UMR IRISA

Activity Report 2025

Team SOTERN

Self-Protecting the Future Internet

D2 – Networks, Telecommunications and Services

Université de Rennes | rennes | INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES | cnrs | Inria | Inserm | CentraleSupélec | IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom | Université Bretagne Sud ubs

1 Team composition

Researchers and faculty

Pierre Alain, Associate professor,	Rennes University
Ahmed Bouabdallah, Associate professor,	IMT Atlantique
Guillaume Doyen, (HDR) Full professor and Team Leader,	IMT Atlantique
Gilles Guette, (HDR) Full professor,	IMT Atlantique
Romaric Ludinard, Associate professor,	IMT Atlantique
Mohammed Nafi, Associate professor,	Rennes University
Renzo E. Navas, Associate professor,	IMT Atlantique
Marc-Oliver Pahl, (HDR) Full professor,	IMT Atlantique

Associate members

Yann Busnel, (HDR) Full professor,	Institut Mines-Télécom

Research engineers, technical staff

Fabien Autrel, Permanent research engineer,	IMT Atlantique
Fabien Eyssartier, Research engineer from Nov. 24,	IMT Atlantique

Post-doctoral researchers

Elie Chedemail from Nov. 24,	IMT Atlantique
Loïc Miller, from Sept. 22 to Aug. 25,	IMT Atlantique
Issam Ikhelef, from Sept. 24 to Aug. 26,	IMT Atlantique

PhD students

Antoine Rebstock, 2021-2025 (withdrawal on sept. 25)	IMT Atlantique
Do Duc Anh Nguyen, 2022-ongoing	IMT Atlantique
Van Tien Nguyen, 2022-ongoing	LAAS-CNRS
Mathis Durand, 2023-ongoing	IMT Atlantique
Hugo Bourreau, 2024-ongoing	IMT Atlantique
Luc Bournaud, 2025-ongoing	IMT Atlantique
Gabriel Bourgeois, 2024-ongoing	Rennes University
Yohann Morel, 2024-ongoing	IMT Atlantique
Daisy Munson, 2025-ongoing	Rennes University
Dorian Pacaud, 2024-ongoing	IMT Atlantique
Constant Rohmer, 2024-ongoing	Rennes University

External PhD students who collaborated with the SOTERN research group

Marius Letourneau (LIST3N – Université de Technologie de Troyes), 2020 to Jul. 2025
Hichem Magnouche (LIST3N – Université de Technologie de Troyes), 2020 to March 2025
Pierre-Marie Lechevalier (ADOPNET/IRISA – IMT Atlantique), 2021-2025, defended on June, 17th 2025
Christian Lübben (TU München), 2018-ongoing
Erkin Kirdan (TU München), 2019-ongoing
Lars Wüstrich (TU München), 2019-2/2025
Alexander Loth (Frankfurt University of Applied Sciences), 2024-ongoing
Virgil Hamici-Aubert (OCIF/IRISA – IMT Atlantique), 2023-ongoing
Ignacio J. Dasso (SIGNAL/IETR – Nantes Université), 2024-ongoing
Radheshyam Singh (Technical University of Denmark), 2020-2024,

Administrative assistant

Sandrine Frouin	IMT Atlantique
Laurianne Viala	IMT Atlantique

2 Overall objectives

2.1 Overview

The SOTERN team, part of the IRISA research institute, focuses on developing methods and tools for the **self-protection of the Future Internet**. This concept refers to systems' ability to autonomously monitor, detect, and respond to malicious behaviors that could compromise services, users, or infrastructures.

Depending on system characteristics and maturity, self-protection solutions can be:

- **Intrinsic**: Implemented within components during design or through corrective measures.
- **Extrinsic**: Utilizing dedicated security components that automatically enforce attack detection, mitigation, and remediation.

Challenges and Research Areas The team's research addresses challenges arising from the Internet's evolution, which increasingly integrates cyberspace into human environments, including:

- **Everyday Life**: Use of mobile devices and smart environments like vehicles and buildings.
- **Critical Infrastructures**: Both civil (e.g., Industry 4.0) and military applications, such as robots and drones in operational settings.

This evolution is driven by advancements in connected objects, telecommunications, and virtualization. Ensuring a secure and trustworthy coupled real/digital space presents complex challenges due to:

- **Scale and Complexity**: Cyber-physical systems are growing in size and consist of increasingly miniaturized elements with atomic functions, like connected objects or micro-services in virtualized infrastructures.
- **Openness**: Many systems are open, not confined to controlled infrastructures with identified trustworthy participants.
- **Autonomy**: The complexity and need for uninterrupted functionality necessitate system autonomy, reducing human control.

By addressing these challenges, SOTERN aims to contribute to a safer and more resilient Future Internet.

2.2 Scientific foundations

The scientific foundations of the SOTERN research group are gathered around three research axes we expose and instantiate through methods and technological tools subsequently.

2.2.1 Experimental Approaches

The SOTERN research group considers experimental approaches as a core research methodology of many if not all its research activities. Indeed, generally speaking, security breaches strongly rely conception flaws or implementation vulnerabilities that attackers leverage in order to implement their kill chains. As such, deploying real implementations or capturing data from real systems deployed in open or controlled environments stands for the most suitable way to assess security threats or evaluate security research outcomes. If the SOTERN considers simulation as a secondary means, it is restricted to those situations where scalability requirements are not compatible with testbeds, even distributed. The team especially advocates the use of experimental approaches for the following research methodological purposes:

Threat assessment in controlled environments: As part of threat anticipation for future networks or to accurately understand and model attacks achieved over current ones, the SOTERN research group deploys dedicated experimental means which rely on concrete hardware/software frameworks, real malicious code, and dedicated instrumentation and monitoring tools. Virtualisation means are often considered for their flexibility, ease of control, reproducibility and isolation features. As illustrative examples, we indicate here malware propagation studies over the Internet deployed over a GNS3 framework, or the security compliance assessment of the Open5GS open-source platform with regards to 3GPP requirements. The team is also part of the LHS[1] where it operates sensitive studies in a secured environment (e.g. malware execution to capture network traces). In cooperation with other research groups part of IRISA Department 2 (Network and Telecommunication), some specific testbeds are also jointly operated, especially to reveal unknown attack scenarios taking part of the threat anticipation. For instance, novel 5G attacks on the Radio Access Network are empirically assessed on a testbed deployed by the IRISA/Adopnet research group which also conducts performance-oriented experiments aside.

Attack captures in open systems: Besides attack reproduction in controlled environments, the team also considers data capture "in the wild", with the purpose of (1) collecting unbiased security data resulting from deployed systems in real operation, and (2) better understand strategies and procedures of today's attackers. This purpose methodologically requires the deployment or access to infrastructures open to attackers, the absence of any bias due to instrumentation or monitoring, and finally, some robust and scalable statistical methods to process the collected data and extract substantial information revealing attacker insights. The team cooperates with external partners such as the INRIA/Pirat research group in this area and also considers the deployment of its own digital twins and honeynets as experimental means. People around our research group (i.e. permanent staff, PhD and postdoc, students of our campuses) also take part of measurement campaigns when real users activities come into legitimate activity captures.

Evaluation of research outcomes: As a a last mile following (1) data capture for attack assessment either in a controlled environment or in the wild and (2) the

[1] Laboratoire de Haute Sécurité – Rennes

proposal of protection, detection/reaction solutions, the SOTERN research group mainly considers an experimental methodology for the performance evaluation of its scientific contributions. The solutions elaborated on various topics are thought to be robust against challenging realistic environments and also reach higher Technological Readiness Levels (TRL), would further cooperation with industrial partners require it. As such, at least performance evaluation is achieved on real data, captured from former threat assessment of real infrastructures datasets. Furthermore, operational constraints are also considered when appropriate (e.g. capability to detect an attack in real-time vs. offline processing).

Software implementations: As a final outcome, and given the experimental methodology we consider, our research results consists also in software pieces developed and made publicly available or shared with partners we cooperate with. For example, a scientific activity on federated IDS led us to design and implement network topology generation tools which are now going to be integrated into an industrial partner Cybersecurity platform.

2.2.2 Data-Oriented Approaches

The exponential growth of connected devices and the increasing complexity of cyber-physical systems generate massive volumes of heterogeneous data, often distributed across decentralized infrastructures. In this context, data-oriented approaches are essential to extract actionable insights, detect anomalies, and ensure the resilience of self-protecting systems. Our research leverages advanced statistical methods, data summarization, and data fusion techniques to address the challenges of scalability, real-time processing, and knowledge integration in dynamic environments.

A core focus of our work is the development of real-time data analysis frameworks, particularly for data streams, where traditional batch processing is inadequate. By combining incremental learning algorithms with adaptive statistical models, we enable continuous monitoring and rapid response to emerging threats. For instance, our contributions in anomaly detection and behavioral analysis rely on lightweight, distributed summarization techniques to reduce computational overhead while preserving the accuracy of security assessments. These methods are critical for applications ranging from IoT security to the protection of critical infrastructures, where latency and resource constraints are paramount.

Another key aspect of our research is the integration of knowledge bases with AI models, bridging symbolic reasoning and machine learning. This hybrid approach enhances the interpretability and robustness of security mechanisms, especially in scenarios where data is sparse or noisy. Recent advancements in our team include the use of federated learning to enable collaborative threat detection without centralizing sensitive data. By clustering participants based on data similarity and incorporating reputation systems, we mitigate risks such as data poisoning and adversarial attacks, while preserving privacy and scalability.

Our work also explores the scalability of data-driven security mechanisms, with a particular emphasis on optimizing resource usage in large-scale systems. For example, we investigate how graph-based representations and probabilistic models can improve

the efficiency of intrusion detection systems, enabling them to operate in resource-constrained environments. These efforts are complemented by research on cross-domain knowledge fusion, where heterogeneous data sources—such as logs, network traffic, and contextual metadata—are combined to build comprehensive situational awareness.

Through these data-centric methodologies, we aim to provide the foundational tools necessary for the Future Internet to autonomously adapt to evolving threats, ensuring both security and operational continuity.

2.2.3 Distributed Algorithms for Security Mechanisms Scalability

In the rapidly evolving landscape of cybersecurity, distributed and collaborative approaches have emerged as indispensable tools in combating increasingly sophisticated threats targeting large scale, dynamic and fully distributed systems. Our research teams addresses scalability aspects of various security features such as the protection of infrastructures, intrusion detection and reaction to attacks, sometimes combining it with safety issues also. Distributed algorithms lies at the core of this methological axis of the SOTERN research group which either considers ready-on-the-shelf solutions which sound relevant in a security application field, or designs dedicated solutions when existing approaches are not aligned with the use-case requirements.

For instance, as exposed in Section 2.2.2, considering federated learning methodologies as a substrate for intrusion detection, to circumvent issues related to data privacy as well as data poisoning, we enhance existing approaches with clustering schemes to gather together participants with similar data. In addition, we leverage reputation mechanisms to weight contributions of the various system participants. Our work on trust metrics provides valuable insights into quantifying and establishing trust among disparate entities within collaborative cybersecurity ecosystems. Second, we also investigate how distributed security enforcement points over the Internet can be synchronized in a decentralized way to react in case of an attack occurrence. We especially investigate the dynamic placement of IDS through decentralized vertex coverage algorithms and study to what extent they need to be adapted or extended for security purposes. Finally, regarding some joint activities with safety purposes, our research team aims at tackling temporal agreement in distributed systems, such as lightweight replication and scalability of blockchain mechanisms. Indeed, current blockchain designs leverage a continuous block appending process to update the system state leading to a steadily increase of storage requirements thus eventually jeopardizing blockchain initial promise: being totally decentralized, without trusted third party. These designs also suffer from poor throughput performance and high energy consumption. We investigate alternative designs relying on different underlying data structure to conjointly handle these issues.

