RESEARCH CENTRE

Inria Centre at Université de Lorraine

IN PARTNERSHIP WITH:

Université de Lorraine, CNRS

2024

ACTIVITY REPORT

Project-Team

RESIST

Resilience and elasticity for security and scalability of dynamic networked systems

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

DOMAIN

Networks, Systems and Services, Distributed Computing

THEME

Networks and Telecommunications

Inria

Contents

Project-Team RESIST

Creation of the Project-Team: 2020 December 01

Keywords

Computer sciences and digital sciences

A1.1.8. – Security of architectures

A1.1.10. – Reconfigurable architectures

A1.1.13. – Virtualization

A1.2. – Networks

A1.2.1. – Dynamic reconfiguration

A1.2.2. – Supervision

A1.2.3. – Routing

A1.2.4. – QoS, performance evaluation

A1.2.5. – Internet of things

A1.2.6. – Sensor networks

A1.2.7. – Cyber-physical systems

A1.2.8. – Network security

A1.3.3. – Blockchain

A1.3.4. – Peer to peer

A1.3.5. – Cloud

A1.3.6. – Fog, Edge

A1.5.2. – Communicating systems

A2.6. – Infrastructure software

A3.2.2. – Knowledge extraction, cleaning

A3.2.3. – Inference

A3.3. – Data and knowledge analysis

A3.4.1. – Supervised learning

A3.4.2. – Unsupervised learning

A3.4.3. – Reinforcement learning

A4.1. – Threat analysis

A4.4. – Security of equipment and software

A4.9. – Security supervision

A9. – Artificial intelligence

A9.2. – Machine learning

Other research topics and application domains

B5. – Industry of the future

B6.3.2. – Network protocols

B6.3.3. – Network Management

B6.4. – Internet of things

B6.5. – Information systems

B6.6. – Embedded systems

B9.2.3. – Video games

1 Team members, visitors, external collaborators

Research Scientists

- Isabelle Chrisment [Team leader, INRIA, Professor Detachement, HDR]
- Nicolas Schnepf [INRIA, Researcher]

Faculty Members

- Laurent Andrey [UL, Associate Professor]
- Rémi Badonnel [UL, Professor, HDR]
- Thibault Cholez [UL, Associate Professor]
- Olivier Festor [UL, Professor, HDR]
- Abdelkader Lahmadi [UL, Associate Professor]

Post-Doctoral Fellow

- Xavier Marchal [UL, until Aug 2024]

PhD Students

- Omar Anser [INRIA]
- Ahmad Atwi [INRIA, from Dec 2024]
- Enzo D'Andrea [UL, ATER, from Sep 2024]
- Enzo D'Andrea [INRIA, until Aug 2024]
- Mohamed Amine El Yagouby [UL, from Nov 2024]
- Katsuki Isobe [INRIA, from Jun 2024]
- Joel Ky [ORANGE, CIFRE, until Sep 2024]
- Jhon Sebastian Rojas Rodriguez [UL, from Dec 2024]
- Runbo Su [UL, from Sep 2024]
- Franco Terranova [UL]

Technical Staff

- Rémi Garcia [INRIA, Engineer, from Nov 2024]
- Matthews Jose [INRIA, Engineer, from Mar 2024]
- Matthews Jose [TELECOM NANCY, Engineer, until Feb 2024]
- Joel Ky [INRIA, Engineer, from Dec 2024]

Interns and Apprentices

- Satou Aurélie Kpoze [INRIA, Intern, from Nov 2024]
- Raphael Michon [UL, Intern, from Jun 2024 until Aug 2024]
- Santiago Rios Guiral [UL, Intern, from May 2024 until Nov 2024]

Administrative Assistants

- Delphine Hubert [UL]
- Cecilia Olivier [INRIA]

External Collaborator

- Jérôme François [University of Luxembourg]

2 Overall objectives

2.1 Context

The increasing number of components (users, applications, services, devices) involved in today's Internet as well as their diversity make **the Internet a very dynamic environment**. Networks and cloud data centers have been becoming vital elements and an integral part of emerging **5G infrastructure**. Indeed, networks continue to play their role interconnecting devices and systems, and clouds are now the de facto technology for hosting services, and for deploying storage and compute resources, and even Network Functions (NFs).

While telecom operators have been historically providing Internet connectivity and managing the Internet infrastructure and services, they are now losing control to other stakeholders, particularly to Over-the-Top (OTT) content and service providers. Therefore, the delivery of Internet services has increased in complexity to mainly cope with the diversity and exponential growth of network traffic both at the core and at the edge. Intermediate players are multiplying and each of them has been proposing solutions to enhance service access performance.

In the Internet landscape, no single entity can claim a complete view of Internet topology and resources. Similarly, a single authority cannot control all interconnection networks and cloud data centers to effectively manage them and **provide reliable and secure services** to end users and devices at scale. The **lack of clear visibility into Internet operations** is exacerbated by the increasing use of encryption solutions which contributes to traffic opacity.

2.2 Challenges

In this context two main challenges stand out:

- **Scalability**: As mentioned above, the Internet ecosystem is continuously expanding in both size and heterogeneity. Scalability was already a challenge in the last decade but solutions mainly focused on scaling one dimension at a time, e.g. increasing the capacity of network links or that of compute resources in order to face peak demand, even if it is infrequent. Such **over-provisioning** however wastes significant resources and **cannot cope with future demand** at a reasonable cost. Scalability must be ensured across multiple dimensions and many orders of magnitude: more users, devices, contents and applications.
- **Security:** Security has gained a lot of importance in the last few years because the Internet has become a lucrative playground for attackers with large numbers of potential victims and numerous ways to reach them. Advanced Persistent Threats (APT) are the most sophisticated representatives of this evolution. Such **targeted attacks do not rely on generic scenarios**, usually described as a set of signatures. They are **complex by nature** and their investigation requires the **analysis of various sources of data**. At the same time, the generalization of encryption renders all deep packet inspection techniques obsolete and threat hunting becomes an even bigger challenge.

  Additionally, an underground economy has been developed by cyber-criminals. Finally, because many applications are now provided as cloud-based services, physical isolation is also harder with potential attackers able to act directly in the field.

The highly dynamic nature of the Internet ecosystem, the requirement for higher and higher scalability, and the rising security threats have shown the **limitations of traditional approaches to address these challenges**. Resist focuses on two complementary paradigms for achieving security and scalability:

- **Elasticity** refers to the ability of a system to **scale up and down on demand**. Elasticity of compute resources became more accessible with the advent of cloud computing. It has been recently leveraged in support of Network Function Virtualization (NFV) coupled with Software-Defined Networking (SDN). Understanding the dynamics of networked systems is critical in order to benefit from and efficiently orchestrate elasticity at all levels of the network, the system and the applications. On the one hand, elasticity facilitates scalability, as well as security by instantiating virtualized network security functions (e.g., firewall, IDS, DPI, etc.) on demand. On the other hand, it could increase the attack surface. This dilemma must be addressed. Moreover, issues inherent to elasticity such as the dynamic deployment and migration of resources bring new challenges in NFV environments since network functions are different from those of common cloud applications deployed in virtual machines and containers, *e.g.* in terms of network throughput.
- **Resilience** refers to the ability of a system to **adapt itself when facing challenging situations**. It is reasonable to assume that any system may face an attack for which protection mechanisms may fail. A comprehensive approach to resilience that considers not only the network and system resources but also the supported users and applications brings both benefits and challenges since users and applications can be very diverse, ephemeral and mobile. Applications are also deployed in dynamic environments like cloud platforms and are frequently reconfigured.

Resist aspires to make **large-scale** networked systems **more secure and more resilient**, leveraging resource **elasticity** and assuming a highly dynamic environment.

3 Research program

3.1 Overview

The project aims at designing, implementing and validating novel models, algorithms and tools to **make networked systems elastic and resilient so as to enhance their scalability and security**, assuming users, applications and devices whose volume and heterogeneity will continue to increase.

Softwarization of networks and data analytics are key enablers for designing intelligent methods to orchestrate – i.e. configure in a synchronized and distributed manner – both network and system resources. Intelligent orchestration leverages indeed data analytics for decision-making. Input data reflecting the past and current states of the system can be used to extract relevant knowledge including future states. To generate knowledge and validate orchestration decisions, a running system has to be monitored. Monitoring will also be steered and dynamically reconfigured through orchestration. Accordingly, the RESIST project is structured into three main complementary research axes detailed hereafter, namely **Monitoring**, **Analytics** and **Orchestration**.

3.2 Monitoring

The evolving nature of the Internet ecosystem and its continuous growth in size and heterogeneity call for a better understanding of its characteristics, limitations, and dynamics, both locally and globally so as to improve application and protocol design, detect and correct anomalous behaviors, and guarantee performance.

To face these scalability issues, **appropriate monitoring models, methods and algorithms are required for data collection, analysis and sharing** from which knowledge about Internet traffic and usage can be extracted. Measuring and collecting traces necessitate user-centered and data-driven paradigms to cover the wide scope of heterogeneous user activities and perceptions. In this perspective, we propose monitoring algorithms and architectures for large scale environments involving mobile and Internet of Things (IoT) devices.

Resist also assesses **the impact of the Internet infrastructure evolution integrating network softwarization on monitoring**, for example the need for dedicated measurement methodologies. We take into account not only the technological specifics of such paradigms for their monitoring but also the ability to use them for collecting, storing and processing monitoring data in an accurate and cost-effective manner.

Crowd-sourcing and third-party involvement are gaining in popularity, paving the way for massively distributed and collaborative monitoring. We thus investigate opportunistic mobile crowdsensing in

order to collect user activity logs along with contextual information (social, demographic, professional) to effectively measure end-users' **Quality of Experience**. However, collaborative monitoring raises serious concerns regarding trust and sensitive data sharing (open data). Data anonymization and sanitization need to be carefully addressed.

Finally, methodological aspects are also important for ensuring **trustworthy and reproducible experiments**, and raise many challenges regarding testbed design, experiment description and orchestration, along with automated or assisted provenance data collection.

3.3 Analytics

A large volume of data is processed as part of the operations and management of networked systems. These include traditional monitoring data generated by network components and components' configuration data, but also data generated by dedicated network and system probes.

Understanding and predicting security incidents or system ability to scale requires the elaboration of novel **data analytics techniques** capable to cope with large volumes of data generated from various sources, in various formats, possibly incomplete, non-fully described or even encrypted.

