SPICe Chronicles 2025: The Year with Hot Papers, a Spicy New Lecture and a Sizzling Round of Applause

Martin Henze[1], Stefan Lenz, Sotiris Michaelides, Gabriel Roson da Silva[2]
Security and Privacy in Industrial Cooperation, RWTH Aachen University, Germany

With the year coming to a close, we reflect on the past twelve months and start a new tradition of an annual report on research, teaching, life, the universe, and everything surrounding the Security and Privacy in Industrial Cooperation (SPICe) group at RWTH Aachen University.

While 2024 was characterized by change, especially concerning the composition of the team and our move to temporary offices while the computer science building gets partly renovated, this year focused on consolidation and embarking on new endeavors spanning across research, teaching, and our team.

Most notably, on the research side, we again managed to land a paper at USENIX Security 2025 this year and were successful in positioning our research at further high-ranked venues (including IEEE EuroS&P and ACM WiSec). On the teaching side, we bootstrapped a new lecture on Industrial Data Security and kicked-off a project to enhance our lecture on Industrial Network Security with hands-on security training. Strategically growing our team, we are happy to welcome Gabriel from the German Aerospace Center (DLR) as an external PhD candidate to the team.

Looking back proudly at the past year ourselves, we were honored by various forms of external recognition of our dedication to research and teaching. Besides nominations for the best paper and teaching awards, we are especially proud that the contributions of our students were recognized through multiple awards.

We report on these and many more notable events, including a timeline of the year at SPICe, an overview of the projects that kept us busy, a brief summary of the scientific publications documenting our research output, a revisit of our teaching activities, as well as the composition of our team. Wrapping up, we provide an outlook for exciting new endeavors for next year.

[1]also with Fraunhofer FKIE
[2]also with German Aerospace Center (DLR)

THE YEAR AT SPICe

January

The year started off on a high note: After a crunch to put together a strong revision over the Christmas break, our paper on generalizable and comprehensible industrial intrusion detection (see Page 4) got accepted at USENIX Security 2025, an A* security conference.

February

We are super proud that our student Laurenz received the runner-up ICT Young Researcher Award, which is a well-earned recognition of his contributions to research on reliable and secure large-scale distributed systems. In addition, we celebrated that our paper on multicast source authentication for CAN bus communication (see Page 4) was accepted at IEEE EuroS&P 2025.

Laurenz at the ICT Young Researcher Award ceremony

March

Ending the time of having to look at empty offices around us, we were extremely happy to welcome our new neighbors from the Combinatorial Optimization Group who moved into the offices next to our (temporary) offices. Furthermore, the final presentations of our seminar on IoT security nicely wrapped-up our teaching activities in the winter semester.

April

We kicked off two exciting new teaching activities: First, with funding provided for the RealistICS project (see Page 3), we started working on integrating hands-on

security training into our lecture on Industrial Network Security. Second, we started to offer a new lecture on Industrial Data Security (see Page 4) to fully represent our research activities in teaching. On the research side, we were extremely happy to learn that our paper assessing the latency of network layer security in 5G networks (see Page 3) was accepted at ACM WiSec.

May

As usual, in May we welcomed a research intern from abroad within RWTH's UROP International program. Over the summer, Leslie worked on realizing a secure, low-power, long-range LoRa-based IoT sensor network. Unfortunately, we learned that the follow-up proposal for the Cluster of Excellence Internet of Production was not selected for funding, prompting us to explore other means of continuing our fruitful collaborations in the context of securing digitized production.

June

One of our highlights of the year is the graduation ceremony of the Department of Computer Science. This year, we not only celebrated the graduation of Fidelius, Jonas, Olav, and Zehra, but were also thrilled to learn that Martin was shortlisted (top 3) for the teaching award of the Department of Computer Science for our lecture on Industrial Network Security.

July

Before leaving for the summer break, we had the opportunity to network and present our research at two prominent international security conferences. At ACM WiSec in Arlington, VA, we presented our research on assessing the latency of network layer security in 5G networks. In beautiful Venice, we shared our findings on multicast source authentication for CAN bus communication and automated security testing of industrial 5G devices at IEEE EuroS&P.

August

Besides enjoying the summer break, we welcomed Gabriel to our team who strengthens our research on sensor network security, particularly for energy-constrained devices, as an external PhD candidate. His research at the Institute for the Protection of Terrestrial Infrastructures of the German Aerospace Center (DLR) nicely complements our interests and activities.

