# Lista de lucrări

[1] Roman, A. S., Bolboacă, R., **Lenard, T.**, & Haller, P. (2025). APU-TrajGen+: GRU-based Adaptive Privacy and Utility Preserving Trajectory Generation. *IEEE Access*.

**Abstract:** Location-Based Service (LBS) are increasingly integrated into our daily life, to offer smart services and applications. However, ensuring user privacy while maintaining data utility remains a critical challenge. Trajectory data, vital for urban planning, mobility analytics or, is particularly sensitive to re-identification even when explicit identifiers are removed. This article introduces APU-TrajGen+, a novel method for real-time, privacy-preserving point-to-point trajectory generation. APU-TrajGen+ leverages a Gated Recurrent Unit-based model to synthesize trajectory points, followed by an adaptive perturbation mechanism that dynamically balances privacy and utility. Designed for local execution, APU-TrajGen+ protects location data at the device level, eliminating the need for centralized processing and preventing unprotected data transmission. Unlike many existing methods, APU-TrajGen+ does not rely on map data or points of interest to generate points in plausible locations. A configurable utility-privacy score guides an adaptive process, to allow data owners to set the protection levels to their specific needs. Experimental results show that APU-TrajGen+ produces realistic trajectories while achieving desired privacy and utility objectives. The method is particularly suitable for LBS and TMS scenarios that require continuous, point-to-point data release, supporting both high utility and strong privacy guarantees without compromising real-time performance.

[2] Cighir, A., Bolboacă, R., & **Lenard, T**. (2025). OpenFungi: A Machine Learning Dataset for Fungal Image Recognition Tasks. *Life*, *15*(7), 1132.

**Abstract:** A key aspect driving advancements in machine learning applications in medicine is the availability of publicly accessible datasets. Evidently, there are studies conducted in the past with promising results, but they are not reproducible due to the fact that the data used are closed or proprietary or the authors were not able to publish them. The current study aims to narrow this gap for researchers who focus on image recognition tasks in microbiology, specifically in fungal identification and classification. An open database named OpenFungi is made available in this work; it contains high-quality images of macroscopic and microscopic fungal genera. The fungal cultures were grown from food products such as green leaf spices and cereals. The quality of the dataset is demonstrated by solving a classification problem with a simple convolutional neural network. A thorough experimental analysis was conducted, where six performance metrics were measured in three distinct validation scenarios. The results obtained demonstrate that in the fungal species classification task, the model achieved an overall accuracy of 99.79%, a true-positive rate of 99.55%, a true-negative rate of 99.96%, and an F1 score of 99.63% on the macroscopic dataset. On the microscopic dataset, the model reached a 97.82% accuracy, a 94.89% true-positive rate, a 99.19% true-negative rate, and a 95.20% F1 score. The results also reveal that the model maintains promising performance even when trained on smaller datasets, highlighting its robustness and generalization capabilities.

[3] Benyahya, M., Collen, A., **Lenard, T.**, & Nijdam, N. A. (2025). TARA 2.0 for Connected and Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems*.

**Abstract:** Connected Automated Vehicles (CAVs) represent a transformative shift in transportation, offering enhanced safety, and efficiency. However, achieving full automation at levels four and five of the Society of Automotive Engineering (SAE) scale poses significant cybersecurity and privacy risks. To address these risks, United Nations Economic Commission for Europe (UNECE) regulations and ISO/SAE 21434 mandate Threat Analysis and Risk Assessment (TARA) as a core methodology for cyber risk management. Existing TARA frameworks, designed for conventional vehicles, fall short for higher automation levels, neglecting complexities such as the absence of human control and data-driven decision making concerns. This work, conducted within ULTIMO, a project tackling the CAVs deployment challenges, introduces TARA 2.0, an enhanced framework addressing cybersecurity, privacy, and expert subjectivity in risk assessment. A step-by-step experimental implementation demonstrates its feasibility, compliance with standards, and potential to secure the deployment of fully automated vehicles.

