UMR IRISA

Activity Report 2024

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
Mohamed Aymen Chalouf, (HDR) Associate professor,	Rennes University
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, 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, *project CyberSecDome*	IMT Atlantique
Sulaiman Mohammad, Research engineer until Aug. 24, *project Chaire Rennes Metropole*	Rennes SoB

Post-doctoral researchers

Elie Chedemail from Nov. 24,	IMT Atlantique
Nisrine Ibadah, from Aug. 22 to Mar. 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

Léo Lavaur, 2020-2024, defended on October, 7th 2024	IMT Atlantique
Antoine Rebstock, 2021-ongoing	IMT Atlantique
Do Duc Anh Nguyen, 2022-ongoing	
Van Tien Nguyen, 2022-ongoing	
Mathis Durand, 2023-ongoing	IMT Atlantique
Hugo Bourreau, 2024-ongoing	IMT Atlantique
Gabriel Bourgeois, 2024-ongoing	Rennes University
Yohann Morel, 2024-ongoing	IMT Atlantique
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-ongoing
Hichem Magnouche (LIST3N – Université de Technologie de Troyes), 2020-ongoing
Awaleh Meraneh (OCIF/IRISA – IMT Atlantique), 2020-2024, defended on May, 24th 2024,
Pierre-Marie Lechevalier (ADOPNET/IRISA – IMT Atlantique), 2021-ongoing
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), 202-ongoing
Virgil Hamici-Aubert (OCIF/IRISA – IMT Atlantique), 2023-ongoing
Ignacio J. Dasso (SIGNAL/IETR – Nantes Université), 2024-ongoing
Menuka Perera Jayasuriya Kuranage (ADOPNET/IRISA – IMT Atlantique), 2021-2024, defended on November, 18th 2024,
Radheshyam Singh (Technical University of Denmark), 2020-2024,
Naoueres Khairallah (SUPCOM Tunis), 2022-2024
Amine Hedfi (SUPCOM Tunis), 2022-ongoing.

Administrative assistant

Sandrine Frouin 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 High-level Security Specification and Enforcement

The relations relating secured networking systems with security operators taking part of the *Human in the loop* question of current research in the field. Indeed, bringing more autonomy through self-protection functions makes the relation and expected operations of the human change. Therefore, we separately study the flow in both direction, from and to human.

Leveraging Natural Language Processing and Generative Neural Networks for Advanced Network Security The Natural Language Processing (NLP) field has deeply evolved in recent years with the raise of neural networks, leveraging their ability to analyze, interpret, and process large volumes of textual and structured data. The approach lies in deep learning, probabilistic modeling, and linguistic analysis, allowing systems to process vast amounts of structured and unstructured network data. Generative neural networks, such as Large Language Models (LLMs) and Variational Autoencoders (VAEs) can model normal network behavior or security intents. Additionally, NLP techniques contribute to security by analyzing textual threat intelligence, classifying malicious communications, and automating the correlation of security alerts. The synergy of NLP and generative neural networks provides a powerful framework for enhancing network security, ensuring adaptive and resilient defense mechanisms against evolving cyber threats.

Formal Derivation of Security Configurations One of the main breach in systems enabling attackers to penetrate or exploit operated networks or services comes from misconfigurations. Our research group addresses this topic under two axes: robustness and timely deployment. Security policies represent for information systems the security regulations they must comply with. When deployed, they are implemented using various security components (e.g. firewalls, access control in operating systems), but are also reflected in the configuration of applications and services. Configuring each of those components directly from security policies expressed in natural language is a very error prone task. Using a formal security model allows the development of an abstract representation which authorizes various useful operations like consistency checking or sound derivations of reified models targeting the low-level configurations. Such a security model requires a description language with a formally defined semantics together with associated logic-based refinement mechanisms. Scalability, as the main weakness of existing methods, is in our context an unavoidable challenge.

2.2.2 Autonomous Security Monitoring

Handling Heterogeneous Inputs in Security Mechanisms In the realm of cybersecurity, the landscape is characterized by a multitude of diverse threats and attack vectors. Recognizing the limitations of traditional approaches that predominantly rely on network-based or host-based anomaly detection, our research endeavors embraces a holistic perspective by incorporating heterogeneous inputs, including biometric data, context-related information (i.e., location, time) and unconventional sources such as sound or current side channels. By integrating these disparate data streams, we aim

to create a comprehensive understanding of system behavior and identify anomalies that may evade detection through conventional means. Leveraging data correlation and fusion techniques, our team explores novel methodologies to amalgamate information from diverse sources, enabling a more robust and adaptive intrusion detection mechanisms which in turn enhance the resilience of critical systems against a broad spectrum of cyber threats.

Scalability of Security Mechanisms In the rapidly evolving landscape of cybersecurity, distributed and collaborative approaches have emerged as indispensable tools in combating increasingly sophisticated threats. Our research teams addresses security and safety issues of distributed components through two orthogonal approaches: knowledge sharing and temporal agreement.

First, the exploration of federated learning methodologies, which enable the collective training of machine learning models across distributed environments without compromising data privacy, is a core research line of the team. To circumvent issues related to data privacy as well as data poisoning, we rely on 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, our research teams 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.

2.2.3 Integrated Security Features

Fast Reactions to Security Breaches The gap time between the detection of an attack and the actual enforcement a reaction, allows fast spreading attacks, such as malware propagation (e.g. *wannacry*) for instance, to make extensive damages. We have measured or retrieved, the configuration and deployment time of some illustrative solutions [BMS+21,LLD+18] from the literature and exhibited their limits in terms of response time. Consequently, the team proposes to fasten the deployment of reaction policies by leveraging (1) micro-services and especially Unikernels [MS13] which can be defined as

[BMS+21] D. Bringhenti, G. Marchetto, R. Sisto, S. Spinoso, F. Valenza, J. Yusupov, "Improving the Formal Verification of Reachability Policies in Virtualized Networks", *IEEE Transactions on Network and Service Management 18*, 1, 2021, p. 713–728.

[LLD+18] D. Lopez, E. Lopez, L. Dunbar, J. Strassner, R. Kumar, "Framework for Interface to Network Security Functions", RFC 8329, RFC Editor, *Request for Comments*, 8329, February 2018, `https://www.rfc-editor.org/info/rfc8329`.

[MS13] A. Madhavapeddy, D. J. Scott, "Unikernels: Rise of the Virtual Library Operating System: What if all the software layers in a virtual appliance were compiled within the

"Single-Purpose Appliances" and could be seen as an easy way to scale networks security horizontally for fast execution time, and (2) opportunistic communications between security micro-services.

2.3 Application Domains

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

Protection of Low-Latency Network and Services We investigated the case of different types of undesirable flows in L4S which can prevent legitimate ones from reaching their latency objectives. We recently transposed this case to 4G/5G networks and studied to what extent an attacker, leveraging the over-shadowing of a base station, is able to strongly impact the latency of a legitimate user equipment. Besides, we are now interested in the case of TSN (Time Sensitive Networking) where attack patterns rather target misconfigurations issues.

Protection of Individual Information Systems People 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. Consequently, 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.

Self-sovereign Identities Self-Sovereign identities [MGGM] (SSI) 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. Blockchain technology is a prime candidate for deploying SSI and storing verifiable claims. We aim at studying the feasibility of Self-Sovereign Identities deployment on public blockchain that will 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.

Security Monitoring of Future Networks The complexity of tools employed by attackers often obscures their traces within legitimate network traffic. Defenders, known as "Blue teams", try to counteract threat actors by sharing tactics, but confidential data limits disclosure. Federated Learning (FL) supports this by sharing local models, creating joint models without compromising privacy. Despite benefits, challenges persist, including potential modifications, susceptibility to adversarial approaches, and issues with poorly curated training datasets.

---

same safe, high-level language framework?", *Queue 11*, 11, dec 2013, p. 30–44, `https://doi.org/10.1145/2557963.2566628`.

[MGGM] A. Mühle, A. Grüner, T. Gayvoronskaya, C. Meinel, "A survey on essential components of a self-sovereign identity", `https://doi.org/10.1016/j.cosrev.2018.10.002`.