We use machine learning techniques (*e.g.* Topological Data Analysis or multilayer perceptrons) and leverage our domain knowledge to fine-tune them. For instance, machine learning on network data requires the definition of new distance metrics capable to capture the properties of network configurations, packets and flows similarly to edge detection in image processing. Resist contributes to developing and making publicly available an **analytics framework dedicated to networked systems** to support Intelligence-Defined Networked Systems.

Specifically, the goal of the Resist analytics framework is to facilitate the extraction of knowledge useful for **detecting, classifying or predicting security or scalability issues**. The extracted knowledge is then leveraged for orchestration purposes to achieve system elasticity and guarantee its resilience. Indeed, predicting when, where and how issues will occur is very helpful in deciding the provisioning of resources at the right time and place. Resource provisioning can be done either reactively to solve the issues or proactively to prepare the networked system for absorbing the incident (resiliency) in a timely manner thanks to its elasticity.

While the current trend is towards centralization where the collected data is exported to the cloud for processing, we seek to extend this model by also developing and evaluating novel approaches in which **data analytics is seamlessly embedded within the monitored systems**. This combination of big data analytics with network softwarization enablers (SDN, NFV) can enhance the scalability of the monitoring and analytics infrastructure.

3.4 Orchestration

The ongoing transformations in the Internet ecosystem including network softwarization and cloudification bring new management challenges in terms of service and resource orchestration. Indeed, the growing sophistication of Internet applications and the complexity of services deployed to support them require novel models, architectures and algorithms for their automated **configuration** and **provisioning**. Network applications are more and more instantiated through the **composition of services, including virtualized hardware and software resources**, that are offered by **multiple providers** and are subject to changes and updates over time. In this dynamic context, efficient orchestration becomes fundamental for ensuring performance, resilience and security of such applications. We are investigating the chaining of different functions for supporting the security protection of smart devices, based on the networking behavior of their applications.

From a resilience viewpoint, this orchestration at the network level allows the dynamic **reconfiguration of resources** to absorb the effects of congestions, such as link-flooding behaviors. The goal is to drastically reduce the effects of these congestions by imposing dynamic policies on all traffic where the network will adapt itself until it reaches a stable state. We also explore mechanisms for **detecting and remediating potential dysfunctions** within a virtualized network. Corrective operations can be performed through dynamically composed VNFs (Virtualized Network Functions) based on available resources, their dependencies (horizontal and vertical), and target service constraints. We also conduct research on verification methods for automatically assessing and validating the composed chains.

From a security viewpoint, this orchestration provides **prevention mechanisms** that capture adversaries' intentions early and **enforces security policies** in advance through the available resources, to be able to proactively mitigate their attacks. We mainly rely on the results obtained in our research activity on security analytics to build such policies, and the orchestration part focuses on the required algorithms and methods for their automation.

4 Application domains

4.1 Internet

Among the different network types, the Internet is the one to link them all and is consequently our most prominent subject, not to mention its prime importance in today's society. The Internet also exhibits its own challenges due to the scale and diversity of stakeholders, applications and network technologies in use.

From a security perspective, **monitoring and analysing Internet traffic is an important part of threat prevention and predictive security**. Indeed, large network telescopes like the one we use in the High Security Laboratory allow detecting world-wide campaigns of attacks which target a specific exploit in some applications. Moreover the monitoring of the Internet traffic at the **edge** is the best way to quickly detect distributed attacks like DDoS (Distributed Denial of Service) and to mitigate them before they become effective. However, the Internet traffic analysis is made much more complicated since the **massive shift towards encryption** that happened few years ago, which requires new traffic classification methods.

The performance and resilience of services running over the Internet is also a major topic of Resist. In particular, it is very difficult to **diagnose the cause of a degradation of performance among the different actors and technologies** that are used to deliver a service over the Internet (access medium, ISP, CDN, web-browser, etc.). Networked systems deployed at Internet scale are also a natural research subject for Resist. Indeed **decentralized systems** like P2P (Peer-to-Peer) networks or blockchains are known to be robust and scalable. However, their security and performance have to be carefully assessed because a single flaw in their design can endanger the whole system.

4.2 SDN and Data-Center Networks

As the SDN paradigm and its implementations bring new opportunities that can be leveraged in different contexts, in particular for security and performance, programmable networks are also part of the research scope of Resist. This includes data-plane **programming models and hardware offloading** that enable very flexible programming at the network level. While OpenFlow was initially designed for academic research, SDN in general has then been adopted by industrial players, above all in **data-center networks**. It supports innovations to better share load and optimize resources among processes, in particular for virtualization platforms. Contributing to the development of these technologies is primordial for us as they are key elements for monitoring and enhancing the performance and security of future data-center networks.

When defining or extending SDN technologies, the strongest constraint is to guarantee a satisfactory level of performance, *i.e.* enabling high flexibility in programming with a **reduced footprint of network throughput**. However, as it may also break isolation principles between multiple tenants, security has to carefully considered, either by adding safeguard mechanisms at run-time or through a priori verification and testing.

4.3 Fog and Cloud computing

Cloud computing has largely evolved in the last years including new networking capabilities as highlighted in the previous section towards the model of XaaS or **everything-as-a-service**. Moreover, cloud computing continues to be more distributed and aims at integrating more heterogeneous resources. One particular example is **fog computing** that consists of a massively distributed number of different resources, including low-performance ones. Large network operators have a great interest in fog computing because they already operate such an infrastructure (*e.g.* a national operator with regional clouds and setup boxes

in end users' homes). Softwarization or virtualization of all functions and services will help them to be competitive by reducing their costs. In general, intelligent orchestration of massively distributed resources will be investigated in various application domains, including **federated cloud infrastructures, fog computing, 5G networks, IoT and big data infrastructures**.

The manageability of such largely distributed systems is a core topic with questions related to monitoring, security and orchestration of resources. Major changes and errors can have dramatic effects on a real system, that actually lead to only minor changes being carried out and slow down innovation and adoption of new propositions. Hence, **controlled and reproducible experiments are vital**.

As shown by our past work, we are able to quickly adjust to experimental needs in most areas of distributed computing and networking, such as *High Performance Computing (HPC)*, *Big Data*, *Peer-to-peer systems*, *Grid computing*, etc. However, in the context of Resist, **we will focus mainly on** *Software-Defined Infrastructures*, gathering *cloud computing* for compute and storage resources, *software-defined networking* and *network function virtualization* for networking. Those infrastructures share many common features: need for performance, for scalability, for resilience, all implemented using flexible software components.

Worth mentioning here is our involvement in the international testbed community (FIRE, GENI). We plan to strengthen our existing links with the Chameleon and CloudLab US projects, to leverage the recently accepted Fed4FIRE+ project on a testbed federation, and, at the national level, to contribute to the SILECS initiative for a new large-scale experimental computer science infrastructure.

4.4 Cyber-Physical Systems

Cyber-Physical Systems (CPSs) used to be well isolated and so designed accordingly. In the last decade, they have become **integrated within larger systems** and so accessible through the Internet. This is the case with **industrial systems**, like SCADA, that have been unfortunately exposed to major threats. Furthermore, the **Internet-of-Things (IoT)** has become a reality with numerous protocols, platforms and devices being developed and used to support the growing deployment of smart* services: smart home, transport, health, city... and even rather usual rigid systems such as industry 4.0.

From an academic perspective, the IoT can be seen as an evolution of sensor networks. It thus inherits from the same problems regarding security and scalability, but with a higher order of magnitude both in terms of number of devices and their capabilities, which can be exploited by attackers. Research in this area has focused on developing dedicated protocols or operating systems to guarantee security and performance, Resist aims to tackle identical problems but **assuming a more practical deployment of IoT systems composed of heterogeneous and uncontrolled devices**. Indeed, this ecosystem is very rich and **cannot be controlled by a unique entity**, *e.g.* services are often developed by third parties, manufacturers of embedded devices are different from those providing connectivity.

As a result, managing an IoT system (monitoring, changing configuration, etc.) is very hard to achieve as most of the devices or applications cannot be directly controlled. For instance, many IoT providers rely on their own cloud services, with their own unknown **proprietary protocols** and most of the time through **encrypted channels**. Above all, the use of middle-boxes like gateways hides the IoT end-devices and applications. We will thus need to infer knowledge from **indirect and partial observations**. Likewise, control will be also indirect for example through filtering or altering communications.

5 Social and environmental responsibility

5.1 Footprint of research activities

Nicolas Schnepf took the responsibility of the group working on numeric sobriety in the *Commission pour l'Action et la Responsabilité Ecologique (CARE)*, a joint committee between Loria and Inria Center at Université de Lorraine. In this context, he animated a café about the energetic cost of streaming download in our research activity, especially with visioconferences. He also presented this group to the project committee of the Inria Center at Université de Lorraine, in order to identify how the numeric sobriety could be explored as a research topic.

6 Highlights of the year

Abdelkader Lahmadi has published the book "Ransomware Analysis: Knowledge Extraction and Classification for Advanced Cyber Threat Intelligence" with Claudia Lanza (University of Calabria, Italy) and Jérôme François (University of Luxembourg) in CRC Press. This book is a major result of our collaboration with Claudia Lanza who is working on Language Science, Terminology and Textual Typologies applied to Cybersecurity.

6.1 Awards

Two students, Lenny LORAND (TELECOM Nancy, FISEA, Cybersecurity) and Xavier MONARD (TELECOM Nancy, FISE, Cybersecurity), under the supervision of Rémi Badonnel, have been awarded in the top 3 of a European Cybersecurity Challenge, organized in November 2024 in the context of the REWIRE Cybersecurity Skills Alliance.

7 New software, platforms, open data

7.1 New software

7.1.1 eCGP

Name: experimental Cloud Gaming Platform

Keyword: Cloud gaming

Functional Description: eCGP features a client, a server and a proxy using the SCReAM congestion control algorithm. It is developed for Linux OS.

URL: https://github.com/mosaico-anr/eCGP

Contact: Thibault Cholez

7.2 New platforms

Electrical Microgrid Security Assessment Platform

Participants: Abdelkader Lahmadi *(contact)*, Aurélie Kpoze.

During 2024, we extended our electrical microgrid platform and its control part with SDN-based communication network [12]. The platform comprises Distributed Generators (DGs), Open vSwitches (OVSs) installed on Raspberry Pi devices, and a POX controller. The platform allows us to validate and evaluate methods of mitigating Man-in-the-Middle (MitM) attacks by demonstrating the effectiveness of SDN in limiting their impact on the microgrid.