September

September marked the successful end of our project on cyber security for flexible and interconnected industry (see right). Together with our project partners (Fraunhofer IPT, UNIBERG GmbH) we demonstrated an end-to-end pipeline to validate the security of 5G-enabled industrial devices. To spend some time as a team outside the office, we went to the Aachen Forest and competed in the first SPICe minigolf tournament (1st: Jonathan, 2nd: Martin, 3rd: Zehra) before spending a nice and cozy evening at a barbecue hut.

Inaugural SPICe minigolf tournament

October

Together with the rest of the Department of Computer Science, we embarked on the exciting journey to found the new Faculty of Computer Science. At IEEE LCN 2025, we not only presented two papers on our research and networked with our international colleagues, but were pleasantly surprised to learn that our paper on bi-directional TLS handshake caching was named as a Best Paper Award Candidate.

November

This year, November meant crunch time with four papers submitted within seven days. Continuing a nice tradition started last year, we went to the student Christmas market organized by RWTH Aachen University's student union and celebrated the conclusion of the year over some cups of tasty Glühwein.

December

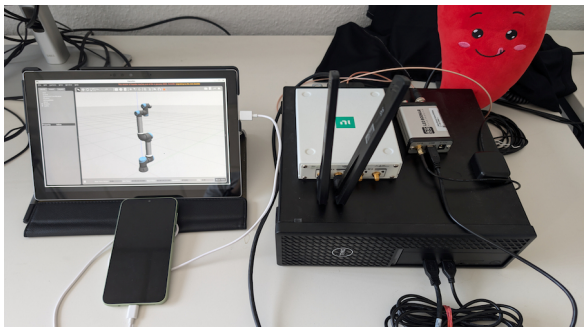
Also ending the year on a high note, Fidelius and Laurenz were selected for the final round of the 25th CAST IT Security Award for outstanding theses in the area of IT security and privacy. They were recognized as the 3rd-best Bachelor's thesis and 4th-best Master's thesis, respectively, in the field of IT security and privacy in Germany during the period 2024/2025.

PROJECTS

CSII (until 09/25)

CSII pursued the goal to establish a certification scheme for 5G-enabled industrial networks based on existing standards. To achieve this, the consortium has developed a comprehensive set of tests designed to uncover vulnerabilities across multiple layers, including the operating system, the 5G stack, and industrial applications. Within this effort, our work focused on developing a testing framework that ensures the secure

transmission of industrial data over 5G infrastructure while also accounting for strict industrial low-latency requirements [1], [2]. Furthermore, to ensure smooth and uninterrupted network operation, our efforts also target the security of the 5G control plane.



Testing infrastructure used in the CSII project

Internet of Production

The Cluster of Excellence Internet of Production strives to integrate the major domains of a producing company along the complete lifecycle of a product, i.e., production, development, and usage. To this end, the collaborative and interdisciplinary research efforts across 35+ research groups targets a new level of cross-domain collaboration by providing semantically adequate and context-aware data from production, development, and usage in real-time, on an adequate level of granularity. Within this context, we contribute our expertise to realize industrial cooperation in a secure and privacy-preserving manner, e.g., in the context of resource-efficient secure industrial communication [3], [4] or intrusion detection in industrial networks [5], [6].

MissionXconnect

The MissionXconnect project is exploring the use of mission-critical broadband applications within a heterogeneous network structure (TETRA, 5G mobile communication, and Wi-Fi) by public safety organizations and critical infrastructure, specifically focussing on the interoperability of services, interfaces, standards, and radio technologies. Within this overarching context, we are evaluating the applicability of end-to-end security for use in such network scenarios and strive to identify optimization potential to account for prevalent bandwidth and latency constraints [4].

RealistICS (since 04/25)

With RealistICS, we aim to provide students the opportunity to apply their theoretical knowledge on industrial network security in a practical and realistic manner. To achieve this goal, we are developing a learning environment in which students can directly apply the theoretical concepts they have learned in our lecture on industrial network security throughout the semester. In order to achieve a high degree of realism and thus high student motivation, we will realize a simulation environment for industrial networks specifically for use in teaching and develop corresponding practical tasks for the continuous development and security of the simulated industrial network [6].

PUBLICATIONS

Secure Integration of 5G in Industrial Networks: State of the Art, Challenges and Opportunities [3]

5G is being increasingly adopted in industrial environments thanks to its ability to meet stringent requirements for ultra-low latency and high reliability, while simultaneously delivering the benefits of wireless technologies such as reduced costs and mobility. To ensure that this shift does not introduce new security risks, our paper, published in Future Generation Computer Systems, examines how 5G can be securely integrated into industrial deployments. The work provides practical and actionable guidance for industrial operators seeking to adopt 5G without compromising security.