Intent-based Security Intent-Based Networking (IBN) seeks to minimize human intervention, reduce errors, and ensure the network dynamically adapts to evolving conditions while meeting performance and security goals. Our work focuses on translating high-level security intents into actionable policies and configurations. Leveraging recent advances with Neural Networks, the system can interpret user intentions expressed in natural language and automatically enforce the necessary security changes. Furthermore, by analyzing monitoring data, the system ensures compliance with specified intents and, when needed, suggests corrective actions to the administrator.

Data Exfiltration using Network Steganography Data exfiltration could have disastrous consequences for a targeted organization (reputation, etc.). On the other hand, network steganography aims to conceal sensitive information by exploiting existing network protocols such as TCP/IP, DNS, HTTP and so on. We examine both methods of data exfiltration based on network steganography and their countermeasures. The main objective is to tackle data exfiltration by developing new and effective detection and prevention approaches by using different tools, such as AI and ML.

Using Generative AI for Disinformation Generative AI has emerged as a powerful tool capable of both creating and combating disinformation. These AI-driven disinformation campaigns exploit natural language processing (NLP) models to produce misleading narratives at scale, making it increasingly difficult for individuals to distinguish between authentic and fabricated content. Conversely, AI is also being developed as a defensive mechanism to detect and mitigate disinformation. Advanced machine learning models analyze textual, visual, and contextual cues to identify inconsistencies, unnatural patterns, and deceptive intent. The integration of AI with blockchain-based verification systems enhances content authenticity by providing immutable proof of origin.

Multi-modal interfaces for Security Operators In the opposite direction, our research team explores to what extent harnessing Virtual Reality (VR) as human-machine communication interface within cybersecurity operations could ease, fasten and make more robust security operations. We aim to enhance situational awareness and facilitate more effective risk analysis for cybersecurity experts in interaction with complex data in a spatial context, enabling rapid decision-making and proactive threat mitigation. Moreover, accessibility and inclusivity in cybersecurity are important and our efforts extend to developing interfaces that enable cybersecurity assessments with ease and confidence.

Modeling Infrastructures for Enhanced Cybersecurity Modeling infrastructures through advanced simulation techniques has become a crucial strategy for threat detection and resilience testing. Two key approaches—honeynets and digital twins—play a significant role in strengthening cybersecurity defenses. These controlled environments provide real-time insights into attack vectors, malware signatures, and intrusion tactics without jeopardizing critical systems. Meanwhile, digital twins offer a more sophisticated, real-time virtual representation of physical infrastructure. Integrating honeynets with digital twin technology creates a dynamic cybersecurity framework that enhances situational awareness,

improves incident response, and fortifies critical infrastructure against evolving cyber threats.

Security of Control and Management Operations Ensuring the security of control and management operations is critical for maintaining the integrity and reliability of modern digital infrastructures. One fundamental aspect is securing software updates, as attackers often exploit vulnerabilities in outdated or improperly authenticated firmware and software. Implementing cryptographic signing, secure boot mechanisms, and end-to-end encryption in update processes helps prevent unauthorized modifications and ensures that only verified code is deployed. Similarly, protocol security plays a vital role in protecting communication channels between control systems, particularly in industrial and critical infrastructure settings. Secure protocols with strong authentication, encryption, and integrity checks help mitigate risks such as man-in-the-middle attacks and command injection.

Smart environments Securing smart environments (i.e. smart cities, intelligent transportation systems, connected healthcare, and automated industrial facilities) requires robust authentication mechanisms, encrypted communication protocols, and continuous monitoring through AI-driven anomaly detection. Implementing Zero-Trust principles ensures that every device and user is verified before accessing network resources, reducing the risk of cyber intrusions. Furthermore, integrating blockchain for data integrity and decentralized identity management enhances trust in connected ecosystems. By prioritizing security alongside innovation, smart environments can achieve resilience against cyber threats while delivering their intended benefits to society.

Critical National Infrastructures Securing Critical National Infrastructures (CNI) requires a multi-layered approach that integrates cybersecurity best practices, physical security measures, and resilient operational frameworks. Strong network segmentation, real-time threat monitoring, and encryption of critical data help prevent unauthorized access and mitigate risks. The adoption of Zero-Trust Architecture (ZTA) ensures that every access request is continuously verified, reducing the risk of insider threats and lateral movement of attackers. Additionally, enhancing security in Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) environments—through secure protocol design, regular patching, and anomaly detection systems—strengthens the resilience of operational technologies.

3 Scientific achievements

3.1 Lightweight Security for IoT Systems leveraging Moving Target Defense and Intrusion Detection

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

Published in the 2024 IEEE/IFIP Network Operations and Management Symposium [19].

As more and more devices have communication capabilities, our world is becoming increasingly interconnected. This paradigm is called the Internet of Things (IoT). Most IoT devices have limitations in memory, computing capacity, and energy, thus making impossible to integrate fully-fledged secured solutions into them. Intrusion Detection Systems (IDS) and Moving Target Defense (MTD) are two acknowledged cyber defense techniques that have attracted researchers' attention but need to fit within the constraints of IoT systems. In this paper, based on our previous MTD work, we propose an in-node MTD strategy exhibiting hybrid (i.e., event- and time-based) movement. We specifically explore the MTD interaction with a lightweight detection mechanism to provide reactive defense on top of the by-design proactive-time-based MTD. We implemented and evaluated our proposal in a real IoT platform exposed to a Reduction-of-Quality (RoQ) attack by measuring the round-trip time and packet-loss rate of the system in four scenarios. Notably, we compared our proposal against a time-based-only MTD alternative, which demonstrates the promising results of our hybrid strategy.

3.2 Protection of Individual Information Systems

3.2.1 Toward Context-aware Security for Individual Information Systems

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

Joint work with Eric Alata and Daniela Dragomirescu from INSA Toulouse/LAAS-CNRS. Published in Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI) 2024 [18].

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.

3.3 Security of E-Health systems

3.3.1 Towards Secure and Privacy Preserving Data Processing in E-Health

Participants: Naoures Khairallah, Aida Ben Chehida Douss, Ryma Abbasi, Mohamed Aymen Chalouf, Omessaad Hamdi.

Joint work with Naoures Khairallah, Aida Ben Chehida Douss, Ryma Abbasi from SUPCOM (Tunis, Tunisia) and Omessaad Hamdi (IEEE member). Published in 2024 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) [10].

Medical data in E-health systems must be accessible at any time and exchanged between stakeholders. Given the highly sensitive nature of this data and the increasing frequency of data breaches, it is crucial to implement strict privacy and security measures. Since patient is considered as the owner of his medical data under laws as the Health Insurance Portability and Accountability Act HIPAA and the General Data Protection Regulation GDPR, he/she must have the right to privacy and to make decisions about sharing sensitive data. On the other hand, the stakeholders with whom the patient will share its information are not similar; each one requires specific data for different purposes. That's why the data transfer should not be performed in the same manner. In this work, we proposed a framework to ensure the security and the privacy of data processing in E-health systems. This framework is based on smart contracts to manage patient consent and traceability of data transfer, as well as mechanisms to classify data and apply the most suitable data masking technique to protect efficiently sensitive information.

3.4 Protection of Low-Latency Networks and Services

3.4.1 Leveraging Overshadowing for Time-Delay Attacks in 4G/5G Cellular Networks: An Empirical Assessment

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 ARES '24: Proceedings of the 19th International Conference on Availability, Reliability and Security [9].

Ensuring both reliable and low-latency communications over 4G or 5G Radio Access Network (RAN) is a key feature for services such as smart power grids and the metaverse. However, the lack of appropriate security mechanisms at the lower-layer protocols of the RAN–a heritage from 4G networks–opens up vulnerabilities that can be exploited to conduct stealthy Reduction-of-Quality attacks against the latency guarantees. This paper presents an empirical assessment of a proposed time-delay attack that leverages overshadowing to exploit the reliability mechanisms of the Radio Link Control (RLC) in Acknowledged Mode. By injecting falsified RLC Negative Acknowledgements, an attacker can maliciously trigger retransmissions at the victim User Equipment (UE), degrading the uplink latency of application flows. Extensive experimental evaluations on open-source and commercial off-the-shelf UEs demonstrate the attack's effectiveness in increasing latency, network load, and buffer occupancy. The attack impact is quantified by varying the bitrate representing different applications and the number of injected negative acknowledgments controlling the attack intensity. This work studies a realistic threat against the latency quality of service in 4G/5G RANs and highlights the urgent need to revisit protocol security at the lower-RAN layers for 5G (and beyond) networks.