2.3 Application Domains

The different research foundations previously exposed target different application domains, all standing for future networks and services. These are:

2.3.1 Threats Understanding and Modeling

The protection of information systems can be viewed in generic terms and implemented by applying the main principles of defense. However, knowing the attacker and their *modus operandi* can be of a great support to improve the effectiveness of such a defense. Attracting an attacker is not a straight-forward operation. As such, a common practice is to let machines be deliberately vulnerable and accessible from the Internet in order to lure the attacker. This practice has evolved over time, taking different forms such as honeypots, honeynets, honeytokens, HoneyX or deceptive security systems, among others. These tools can be considered in two situations. The first basically consists to create a diversion by decoying the attacker, who will strive to attack a fake system rather than the real information system, thus allowing them to be detected and evicted from the system before they cause any damage. The second use case consists in observing an attacker without their knowledge. This raises several challenges: how to monitor a system in a way that is completely undetectable to the attacker? How to know what the attacker is looking for by simply observing their actions? How to automatically offer them what they are looking for in order to get them to reveal their techniques and procedures? And, of course, how to provide them with all this without becoming completely corrupted and participating in the attack on other systems? In this application field, the SOTERN research group addresses the realism of honeynets as advanced attack capture infrastructures. The goal is to enhance the credibility and behavioral fidelity of honeynet deployments in order to collect high-quality threat intelligence against sophisticated adversaries. Rather than relying on static or easily fingerprintable environments, this research investigates adaptive, large-scale honeynets capable of emulating realistic services, traffic patterns, and user behaviors.

2.3.2 Reactive Security Mechanisms

The SOTERN research group applies a substantial part of its research to reactive security mechanisms. First, intrusion detection applications mainly focus on distributed and advanced IA methods for attack detection. GNN for APT detection or security of Federated Learning for intrusion detection are examples of such uses cases. Leveraging the self-protection paradigm, it also studies to what extent contextual information can enhance intrusion detection, especially for Individual Information Systems used in end-user smartphones. Attack reaction is the second reactive security mechanisms the research group handles. Especially, the team background in networking and distributed systems allows to propose decentralized mechanisms whose final aim is to propose fast and scalable reaction schemes to attacks. Those works are especially instantiated in several PhD topics focusing on distributed orchestration of security reactions with blockchains and automatic malware propagation mitigation at the Internet scale. Finally, taking part of reactive security mechanisms, the SOTERN research group also dedicates a substantial part of his work on threat anticipation with more specifically research works on intrusion detection mechanisms applied to emerging/future networks. We cite here some relevant cases: Reduction of Quality (RoQ) attacks at the RLC layer in 5G networks, threats leveraging misconfigurations in TSN and MAC/Channel Allocation attacks and counter-measures in WiFi HaLow (802.11ah).

2.3.3 Security Management and Protection Mechanisms

Security management and protection mechanisms are essential to safeguard modern digital infrastructures against the state-of-the-art complex threats. Intent-based security (IBS) seeks to minimize human intervention, reduce errors, and ensure the network dynamically adapts to evolving conditions while meeting security goals. By leveraging techniques such as neural networks, our work focuses on user intents expressed in natural language to be interpreted and, once deployed, continuously verified through monitoring data. In this context, 5G networks represent a key use case, where security requirements defined by standards and norms can be parsed as intents and automatically translated into formal models to be compared against deployed configurations. In parallel, the security of control and management operations is critical for maintaining the integrity and reliability of modern digital infrastructures. This includes protecting cryptographic key exchange protocols as well as securing control protocols against, for instance, man-in-the-middle attacks. Finally, identity management further complements these mechanisms by placing the user at the center of service-centric systems. Emerging approaches such as Self-Sovereign Identity (SSI) enable users to manage their digital identities in a decentralized manner without relying on centralized providers. By leveraging blockchain technologies to store verifiable claims, these solutions aim to be secure against a strong adversary, parsimonious in terms of energy and storage, and requiring the weakest synchrony assumptions as possible, so that smartphones will be able to actively and sporadically participate to its construction.

2.3.4 Emerging Cybersecurity Tools

The SOTERN research group develops emerging cybersecurity tools that complement its work on detection and protection by focusing on visualization and attack capture, two key enablers for understanding, anticipating, and mitigating complex threats. These activities provide advanced experimental environments and innovative interaction mechanisms designed to address the scale, heterogeneity, and dynamic nature of modern digital infrastructures. A first application field concerns digital twins for cybersecurity. The objective is to design virtual replicas of networked infrastructures that remain synchronized with operational systems and can be used for security validation, attack simulation, and configuration assessment. These twins enable safe experimentation with intrusion scenarios, misconfigurations, or cascading failures without impacting production systems. As an early work started recently, we established requirements and guidelines a digital twins, as a foundational tool for proactive security evaluation and cyber-range–like experimentation, has to provide. Second, XR-based cybersecurity visualization tools explores immersive extended reality (XR) interfaces to enhance situational awareness and collaborative analysis in security operations contexts. Recently, several proof-of-concept prototypes were implemented to visualize network topologies, alert correlations, and simulated attack propagation within three-dimensional interactive environments. These developments are evaluated from both technical and human-centric perspectives, with particular attention to usability, cognitive load, and decision support. Together, these activities illustrate the team's commitment to advancing innovative cybersecurity tooling grounded in experimentation, realism, and advanced human–machine interaction. By combining digital twins and immersive visualization environments, the group

contributes to a new generation of tools that strengthen both the observation and understanding of complex cyber threats.

3 Scientific achievements

3.1 Threats Understanding and Modeling

3.1.1 Sécurité des réseaux TSN : Vulnérabilités et Exploitations des Mauvaises Configurations

Participants: Gabriel Bourgeois, Mohamed-Aymen Chalouf, Guillaume Doyen, David Espes.

Published in Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI) 2025 [7]

Le terme Time-Sensitive Networking (TSN) désigne un ensemble de standards développés par le groupe de travail IEEE 802.1 qui vise à rendre Ethernet déterministe. TSN s'est révélé comme un levier vers une convergence des Technologies de l'Information (IT) et des Technologies Opérationnelles (OT), permettant de faciliter le transfert des données dans un contexte critique en utilisant une technologie non propriétaire et peu coûteuse. La sécurité des réseaux TSN est une question peu abordée dans la littérature mais essentielle pour permettre son adoption à grande échelle. Malgré une conception sécuritaire par défaut, certains standards ont des vulnérabilités identifiées et il n'existe pas d'outil de vérification de l'intégrité d'un réseau TSN. La complexité de configuration des standards peut amener à des réseaux TSN opérationnels mais vulnérables à leur exploitation par un attaquant désirant nuire aux performances du système. L'objectif de cet article est d'aborder le thème de la sécurité de TSN à travers le prisme des paramètres de configuration ayant un impact sur la robustesse du réseau.

3.1.2 Exploiting Congestion Control Parameter Manipulation in QUIC for Security Implications

Participants: Guillaume Doyen.

Joint work with Concordia University. Published in 2025 21st International Conference on Network and Service Management (CNSM) [16]

QUIC has emerged as a fundamental transport protocol for modern Internet infrastructure, serving as the foundation for HTTP/3. Although QUIC implements congestion control algorithms (CCA) to ensure fair network resource allocation, its user-space implementation architecture creates significant security vulnerabilities through accessible parameter manipulation. As transport layers become increasingly programmable, these vulnerabilities represent a broader security challenge for future network infrastructures where applications may deploy custom transport implementations. This paper presents a systematic analysis of selfish behaviors in QUIC through deliberate congestion control parameter (CCPM). Using the aioquic implementation, we experimentally

demonstrate how strategic parameter manipulation in both NewReno and CUBIC algorithms provides substantial unfair bandwidth (BW) advantages. NewReno exhibits a major vulnerability with Loss Reduction Factor (LRF) and Congestion Avoidance Growth Rate (CAGR) manipulation, while CUBIC demonstrates better resilience, but remains exploitable, with combined LRF (beta-cubic) and Maximum Idle Time (MIT) manipulations.

3.1.3 A Grammar-Driven Approach to Model and Detect APT Attack Sequences

Participants: Antoine Rebstock, Yann Busnel, Romaric Ludinard.

Published in 18th International Symposium on Foundations and Practice of Security (FPS) 2025 [23]

This paper introduces a grammar-driven approach to model and detect sequences of Advanced Persistent Threat (APT) attacks. APTs are characterized by their complexity and multi-step nature, making them challenging to detect with traditional systems. The proposed method employs interpretable rules to capture malicious behaviors and aligns semantically with the MITRE ATT&CK framework. This approach enables the detection of plausible attack scenarios even in the presence of incomplete or noisy data. We evaluate it using a public large CTF dataset which provides realistic and diverse attack scenarios. Experiments illustrate the effectiveness of the method in reconstructing plausible attack progressions, even with incomplete data. The main contribution of this study is an open-source implementation in Rust, ensuring reproducibility and extensibility. We also propose future enhancements to better model contextual dependencies between tactics in APT attack sequences. In a nutshell, this grammatical approach offers a robust method for detecting sophisticated threats, bridging the gap between low-level observations and high-level strategic reasoning.

3.1.4 Investigating the Impact of Label-flipping Attacks against Federated Learning for Collaborative Intrusion Detection

Participants: Léo Lavaur, Yann Busnel, Fabien Autrel.

Published in Computers & Security, 2025, 156, pp.104462 [2]

The recent advances in Federated Learning (FL) and its promise of privacy preserving information sharing have led to a renewed interest in the development of collaborative models for Intrusion Detection Systems (IDSs). However, its distributed nature makes FL vulnerable to malicious contributions from its participants, including data poisoning attacks. Label-flipping attacks-where the labels of a subset of the training data are flipped-have been overlooked in the context of IDSs that leverage FL primitives. This work contributes to closing this gap by providing a systematic and comprehensive overview of the impact of label-flipping attacks on Federated Intrusion Detection Systems (FIDSs). We show that the elects of such attacks can range from severe to highly mitigated, depending on hyperparameters and dataset characteristics, and that their mitigation is non-trivial in heterogeneous settings. We discuss these findings in

the context of existing literature and propose recommendations for the evaluation of FIDSs. Finally, we provide a methodology and tools to extend our findings to other models and datasets, thus enabling the comparable evaluation of existing and future countermeasures.

3.1.5 Dissecting 5G New-Radio Latency: Interacting Layers and Latency-Generating Operations

Participants: Virgil Hamici-Aubert, Renzo E. Navas, Guillaume Doyen.

Joint work with Julien Saint-Martin (ADOPNET/IRISA), Georgios Z. Papadopoulos (OCIF/IRISA), and Xavier Lagrange (ADOPNET/IRISA) from IMT Atlantique. Published in SLICES workshop collocated with the 24th IFIP Networking Conference (Networking 2025) [15].

The fifth-generation (5G) mobile network improvements in the Radio Access Network (RAN), including low latency, reliability, and massive connections, are key enablers for emerging technologies and applications, such as smartgrids, factory automation, and metaverse. Latency on the RAN relies on a multiplicity of 5G parameters that can be configured as needed. Current End-to-End (E2E) latency diagnostic capabilities are unsatisfactory in understanding the RAN involvement, and exhibit the importance of improving our diagnostic capabilities for 5G RAN implementations. In this paper, we aim to dissect the Uplink (UL) RAN latency in order to understand the origins of latency generation. An extensive experimental campaign on a 5G open-source implementation (OpenAirInterface) allows us to study the UL E2E latency through several bitrates. We mark each packet in its payload, and use the identifiers of each New Radio (NR) layers to track its E2E latency at the protocol level. We identify the layers mainly involved in the RAN latency composition, exhibit their operations, and explain their origin. This work leverages the collected information and latency measurements through all NR protocol layers to improve the understanding and diagnostics of the UL E2E latency through the RAN. Last but not least, the source code and experimental data are publicly available.