[4] **Lenard, T.**, Collen, A., & Nijdam, N. A. (2024, October). Using the Trusted Platform Module to Generate Secure Logs for Automotive Systems. In *2024 IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP)* (pp. 1-6). IEEE.

**Abstract:** Modern automotive systems are starting to incorporate complex functional software features. With an increase in system complexity comes different requirements for security. In this paper, we propose a design for secure logging that uses the functionalities of an automotive Trusted Platform Module. Our logging solution guarantees log integrity, authenticity, non-repudiation and tamper-proofness, while assuming a threat actor that has physical access to the storage medium of the protected logs. An experimental performance assessment was conducted to measure the performance of the Trusted Platform Module functions used in logging with different cryptographic and hashing algorithms.

[5] **Lenard, T.**, Genge, B., Collen, A., & Nijdam, N. A. (2023, October). LOKI-2: An Improved Lightweight Cryptographic Key Distribution Protocol for Automotive Systems. In *2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)* (pp. 187-194). IEEE.

**Abstract**: The Lightweight Cryptographic Key Distribution Protocol (LOKI) was initially proposed as a solution that enables computationally restricted automotive control units to periodically update short-term authentication keys. After analysing the protocol messaging from a security and a formal point of view, we found that the protocol lacks critical security properties. The work at hand introduces an improved protocol version that intents to address the initial design flaws. Moreover, a formal automated verification was conducted on both protocols, first to demonstrate the shortcomings of LOKI, and secondly, the correctness of the improved variant. Finally, the improved protocol is formally verified with a Burrows-Abadi-Needham (BAN) logic analysis.

[6] **Lenard, T.** (2023, October). A Tale of Two Automotive Security Services: A Formal Analysis. In *International Conference Interdisciplinarity in Engineering* (pp. 441-458). Cham: Springer Nature Switzerland.

**Abstract**: Automotive system faced in the past decade an abundance of security services proposed by the scientific literature to strengthen their system security. The solutions solve problems in terms of key distribution, data authentication, or system monitoring. While the volume of research done brings in consequence novel ideas, strong validation and extensive experimentation is a must to prove their viability and correctness. Consequently, the work at hand offers a formal analysis of two existing security services for automotive systems, namely for a Key Distribution Service (KDS) and for a data authentication and aggregation method titled Mixed data authentication for Controller Area Network (MixCAN). While the KDS aims to distribute long-term and short-term cryptographic keys, MixCAN envisions a lightweight authentication protocol through Encrypted Bloom Filters (EBFs). The objective of the formal analysis is to prove the correctness of the mentioned security solutions through a Burrows-Abadi-Needham (BAN) logic analysis.

[7] **Lenard, T.**, Collen, A., Benyahya, M., Nijdam, N. A., & Genge, B. (2023). Exploring Trust Modelling and Management Techniques in the Context of Distributed Wireless Networks: A Literature Review. *IEEE Access*.

**Abstract**: Trust Modelling and Management (TMM) techniques are frequently applied in ad-hoc Distributed Wireless Networks (DWNs) to stimulate and improve cooperation between network nodes. TMM facilitate DWNs in building a trust network that assures reliability of communication channels, offers an additional layer of security, and enables group decision making processes. Likewise, TMM became in the past decades an attractive solution for solving problems in cooperative ad hoc DWN. The proposed solutions focus on modelling trust in a social-centric approach to maintain a system where nodes trust each other, and detect untrustworthy (malicious) neighbours. The work at hand considers a time span of three years, from 2020 to 2022, where the scientific research in the domain of TMM and DWN is analysed. Our survey aggregates over 130 research papers and investigates the quality of experimental assessment done by each work. Additionally, we establish an indication on the level of experimental analysis done by each study from a TMM security perspective. Lastly, the survey offers a trust ontology, a general overview of a trust models, together with a concise description of trust threats to facilitate the reader's understanding of TMM.

[8] Benyahya, M., **Lenard, T.**, Collen, A., & Nijdam, N. A. (2023, August). A Systematic Review of Threat Analysis and Risk Assessment Methodologies for Connected and Automated Vehicles. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-10).

