Activity Report 2023

Team SOTERN

Self-Protecting the Future Internet

D2 – Networks, Telecommunications and Services

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
Romaric Ludinard, Associate professor,	IMT Atlantique
Renzo E. Navas, Associate professor,	IMT Atlantique
Marc-Oliver Pahl, Research director,	IMT Atlantique

Associate members

Yann Busnel, (HDR) Full professor,	IMT Nord Europe

Research engineers, technical staff

Fabien Autrel, Permanent research engineer

Sulaiman Mohammad, Research engineer from Apr. 23 to Aug. 24

Post-doctoral researchers

Nisrine Ibadah, from Aug. 22 to Mar. 24,	IMT Atlantique
Loïc Miller, from Sept. 22 to Aug. 25,	IMT Atlantique

PhD students

Léo Lavaur, 2020-ongoing

Antoine Rebstock, 2021-ongoing

Do Duc Anh Nguyen, 2022-ongoing

Van Tien Nguyen, 2022-ongoing

Mathis Durand, 2023-ongoing

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-ongoing

Nicolas Delcombel (INUIT/LAB-STICC – IMT Atlantique), 2020-ongoing

Pierre-Marie Lechevalier (ADOPNET/IRISA – IMT Atlantique), 2021-ongoing

Lucie David (INUIT/LAB-STICC – IMT Atlantique), 2022-ongoing
Christian Lübben (i8 – TU München), 2018-ongoing
Erkin Kirdan (i8 – TU München), 2019-ongoing
Lars Wüstrich (i8 – TU München), 2019-ongoing
Igor Dias Da Silva (COATI/L3S-Inria Sophia Antipolis), 2020-2023
Virgil Hamici-Aubert (OCIF/IRISA – IMT Atlantique), 2023-ongoing
Arnol Lemogue (OCIF/IRISA – IMT Atlantique), 2020-2023
Menuka Perera Jayasuriya Kuranage (ADOPNET/IRISA – IMT Atlantique), 2021-ongoing

Administrative assistant

Sandrine Frouin	IMT Atlantique

2 Overall objectives

2.1 Overview

After one year of existence, as a preliminary presentation of the the research group, we remind here the teams objectives and research hypotheses, as stated in the initial founding document of the team. Then, we highlight six core research issues the team tackles currently, all taking part of the different research axes and challenges identified at start. Finally, we close this section by emphasizing the five application fields targeted by the research activities of the team.

2.1.1 Team's Objectives and Research Hypotheses

The evolution of the Internet leads to an ever-stronger integration of this cyberspace in places and devices manipulated by humans: (1) in everyday life, from the use of mobile devices, to smart environments (vehicles, buildings, *etc.*), but (2) also in critical infrastructures, whether civil, such as industry 4.0, or military, including robots and drones operating in theatres of operations or protecting the sovereignty of digital spaces. This evolution of the cyberspace is based on the concomitant maturity of connected objects, the development of telecommunication capabilities and virtualization, and in this context, it is necessary to offer users a coupled real/digital space which is secure, safe and above all trustworthy. However, without even dealing with guarantees, ensuring a minimum level of protection proves to be a complex challenge for several reasons:

1. Cyber-physical systems are of an ever-increasing size, reaching very **large scales**, and they are composed of ever more miniaturized elements exhibiting atomic functions, such as connected objects or micro-services deployed in virtualized infrastructures.

2. Cyber-physical systems surrounding people are, for part of them, **open**, meaning that they are not limited to an operated or controlled infrastructure where each participant has been identified as being trustworthy.

3. Cyber-physical systems, due to their complexity and the need to maintain their functionality regardless of the unpredictable phenomenon and timeliness, no longer allow humans to be at the heart of their control. This need for **system autonomy** is a pervasive reality that must be integrated by design.

To address these issues, the SOTERN team sets out to design, develop and validate methods and tools for the self-protection of the Future Internet. Self-protection is considered as the capability of systems to monitor, detect and remedy by themselves to deliberately malicious behaviors, whose objectives, varied by nature, may be to undermine the proper provision of a service, a user or an infrastructure. Depending on the characteristics of the system and its maturity, the self-protection solutions may be intrinsically implemented into its components, such as during the design stage or by corrective means, or extrinsic, thereby implemented through dedicated security components automatically enforcing attack detection, mitigation and remediation.

2.1.2 Overall Position of the Team Project

Self-protection is not intrinsically a novel concept since it has been early identified by Kephart [KC03] in 2003 as one of the four ground self-* taking part of an autonomous networking system and instantiated on the MAPE-k control loop. Beyond, several other frameworks propose similar loops such as the NIST [B+18] which defines the five Identify, Protect, Detect, Respond and Recover functions for the management of cybersecurity risk. If self-protection has historically not been the self-* function that attracted most of the efforts, recent outcomes in (1) technologies of network and services (IoT and 5G and beyond as flagships), (2) technical means now offering straightly implementable self-* functions (*e.g.*, network softwarization), and (3) the ever increasing threats and actual attacks targeting these systems, have brought self-protection and, in a minimal consideration, security automation, at the front of the scene [YEM14,ICW21]. Recently, Dobson *et al.* [DHM+19] identified the key research areas and related challenges to provide network systems with resilience to faults and attacks. These are Intent-based networking, network function virtualization, programmable self-organization, cyber-physical systems resilience and resilient system design/operation and the relation with human and their role. All of them perfectly fit with the Sotern vision. As some illustrative examples of this paradigm, we mention some relevant works in the area of (1) IoT self-protection schemes identification [AH15], (2) the EU SelfNet-5G project which brings the 5G&Beyond architecture self-protection capabilities against distributed attacks [HCGPGCMP19], (3) the complexity to deal with security vs. functional objectives in self-protected systems [JRW+20] and finally (4) a formal to human-friendly model trans-

[KC03] J. Kephart, D. Chess, "The vision of autonomic computing", Computer 36, 1, 2003, p. 41–50.

[B+18] M. P. Barrett et al., "Framework for improving critical infrastructure cybersecurity version 1.1", 2018, `https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf`.

[YEM14] E. Yuan, N. Esfahani, S. Malek, "A Systematic Survey of Self-Protecting Software Systems", ACM Trans. Auton. Adapt. Syst. 8, 4, 1 2014, `https://doi.org/10.1145/2555611`.

[ICW21] S. Iannucci, E. Casalicchio, B. Williams, "Editorial for FGCS special issue: Advances in self-protecting systems", Future Generation Computer Systems 123, 2021, p. 178–180, `https://www.sciencedirect.com/science/article/pii/S0167739X21001552`.

[DHM+19] S. Dobson, D. Hutchison, A. Mauthe, A. Schaeffer-Filho, P. Smith, J. P. G. Sterbenz, "Self-Organization and Resilience for Networked Systems: Design Principles and Open Research Issues", Proceedings of the IEEE 107, 4, 2019, p. 819–834.

[AH15] Q. M. Ashraf, M. H. Habaebi, "Autonomic schemes for threat mitigation in Internet of Things", Journal of Network and Computer Applications 49, 2015, p. 112–127, `https://www.sciencedirect.com/science/article/pii/S1084804514002732`.

[HCGPGCMP19] A. Huertas Celdrán, M. Gil Pérez, F. J. García Clemente, G. Martínez Pérez, "Towards the autonomous provision of self-protection capabilities in 5G networks", Journal of Ambient Intelligence and Humanized Computing 10, 12, 2019, p. 4707–4720, `https://doi.org/10.1007/s12652-018-0848-6`.

[JRW+20] S. Jahan, I. Riley, C. Walter, R. F. Gamble, M. Pasco, P. K. McKinley, B. H. Cheng, "MAPE-K/MAPE-SAC: An interaction framework for adaptive systems with security assurance cases", Future Generation Computer Systems 109, 2020, p. 197–209, `https://www.sciencedirect.com/science/article/pii/S0167739X19320527`.

lation [IAM+20] which eases the adoption of self-protected systems. Beyond the above-mentioned examples of contributions, standardization bodies exhibit a growing interest in self-protected distributed systems. Firstly, the European Telecommunications Standards Institute[1] (ETSI), through the Zero-touch network and Service Management[2] (ZSM) working group, initially focused its effort on performance issues. However, security has been recently considered [ETS21] through the ability of ZSM to automate the security of managed entities, which is well-aligned with the SOTERN positioning and reinforces the project in its timely relevance. Also, recently the Internet Engineering Task Force[3] (IETF) has identified the concept of Intent-Based Networking (IBN) [CCGT21], which consists in (1) entrusting more autonomy to the mechanisms of networks and services and (2) redesigning the relation with the human, which should only define concise and high-level objectives that the network must reach without specifying means of implementation. They identified the need to design distributed algorithms performed by the devices themselves, which is here again well-aligned with the SOTERN project. Besides, leveraging Intents for security is also at the core of questions currently addressed in this standardization body [HLZ+17].

2.2 Scientific Foundations

In this section, we briefly expose the six research questions the research group currently tackles. For each question, we introduce its motivation and we highlight the methodological approach we consider to provide some answers. The latter can be either empirical, with an experimental approach or grounded by some theoretical tools that we introduce. The common ground of all the research questions we tackle relies in their objective to make security frameworks (1) able to cope with current networks evolution (e.g. capability to handle heterogeneous inputs, scalability and fast reaction times of security mechanisms), (2) more robust (e.g. formal verification of configurations, security of control and management) and eventually, (3) able to act autonomously while preserving relevant interactions with a human security operator.