3.1.6 Industrial IoT cybersecurity: a bibliometric analysis

Participants: Ignacio J. Dasso, Renzo E. Navas.

Joint work with Sébastien Maudet and Guillaume Andrieux from Nantes Université (IETR/SIGNAL).

Published in

- *SpliTech 2025: 10th International Conference on Smart and Sustainable Technologies (IEEE)[12].*
- *RESSI 2025 : Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information[11].*

Industrial Internet of Things (IIoT) cybersecurity has become critical to our societies as industrial systems increasingly rely on interconnected devices. Several literature studies exist regarding cybersecurity for IoT or security topics in Industry 4.0. Still, very

few are exclusively dedicated to cybersecurity for IIoT—and they approach the subject non-systematically. In this study, we conduct a systematic bibliometric analysis of over 12,000 academic publications from 2014 to 2024 to map the research landscape of IIoT cybersecurity. Guided by eight Research Questions and a methodological approach, we examine publication types, key venues, and dominant topics to highlight trends and research clusters within the field. Our findings show that conference papers and journal articles are predominant, with IEEE and Springer serving as the leading publishers. Among the most cited works, "blockchain" is the most popular topic. A keyword co-occurrence analysis identifies four thematic clusters led by: (1) "blockchain" and "security," (2) "network security" and "industrial IoT," (3) "industrial embedded systems" and "cyber-physical systems," and (4) "automation" and "network architecture." The first two clusters are the most prominent grouping 80% of the top 20 keywords. Regarding future trends, the growing prominence of "machine learning" and "intrusion detection," and a slight deceleration of "blockchain" in 2024, suggests shifting research priorities. We publicly share the bibliographic data and source code used to create this bibliometric analysis.

3.1.7 Revealing Embedded System Behaviors: A Comparative Analysis of Power Consumption and Hardware Performance Counters

Participants: Mohammed Mezaouli, Yehya Nasser, Samir Saoudi, Marc-Oliver Pahl.

Published in HS3 2025: 1st Workshop on Hardware-Supported Software Security-Co-located with ESORICS 2025, 25th of September 2025 in Toulouse, FR. [19].

As computing evolves, analyzing system behavior has become as critical as optimizing performance and energy efficiency. Traditional methods of behavioral analysis often rely on software-level profiling or predefined signatures, which limit their applicability in dynamic and resource-constrained environments. This study takes a novel approach by identifying and characterizing system workloads based on distinct behavioral patterns, such as memory usage, arithmetic operations, and control flow. By leveraging hardware performance counters (HPCs) and power consumption metrics, this work demonstrates how hardware-level insights can reveal unique operational signatures. These findings highlight the potential of HPCs and power consumption to enhance the understanding of system behaviors, offering practical solutions for behavior identification that could be instrumental in detecting vulnerabilities or anomalies. The results underscore both the opportunities and challenges of using these metrics for behavioral analysis in embedded systems.

3.2 Reactive Security Mechanisms

3.2.1 A Methodological Assessment and Performance Evaluation of Hyperledger Fabric

Participants: Constant Rohmer, Pierre Alain, Mohamed-Aymen Chalouf, Guillaume Doyen.

Published in the 34th International Conference on Computer Communications and Networks (ICCCN 2025) [24]

The expanding attack surface and increasing complexity of information systems render human responses insufficient against modern threats. The introduction of concepts such as self-protection and collaborative cybersecurity opens up possibilities for new defence systems tailored to today's requirements. Distributed Denial-of-Service (DDoS) attacks, in particular, demand automated and wide-reaching responses due to their disruptive nature and broad impact across networks. Recent research is exploring blockchain-based solutions to address the fundamental challenge of trust among collaborators, as blockchain provides a secure and transparent framework for sharing threat intelligence and enforcing consensus. However, the literature did not establish the relevance of blockchain technology for collaborative DDoS mitigation before its application. The contribution of this paper is twofold. First, we methodologically analyse the relevance of blockchain technology for our use-case and determine that Hyperledger Fabric (HLF) is a promising solution. Second, we evaluate the performance impacts of HLF combined with the SmartBFT consensus algorithm for collaborative DDoS attack mitigation. Our performance analysis measured system durations ranging from 200 to 1500 ms under various network configurations, influenced by topological size (number of nodes) and geographical size (communication delays). The modeling of our results showed quadratic scaling with the number of HLF orderers and stronger, linear scaling with communication delays. These findings provide actionable insights to optimise collaborative blockchain-based DDoS mitigation solutions.

3.2.2 Vers une Auto-protection Collaborative des Systèmes Connectés fondée sur la Blockchain et les Microservices Unikernels

Participants: Constant Rohmer, Pierre Alain, Mohamed-Aymen Chalouf, Guillaume Doyen.

Published in Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI) 2025 [25]

L'augmentation de la surface d'attaque et la complexité croissante des systèmes d'information rendent les réponses humaines inadaptées face aux menaces modernes. L'introduction de concepts comme l'auto-protection et la cybersécurité collaborative permet d'envisager de nouveaux systèmes de défense adaptés aux exigences actuelles. Il se pose alors la question de concevoir une architecture autonome de confiance, qui soit capable d'orchestrer en temps réel des réponses coordonnées et d'appliquer des contre-mesures ciblées et adaptatives. Cette thèse vise à répondre à ce besoin en conciliant fiabilité, robustesse et performance. L'approche proposée s'appuiera sur la blockchain pour garantir l'inaltérabilité et la traçabilité des actions, tout en automatisant les réactions via des contrats intelligents (smart contracts). Les microservices unikernels viendront compléter cette architecture en assurant l'adaptabilité et la parallélisation des opérations, améliorant ainsi la scalabilité et le temps de réponse. Une fonction d'orchestration multi-objectifs sera également introduite pour coordonner les ressources, prioriser les actions et éviter les conflits. Enfin, une évaluation rigoureuse permettra de valider les performances de la solution et de garantir une réaction collaborative efficace et opti-

misée.

3.2.3 Federated apprenticeship seeks quality models, good reputation required

Participants: Yann Busnel, Léo Lavaur, Pierre-Marie Lechevalier, Romaric Ludinard, Géraldine Texier.

Published in 27ème Rencontre Francophone sur les Aspects Algorithmiques des Télécommunications (AlgoTel) [10]

Cross-silo federated learning (CS-FL) is a distributed collaborative learning paradigm that enables a group of organisations to train a shared model. However, these systems are vulnerable to poor-quality contributions, making protections against negligent or malicious participants crucial. Furthermore, the heterogeneity of CS-FL use cases complicates the distinction between malicious and legitimate contributions. To address these challenges, we introduce RADAR, a CS-FL architecture capable of evaluating the quality of contributions without making assumptions about data similarity. Through cross-evaluation, RADAR groups participants perceived as similar and assigns a reputation score to weight their contributions during aggregation. We evaluated our approach in concrete collaborative intrusion detection system (CIDS) scenarios, disrupting data labelling to simulate variations in quality. The results show that by combining participant partitioning and a reputation system, RADAR can counter a wide range of Byzantine behaviours, demonstrating its versatility.

3.2.4 Towards Context-aware Intrusion Detection in Individual-oriented Information Systems: An Empirical Study on Android Malware

Participants: Van-Tien Nguyen, Renzo E. Navas, Guillaume Doyen.

Published in 2025 21st International Conference on Network and Service Management (CNSM) [21].

In recent years, the range and volume of Internet services utilized by an individual have significantly expanded. This growing relationship between an individual user and diverse digital services has led to the emergence of Individual oriented Information System (IIS) that encompasses the user, their physical devices, and the information systems they interact with. Current security approaches within an IIS suffer from three main limitations: (1) they are restricted to specific services, (2) they require intrusive instrumentation of each user single device, or (3) they rely on specific integration between client and server components. As a result, they fail to globally protect against attackers who possess enough information to bypass standalone security schemes. To overcome these constraints, we propose to (1) consider a network-oriented approach to detect intrusions which may occur within an IIS and (2) to make sensors taking part of the IIS contribute to the intrusion detection by providing user-related contextual data. In the absence of any suitable dataset that mixes network and physical contextual data, we construct a new integrated dataset comprising benign data captured through an in-situ experiment and intrusion traces extracted from CIC-AndMal2017-a widely referenced

dataset in the literature. Our evaluation confirms that consider both user physical context and network features improves the performance of intrusion detection, thereby making IIS more resilient to attackers.

3.2.5 Decentralized Anomaly Detection Using Deep Feed-Forward Neural Networks

Participants: Christian Lübben, Marc-Oliver Pahl.

Published in al International Journal of Network Management [3].

As computing evolves, analyzing system behavior has become as critical as optimizing performance and energy efficiency. Traditional methods of behavioral analysis often rely on software-level profiling or predefined signatures, which limit their applicability in dynamic and resource-constrained environments. This study takes a novel approach by identifying and characterizing system workloads based on distinct behavioral patterns, such as memory usage, arithmetic operations, and control flow. By leveraging hardware performance counters (HPCs) and power consumption metrics, this work demonstrates how hardware-level insights can reveal unique operational signatures. These findings highlight the potential of HPCs and power consumption to enhance the understanding of system behaviors, offering practical solutions for behavior identification that could be instrumental in detecting vulnerabilities or anomalies. The results underscore both the opportunities and challenges of using these metrics for behavioral analysis in embedded systems.

3.3 Security Management and Protection Mechanisms

3.3.1 A translation corpus based on a robust methodology for Intent Based Networking

Participants: Daisy Munson, Pierre Alain, Guillaume Doyen.

Published in Computer Network Special Issue "Generative and Explainable Artificial Intelligence for Internet Traffic and Architectures" [4]

The rise of Intent Based Networking (IBN) has paved the way for more efficient network and security management, reduced errors, and accelerated deployment times by leveraging AI processes capable of translating natural language intents into policies or configurations. Specialized neural networks could offer a promising solution at the core of translation operations. Still, they require dedicated, large-scale corpora for training generative models, which are not currently available due to the restricted and confidential nature of the information they convey. This paper fills this gap by proposing a novel methodology for creating a corpus specifically tailored to train a Large Language Model (LLM) for this translation task. Our approach leverages advancements in Natural Language Processing (NLP) to overcome the challenges posed by the limited training data, enabling accurate interpretation and translation of high-level performance and security directives from natural language into structured, actionable formats, represented by the intermediate Network Intent LanguagE (Nile). Our experimental evaluations, grounded

by human experts, indicate that our corpus generation methodology yields promising results in terms of translation accuracy and language naturalness. As a result, we have been able to generate Nile-English Aligned Translations (NEAT), a corpus, which is to date two orders of magnitude larger than currently available datasets, exhibits a wide coverage of the Nile syntax, and has much lower perplexity values than other generated corpora. NEAT has been made publicly available to facilitate further research and development in adapting generative models to network management and security. The NEAT dataset is publicly available.

3.3.2 Non Interactive Proof of Proof-of-Work in dynamic setting

Participants: Loïc Miller, Dorian Pacaud, Nathanël Derousseaux-Lebert, Emmanuelle Anceaume (IRISA/Pirat‘\)), Romaric Ludinard.