Simulation of Multi-Stage Attack and Defense Mechanisms in Smart Grids [7]

Machine learning-based intrusion detection systems are a vital asset for power grid security, but their effectiveness is hindered by the lack of high-quality training data. To alleviate this issue, our paper published in the International Journal of Critical Infrastructure Protection introduces a simulation environment that enables the simulation of complex, multi-stage cyber attacks to generate a diverse set of realistic attack data that can be used to train machine learning algorithms for detecting cyber attacks against power grids.

Assessing the Latency of Network Layer Security in 5G Networks [2]

5G provides a set of security controls to protect data across the network, but their use is left to the operator's discretion. Enabling these controls introduces cryptographic overhead that can affect latency. Our paper—published at ACM WiSec 2025—investigates the performance impact of IPsec, the primary tunneling protocol defined by 3GPP for 5G, and compares it with WireGuard and TLS. By deploying and utilizing a 5G testbed[3] that implements these controls, we show that when properly configured, IPsec adds only 55 µs of

[3] Open source testbed available at https://github.com/RWTH-SPICe/5G-Network-Layer-Security

overhead on the user plane and less than 1 ms on the control plane, outperforming its alternatives.

CAIBA: Multicast Source Authentication for CAN Through Reactive Bit Flipping [8]

To protect safety-critical in-car communication, multicast source authentication promises to reliably identify senders of messages. Turning this promise into practice, our IEEE EuroS&P 2025 paper introduces CAIBA[4], a multicast source authentication scheme specifically designed for communication buses such as CAN. CAIBA protects receivers using the AUTOSAR SecOC standard against masquerading attacks without introducing communication overhead or verification delays and achieves interoperability with legacy devices.

Towards an Automated Security Testing Framework for Industrial UEs [1]

UEs in industrial 5G networks can come from different manufacturers and may have varying baseband implementations. For this reason, our poster at IEEE EuroS&P 2025 presented a framework[5] for testing industrial UEs before network integration. The framework focuses on evaluating higher-layer security mechanisms such as TLS, for industrial data, while testing control plane security as defined by the 5G specification.

GeCos Replacing Experts: Generalizable and Comprehensible Industrial Intrusion Detection [5]

To bridge the gap between striving for a fully automated intrusion detection system in industrial networks and highly-reliable expert systems relying on detailed system knowledge, our USENIX Security 2025 paper presents GeCo[6]. GeCo automatically derives comprehensible models of benign system behavior by creating state-space models based on historical process data. An evaluation on state-of-the-art datasets shows superior detecting performance compared to competing approaches, while still performing on par with manually crafted rules by system experts.

CoFacS – Simulating a Complete Factory to Study the Security of Interconnected Production [6]

To enable research, testing, and validation of security measures protecting industrial networks such cyber-attacks, we present CoFacS[7], a factory simulation that replicates an entire production line and affords the integration of real-life industrial applications. Validating its accuracy, we compare the behavior of CoFacS against a physical model factory widely used in security research. We demonstrate its ability to spur security research alongside two use cases in the area of attack detection and resilience of 5G communication.

Bidirectional TLS Handshake Caching for Constrained Industrial IoT Scenarios [4]

To address prevalent resource constraints of devices and networks in industrial IoT scenarios, our work presented at IEEE LCN 2025 strives to reduce the substantial bandwidth and processing overhead of the TLS handshake. We present BiTHaC[8] to realize bidirectional caching of static parts of the TLS handshake and thus prevent unnecessary transmissions and computations during the TLS handshake. Concretely, we can reduce the bandwidth consumption by up to 61.1% and the computational overhead by up to 8.5%, still preserving the strict security guarantees of TLS. We were thrilled to learn that our paper was nominated as a Best Paper Award Candidate at the conference.

TEACHING

New Lecture: Industrial Data Security

Complementing our lecture on Industrial Network Security, we created a new lecture on Industrial Data Security, providing students with an introduction into current security problems surrounding industrial data and state-of-the-art security solutions. After an introduction into industrial data—its storage, processing, and the security challenges it faces—students learn about approaches to secure industrial data across files, databases, and machine learning. Topics include encryption and integrity-protection of structured industrial data in files, database security in industrial contexts, as well as machine learning security for industrial data. Across all topics, a special emphasis is put on the privacy-preserving processing of industrial data.