[1] `https://www.etsi.org`

[2] `https://www.etsi.org/technologies/zero-touch-network-service-management`

[3] `https://www.ietf.org`

[IAM+20] S. Iannucci, S. Abdelwahed, A. Montemaggio, M. Hannis, L. Leonard, J. S. King, J. A. Hamilton, “A Model-Integrated Approach to Designing Self-Protecting Systems”, IEEE Transactions on Software Engineering 46, 12, 2020, p. 1380–1392.

[ETS21] ETSI, “Zero-touch network and Service Mgmt: General Security Aspects”, research report, ETSI, 2021.

[CCGT21] A. Clemm, L. Ciavaglia, L. Z. Granville, J. Tantsura, “Intent-Based Networking - Concepts and Definitions”, Internet Engineering Task Force, draft-irtf-nmrg-ibn-concepts-definitions-06, December 2021, Work in Progress, `https://datatracker.ietf.org/doc/html/draft-irtf-nmrg-ibn-concepts-definitions-06`.

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

2.2.1 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.

2.2.2 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 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. This point has been briefly addressed in the development of a method for conflict detection in large-scale I2NSF policies. Grounded by this initial work, we reconsider it in the context of 5G slices security using a metagraph-based approach [RRN22].

2.2.4 Fast reactions to security breaches

As a core aspect of security the team addresses, timely detection and reaction are explored in different contexts.

First, among the security requirements expressed by a security policy, reaction policy, which specifies the security requirements that should be enforced when an intrusion has been detected, is considered. Indeed, 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 "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.

Second, as an even more challenging case to address, the research group handles the case of latency constraints networks such as case of L4S[4] and TSN[5], whose configuration for the latter remains a challenging task due to (1) the distributed nature of security

[4] Low-Latency, Low-Loss, Scalable throughput

[5] Time Sensitive Networking

[RRN22] D. Ranathunga, M. Roughan, H. Nguyen, "Verifiable Policy-Defined Networking Using Metagraphs", Transactions on Dependable and Secure Computing 19, 1, 2022.

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

components implying both core network and terminal entities, (2) the dynamic nature of flows and terminal entities and (3) the very fine vision of the configuration of those components. Thus, providing at all times a fairly robust configuration against attacks targeting latency and jitter constraints while respecting these constraints appears to be a complex problem. Consequently, configuration simplifications and errors offer a novel attack surface by injecting disruptive malicious flows differing from a well-explored distributed denial of service. In this context, our research group adopts an empirical approach which consists in deploying dedicated platforms in order to characterize empirically how, hacked, erroneous and/or simplified configurations can be exploited by attacks and the impact of these last on legitimate streams. This eventually leads us to feed models of latency-constrained networks configuration which may be expressed in different ways such as statistical ones or optimization problems consisting in identifying solutions respecting both security constraints and quality of service ones (jitter and latency).

2.2.5 Security of Control and Management Operations

Distributed system activities are accompanied by control protocols and management operations or updates which must operate in a secure way even when the devices involved are constrained. Our research group addresses this aspect from two different perspectives. First, we integrate security-by-design considerations (integrity, confidentiality, and authenticity) into the secure remote software update phase of distributed devices. We embed those security measures into the design and implementation of update mechanisms. Through the adoption of cryptographic techniques, secure communication protocols, and rigorous validation mechanisms, we aim to instill confidence in the reliability and trustworthiness of remote software updates. This proactive approach not only enhances the resilience of software systems against evolving threats but also minimizes the disruption and potential vulnerabilities associated with outdated software. Second, to face the Quantum Menace, we aim at deploying post-quantum (PQC) technologies. In particular, we focus on Key Encapsulation Methods (KEM) for constrained end-devices which are potential vectors of attacks. Current PQC proposals use more resources (e.g., ram, flash, cpu) than non-PQC cryptography, in particular requiring larger key sizes, and the question of their usability for embedded systems and constrained networks–like Internet of Things (IoT) systems remains unanswered. In this regard, we are exploring the feasibility the NIST-standard PQC KEM named Kyber, with a focus on the network messages to send on real networks (fragmentation, message standardization), we aim at standardizing the message formats at the IETF[6].

2.2.6 Interfaces with Security Operators

As a last research line, our research group addresses the novel 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. In the

[6] Internet Engineering Task Force

former direction, intent-based networking stands for a paradigm based on several steps, from the intention detection and understanding, up to the policy deployment, through intention translation, and detection of conflicts in the policies. State of the art use dedicated approaches, using named entities recognition and deriving them in a specialized language. However one could benefits from the latest neural networks studies with large language models. The main issue for learning or fine-tuning a language model is the lack of datasets and the research group starts investigating relevant datasets generation or manually crafted ones. In the opposite direction, our research team has been at the forefront for the exploration of multi-modal interfaces as powerful tools in the realm of cybersecurity, particularly in harnessing Virtual Reality (VR) as human-machine communication interface within cybersecurity 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.

2.3 Application domains

The different research topics exposed previously target different applications domains, all standing for future networks and services. Briefly, these are:

2.3.1 Protection of Low-Latency Network and Services

As a substantial requirement of future networks and services, minimizing latency or mastering it from a control perspective occurs in several situations that our research group tackles as use-cases. First, 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 now plan to cover the case of TSN where attack patterns rather target misconfigurations issues.

2.3.2 Protection of Individual Information Systems

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.

2.3.3 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.

2.3.4 Security Monitoring of Future Networks

The main goal in cybersecurity is to thwart attackers by detecting their actions, understanding their methodologies, and enhancing resilience against subsequent attempts. However, 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. Machine Learning (ML) offers a potential solution, generating non-reversible abstract models, but the challenge lies in the substantial data needed for a reliable impression. Federated Learning (FL) addresses 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.

2.3.5 Smart environments

For a decade, smart environments form the future of network and services, promising to provide novel services and experiences to customers assisted by plethora of sensors, actuators, altogether controlled by AI-based engines. Our research group handles such those environments in particular around Industry 4.0, Smart Buildings, and smart mobility.

[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.

3 Scientific achievements

3.1 Blockchain Alternative Structures and Applications

3.1.1 Mining in Logarithmic Space with Variable Difficulty

Participants: Benjamin Loison, Romaric Ludinard, Loïc Miller.

This work [15] has been published as Student paper in the IEEE BRAINS'23 conference. This is a joint work with Emmanuelle Anceaume from CIDRe/IRISA – UMR CNRS 6074 team.

This paper addresses the problem of scalability, which is preventing the widespread adoption of blockchains. Blockchain data is categorised into an application part and a consensus part, the latter growing linearly over time. Mining in Logarithmic Space, Kiayias et al. [KLZ21] provably solved this problem for a proof-of-work blockchain with a static difficulty by reducing storage and communication complexity to polylogarithmic. This paper focuses on the modification of this protocol to adapt it to a context with variable difficulty.

3.1.2 Collaborative Cybersecurity Using Blockchain: A Survey

Participants: Loïc Miller, Marc-Oliver Pahl.

Paper submitted to ACM Computing Survey [25]. Under review.

Our research team conducted a comprehensive survey on the application of Blockchain for cybersecurity, shedding light on its potential benefits, challenges, and open research avenues. Through an exhaustive review of existing literature and real-world implementations, our survey offers valuable insights into the evolving landscape of blockchain-based cybersecurity solutions. By synthesizing key findings and identifying emerging trends, we contribute to a deeper understanding of how blockchain technology can be leveraged to enhance security across various domains. Furthermore, our survey highlights critical research gaps and open issues, paving the way for future investigations and advancements in this burgeoning field. Through our scientific contributions, we aim to foster innovation and drive progress in the integration of blockchain technology for cybersecurity purposes.

3.1.3 Multipath Neural Networks for Anomaly Detection in Cyber-Physical Systems

Participants: Marc-Oliver Pahl.

Joint work with Raphaël M. J. I. Larsen, Gouenou Coatrieux: Work published in the Annals of Telecommunication [3] international journal.

[KLZ21] A. Kiayias, N. Leonardos, D. Zindros, "Mining in Logarithmic Space", in: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, CCS '21, ACM, 2021, https://doi.org/10.1145/3460120.3484784.

An Intrusion Detection System (IDS) is a core element for securing critical systems. An IDS can use signatures of known attacks, or an anomaly detection model for detecting unknown attacks. Attacking an IDS is often the entry point of an attack against a critical system. Consequently, the security of IDSs themselves is imperative. To secure model-based IDSs, we propose a method to authenticate the anomaly detection model. The anomaly detection model is an autoencoder for which we only have access to input-output pairs. Inputs consist of time windows of values from sensors and actuators of an Industrial Control System. Our method is based on a multipath Neural Network (NN) classifier, a newly proposed deep learning technique for which we provide an in-depth description. The idea is to characterize errors of an IDS's autoencoder by using a multipath NN's confidence measure c. We use the Wilcoxon-Mann-Whitney (WMW) test to detect a change in the distribution of the summary variable c, indicating that the autoencoder is not working properly. We compare our method to two baselines. They consist in using other summary variables for the WMW test. We assess the performance of these three methods using simulated data. Among others, our analysis shows that: 1) both baselines are oblivious to some autoencoder spoofing attacks while 2) the WMW test on a multipath NN's confidence measure enables detecting eventually any autoencoder spoofing attack.

