RESEARCH CENTRE

Inria Centre at Université de Lorraine

IN PARTNERSHIP WITH:

Université de Lorraine, CNRS

2023

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]
- Jerome François [INRIA, Researcher, until Feb 2023]
- 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 Fellows

- Xavier Marchal [UL, from May 2023]
- Xavier Marchal [CNRS, Post-Doctoral Fellow, until Jan 2023]

PhD Students

- Omar Anser [INRIA]
- Enzo D'Andrea [INRIA]
- Philippe Graff [UL, from Sep 2023]
- Philippe Graff [CNRS, until Sep 2023]
- Joel Ky [ORANGE, CIFRE]
- Mohamed Oulaaffart [UL, until Jul 2023]
- Franco Terranova [UL, from Oct 2023]
- Mehdi Zakroum [Université Internationale de Rabat, until Aug 2023]

Technical Staff

- Karim Baccar [INRIA, Engineer, until Sep 2023]
- Matthews Jose [TELECOM NANCY, Engineer]
- Alexandre Merlin [INRIA, Engineer, until Jan 2023]

Interns and Apprentices

- Thomas Bigel [UL, Intern, from Mar 2023 until Aug 2023]
- Paul Cambon [UL, Intern, until May 2023]
- Sami Daafouz [INRIA, Intern, from Apr 2023 until Jul 2023]
- Victor Henrique De Moura Netto [UL, Intern, from May 2023 until Aug 2023]
- Mohamed El Amri [INRIA, Intern, from Apr 2023 until Jul 2023]
- Christian Garzon Vaquez [UL, Intern, from May 2023 until Oct 2023]
- Christian Camilo Garzón [UL, Intern, from May 2023 until Oct 2023]
- Quentin Hopp [INRIA, Intern, from Jun 2023 until Aug 2023]
- Hugues Kameni Tonga [INRIA, Intern, from Apr 2023 until Jul 2023]
- Satou Kpoze [UL, Intern, from Jun 2023 until Sep 2023]
- Satou Kpoze [INRIA, Intern, from Mar 2023 until Jun 2023]
- Theo Rusinowitch [INRIA, Intern, from Apr 2023 until Aug 2023]

Administrative Assistants

- Delphine Hubert [UL, from Sep 2023]
- Cecilia Olivier [INRIA, from Jul 2023]

Visiting Scientists

- Ruslan Bondaruc [Università degli Studi di Milano, from May 2023 until Oct 2023]
- Raouf Boutaba [University of Waterloo, CA]
- Claudia Lanza [Università della Calabria, from Jun 2023]

External Collaborator

- Jérôme François [University of Luxembourg, from Mar 2023]

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 Resist 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.

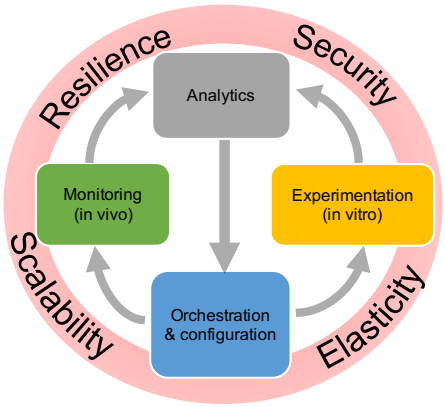

Figure 1: The Resist project

Softwarization of networks and **data analytics** are key enablers to design intelligent methods to orchestrate – *i.e.* configure in a synchronized and distributed manner – both network and system resources. Intelligent **orchestration** leverages relevant data for decision-making using **data analytics**. Input data reflecting the past, current and even future (predicted) states of the system are used to build relevant knowledge. Two approaches are pursued to generate knowledge and to validate orchestration decisions. First, a running system can be **monitored in vivo**. Second, **in vitro experimentation** in a controlled environment (simulators, emulators and experimental platforms) is helpful to reproduce a running system with a high reliability and under different hypotheses. Monitoring and experimentation are steered and configured through orchestration according to the two intertwined loops illustrated in Figure 1.

Accordingly Resist is thus structured into four main research objectives (activities) namely Monitoring, Experimentation, 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.

3.3 Experimentation

Of paramount importance in our target research context is experimental validation using testbeds, simulators and emulators. In addition to using various existing experimentation methodologies, Resist contributes in **advancing the state of the art in experimentation methods and experimental research practices**, particularly focusing on elasticity and resilience.