Published in

- *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security, CCS 2025 [20],*
- *Rencontre Francophones sur les Aspects Algorithmiques des Télécommunications 2025 (Algotel 2025) [22]*

This paper presents the first non-interactive, succinct, and secure representation of a PoW-based blockchain that operates under variable mining difficulty while satisfying both completeness and onlineness properties. Completeness ensures that provers can update an existing NIPoPoW by incorporating a newly mined block, whereas onlineness ensures that miners can extend the chain directly from a NIPoPoW. The time complexity for both the prover (to update a NIPoPoW with a new block) and the verifier is logarithmic in the number of blocks of the underlying PoW blockchain. The communication complexity required for synchronization is polylogarithmic in the length of the blockchain. We prove the correctness of our scheme in the presence of a 1/3-bounded PPT adversary.

3.4 Emerging Cybersecurity Tools

3.4.1 Constraint-based Network Topology Generation for Evaluating Federated Intrusion Detection Systems

Participants: Léo Lavaur, Yann Busnel, Fabien Autrel.

Published in 1st International Workshop on Assessment with New methodologies, Unified Benchmarks, and environments, of Intrusion detection and response Systems (ANUBIS) [17]

Federated Intrusion Detection Systems (FIDSs) emerged as a promising approach to collaborative cybersecurity, enabling organizations to train intrusion detection models without sharing sensitive data. However, evaluating such systems faces significant challenges due to the lack of available datasets that capture the heterogeneity of real-world distributed networks. Existing datasets are typically generated using single network topologies, forcing researchers to rely on artificial partitioning strategies that cannot

replicate heterogeneous data distributions that exist in practice. To address this limitation, we propose a novel approach for generating heterogeneous network topologies specifically designed to evaluate distributed and federated intrusion detection systems. Because creating realistic topologies from scratch is particularly complex, we construct complex topologies from a library of predefined sub-topologies using constraint programming, and compose them into larger, realistic network structures. We implement a prototype and evaluate its performance across multiple parameters including library size, maximum number of nodes, tree depth, and service constraints. The results highlight that, while the derivation time scales rapidly with most parameters due to the combinatorial nature of the problem, the tool successfully generates large numbers of diverse topologies while maintaining control over their heterogeneity characteristics.

3.4.2 L'Apprentissage Machine au Sein des Jumeaux Numériques pour l'Estimation et la Détection des Menaces

Participants: Hugo Bourreau, Marc-Oliver Pahl, Fabien Dagnat (LAB-Sticc), Fehmi Jaafar (UCAQ, Canada).

Published in Proceedings of the 32nd C&ESAR [9].

The convergence of digital twins (DT) and machine learning (ML) represents a promising combination for enhancing cybersecurity by proactively predicting threats and attacks. This article presents a taxonomy of the use of the digital twin concept in cybersecurity, categorizing their roles in threat prediction and attack detection. By analyzing methodologies, system feature selection strategies, and the artificial intelligence tools employed in various implementations, the article highlights their current capabilities and limitations.

3.4.3 Pouvez-vous détecter le piège? Détection de pots de miel face à l'évolution des tactiques d'évasion

Participants: Mathis Durand, Alexandre Dey, Yvon Kermarrec, Marc-Oliver Pahl.

Published in Proceedings of the 32nd C&ESAR [13].

Honeypots are important tools for network security, as they enable the detection, diversion, and analysis of malicious activities. However, their effectiveness depends on remaining undetected. The most advanced attackers are familiar with the concept of honeypots and develop detection and evasion tactics. This article presents a systematization of knowledge on the current state of honeypot detection, providing an overview of techniques used both in laboratory settings and in the real world.

3.4.4 Enhancing cybersecurity using Digital Twin and AI

Participants: Hugo Bourreau, Fabien Dagnat, Marc-Oliver Pahl, Fehmi Jaafar.

Published in RESSI 2025 : Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information [8].

This paper examines the state of the art in the use of digital twins (DT) for the cybersecurity of cyber-physical systems (CPS). Digital twins enable real-time monitoring, predictive analytics, and adaptive decision-making. The study highlights the main advantages of using DTs and identifies key challenges, such as the lack of impact evaluation and the need to standardize their operation. It also emphasizes advances driven by artificial intelligence (AI). Furthermore, it outlines open issues and future perspectives for the successful integration of digital twins into critical environments.

3.4.5 Secure Distributed Microservice Architectures

Participants: Marc-Oliver Pahl.

Published in Technische Universität München [1].

Modern services like Amazon, Facebook, AirBnB, or Google often use collaborating microservices to render their functionalities. Shifting from monolithic architectures to highly distributed, mashed-up services brings many advantages. It allows benefiting from recent compute paradigms like fog or edge: locating critical functionality closer to the users results in lower latency and higher throughput to the user. But distributed microservice mash-ups are also challenging. The distribution of the computation requires advanced cybersecurity mechanisms. The management and ex- change of data are central challenges in such architectures. Also, the efficient mana- gement of the masses of services requires adequate algorithms. Finally, the teaching of competencies required to manage such complicated software architectures and pro- perties of their underlying substrate networks and hosts requires novel approaches. This habilitation project makes 88 contributions in all four research areas and connects them. Central contributions in cybersecurity are early contributions in the emerging field of federated learning, collaborative algorithms for anomaly detection. The work also cov- ers multi-modal anomaly detection, and advanced security-by-design methodologies, like multi-stakeholder security concepts, ontology-based access control, or optimiza- tion for established security mechanisms. In data management, the habilitation project proposes the introduction of a common data management layer. It enables a stateless service design, significantly increases security and development effort, and enables optimizing this common functionality globally. It also proposes collaborative ontologies that enable structuring the com- plexity of the emerging data space. In the service management domain, this research proposes novel service-coupling based-on data and continuously optimized service placement. Some of the optimiza- tions use automated reasoning on domain knowledge including algorithms using arti- ficial intelligence. In the teaching domain, this research proposes a hybrid teaching methodology that makes learning and teaching more efficient, as well as a methodology for a structured integration of learning by teaching by including students in the learning-material creation.

3.5 Miscellaneous

3.5.1 Federated Learning and Network Security: Foundations, Potential, and Resilience

Participants: Léo Lavaur, Yann Busnel.

Published in the 45th IEEE International Conference on Distributed Computing Systems (ICDCS) [18]

Federated Learning (FL) is a distributed learning paradigm that enables training models across distributed clients without accessing their data. In the context of network security, FL can be used to collaboratively train Intrusion Detection System (IDS) models across multiple organizations, allowing participants to share knowledge without compromising data privacy. However, the distributed nature of FL raises new challenges, notably the heterogeneity of clients' data distributions and the identification of malicious contributions.

This three-part tutorial introduces the audience to (i) the principles of FL, (ii) its application to network security, focusing on building Collaborative Intrusion Detection Systems (CIDSs) using FL, and (iii) the security challenges associated with deploying Federated Intrusion Detection System (FIDS), with a focus on poisoning attacks. Each part is illustrated with hands-on exercises, with step-by-step instructions provided in the companion material..

3.5.2 drone-trajectory-prediction

AI algorithm for predicting and optimizing trajectory of massive UAV swarm

Participants: Amit Raj, Kapil Ahuja, Yann Busnel.

Published in Robotics and Autonomous Systems, 2025, 186, pp.104910 [6]

This work explores the application of Artificial Intelligence (AI) techniques for generating the trajectories of massive swarm of Unmanned Aerial Vehicles (UAVs). The two main challenges addressed include accurately predicting the trajectories of UAVs and efficiently avoiding collisions between them, which we discuss in the two paragraphs below, respectively. In previous works that did trajectory predictions, a Neural Network (NN) was used. The activation functions used were all standard like Sigmoid, Tanh, and ReLU, which resulted in low trajectory prediction accuracy. In this work, we apply application-oriented activation functions of Swish and Elliott that are known to be resilient to noisy data, which is common in UAV trajectory prediction. We also propose our new activation function, AdaptoSwelliGauss that is fusion of Swish, Elliott and a scaled and shifted Gaussian. This combination better captures the complexities of UAV trajectory prediction (noisy data as well as non-linear trajectory). The trajectory prediction accuracy obtained with our new activation function is three to four orders-of-magnitude better than that obtained from the standard activation functions. In the UAV context, collision detection and avoidance of UAVs is of utmost importance. While there is a common standard for collision detection, collision avoidance can be done by multiple methods. The first method is by changing their trajectories

and the second method is by changing their start times (called batching). When we try to smoothly change the trajectories, then the algorithm gets complicated and runs into an infinite loop. On other hand, when we apply the batching method to our setup, then the number of batches is large delaying the launch of all UAVs. Therefore, in this paper we propose a novel collision avoidance strategy that combines a new trajectory change method with the batching method. This results in smooth, simple, and finite trajectory changes in the first method, and reduction-by-half in the number of batches in the second method.

3.5.3 Game over... für die Medienkompetenz? Ein Blick auf generative KI und Echo-Oasen

Participants: Marc-Oliver Pahl.

Published in Informatik Radar Gesellschaft für Informatik [5].

Game over for our information society? While generative AI levels up from one stage to the next, media literacy seems unable to keep pace. Why this is the case—and what must be considered in the race to catch up—is explored by our author through a journey into the "Echo Oasis."

3.5.4 Multi-Partner Project: CyberSecDome-Framework for Secure, Collaborative, and Privacy-Aware Incident Handling for Digital Infrastructure

Participants: Mohammad Hamad, Michael Kühr, Haralambos Mouratidis, Eleni-Maria Kalogeraki, Christos Gizelis, Dimitris Papanikas, Athanasios Bountioukos-Spinaris, Charilaos Skandylas, Evangelos Raptis, Andreas Alexopoulos, Grigorios Chrysos, Mina Marmpena, Sevasti Politi, Konstantinos Lieros, Papagiannopoulos Nikolaos, Iordanis Xanthopoulos, Spyros Papastergiou, Sotiris Ioannidis, Mikael Asplund, Marc-Oliver Pahl, Sebastian Steinhorst.

Published in 2025 Design, Automation & Test in Europe Conference (DATE) [14].

Digital infrastructure is vital for the economy, democracy, and everyday life, yet it is becoming increasingly vulnerable to strategic cyber-attacks. These attacks can lead to significant disruptions, resulting in widespread service outages, financial losses, and a decline in public trust. Ensuring resilience is difficult due to the infrastructure's complexity, the large volume of data involved, and the growing need for quick, coordinated responses. In the EU Horizon project CyberSecDome, we propose a multi-layered framework that provides AI-driven solutions for incident prediction and detection, automated testing, risk assessment, and rapid incident response, supporting continuity amid complex, large-scale cyber threats. Additionally, Cyber-SecDome introduces a virtual reality interface to enhance AI model explainability and provide real-time contextual awareness of ongoing attacks and defense mechanisms. It also enables privacy-aware model sharing across AI systems, fostering secure collaboration among different domes.

4 Software development

4.1 Software Development

Most of our research code is being made available through `https://gitlab.inria.fr/sotern/` for reproducibility purposes. The team contributed to the following pieces of software. This section is organized in two subsections, the first presents the platforms that have been updated or created in 2025, and the second lists those which have not been modified during this period.

4.2 Updated and New Platforms

4.2.1 Analysing and Blocking Fast Spreading Malwares

Participants: Anh Nguyen.

This platform is composed of a hypervisor (GNS3) in which a LAN is deployed, to which several Virtual Machines (VM) are connected. Those VMs run a Windows version vulnerable to the eternal blue exploit. One of the VM executes the Wannacry malware to enable its propagation in the virtual network. The VMs are instrumented to analyze the malware behavior.