3.2 Immersive Analytics

Participants: Marc-Oliver Pahl.

Joint work with Nicolas Delcombel and Thierry Duval(INIUT/LabSSTIC UMR CNRS 6285). This work has been published in the journal Frontiers Virtual Reality [1].

This paper assesses the usefulness of an interactive and navigable 3D environment to help decision-making in cybersecurity. Malware programs frequently emit periodic signals in network logs; however, normal periodical network activities, such as software updates and data collection activities, mask them. Thus, if automatic systems use periodicity to successfully detect malware, they also detect ordinary activities as suspicious ones and raise false positives. Hence, there is a need to provide tools to sort the alerts raised by such software. Data visualizations can make it easier to categorize these alerts, as proven by previous research. However, traditional visualization tools can struggle to display a large amount of data that needs to be treated in cybersecurity in a clear way. In response, this paper explores the use of Immersive Analytics to interact with complex dataset representations and collect cues for alert classification. We created a prototype that uses a helical representation to underline periodicity in the distribution of one variable of a dataset. We tested this prototype in an alert triage scenario and compared it with a state-of-the-art 2D visualization with regard to the visualization efficiency, usability, workload, and flow induced.

3.3 Collaborative Anomaly Detection

3.3.1 Federated Learning × Security in Network Management

Participants: Yann Busnel, Leo Lavaur.

This work [7] has been presented as a tutorial at the 14th IEEE International Conference on Network of the Future (NoF).

Federated learning (FL) is a machine learning (ML) paradigm that enables distributed agents to learn collaborative models without sharing data. In the context of network security, FL promises to improve the detection and mitigation of attacks, notably by virtually extending the local dataset of each participant. However, one of the major challenges of this recent technology is the heterogeneity of the data used by the participants. Indeed, some participants with very different monitoring contexts could penalize the global model. Furthermore, identifying malicious contributions is made more difficult in heterogeneous environments. In this work, we introduce the fundamentals of federated learning, then focus on its use in network monitoring, and more specifically, in collaborative intrusion detection (Federated Learning-based Intrusion Detection System-FIDS). Secondly, we address some of the open research questions in this context [4], before focusing on the problem of training data heterogeneity. Finally, we investigate the security of FL architectures, and more specifically, the problem of poisoning attacks.

3.3.2 Distributed Cross-evaluation for Reputation-aware Model Weighting in Federated Learning

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

Joint work with Pierre-Marie Lechevalier, Géraldine Texier (ADOPNET/IRISA – UMR CNRS 6074) and Hélène Le Bouder (OCIF/IRISA – UMR CNRS 6074), currently under submission at Esorics'24.

In the same context of Federated Learning for Collaborative IDS, negligent or malicious clients might, however, negatively contribute to the global model and degrade its performance. Existing approaches to detect adversaries tend to falter in heterogeneous settings, while Collaborative IDS federations are inherently heterogeneous.

In this work, we propose a novel Federated Learning architecture for intrusion detection, able to deal with both, heterogeneous and malicious contributions, without the need for a single source of truth. We leverage client-side evaluation for clustering participants based on their perceived similarity, and then feed these evaluations to a reputation system that weights participants' contributions based on their trustworthiness.

We evaluate our approach against four intrusion detection datasets, in both benign and malicious scenarios. We show that our clustering successfully groups participants originating from the same dataset together, while excluding the noisiest attackers. The reputation system then strongly limits the impact of stealthier attackers within each cluster, as long as they remain a minority. The comparison of our work with a state-of-the-art mitigation strategy highlights its versatility on both IID, and non-IID data for the different attack scenarios.

3.3.3 Collaborative Cybersecurity for Resource Constraint Devices using Data Gravity and Federated Learning

Participants: Marc-Oliver Pahl.

Joint work with Christian Lübben (Technical University of Munich), published and presented as a full paper and a demo in IEEE/IFIP Network Operations and Management Symposium (NOMS 2023) [17, 16].

Our efforts focus on harnessing the computational capabilities of edge devices, IoT sensors, and other distributed endpoints to collectively analyze and detect anomalies in data streams. By employing lightweight algorithms and intelligent task allocation strategies, we optimize the utilization of resources across the network while minimizing latency and energy consumption.

Furthermore, our research extends to the development of decentralized anomaly detection frameworks, where distributed devices collaborate autonomously to detect and mitigate anomalies in real-time. Through the integration of machine learning algorithms and distributed consensus mechanisms, we enable adaptive and resilient anomaly detection capabilities that scale with the size and complexity of the network.

By embracing collaborative anomaly detection, we aim to democratize the detection of cybersecurity threats, empowering distributed devices to contribute to the collective defense against emerging risks. Our ongoing research in this area holds the promise of enhancing the resilience and agility of cybersecurity systems in the face of evolving threats and vulnerabilities.

3.4 Securing the Industrial Internet of Things

Participants: Marc-Oliver Pahl.

Joint work with Erkin Kirdan (Technical University of Munich), published in IEEE/IFIP Network Operations and Management Symposium (NOMS 2023) [23], and here [2].

Through meticulous experimentation and analysis, we scrutinized the security posture of prominent IIoT protocols, such as MQTT, CoAP, and OPC UA, under various attack scenarios and operational conditions. Our research shed light on the strengths and weaknesses of each protocol in terms of data integrity, authentication, encryption, and resilience against common cyber threats.

Furthermore, our investigations extended to the evaluation of different security solutions, including lightweight encryption algorithms, secure bootstrapping mechanisms, and intrusion detection systems tailored for IIoT deployments. By benchmarking these solutions against key performance metrics, we gained valuable insights into their suitability for securing IIoT infrastructures while minimizing overhead and ensuring scalability.

3.4.1 Slow Denial of Service Attack on MQTT-Based IoT

Participants: Marc-Oliver Pahl.

Joint work with Erkin Kirdan, Patricia Horvath (Technische Universität München, Germany), published in the IEEE International Black Sea Conference on Communications and Networking [10].

This work presents an in-depth study of Slow Denial of Service (DoS) attacks on MQTT, a widely used communication protocol in loT networks, building upon the existing literature. Our research focuses on extending the capabilities of such attacks, successfully lifting the simultaneous client limit, and achieving more than 25,000 active connections. This increase resulted in a notable escalation in resource consumption, underscoring the potential vulnerabilities in MQTT-based loT systems. Furthermore, we have implemented a Distributed DoS (DDoS) variant of the attack for the first time by randomizing source IP addresses and simulating packets originating from multiple sources. This approach complicates the detection and mitigation efforts by Intrusion Detection Systems, revealing additional weaknesses in loT security. The findings emphasize the importance of developing robust security mechanisms and strategies to protect against Slow DoS and DDoS attacks in resource-constrained loT environments. This study contributes to the growing body of research in loT security, particularly concerning the MQTT protocol. By addressing these security challenges, we aim to facilitate loT deployments' continued growth and success across various domains.

3.4.2 Real-Time Sound-Based Anomaly Detection for Industrial Systems

Participants: Marc-Oliver Pahl, Fabien Autrel.

Joint work with Awaleh Houssein Meranehand Hélène Le Bouder (OCIF/IRISA – UMR CNRS 6074), published in the 16th International Symposium on Foundations Practice of Security (FPS) conference [19].

Industrial cyber-physical systems are critical infrastructures vulnerable to cyber-attacks. Anomaly and intrusion detection are widely used approaches to enhance the security of these systems. This paper investigates side-channel leakages, particularly sound, for high-accuracy detection of intrusions and anomalies in various industrial systems. Despite sound signal's advantages, such as low-cost equipment, minimal computational requirements, and non-invasive measurement. Current sound-based anomaly detection (SAD) methods face challenges such as sensitivity to background noise, unbalanced sound data, computational costs, and detection accuracy. To tackle these issues, we introduce robot-arm sound dataset (RASD) and present a real-time sound-based anomaly detection for industrial systems (SADIS) approach that uses a simple and efficient method to fingerprint expected sound data with reduced dimensions. Our experiments demonstrate that the SADIS approach achieves an average attack detection rate of over 96%, with a detection time of less than 1 s and low computational costs.

3.5 Protection of Low-Latency Networks and Service

3.5.1 A Comprehensive Characterization of Threats Targeting Low-Latency Services: The Case of L4S

Participants: Guillaume Doyen.

Joint work with Marius Letourneau, Rémi Cogranne (LIST3N/Université de Technologie de Troyes) and Bertrand Matthieu (Orange Innovation) published in the Journal of Network and Service Management [5].