KP-ABE Content Filtering

Participants: Thibault Cholez *(contact)*, Xavier Marchal.

In the context of the ANR PRESTO project, we developped several programs to build a platform demonstrating that our new cryptographic scheme based on KP-ABE can replace intrusive security solutions enforcing content access policies, like firewalls leveraging an HTTPS-proxy, while keeping all content private and with acceptable levels of performance (overhead). Our KP-ABE content filtering platform is made of the following programs:

- Proxy: As current web browsers do not understand KP-ABE encryption, the proxy is here to add the needed missing logic. It is expected to be removed from the chain in case of standardization and massive adoption.

- Authority: This component manages the keys for each client, generates decryption keys based on policies (whitelist, blacklist and rules based on attributes).

- Verifier: This component performs deep packet inspection to get the clienthello of the TLS sessions in order to check if the two added TLS extensions (KP-ABE public key and an encrypted scalar for anonymity) are present and verify if there are derived from the Authority public key. If the clienthello is not compliant, the verifier drops the packets related to the client TLS session.

- Server: This is a basic web server that implements the logic needed to encrypt content with KP-ABE. It maps contents with attributes for encryption. KP-ABE encryption is enable only if the client provides a KP-ABE public key in its clienthello else it works as a normal web server.

GIT Hub repository

8 New results

8.1 Monitoring

8.1.1 Security of IPFS DHT

Participants: Thibault Cholez *(contact)*, Victor De Moura Netto *(COAST team)*, Claudia Ignat *(COAST team)*.

The Distributed Hash Table (DHT) architecture is known to be a very efficient way to implement peer-to-peer (P2P) computer networks. However, the scientific literature also proved that DHT functioning in P2P networks can be easily disrupted by a single entity controlling many peers, known as the Sybil Attack. Various defensive mechanisms are known to prevent such attacks, or at least hinder them.

In 2024, we conducted a study in the context of the PEPR Cloud - TRUSTINClouds project, to evaluate the resiliency of the InterPlanetary File System (IPFS) P2P network to a legacy Sybil Attack. We showed that, surprisingly, IPFS does not implement basic defense mechanisms, allowing the most simple attack from a single computer to easily take the control of any DHT entry. A practical use of this attack is to almost entirely deny access to a given content on the network. Thus, we have provided some recommendations to quickly remediate this vulnerability [7]. This work was done in collaboration with the Inria COAST team.

8.1.2 Monitoring of Handshake Blockchain

Participants: Thibault Cholez *(contact)*, Katsuki Isobe.

A popular application of blockchains is to provide an alternative to the current domain name system (DNS) where a distributed ledger can replace the Internet Assigned Numbers and subsequent authorities. We investigated the Handshake blockchain data to evaluate its reliability.

In particular, we showed that there is an increased possibility of domain name abuse at a lower cost in general. Furthermore, by discussing system redundancy as part of the blockchain-based DNS, we demonstrated that there is a critically low redundancy of authoritative DNS servers, putting the service at risk [11]. This work was done in collaboration with Osaka Metropolitan University, Japan.

8.1.3 Understanding Cloud Gaming Network Traffic and Optimizing its Transport

Participants: Thibault Cholez *(contact)*, Olivier Festor, Xavier Marchal.

In the context of the ANR MOSAICO project, we worked on the transport of low-latency traffic in networks, and in particular on Cloud Gaming (CG) services. CG plaforms have gained much popularity recently and are expected to become a significant part of Internet traffic in the upcoming years. However, the characteristics of their traffic, requiring at the same time high bandwidth and low latency, are challenging for networks and make it difficult to maintain a good quality of service (QoS) in degraded network conditions, when congestion occurs.

In 2024, we published in IFIP Network Traffic Measurement and Analysis Conference (TMA 2024) our last study optimizing CG traffic transport [10]. Our objective was to evaluate the transport of CG traffic in a double queue architecture in order to avoid oversized buffers which generate latency when competing with flows driven by loss-based CCAs (Congestion Control Algorithms). We considered a HTB (Hierarchical Token Bucket) queuing discipline or the AQM DualPI2 with a "Low Latency, Low Loss, and Scalable Throughput" (L4S) queues. As current CG platforms are not compatible with these queuing disciplines, we developed our own experimental platform coupled with SCReAM, a CCA based on loss and delays for the RTP protocol (Real-time Transport Protocol) and supporting explicit congestion notification (ECN). We then monitored the traffic on the bottleneck against different competing flows (TCP Cubic and BBRv2). Our results showed that, when a simple droptail queue is considered, fairness issues create a bandwidth starvation of CG traffic and a high queuing delay while both dual queue approaches perfectly preserve the QoS of CG traffic. This work was done in collaboration with Orange Innovation.

8.2 Analytics

8.2.1 Efficient Distribution of Security Filtering Rules in SDN

Participants: Abdelkader Lahmadi *(contact)*, Wafik Zahwa *(PESTO team)*, Michael Rusinowitch *(PESTO team)*.

Software Defined Networks (SDN) heavily rely on diverse management rules (ACL, traffic control, etc.) to satisfy security and business requirements of their associated services. As these networks are increasing in size and complexity, their management rules configured in devices are becoming more complex. These rules are constantly growing in size and it is challenging to distribute them across network devices with limited capacities. Typically implemented in switches using Ternary Content-Addressable Memory (TCAM), ACLs placement faces challenges due to the limited capacity of TCAM memory.

To address this, large ACLs must be divided and distributed across multiple switches, ensuring that each packet traveling from source to destination undergoes the necessary match-action rules. In [19], we developed a novel approach that combines graph-embedding neural networks (GNN) with deep Q-learning (DQN) to automate the distribution of ACLs across network switches while minimizing TCAM memory usage. By allowing additional constraints and evaluating our trained models on both synthetic and real-world network topologies, we have shown that our approach has a placement success score of up to 99% on unseen graphs. This work was done in collaboration with the Inria PESTO team and the NUMERYX Company.

8.2.2 Characterization and Troubleshooting of Cloud Gaming Applications on Mobile Networks

Participants: Abdelkader Lahmadi *(contact)*, Joël Ky.

Detecting abnormal network events is an important activity of Internet Service Providers particularly when running critical applications (*e.g.*, ultra low-latency applications in mobile wireless networks).

Abnormal events can stress the infrastructure and lead to severe degradation of user experience. Machine Learning (ML) models have demonstrated their relevance in many tasks including Anomaly Detection (AD). However, applying ML-based AD methods is challenging for operators due to the proliferation of ML models and the lack of well-established methodology and metrics to evaluate them and select the most appropriate one.

Traditional AD approaches, predominantly based on reconstruction techniques, often yield suboptimal performance, particularly when anomalies are present in the training set. Conversely, contrastive learning (CL) has shown significant performance in image processing tasks and is increasingly applied in time series data classification and forecasting. However, traditional CL frameworks are not well-adapted for time series AD due to two key challenges. First, AD is typically performed only on normal instances, and thus CL does not benefit from knowledge about anomalous instances. Second, the temporal nature of time series data is often neglected when computing time series similarity. To overcome these limitations, in [14], we proposed CATS, a novel approach that leverages a temporal similarity measure to learn time series representations. Moreover, through negative data augmentation, CATS generates a more realistic distribution of anomalies, which enables anomaly-informed CL. This work was done in collaboration with University of Waterloo and Orange Innovation

8.2.3 Mitigating Synchronization Attacks on Distributed and Cooperative Microgrid Control Systems

Participants: Abdelkader Lahmadi *(contact)*, Satou Aurélie Kpoze, Isabelle Chrisment.

Industrial Control Systems (ICSs) are widely used in various industries, enabling the control and monitoring of critical infrastructures such as microgrids. In these infrastructures, distributed and cooperative control systems are commonly employed to synchronize set points through information exchange over communication networks. However, these systems are increasingly vulnerable to various security threats, particularly those targeting synchronization data.

In [12, 13], we developed a network reconfiguration mechanism leveraging Software-Defined Networking (SDN) to mitigate synchronization attacks based on Man-in-the-Middle (MitM) and targeting distributed and cooperative microgrid control systems. We implemented and evaluated our proposed mitigation algorithm using MiniCPS and a hardware platform to show its efficacy in avoiding synchronization attacks within such distributed energy systems. This work was done in collaboration with University of Abomey-Calavi, Benin.

In [9], we focused on the detection of these MitM attacks at P4-based Programmable Data Planes (PDP) by performing in-band processing of the Address Resolution Protocol (ARP) packets. To this end, we designed and developed an effective detection system for MitM based on real-time statistical data by measuring, in the data plane, the ARP messages for each connected host to the programmable switch that raise alarms according to configurable burst sizes. The results of experiments showed that at high rates our detection system achieves mean detection times of 1.7 seconds for Network Discovery (ND) attack and 3.13 seconds for Spoofing-Poisoning (SP) attack. Also, at high rates, we obtained reduced false positive alarms, 0.69% and 2.59% for ND and SP attacks, respectively. The results are consistent compared with a SDN existing approach. This work was done in collaboration with University of Antioquia, Colombia.

8.2.4 Cyber-Attack Paths Prediction

Participants: Abdelkader Lahmadi *(contact)*, Franco Terranova, Isabelle Chrisment.

Attack paths represent the sequences of network nodes compromised by attackers while exploiting their respective vulnerabilities. Current methods for predicting such attack paths largely depend on existing human expertise or established heuristics. These traditional methods are time-consuming and require highly skilled threat-hunting analysts to identify these attack paths and proactively apply

security measures. However, the task becomes challenging when facing large-scale and highly vulnerable networks.

In [18, 24], we proposed an alternative approach leveraging Deep Reinforcement Learning (DRL) techniques aiming to approximate the decision-making of attackers. Our approach embodies the attacker's perspective and tactics to exploit discovered paths for proactive security analysis and establish defense strategies. We introduced a novel re-formulation of the problem with a local view for the DRL agent, representing the source and target node of the attack at each timestep. Additionally, our training methodology involves a diverse set of network topologies of different sizes and exploitable vulnerabilities, demonstrating the ability of DRL algorithms to navigate topologies, and to identify attack paths and compromise nodes. Our results showed the capability of the learned policies to generalize within entirely new topologies, arriving to discover 80% ± 0.08% of the attack paths in 1500 steps.

8.2.5 Analysis of Ransomware Vulnerabilities

Participants: Abdelkader Lahmadi *(contact)*, Jérôme François.