A subpart of the platform has been initially used to study the propagation speed of Wannacry on a virtualized LAN with 100 VMs. The latest experiments consisted in precisely analyzing the malware behavior to construct a statistical model of the propagation mechanism. This model is to be used in a simulation environment to test the malware behavior at large scale, i.e Internet scale.

repository URL: `https://gitlab.inria.fr/sotern/malware-spreading`

Another subpart of the platform is used to test an intrusion detection approach to block fast spreading malwares. It uses an opportunistic approach to enable fast and decentralized communications between IDS and firewalls deployed in the network. The deployment is based on a vertex coverage analysis. Micro-kernels are used to implement the IDS and firewalls.

repository URL: `https://gitlab.inria.fr/sotern/opportunistic-reaction`

4.2.2 DatasetGen

Participants: Fabien Autrel.

DatasetGen, which has been used within the context of Léo Lavaur's PhD thesis, can be used to generate datasets which are used to evaluate federated approaches to intrusion detection. This tool generates random network topologies on a virtualization environment, execute attacks as well as life generators, capture network traffic, and labelize it. The random generator is seeded to make the topology generation reproducible. The tool is written in Python and interacts with the Airbus Cyberrange virtualization platform to instantiate the topologies. The tool abstracts the virtualization platform, so that in

the future, other virtualization backend can be used, such as. KVM. A library of sub-topologies, each one consisting of virtual machines and containers connected together to the same subnet, is used by the tool to generate various combinations, i.e. the sub-topologies are combined to instantiate bigger topologies. Each sub-topology contains a router, which is then connected to a unique subnet during topology generation. The attacks currently supported by DatasetGen are network attacks: bruteforce on various network services (FTP, SSH, Mysql, RDP, SMB, Telnet, VNC), DoS attacks (ICMP and IGMP flooding, RUDY, DNS amplification, SYN flood, UDP flood), port scans. The tool also uses several life generators to generate normal traffic (DNS, FTP, HTTP, SMTP, SSH, Syslog).

repository URL: `https://gitlab.inria.fr/sotern/topology-generator`

4.2.3 JudgeGPT

Participants: Marc-Oliver Pahl.

In today's world, fake news spreads faster than ever before, impacting everything from public opinion to election outcomes. Whether it is the U.S. elections or Germany's upcoming ones, misinformation is reshaping the way people think, talk, and vote. The CNI Chair created JudgeGPT—a free tool designed to put your news-detecting instincts to the test. This tool gives you real and fake news snippets to evaluate, including computer- and human-generated content. The responses will help researchers of the research group understand how people interpret news content, especially leading up to important election.

repository URL: `https://judgegpt.streamlit.app/`

4.2.4 Eiffel

Participants: Léo Lavaur.

Eiffel is a Python library that provides a set of tools to automate the evaluation of FL algorithms, such as instantiating various types of data distribution, local models, and aggregation strategies. It further provides multiple label-flipping attacks, and automates metric collection and plotting to quickly evaluate the impact of each parameter.

repository URL: `https://gitlab.inria.fr/sotern/eiffel/`

4.2.5 Dissecting 5G New-Radio Latency: Interacting Layers and Latency-Generating Operations: Code and Data.

Participants: Hamici-Aubert Virgil.

This source code and data [27] goes with the paper: Virgil Hamici-Aubert, Julien Saint-Martin, Renzo E. Navas, Georgios Z. Papadopoulos, Guillaume Doyen, Xavier Lagrange "Dissecting 5G New-Radio Latency: Interacting Layers and Latency-Generating Operations", accepted for publication in the Workshop SLICES at IFIP Networking 2025[15].

Code and Data URL: `https://zenodo.org/records/15377254`

4.2.6 Industrial IoT cybersecurity: a bibliometric analysis (code and data)

Participants: Dasso Ignacio.

This release [26] represents the code development used in the development of the following article: Ignacio J. Dasso, Sébastien Maudet, Renzo E. Navas, Guillaume Andrieux, "Industrial IoT cybersecurity: a bibliometric analysis," in Proceedings of the 10th International Conference on Smart and Sustainable Technologies (SpliTech), Split, Croatia, June 2025.[12].

Code and Data URL: `https://zenodo.org/records/15305102`

4.2.7 [DATA] ibIDS - A dataset of real-world network communication and user physical contextual data

Participants: Nguyen Van-Tien.

This [29] is a novel dataset that integrates both synthetic attack traces and real-world benign behaviour. Specifically, the malicious data is sourced from the widely referenced CIC-AndMal2017 dataset, while the benign data (ibIDS) is collected through our in-situ data acquisition process using a real Android device. [21].

Data URL: `https://zenodo.org/records/17174335`

4.3 Legacy platforms

4.3.1 Software repository: Automation framework software

Participants: Renzo Navas.

This deliverable [28] reports the content of two software repositories which contain software codes developed in the INTELLIGENTSIA project. The first software repository implements multi-arm bandit algorithms for spreading factor (SF) selection in LoRaWAN networks. This repository includes: (i) source codes used to generate the experimental results associated to a published paper related to the project, (ii) the data of the experiments, and (iii) some useful scripts used to compute metrics and generate plots. The second software repository is related to a LoRaWAN emulator, called ELoRa, developped in the project. This tool allows to emulate LoRaWAN traffic compatible with two widespread open-source implementations of a real LoRaWAN server stack, ChirpStack and The Things Stack. This repository includes: (i) source codes of the tool, (ii) a documentation to install the tool, and (iii) examples to use the tool.

Code and Data URL: `https://zenodo.org/records/7876244`

4.3.2 I2NSF policy conflict detection and mitigation implementation

Participants: Anh Nguyen.

The Interface to Network Security Function (I2NSF [HLZ+17]) is the result of an IETF working group which defines a set of software interfaces and data models for controlling and monitoring physical and virtual NSFs, enabling clients to specify rulesets, or more formally security requirements, i.e. DatasetGensecurity policies. In [**?**], we proposed an approach to detect and mitigate policy conflicts, which has been implemented as a extension to the reference implementation[2] of the I2NSF specification. The implementation of this approach consists in two additional modules to the original I2NSF implementation:

- Real-time conflict checker: this module exhaustively finds all the conflicts in a policy given as an input
- Separation Constraint and Partial Ordering Relationship checker checker: this module takes as an input the set of separation constraints and rule ordering relationships to check if they eliminate all the detected conflicts.

The python code consists in 302 lines of code added to the security controller.

repository URL: `https://gitlab.inria.fr/sotern/i2nsf-conflicts`

5 Contracts and collaborations

5.1 International Initiatives

5.1.1 CyberSecDome

Participants: Marc-Oliver Pahl, Fabien Eyssartier.

- Project type: Horizon Europe
- Dates: 2023–2026
- PI institution: Marc-Oliver Pahl
- Other partners: Maggioli Spa, Technische Universitaet Muenchen, Airbus Cybersecurity Sas, Athens International Airport S.A., EIT Digital, Organismos Tilepikoinonion Tis Ellados OTE AE, Institut Mines-Telecom (IMT Atlantique), Linkopings Universitet, Aegis IT Research GmbH, Security Labs Consulting Limited, Erevnitiko Panepistimiako Institouto Tilepikononiakon Systimaton, Cyberalytics Limited, Iotam Internet of Things Applications and Multi Layer Development Ltd

[2] See `https://github.com/jaehoonpaul/i2nsf-framework`

[HLZ+17] S. Hares, D. Lopez, M. Zarny, C. Jacquenet, R. Kumar, J. P. Jeong, "Interface to Network Security Functions (I2NSF): Problem Statement and Use Cases", RFC 8192, RFC Editor, *Request for Comments*, 8192, July 2017, `https://www.rfc-editor.org/info/rfc8192`.

Organisations across the sectors are significantly benefited with the digital transformation to support evolving business models, services and customer experience. Despite of the benefits of Digital Infrastructure adoption, there are numerous security challenges that could pose any digital disruption and risks for the critical service delivery and overall business continuity. There is a need to understand the overall digital infrastructure context and analyse and predict the possible threats and incident in real time so that quick and accurate responses can be taken into consideration for ensuring resilience of service delivery. Additionally, collaborative response and sharing of threat intelligence information is necessary to create overall awareness and increase the response capability of all stakeholders within the ecosystem. In this proposal, CyberSecDome project will integrate advanced virtuality reality to extend the capability of the security solutions aiming to enhance security , privacy and resilience of the Digital Infrastructure. The project will consider AI enabled security solutions to provide a better prediction of cybersecurity threats and related risks towards an efficient and dynamic incident management and optimise collaborative response among the stakeholders within the Digital Infrastructure ecosystem. CyberSecDome project is built on a collaboration of 15 organisations from 6 EU member states (IT, DE, IE, SE, EL, CY) and 2 affiliated countries (UK, CH) which is composed by 5 industrial partners , 6 scientific partners and 5 SMEs. The project will be coordinate by MAGGIOLI SPA one of the industry partners who has extensive experiences in designing and managing national and international R&D projects.

5.2 National Initiatives

5.2.1 Towards Public Blockchain for Self-Sovereign Identities – BC4SSI

Participants: Romaric Ludinard, Loïc Miller, Dorian Pacaud.

- Project type: ANR JCJC
- Dates: 2023–2027
- PI institution: Romaric Ludinard
- Other partners: Emmanuelle Anceaume from PIRAT\')/IRISA – UMR CNRS 6074 team

Digital identity is the foundation of trust. It is traditionally managed centrally within a given perimeter. On the contrary, Self-sovereign identities are digital identities that are managed in a decentralized manner. This technology allows users to self-manage their digital identities without depending on third-party providers to store and centrally manage the data, including the creation of new identities. However, these identities are more than simple identifiers: they need to be checked by the service provider via, for instance, verifiable claims. Public Blockchain technology is a strong candidate to deploy SSI and store verifiable claims. Blockchain is indeed an extremely clever assembly of simple technological bricks, and according to the model assumptions, their combination gives rise to a large panel of blockchains. BC4SSI aims at studying and developing new public Blockchain paradigm to handle SSI with the weakest model assumptions.

5.2.2 Superviz

Participants: Fabien Autrel, Ahmed Bouabdallah, Guillaume Doyen, Anh Do Duc Nguyen, Gilles Guette.

- Project type: Priority Program and Equipment for Research (PEPR) Cybersecurity
- Dates: 2022–2029
- PI institution: Guillaume Doyen
- Other partners: INRIA, Centrale-Supelec, Université de Rennes, CEA, CNRS, Université de Lorraine, Grenoble INP, Eurecom

The SuperviZ project contributes to the field of "systems, software and network security". More precisely, it targets the detection, response and remediation of computer attacks, subjects grouped under the name "security monitoring". Security monitoring faces significant challenges, with the increase in the number of components to monitor and the increasing heterogeneity of the capabilities of these components (servers, personal computers, tablets, telephones, various objects) in terms of communication, storage and calculation.

5.2.3 NF-HiSec

Participants: Fabien Autrel, Grégory Blanc(Télécom SudParis), Ahmed Bouabdallah, Guillaume Doyen, Issam Ikhelef.

- Project type: Priority Equipment and Program for Research (PEPR) 5G
- Dates: 2022–2026
- PI institution: Guillaume Doyen
- Other partners: Télécom Paris, Télécom SudParis, Eurecom, Mines Saint Étienne, CEA, INRIA, Université de Nantes, Université de Limoges, LAAS, ETIS

The HiSec project focuses on cyber-security issues in future networks. These networks have played a key role in service delivery for digital infrastructures. These new networking technologies have also penetrated essential and critical services for our daily lives, such as energy, transportation or healthcare. The pervasive use of digital services and networks to control these critical infrastructures significantly increases the attack surface and the opportunities for attackers. We regularly observe attacks against these infrastructures, leading to successful compromise and very significant impacts. The objective of the NF-HiSec project is thus to handle cybersecurity issues in these environments, and propose new mechanisms to protect these networks and detect attacks, attacks against the networking infrastructure itself, or against the services hosted or the users of the network.