We develop and deploy testbeds and emulators for **experimentation with new networking paradigms** such as SDN and NFV, to enable large-scale in-vitro experiments combining all aspects of Software-Defined Infrastructures (server virtualization, SDN/NFV, storage). Such fully controlled environments are particularly suitable for our experiments on resilience, as they ease the management of fault injection features.

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.

3.4 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.

3.5 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 Deied 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)*. In this context he animated a café about the energetic cost of streaming download in our research activity, especially in the context of visioconferences. He also presented this group at the project committee of the INRIA center at Nancy in order to identify how the numeric sobriety could be explored as a research topic.

6 Highlights of the year

6.1 Awards

Joël Roman Ky won the Audience Award @ « Ma thèse en 3 minutes » organized by Orange Innovation Research. See the Press article.

7 New software, platforms, open data

7.1 New software

7.1.1 5GFuzz

Name: Fuzzing tool for 5G protocols

Keywords: Fuzzing, 5G protocols

Scientific Description: 5GFuzz is a tool used to generate and inject on the fly ASN1 compliant messages for the RRC, NAS and NGAP protocols.

Functional Description: This tool is dedicated to the fuzzing of 5G protocols. It automatically generates 5G messages by using ASN.1 specification and it injects them at the 5G air interface.

Authors: Karim Baccar, Abdelkader Lahmadi

Contact: Abdelkader Lahmadi

7.2 New platforms

5G Security Assessment Platform

Participants: Abdelkader Lahmadi *(contact)*, Karim Baccar.

During 2023, we enhanced and extended our platform [8] dedicated to the security assessment of 5G networks and their respective protocols. Our platform provides a full end-to-end 5G network and operates in standalone mode (SA). It relies on hardware base station (Amarisoft CallBox) and uses Ettus USRP B210 SDR cards for radio transmission. It also contains mobile 5G devices operating and UE emulators. This platforms is used to develop mainly fuzzing and security assessment tools dedicated to 5G protocols [7]. First prototypes of these tools are already integrated in the platform to generate and inject on the fly 5G packets. This platform is restricted to be used by the RESIST team.

7.3 Open data

7.3.1 Cloud Gaming traffic captures

Participants: Thibault Cholez *(contact)*, Olivier Festor, Philippe Graff, Joël Ky, Bertrand Mathieu, Xavier Marchal.

- **Network captures of Cloud Gaming traffic:** `pcap` traces of 4 major commercial platforms (GeForce Now, Playstation Now, Stadia, xbox Cloud Gaming), varying resolutions, framerates, games, types of controls (35GB).
- **Network captures of high-bitrate UDP applications:** `pcap` traces including video conferencing services, video streaming, live video streaming, QUIC navigation, and remote desktop (17GB).
- **Network captures of Cloud Gaming traffic on a fixed capacity network under different constraints:** `pcap` traces of 4 CG platforms subject to throughput constraints, latency, loss rate and jitter occurring before the game session (60GB) or during it (25GB).
- **Network captures of Cloud Gaming traffic on 4G network:** `pcap` traces of 4 CG platforms run over 6 different Orange 4G cellular network environments (71GB).

Link to the datasets: `https://cloud-gaming-traces.lhs.loria.fr`

7.3.2 Snapshots of Ethereum's nodes

Participants: Thibault Cholez *(contact)*, Jean-Philippe Eisenbarth.

Our **Crawleth** software keeps crawling the Ethereum network on a regular basis (hourly) to discover the nodes composing it and how their characteristics evolve in time. A public API is available to retrieve either the complete fresh data or aggregated data (on a daily basis) for older periods. http://crawleth.loria.fr:5000/.

An example of dataset (period from September 1 to September 30, 2021) including a description of its format is also available: https://concordia-eth-p2p.lhs.loria.fr/index.html.

Please note that for privacy reasons all the IP addresses are anonymized using a salted SHA256 hash and the last byte of the address is set to 0.

8 New results

8.1 Monitoring

8.1.1 Predictive Security Monitoring for Large-Scale Internet-of-Things

Participants: Rémi Badonnel *(contact)*, Isabelle Chrisment, Jérôme François, Adrien Hemmer.

The Internet-of-Things has become a reality with numerous protocols, platforms and devices being developed and used to support the growing deployment of smart services. Providing new services requires the development of new functionalities, and the elaboration of complex systems that are naturally a source of potential threats. Real cases recently demonstrated that the IoT devices can be affected by naïve weaknesses. Therefore, security is of paramount importance.