3.5 Security Monitoring of Future Networks

3.5.1 RADAR: Model Quality Assessment for Reputation-aware Collaborative Federated Learning

Participants: Leo Lavaur, Yann Busnel, Romaric Ludinard, Marc-Oliver Pahl.

Joint work with Pierre-Marie Lechevalier and Géraldine Texier from IMT Atlantique/IRISA-ADOPNET. Published in the 43rd International Symposium on Reliable Distributed Systems - SRDS 2024, Sep 2024, Charlotte (NC), United States [13].

Cross-silo federated learning (CS-FL) is a distributed learning setting which allows an identified set of organizations to collaboratively train a single global model. Since CS-FL use cases are often heterogeneous, it may be more appropriate to dynamically provide different models to more homogeneous subfederations. In addition, such systems can be undermined by contributions of poor quality, making negligent or even malicious participants critical to consider. However, distinguishing such participants in a heterogeneous context is especially difficult. We present RADAR [13], a novel architecture for CS-FL able to assess the quality of the participants' contributions, regardless of data similarity. RADAR leverages client-side evaluation to directly collect feedbacks from the participants. The same evaluations allow grouping participants according to their perceived similarity and weighting the model aggregation based on their reputation. To evaluate our approach on concrete experiments, we implement a collaborative intrusion detection system (CIDS) scenario and test our architecture in various data-quality settings using labelflipping. Our results confirm that combining clustering and a reputation system succeeds in detecting a wide range of Byzantine behaviors, including colluding attackers, which highlights RADAR's versatility.

3.5.2 A Fuzzy Reputation System for Radio Access Network Sharing

Participants: Romaric Ludinard, Yann Busnel.

Joint work with Pierre-Marie Lechevalier and Géraldine Texier from IMT Atlantique/IRISA-ADOPNET. Published in the 22nd International Symposium on Network Computing and Applications (NCA 2024), Oct 2024, Bertinoro, Italy [14].

5G network slicing allows the coexistence of multiple virtualized networks on the same infrastructure. Leveraging this concept, it becomes possible to create marketplaces where Infrastructure Providers (InPs) lease network resources to different Mobile Virtual Network Operators (MVNOs) while accommodating their specific Quality of Service (QoS) requirements. In addition to the cost criteria, an MVNO choosing between several InP might be interested in evaluating the InPs actual capacity to deliver the expected Service Level Agreement (SLA). Existing 5G literature on trust evaluation is often based on blockchain. While this technology offers transparency and auditability, the inherent consensus mechanism often brings additional costs.

In [14], we propose a distributed reputation system based on fuzzy logic that can provide a robust and dynamic estimation of an InP behavior while respecting the subjective requirements of MVNOs. We evaluate this system in a Radio Access Network

(RAN) sharing simulation and we show that it can redirect MVNO to InP that are capable of meeting their needs. We further test different trust decay strategy in order to find one that is able to both quickly react to a network outage and forgive InP once the punctual outage is solved.

3.5.3 Highlighting the Limits of Federated Learning in Intrusion Detection

Participants: Leo Lavaur, Yann Busnel, Fabien Autrel.

Published in the 44th IEEE International Conference on Distributed Computing Systems (ICDCS 2024), IEEE, Jul 2024, Jersey City, NJ, United States [11].

Federated learning (FL) is a distributed learning paradigm enabling participants to collaboratively train a machine learning (ML) model. In security-oriented tasks, FL can be used to share attack knowledge, without sharing participants' local data. Recent research results reveal that highly heterogeneous data distributions can prevent federations from converging towards an appropriate global model. Moreover, maintaining trustworthiness is challenging, as FL-based collaborative intrusion detection systems (CIDSs) are vulnerable to malicious updates. In [11], we present critical examples of these challenges using a set of standardized public datasets and a dedicated automation tool. We review the impact of heterogeneity using different data-distribution, before looking at a scenario with malicious actors.

3.5.4 Systematic Analysis of Label-flipping Attacks against Federated Learning in Collaborative Intrusion Detection Systems

Participants: Leo Lavaur, Yann Busnel, Fabien Autrel.

Published in the 19th International Conference on Availability, Reliability and Security, Jul 2024, Vienna, Austria [12].

With the emergence of federated learning (FL) and its promise of privacy-preserving knowledge sharing, the field of intrusion detection systems (IDSs) has seen a renewed interest in the development of collaborative models. However, the distributed nature of FL makes it vulnerable to malicious contributions from its participants, including data poisoning attacks. The specific case of label-flipping attacks, where the labels of a subset of the training data are flipped, has been overlooked in the context of IDSs that leverage FL primitives. This study [12] aims to close this gap by providing a systematic and comprehensive analysis of the impact of label-flipping attacks on FL for IDSs. We show that such attacks can still have a significant impact on the performance of FL models, especially targeted ones, depending on parameters and dataset characteristics. Additionally, the provided tools and methodology can be used to extend our findings to other models and datasets, and benchmark the efficiency of existing countermeasures.

3.5.5 Federated Learning × Security for Network Monitoring

Participants: Yann Busnel, Leo Lavaur.

Published in the 44th IEEE International Conference on Distributed Computing Systems (ICDCS 2024), IEEE, Jul 2024, Jersey City, NJ, United States [6].

Federated Learning (FL) is a Machine 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, virtually extending the local dataset of each participant. Among the new challenges raised by this approach, the heterogeneity of the clients' environments induces consequent differences in the data distributions, and therefore contributions. Further, identifying and mitigating malicious contributions is made more complex in heterogeneous environments. This paper [6] introduces the audience to the principles of FL and its application to network security, and more specifically to build Collaborative Intrusion Detection Systems (CIDSs) using FL. We address open challenges on that regard, before focusing on the problem of training on heterogeneous data. Finally, we discuss the issues raised by using FL in the context of network security, with a particular focus on poisoning attacks

3.5.6 Securing the Future of Railway Systems: A Comprehensive Cybersecurity Strategy for Critical On-Board and Track-Side Infrastructure

Participants: Nisrine Ibadah, César Benavente-Peces, Marc-Oliver Pahl.

Published in Sensors 24 (24), 8218, 2024 [2].

The growing prevalence of cybersecurity threats is a significant concern for railway systems, which rely on an extensive network of onboard and trackside sensors. These threats have the potential to compromise the safety of railway operations and the integrity of the railway infrastructure itself. This paper aims to examine the current cybersecurity measures in use, identify the key vulnerabilities that they address, and propose solutions for enhancing the security of railway infrastructures. The report evaluates the effectiveness of existing security protocols by reviewing current standards, including IEC62443 and NIST, as well as case histories of recent rail cyberattacks. Significant gaps have been identified, especially where modern and legacy systems need to be integrated. Weaknesses in communication protocols such as MVB, CAN and TCP/IP are identified. To address these challenges, the paper proposes a layered security framework specific to railways that incorporate continuous monitoring, risk-based cybersecurity modeling, AI-assisted threat detection, and stronger authentication methodologies. The aim of these recommendations is to improve the resilience of railway networks and ensure a safer, more secure infrastructure for future operations.

3.5.7 A Gamified Learning Approach for IoT Security Education Using Capture-the-Flag Competitions: Architecture and Insights

Participants: Mohammad Hamad, Andreas Finkenzeller, Monowar Hasan, Marc-Oliver Pahl, Sebastian Steinhorst.

Published in Nordic Conference on Secure IT Systems, 161-175, 2024 [8]

Cybersecurity is one of the most critical issues for Internet of Things (IoT) systems today and in the future. Therefore, it is essential to educate students about cybersecurity and provide them with the skills needed to design and protect secure IoT systems. We share the experience we gained using a gamified learning approach to IoT security by integrating Capture the Flag (CTF) competitions into our university course. During the semester, students form teams and compete against each other in hacking various educational systems designed in a practically relevant way on our CTF platform. In our paper, we introduce the architecture of the CTF platform and provide student feedback on its effectiveness in teaching IoT security. The evaluation reflects student feedback over three semesters. We also share our lessons learned from creating and maintaining the CTF platform and discuss ideas on how to improve it further. Overall, the students engaged extensively in the CTF, had positive experiences with the provided platform and challenges, and were highly satisfied with our teaching approach. Based on the positive feedback, we believe our approach is an effective way to educate students in IoT security, and we encourage others to adopt this method.