5.2.4 Toward context aware Security for Individual Information Systems

Participants: Van-Tien Nguyen, Renzo E. Navas, Guillaume Doyen.

- Project type: Co-founded by ICO (Institut Cybersécurité Occitanie) (LAAS side) and a Carnot TSN Grant (IMT Atlantique side)
- Dates: 2022–2026
- PI institution: Guillaume Doyen
- Other partners: Eric Alata and Daniela Dragomirescu (LAAS/CNRS)

For a few decades, the multiplicity of Internet services humans consume are increasing, leading people to actually manage their own Individual-oriented Information System (IIS), whose server sides are spread over the internet and operated by different service providers. The security of such systems is essentially service-centric while the user is the focal point of all their usage. If some user-centric solutions exist to date, they are either (1) restricted to some particular services, ignoring a global user activity, (2) intrusive, by requiring a complete instrumentation of user-side terminals, or (3) too specific by requiring the cooperation between the client interface and the server side. To cope with these limitations, we propose to develop a novel approach which consists in monitoring encrypted network flows issued by a user terminal and correlating this network activity with some external contextual information related to the user activity. Due to the lack of existing comprehensive datasets, our ongoing work consists in designing a long-term measurement campaign with real users using smartphones augmented with body sensors while facing security breaches such as malware activity or smartphone theft.

5.2.5 BPI 5G Metavers (2023 - 2026)

Participants: Renzo E. Navas, Guillaume Doyen, Virgil Hamichi (OCIF).

- Project type: BPI 5G Metavers
- Dates: 2023–2026
- PI institution: Georgios Papadopoulos
- Other partners: Georgios Papadopoulos (OCIF), Xavier Lagrange (ADOPNET), Julien SAINT MARTIN (ADOPNET)

Low latency and high throughput are two requirements for Metaverse applications on 5G networks (and beyond). The term Mobile Broadband Reliable Low Latency Communication" (MBRLLC) sums up these requirements for these future applications. At the same time, these 5G networks are the target of attacks; in particular, several attacks target the Radio Access Network (RAN) part, i.e., the part closer to the user equipment (UE) and -potentially- impact MBRLLC guarantees. In this context, it is proposed to study synthetic MBRLLC traffic between UEs and a 5G base station (eNB) in the context of adverse behavior whose aim is to disrupt the Quality of Service (QoS)/Quality of Experience (QoE) of the MBRLLC flow, thus harming the availability of the service offered. After selecting and implementing these attacks from the state of the art, our work will focus on the defensive aspect. To this end, countermeasures will be proposed,

implemented, and evaluated in the platform. At least one countermeasure will be put forward.

5.2.6 Realtime AI-Based Power Assisted Malware Predictor

Participants: Yehya Nasser(external), Saoudi Samir(external), Marc-Oliver Pahl.

- Project type: Creach Labs PhD Grant
- Dates: 2023–2026
- PI institution: Marc-Oliver Pahl

Malicious software is considered as a critical security problem in modern computational systems. Detection of malware in these systems is emerging as an effective solution to increasing security threats. Anti-virus software is not enough to detect malware, especially with the advancement of malware evasion techniques that integrate new obfuscation features. Recent research outcomes show the importance of exploiting hardware features such as hardware performance counters (HPCs) and power consumption in hardware security. In this project, we propose a real-time power assisted AI-based malware detection for modern processors integrated in the Industrial Internet of Things (IIoT). In-depth analysis of the practicalities of integrating the power consumption profiles and execution performance (of an application running on a processing system) in malware detection AI models on emerging RISC-V ISA (Instruction Set Architecture) will be conducted. In parallel, deep learning (DL) will be used for malware analysis, binary (malware-benign) classification and malware family classification. DL was found efficient to replace manual feature engineering (e.g., Malconv). The advantage of DL is that it can consume raw malware data, including hardware features such as power consumption and software features such as execution performance indicators.

5.2.7 AI against AI: AI-based Side-Channel Attacks Against AI SoC

Participants: Yehya Nasser (external), Amer Baghadi (external), Marc-Oliver Pahl.

- Project type: TSN Carnot Futures & Ruptures
- Dates: 2023–2026
- PI institution: Marc-Oliver Pahl

Artificial Intelligence (AI) is showing tremendous success in almost every application field. Similarly, the emerging open source instruction set architecture (ISA) RISC-V processor is gaining huge attention in both academia and industry to become the backbone of future embedded systems. Recent RISC-V development efforts embrace Machine learning (ML), Deep Learning (DL), and other high-performance embedded applications. Studying and analyzing the security vulnerabilities of RISC-V running AI-based applications is an active research area. Most recent works target side-channel attacks on microprocessors and RISC-V in particular irrespective of the application running on

top. It is imperative for the low-level security analysis to consider the high-level application. In this research proposal, we intend to investigate AI-based side-channel attacks against AI system-on-chip based on RISC-V. The project has the following objectives: 1) to review the hardware-based attack techniques that aim at leaking or corrupting an AI application; 2) to showcase real attacks against selected neural networks architectures; and 3) to propose original solutions stemming from hardware security for securing AI-based applications.

5.3 Bilateral industry grants

5.3.1 Cyber CNI: Chaire Cybersécurité des Infrastructures Critiques – Phase 4

Participants: Marc-Oliver Pahl.

- Project type: Industrial Research Chair
- Dates: 2025–2027
- PI institution: Marc-Oliver Pahl
- Other partners:, Télécom Paris, Télécom SudParis, Airbus, EDF

The Cyber CNI Chair at IMT Atlantique is devoted to research, innovation, and teaching in the field of the cybersecurity of critical infrastructures, including industrial processes, financial systems, building automation, energy networks, water treatment plants, transportation. The chair covers the full stack from sensors and actuators and their signals over industrial control systems, distributed services at the edge or cloud, to user interfaces with collaborative Mixed Reality, and security policies. The chair currently hosts 6+3 PhD students, 1+3 PostDocs, 11 Professors, 1+1 engineers, and 1 internship student. The chair runs a large testbed that enables applied research together with the industry partners. The chair is located in Brittany, France. Brittany is the cybersecurity region number 1 in France. The chair Cyber CNI is strongly embedded in the cybersecurity ecosystem through its partnerships with the Pôle d'Excellence Cyber (PEC) and the Brittany Region.

5.3.2 AI@IMT

Participants: Antoine Rebstock, Yann Busnel, Romaric Ludinard.

- Project type: research action between IRT b<>com and IMT Atlantique, cofunded by ANR within the project AI@IMT
- Dates: 2021–2025
- PI institution: Yann Busnel
- Other partners: The project involves several researchers from the overall Institut Mines-Télécom. For this workpackage, several faculties from IMT Atlantique are involved (Patrick Maillé (Inria / Ermine) and Romaric Ludinard) and involves the work of several PhD students.

The objective is to carry out common research on the usage of AI in Cybersecurity for Networking context. Despite the progress made in recent years in the detection of Advanced Persistent Threat (APT) attacks, it does not exist a fully solution today. To solve this problem, researchers have relied on different methods. The most promising is the similarity-based method as it is well adapted to the detection of unknown attacks. Moreover, the existing solutions share some limitations, sometimes induced by the data representation used. To encounter this issue we propose a graph-based approach to represent the interactions between the hosts of a network, taking into account both their localisation, their temporality and their relationships with other interactions.

5.4 Collaborations

5.4.1 Dipartimento di Automatica e Informatica, Politecnico di Torino

Participants: Pierre Alain, Guillaume Doyen.

- Other partners: Daniele Bringhenti, Riccardo Sisto, Fulvio Valenza

We continued a research collaboration with the netgroup team in the Dipartimento di Automatica e Informatica at Politecnico di Torino on the field of intent-based security solutions. In this collaboration, we co-supervised an internship on the intent translation from the Nile language to structured files for the VEREFOO tool. By focusing on intent-driven security, we seek to develop more autonomous and resilient cybersecurity systems. Through this collaboration, we look forward to combining expertise, and driving research that addresses emerging security challenges in networks.

5.4.2 Concordia Institute for Information Systems Engineering

Participants: Guillaume Doyen.

- Other partners: Y. A. Joarder (PhD student), Carol Fung

This collaboration is grounded by a common work on the QUIC protocol security. Formerly, the SOTERN research group worked on how Explicit Congestion Notification (ECN) can be leveraged to implement Reduction of Quality (RoQ) Denial of Service attacks while Concordia worked on QUIC security. The collaboration topic focuses on how a selfish user can take profit of Congestion Control Algorithms (CCA) located in the user space of QUIC to hack the CCA parameters and steal bandwidth to legitimate users. An empirical study conducted at Concordia and co-directed by researchers from both sides has conducted to a publication in CNSM 2025 [16].

5.4.3 IETR Lab/Nantes Université joint PhD (2023 - 2027)

Participants: Renzo E. Navas.

- Project type: Co-founded between Région des Payes de la Loire and IETR UMR 6164 (team SIGNAL)
- Dates: 2023–2027
- PI institution: Renzo E. Navas
- Other partners: Guillaume Andrieux, Sébastien Maudet, Ignacio José Dasso (Nantes University, IETR Lab team SIGNAL).

This work is in the context of Industrial IoT (IIoT) networks. At the network level and in a simplified manner, the IoT architecture can be broken down into three layers: the perception layer (physical, device), the network layer (MAC, transport, etc.) and the application layer. The first objective of this work will be, through a state of the art, to identify existing threats on IoT networks by specifying which layer(s) they impact. The threats can be external or internal (coming from a sensor already present and registered on the network but faulty). A specific attack, impacting at least the network layer, will be highlighted among these threats and the security solutions responding to it will be identified and studied. Once attacks on IoT networks and security solutions have been identified, the study can focus on a specific IoT network (LoRa, Wi-Fi Halow, IEEE 802.15.4, etc.). Real equipment can be used to assess the impact of attacks and verify the robustness of existing solutions. Depending on the results obtained, a second objective will be to propose and implement i) an improvement of the contributions considered and/or ii) a new approach dealing with security. The PhD candidate is Ignacio José Dasso (IETR, SIGNAL) and the thesis subject is *Study and impact of IoT network security in Industry 4.0.*. Co-supervised with Guillaume Andrieux and Sébastien Maudet (Nantes University, IETR Lab team SIGNAL).

5.4.4 INSA Lyon / Inria (Team AGORA) & Université du Luxembourg

Participants: Yann Busnel.

- Other partners: Hervé Rivano (INSA Lyon, leader of Inria AGORA team), Léo Lavaur (Université du Luxembourg)

This collaboration builds on shared interests in wireless network security and distributed protocols, with a focus on the resilience of large-scale IoT deployments. While the SOTERN team has developed expertise in real-time anomaly detection and data-driven security mechanisms, Hervé Rivano's group at Inria specializes in network protocol design and adversarial robustness in constrained environments. Our joint work investigates how malicious actors can exploit vulnerabilities in low-power wireless protocols (e.g., 6TiSCH or LoRaWAN) to disrupt or manipulate data flows, particularly in critical infrastructure scenarios. A recent empirical study, co-supervised by both teams, is going to led to publications, highlighting improving the use of broadcasting in wireless communications for federated learning.

6 Dissemination

6.1 Promoting scientific activities

6.1.1 Scientific Events Organization

General Chair, Scientific Chair

Romaric Ludinard and Guillaume Doyen served as General Chairs of the 10èmes Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI'25).

Member of the Organizing Committees

Guillaume Doyen served as an Organization Committee member of IEEE International Conference on Network Softwarization - Netsoft 2025 as a PhD Symposium co-chair.