In 2023, in the continuation of Adrien Hemmer thesis [16], we have pursued our efforts on an ensemble learning-based architecture for supporting an early detection of multi-phase attacks in IoT systems. This

architecture leverages the performance of five major detection methods, namely process mining, elliptic envelope, one class support vector machine, local outlier factor and isolation forest. We have described the main components of this architecture, their operations and the interactions amongst them. We have complemented this architecture with a feedback loop mechanism, that enables improving the reactivity of attack detection in these systems. In particular, it permits to adjust the parameterization of considered detection methods, when the premises of potential attacks are identified on some data sources characterizing the IoT system. We have also extended our performance evaluation through additional extensive set of experiments based on industrial environments, in order to quantify the impact of perturbations, namely data noises and data losses, on the overall detection results. As future work, we are interested in integrating complementary detection methods to our ensemble-based solution, and elaborating cost-based strategies to determine the best sub-set of detection methods to be considered per data source. We also would like to investigate the coupling of our solution with threat intelligence, such as exploiting vulnerability descriptions to adapt the attack detection strategy based on this additional knowledge.

8.1.2 Monitoring and exploitation of Blockchains' Networking Infrastructure

Participants: Thibault Cholez *(contact)*, Jean-Philippe Eisenbarth.

Blockchains rely on P2P networks that are essential to their proper functioning, as they ensure the dissemination of transactions and blocks to all parties. While Bitcoin and Ethereum – the two main public blockchains – are now worth trillions of dollars, attracting new users and applications (Smart Contracts) every day, few studies focus on the network aspects, although the literature shows that many problems can reduce the reliability or performance of public P2P networks.

In 2023, we finalized and published our last contribution on this subject that aims to exploit the distributed hash table (DHT) of Ethereum to reduce peers' storage needs. We noticed that, on the one hand, the Ethereum P2P network features a DHT that is functional but largely unexploited, as no data is stored inside. On the other hand, the storage of blockchain's data is ever growing at a high rate which will eventually be problematic as fewer nodes will be able to afford the storage costs and participate to the distributed system. We investigated the data storage architecture of the main client of Ethereum (Geth) and its ways of synchronizing the state of the blockchain between the peers. Based on that new knowledge, we designed a new distributed storage architecture for Ethereum taking full advantage of the DHT, that is fully backward compatible with current clients. Thus, the proposed solution allows an incremental deployment, and is able to reduce the disk space used for long-term storage by 95% (58% of the total storage of a node), without impacting the safety guarantees or the performance of the Ethereum blockchain. This work was published in an international conference, ACM BSCI 2023 [10], affiliated to ACM ASIACCS, and in a national conference *Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication (CoRes 2023)* [11].

This work was done in collaboration with Olivier Perrin (INRIA COAST team).

8.1.3 Monitoring Internet-wide threat with a network telescope

Participants: Jérôme François *(contact)*, Isabelle Chrisment, Enzo D'andréa, Mehdi Zakroum.

Network reconnaissance is the first step preceding a cyber-attack. Hence, monitoring the probing activities is imperative to help security practitioners enhancing their awareness about Internet's large-scale events or peculiar events targeting their network. Improving the monitoring of security events and detecting attacks at an early stage are key features to prevent against eventual damages or at least alleviate their impact.

In Mehdi Zakroum's PhD thesis [18], we combined research works on cyber-threat monitoring and cyber-attack classification and forecasting. We designed a cyber-threat monitoring framework intended

for an improved and efficient modeling of large-scale probing activities captured by network telescopes. We also developed a finer-grain model for the inference of cyber-incidents through the characterization of their corresponding network flows [5]. We proposed a method to encode raw network flows into robust latent representations by transforming the latter into intermediate graph-based representations to be analyzed using Graph Auto-Encoders and Anonymous Walk Embeddings. This results in semantically-rich and robust representation vectors which can be manipulated by machine learning algorithms to support different applications. We demonstrated the benefit of our approach to automate the traffic classification of darknet traffic.

In [9], we proposed a new multi-label classification method by representing traffic generated by a host as a graph and leveraging machine learning algorithms (Node embedding and Graph Convolutional Networks). Our technique is able to automatically assign the type of malicious activities associated to observed IP addressed in the darknet knowing that the activities themselves might not be directly observed (such as phishing or spamming).