Cyber threat awareness requires the building of an accurate knowledge and analysis of the vulnerabilities used by the attackers and their respective attack toolkits. Ransomware are today one of the most significant threats faced by information systems and their number continues to grow. They are a type of malware targeting the information system by locking its equipment and users data and claiming a ransom for its release. They have been becoming more and more sophisticated and mainly relying on software vulnerabilities to access and lock the system data.

In [15], we have carried out an empirical analysis of the Common Vulnerabilities Enumeration (CVE) exploited by known ransomware using a semantic annotation technique in order to create the condition from which to start to build a knowledge base of ransomware behaving processes. The main focus of this work is towards the way vulnerabilities are commonly exploited by ransomware, their sharing ratio and the definition of their common causes and impacts. We have applied a semantic annotation methodology which encompasses a semantic analysis of the CVE dataset through a pattern recognition process. This latter has enabled the extraction for each CVE of its key features, i.e., the cause, the performed exploit action and effect, as well as its impact. In the resulting collected and extracted knowledge we show a twofold analysis, statistical and semantic, of the CVE descriptions and their extracted features. In the book [20], we have extended this methodology and its application to a large dataset of ransomware CVE descriptions by integrating their mapping with ATT&CK framework to significantly refine the granularity of their threat intelligence knowledge extraction. These contributions were done in collaboration with University of Calabria, Italy.

8.2.6 Automated Configuration of ML-based Intrusion Detection System

Participants: Jérôme François *(contact)*, Omar Anser, Isabelle Chrisment.

ML-based Network Intrusion Detection Systems (NIDS) have benefited of advances in ML to improve their accuracy when tracking attacks in network traffic. Nevertheless, ML solutions face issues like overfitting or insufficient training data, which may necessitate retraining or adjustments to maintain long-term efficiency. From data collection to model training, all efforts are crucial for deploying a robust ML-based intrusion detector. Among these efforts, optimizing model hyperparameters, a time-consuming task, can be automated by existing methods.

Yet, such AutoML methods require a validation set, making them unsuitable for training a detector on an attack-free dataset, as in anomaly-based intrusion detection. Additionally, setting the anomaly detectors' threshold, usually beyond hyperparameters configuration, requires knowledge of attacks. To overcome these challenges, we introduced an automated solution [6] to infer the hyperparameters and the threshold jointly from an attack free training dataset. Pre-learned optimal configurations are transferred

and fine-tuned across datasets. This is a continuation of our work of the previous year focusing on optimizing hyper-parameters only and assuming attacks to be detected. Our new technique can be thus qualified as a meta-learning-based semi-supervised configuration approach that relies solely on the training set to infer an efficient configuration.

8.3 Orchestration

8.3.1 Security Configuration for Cloud Services

Participants: Rémi Badonnel *(contact)*, Olivier Festor.

Cloud infrastructures provide new facilities to build elaborated added-value services by composing and configuring a large variety of computing resources, from virtualized hardware devices to software products. They are however further exposed to security attacks than traditional environments.

We continued our work on the design of a moving target defense strategy for cloud environments, which combines artificial intelligence with vulnerability prevention, in particular to counter reconnaissance activities performed by attackers. Our moving target defense strategy aims at bridging the gap between artificial intelligence and configuration verification techniques. It selects the movements to be applied on the cloud composite service, in order to reduce the predictability of configuration changes, while minimizing the risk of critical vulnerable configurations. We have conducted additional series of experiments to quantify the benefits and limits on realistic scenarios, considering vulnerability descriptions from the official OVAL repository.

In collaboration with University of Milan, we also extended our vulnerabity management efforts to the edge-cloud continuum. We investigated a comprehensive methodology for vulnerability-aware service deployment in that context. The proposed approach aims at finding a suitable deployment recipe for a given workflow by evaluating the vulnerability footprint of each platform, computing the set of candidate deployment platforms, and finding the optimal deployment solution [21]. The solution is also capable of migrating already deployed workflows in case the vulnerability requirement is no longer satisfied. It addresses a critical gap in current practices by providing a mechanism to quantify and mitigate the risks associated with service deployment, thereby improving the overall trustworthiness and reliability of distributed computing environments.

8.3.2 Intelligent Configuration and Update for Future Networks

Participants: Nicolas Schnepf *(contact)*, Katsuki Isobe, Rémi Badonnel.

Effective management of configuration and software updates on network and security equipments like firewalls and intrusion detection systems is a significant challenge in network operations and management, particularly when considering specific performance and security requirements like ensuring that the traffic will always traverse a certain network function. This challenge is increased by the dynamics and heterogeneity of future networks that are ever more driven by artificial intelligence methods and techniques.

In this context, we pursued our efforts on analyzing how to update a softwarized communication network in a provably correct manner, transiently accounting for software vulnerabilities (e.g., related to software compatibility) and congestion given the actual load in the network. This work was performed in collaboration with TU Berlin, Aalborg University and the Inria DIANA team. After formalizing the problem, we proposed an algorithmic solution, called Eagle, which relies on formal methods and linear programming, supporting an easy, automated and fast synthesis of correct updates [22]. We are not aware of any existing update synthesis approach in the networking literature which combines both logical (vulnerability constraints) and quantitative (congestion) properties. We have continued our experiments in the context of a 5G architecture, to evaluate the performance and scalability of the proposed strategy.

We also started, with the PhD thesis of Katsuki Isobe, to investigate the relationships amongst orchestration, verification and optimization techniques for supporting automated security configuration in the context of future networks. The review of existing works in these areas and their intersections highlighted three major issues in such networks, namely the coupling of artificial intelligence with verification techniques to prevent errors and inadequate decisions, the adequate and consistent distribution over the computing continuum, and the adaptative management of resources to maintain service continuity and efficiency. A particular interest is given to the extension of the Eagle algorithmic solution mentioned below to address the case of dynamic security chains in 5G/B5G networks.

8.3.3 Chaining Functions at Different Programmable Network Levels

Participants: Thibault Cholez *(contact)*, Joël Ky.

Today, new network functions can be implemented either as pure software (Virtualized Network Functions) or in a programmable network appliance using the Programming Protocol-independent Packet Processors (P4) solution. Each of the two programmable concepts has its own advantages and drawbacks and micro-services should be preferably developed in one or the other solution depending on their constraints and requirements. To combine both approaches, we proposed to leverage Segment Routing (SR) to define a solution allowing to chain the micro-services to be executed at both levels. This signaling protocol is integrated within network equipment but not within a NFV infrastructure. To overcome it, we designed an intermediary proxy between the P4 nodes and the VNFs. This proxy is in charge of managing the SR labels and their association with the related VNF. It opens the way towards a composition of network services taking the best of the two levels of programmable networks [16]. This work was done in collaboration with Orange Innovation.

9 Bilateral contracts and grants with industry

9.1 Bilateral grants with industry

Numeryx Technologies (Paris, France)

Participants: Abdelkader Lahmadi *(contact)*, Wafik Zahwa *(PESTO team)*, Michael Rusinowitch *(PESTO team)*.

- Wafik Zahwa, CIFRE PhD Student, is supervised by Abdelkader Lahmadi, Michael Rusinowitch (Inria PESTO team) and Mondher Ayadi (NUMERYX) on *Building Self-Driven Network Functions* [19]. Since October 2022.

Orange Innovation (Lannion, France)

Participants: Abdelkader Lahmadi *(contact)*, Joël Ky.

- Joël Ky, CIFRE PhD Student, is supervised by Abdelkader Lahmadi, Raouf Boutaba (University of Waterloo) and Bertrand Mathieu (Orange Innovation) on *Automatic Characterization, Classification and Troubleshooting of Cloud Gaming Applications* [14]. Since October 2021.

Hospices Civils de Lyon, France)

Participants: Abdelkader Lahmadi *(contact)*, Rémi Garcia, Isabelle Chrisment, Pierre-François Gimenez *(PIRAT team)*.

- Rémi Garcia, Research Engineer, is supervised by Abdelkader Lahmadi, Isabelle Chrisment and Pierre-François Gimenez (Inria PIRAT Team, Rennes) on *False Positive Reduction in Intrusion Detection Systems for Hospital Environments*. Since November 2024.

10 Partnerships and cooperations

10.1 International initiatives

10.1.1 Associate Teams in the framework of an Inria International Lab or in the framework of an Inria International Program

NSSICS

Title: Network Softwarization for Secure Industrial Control Systems

Duration: 2024 to 2026

Coordinator: Jules Deliga (jules.degila@imsp-uac.org)

Partners: University of Abomey Calavi (Bénin)

Inria contact: Abdelkader Lahmadi

Summary: In this associated team project with the University of Abomey Calavi (Benin), we are addressing the problems of securing industrial control systems using machine learning (ML) techniques and software-defined networking (SDN). The work focuses on the development of new techniques for detecting complex attacks, the automated generation of security policies and the orchestration of these policies for their effective deployment. These new techniques must also respect the operational constraints of these critical systems.

10.1.2 Inria associate team not involved in an IIL or an international program

CyberGenAI

Title: Alleviation of Generalization Problems in AI-based Cyber-Deception and Network Anomaly Detection

Duration: 2022 to 2024

Coordinator: Hans Dieter Schotten (schotten@dfki.uni-kl.de)

Partners: DFKI (German Research Center for Artificial Intelligence) and OMU (Osaka Metropolitan University, Japan)

Inria contact: Isabelle Chrisment

Summary: Prediction techniques have gained in performance thanks to Artificial Intelligence (AI) which became the unavoidable enabler for building the new cyber-security solutions to detect, forecast and mitigate threats. On top of the methods used, ML (Machine Learning) is the widely adopted one, for example for intrusion detection. While these techniques are good to recognize previously observed attacks or malicious behaviors, they suffer from their ability to generalize their knowledge with a good accuracy and anticipate new types of attacks.

Therefore, our main objective was to make robust ML techniques when faced with new types of attacks or when deployed within new environments, despite the lack of large and comprehensive datasets.

NetMSS

Title: NETwork Monitoring and Service orchestration for Softwarized networks

Duration: 2018 to 2024

Coordinator: Raouf Boutaba (rboutaba@uwaterloo.ca)

Partners: University of Waterloo (Canada)

Inria contact: Jérôme François

Summary: ML-based solutions in networking involve the selection and configuration of the appropriate ML techniques, and sometimes their extension to fit a particular need. The selection of features, performance metrics and ML algorithms is particularly challenging in this context, which is exacerbated by the limited re-usability of existing results. For instance, ML data processing pipeline starts with data collection and pre-processing both of which are context-specific with respect to the type of data (e.g., network traffic, resource consumption, etc.) and the goals of the analysis.