3.5.8 Decentralized and Data-driven Security in Networking

Participants: Diogo Menezes Ferrazani Mattos, Marc-Oliver Pahl, Carol Fung.

CSNet 2022 special issue, published in Annals of Telecommunications 79 (7), 455-456, 2024 [4]

Decentralized security in networking is at the forefront of the current technological revolution, profoundly impacting society and industry. As ubiquitous systems generate vast amounts of data, cybersecurity must evolve to address new challenges, including the integration of big data, machine learning, data science, and extensive network softwarization. Modern data-driven approaches enhance the cognitive abilities of security analysts, allowing them to counter sophisticated cyber threats. The decentralization of security introduces novel challenges, urging researchers and companies to devise proactive strategies aligned with technological advancements. The six papers in this special issue illustrate the theme of security enhancement and decentralization in modern networking systems. Each paper addresses different aspects of networking, from malicious domain detection and intrusion prevention to performance evaluation of virtualized environments and secure session management using blockchain. Together, they tackle critical challenges and propose innovative solutions to improve network security, efficiency, and reliability amid evolving threats and increasing data demands.

3.5.9 Real-world detection and mitigation of AI-based cyberattacks and defence mechanisms

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

Published in RESSI 2024 [1]

Cyber-physical systems are a major part of the industry. Because attacks constantly change and compromise multiple devices or components, ensuring security in these systems becomes critical. As threats to the company's systems are increasingly understood,

one needs proper tools to analyze attacks or suspicious behaviors. Honeypots have existed since the eighties and evolved into different varieties of security tools, classified depending on their purpose, behavior, and architecture. Honeynets are realistic imitations of a system of information presented as an ideal target for attackers without any risk to the company. The main goal of honeynets consists of maintaining as long as possible any attacker into the fake system, capturing data such as behavior, tools, and exploits involved during the attack. When this data is collected, one can analyze it to build a more efficient defense. This paper gives a reference architecture of honeynet technology and future directions for honeynets leading to a survey. Future directions concern the legal issue of using honeypots, risks added by the implementation of honeynets, how reproducible collected attacks are, and how to motivate attackers to compromise a honeypot.

3.5.10 Similarity-Based Selective Federated Learning for Distributed Device-Specific Anomaly Detection

Participants: Christian Lübben, Marc-Oliver Pahl.

Published in NOMS 2024-2024 IEEE Network Operations and Management Symposium [15]

Resource constraints and heterogeneity make securing the IoT a challenge. Device-specific AD can address these challenges. Depending on the algorithm used, training device-specific models takes time. This makes it difficult to bootstrap new devices. Transfer learning via federated learning and model aggregation can speed up the creation of AD models. The novel approach implements an automatic selection of similar devices and creates an aggregated model for new devices. The evaluation uses the UNSW NB 15 dataset. The results show good performance and >90% reduction in bootstrapping time. The approach also satisfies security concerns as it mitigates injection attacks by not using too different models for aggregation.

3.5.11 Shells Bells: Cyber-Physical Anomaly Detection in Data Centers

Participants: Lars Wüstrich, Sebastian Gallenmüller, Stephan Günther, Georg Carle, Marc-Oliver Pahl.

Published in NOMS 2024-2024 IEEE Network Operations and Management Symposium [21]

Monitoring the side-channel sound can improve anomaly detection (AD) in data centers (DCs). However, a DC's dense setup results in a composite soundscape which makes it difficult to attribute sounds to individual devices.We propose a novel cyber-physical AD approach that validates device activity in realistic composite audio signals. By leveraging information from management network traffic, we predict changes in the DC soundscape. We use a convolutional neural network to compare our predictions with real observations to validate correct device activity and identify anomalies. Our evaluation using data from a real DC environment identifies spoofed and masqueraded activity with an accuracy of 98.62 %.

3.5.12 Blessing or curse? A Survey on the Impact of Generative AI on Fake News

Participants: Alexander Loth, Martin Kappes, Marc-Oliver Pahl.

Published in arXiv preprint arXiv:2404.03021 [24]

Fake news significantly influence our society. They impact consumers, voters, and many other societal groups. While Fake News exist for a centuries, Generative AI brings fake news on a new level. It is now possible to automate the creation of masses of high-quality individually targeted Fake News. On the other end, Generative AI can also help detecting Fake News. Both fields are young but developing fast. This survey provides a comprehensive examination of the research and practical use of Generative AI for Fake News detection and creation in 2024. Following the Structured Literature Survey approach, the paper synthesizes current results in the following topic clusters 1) enabling technologies, 2) creation of Fake News, 3) case study social media as most relevant distribution channel, 4) detection of Fake News, and 5) deepfakes as upcoming technology. The article also identifies current challenges and open issues.

3.5.13 Collaborative Cybersecurity using Blockchain: A Survey

Participants: Loïc Miller, Marc-Oliver Pahl.

Published in arXiv preprint arXiv:2403.04410 [25]

Collaborative cybersecurity relies on organizations sharing information to boost security, but trust management is a key concern. Decentralized solutions like distributed ledgers, particularly blockchain, are crucial for eliminating single points of failure. However, the existing literature on blockchain-based collaborative cybersecurity is limited, lacking comprehensive insights. This paper addresses this gap by surveying blockchain's role in collaborative cybersecurity from 2016 to 2023. It explores various applications, trends, and the evolution of blockchain technology, focusing on access control, data validation policies, underlying tech, and consensus mechanisms. A key finding is the fragmentation of the field with no dominant research group or venue. Many recent projects poorly select consensus protocols for their blockchain. To aid researchers and practitioners, this paper offers guidelines for choosing the right blockchain for specific purposes and highlights open research areas and lessons learned from past blockchain applications in collaborative cybersecurity, encouraging further exploration in this field.

3.5.14 Intent-Based Attack Mitigation through Opportunistic Synchronization of Micro-Services

Participants: Do Duc Anh Nguyen, Pierre Alain, Fabien Autrel, Ahmed Bouabdallah, Jérôme François.

Published in 10th IEEE International Conference on Network Softwarization – Netsoft 2024 [17]

The escalating number of cyberattacks poses a significant threat to digital infrastruc-

tures. Defining and deploying accurate countermeasures is challenging because of (1) the variety of threats and their possible evolution over time and (2) the need to enforce them as fast as possible, especially for fast-propagating attacks. Intent-Based Networking (IBN) stands for a promising solution for security management, especially to mitigate attacks through the specification of reaction intents, saving time and avoiding error-prone tasks. Nevertheless, most current IBN solutions rely on centralized architectures performing time-consuming operations, which makes them inappropriate to timely deploy countermeasures, especially in the case of fast-propagating attacks spreading large-scale systems. As a solution to shorten the reaction time while supporting scalability, we first consider fast micro-services technologies (e.g., Unikernels) as the substrate of security functions acting as Policy Enforcement Points (PEP). Second, we propose to enable an opportunistic synchronization of those PEPs to react, at least partially but autonomously, against the ongoing attacks in a decentralized fashion. Such a solution raises challenges related to the consistency and performance of the overall enforced reaction policies. This paper presents the early stage of the PhD, outlining the specific challenges, limitations, and research required to leverage decentralized reaction using opportunistic synchronization of micro-services in an IBN framework for security.

3.5.15 How Fast Does Malware Leveraging EternalBlue Propagate? The case of WannaCry and NotPetya

Participants: Do Duc Anh Nguyen, Pierre Alain, Fabien Autrel, Ahmed Bouabdallah, Jérôme François, Guillaume Doyen.

