems (IDSes), both in academia and industry [10, 16]. Licensing costs or the need for a dedicated ECU have held carmakers back from adopting it in their vehicles. Hence, DoS attacks need to be detected with existing ECUs as fast as possible. Some recent work proposed solutions to bus-off the attacking ECU according to CAN protocol specifications with the drawback of introducing a long detection latency or severely increasing the bus load [6]. To mitigate these drawbacks, I proposed a new backwards-compatible approach called MichiCAN to defend against DoS and spoofing attacks by using on-chip CAN controllers which are already widely used in existing ECUs. On-chip CAN controllers allow the ECU to bypass the CAN controller, enabling fast detection of attacks on a bit level.

Connected Vehicle Security

Cars are becoming increasingly connected to support an increasing number of convenience and safety functions. The future of intelligent transportation systems (ITS) will be spearheaded by V2X (vehicle-to-everything) communication which can complement and enhance Advanced Driver-Assistance Systems (ADAS) and autonomous vehicles (AVs).

CARdea [in progress]: Vehicle-to-vehicle (V2V) communication as a complementary source to in-vehicle cameras, radars, and lidars can help connected vehicles improve traffic management, provide driver assistance and prevent possible crashes [3]. On the other hand, compromised vehicles can broadcast malicious information to trick vehicles into collisions or cause traffic congestion. Existing solutions to sanitize incoming V2V data either focus on certain attacks (e.g., GPS spoofing) or rely on computationally-heavy algorithms that are impractical on the restricted resources of existing ECUs. To address this, I designed and implemented a novel intrusion detection system for V2V which detects anomalous broadcasts from malicious or faulty vehicles. My system called CARdea uses a two-phase approach with a statistics-based, light-weight Phase 1 deployed on the vehicle and a machine learning-based, resource-heavy Phase 2 that can be executed on the vehicle, edge, or cloud. The first phase detects anomalous BSMs from vehicles with up to 98% sensitivity in only 0.04ms, whereas the second phase handles certain cases that the first phase cannot detect. The experimental evaluation consists of 132 hours of simulated BSM data in realistic traffic scenarios and multiple attack types. I showed that using a two-stage approach, practicability does not need to be compromised at the expense of detection performance. We have filed a patent application to the USPTO.

Vehicle Data Privacy

Besides my thesis work, I have also pioneered work on automotive privacy during the course of my Ph.D. Vehicle data privacy is a novel field that is receiving more attention due to the rise of telematics as part of increasingly connected vehicles and recent regulations (General Data Protection Regulation in the EU). Large amounts of data are being generated in vehicles which can then be shared with carmakers and third-parties. This is mainly driven by monetization opportunities for carmakers. Sensitive driver/user data must be protected by the carmaker since it could be exploited by malicious third-parties. To show this, I published an attack paper called **SPy** [PETS'20] and am currently working on a holistic defense framework for the connected vehicle ecosystem called **PRICAR**.

SPy [12]: To show the privacy threat of vehicular data, I conducted a survey to assess the likelihood of users to share certain sensor data with carmakers and third-parties. Then, I showed how to compromise drivers' location privacy by inferring a vehicle's location from seemingly benign steering wheel angle (SWA) traces. By collecting and processing real-life SWA traces, I demonstrated that users' exact traveled routes can be inferred with up to 71% accuracy, which is higher than the state-of-the-art and makes no assumptions about the starting point of their trip.

PRICAR [in progress]: To defend against privacy attacks, I developed a reference architecture called PRICAR for privacy-preserving vehicular data collection and sharing with third-party entities. It enforces the three privacy goals of data minimization, anonymization, and sanitization. Instead of sending sensor data to the third-party directly, I show how to anonymize and sanitize user data using a neutral server (e.g., Amazon AWS, Google Cloud) first. For data sanitization, I adapted two techniques, namely Change-Point Detection (CPD) and Entropy-Based Detection (EBD). The evaluation with real vehicular sensor data and third-party apps shows that both techniques can detect inferred data (e.g., the location from SWA) which will be denied from being shared with the malicious third-party. We have been granted a patent by the USPTO [15]. I have written the accepted Ford-UM Alliance grant for this project together with my Ph.D. advisor.

Future Research Agenda

Threats to vehicles and its ecosystem will continue to present unique challenges in the future, mainly due to novel technologies in this area still being in their infancy. In my future endeavor, I plan to shift my focus from the well-researched area of CAN security to connected and autonomous vehicles, with some work being already undertaken during my Ph.D. I would like to leverage my industry connections and collaborations to the fullest extent in my future research endeavor. I am already no stranger to writing industry grant proposals, having successfully co-authored one accepted proposal with my Ph.D. advisor.