Theses

During the course of this year, 8 Bachelor's theses and 6 Master's theses were submitted, covering a wide range of topics spanning from dataset and testbeds over 5G and power grid security to transport layer security and intrusion detection.

[4] Open source implementation available at https://github.com/fkie-cad/caiba

[5] Open source tool available at https://github.com/RWTH-SPICe/Industrial-UE-Security-Framework

[6] Open source implementation available as part of the IPAL framework at https://github.com/fkie-cad/ipal_ids_framework/tree/master/ids/geco

[7] Open source implementation available at https://github.com/RWTH-SPICe/CoFacS

[8] Open source implementation available at https://github.com/RWTH-SPICe/BiTHaC

TEAM

The SPICe group at the Christmas market

Scientific Staff

- Prof. Dr. Martin Henze
  Head of Group
- Stefan Lenz
  Researcher
- Sotiris Michaelides
  Researcher
- Gabriel Roson da Silva (since 08/25)
  External PhD Candidate

Student Assistants

- Daniel Eguiguren Chavez
- Jakub Lapawa
- Jonas Holtwick (until 09/25)
- Jonathan Mucke
- Marius Birmans (since 05/25)
- Maximilian Zimmer (since 03/25)
- Sibel Terzi (since 05/25)
- Simon Jonas (since 03/25)

Interns

- Leslie Garcia-Sanchez (05/25–07/25)
  University of Southern California

OUTLOOK

Looking into the future, we already anticipate exciting new developments in research and teaching. We have multiple interesting papers on topics such as securing wireless communication in industrial networks and modeling attack behavior under submission and hope that we will be able to share them more broadly soon. In parallel, we are pushing hard to finalize different streams of research surrounding security of 5G.

We will further deepen such research within the upcoming 6GEM+ transfer hub, in which we will be working with various academic partners on 6G communication system for connected, digitized industries and especially strive to transfer our research results into practical application.

Finally, our activities in the RealistICS project (see Page 3) will result in a substantially enhanced version of our lecture on Industrial Network Security which will enable students to try out the theoretical concepts from the lecture in a practical, hands-on manner.

REFERENCES

1. S. Michaelides, D. Eguiguren Chavez, and M. Henze, “Poster: Towards an Automated Security Testing Framework for Industrial UEs,” in Proceedings of the Poster Session of the 2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P), 2025. doi: 10.5281/zenodo.16740527 .
2. S. Michaelides, J. Mucke, and M. Henze, “Assessing the Latency of Network Layer Security in 5G Networks,” in Proceedings of the 18th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2025. doi: 10.1145/3734477.3734722 .
3. S. Michaelides, S. Lenz, T. Vogt, and M. Henze, “Secure Integration of 5G in Industrial Networks: State of the Art, Challenges and Opportunities,” Future Generation Computer Systems, vol. 166, 2025. doi: 10.1016/j.future.2024.107645 .
4. J. Bodenhausen, S. Mangel, T. Vogt, and M. Henze, “Bidirectional TLS Handshake Caching for Constrained Industrial IoT Scenarios,” in Proceedings of the 50th IEEE Conference on Local Computer Networks (LCN), 2025. doi: 10.1109/LCN65610.2025.11146343 .
5. K. Wolsing, E. Wagner, L. Lux, K. Wehrle, and M. Henze, “GeCos Replacing Experts: Generalizable and Comprehensible Industrial Intrusion Detection,” in Proceedings of the 34th USENIX Security Symposium (USENIX Sec), 2025.
6. S. Lenz, D. Schachtschneider, S. Jonas, L. Tirpitz, S. Geisler, and M. Henze, “CoFacS – Simulating a Complete Factory to Study the Security of Interconnected Production,” in Proceedings of the 50th IEEE Conference on Local Computer Networks (LCN), 10 2025. doi: 10.1109/LCN65610.2025.11146332 .
7. Ö. Sen, B. Ivanov, C. Kloos, C. Zöll, P. Lutat, M. Henze, A. Ulbig, and M. Andres, “Simulation of Multi-Stage Attack and Defense Mechanisms in Smart Grids,” International Journal of Critical Infrastructure Protection, vol. 48, 2025. doi: 10.1016/j.ijcip.2024.100727 .
8. E. Wagner, F. Basels, J. Bauer, T. Zimmermann, K. Wehrle, and M. Henze, “CAIBA: Multicast Source Authentication for CAN Through Reactive Bit Flipping,” in Proceedings of the 2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P), 2025. doi: 10.1109/EuroSP63326.2025.00045 .