New services with low-latency (LL) requirements are one of the major challenges for the envisioned Internet. Many optimizations targeting the latency reduction have been proposed, and among them, jointly re-architecting congestion control and active queue management (AQM) has been particularly considered. In this effort, the Low Latency, Low Loss and Scalable Throughput (L4S) proposal aims at allowing both Classic and LL traffic to cohabit within a single node architecture. Although this architecture sounds promising for latency improvement, it can be exploited by an attacker to perform malicious actions whose purposes are to defeat its LL feature and consequently make their supported applications unusable. In this paper, we exploit different vulnerabilities of L4S which are the root of possible attacks and we show that application-layer protocols such as QUIC can easily be hacked in order to exploit the over-sensitivity of those new services to network variations. By implementing such undesirable flows in a real testbed and characterizing how they impact the proper delivery of LL flows, we demonstrate their reality and give insights for research directions on their detection.

3.5.2 A Comprehensive P4-based Monitoring Framework for L4S leveraging In-band Network Telemetry

Participants: Guillaume Doyen.

Joint work with Marius Letourneau (LIST3N/Université de Technologie de Troyes), Huu Nghia Nguyen and Edgardo Montes De Oca (Montimage), Bertrand Matthieu and Stéphane Tuffin (Orange Innovation) published in the IFIP/IEEE Network Operations and Management Symposium, NOMS [22].

The Low-Latency Low-Loss Scalable throughput (L4S) architecture has recently been proposed to reduce the network latency of low-latency services and to allow their flows to coexist with classic ones in the same domain. This coexistence implies monitoring and security challenges. However current monitoring methods, primarily based-on sampling and polling, exhibit performance and granularity limitations. This paper describes the challenges for monitoring LL services and details our solution when introducing a fine-grained and real-time monitoring capability in our P4-based L4S implementation using In-band Network Telemetry. The initial experimental evaluation shows that our solution is able to monitor the metrics of an L4S switch with very few networking and processing overhead and without disturbing the L4S behaviour.

3.6 Robust Security Configurations

3.6.1 A Robust Approach for the Detection and Prevention of Conflicts in I2NSF Security Policies

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

This work has been published in the IEEE/IFIP Network Operations and Management Symposium, NOMS [21].

In order to maintain a sufficient protection level of their infrastructure, automating security management is at the core of current operators issues. The Interface to Network Security Function (I2NSF) is a framework that takes part of the Intent-Based Networking (IBN) paradigm. It consists of automating the translation of high-level policies into low-level configurations of Network Security Functions (NSF) and appears as a promising way to overcome the complexity of this challenging task. However, if the I2NSF framework provides a comprehensive architectural and data model for such an automation, it provides neither detection nor prevention mechanisms against conflicting security requirements. In this paper, we assess to what extent state-of-the-art mechanisms can shift the initial I2NSF proposal toward a robust framework. As such, we extend (1) the reference architecture to integrate some checking components and (2) the consumer-facing data model to enforce separation constraints and partial ordering relationships. By considering a large set of rules and conflicting situations, we evaluate the performance of our solution within an early implementation of I2NSF achieved in an IETF Hackathon.

4 Results of Research Activities Aside from the Team Project

Since the SOTERN research group officially exists for one year while all the permanent people is already involved in research activities, several results of this year are issued by existing of ending activities and projects which are aside from the core team project exposed above. Those results are provided here and for most of them, they act as substrates or backgrounds that feed the current team own activities.

4.1 Management of NFV and Microservices for Low-Latency service chains

4.1.1 AI-based Dynamic Scaling of Containerised Network Functions

Participant: Ahmed Bouabdallah.

Joint works [12, 11] co-authored with: Menuka Perera Jayasuriya Kuranage and Loutfi Nuaymi (IRISA/INRIA OCIF, IMT Atlantique), Thomas Ferrandiz, Elisabeth Hanser and Philippe Bertin (BCom, France), Anwer Al-Dulaimi (EXFO, France)

By adopting a Kubernetes-based cloud-native approach, 5G and more generally NFV-based networks exploit the potential for great flexibility through dynamic scalability of network functions. Complexity of the concerned infrastructures requires however the development of automated network resources management approaches. To this end a new deep learning-based resource usage forecasting approach in the Kubernetes environment, is introduced. The approach is benchmarked against other deep learning-based resource forecasting approaches and proved providing more accurate forecasting. Compared with the native Horizontal Pod Autoscaling (HPA) approach of Kubernetes, the proposed approach is also proved to outperform such scaling mechanisms in terms of maintaining QoS levels during scaling and reducing operational costs.

4.1.2 A Fair Sharing Approach for Micro-Services Function Chains Placement in Ultra-Low Latency Services

Participants: Guillaume Doyen.

Joint work with Hichem Magnouche and Caroline Prodhon(LIST3N/Université de Technologie de Troyes), accepted in 2023 and published in 2024 in IEEE Transactions of Network and Service Management (TNSM) [6].

The evolution of Internet services, such as drone piloting or metaverse, tends toward ultra-Low Latency (LL) requirements, thus inducing new challenges in the placement of Service Function Chains (SFCs) deployed over virtualized infrastructures. On the one hand, this challenge requires novel optimization means. In particular, decomposing monolithic Network Functions (NFs) into micro-services acts as a promising approach thanks to their mutualization and highly parallelization characteristics, which makes it possible to reduce the length of the service chains and consequently their execution latency. On the other hand, since a core feature of the Internet relies on the coexistence of several types of services, fair sharing of resources between LL SFCs and Best Effort (BE) services appears as a core question to address. In this paper, we present an optimization model, which leverages the characteristics of micro-services to place and chains different types of SFCs in a common infrastructure. We first consider the case of standalone LL SFCs to demonstrate the benefits of mutualization and parallelization. Then, we consider the more complex situation of a fair cohabitation between BE and LL SFCs. This leads us to propose and compare three variants of our initial objective function, all supporting different resource sharing strategies. By confronting our model to several realistic scenarios in terms of topology and service function chains, we demonstrate (1) to what extent it improves the overall performance of SFCs by minimising the gap between expected and actual latency, and (2) it allows LL and BE SFCs to coexist without impacting the latency of the deployed LL SFCs.

4.1.3 A Lightweight Heuristic for Micro-Services Placement and Chaining in Low Latency Services

Participants: Guillaume Doyen.

Joint work with Hichem Magnouche and Caroline Prodhon (LIST3N/Université de Technologie de Troyes) published in the IFIP/IEEE Conference on Network and Service Management (CNSM) [18].

The rise of novel Low-Latency (LL) applications, such as cloud gaming or the metaverse, imposes rigorous end-to-end LL constraints. Decomposing Virtualized Network Functions (VNFs) into micro-services has proven its effectiveness to reduce the Service Function Chaining (SFC) latency thanks to key characteristics: lighter entities, less resource consumption, and a strong capacity to operate in parallel. However, to make such a promising technology actually deployed in real operated networks, novel dedicated placement and chaining methods are required. Current solutions either do not fit with tied LL constraints or exhibit a prohibitive computation time by relying on exact resolution methods. In this paper, we propose a heuristic method dedicated to the placement and chaining of micro-services. Its purpose is to maximize the deployment of SFCs while respecting the required LL by considering intrinsic features of micro-services and integrating suitable load balancing, which makes it highly scalable. A comprehensive evaluation campaign highlights that generated solutions achieve results that are at most a factor of 1.1 to the optimal with an execution time up to 20,000 times faster.

4.1.4 Applying Fuzzy Logic to Efficiently Manage Shared Edge Infrastructure

Participants: Mohamed Aymen Chalouf.

Joint work [24] with Tidiane Sylla, Leo Mendiboure, Francine Krief, Hasnaa Aniss and Lylia Alouache (Ifsttar/Université Gustave Eiffel)

Edge Computing promise a bright future for Internet of Things (IoT). Edge Computing servers can be geographically distributed to be closer to users and ensure low latency communications and real-time data processing for the third-party applications using this infrastructure. However, user mobility and limited Edge servers capabilities (CPU, memory, bandwidth) may cause many services placement failures. That's why in this article we propose a new strategy aimed at enabling a fair sharing of available Edge resources through a dynamic and real-time IoT service placement. Our strategy uses Fuzzy Logic to enable 1) quick and low-cost deployment of the solution and 2) real-time modification of the policies defined by the Edge operator. It takes advantage, among others, of a microservice decomposition to optimize the use of the Edge architecture. Experiments demonstrate the benefits of our approach in terms of placement reliability, execution time and resources utilization.

4.2 IoT and Autonomous Wireless Systems

4.2.1 Energy-Aware Spreading Factor Selection in LoRaWAN Using Delayed-Feedback Bandits

Participants: Renzo E. Navas.

Joint work [20] in the context of INTELLIGENTSIA ANR Project (ANR-20-CE25-011). Co-authored with: Ghina Dandachi, Yassine Hadjadj-Aoul (IRISA/INRIA Ermine, University of Rennes 1), and Patrick Maillé (IRISA/INRIA Ermine, IMT Atlantique).

LoRaWAN networks can involve large numbers of wireless devices relying on batteries to sense the environment and send data to gateways. A critical trade-off for transmission performance (packet delivery ratio) versus energy conservation (and hence, the device lifespan) appears when deciding the transmission parameters, in particular, the Spreading Factor (SF) to be used by each node. In this paper, we use lightweight reinforcement learning techniques, namely multi-armed bandits, for each node to select an appropriate SF, based on preferences regarding that trade-off. Unlike previous works on that topic, we relax some assumptions to aim at a realistic implementation: our solution does not assume immediate rewards, or that each device communicates with only one gateway. Additionally, we build explicit MAC commands for the method to work in practice and implement it in the ns-3 simulator using a state-of-the-art LoRaWAN module. We share the source code of our implementation and our simulation results. Those simulations show that when energy conservation is critical for IoT nodes, such lightweight learning algorithms outperform LoRaWAN's legacy Adaptive Data Rate algorithm, both in single-and multi-gateway scenarios.