The focus on the associate team was to enhance monitoring techniques by defining network-specific features which can be transformed into ML-compatible objects such as graphs or vectors. Our aim was also to research on objective-guided feature selection in the context of new network usage including network softwarization technologies and encrypted applications.

10.2 International research visitors

10.2.1 Visits of international scientists

Arnaud Ahouandjinou

Status: Associate Professor

Institution of origin: University of Abomey Calavi

Country: Benin

Dates: from 27/11/2024 to 31/11/2024

Context of the visit: We worked on attack mitigation in industrial control systems as part of the NSSICS associate team.

Mobility program/type of mobility: research stay

Juan Felipe Botero

Status: Associate Professor

Institution of origin: University of Antioquia

Country: Colombia

Dates: from 30/09/2024 to 29/10/2024

Context of the visit: In the context of the collaboration with Prof. Botero, we co-supervise master students on 6-month internships, funded by the ORION program of LUE (Lorraine Université d'Excellence). We work on novel strategies for the mitigation of a predefined cyberattack by leveraging the capabilities of programmable data planes. During this visit, we identified new research directions for Programmable Networks, mainly to extend them with more self driven capabilities.

Mobility program/type of mobility: research stay funded by Inria

Jules Degila

Status: Professor

Institution of origin: University of Abomey Calavi

Country: Benin

Dates: from 27/11/2024 to 31/11/2024

Context of the visit: We worked on attack mitigation in industrial control systems as part of the NSSICS associate team.

Mobility program/type of mobility: research stay

Daishi Kondo

Status: Associate Professor

Institution of origin: Osaka Metropolitan University

Country: Japan

Dates: from 16/09/2024 to 24/09/2024

Context of the visit: We worked on AI-based attack detection methods as part of the CyberGenAI associate team.

Mobility program/type of mobility: research stay

Aurelie Kpoze

Status: PhD Student

Institution of origin: University of Abomey Calavi & ISMP (Institute of Mathematics and Physical Sciences)

Country: Benin

Dates: from November 2024 to April 2025

Context of the visit: As part of her PhD thesis and the NSSICS associate team, she did an internship from November 2024 until April 2025 to work on the security of industrial control systems using SDN and programmable networks.

Mobility program/type of mobility: internship

Michel Nogueira

Status: researcher

Institution of origin: Federal University of Minas Gerais

Country: Brazil

Dates: from 19/06/2024 to 19/07/2024

Context of the visit: Michele Nogueira from UFMG performed a 1-month visit at our research team to establish research collaborations on security management. In that context, she gave a seminar on artificial intelligence for cybersecurity and its application to networking. This resulted in the design and organization of a joint french-brazilian cybersecurity challenge, mixing students from UFMG and UL, organized over the Airbus cyber-range platform of TELECOM Nancy in December 2024.

Mobility program/type of mobility: visiting professor (Université de Lorraine)

10.3 European initiatives

10.3.1 Other european programs/initiatives

ERASMUS+ REWIRE

Participants: Rémi Badonnel, Matthews Jose, Thibault Cholez, Olivier Festor.

Title: Cybersecurity Skills Alliance: a new Vision for Europe

Url: rewireproject.eu

Duration: 2020 to 2024

Coordinator: Mykolas Romeris University – MRU (Lithuania)

Partners: 12 education and training providers, 11 industry/certification partners, and 2 EU umbrella organisations for VET

Local contact: Rémi Badonnel

Summary: REWIRE was the Alliance formed from the four winning pilot projects of the Horizon 2020 cybersecurity call establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap: CONCORDIA, ECHO, SPARTA and CyberSec4Europe. Thus, the REWIRE Alliance represented in total more than 160 partners of the four pilot projects, including big companies, SMEs, universities and cybersecurity research institutes, from 26 EU Member States.

This project provided concrete recommendations and solutions that led to the reduction of skill gaps between industry requirements and sectoral training provision and contributed to support growth, innovation and competitiveness in the field of Cybersecurity. The objective was to build a Blueprint for the Cybersecurity industry and a concrete European Cybersecurity Skills Strategy. The activities included the development of a common methodology for the assessment of the current situation and to anticipate future needs, through identification of existing and emerging skills needs, the creation of a cybersecurity skills framework containing profiles for the needed cybersecurity profiles and their analysis, and the creation of four educational curricula and relevant skills certification schemes for profiles contained in the cybersecurity skills framework.

10.4 National initiatives

10.4.1 ANR

ANR PRESTO

Participants: Thibault Cholez *(contact)*, Xavier Marchal.

Title: PRocessing Encrypted Streams for Traffic Oversight

Coordinator: ENS Paris (David Pointcheval)

Duration: 2020 to 2024

Partners: Institut Mines-Telecom (IMT), Orange Labs, 6cure, CNRS-LORIA

Local contact: Thibault Cholez

Summary: While GDPR (General Data Protection Regulation) imposes some privacy constraints, growing threats against the servers require traffic analysis to detect malicious behaviors. This analysis includes identification of illegitimate connections to mitigate denial of service attacks, content filtering to limit content exposition or content leakage, and log management for later forensic analysis. Security Information and Event Management (SIEM) that deals with internal and external threats should still remain effective under GDPR constraints. Data protection usually means encryption, which in turn heavily limits the traffic analysis capabilities. The main goal of this project was to bridge the gap between these two security and privacy requirements, with advanced cryptographic tools (such as searchable encryption, functional encryption, fully homomorphic encryption, and multi-party computation) in order to provide privacy to the end users while allowing traffic monitoring by the network security manager.

The RESIST team developed a proof of concept (cf. 7.2) to demonstrate that web contents can be exchanged between a client and a server using KP-ABE to enforce security policies similar to those usually implemented by firewalls that leverages HTTPS-proxy but without any decryption from the middle box and an acceptable level of performance (overhead).

ANR COMMITS

Participants: Abdelkader Lahmadi *(contact)*.

Title: COnverged coMMunication, control and scheduling Infrastructure for multi pods-based Transport Systems

Coordinator: Université de Lorraine(Abdelkader Lahmadi)

Duration: 2024 to 2028

Partners: Urbanloop SME, CNAM, CRAN

Local contact: Abdelkader Lahmadi

Summary: The main goal of the project is to develop a converged communication, control and scheduling infrastructure to build a cyber-physical system for managing the Urbanloop transport network at a large scale. The main challenge is to control the entire transport network while respecting safety, security and timing constraints. COMMITS will develop its own control and scheduling system as well as the low-latency communication architecture on which the system relies in order to automate an on-demand and rail-based transport system.

The RESIST team is coordinating this project and is mainly involved in the development and the evaluation of the management of the communication system based on 5G to guarantee the scalability, the security and the QoS of the Urbanloop transport network when deployed with thousands of capsules.

10.4.2 PEPR

PEPR CyberSecurity / SuperviZ

Participants: Jérôme François *(contact)*, Abdelkader Lahmadi, Frédéric Beck *(SED)*.

Acronym: SuperviZ

Title: Supervision and orchestration of cybersecurity

Coordinator: Inria (Ludovic Mé)- Télécom SudParis (Hervé Debar)

Duration: 2022 to 2028

Partners: CentraleSupélec, EURECOM, Institut Mines-Télécom, Institut Polytechnique de Grenoble, Université de Rennes 1, Université de Lorraine, CEA, CNRS

Local contact: Jérôme François

Summary: SuperviZ is one of the projects of PEPR on cybersecurity under the axis *security of systems* and under the domain *security of systems, networks and software*. It aims at improving methods in detection, response and mitigation of cyber attacks. Because it is impossible to ensure that a system is 100% secure, supervision of security aims at improving preventive techniques and mitigate the threats when those techniques failed to provide a sufficient level of security. This project considers the following challenges: increase of the volume and heterogeneity of devices to be managed, complexity of the interconnection of different systems grouped into large-scale critical infrastructure (system of systems), sophistication of attacks becoming more and more stealthy, massive attacks targeting a significant number of devices within a short-term attack campaign.

The RESIST team is involved in the following topics of research: reinforcement learning for automated risk assessment, robust and explainable automated machine learning pipeline, automated mitigation of cyber-threats, generalization of behavioral detection techniques, creation of a SDN-capable platform for network experiment.

PEPR Networks of the Future / NF-HiSec

Participants: Isabelle Chrisment *(contact)*, Rémi Badonnel, Nicolas Schnepf.

Title: End-to-end security for the network of the future

Coordinator: IMT (Hervé Debar)

Duration: 2023 to 2027

Partners: IMT, CEA, INRIA, LORIA, CNRS

Local contact: Isabelle Chrisment, Rémi Badonnel

Summary: The NF-HiSec project designs new methods and tools to secure the networks of the future. More specifically its covers five 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 focuses on the protection of 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 is 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.

The RESIST team is interested in automating and formally verifying the building and off-loading of chains of security functions at the edge level in the context of networks of the future.

PEPR Networks of the Future / NF-NAI

Participants: Thibault Cholez *(contact)*, Olivier Festor.

Title: Networks Architecture and Infrastructure and Networks, Cloud, and Sensing Convergence

Coordinator: IMT (Gérard Memmi)

Duration: 2023 to 2027

Partners: IMT, CEA, Eurecom, INRIA, CNRS

Local contact: Thibault Cholez, Olivier Festor

Summary: Beyond traditional objectives, including advances in throughput, execution speed, latency, or object connection density, the outcomes of the NF-NAI project will enable the effective integration of multiple new technologies, including technologies for the physical layer (e.g. reconfigurable intelligent surfaces), transition to 3D systems (e.g. NTN – non-terrestrial networks) and architectural principles (e.g. slicing and dynamic end-to-end orchestration). The project will facilitate the emergence of new applications and services by reaching the objective of transparency – towards uses – in terms of performance, robustness and security. The project will also design interfaces offering a rich level of capabilities and personalization to the service plane and to application developers, over the whole chain, from connected mini-objects to large data centres through multi-access edge computing (MEC).

The RESIST team is interested in improving radio network support for low-latency high-bitrate applications by proposing either new Active Queue Management algorithms or by improving scheduling decisions of the base station to better take into account the QoS requirements of network flows.