Connected Vehicle Ecosystem

New wireless interfaces are emerging in contemporary vehicle ecosystems. One example are novel infotainment operating systems, such as Android Automotive (a car-specific version of the popular mobile operating system Android) [2]. It can collect sensor data directly from the vehicle and share it with the carmaker and interested third-parties. I conducted the first high-level security analysis of Android Automotive in 2020 [11]. Due to the integration of Android Automotive with the IVN, it must have a secure system architecture to prevent any potential attacks that might compromise the security and privacy of vehicles and drivers. In particular, malicious third-party apps could remotely compromise a vehicle's functionalities to impact vehicle safety and the driver's privacy. During my stint at CISPA in 2021, my collaborators and I started analyzing privacy trackers included by Google Automotive Services on production builds. Since both Google and carmakers are interested in monetizing user data from vehicles, we want to determine what data is shared for what purpose. We have started conducting a privacy analysis on vehicle models that have already introduced Android Automotive.

Besides continuing this work, I would like to research the possibility of malicious third-party apps writing to the IVN. This vulnerable interface will open the doors to a new generation of increasingly scalable cyber-attacks against vehicles, eliminating the need to be physically near a target vehicle. Unfortunately, the Android Automotive source code is constantly changing and IVN integration into the automotive stack has not been completed yet. Furthermore, Google only allows limited categories of third-party apps (e.g., media, charging). Once Google opens up more APIs for third-party apps that can access various vehicle data, I plan to conduct an in-depth analysis of Play Store apps that violate drivers' privacy by collecting sensitive user data. Another example of novel interfaces for the connected vehicle ecosystem are widely available mobile companion apps (e.g., BMW Connected) to remotely start or even *steer* the vehicle, further increasing the interconnection of carmakers' infrastructure with their cars. Vulnerabilities in this ecosystem can seriously impact safety. So far, research has been very sparse in this field. I propose to study carmakers' connected infrastructure to understand the novel threat model. This will help me to analyze existing commercial solutions and design countermeasures to protect against attacks in the future.

Adversarial Attacks on Autonomous Vehicles

In recent years, many deep learning models have been adopted in autonomous perception systems. Security vulnerabilities are an ever-present concern to drivers' safety and manufacturers' liability. Recently, it has been shown that the underlying perception systems exhibit severe vulnerabilities when exposed to adversarial conditions. Among others, attacks can be classified by the vehicular sensor they target (i.e., cameras, lidars) to the type of adversarial knowledge (i.e., white-box vs black-box). While some attacks have been demonstrated in research settings, the extent to which deployed autonomous vehicles (AVs) are susceptible to physical world attacks is still not fully understood. To address this challenge, I plan to investigate the vulnerability of deployed AV perception systems under novel physical world attacks and propose defenses for these trending and pressing security issues.

References

[1] Un regulations on cybersecurity and software updates to pave the way for mass roll out of connected vehicles. https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll, Jun 2020.

[2] Android automotive. https://en.wikipedia.org/wiki/Android_Automotive#Vehicles_with_Android_Automotive, Oct 2021.

[3] Automated vehicles for safety. https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety, Nov 2021.

[4] Cybersecurity in automotive: Mastering the challenge. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/cybersecurity-in-automotive-mastering-the-challenge, Jan 2021.

[5] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, volume 4, page 2021. San Francisco, 2011.

[6] Tsvika Dagan and Avishai Wool. Parrot, a software-only anti-spoofing defense system for the can bus. *ESCAR EUROPE*, page 34, 2016.

[7] Road vehicles — Cybersecurity engineering. Standard, International Organization for Standardization, Geneva, CH, August 2021.

[8] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy*, pages 447–462. IEEE, 2010.

[9] Charlie Miller and Chris Valasek. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, 2015(S 91), 2015.

[10] Shuji Ohira, Araya Kibrom Desta, Ismail Arai, Hiroyuki Inoue, and Kazutoshi Fujikawa. Normal and malicious sliding windows similarity analysis method for fast and accurate ids against dos attacks on in-vehicle networks. *IEEE Access*, 8:42422–42435, 2020.

[11] Mert Pese, Kang Shin, Josiah Bruner, and Amy Chu. Security analysis of android automotive. *SAE International Journal of Advances and Current Practices in Mobility*, 2(2020-01-1295):2337–2346, 2020.

[12] Mert D Pesé, Xiaoying Pu, and Kang G Shin. Spy: Car steering reveals your trip route! *Proc. Priv. Enhancing Technol.*, 2020(2):155–174, 2020.

[13] Mert D Pesé, Jay W Schauer, Junhui Li, and Kang G Shin. S2-can: Sufficiently secure controller area network. *Annual Computer Security Applications Conference (ACSAC'21)*, 2021.

[14] Mert D Pesé, Troy Stacer, C Andrés Campos, Eric Newberry, Dongyao Chen, and Kang G Shin. Librecan: Automated can message translator. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 2283–2300, 2019.

[15] Mert Dieter Pesé, Evripidis Paraskevas, Fan Bai, Massimo Osella, and Soheil Samii. Systems and methods for preserving the privacy of collected vehicular data, June 4 2020. US Patent App. 16/180,767.

[16] Stephen Stachowski, Ron Gaynier, David J LeBlanc, et al. An assessment method for automotive intrusion detection system performance. Technical report, United States. Department of Transportation. National Highway Traffic Safety . . . , 2019.