4.2.2 Leveraging IoT technologies for DNS "RESTification"

Participant: Ahmed Bouabdallah.

Joint works [13, 14] in the context of the ANR project DiNS (ANR-19-CE25-0009-01). Co-authored with: Arnol Lemogue, Laurent Toutain(IRISA/INRIA OCIF, IMT Atlantique) and Ivan Martinez (Nokia Bell Labs).

DNS RESTification is an attractive solution to allow the Naming System to evolve at the same pace as the Internet. However, if implemented directly, RESTification may lead to an unacceptable degradation of Internet performance. A first contribution, exploiting advances in the Internet of Things, leads to the development of an efficient encoding of DNS messages based on CBOR, providing a compact, flexible and high-performance DNS/DNSSEC format while maintaining compatibility with existing protocols. A second contribution concerns the ability to segment traditional architectures to allow private resolutions to control access to network resources, while reducing the number of messages exchanged when these resolutions are authorised. These approaches are illustrated in the use case of roaming between LoRaWAN network operators.

4.2.3 FTM-Broadcast: Efficient Network-wide Ranging

Participants: Yann Busnel.

Joint work [8] with Hervé Rivano from CITI, INSA Lyon.

Indoor geolocation has witnessed a significant advancement through the refinement of the 802.11 FTM (Fine Timing Measurement) protocol. Accurate indoor geolocation has numerous applications in areas such as asset tracking, indoor navigation, and location-based services. The standard 802.11 FTM protocol enables accurate indoor positioning by measuring the time-of-flight between a mobile device and multiple access points (APs). It can be generalized to device-to-device ranging. However, the conventional implementation of FTM suffers from increased complexity as the number of devices grows, limiting its scalability. FTM indeed involves a point-to-point exchange of messages between each pair of devices, leading to a quadratic increase in the number of messages as the number of neighboring devices increases. In this work, a breakthrough method is proposed to enhance the FTM protocol by leveraging broadcast communication, resulting in a substantial reduction in message complexity from quadratic to linear [8]. By taking into account broadcast in the protocol, our approach eliminates the need for multiple individual exchanges and devises a mechanism where a single message from the mobile device is broadcasted to all neighbors simultaneously. Each message exchanged will then be useful for computing every pairwise time-of-flight, by piggy-backing all timestamps, making the protocol more efficient and scalable. We conducted extensive simulated experiments to evaluate the performance of the enhanced FTM protocol. The results demonstrated the effectiveness of the proposed method, showcasing a substantial reduction in computational overhead compared to the conventional FTM implementation.

4.2.4 Trajectory Optimization for Fast Sensor Energy Replenishment using UAVs as RF sources

Participants: Yann Busnel.

Joint work [9] with Igor Dias da Silva and Christelle Caillouet from Inria Sophia Antipolis, Université de Côte d'Azur.

The problem of the lifetime of connected objects, in most use cases (Industrial Internet of Things (IIoT), disaster management, etc.) is an essential element of the proposed solutions. Radio frequency (RF) harvesting of sensor batteries is an attractive solution, however, it does not scale up if it has to be done by human operators, and becomes impossible if the objects are located in unreachable places. An innovative solution consists of using fleets of drones to take care of this regular recharge. In this work, we focus on the self-organised deployment of a fleet of drones to solve this problem, taking into account the multiple constraints involved [9]. We propose a two-step optimization framework based on an optimal orchestration solution to reduce the recharging time of a complete sensor system, by optimizing the number of drones, the overall flight time and their energy consumption. We illustrate the performance of our framework that ensures the drones avoid conflicts to guarantee a higher energy harvesting efficiency (establishment of optimal drone positions and planning of the global flight plan).

5 Software development

5.1 Platforms and Modules

During the first year of the research team activities, several codes have been produced, all of them accompanying some scientific contributions exposed previously.

Participants: Fabien Autrel, Léo Lavaur, Do Duc Anh Nguyen, Renzo Navas.

5.1.1 DatasetGen

DatasetGen is used within the context of Léo Lavaur's PhD thesis 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).

The code is currently hosted on the IMT Atlantique gitlab service: `https://gitlab.imt-atlantique.fr/fautrel/feditn-topology-generator`. The Python code consists in 1323 lines of code.

5.1.2 I2NSF policy conflict detection and mitigation implementation

The Interface to Network Security Function (I2NSF [HLZ+17]) is the result of an IETF working group which defines a set of software interfaces and data models for controlling and monitoring physical and virtual NSFs, enabling clients to specify rulesets, or more formally security requirements, i.e. security policies. In [21], we proposed an approach to detect and mitigate policy conflicts, which has been implemented as a extension to the reference implementation[7] of the I2NSF specification. The implementation of this approach consists in two additional modules to the original I2NSF implementation:

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

The code is currently hosted on the IMT Atlantique gitlab service: `https://gitlab.imt-atlantique.fr/d22nguye/i2nsf-conflict-detection`. The python code consists in 302 lines of code added to the security controller.

5.1.3 Energy-Aware Spreading Factor Selection in LoRaWAN Using Delayed-Feedback Bandits: Code and Data

Participants: Renzo E. Navas.

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

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

This source code [26] goes with the peer-reviewed paper [20] presented in section 4.2.2. This C++ code is based on the ns-3 discrete event simulator and a state-of-the-art LoRaWAN module. We use lightweight reinforcement learning techniques, namely multi-armed bandits, for each LoRaWAN node to select an appropriate Spreading Factor, based on preferences regarding that trade-off. We relax some assumptions to aim at a realistic implementation: our solution does not assume immediate rewards, or that each device communicates with only one gateway. Additionally, we build explicit LoRaWAN MAC commands for the method to work in practice. We share the source code of our implementation, our simulation results (including scripts we used to calculate metrics and do some plots), and design information that justifies the metrics and some important decisions we took along the way [26].

Direct URLs are `https://doi.org/10.5281/zenodo.7876244`https://doi.org/10.5281/zenodo.7876244 (perennial) or `https://github.com/renzoe/LoRaWAN-Bandits/tree/v1.0.0`https://github.com/renzoe/LoRaWAN-Bandits/tree/v1.0.0. The C++ code consist on a bit more than 3000 lines of code, almost exclusively on the ns-3 LoRaWAN module and mostly on `https://github.com/renzoe/LoRaWAN-Bandits/tree/v1.0.0/ns-3/src/lorawan/model/bandits`https://github.com/renzoe/LoRaWAN-Bandits/tree/v1.0.0/ns-3/src/lorawan/model/bandits.

6 Contracts and collaborations

6.1 International Initiatives

6.1.1 CyberSecDome

Participants: Marc-Oliver Pahl.

- Project type: Horizon Europe
- Dates: 2023–2026
- PI institution: IMT Atlantique
- 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.

6.1.2 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: IMT Atlantique
- 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.

6.2 National Initiatives

6.2.1 Superviz

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

- 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.

6.2.2 HiSec

Participants: Fabien Autrel, Ahmed Bouabdallah, Guillaume Doyen..

- Project type: Priority Program and Equipment for Research (PEPR) Network of Future
- Dates: 2022–2026
- PI institution: Guillaume Doyen
- Other partners: IMT-Télécom Paris, IMT Télécom SudParis, Eurecom, CNRS and related labs: ETIS, IETR, IRISA, LAAS, XLIM CEA LIST, INRIA related labs: LORIA

Networks, due to their necessary openness and their economic value, are prime targets for attackers. The HiSec project develops new methods and tools to secure the networks of the future. More specifically, it covers 5 major objectives. The first objective concerns the protection of these networks, through the specification and deployment of end-to-end security policies. The second objective aims to detect and manage attacks in these complex environments. The third objective aims to protect personal data in the case of lawful interception. The fourth objective aims to model the operation of the security mechanisms of these networks, so as to ensure that the security services provided correspond to the needs of the applications which request them. The fifth objective aims to formalize the link between hardware and software layers on the one hand, and security properties, to ensure the integration of cyber mechanisms in all layers of the network.

6.2.3 Towards Public Blockchain for Self-Sovereign Identities – BC4SSI

Participants: Romaric Ludinard, Loïc Miller..

- Project type: ANR JCJC

- Dates: 2023–2027
- PI institution: Romaric Ludinard
- Other partners: Emmanuelle Anceaume from CIDRe/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.

6.2.4 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.

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

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

6.2.6 INTELLIGENTSIA: INTelligent Edge using Learning Loops & Information GEneration for NeTwork State Inference-based Automation

Participants: Renzo E. Navas.