PEPR Cloud / TRUSTINCloudS

Participants: Isabelle Chrisment *(contact)*, Rémi Badonnel *(contact)*, Nicolas Schnepf, Thibault Cholez, Olivier Festor.

Title: Cybersecurity of cloud infrastructures

Coordinator: CEA (Aymen Boudguiga)

Duration: 2023 to 2030

Partners: AMU, IMT, UL, EURECOM, UT3, CEA, INRIA

Local contact: Isabelle Chrisment, Rémi Badonnel

Summary: The TRUSTINCloudS project will design solutions for the major cybersecurity challenges specific to Cloud environments. The work carried out in this project aims at adapting traditional security mechanisms (*e.g.* PEPR Cyber) to the characteristics of the Cloud in order to address the specific threats of the different types of Clouds (IaaS, PaaS,...). The main objective of TRUSTINCloudS is to study and develop new methodologies to strengthen Cloud security and implement them in platforms in order to build a sovereign and trusted Cloud. It must also raise awareness of the possibilities and limitations of these methodologies. The project is organized in such a way as to work on the one hand on the security of the infrastructures, and on the other hand on the security of the data (in the broad sense) that these infrastructures host. When relevant, prototypes will be implemented within the shared infrastructure provided by the SILECS project of the PEPR Cloud.

The RESIST team is planning to investigate two different topics. The first is related to the security management of cloud infrastructures, in link with the activities developed in the SPIREC project (see paragraph 10.4.2 below) also part of the PEPR Cloud. The second axis is done in collaboration with the Inria COAST team and aims to improve the security and the performance of P2P systems using a DHT, such as IPFS.

PEPR Cloud / SPIREC

Participants: Isabelle Chrisment *(contact)*, Abdelkader Lahmadi *(contact)*.

Title: Multi-level supervision and prediction for geo-distributed, heterogeneous infrastructures in the Cloud/Edge/IoT continuum

Coordinator: IMT (Mario Südholt)

Duration: 2023 to 2030

Partners: IMT, CEA, CNRS, INRIA, UVSQ, UL

Local contact: Isabelle Chrisment, Abdelkader Lahmadi

Summary: The Cloud-Edge-IoT continuum (CEI) is characterized by highly heterogeneous infrastructures as well as applications and services that are built using different multi-layer software stacks. The monitoring of infrastructures and applications, anomaly detection of service and application executions as well as the prediction of resources usage are fundamental services for the management of the CEI, just like for the Cloud. The SPIREC project will meet the challenges of supervising services of the continuum, detecting their execution anomalies and predicting their resource usage. The project aims to define methods and techniques, notably using distributed machine learning, to enable its efficient management, provide means to secure them and, more generally, ensure a variety of quality of service properties. The partners will also develop software components and tools in order to integrate these functionalities in existing infrastructures and applications, in particular SLICES, industrial systems and future software ecosystems.

The RESIST team is planning to investigate methods and techniques for monitoring hardware and software resources in Cloud/Fog/IoT infrastructures. The team is also interested in studying AI-based approaches to improve multi-level anomaly detection and to facilitate the placement of supervision probes and the analysis of large volumes of logs.

10.4.3 Inria joint Labs

Inria-Orange Joint Lab

Participants: Jérôme François *(contact)*, Olivier Festor, Matthews Jose, Abdelkader Lahmadi, Joël Roman Ky, Raouf Boutaba, Nicolas Schnepf.

Title: Inria - Orange Joint Laboratory

Duration: 2015 to 2025

Summary: The challenges addressed by the Inria-Orange joint laboratory relate to the massively distributed infrastructure and fog/edge computing virtualization. In particular the management of these infrastructures with the use of AI-based techniques and the lifecycle of deployed applications will be considered including different perspectives: performance, energy, security...

11 Dissemination

Participants: Rémi Badonnel, Thibault Cholez, Isabelle Chrisment, Olivier Festor, Abdelkader Lahmadi, Jérôme François, Nicolas Schnepf.

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

Member of the organizing committees

- Rémi Badonnel: IEEE/IFIP Network Operations and Management Symposium (NOMS 2024), experience track co-chair, IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), travel grant co-chair.
- Olivier Festor: IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), Distinguished Experts Panels co-chair.

11.1.2 Scientific events: selection

Member of the conference program committees

- Rémi Badonnel: IEEE/IFIP Network Operations and Management Symposium (NOMS 2024), IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), IEEE/IFIP International Conference on Network and Service Management (CNSM 2024) (TPC & best paper award committee member), Cyber Security in Networking Conference (CSNet 2024), IEEE Conference on Network Softwarization (NetSoft 2024), IEEE Global Information Infrastructure and Networking Symposium (GIIS 2024), IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2025)
- Thibault Cholez: IEEE/IFIP Network Operations and Management Symposium (NOMS 2024), IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), IEEE Conference on Network Softwarization (NetSoft 2024)(PhD Symposium), Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication (CoRes 2024), ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI 2024)
- Isabelle Chrisment: IEEE/IFIP Network Operations and Management Symposium (NOMS 2024), IEEE/IFIP International Conference on Network and Service Management (CNSM 2024), IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2024), International Workshop on Traffic Measurements for Cybersecurity (WTMC 2024), IEEE/IFIP Network Operations and Management Symposium (NOMS 2025)
- Olivier Festor: IEEE/IFIP Network Operations and Management Symposium (NOMS 2024), IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), IEEE/IFIP International Conference on Network and Service Management (CNSM 2024), IEEE Conference on Network Softwarization (NetSoft 2024)
- Abdelkader Lahmadi: IEEE/IFIP Network Operations and Management Symposium (NOMS 2024), IEEE/IFIP Network Operations and Management Symposium (NOMS 2025), IEEE/IFIP International Conference on Network and Service Management (CNSM 2024), IEEE International Conference on Communications (ICC 2024), IEEE International Mediterranean Conference on Communications and Networking (MeditCom 2024), IEEE Annual Consumer Communications & Networking Conference (CCNC 2024), IEEE Conference on Standards for Communications (CSCN 2024)

11.1.3 Journal

Member of the editorial boards

- Rémi Badonnel: Editor-in-Chief for Springer Journal of Network and System Management (JNSM) since January 2023, Associate Editor for IEEE Transactions on Network and Service Management (TNSM), Associate Editor for IEEE Transactions on Cloud Computing, Associate Editor for Wiley International Journal of Network Management (IJNM).

- Thibault Cholez: Associate Editor for Springer Journal of Network and System Management (JNSM).
- Abdelkader Lahmadi: Associate Editor for Wiley International Journal of Network Management (IJNM)

Reviewer - reviewing activities

- Rémi Badonnel: IEEE Transactions on Network and Service Management (TNSM), IEEE Transactions on Cloud Computing (TCC), Springer Journal of Network and System Management (JNSM), Wiley International Journal of Network Management (IJNM)
- Thibault Cholez: IEEE Transactions on Network and Service Management (TNSM), Springer Journal of Network and System Management (JNSM)
- Abdelkader Lahmadi: IEEE Transactions on Network and Service Management (TNSM), IEEE Communications Magazine (COMMAG), IEEE Transactions on Information Forensics and Security, IEEE Network Journal, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Software Engineering, IEEE Internet of Things Journal
- Nicolas Schnepf: Springer Journal of Network and System Management (JNSM)

11.1.4 Invited talks

- Rémi Badonnel:
  - Talk on the TELECOM Nancy Cyber-Security Training Platform for the Cyber-Range Inauguration Launch Event with Airbus Defense and Space Cyber, in March 2024.
  - Talk on Cybersecurity (Research, Education, Innovation) at the European Forum InCyber, Lille in April 2024.
  - Participation in a Panel on Cybersecurity at the AN2V Assises, Strasbourg in May 2024.
  - Presentation of the REWIRE European Project and its Results, at the EuroSatory European Defense and Security Exhibition, Paris in June 2024.
  - Talk on Cybersecurity at the IMT/Inria Technological Event organized at the Campus Cyber, Paris in November 2024.
- Thibault Cholez: Talk on the state of P2P networks security against the Sybil attack at Workshop coorganized by 3 CNRS research workgroups (GDR RSD, GPL and SI) on the security of network stacks, Orléans, September 2024.
- Isabelle Chrisment:
  - Presentation of the HiSec Project on end-to-end security for the network of the future at the B5G/6G Japan-France Joint Workshop in Tokyo, July 2024 ;
  - Participation in a Panel on cybersecurity threats to critical infrastructures at the PEPR Cybersecurity Scientific Day, December 2024.
- Abdelkader Lahmadi:
  - Talk on attack paths management and prediction during the Cyber day organised by Clusir-Est (professional association of cyber security), Juin 2024.
  - Participation in a Panel on "Attack Path Management" at Campus Cyber (Forum InCyber), Paris, February 2024.

11.1.5 Leadership within the scientific community

- Rémi Badonnel is chair of the IFIP (International Federation for Information Processing) WG6.6 (Working Group 6.6) dedicated to the management of networks and distributed systems, and is member of the SSLR Working Group (Security of Systems, Software and Networks) of the CNRS GDR on Cybersecurity.
- Olivier Festor is member of the NISC Board. NISC stands for NOMS IM steering committee. The board coordinates the organization, management and evolution of the major conferences in the Network and Service Management scientific community and interacts with the associated Scientific and Professionnal organizations.

11.1.6 Scientific expertise

- Rémi Badonnel is, together with Marine Minier, in charge of the coordination of research, teaching and innovation activities on cybersecurity at the University of Lorraine. He also serves as an international expert for the Belgian Win2Wal program, and as a reviewer for the ANR Generic Call for Proposals.
- Thibault Cholez: Reviewer for ANRT.
- Isabelle Chrisment is a member of the SLICES-PP project's general assembly. She participates in the steering committee of ECLAT (Extreme Computing Lab for Astronomical Telescopes), a joint laboratory between Inria, the Côte d'Azur Observatory, the Paris-PSL Observatory and Eviden. She is also the regional scientific coordinator for the Alliage project in the context of the CPER Grand-Est (2021-2027). In 2024, she chaired the CRCN/ISFP recruitment committee at Inria Centre at Rennes University.
- Olivier Festor is member of the Scientific Board of Orange.

11.1.7 Research administration

- Rémi Badonnel is a member of the COMIPERS at Inria Nancy Grand Est, and of the CMI at University of Lorraine.
- Isabelle Chrisment is Deputy Scientific Director at Inria in charge of the national scientific domain "Networks, Systems ans Services, Distributed Computing".
- Abdelkader Lahmadi is the scientific head of the High Security Lab of Nancy.