Published the 6th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures – SecSoft 2024 [16]

Malware attacks pose a critical threat to digital infrastructures particularly given their potential for widespread and fast propagation. Mitigating them involves limiting their expansion, which requires a thorough understanding of their propagation mechanisms. However, few studies have been conducted on their propagation behaviors in large-scale networks. In this paper, we present the results of an empirical study focusing on the propagation strategy of WannaCry and NotPetya, two malware instances leveraging EternalBlue, an exploit developed by the NSA and stolen by The Shadow Brokers hacker group, which has been used to implement rapid spreading in some mal-ware instances. Our experiments qualify the speed of infection, epidemic behavior, and spreading strategies in a local network of 50 VMs. We have especially measured for WannyCry that (1) nearly 20

3.6 Smart environments

3.6.1 FTM-Broadcast : Détermination efficace de coordonnées sur un réseau à grande échelle

Participants: Yann Busnel.

Joint work with Hervé Rivano from INSA Lyon/CITI-AGORA. Published in CoRes 2024:

9èmes Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication, May 2024, Saint-Briac-sur-Mer, France [7].

Cross-silo federated learning (CS-FL) is a distributed learning setting which allows an identified set of organizations to collaboratively train a single global model. Since CS-FL use cases are often heterogeneous, it may be more appropriate to dynamically provide different models to more homogeneous subfederations. In addition, such systems can be undermined by contributions of poor quality, making negligent or even malicious participants critical to consider. However, distinguishing such participants in a heterogeneous context is especially difficult. We present RADAR [13], a novel architecture for CS-FL able to assess the quality of the participants' contributions, regardless of data similarity. RADAR leverages client-side evaluation to directly collect feedbacks from the participants. The same evaluations allow grouping participants according to their perceived similarity and weighting the model aggregation based on their reputation. To evaluate our approach on concrete experiments, we implement a collaborative intrusion detection system (CIDS) scenario and test our architecture in various data-quality settings using labelflipping. Our results confirm that combining clustering and a reputation system succeeds in detecting a wide range of Byzantine behaviors, including colluding attackers, which highlights RADAR's versatility.

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.

4.2 Analysis of 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 speed at which the malware spreads. To this day, the spreading behavior of Wannacry has been tested on a network with 100 virtual machines.

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

4.3 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. This platform is based on the aforementioned platform used to analyze the Wannacry propagation behaviour. This 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`

4.3.1 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`

4.4 I2NSF policy conflict detection and mitigation implementation

Participants: Anh Nguyen.

The Interface to Network Security Function (I2NSF [?]) 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[1] of the I2NSF specification. The implementation of this approach consists in two additional modules to the original I2NSF implementation:

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

[?] *** ERROR: citation '**rfc8192**' undefined ***

- 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`

4.4.1 JudgeGPT

Participants: Pahl Marc-Oliver.

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/`

4.4.2 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/`

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

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.

5.1.2 DTACK: Digital Twin–based Framework for Analyzing Cyberattacks for Intelligent Transportation System

Participants: Marc-Oliver Pahl.

- Project type: Bi-national funding
- Dates: 2023–2024
- PI institution: Marc-Oliver Pahl
- Other partners: Technische Universitaet Muenchen

Intelligent Transportation Systems (ITS) have evolved from electro-mechanical to sophisticated Electrical and Electronic (E/E) systems, enhancing capabilities but also introducing cybersecurity vulnerabilities. To safeguard against attacks, cybersecurity must be integrated across the ITS life cycle, including comprehensive testing of all security mechanisms. However, this is costly, time-consuming, and requires a unique test

environment. While Digital Twins are used by automotive manufacturers for system performance and production efficiency, they are rarely used for ITS security testing. DTACK project aims to use Digital Twins to replicate security attacks on ITS components in different life-cycle phases, creating a safe environment for emulating attacks and testing security mechanisms. The developed environment can also be used to benchmark these mechanisms for effectiveness and efficiency.

5.1.3 6th Future-IoT PhD school

Participants: Marc-Oliver Pahl.

- Project type: Bi-national funding
- Dates: 2024
- PI institution: Marc-Oliver Pahl
- Other partners: Technische Universitaet Muenchen

Explore the intricate web of Secure Supply Chain within the IoT landscape where hardware and software intertwine to drive the industries of tomorrow. Join us as we delve into the complexities of supply chain dynamics, from scalability challenges to usability concerns, in an increasingly interconnected global economy.

The trailer to our 2024 FIOT6 event "IoT meets Secure Supply Chain" At the 6th edition of the Future-IoT PhD School, we're excited to dive deep into the multifaceted realm of supply chain management. From examining security vulnerabilities to addressing scalability hurdles and enhancing usability, we'll explore a range of topics crucial to shaping resilient and efficient supply chains for the industry of the future.

Throughout the event, you'll have the opportunity to engage with several industry partners who will share invaluable insights and expertise. With a diverse array of activities including Masterclasses, a hackathon element, lightning talks, and the chance to present your PhD research, you'll be immersed in a dynamic learning environment. Plus, seize the opportunity to network with peers and professionals alike, fostering collaborations that extend beyond the confines of the classroom.

Set against the vibrant backdrop of Paris, the event will take place at the Cybercampus from September 30th to October 4th, 2024. As France's premier hub for cybersecurity research and development, the Cybercampus provides an ideal setting for exploring cutting-edge advancements and fostering innovation.

5.1.4 CyberCTF - A Reusable French-German Capture The Flag Platform Including Demonstrational Cybersecurity Teaching Elements

Participants: Marc-Oliver Pahl.

- Project type: Bi-national funding
- Dates: 2024
- PI institution: Marc-Oliver Pahl

- Other partners: Technische Universitaet Muenchen

Capture the Flag (CTF) challenges are probably best known from cybersecurity contexts. However, the concept can also be applied to other learning material, putting gamification elements and competition in the foreground for motivating learners to invest a lot of energy in learning. Cybersecurity is a key competency for industry today. It is necessary for almost all branches since Information Technology (IT) and Operational Technology (OT) systems are ubiquitous. Providing more and better teaching in cybersecurity is therefore a central requirement on a global scale. This project focuses on the German-French context, giving learners in our tandem area an advantage that can help increasing productivity in both countries. Beyond these abstract goals, the project aims to bring together German and French students for working together in a gamified competitive way on acquiring crucial skills. For teachers we want to leverage the creation of attractive teaching material. Besides a strong tooling, the project will provide initial teaching material in the platform, enabling learning from it and directly using it. The final point we want to mention here is that the teaching traditions and styles vary in both countries. Bringing the German-French tandem together will enrich the learning materials and enable out-of-the-box thinking on both sides.

5.1.5 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.

5.1.6 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.

5.1.7 Exploring Graph Neural Networks (GNNs) for Data-driven Modeling of Poly-pharmacy Adverse Drug Events from drug-drug interactions

Participants: Yann Busnel.

- Project type: CEFIPRA CSRP Project
- Dates: 2022–2025
- PI institution: Yann Busnel
- Other partners: Indian Statistical Institute (Kolkata), Jadavpur University (Kolkata), CHU Rennes

This research project aims to predict **adverse drug events (ADEs)** resulting from **drug-drug interactions (DDIs)** in **poly-pharmacy** scenarios using **graph neural networks (GNNs)**. By analyzing historical data on drug interactions and side effects, the project will model how drug combinations affect patients, considering both individual drug properties and complex multi-drug interactions. The study will also explore how a patient's biological conditions influence ADEs. Over three years, the project will focus on four key phases: predictive modeling of ADEs, linking ADEs to biological conditions, identifying high-order drug interactions, and predicting ADEs from complex interactions.

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 AI@IMT

Participants: Antoine Rebstock, Yann Busnel, Romaric Ludinard.

- Project type: research action between IRT b<>com and IMT Atlantique, co-funded by ANR within the project AI@IMT
- Dates: 2021–2024
- 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.

5.2.3 Beyond5G – Sovereign and resilient solutions for 5G and Beyond

Participants: Yann Busnel, Pierre-Marie Lechevallier (ADOPNET/IRISA), Romaric Ludinard.

- Project type: BPI France / France Relance
- Dates: 2021–2024
- PI institution: Yann Busnel
- Other partners: Thales, Ericsson, Institut Mines-Télécom (IMT Nord Europe, IMT Atlantique, EURECOM, Télécom SudParis, Télécom Paris)

Sovereignty in Telecommunications Networks to Accelerate 5G Applications in Vertical Markets. The project aims to design technical solutions for the development of sovereign and secure next-generation 5G networks, while developing innovative uses for the industry of the future. Project involves several industrial partners as Thales and Ericson at least.