**Abstract**: With the prevalence of high cyber risks within the Connected Automated Vehicle (CAV)'s environment, the core regulation bodies mandated applying Threat Analysis and Risk Assessment (TARA) methodologies. Conducting auspicious TARA is essential to ensure acceptable level of risk by analysing potential threats and determining corresponding mitigation strategies. Albeit plethora of standardised TARA versions are available, they are not-ready-to-use methods or they do not encapsulate heterogeneous CAVs properties. By considering the TARA emerging trends and the CAVs' SAE automation levels, the present work provides a systematic study of salient TARA methodologies in the last ten years. The methodology we applied starts with a systematic review identifying TARA approaches that are relevant to the automotive domain at a large scope. After that, the methods' applicability to CAVs is evaluated based on their threat analysis avenues and risk metrics. We elevate our appraisal further with a focus on how the automation level is considered, how the privacy impact is assessed by each TARA method, and how subjective the

experts were while assessing scores to the risk metrics. Our investigation spotlights how different methods are intertwined and joint to meet the compliance with key standards such as ISO/SAE 21434. We believe that the present study's findings identify knowledge gaps and help to shape the next generation of TARA methods to keep pace with rapidly evolving automotive technologies and support the readiness of CAV of SAE levels four and five.

[9] **Lenard, T.**, Collen, A., Nijdam, N. A., & Genge, B. (2023, July). A Key to Embedded System Security: Locking and Unlocking Secrets with a Trusted Platform Module. In 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 329-335). IEEE.

**Abstract:** Security hardware modules were designed to provide a viable solution that can empower Embedded Systems (ES) with state-of-the-art cryptographic and security capabilities. They can execute cryptographic operations, securely store sensitive information, or provide measurements for attestation. A key element in designing and implementing security solutions on top of a security hardware, such as the Trusted Platform Module (TPM), is secure secret storage. The work at hand addresses the problem of secret protection by showcasing how the TPM standard can serve as a vault in protecting sensitive information in ES. This is accomplished as follows. Secrets are locked in the TPM according to Platform Configuration Register (PCR) policies created on top of the system state and sealing. In contrast, unlocking is achieved through TPM unsealing. In both cases, secure and authenticated sessions are enforced while communicating with the TPM. Furthermore, our work goes a step further and presents a simple TPM attestation protocol, destined to verify the system state and TPM application. Lastly, a series of experiments were conducted on a reference hardware, with two different TPM configurations, to measure execution times of TPM operations.

[10] **Lenard, T.**, Genge, B., Haller, P., Collen, A., & Nijdam, N. A. (2023). An automotive reference testbed with trusted security services. *Electronics*, *12*(4), 888.

**Abstract**: While research in the field of automotive systems inclined in the past years towards technologies such as Vehicle-to-Everything (V2X) or Connected and Automated Vehicle (CAV), the underlying system security still plays a crucial role in assuring trust and system safety. The work at hand tackles the issue of automotive system security by designing a multi-service security system specially tailored for in-vehicle networks. The proposed trusted security services leverage Trusted Platform Module (TPM) to store secrets and manage and exchange cryptographic keys. To showcase how security services can be implemented in a in-vehicle network, a Reference TestBed (RTB) was developed. In the RTB, encryption and authentication keys are periodically exchanged, data is sent authenticated, the network is monitored by a Stateful Firewall and Intrusion Detection System (SF/IDS), and security events are logged and reported. A formal individual and multi-protocol analysis was conducted to demonstrated the feasibility of the proposed services from a theoretical point of view. Two distinct scenarios were considered to present the workflow and interaction between the proposed services. Lastly, performance measurements on the reference hardware are provided.

[11] **Lenard, T.**, & Bolboaca, R. (2021, November). A statefull firewall and intrusion detection system enforced with secure logging for controller area network. In *Proceedings of the 2021 European Interdisciplinary Cybersecurity Conference* (pp. 39-45).