Pierre Alain served as a:

- Member of Organization Committee member of the 10èmes Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI'25)
- Shepherd of the PhD track of the 10èmes Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI'25).

Marc-Oliver Pahl served as an Organization Committee member of:

- IFIP/IEEE International Network Operations and Management Symposium - NOMS 2025 (Workshop Co-Chair)
- Computer & Electronics Security Application Rendezvous - C&ESAR (OC and TPC member)
- 5th IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT) co-located with NOMS 2025 (General Chair)
- Computer & Electronics Security Application Rendezvous - C&ESAR

Renzo E. Navas served as an organization committee member of the 5th IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT) co-located with NOMS 2025 (manage-IoT'25).

6.1.2 Scientific Events Selection

Chair of Conference Program Committees

Renzo E. Navas served as a TPC chair of the 5th IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT) co-located with NOMS 2025 (manage-IoT'25).

Yann Busnel served as a TPC Demo Chair at the 45th IEEE International Conference on Distributed Computing Systems (ICDCS 25).

Member of Conference Program Committees

Msrc-Oliver Pahl served as an Program Committee member of:

- IFIP/IEEE International Network Operations and Management Symposium - NOMS 2025
- IFIP/IEEE International Conference on Network and Service Management - CNSM 2025
- Track Co-Chair, KES 2025 Session: Detection of Complex Attacks through Advanced Learning Models, International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, KES
- Computer & Electronics Security Application Rendezvous - C&ESAR

Pierre Alain served as a Program Committee member of the 7th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft) (SECSOFT'25).

Guillaume Doyen served as an Program Committee member of:

- IEEE International Conference on Network Softwarization - Netsoft 2025
- IFIP/IEEE International Network Operations and Management Symposium - NOMS 2025
- IFIP/IEEE International Conference on Network and Service Management - CNSM 2025
- Computer & Electronics Security Application Rendezvous - C&ESAR

Gilles Guette served as Program Committee member for the following conferences:

- 11th International Conference on Information Systems Security and Privacy (ICISSP'25).
- 8th International Workshop on Emerging Network Security (ENS'25, co-located with ARES).

Romaric Ludinard served as a Program Committee member in the following conferences:

- 27èmes Rencontres Francophones sur les Aspects Algorithmmiques des Télécommunications (AlgoTel'25);
- 7th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS'25);

Reviewer

Pierre Alain served as a reviewer for the following conferences:

- IEEE/IFIP Conference on Network and Service Management, CNSM
- IEEE/IFIP Network Operations and Management Symposium (NOMS'26).
- 7th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft) (SECSOFT'25)
- 11th IEEE International Conference on Network Softwarization (NetSoft)

Gilles Guette served as reviewer for the IEEE/IFIP Network Operations and Management Symposium (NOMS'25).

6.1.3 Journal

Member of the Editorial Boards

Guillaume Doyen served as:

- the lead guest editor of the Springer Journal of Network and System Management - JNSM. Special Issue on Cyber-Security in Software-defined and Virtualized Infrastructures.
- an associated editor of the Springer Journal of Network and System Management - JNSM.

Marc-Oliver Pahl served as:

- Associate Editor, Springer Journal of Network and Systems Management, JNSM
- Associate Editor, ACM International Journal of Network Management, IJNM
- Guest Editor, MDPI Sensors special issue on Cyber Physical System: Security and Resilience Challenges and Solutions, Sensors, (Q1)

Reviewer - Reviewing Activities

Pierre Alain served as a reviewer for the following journals:

- Elsevier Journal Computer Networks, COMNET
- Springer Journal of Network and Systems Management, JNSM

6.1.4 Standards organizations

Responsibilities

Renzo E. Navas is co-chair at the Lightweight Authenticated Key Exchange (lake) IETF Working Group.

Reviewer - Reviewing Activities

Renzo E. Navas is a reviewer at the following IETF Directorates :

- Security Area Directorate (secdir).
- Internet of Things Directorate (iotdir).

6.1.5 Invited Talks

Pierre Alain was invited to give a keynote in the Sosysec (DGA/INRIA) seminar series.

Marc-Oliver Pahl was invited to a:

- Keynote on “The Next Front Line: Resilience of Critical Infrastructure in the Age of AI and Global Tensions”, at the European Cyber Week 2025.
- Keynote on “The Cyber CNI research ecosystem”, at the European Cyber Week 2025.
- Panel on "Intrusion Detection: How to Manage IT/OT Convergence", at the European Cyber Week 2025.
- Panel on "Cyber and AI training", at the European Cyber Week 2025.

6.1.6 Leadership within the Scientific Community

Yann Busnel and Romaric Ludinard are members of the Network and Distributed Systems CNRS Research group (GDR RSD) steering committee.

Yann Busnel served as:

- member of the Scientific Advisory Board for the Cloud, System and Network Programme of the Inria Digital Programmes Agency.
- member of the Scientific Council of CEFIPRA — Indo-French Centre for Promotion of Advanced Research.

Guillaume Doyen served as:

- the chair of the Rendez-vous de la Recherche et de l’Enseignement de la Sécurité des Systèmes d’Information - RESSI Steering Committee.

- the co-chair of the IMT Digital Trust Community.

Marc-Oliver Pahl served as:

- Steering committee member of the German-French Academy for the industry of the future (GFA).
- Member of the expert council of the LAB-Cyber at the Campus Cyber, Paris.

6.1.7 Scientific Expertise

Pierre Alain and Romaric Ludinard served as ANR Reviewers at ANR.

6.1.8 Research Administration

Guillaume Doyen served as:

- the chair of the Scientific, Technological and International Initiative on Cybersecurity at IMT Atlantique.
- a steering committee member of the Sécurité des Systèmes des Logiciels et des Réseaux (SSLR) working group of the Computer Security CNRS Groupement De Recherche (GDR).

Marc-Oliver Pahl served as:

- Director of the chair Cybersecurity for Critical National Infrastructures (Cyber-CNI).
- Member of the administrative council of the Pôle d'EXcellence Cyber (PEC).

Yann Busnel served as:

- Sevnior Vice-President for Research at Institut Mines-Télécom headquarters.
- chairman of the Scientific Advisory Board of EURECOM.
- member of the Scientific Advisory Board of IRSEEM (ESIGELEC laboratory).
- member of the Institut Mines-Télécom Executive Committee.

6.2 Teaching, supervision

6.2.1 Teaching

- Network Security, IMT Atlantique, Mastère Spécialisé, Gilles Guette
- Introduction to Network and System Security, IMT Atlantique, Engineer degree (2nd year), Gilles Guette

- Introduction to cybersecurity, IMT Atlantique, International Master IT, track cybersecurity, Gilles Guette
- Blockchain & Consensus, coopération dans les systèmes distribués, IMT Atlantique, Engineering track, Romaric Ludinard
- Blockchain, EUR Cyberschool, Master 2, Romaric Ludinard
- Systèmes concurrents et répartis, CentraleSupélec, Engineer degree 3rd year, Romaric Ludinard
- Pentest, Guillaume Doyen (responsible for the course, provided by external engineers from SynAckTiv).
- Security Monitoring and Audit, Guillaume Doyen (responsible for the course, provided by external engineers from Orange Cyberdefence and ANSSI).
- Sécurité des réseaux, IMT Atlantique, TAF Cyber, Ahmed Bouabdallah, Guillaume Doyen.
- Sécurité Windows, ENSSAT, Engineer degree (3rd year), Mohammed Nafi
- Mise en oeuvre des réseaux locaux, ENSSAT, Engineer degree (2nd year), Mohammed Nafi
- Réseaux 1, ENSSAT, Engineer degree (2nd year), Mohammed Nafi
- Théorie des langages et compilation, ENSSAT, Engineer degree (2nd year), Mohammed Nafi
- Algorithmique répartie, ENSSAT, Engineer degree (2nd year), Mohammed Nafi
- Introduction à la cybersécurité, ENSSAT, Engineer degree (2nd year), Mohammed Nafi
- Operating Systems, IMT Atlantique, Engineering track and International Master IT (track cybersecurity), Renzo E. Navas and Guillaume Doyen.
- Cryptography Introduction, IMT Atlantique, Engineering track and International Master IT (track cybersecurity), Renzo E. Navas.
- Sécurité des réseaux, IMT Atlantique, Engineering track (Apprentice), Renzo E. Navas.
- Sécurité des applications web, IMT Atlantique, Engineering track and International Master IT (track cybersecurity), Ahmed Bouabdallah , Renzo E. Navas.
- Authentication and Authorization Infrastructures, Universidad de Murcia, Master's Degree in Cybersecurity, Renzo E. Navas
- Informatique et Réseaux, IMT Atlantique, Engineer degree (1st year), Gilles Guette, Renzo E. Navas, and Guillaume Doyen
- Cybersecurity of Critical Infrastructures, EUR Cyberschool, Master 2, Marc-Oliver Pahl
- Cybersecurity of Embedded Systems, IMT Atlantique, TAF IoT and 5G, Marc-Oliver Pahl

6.2.2 Supervision

- PhD 2022-: Van-Tien Nguyen, *Intrusion detection using body measures to protect individual-based information systems*, supervised by Renzo E. Navas, Guillaume Doyen, and Eric Alata (LAAS/INSA Toulouse).
- PhD 2022-: Anh Do Duc Nguyen, *Opportunistic Microservices for fast Mitigation of Attacks*, supervised by Pierre Alain, Ahmed Bouabdallah, Fabien Autrel and Jérome François (SNT, Luxembourg)
- PhD 2022-2025: Antoine Rebstock, Extraction of probable scenarios by correlation of alerts, supervized by Yann Busnel and Romaric Ludinard.

- PhD 2022-2025: Pierre-Marie Lechevalier, *Ensuring trust and security in the composition of distributed network services and functions*, supervized by Yann Busnel, Géraldine Texier, Romaric Ludinard and Hélène Le Bouder.
- PhD 2023-: Mathis Durand, *Real-world detection and mitigation of AI-based cyberattacks and defence mechanisms*, co-supervised by Marc-Oliver Pahl, Yvon Kermarrec (Lab-Sticc).
- PhD 2023-: Virgil Hamichi, *Protection of Quality of Service and Experience against attacks targetting Metaverse-like Traffic in 5G Networks*, supervised by Renzo E. Navas, Guillaume Doyen, Xavier Lagrange (ADOPNET/IRISA), and Georgios Papadopoulos (OCIF/IRISA).
- PhD 2024-: Ignacio J. Dasso, *Study and impact of IoT network security in Industry 4.0.*, supervised by Renzo E. Navas, Guillaume Andrieux (SIGNAL/IETR – Nantes Université) , and Sébastien Maudet (SIGNAL/IETR – Nantes Université).
- PhD 2024-: Gabriel Bourgeois, *Security of Time Sensitive Networking*, supervised by Mohamed Aymen Chalouf, Guillaume Doyen, and David Espes (Lab-Sticc).
- PhD 2024-: Hugo Bourreau, *Modular Digital Twin-based cyber resilience*, co-supervised by Marc-Oliver Pahl, Fabien Dagnat (Lab-Sticc).
- PhD 2024-: Constant Rohmer, *Towards robust, reliable and high-performance self-protection for connected systems: an approach based on blockchain and microservices*, supervised by Pierre Alain, and Mohamed Aymen Chalouf.
- PhD 2024-: Yohann Morel, *Automatic tracking of attackers in an IS and real-time adaptation of the system to make them reveal their TTPs*, coadvised by Gilles Guette, and Valérie Viet Triem Tong (CentraleSupélec).
- PhD 2025-: Daisy Munson, *The control of intents in intent-based security systems*, supervised by Pierre Alain, and Guillaume Doyen.
- PhD 2025-: Juliette Jacquot, *Development of detection models based on foundation models for network analysis using netflow* , supervised by Gilles Guette, Pierre Parrend (EPITA), and Eric Aubourg (CEA).
- PhD 2025-: Luc Bournaud, *Fully-Decentralized Cybr Defense*, co-supervised by Marc-Oliver Pahl, Yvon Kerrmarrec (Lab-Sticc).
- PhD 2019-: Christian Lübben, *Optimizing IoT Smart Spaces using advanced Data Analytics*, co-supervised by Marc-Oliver Pahl, Georg Carle (TUM).
- PhD 2019-: Erkin Kirdan, *Industrial IoT Engineering: Unleashing the Full Potential of Machine-to-Machine Communication Protocols*, co-supervised by Marc-Oliver Pahl, Georg Carle (TUM).