5.2.4 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.

5.2.5 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.

5.2.6 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: 2022–2025
- 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.

5.2.7 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.

5.2.8 ANR CMA CyberSkills4ALL project (2023 - 2028)

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

- Project type: ANR CMA
- Dates: 2023–2028
- PI institution: Mohamed Aymen Chalouf
- Other partners: Université de Bretagne SUD, Rennes School of Business, Orange, Institut Polytechnique de Brest, Orange, Pole d'Excellence Cyber.

The increasing attack surface and the growing complexity of information systems make human responses inadequate in the face of new threats. The introduction of concepts such as self-protection and collaborative cybersecurity makes it possible to implement new defense systems adapted to current requirements. This raises the question of designing a trusted autonomous architecture, capable of orchestrating coordinated responses in real time and applying targeted and adaptive countermeasures. The thésis of Constant Rohmer (Phd. Student) aims at meeting this need by reconciling reliability, robustness and performance. The proposed approach will rely on blockchain to guarantee the inalterability and traceability of actions, while automating reactions thanks to smart contracts. Unikernels will complement this architecture by ensuring the adaptability and parallelization of operations, thus improving scalability and response time. A multi-objective orchestration function will also be introduced to coordinate resources, prioritize actions and avoid conflicts. Finally, a rigorous evaluation will validate the performance of the solution and ensure an efficient and optimized collaborative response.

5.3 Bilateral industry grants

5.3.1 Cyber CNI: Chaire Cybersécurité des Infrastructures Critiques – Phase 3

Participants: Marc-Oliver Pahl.

- Project type: Industrial Research Chair
- Dates: 2022–2024
- PI institution: Marc-Oliver Pahl
- Other partners:, Télécom Paris, Télécom SudParis, Airbus, BNP Paribas, EDF, and SNCF

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.

5.4 Collaborations

5.4.1 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).

5.4.2 Dipartimento di Automatica e Informatica, Politecnico di Torino

Participants: Pierre Alain, Fabien Autrel, Guillaume Doyen.

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

We started 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 had reciprocal meetings to explore innovative approaches that leverage artificial intelligence and network security automation. 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.

6 Dissemination

6.1 Promoting scientific activities

6.1.1 Scientific Events Organization

General Chair, Scientific Chair

Guillaume Doyen served as a general co-chair of the 6th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft) co-located with IEEE Netsoft 2024 (Secsoft'24).

Marc-Oliver Pahl served as a general co-chair of the The 4th International Workshop on Internet of Things Management (manage-IoT) co-located with IEEE/IFIP NOMS 2024 (manage-IoT'24).

Member of the Organizing Committees

Guillaume Doyen served as an organization committee member in the following conferences:

- 10th IEEE International Conference on Network Softwarization (Netsoft'24) – PhD Symposium co-chair;
- 15th International Conference on Network of the Future (NoF'24) – Keynotes and Panel co-chair.

Romaric Ludinard served as an organization committee member in the following conferences:

- 26èmes Rencontres Francophones sur les Aspects Algorithmmiques des Télécommunications (AlgoTel'24);
- 9èmes Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication (CoRes'24);
- Journées commune aux GDR RSD, GPL (GT GLSEC) et SI (GT SSLR) sur la sécurité des piles réseau (SecRes'24);
- 6th Conference on Blockchain Research & Applications for Innovative Networks and Services as Publicity chair, (BRAINS'24).

Renzo E. Navas served as an organization committee member of the 4th IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT) co-located with NOMS 2024 (manage-IoT'24).

6.1.2 Scientific Events Selection

Chair of Conference Program Committees

Yann Busnel served as Scientific Track Chair (*Federated Learning, Analytics, and Deployment*) of the 44th IEEE International Conference on Distributed Computing Systems ((ICDCS 2024), in Jersey City, New Jersey, USA – July 2024.

Gilles Guette served as Scientific Track Chair of International Conference on Information and Communication Technologies for Disaster Management (ICT-DM 2024).

Romaric Ludinard served as Scientific chair of 9èmes Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI'24).

Renzo E. Navas served as a TPC chair of the 4th IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT) co-located with NOMS 2024 (manage-IoT'24).

Marc-Oliver Pahl served as Scientific Track Chair (*Detection of Complex Attacks*) in the following the 28th International Conference on Knowledge Based and Intelligent information and Engineering Systems (KES2024) (KES-DCA 2024).

Member of Conference Program Committees

Pierre Alain served as Shepherd of the PhD track of the 9èmes Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI'24).

Ahmed Bouabdallah served as a TPC member of the COMPSAC 2024 Symposium on Security, Privacy & Trust in Computing SEPT'24.

Yann Busnel served as a TPC member of the 23rd International Symposium on Network Computing and Applications (NCA'24)

Mohamed Aymen Chalouf served as a TPC member in the following conferences:

- IEEE Symposium on Computers and Communications (ISCC'24)
- IEEE International Workshop on Edge Systems for Future Mobile Network (Edge4Future'24)
- IEEE International Workshop on e-Health Pervasive Wireless Applications and Services (eHPWAS'24)

Gilles Guette served as a TPC member in the following conference:

- 11th International Conference on Information Systems Security and Privacy (ICISSP'25).

Romaric Ludinard served as a TPC member in the following conferences:

- 26èmes Rencontres Francophones sur les Aspects Algorithmmiques des Télécommunications (AlgoTel'24);
- 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS'24);
- 6th International Workshop on Foundations and Applications of Blockchain (FAB 2024);
- 23rd International Symposium on Network Computing and Applications (NCA'24).

Mohammed Nafi served as a TPC member in the 6th International Workshop on Graph-based Approaches for CyberSecurity (GRASEC'24).

Marc-Oliver Pahl served as a TPC member in the following conferences:

- IEEE/IFIP Network Operations and Management Symposium 6–10 May 2024 // Seoul, South Korea
- The 4th IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT) co-located with NOMS 2024
- The 9th IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet) co-located with NOMS 2024
- Computer & Electronics Security Application Rendezvous (C&ESAR) at the European Cyber Week (ECW)
- IEEE/ IFIP Conference on Network and Service Management, CNSM

Reviewer

Pierre Alain served as an external reviewer for:

- 6th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft) (SECSOFT'24),
- IEEE/IFIP Network Operations and Management Symposium (NOMS'25).

Ahmed Bouabdallah served as an external reviewer for:

- 6th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft) (SECSOFT'24),
- IEEE/IFIP Network Operations and Management Symposium (NOMS'25)

Mohamed Aymen Chalouf served as an external reviewer for the International Conference on Software, Telecommunications and Computer Networks (SoftCOM'24).

Guillaume Doyen served as an external reviewer for the 3rd International Conference on 6G Networking (6GNet'24).

Romaric Ludinard served as an external reviewer for IEEE/IFIP Network Operations and Management Symposium (NOMS'24).

Renzo E. Navas served as a reviewer in the following conferences:

- The 4th IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT) co-located with NOMS 2024 (manage-IoT'24).
- The 38th IEEE/IFIP Network Operations and Management Symposium (NOMS'25).

6.1.3 Journal

Member of the Editorial Boards

Guillaume Doyen served as an Associate Editor for the Springer Journal of Network and Systems Management, JNSM.

Marc-Oliver Pahl served as an Associate Editor for the following journals:

- Springer Journal of Network and Systems Management, JNSM
- Wiley International Journal of Network Management, IJNM

Reviewer - Reviewing Activities

Pierre Alain served as a reviewer for IEEE Transactions on Network and Service Management.

Ahmed Bouabdallah served as a reviewer for the following journals:

- Elsevier Computer Communications;
- Springer Journal of Network and Systems Management;
- Oxford Academic The Computer Journal.

Mohamed Aymen Chalouf served as a reviewer for the following journals:

- Springer Nature Wireless Personal Communications
- Springer Nature Journal of Network and Systems Management

Guillaume Doyen served as a reviewer for IEEE Transactions on Network and Service Management.

Gilles Guette served as a reviewer for ASET Journal of Networks.

Romaric Ludinard served as a reviewer for IEEE Transactions on Computers.

Renzo E. Navas served as a reviewer for Springer Journal of Network and Systems Management, JNSM.