**Abstract**: The Controller Area Network standard represents one of the most commonly used communication protocol present in today's vehicles. While it's main properties facilitate the communication between different control units, several protocol design considerations represent security problems. While it's trivial for an attacker to gain access and control the system, solutions capable of mitigating such

incidents lack from a vehicle's network. The current work proposes a Statefull Firewall, together with a signature based Intrusion Detection System as a response. Beside this, a Secure Logging unit is brought up in addition to support our methods, enforcing them with integrity verifiable logs.

[12] **Lenard, T.**, Bolboacă, R., & Genge, B. (2020, September). LOKI: A lightweight cryptographic key distribution protocol for controller area networks. In *2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)* (pp. 513-519). IEEE.

**Abstract**: The recent advancement in the automotive sector has led to a technological explosion. As a result, the modern car provides a wide range of features supported by state of the art hardware and software. Unfortunately, while this is the case of most major components, in the same vehicle we find dozens of sensors and sub-systems built over legacy hardware and software with limited computational capabilities. This paper presents LOKI, a lightweight cryptographic key distribution scheme applicable in the case of the classical invehicle communication systems. The LOKI protocol stands out compared to already proposed protocols in the literature due to its ability to use only a single broadcast message to initiate the generation of a new cryptographic key across a group of nodes. It's lightweight key derivation algorithm takes advantage of a reverse hash chain traversal algorithm to generate fresh session keys. Experimental results consisting of a laboratory-scale system based on Vector Informatik's CANoe simulation environment demonstrate the effectiveness of the developed methodology and its seamless impact manifested on the network.

[13] Bolboacă, R., **Lenard, T.**, Genge, B., & Haller, P. (2020, August). Locality sensitive hashing for tampering detection in automotive systems. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-7).

**Abstract**: In modern auto vehicles we find dozens of Electronic Control Units (ECUs) running several hundred MBs of code, alongside sophisticated dashboards with integrated wireless communications. While this technological advancement has brought upon a wide range of advantages and integrated features, it also exposed the modern vehicle to significant cyber threats, as documented in prior works. Unfortunately, besides traditional cyber attacks, the security and normal operation of the modern vehicle are nowadays exposed to a different kind of threat. This is the tampering, which denotes a procedure that alters the vehicle's behavior in order to gain particular advantages (e.g., financial, operational). A fundamental distinction between tampering and cyber attacks, is that tampering occurs with the owner's consent. This paper presents an approach for detecting tampering within modern vehicles by leveraging the advantages of sensitive hashing, namely the Exact Euclidean Locality Sensitive Hashing (E2LSH) method. Experimental results based on a dataset collected from the On-Board Diagnostics port (OBD) of a Kia SOUL vehicle demonstrate the practical applicability of the developed methodology.

[14] **Lenard, T.**, Bolboacă, R., Genge, B., & Haller, P. (2020, June). MixCAN: Mixed and backward-compatible data authentication scheme for controller area networks. In *2020 IFIP Networking Conference (Networking)* (pp. 395-403). IEEE.

**Abstract**: The massive proliferation of state of the art interfaces into the automotive sector has triggered a revolution in terms of the technological ecosystem that is found in today's modern car. Accordingly, on the one hand, we find dozens of Electronic Control Units (ECUs) running several hundred MB of code, and more and more sophisticated dashboards with integrated wireless communications. On the other hand, in the same vehicle we find the underlying communication infrastructure struggling to keep up with the pace of these radical changes. This paper presents MixCAN (MIXed data authentication for Control Area Networks), an approach for mixing different message signatures (i.e., authentication tags) in order to reduce

the overhead of Controller Area Network (CAN) communications. MixCAN leverages the attributes of Bloom Filters in order to ensure that an ECU can sign messages with different CAN identifiers (i.e., mix different message signatures),and that other ECUs can verify the signature for a subset of monitored CAN identifiers. Extensive experimental results based on Vectors Informatik's CANoe/CANalyzer simulation environment and the data set provided by Hacking and Countermeasure Research Lab (HCRL) confirm the validity and applicability of the developed approach. Subsequent experiments including a test bed consisting of Raspberry Pi 3 Model B+ systems equipped with CAN communication modules demonstrate the practical integration of MixCAN in real automotive systems.