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

Teaching responsibilities

- Rémi Badonnel is heading the Internet Systems and Security specialization of the 2nd and 3rd years at the TELECOM Nancy engineering school, and is responsible for the pedagogical coordination of the cybersecurity platform of this school (including two professional cyber-ranges). He was also in charge of coordinating the design of a new training curriculum on cybersecurity by apprenticeship (one year as a student, two years as apprentice), which has been accredited by the CTI in April 2023, and started in September 2024.
- Thibault Cholez is in charge of the diplomas in apprenticeship at TELECOM Nancy engineering school.
- Olivier Festor is the Director of *Lorraine INP* which groups all eleven engineering schools of University of Lorraine and one undergraduate programme (classe préparatoire aux grandes écoles).
- Abdelkader Lahmadi is heading the Engineering of Digital Systems (ISN) degree at ENSEM engineering school.

Teaching courses

- Rémi Badonnel: 242 hours - L3, M1, M2 - Networks, Systems and Services, Software Design and Programming, Cloud Computing, Network and Security Management - TELECOM Nancy, Université de Lorraine
- Thibault Cholez: 200 hours (half-delegation in CNRS) - L3, M1, M2 - Computer Networks, Network Services Administration, Mobile applications and Internet of Things, Git, Linux Commands and Tools - TELECOM Nancy, Université de Lorraine
- Olivier Festor: 192 hours - L3, M1, M2 - Advanced algorithmics and problem solving, Advanced data structures, Competitive programming, Databases and data management, Assembly language, network security, network management, Software testing Devops and SCRUM, Project Management - TELECOM Nancy, Université de Lorraine
- Jérôme François: 70 hours - M1, M2 - Network security, network management, big data - TELECOM Nancy, Université de Lorraine
- Abdelkader Lahmadi: 280 hours - L3, M1, M2 - Sensor Networks, Distributed Systems and Algorithms, Algorithms and Advanced Programming, Security of Cyber Physical Systems - ENSEM Engineering School, Université de Lorraine

E-learning

- MOOC *Supervision de Réseaux et Services*, FUN Project, Université de Lorraine, Ingénieur, formation initiale et continue, Thibault Cholez, Rémi Badonnel, Laurent Andrey, Olivier Festor, Abdelkader Lahmadi, Jérôme François. The content of the MOOC has been opened to other academic curricula through the FUN CAMPUS platform. Two local sessions have also been organized in 2024 at TELECOM Nancy for students and apprentices.
- MOOC *Sécurité des Réseaux Informatiques (Session 4)*, FUN Project, IMT (SudParis et Saint Étienne), Inria (Jérôme François), from October to November 2024.
- MOOC *Becoming a Cybersecurity Consultant*, Concordia Project, Rémi Badonnel, Thibault Cholez and Lama Sleem. The course contents were on open access on the Coursera MOOC platform in 2024.
- MOOC *Penetration Tester and Cyber Threat Intelligence Specialist*, REWIRE European Skills Alliance on Cybersecurity, Matthews Jose, Remi Badonnel. Contributions to MOOCs related to two cybersecurity profiles, including courses and practical exercices related to the cyber-kill chain hosted over the KYPO open-source cyber-range.

11.2.2 Supervision

PhD in progress

- Omar Anser, *Automation of Attack Mitigations in 5G Environments*, since December 2021, supervised by Isabelle Chrisment and Jérôme François.
- Ahmad Atwi, *Adaptive and Optimal Placement of Monitoring Probes Based on Reinforcement Learning*, since December 2024, supervised by Isabelle Chrisment and Abdelkader Lahmadi.
- Enzo D'Andrea, *Graph-based Network Data Representation for Machine Learning*, since October 2021, supervised by Olivier Festor and Jérôme François.
- Victor De Moura Neto, *Improving security and performance of IPFS's DHT*, since October 2024, supervised by Thibault Cholez and Claudia Ignat (COAST team).
- Mohamed Amine El Yagouby, *Modeling and Detection of AI-Assisted Cyberattacks*, since November 2024, supervised by Olivier Festor and Abdelkader Lahmadi in cooperation with Mounir Ghogho and Mehdi Zakroum (International University of Rabat, Morocco).

- Katsuki Isobe, *Security Orchestration at the Edge for Future Networks*, since October 2024 (pre-thesis from June to September 2024), supervised by Rémi Badonnel and Nicolas Schnepf.
- Joël Ky, *Characterization, Classification and Diagnosis of Cloud Gaming Applications*, since October 2021, supervised by Raouf Boutaba (University of Waterloo, Canada) and Abdelkader Lahmadi.
- Jhon Sebastian Rojas Rodriguez, *Anomaly Detection in Heterogeneous and Multi-level Monitoring Data*, since December 2024, supervised by Isabelle Chrisment and Abdelkader Lahmadi.
- Franco Terranova, *Reinforcement Learning-Based Approaches for Automated Security Analysis of Networked Systems*, since October 2023, supervised by Isabelle Chrisment and Abdelkader Lahmadi.
- Wafik Zahwa, *Building Self-Driven Network Functions*, since October 2022, supervised by Michael Rusinowitch (PESTO team) and Abdelkader Lahmadi.

11.2.3 Juries

Team members participated in the following Ph.D. defense committees:

- Farouk Damoun, PhD in Computer Science from Université Claude Bernard Lyon 1 and University of Luxembourg. Title: *Enhancing Federated Learning for Financial Sector via Graph Learning and Language Models*, November 2024 - (Rémi Badonnel as reviewer).
- Stanislav Špaček, PhD in Computer Science from Faculty of Informatics, Masaryk University, Brno (Czechia). Title: *Improving Cyber Situational Awareness through Event-Flow Correlation*, March 2024 - (Isabelle Chrisment as reviewer).
- Estelle Hotellier, PhD in Computer Science from Université Grenoble Alpes. Title: *Specification-based Intrusion Detection for Hierarchical Hybrid Industrial Control Systems*, April 2024 - (Isabelle Chrisment as examiner).
- Marwan Abbas Escribano, PhD in Computer Science from Institut Polytechnique de Paris (Telecom SudParis). Title: *Modélisation de systèmes de leurres complexes*, April 2024 - (Isabelle Chrisment as president).
- Camille Moriot, PhD in Computer Science from INSA Lyon. Title: *Méthodologie de caractérisation socio-organisationnelle des adresses IPs appliquée à la sécurité*, September 2024 - (Isabelle Chrisment as reviewer).
- Jeremy Mechouche, PhD in Computer Science from Institut Polytechnique de Paris (Telecom SudParis). Title: *Gérer et assurer la qualité de services de ressources dans un environnement multi-cloud*, October 2024 - (Isabelle Chrisment as reviewer).
- Sorithy Seng, PhD in Computer Science from Institut Polytechnique de Paris (Telecom SudParis). Title: *Sonde de détection d'intrusion réseau avec suivi d'état de protocole et détection d'anomalie, de la modélisation à la combinaison entre des méthodes de spécification et de fouille de données (data mining)*, November 2024 - (Isabelle Chrisment as reviewer).
- Robin Duraz, PhD in Computer Science from École Nationale Supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire - IMT Atlantique. Title: *Trustable machine Learning for intrusion detection system*, November 2024 - (Isabelle Chrisment as examiner).
- Pierre-Antoine Rault, PhD in Computer Science from University of Lorraine. Title: *Access control mechanisms for collaborative systems without central authority*, December 2024 - (Isabelle Chrisment as president).
- Céline Minh, PhD in Computer Science from University of Toulouse (INSA Toulouse). Title: *Utilisation de techniques d'intelligence artificielle pour reconstituer et expliquer des cyberattaques à partir d'anomalies réseau*, December 2024 - (Isabelle Chrisment as examiner).

- Abderaouf Khichane, PhD in Computer Science from Paris Saclay University. Title: *Diagnostic de performances par interprétation de données et actions correctives pour des fonctions réseau cloud natives*, March 2024 - (Olivier Festor as President of the Committee).
- Lionel Tailhardat, PhD in Computer Science from Sorbonne Université. Title: *Anomaly Detection using Knowledge Graphs and Synergistic Reasoning: Application to Network Management and Cyber Security*, September 2024 - (Olivier Festor as reviewer).
- Niels Rodday, PhD in Computer Science from Universität der Bundeswehr München. Title: *Improving Internet Routing Security: From Origin Validation to Path Validation* , March 2024 - (Olivier Festor as examiner).
- Dun LI, PhD in Computer Science from Institut Polytechnique de Paris (Telecom SudParis). Title: *Optimized Blockchain Deployment and Application for Trusted Industrial Internet of Things*, September 2024 - (Abdelkader Lahmadi as reviewer).
- Yiqun WANG, PhD in Computer Science from University of Luxembourg. Title : *Cross Domain Early Crop Mapping based on Time-series Remote Sensing Data*, December 2024 - (Abdelkader Lahmadi as reviewer).

Team members participated in the following Habilitation Degree committees:

- Gilles Guette, HDR in Computer Science from Rennes University (France). Title: *Contribution à la sécurité des réseaux et à la compréhension des attaques et des attaquants*, March 2024 - (Isabelle Chrisment as reviewer).
- Francesco Bronzino, HDR in Computer Science from ENS Lyon (France). Title: *Bridging the Gap Between Machine Learning and Networked Systems*, September 2024 - (Isabelle Chrisment as reviewer).

11.3 Popularization

11.3.1 Specific official responsibilities in science outreach structures

- Rémi Badonnel coordinated in 2024 the organization of two Capture The Flag events on cybersecurity which took place at TELECOM Nancy, the Engineering school of Computer Science of University of Lorraine, which targets Bachelor-level and Master-level students in Cybersecurity, with the objective of finding the maximum number of vulnerabilities on a specific system hosted over a cyber-range platform.
- Rémi Badonnel participated to the organization of the Cyber Humanum Est event, which corresponds to a 5-days cyber wargame exercise dedicated to cyber crisis management, bringing together more than 100 participants, and organized under the aegis of the Cyber Defense Command (COMCYBER) of the Ministry of Armed Forces, and of Lorraine INP, the Collegium of Engineering Schools of the University of Lorraine.

11.3.2 Participation in Live events

- The RESIST team pursued its involvement in the Erasmus+ REWIRE Cybersecurity Skills Alliance, which aims at designing a European blueprint for the cybersecurity sectorial market together with the development of four VOOCs (Vocational Open Online Courses), including certifications, dedicated to the area of cybersecurity, targeting professionals and specialized students. In that context, Matthews Jose and Rémi Badonnel have organized two new national infodays dedicated to REWIRE, in order to promote its last results in 2024.