Marc-Oliver Pahl served as a reviewer for the following journals:

- IEEE Transactions on Network and Service Management, TNSM
- IEEE Transactions on Industrial Informatics
- IEEE Transactions on Industrial Electronics

6.1.4 Invited Talks

6.1.5 Leadership within the Scientific Community

Yann Busnel is leading the Distributed System axis of the Network and Distributed Systems CNRS Research group (GDR RSD) steering committee.

Guillaume Doyen served the different national communities:

- Steering Committee member of RESSI (Comité de Pilotage);
- Board member of the SSLR working group of the Computer Science Security Research group (GT SSLR[2]);
- co-chair of the Digital Trust Community of Institut Mines Télécoms;
- Member of the scientific board of Sosysec (Sosysec).

[2]The web page was not up to date at the time of the activity report delivery

Romaric Ludinard is member of the Network and Distributed Systems CNRS Research group (GDR RSD) steering committee.

Marc-Oliver Pahl has acted as an:

- elected president of the German Chapter of the Association of Computing Machinery (ACM).
- board member of the German Informatics Society.
- elected expert board member of the LabCyber at the PTTC au Campus Cyber, Paris.
- board member of the German-French Academy for the Industry of the Future.

6.1.6 Scientific Expertise

Romaric Ludinard served as external expert for 14e "Concours d'innovation i-Nov" Bpifrance (thématique Numérique).

Yann Busnel is member of the Scientific Council of CEFIPRA — Indo-French Centre for Promotion of Advanced Research.

Marc-Oliver Pahl contributed as a co-author of the 2nd Whitebook of the Pole d'excellence Cyber on LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION.

6.1.7 Research Administration

Yann Busnel has acted as Vice-President for Research and Innovation at IMT Nord Europe, until septembre 2024.

Yann Busnel acted as Senior Vice-President for Research at Institut Mines-Télécom, since october 2024.

Yann Busnel has acted as Member of 11 selections committees for position of Professors and Associate Professors at IMT Nord Europe, during spring and summer 2024

Guillaume Doyen served as the chair of the Scientific, Technological and International Initiative on Cybersecurity at IMT Atlantique.

6.2 Teaching, supervision

6.2.1 Teaching

For researchers, all activities are given. For professors and assistant professors, only courses at the M. Sc. level are listed.

- 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
- Sécurité Réseau, IMT Atlantique, Mastère spécialisé, Gilles Guette.
- 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).
- Operating Systems, IMT Atlantique, Engineering track, Renzo E. Navas and Guillaume Doyen.
- Operating Systems, IMT Atlantique, Engineering track, Renzo E. Navas and Guillaume Doyen.
- Cryptography Introduction, IMT Atlantique, TAF Cyber, Renzo E. Navas.
- Sécurité des réseaux, IMT Atlantique, Formation continue, Renzo E. Navas.
- Bibliographical Project, IMT Atlantique, MSc IT (M1), Renzo E. Navas.
- Sécurité des réseaux, IMT Atlantique, TAF Cyber, Ahmed Bouabdallah, Guillaume Doyen.
- Sécurité des applications, IMT Atlantique, TAF Cyber, Ahmed Bouabdallah , Renzo E. Navas.
- Architectures de services de l'Internet, IMT Atlantique, TAF PNUM, Ahmed Bouabdallah.
- Virtualisation des réseaux, IMT Atlantique, TAF PNUM, Ahmed Bouabdallah.
- Sécurité Windows, ENSSAT, Engineer degree (3rd year), Mohammed Nafi
- Mise en oeuvre des réseaux locaux, ENSSAT, Engineer degree (2rd year), Mohammed Nafi
- Réseaux 1, ENSSAT, Engineer degree (2rd year), Mohammed Nafi
- Théorie des langages et compilation, ENSSAT, Engineer degree (2rd year), Mohammed Nafi
- Algorithmique répartie, ENSSAT, Engineer degree (2rd year), Mohammed Nafi
- SecIoT, Engineering track, Marc-Oliver Pahl
- Principaux modèles de contrôle d'accès, TAF Cyber, Fabien Autrel.
- Sécurité des principaux protocoles industriels, TAF Cyber, Fabien Autrel.
- Network security, Bordeaux INP, Engineering track, Mohamed Aymen Chalouf.

6.2.2 Supervision

- Master 2 intern: Dorian Pacaud supervised by Romaric Ludinard and Loïc Miller,
- Master 2 intern: Nathanaël Derousseaux supervised by Romaric Ludinard and Loïc Miller,
- Master 2 intern: Constant Rohmer supervised by Pierre Alain and Mohamed Aymen Chalouf,
- Master 2 intern: Daisy Munson supervised by Pierre Alain,
- Master 2 research project: Vincent Bonnet and Pierre Chevet, supervized by Pierre Alain.
- Master 2 intren: Melek Katri supervised by Sinda Boussen (Faculté des Sciences de Tunis, Tunisia), Mohamed Aymen Chalouf and Omessaad Hamdi (IEEE Member).
- Master 1 intern: Kouassi Amangoua supervised by Mohamed Aymen Chalouf, Guillaume Doyen and David Espes (LabSticc).
- Master 1 intern: Yassine Hamimaz supervised by Mohamed Aymen Chalouf, Ciprian Dobre (Politechnica Bucharest, Roumania) and Laurent D'Orazio (Shaman Team, Irisa).

- PhD 2018-2025: Christian Lübben, *Optimizing IoT Smart Spaces using advanced Data Analytics*, co-supervised by Marc-Oliver Pahl, Georg Carle (i8 – TU München)
- PhD 2019-2025: Erkin Kirdan, *Industrial IoT Engineering: Unleashing the Full Potential of Machine-to-Machine Communication Protocols OPC UA, MQTT and CoAP*, co-supervised by Marc-Oliver Pahl, Georg Carle (i8 – TU München)
- PhD 2019-2025: Lars Wüstrich, *Multi-Layer Dependency Identification in Computer Networks*, co-supervised by Marc-Oliver Pahl, Georg Carle (i8 – TU München)
- PhD 2020-2024: Awaleh Houssein Meraneh, *Enhancing the Security of Industrial Cyber-Physical Systems through Side-Channel Leakages*, coadvised by Marc-Oliver Pahl, Hélène Le Bouder (OCIF).
- PhD 2020-2025: Marius Letourneau, *Featuring and Detecting novel threats on Low-Latency networks: the case of L4S*, supervized by Guillaume Doyen and Rémi Cogranne (UTT).
- PhD 2020-2025: Hichem Magnouche, *Orchestrating Micro-Service Chains for a Low-Latency Internet*, supervized by Guillaume Doyen and Caroline Prodhon (UTT).
- PhD 2021-2024: Leo Lavaur, *Improving intrusion detection in distributed systems with federated learning*, supervized by Yann Busnel and Fabien Autrel.
- 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-: Antoine Rebstock, *Extraction of probable scenarios by correlation of alerts*, supervized by Yann Busnel and Romaric Ludinard.
- PhD 2022-: 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*, coadvised 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-: Constant Rohmer, *Towards robust, reliable and high-performance self-protection for connected systems: an approach based on blockchain and microservices*, supervised by Pierre Alain, Mohamed Aymen Chalouf and Guillaume Doyen.
- 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*, coadvised by Marc-Oliver Pahl, Fabien Dagnat (Lab-Sticc).

6.2.3 Juries

Yann Busnel has acted as a Reviewer of PhD thesis of Obsa Gilo Wakuma (IIT Patna), 2024.

Mohamed Aymen Chalouf acts as a reviewer of the PhD thesis of Dionysia Varvarigou, Université de Bretagne Occidentale, France.

Guillaume Doyen participated in the following PhD juries:

- Sonorithy Send, Télécom Sud Paris, France;
- Céline Minh, LAAS-CNRS, France;
- Wassim Koribeche, Université Bretagne Ouest, France.

Guillaume Doyen participated in the HDR jury of Gilles Guette, Université de Rennes, France.

Marc-Oliver Pahl participated in the following PhD juries:

- Amani Abou Rida, Université de Strasbourg, France;
- Michael Zipperle, University of South Wales, Australia.