6.2.3 Juries

Marc-Oliver Pahl participated in the jury of:

- Lars Wüstrich, Dr. rer. nat., Technische Universität München, as Zweitgutachter.
- M. Majed JABER, PhD, Université de Strasbourg, as president (and exminer).

Guillaume Doyen participated in the jury of:

- Abdelkader Lahmadi, HDR, at University of Lorraine, as the president.
- Louis Sahi, PhD, at University of Toulouse, as a reviewer.

- Jolahn Vaudey, PhD, at University of Grenoble Alpes, as a reviewer.
- Ines Carole Kombou Sihomnou, PhD, at University of Avignon, as a reviewer.

Gilles Guette participated in the jury of:

- Solayman Ayoubi, PhD, at Sorbonne Université, as the president.
- Sara Chennoufi, PhD, at Télécom Sud Paris, as an examinator.

Romaric Ludinard participated in the PhD jury of Fredéric A. Hayek at University of Clermont-Ferrand, as an examinator.

Yann Busnel participated in the PhD jury of Shubhajit Datta at IIT Kharagpur, as an reviewer.

6.2.4 Responsabilities

- Pierre Alain is member of Conseil de département Réseaux & Télécoms at IUT Lannion.
- Pierre Alain is member of Conseil d'institut at IUT Lannion.
- Gilles Guette is co-Head of the international master IT, track cybersecurity Cybersecurity
- Romaric Ludinard is co-Head of the post-master professional certificate Cybersecurity
- Romaric Ludinard is Deputy head for Education in the SRCD department at IMT Atlantique
- Renzo Navas is co-Head (up until end 2025) of the international master IT, track cybersecurity
- Mohammed Nafi is head of Research Master EUR CyberSchool track, ENSSAT
- Guillaume Doyen is the co-chair Cyber Security TAF (Thématique d'Approfondissement) at IMT Atlantique
- Ahmed Bouabdallah is the co-chair Cyber Security TAF (Thématique d'Approfondissement) at IMT Atlantique
- Marc-Oliver Pahl is director of the chair Cybersecurity for Critical National Infrastructures (CyberCNI) at IMT Atlantique
- Marc-Oliver Pahl is member of the administrative council of the Pôle d'EXcellence Cyber (PEC) at IMT Atlantique
- Marc-Oliver Pahl is president of the German Chapter of the Association of Computing Machinery (ACM)
- Marc-Oliver Pahl is board member of the German Informatics Society (GI).

6.3 Popularization

- Pierre Alain is a core team member of MirageOS.
- Marc-Oliver Pahl animates the public speaker series TALK.CYBER. Since 2021, the TALK.CYBER Speaker series raises awareness and understanding of cybersecurity topics. TALK.CYBERcni.fr fosters a continuous dialog between experts from industry and academia and the general public, including individuals, families, companies from small to large sizes, and public bodies. More info and recordings at `https://TALK.CYBERcni.fr/`.

7 Bibliography

Books and Monographs

[1] M.-O. Pahl, *Secure Distributed Microservice Architectures*, Technische Universität München, 2025.

Articles in referred journals and book chapters

[2] L. Lavaur, Y. Busnel, F. Autrel, "Investigating the Impact of Label-flipping Attacks against Federated Learning for Collaborative Intrusion Detection", *Computers & Security 156*, September 2025, p. 104462, `https://hal.science/hal-05007843`.

[3] C. Lübben, M.-O. Pahl, "Decentralized Anomaly Detection Using Deep Feed-Forward Neural Networks", *International Journal of Network Management 35*, 6, 2025, p. e70032.

[4] D. Munson, P. Alain, G. Doyen, "NEAT: A Nile-English Aligned Translation corpus based on a robust methodology for Intent Based Networking", *Computer Networks*, 2025.

[5] M.-O. Pahl, "Game over… für die Medienkompetenz? Ein Blick auf generative KI und Echo-Oasen".

[6] A. Raj, K. Ahuja, Y. Busnel, "AI algorithm for predicting and optimizing trajectory of massive UAV swarm", *Robotics and Autonomous Systems 186*, 2025, p. 104910, `https://hal.science/hal-04882239`.

Publications in Conferences and Workshops

[7] G. Bourgeois, M.-A. Chalouf, G. Doyen, D. Espes, "Sécurité Des Réseaux TSN : Vulnérabilités et Exploitations Des Mauvaises Configurations", *in : RESSI 2025 : Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information.*, `https://ressi2025.sciencesconf.org/615568`.

[8] H. Bourreau, F. Dagnat, M.-O. Pahl, F. Jaafar, "Enhancing cybersecurity using Digital Twin and AI", *in : RESSI 2025*, 2025.

[9] H. Bourreau, M.-O. Pahl, F. Dagnat, F. Jaafar, "L'Apprentissage Machine au Sein des Jumeaux Numériques pour l'Estimation et la Détection des Menaces", p. 9, 2025.

[10] Y. Busnel, L. Lavaur, P.-M. Lechevalier, R. Ludinard, G. Texier, "Apprentissage fédéré cherche modèles de qualité, bonne réputation exigée", *in : 27ème Rencontre Francophone sur les Aspects Algorithmiques des Télécommunications (AlgoTel)*, Saint Valéry-sur-Somme, France, June 2025, https://hal.science/hal-05034041.

[11] I. J. Dasso, S. Maudet, R. E. Navas, G. Andrieux, "Analyse bibliométrique de la cybersécurité dans l'IoT industriel", *in : RESSI 2025 : Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information.*, CNRS GDR Sécurité Informatique, p. sciencesconf.org:ressi2025:615412, Lanniron, France, May 2025, https://hal.science/hal-04993507.

[12] I. J. Dasso, S. Maudet, R. E. Navas, G. Andrieux, "Industrial IoT cybersecurity: a bibliometric analysis", *in : SpliTech 2025: 10th International Conference on Smart and Sustainable Technologies*, IEEE (editor), *SpliTech 2025*, IEEE, p. #1571125762, Split, Croatia, June 2025, https://hal.science/hal-05039566.

[13] M. Durand, A. Dey, Y. Kermarrec, M.-O. Pahl, "Pouvez-vous détecter le piège? Détection de pots de miel face à l'évolution des tactiques d'évasion", p. 83, 2025.

[14] M. Hamad, M. Kühr, H. Mouratidis, E.-M. Kalogeraki, C. Gizelis, D. Papanikas, A. Bountioukos-Spinaris, C. Skandylas, E. Raptis, A. Alexopoulos *et al.*, "Multi-Partner Project: CyberSecDome-Framework for Secure, Collaborative, and Privacy-Aware Incident Handling for Digital Infrastructure", *in : 2025 Design, Automation & Test in Europe Conference (DATE)*, IEEE, p. 1–7, 2025.

[15] V. Hamici-Aubert, J. Saint-Martin, R. E. Navas, G. Papadopoulos, G. Doyen, X. Lagrange, "Dissecting 5G New-Radio Latency: Interacting Layers and Latency-Generating Operations", *in : 24th IFIP Networking Conference (Networking 2025)*, Limassol, Cyprus, May 2025, https://hal.science/hal-05138315.

[16] Y. A. Joarder, S. Sinha, G. Doyen, C. Fung, "Exploiting Congestion Control Parameter Manipulation in QUIC for Security Implications", *in : 2025 21st International Conference on Network and Service Management (CNSM)*, p. 1–9, 2025.

[17] L. Lavaur, F. Autrel, Y. Busnel, "Constraint-based Network Topology Generation for Evaluating Federated Intrusion Detection Systems", *in : 1st International Workshop on Assessment with New methodologies, Unified Benchmarks, and environments, of Intrusion detection and response Systems (ANUBIS)*, Toulouse, France, September 2025, https://hal.science/hal-05288602.

[18] L. Lavaur, Y. Busnel, "Federated Learning and Network Security: Foundations, Potential, and Resilience", *in : Proceedings of the 45th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW)*, Glasgow, United Kingdom, July 2025, https://hal.science/hal-05288649.

[19] M. Mezaouli, Y. Nasser, S. Saoudi, M.-O. Pahl, "Revealing Embedded System Behaviors: A Comparative Analysis of Power Consumption and Hardware Performance Counters", *in : HS3 2025: 1st Workshop on Hardware-Supported Software Security-Co-located with ESORICS 2025, 25th of September 2025 in Toulouse, FR.*, 2025.

[20] L. Miller, D. Pacaud, N. Derousseaux-Lebert, E. Anceaume, R. Ludinard, "Mining in Logarithmic Space with Variable Difficulty", *in : Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security, CCS*, ACM, 2025.

[21] V.-T. Nguyen, R. E. Navas, G. Doyen, "Towards Context-aware Intrusion Detection in Individual-oriented Information Systems: An Empirical Study on Android Malware", *in : CNSM 2025*, Bologna, Italy, October 2025, https://hal.science/hal-05242246.

[22] D. Pacaud, L. Miller, E. Anceaume, R. Ludinard, "Preuves non-interactives : la nouvelle ère des chaînes compressées", *in : ALGOTEL 2025 : 27èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications*, 2025.

[23] A. Rebstock, Y. Busnel, R. Ludinard, "A Grammar-Driven Approach to Model and Detect APT Attack Sequences", *in : Foundations and Practice of Security - 18th International Symposium*, *FPS*, 2025.

[24] C. Rohmer, P. Alain, M.-A. Chalouf, G. Doyen, "On the relevance of Blockchains for DDoS Mitigation: a Methodological Assessment and Performance Evaluation of Hyperledger Fabric", *in : 34th International Conference on Computer Communications and Networks (ICCCN)*, IEEE, 2025.

[25] C. Rohmer, M.-A. Chalouf, P. Alain, G. Doyen, "Vers une Auto-protection Collaborative des Systèmes Connectés fondée sur la Blockchain et les Microservices Unikernels", *in : RESSI 2025 : Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information.*, `https://ressi2025.sciencesconf.org/615526`.

Miscellaneous

[26] I. Dasso, "Industrial IoT cybersecurity: a bibliometric analysis (code and data)", Zenodo, April 2025, `https://doi.org/10.5281/zenodo.15305102`.

[27] V. Hamici-Aubert, J. Saint-Martin, R. Navas, G. Z. Papadopoulos, G. Doyen, X. Lagrange, "Dissecting 5G New-Radio Latency: Interacting Layers and Latency-Generating Operations: Code and Data.", Zenodo, May 2025, `https://doi.org/10.5281/zenodo.15377254`.

[28] R. E. Navas, A. Aimi, "Software repository: Automation framework software", May 2025, `https://hal.science/hal-05091094`.

[29] V.-T. Nguyen, "ibIDS - A dataset of real-world network communication and user physical contextual data", Zenodo, September 2025, `https://doi.org/10.5281/zenodo.17174335`.