12 Scientific production

12.1 Major publications

[1] P. Graff, X. Marchal, T. Cholez, B. Mathieu, S. Tuffin and O. Festor. 'Improving Cloud Gaming traffic QoS: a comparison between class-based queuing policy and L4S'. In: *2024 8th Network Traffic Measurement and Analysis Conference (TMA)*. Network Traffic Measurement and Analysis Conference (TMA 2024). Dresden, Germany: IEEE, 22nd May 2024, p. 10. DOI: 10.23919/TMA62044.2024.10558920. URL: https://inria.hal.science/hal-04594817.

[2] M. Jose, K. Lazri, J. François and O. Festor. 'Stateful InREC: Stateful In-network REal Number Computation with Recursive Functions'. In: *IEEE Transactions on Network and Service Management* (10th Aug. 2022), pp. 1–1. DOI: 10.1109/TNSM.2022.3198008. URL: https://inria.hal.science/hal-03794876.

[3] A. Laraba, J. François, S. Rahman Chowdhury, I. Chrisment and R. Boutaba. 'Mitigating TCP Protocol Misuse With Programmable Data Planes'. In: *IEEE Transactions on Network and Service Management* 18.1 (Mar. 2021), pp. 760–774. DOI: 10.1109/TNSM.2021.3054528. URL: https://inria.hal.science/hal-03480222.

[4] N. Schnepf, R. Badonnel, A. Lahmadi and S. Merz. 'Automated Orchestration of Security Chains Driven by Process Learning'. In: *Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning*. Wiley, 12th Oct. 2021. DOI: 10.1002/9781119675525.ch12. URL: https://inria.hal.science/hal-03518390.

[5] F. Terranova, A. Lahmadi and I. Chrisment. 'Leveraging Deep Reinforcement Learning for Cyber-Attack Paths Prediction: Formulation, Generalization, and Evaluation'. In: The 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2024). Padua, Italy, 30th Sept. 2024, pp. 1–16. DOI: 10.1145/3678890.3678902. URL: https://hal.science/hal-04662428.

12.2 Publications of the year

International peer-reviewed conferences

[6] O. Anser, J. François and I. Chrisment. 'Automated Machine Learning Configuration to Learn Intrusion Detectors on Attack-Free Datasets'. In: 2024 IEEE 49th Conference on Local Computer Networks (LCN). Normandy, France: IEEE, 8th Oct. 2024, pp. 1–7. DOI: 10.1109/LCN60385.2024.10639690. URL: https://hal.science/hal-04754391 (cit. on p. 13).

[7] T. Cholez and C.-L. Ignat. 'Sybil Attack Strikes Again: Denying Content Access in IPFS with a Single Computer'. In: *Proceedings of the 19th International Conference on Availability, Reliability and Security*. ARES 2024: The 19th International Conference on Availability, Reliability and Security. Vienna, Austria: ACM, 30th July 2024, pp. 1–7. DOI: 10.1145/3664476.3664482. URL: https://inria.hal.science/hal-04666290 (cit. on p. 10).

[8] E. d'Andréa, J. François, A. Lahmadi and O. Festor. 'Vulnet: Learning Navigation in an Attack Graph'. In: *2024 IEEE 10th International Conference on Network Softwarization (NetSoft)*. 2024 IEEE 10th International Conference on Network Softwarization (NetSoft). Saint Louis, MO, United States: IEEE, 24th June 2024, pp. 393–398. DOI: 10.1109/NetSoft60951.2024.10588918. URL: https://hal.science/hal-04782284.

[9] C. Garzón, A. Lahmadi, J. Vergara, A. Leal and J. F. Botero. 'In-Band ARP-based Man-in-the-Middle Attack Detection Using P4 Programmable Switches'. In: 2024 IEEE Latin-American Conference on Communications (LATINCOM). Medellin, Colombia: IEEE, 6th Nov. 2024, pp. 1–6. DOI: 10.1109/LATINCOM62985.2024.10770688. URL: https://inria.hal.science/hal-04878851 (cit. on p. 12).

[10] P. Graff, X. Marchal, T. Cholez, B. Mathieu, S. Tuffin and O. Festor. 'Improving Cloud Gaming traffic QoS: a comparison between class-based queuing policy and L4S'. In: *2024 8th Network Traffic Measurement and Analysis Conference (TMA)*. Network Traffic Measurement and Analysis Conference (TMA 2024). Dresden, Germany: IEEE, 22nd May 2024, p. 10. DOI: 10.23919/TMA62044.2024.10558920. URL: https://inria.hal.science/hal-04594817 (cit. on p. 11).

[11] K. Isobe, J.-P. Eisenbarth, D. Kondo, T. Cholez and H. Tode. 'A Deeper Grasp of Handshake: A Thorough Analysis of Blockchain-based DNS Records'. In: BRAINS 2024 - 6th Conference on Blockchain Research & Applications for Innovative Networks and Services. Berlin, Germany, 9th Oct. 2024, p. 10. URL: https://inria.hal.science/hal-04733791 (cit. on p. 10).

[12] A. Kpoze, A. Lahmadi, I. Chrisment and J. Degila. 'SDN-based Mitigation of Synchronization Attacks on Distributed and Cooperative Controls in Microgrid'. In: NOMS 2024-2024 IEEE Network Operations and Management Symposium. Vol. 6. Seoul, South Korea: IEEE, 6th May 2024, pp. 1–3. DOI: 10.1109/NOMS59830.2024.10575853. URL: https://inria.hal.science/hal-04703920 (cit. on pp. 9, 12).

[13] A. Kpoze, A. Lahmadi, I. Chrisment and J. Degila. 'SDN-Based Reconfiguration of Distributed and Cooperative Microgrid Control Systems for Mitigating Synchronization Attacks'. In: IEEE International Conference on Cyber Security and Resilience (CSR 2024). London, France: IEEE, 2nd Sept. 2024, pp. 789–794. DOI: 10.1109/CSR61664.2024.10679389. URL: https://inria.hal.science/hal-04709268 (cit. on p. 12).

[14] J. R. Ky, B. Mathieu, A. Lahmadi and R. Boutaba. 'CATS: Contrastive learning for Anomaly detection in Time Series'. In: 2024 IEEE International Conference on Big Data (Big Data). Washinghton DC, United States, 16th Jan. 2025. DOI: 10.1109/BigData62323.2024.10825476. URL: https://hal.science/hal-04881349 (cit. on pp. 12, 15).

[15] C. Lanza, A. Lahmadi and F. Osmond. 'An Empirical Study of Ransomware Vulnerabilities Descriptions'. In: 10th International Conference on Information Systems Security and Privacy. Rome, Italy: SCITEPRESS - Science and Technology Publications, 26th Feb. 2024, pp. 146–153. DOI: 10.5220/0012378700003648. URL: https://inria.hal.science/hal-04602391 (cit. on p. 13).

[16] B. Mathieu, O. Dugeon, J. R. Ky, P. Graff and T. Cholez. 'Segment Routing for Chaining Micro-Services at Different Programmable Network Levels'. In: 27th Conference on Innovation in Clouds, Internet and Networks (ICIN). Paris, France: IEEE, 11th Apr. 2024, pp. 171–178. DOI: 10.1109/ICIN60470.2024.10494472. URL: https://hal.science/hal-04544951 (cit. on p. 15).

[17] A. A. Razzac, T. Chahed, Z. Shamseddine and W. Zahwa. 'Advanced sleep modes in 5G multiple base stations using non-cooperative multi-agent reinforcement learning'. In: *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*. IEEE Global Communications Conference (GLOBECOM). Kuala Lumpur, Malaysia: IEEE, 26th Feb. 2024, pp. 7025–7030. DOI: 10.1109/GLOBECOM54140.2023.10437599. URL: https://hal.science/hal-04492371.

[18] F. Terranova, A. Lahmadi and I. Chrisment. 'Leveraging Deep Reinforcement Learning for Cyber-Attack Paths Prediction: Formulation, Generalization, and Evaluation'. In: The 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2024). Padua, Italy, 30th Sept. 2024, pp. 1–16. DOI: 10.1145/3678890.3678902. URL: https://hal.science/hal-04662428 (cit. on p. 13).

[19] W. Zahwa, A. Lahmadi, M. Rusinowitch and M. Ayadi. 'In-Network ACL Rules Placement using Deep Reinforcement Learning'. In: 2024 IEEE International Mediterranean Conference on Communications and Networking (MeditCom). Madrid, Spain: IEEE, 8th July 2024, pp. 341–346. DOI: 10.1109/MeditCom61057.2024.10621188. URL: https://inria.hal.science/hal-04703877 (cit. on pp. 11, 15).

Scientific books

[20] C. Lanza, A. Lahmadi and J. François. *Ransomware Analysis: Knowledge Extraction and Classification for Advanced Cyber Threat Intelligence*. 1. CRC Press, 13th Nov. 2024, p. 112. DOI: 10.1201/9781003528999. URL: https://inria.hal.science/hal-04704329 (cit. on p. 13).

Reports & preprints

[21] R. Bondaruc, N. Schnepf, R. Badonnel, C. A. Ardagna and M. Anisetti. *Towards Secure Service Deployment in Cloud-Edge Continuum*. 22nd Jan. 2025. URL: https://inria.hal.science/hal-04907033 (cit. on p. 14).

[22] N. Schnepf, R. Badonnel, D. Saucez, J. Sbara and S. Schmid. *Towards Vulnerability and Congestion Aware Software Update Synthesis for Softwarized Networks*. 22nd Jan. 2025. URL: https://inria.hal.science/hal-04906917 (cit. on p. 14).

Other scientific publications

[23] G. Mirsky, J. Halpern, X. Min, A. Clemm, J. Strassner and J. François. *RFC 9544 Precision Availability Metrics (PAMs) for Services Governed by Service Level Objectives (SLOs)*. 1st Mar. 2024. URL: https://hal.science/hal-04781758.

[24] F. Terranova. 'Deep Reinforcement Learning for Automated Cyber-Attack Path Prediction in Communication Networks'. In: Geilo Winter School 2024 - Graphs and Applications. Ed. by A. Lahmadi and I. Chrisment. Geilo, Norway, 21st Jan. 2024. URL: https://hal.science/hal-04462876 (cit. on p. 13).