6.2.4 Responsabilities

- Guillaume Doyen is the chair of Scientific, Technological and International Initiative on Cyber Security of IMT Atlantique
- Mohammed Nafi is head of Research Master EUR CyberSchool track, ENSSAT
- Renzo E. Navas was head of the newly created Cybersecurity track in the IMT Atlantique Master of Science (MSc) in Information Technology (MScIT / Track Cybersecurity) Degree ENSSAT and Research Master EUR Cyberschool
- Ahmed Bouabdallah and Guillaume Doyen are co-Head of the FISE TAF Cyber
- 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
- Marc-Oliver Pahl is Director of the Chair Cybersecurity of Ciritcal National Infrastructures

6.3 Popularization

- Pierre Alain is a core team member of MirageOS
- Gilles Guette has participated to the program *À la découverte de la recherche.*
- Gilles Guette has participated to the program "Plan National de Formation, Rendez vous de l'informatique : atelier réseaux" a training workshop for high school SNT/SNI teachers

7 Bibliography

Articles in referred journals and book chapters

[1] M. Durand, Y. Kermarrec, M.-O. Pahl, "Real-world detection and mitigation of AI-based cyberattacks and defence mechanisms".

[2] N. Ibadah, C. Benavente-Peces, M.-O. Pahl, "Securing the Future of Railway Systems: A Comprehensive Cybersecurity Strategy for Critical On-Board and Track-Side Infrastructure", *Sensors 24*, 24, 2024, https://www.mdpi.com/1424-8220/24/24/8218.

[3] H. Magnouche, G. Doyen, C. Prodhon, "A Fair Sharing Approach for Micro-Services Function Chains Placement in Ultra-Low Latency Services", *IEEE Transactions on Network and Service Management 21*, 1, 2024, p. 20–34.

[4] D. M. F. Mattos, M.-O. Pahl, C. Fung, "CSNet 2022 special issue—decentralized and data-driven security in networking", *Annals of Telecommunications 79*, 7, 2024, p. 455–456.

[5] A. Mühle, A. Grüner, T. Gayvoronskaya, C. Meinel, "A survey on essential components of a self-sovereign identity", https://doi.org/10.1016/j.cosrev.2018.10.002.

Publications in Conferences and Workshops

[6] Y. Busnel, L. Lavaur, "Tutorial: Federated Learning x Security for Network Monitoring", *in : 44th IEEE International Conference on Distributed Computing Systems (ICDCS 2024)*, IEEE, Jersey City, NJ, United States, July 2024, https://hal.science/hal-04606894.

[7] Y. Busnel, H. Rivano, "FTM-Broadcast : Détermination efficace de coordonnées sur un réseau à grande échelle", *in : CoRes 2024: 9èmes Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication*, Saint-Briac-sur-Mer, France, May 2024, https://hal.science/hal-04569538.

[8] M. Hamad, A. Finkenzeller, M. Hasan, M.-O. Pahl, S. Steinhorst, "A Gamified Learning Approach for IoT Security Education Using Capture-the-Flag Competitions: Architecture and Insights", *in : Secure IT Systems*, L. Horn Iwaya, L. Kamm, L. Martucci, T. Pulls (editors), Springer Nature Switzerland, p. 161–175, Cham, 2025.

[9] V. Hamici-Aubert, J. Saint-Martin, R. E. Navas, G. Z. Papadopoulos, G. Doyen, X. Lagrange, "Leveraging Overshadowing for Time-Delay Attacks in 4G/5G Cellular Networks: An Empirical Assessment", *in : ARES '24: Proceedings of the 19th International Conference on Availability, Reliability and Security*, Vienna, Austria, July 2024, https://hal.science/hal-04628498.

[10] N. Khairallah, A. B. Chehida Douss, R. Abassi, M. Aymen Chalouf, O. Hamdi, "Towards Secure and Privacy Preserving Data Processing in E-Health", *in : 2024 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, p. 136–141, 2024.

[11] L. Lavaur, Y. Busnel, F. Autrel, "Demo: Highlighting the Limits of Federated Learning in Intrusion Detection", *in : 44th IEEE International Conference on Distributed Computing Systems (ICDCS 2024)*, IEEE, Jersey City, NJ, United States, July 2024, https://hal.science/hal-04606824.

[12] L. Lavaur, Y. Busnel, F. Autrel, "Systematic Analysis of Label-flipping Attacks against Federated Learning in Collaborative Intrusion Detection Systems", *in : The 19th International Conference on Availability, Reliability and Security (ARES 2024)*, ACM (editor), *4th International Workshop on Behavioral Authentication for System Security (BASS)*, Vienna, Austria, July 2024, https://hal.science/hal-04559018.

[13] L. Lavaur, P.-M. Lechevalier, Y. Busnel, R. Ludinard, G. Texier, M.-O. Pahl, "RADAR: Model Quality Assessment for Reputation-aware Collaborative Federated Learning", *in : 43rd International Symposium on Reliable Distributed Systems - SRDS 2024*, Charlotte (NC), United States, September 2024, https://hal.science/hal-04681789.

[14] P.-M. Lechevalier, R. Ludinard, Y. Busnel, G. Texier, "A fuzzy reputation system for Radio Access Network sharing", *in : The 22nd International Symposium on Network Computing and Applications (NCA 2024)*, Bertinoro, Italy, October 2024, https://hal.science/hal-04846409.

[15] C. Lübben, M.-O. Pahl, "Similarity-Based Selective Federated Learning for Distributed Device-Specific Anomaly Detection", *in : NOMS 2024-2024 IEEE Network Operations and Management Symposium*, p. 1–5, 2024.

[16] D. D. A. Nguyen, P. Alain, F. Autrel, A. Bouabdallah, J. François, G. Doyen, "How Fast Does Malware Leveraging EternalBlue Propagate? The case of WannaCry and NotPetya", *in : 2024 IEEE 10th International Conference on Network Softwarization (NetSoft)*, p. 399–404, 2024.

[17] D. D. A. Nguyen, P. Alain, F. Autrel, A. Bouabdallah, J. François, "Intent-Based Attack Mitigation through Opportunistic Synchronization of Micro-Services", *in : 2024 IEEE 10th International Conference on Network Softwarization (NetSoft)*, p. 149–152, 2024.

[18] V.-T. Nguyen, G. Doyen, V.-T. Nguyen, R. E. Navas, E. Alata, D. Dragomirescu, "Toward Context-aware Security for Individual Information Systems", *in : Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI)*, Eppe-Sauvage, France, May 2024, https://hal.science/hal-04602354.

[19] V.-T. Nguyen, R. E. Navas, G. Doyen, "Lightweight Security for IoT Systems leveraging Moving Target Defense and Intrusion Detection", *in : NOMS 2024-2024 IEEE/IFIP Network Operations and Management Symposium*, IEEE, Seoul, South Korea, May 2024, https://hal.science/hal-04537696.

[20] R. Singh, M. A. Chalouf, L. Mendiboure, M. Berger, L. Dittmann, "Towards an SDN-based Reconfigurable Edge Architecture for Railway Environment", *in : 2024 7th International Conference on Advanced Communication Technologies and Networking (CommNet)*, p. 1–7, 2024.

[21] L. Wüstrich, S. Gallenmüller, S. Günther, G. Carle, M.-O. Pahl, "Shells Bells: Cyber-Physical Anomaly Detection in Data Centers", *in : NOMS 2024-2024 IEEE Network Operations and Management Symposium*, p. 1–10, 2024.

Miscellaneous

[22] A. Bouabdallah, "The fractal nature of the properties of reactive and concurrent programs", *in : 13th International Workshop on Geometric and Topological Methods in*

Computer Science (GETCO 2024), workshop associated with ICALP, LICS and FSCD, 2024, https://getco-conf.github.io/2024/.

[23] M. P. J. Kuranage, E. Hanser, A. Bouabdallah, L. Nuaymi, P. Bertin, "CPU throttling-aware AI-based autoscaling for Kubernetes", *in : 2024 IEEE 35th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2024.

[24] A. Loth, M. Kappes, M.-O. Pahl, "Blessing or curse? A survey on the Impact of Generative AI on Fake News", 2024, https://arxiv.org/abs/2404.03021.

[25] L. Miller, M.-O. Pahl, "Collaborative Cybersecurity Using Blockchain: A Survey", 2024, https://arxiv.org/abs/2403.04410.