- Project type: ANR PRCE
- Dates: 2020–2024
- PI institution: Patrick Maillé
- Other partners: Orange, Aguila, Acklio, CNAM, Inria (Ermine)

In the era of network softwarization, INTELLIGENTSIA objective is to fast move towards automation of end-to-end network operations by leveraging advanced learning algorithms able to scale with large-scale virtualized networks and to meet control and operations requirements of massive IoT use-cases. The targeted scientific contributions are related to the elaboration of a dynamic state machine framework for modeling a network virtualization platform, based on clustering and classification algorithms. The learning framework is meant to discover in real-time known and unknown network states, as well as to anticipate reconfigurations of the network and in particular of novel IoT radio access functions in addition to device behavior and network backhauling. The expected impact includes the enhancement of network automation platforms considered by the Industry and the design of novel IoT radio access functions.

6.2.7 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.

6.2.8 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.

6.3 Regional Initiatives

6.3.1 Rennes Metropole Chair : OM&AI2MD (2021 - 2024)

Participants: Fabien Autrel, Yann Busnel, Sulaiman Mohammad.

Operations Models and Artificial Intelligence to Manage Disasters The objective of this Chair is to provide decision-makers (public organisations, governments, cities, etc.) with decision support tools (mathematical models, decision support systems, software) to deal with natural (including pandemics/ epidemics) and man-made disasters (including technological disasters). We will propose solutions based on distributed algorithms and real-time data processing regarding natural and technological disasters. In particular, we utilize artificial intelligence to ensure near-optimal solutions to the problems raised (e.g., victim location and rescue, aid distribution etc.).

Joint work with Rennes School of Business

6.4 Bilateral industry grants

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

Participants: Marc-Oliver Pahl.

- Project type: Industrial Research Chair
- Dates: 2022–2024
- PI institution: IMT Atlantique
- 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. The chair provides a unique environment for cybersecurity research with lots of development possibilities.

6.5 Collaborations

6.5.1 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: IMT Atlantique

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.

6.5.2 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: IMT Atlantique

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.

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

Participants: Renzo E. Navas.

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

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

6.5.4 SUPCOM/University of Carthage PhDs (2023 - 2027)

Participants: Mohamed Aymen Chalouf.

- Project type: Co-supervision of PhDs work in the context of International collaboration with Tunisia ("Digital Security" research lab, SUPCOM, Tunisia)
- Dates: 2023–2027
- PI institution: Mohamed Aymen Chalouf
- Other partners: Ryma Abassi and Aida Ben Chehida Douss ("Digital Security" research lab, SUPCOM, Tunisia), Omessaad Hamdi (IEEE Member, France).

Given its numerous advantages (decentralized management removing the single point of failure, robustness, availability, interoperability, etc.), blockchain represents an alternative to traditional secure communication and storage systems and can be very interesting in new network architectures. The use of blockchain for the security of networks and applications presents several challenges in relation with the intrinsic functioning of this technology. Among these challenges, we will focus on those related to anonymity and security of the blockchain itself. Anonymity is a very important property, especially in certain areas such as electronic government systems (e-government). Since blockchain provides only pseudonymity thanks to identifiers associated to users and because of the complete anonymization is starting to be criticized because it is incompatible with the KYC (Know Your Customer) system, we must define new anonymization mechanisms allowing a compromise between anonymity and legal responsibility. Furthermore, blockchain security relies on the integrity of the nodes participating in the consensus. In a highly mobile environment with frequent nodes departures and arrivals like drone networks, this security can be quickly compromised. This requires new solutions to ensure the integrity of a large part of the key nodes in a blockchain with several mobile ones. These solutions could, for example, be based on specific types of consensus (e.g. Proof of Authority) coupled with the maintenance of certain key nodes in the blockchain regardless of the mobility of the other ones. PhD students are Naouress Kairallah and Amine Hedfi ("Digital Security" research lab, SUPCOM, Tunisia) and theirs thesis subjects are respectively *Security of e-govenment systmes* and *Security of Internet of Drones*. Co-supervised with Ryma Abassi, Aida Ben Chehida Douss and Omessaad Hamdi.

7 Dissemination

7.1 Promoting scientific activities

7.1.1 Scientific Events Organisation

General Chair, Scientific Chair

Guillaume Doyen served as a co-chair of the Research and Innovation Roadmap for Brittany Workshop organized by EDIH Bretagne during the European Cyber Week, ECW.

Member of the Organizing Committees

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

- 25èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel 2023).
- 8èmes Rencontres Francophones sur la Conception des protocoles, l'évaluation de performance et l'expérimentation des réseaux de communication (CoRes 2023),
- 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2023),
- French/Japanese Workshop on Blockchain technologies and applications to digital trust.

Renzo E. Navas served as an organization committee member in the following conference:

- The 3rd IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT) co-located with NOMS 2023.

Marc-Oliver Pahl served as an organization committee member in the following conferences

- Demo Co-Chair, IFIP/IEEE Conference on Network and Service Management, CNSM
- TPC-Co-Chair, ACM SigComm 1st Workshop on Enhanced Network Techniques and Technologies for the Industrial IoT to Cloud Continuum, IIoT-Nets
- Demo Co-Chair, IFIP/IEEE Network Operations and Management Symposium, NOMS
- The 3rd IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT) co-located with NOMS 2023.

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

- Workshops Co-Chair, IFIP/IEEE Network Operations and Management Symposium, NOMS,
- Tutorial co-chair, IEEE Networks of Future, NoF,
- PhD Symposium Co-Chair, IEEE Conference on Network Softwarization, Netsoft.

7.1.2 Scientific Events Selection

Chair of Conference Program Committees

Renzo E. Navas served as a TPC chair in the following conference:

- The 3rd IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT) co-located with NOMS 2023.

Member of Conference Program Committees

Ahmed Bouabdallah served as a TPC member in the following conferences:

- COMPSAC 2024 Symposium on Security, Privacy & Trust in Computing (SEPT)
- COMPSAC 2023 Symposium on Security, Privacy & Trust in Computing (SEPT)

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

- 8th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM 2023),

- 11th IEEE International Workshop on e-Health Pervasive Wireless Applications and Services (eHPWAS 2023).

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

- 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2023),
- 5th Conference on Advances in Financial Technology (AFT 2023),
- 25èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel 2023).

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

- IEEE/ IFIP Conference on Network and Service Management, CNSM,
- ACM SigComm 1st Workshop on Enhanced Network Techniques and Technologies for the Industrial IoT to Cloud Continuum, IIoT-Nets,
- IEEE Network Operations and Management Symposium, NOMS,
- The 3rd IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT) co-located with NOMS 2023.

Guillaume Doyen served as a TPC member in the following conferences:

- IFIP/IEEE Network Operations and Management Symposium, NOMS,
- IEEE Networks of Future, NoF,
- IEEE Conference on Network Softwarization, Netsoft,
- IFIP/IEEE Conference on Network and Service Management, CMSN,
- ACM SIGCOMM – Internet Measurement Conference, IMC (Posters TPC),
- IEEE Conference on Network Functions Virtualization and Software-Defined Networking, NFV-SDN (Doctoral Symposium),
- Forum International de la Cybersecurité, FIC (Master Class).

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

- IFIP/IEEE Network Operations and Management Symposium, NOMS - Demo Session.

7.1.3 Journal

Member of the Editorial Boards 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.

Guillaume Doyen served as an Associate Editor for the following journal:

- Springer Journal of Network and Systems Management, JNSM.

Reviewer - Reviewing Activities

Ahmed Bouabdallah served as a Reviewer for the following journals:

- Elsevier Computer Communications,
- Oxford Academic, The Computer Journal.

Mohamed Aymen Chalouf served as a Reviewer for Elsevier International Journal of Computer and Telecommunications Networking.

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.

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

- Springer Journal of Network and Systems Management, JNSM
- Wiley International Journal of Network Management, IJNM
- IEEE Transactions on Network and Service Management, TNSM
- IEEE Transactions on Industrial Informatics, TII
- IEEE Transactions on Industrial Electronics, TIE

Guillaume Doyen served as a Reviewer for the following journals:

- Springer Journal of Network and Systems Management, JNSM
- IEEE Transactions on Network and Service Management, TNSM
- IOS Press Journal of Computer Security

7.1.4 Invited Talks

Yann Busnel gave the following invited talks:

- *How Federated Learning Help in Incident Detection of Large-scale Network Security?* Keynote with Leo Lavaur at EUR CyberSchool, Rennes, France, April 2023
- *How AI and federated learning will revolutionize large-scale network security ?* Invited talk at IIT Indore, India, March 2023
- *The value of learning for securing large-scale networks.* Invited talk at IMT Webinar – Cyber&Risque, Online, March 2023
- *The value of learning for securing large-scale networks.* Invited talk at IMT-Inria-NICT Cybersecurity Workshop, Campus Cyber, Paris, France, March 2023
- *Blockchain : an introduction to large-scale distributed systems.* Invited talk at IIT Indore, India, January 2023

Marc-Oliver Pahl gave the following invited talks:

- *The Metaverse – Risk or Chance: a Cybersecurity Perspective*, FIC 2023, Masterclasses and Research Presentations of the CNRS
- *Making use of the Metaverse for increasing CyberSecurity: Immersive Data Analytics*, Siemens Research and Innovation Ecosystem (Siemens RIE) "Digitalization & Low Code Engineering in Industry"
- *Current challenges and opportunities with the chaire Cyber CNI*, Pôle Excellence Cyber (PEC), La French Tech Rennes – St Malo POOOL.
- *Cybersecurity and Metaverse*, Supply Chain and Logistics Institute of Georgia Institute of Technology
- *Securing the world of tomorrow*, School of Cybersecurity and Privacy of Georgia Institute of Technology
- *Cybersecurity as Central Factor towards Resilient Networks and Services*, Panel at NOMS 2023
- *Cybersecurity – a European perspective*, Florida International University
- *The technological millefeuille: from sensor security to data processing*, ESAIP École d'Ingénieurs
- *Defending the Digital Realm: A Holistic Approach to Cybersecurity from the sound of Robot Arms over collaborating competitors to Human Retinas*, Keynote at the 8th International Conference on Mobile, Secure and Programmable Networking in Paris
- *Recent advances of the chaire Cyber CNI*, ECW 2023

Guillaume Doyen gave the following invited talks:

- *Challenges et contributions sur l'autoprotection de l'Internet du futur*, Colloque IMT Cyber et Résilience
- *Besoin de compétences en Cyber dans le paysage national*, Cybermatinées Le Monde Informatique, Table Ronde
- *When (low-) latency matters: protecting Future Internet services against malicious flows*, Délégation de doctorants américains et français, réunis par l'ambassade de France à Washington dans le cadre du programme FADEX

7.1.5 Leadership within the Scientific Community

Yann Busnel is member of the Scientific Council of CEFIPRA — *Indo-French Centre for Promotion of Advanced Research* since june 2023.

7.1.6 Scientific Expertise

Mohamed Aymen Chalouf served as scientific expert for:

- ANR on PRC projects,
- ANRT on CIFRE projects.

Ahmed Bouabdallah served as scientific expert for ANR on PRC projects.

Romaric Ludinard served as scientific expert for ANR on PRCI projects.

Marc-Oliver Pahl contributed with two articles to two research initiatives:

- Co-authorship of the Whitebook of the Pole d'excellence Cyber on LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION
- Vision paper on "Open Standards and Open Education as Motor for Innovation"

7.1.7 Research Administration

Yann Busnel acts as the co-chair of Distributed System topix in the Network and Distributed Systems CNRS Research group (GDR RSD) ans is member of the steering committee.

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

Guillaume Doyen is a Steering Committee member of RESSI - *Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information.*

Marc-Oliver Pahl is member of the Steering Committee of

- German-French Academy for the Industry of the Future (GFA)

- German Informatics Society (GI)

Marc-Oliver Pahl is president of the German Chapter of the ACM (GChACM).

7.2 Teaching, supervision

7.2.1 Teaching

- École d'Hiver Recherche EUR CYberschool : Les blockchains publiques comme support aux identités auto-souveraines : verrous et enjeux, Romaric Ludinard
- Blockchain & Consensus, coopération dans les systèmes distribués, IMT Atlantique, Engineering track, Romaric Ludinard & Yann Busnel
- Blockchain, EUR Cyberschool, Master 2, Romaric Ludinard
- Systèmes concurrents et répartis, CentraleSupélec, Engineer degree 3rd year, Romaric Ludinard
- Operating Systems, IMT Atlantique, Engineering track, Renzo E. Navas and Guillaume Doyen.
- Web Security, IMT Atlantique , Engineering track, 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 réseaux, IMT Atlantique et Centrale Supélec, Mastère Spécialisé Cyber, Ahmed Bouabdallah, Guillaume Doyen.
- Sécurité des applications, IMT Atlantique, TAF Cyber, Ahmed Bouabdallah.
- Supervision des Systèmes et Audit, IMT Atlantique, TAF Cybver, Guillaume Doyen.
- Architectures de services de l'Internet, IMT Atlantique, TAF PNUM, Ahmed Bouabdallah.
- Virtualisation des réseaux, IMT Atlantique, TAF PNUM, Ahmed Bouabdallah.
- Cybersécurité des systèmes embarqués, IMT Atlantique, Engineering track, Marc-Oliver Pahl.
- Network security, Bordeaux INP, Engineering track, Mohamed Aymen Chalouf.

7.2.2 Supervision

- Licence 2 intern: Thomas Sericola supervised by Romaric Ludinard
- Master 1 intern: Benjamin Loison [15] supervised by Romaric Ludinard and Loïc Miller
- Master2 research project: Ahmed Abid, *blockchain based unikernel deployment*, supervised by Pierre Alain
- Master2 research project: Thibaut Laurent and Valentin Thury-Guenin, *Android malware classification using neural networks*, supervised by Pierre Alain
- Master2 research project: Rémi Jean, *Phishing e-mail classification using neural networks*, supervised by Pierre Alain
- Master 2 intern: Juan Ignacio Migliorisi (UBA, Argentina), *Post-Quantum Cryptography Key Establishment for constrained IoT nodes and networks*, supervised by Renzo E. Navas.

- PhD 2020-: Leo Lavaur, *Threat intelligence tools for IoT threat indexing and cooperative sharing*, coadvised by Yann Busnel & Fabien Autrel & Marc-Oliver Pahl
- PhD 2021-: Antoine Rebstock, *Extraction de scénarios probables d'attaques*, coadvised by Yann Busnel & Romaric Ludinard
- PhD 2021-: Pierre-Marie Lechevalier, *Mécanismes de confiance dans les environnements 5G*, coadvised by Yann Busnel, Hélène Le Bouder (OCIF), Romaric Ludinard, Géraldine Texier (ADOPNET).
- PhD 2020-: 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 2020-2023: Nicolas Delcombel, *Cyber sécurité en réalité virtuelle : améliorer le processus de détection d'intrusion d'investigation et de décision via l'utilisation de techniques de visualisations 3D immersives*, coadvised by Marc-Oliver Pahl, Thierry Duval (Lab-Sticc/INUIT).
- PhD 2018-2024: Christian Lübben, *Optimizing IoT Smart Spaces using advanced Data Analytics*, co-supervised by Marc-Oliver Pahl, Georg Carle (i8 – TU München)
- PhD 2019-2024: 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 2019-2024: Lars Wüstrich, *Multi-Layer Dependency Identification in Computer Networks*, co-supervised by Marc-Oliver Pahl, Georg Carle (i8 – TU München)
- PhD 2022-2023: Lucie David, *Assisted immersive interfaces for cybersecurity*, coadvised by Marc-Oliver Pahl, Thierry Duval (Lab-Sticc/INUIT).
- 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*, supervized by Pierre Alain, Ahmed Bouabdallah, Fabien Autrel and Jérome François (SNT, Luxembourg)
- 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), and Georgios Papadopoulos (OCIF).
- PostDoc 2022-2024, Loic Miller, *Blockchain security*, co-supervised by Marc-Oliver Pahl, Romaric Ludinard
- PostDoc 2022-2024, Nisrine Ibadah, *Secure Software Updates*, supervised by Marc-Oliver Pahl

7.2.3 Juries

Yann Busnel has been a reviewer for the following PhD juries:

- Fazail Amin (Indian Institute of Technology, Patna), in September 2023,
- Suchitra Agarwal (Indian Institute of Technology, Indore), in November 2023.

Mohamed Aymen Chalouf participated in the following PhD juries:

- Ziad TLAISS, Automated network packet traces analysis methods for fault recognition and TCP flavor identification, IMT Atlantique, Brest.

Marc-Oliver Pahl participated in the following PhD juries:

- Nataasha Alkhatib, Intrusion Detection with Deep Learning for In-Vehicle Networks, Télécom Paris
- Mehdi Zakroum, Machine Learning for the Automation of Cyber-threat Monitoring and Inference, UNIVERSITÉ DE LORRAINE, Université Internationale de Rabat

Guillaume Doyen has been a reviewer for the following PhD jury:

- Raoul Raftopoulos, *Integrating Deep Reinforcement Learning in 6G Edge Environments: Towards Intelligent Network Optimization*, University of Catania

7.2.4 Responsabilities

- Pierre Alain is head of a double degree track: Computer Science Engineering Degree ENSSAT and Research Master EUR Cyberschool
- Guillaume Doyen is the chair of Scientific, Technological and International Initiative on Cyber Security of IMT Atlantique
- Ahmed Bouabdallah and Guillaume Doyen are co-Head of the FISE TAF Cyber
- Yann Busnel has been Head of department « Network Systems, Cybersecurity and Digital law » at IMT Atlantique until june 2023 ;
- Yann Busnel has been Head of department « D2 – Network, Telecommunication and Services » at UMR IRISA until june 2023 ;
- Yann Busnel is Vice-President for Research and Innovation at IMT Nord Europe since June 2023, and belongs to the Executive Committee.
- Romaric Ludinard is co-Head of the post-master professional certificate in 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

7.3 Popularization

- Romaric Ludinard introduced *Les blockchains publiques comme support aux identités auto-souveraines : verrous et enjeux* at Forum International de la Cybersécurité, FIC
- Pierre Alain is a core team member of MirageOS
- Renzo E. Navas, produced two short interviews *Être ingénieure de recherche* focus on women research engineers, to appear in *FUN-MOOC : Ose les métiers de l'Industrie du Futur*

- Marc-Oliver Pahl ran several editions of the TALK.CYBER speaker series on cybersecurity:
  - TALK33 - 13.12.2023 *Revisiting Wireless Security* – Muriel Medard (MIT)
  - TALK32 - 24.11.2023 *Generative AI: Ethical Quandaries and the Spread of Misinformation* – Alexander Loth (Microsoft, DE)
  - TALK31 - 12.05.2023 *Enabling Machine-to-Machine Crypto Economy* - Kemal Akkaya (FIU, USA)
  - TALK30 - 26.04.2023 *Trusted Graph for explainable detection of cyberattacks* - Pierre Parrend, University of Strasbourg
  - TALK29 - 22.03.2023 *Un portefeuille européen d'identité numérique pour tous les citoyens et résidents de l'UE : apports, risques et garanties* - Claire Levallois-Barth, Chaire VP-IP Valeurs et Politiques des Informations Personnelles
  - TALK28 - 22.02.2023 *Virtual Reality-based Risk Analysis* - Frédérick Benaben, IMT Mines Albi, Georgia Institute of Technology
  - TALK27 - 25.01.2023 *Defants : Un système d'investigation sémantique* - François Khourbiga, David Fontaine
  - TALK26 - 11.01.2023 *Securing the Cloud: Encryption and Data Protection* - Guillaume Neau (Cybersecurity specialist at Amazon Web Services, France)

8 Bibliography

Articles in referred journals and book chapters

[1] N. Delcombel, T. Duval, M. Pahl, "Cybercopters Swarm: Immersive analytics for alerts classification based on periodic data", Frontiers Virtual Real. 4, 2023, https://doi.org/10.3389/frvir.2023.1156656.

[2] E. Kirdan, F. Rezabek, N. Mühlbauer, G. Carle, M. Pahl, "Real-Time Performance of OPC UA", CoRR abs/2310.17052, 2023, https://doi.org/10.48550/arXiv.2310.17052.

[3] R. M. J. I. Larsen, M. Pahl, G. Coatrieux, "Multipath neural networks for anomaly detection in cyber-physical systems", Ann. des Télécommunications 78, 3-4, 2023, p. 149–167, https://doi.org/10.1007/s12243-022-00922-x.

[4] L. Lavaur, M.-O. Pahl, Y. Busnel, F. Autrel, "The Evolution of Federated Learning-based Intrusion Detection and Mitigation: a Survey", IEEE Transactions on Network and Service Management 19, 3, September 2022, p. 2309–2332, https://imt-atlantique.hal.science/hal-03831513.

[5] M. Letourneau, G. Doyen, R. Cogranne, B. Mathieu, "A Comprehensive Characterization of Threats Targeting Low-Latency Services: The Case of L4S", Journal of Network and Systems Management 31, 1, 2023, p. 19.

[6] H. Magnouche, G. Doyen, C. Prodhon, "A Fair Sharing Approach for Micro-Services Function Chains Placement in Ultra-Low Latency Services", IEEE Trans. Netw. Serv. Manag. 21, 1, 2024, p. 20–34, https://doi.org/10.1109/TNSM.2023.3313647.

Publications in Conferences and Workshops

[7] Y. Busnel, L. Lavaur, "Tutorial: Federated Learning x Security in Network Managements", in : 14th IEEE International Conference on Network of the Future, IEEE ComSoc, IEEE, Izmir, Turkey, October 2023, `https://hal.science/hal-04217922`.

[8] Y. Busnel, H. Rivano, "FTM-Broadcast: Efficient Network-wide Ranging", in : IPIN 2023: 13th International Conference on Indoor Positioning and Indoor Navigation, 13th International Conference on Indoor Positioning and Indoor Navigation (IPIN 2023), IEEE, p. 1–6, Nuremberg, Germany, September 2023, `https://hal.science/hal-04184961`.

[9] I. Dias da Silva, Y. Busnel, C. Caillouet, "Optimisation de plan de vol de drones autonomes pour une recharge rapide de capteurs", in : AlgoTel 2023 - 25èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications, Cargese, France, May 2023, `https://hal.science/hal-04087105`.

[10] E. Kirdan, P. Horvath, M. Pahl, "Work-in-Progress: Slow Denial of Service Attack on MQTT-Based IoT", in : IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2023, Istanbul, Turkey, July 4-7, 2023, IEEE, p. 426–431, 2023, `https://doi.org/10.1109/BlackSeaCom58138.2023.10299779`.

[11] M. P. J. Kuranage, E. Hanser, L. Nuaymi, A. Bouabdallah, P. Bertin, A. Al-Dulaimi, "AI-assisted proactive scaling solution for CNFs deployed in Kubernetes", in : IEEE International Conference on Cloud Networking, CloudNet 2023, New York, USA, November 1-3, 2023, IEEE, 2023.

[12] M. P. J. Kuranage, L. Nuaymi, A. Bouabdallah, T. Ferrandiz, P. Bertin, "Deep learning based resource forecasting for 5G core network scaling in Kubernetes environment", in : 8th IEEE International Conference on Network Softwarization, NetSoft 2022, Milan, Italy, June 27 - July 1, 2022, IEEE, p. 139–144.

[13] A. Lemogue, I. Martinez, L. Toutain, A. Bouabdallah, "Federated IoT Roaming using Private DNS Resolutions", in : 2022 IEEE/IFIP Network Operations and Management Symposium, NOMS 2022, Budapest, Hungary, April 25-29, 2022, IEEE, p. 1–6, 2022.

[14] A. Lemogue, I. Martinez, L. Toutain, A. Bouabdallah, "Towards Flexible and Compact encoded DNS Messages using CBOR Structures", in : 2023 IEEE International Performance, Computing, and Communications Conference, IPCCC 2023, Anaheim, CA, USA, November 17-19, 2023, IEEE, p. 1–6, 2023.

[15] B. Loison, "Mining in Logarithmic Space with Variable Difficulty", in : 5th Conference on Blockchain Research & Applications for Innovative Networks and Services, BRAINS, 2023, `https://doi.org/10.1109/BRAINS59668.2023.10317023`.

[16] C. Lübben, M. Pahl, "Distributed Device-Specific Anomaly Detection for Resource-Constrained Devices", in : NOMS 2023, IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA, May 8-12, 2023, IEEE, p. 1–3, 2023, `https://doi.org/10.1109/NOMS56928.2023.10154372`.

[17] C. Lübben, M. Pahl, "Distributed Device-Specific Anomaly Detection using Deep Feed-Forward Neural Networks", in : NOMS 2023, IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA, May 8-12, 2023, IEEE, p. 1–9, 2023, `https://doi.org/10.1109/NOMS56928.2023.10154360`.

[18] H. Magnouche, G. Doyen, C. Prodhon, "A Lightweight Heuristic for Micro-Services Placement and Chaining in Low Latency Services", in : 2023 19th International Conference on Network and Service Management (CNSM), p. 1–9, 2023.

[19] A. H. Meraneh, F. Autrel, H. L. Bouder, M. Pahl, "SADIS: Real-Time Sound-Based Anomaly Detection for Industrial Systems", in : Foundations and Practice of Security - 16th International Symposium, FPS 2023, Bordeaux, France, December 11-13, 2023, Revised Selected Papers, Part II, M. Mosbah, F. Sèdes, N. Tawbi, T. Ahmed, N. Boulahia-Cuppens, J. García-Alfaro (editors), Lecture Notes in Computer Science, 14552, Springer, p. 82–92, 2023, https://doi.org/10.1007/978-3-031-57540-2_7.

[20] R. E. Navas, G. Dandachi, Y. Hadjadj-Aoul, P. Maillé, "Energy-Aware Spreading Factor Selection in LoRaWAN Using Delayed-Feedback Bandits", in : 2023 IFIP Networking Conference (IFIP Networking), p. 1–9, 2023.

[21] D. D. A. Nguyen, F. Autrel, A. Bouabdallah, G. Doyen, "A Robust Approach for the Detection and Prevention of Conflicts in I2NSF Security Policies", in : NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, p. 1–7, 2023.

[22] H. N. Nguyen, B. Mathieu, M. Letourneau, G. Doyen, S. Tuffin, E. M. d. Oca, "A Comprehensive P4-based Monitoring Framework for L4S leveraging In-band Network Telemetry", in : NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, p. 1–6, 2023.

[23] D. Pop, E. Kirdan, M. Pahl, "Performance Comparison of UDP and TCP for Different CoAP Load Profiles", in : NOMS 2023, IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA, May 8-12, 2023, IEEE, p. 1–6, 2023, https://doi.org/10.1109/NOMS56928.2023.10154441.

[24] T. Sylla, L. Mendiboure, M. A. Chalouf, F. Krief, H. Aniss, L. Alouache, "Applying Fuzzy Logic to Efficiently Manage Shared Edge Infrastructure", in : 31th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE-2023) Paris, December 14-16, 2023, 2023.

Miscellaneous

[25] L. Miller, M.-O. Pahl, "Collaborative Cybersecurity Using Blockchain: A Survey", 2024.

Miscellaneous

[26] R. E. Navas, "Energy-Aware Spreading Factor Selection in LoRaWAN Using Delayed-Feedback Bandits: Code and Data.", Zenodo, April 2023, https://doi.org/10.5281/zenodo.7876244.