8.2 Experimentation

8.2.1 Understanding Cloud Gaming Network Traffic and optimizing its transport

Participants: Thibault Cholez *(contact)*, Olivier Festor, Philippe Graff, Joël Ky, Bertrand Mathieu, Xavier Marchal.

In the context of the ANR MOSAICO project (see Section 10.4.1), 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 2023, we published in [2] an extension of our previous work that analyzed the traffic of four CG platforms (Google Stadia, Nvidia GeForce Now, Microsoft xCloud, Sony PlayStation Now) to evaluate the capacity of adaptation and responsiveness of their congestion control algorithm (CCA). We synthetically restricted the network conditions by impacting in turn the delay, jitter, loss rate and available bandwidth with different intensities, and observed the resulting traffic. In particular, we added a new study of CG traffic on cellular networks by reproducing the conditions observed on the Orange 4G network, including a user mobility scenario. We noted some disparities in the platforms' behaviors. Some do not adapt adequately to the different constraints and are therefore exposed to long queuing delays, sometimes resulting in packet losses. Others overreact, to the detriment of their video quality. All of the collected data are available to the community: cloud-gaming-traces.lhs.loria.fr (see Section 7.3.1).

Considering the limitations of end-to-end CCA, we proposed to identify CG traffic in the network to make it benefit from an optimized traffic processing in problematic queues that can induce latency in case of congestion. In 2023, we published in [12] our work regarding the classifier we developed to recognize CG traffic. It achieves a high precision (98.5%) by relying on a machine learning approach featuring the statistical properties of CG traffic which are calculated on the fly. We proposed an implementation of our classifier as a set of virtual network functions (VNF) that can handle 10Gb/s.

In collaboration with Orange Labs, we also proposed an hybrid P4/NFV architecture to implement the classifier that takes the best of both technologies: some fast line-rate but simple processing of packets (extraction of flow statistical features) is performed on an hardware P4 switch, while more complex and computation intensives ones are done by VNFs (classification by a ML model) [14]. The throughput given by our evaluation ultimately proved that a realistic deployment at an ISP (Internet Service Provider) level is possible.

Lastly, we proposed to experiment the transport of CG traffic in a double queue architecture in order to avoid oversized buffers which generate latency and the poor cohabitation with flows driven by loss-based CCAs. 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. Our results show that both approaches perfectly preserve the QoS of CG traffic.

8.2.2 Experimental study of the security of 5G protocols

Participants: Abdelkader Lahmadi *(contact)*, Karim Baccar.

While a significant efforts have been made in the specification and deployment of the 5th generation mobile systems (5G), there is a noticeable lack of practical experiments regarding its security. The 3GPP standardisation body has already defined numerous protocols, procedures and implementation guidelines for 5G. However, many of these requirements and procedures are missing assessment and experiments to validate their security conformance.

During the year 2023, we developed an experimentation testbed and support tools for generating and injecting on the fly 5G packets to realize multiple security assessing tasks in particular fuzzing operations for vulnerabilities discovery. Our tool is implemented and tested within a controlled testbed environment built on top of a 5G standalone core server provided by a hardware base station (gNb) and uses a Software Defined Radio (SDR) card for radio transmission. We validated our testbed and the developed tools by successfully injecting at the 5G air interface and the network control levels different messages including RRC and NGAP/NAS over already established communications [8]. In a next step, we will rely on this experimental platform to implement various DoS attacks in the 5G protocol stack. We mainly show through these experiments that numerous potential misconfigurations and misuses pose significant threats to the security of 5G networks [7].

8.3 Analytics

8.3.1 Efficient Distribution of Security Filtering Rules in SDN

Participants: Abdelkader Lahmadi *(contact)*, Wafik Zahwa.

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. The most challenging task is to deploy in-network rules with a fast and efficient way to avoid a security breach or to meet service needs.

In [15], we developed and compared three algorithms based on graph theory (s-t mincut, greedy) and Reinforcement Learning (RL) techniques to automatically distribute ACLs across networks switches, while minimizing their TCAM (Ternary Content-Addressable Memory) occupancy. We compared these algorithms on several network topologies to evaluate their efficiency in terms of memory occupancy. Our results show the efficiency of the s-t mincut approach in resources utilization, overcoming greedy and RL-based algorithms.

This work was done in collaboration with Michael Rusinowitch (INRIA PESTO team).

8.3.2 Characterization and troubleshooting of cloud gaming applications on mobile networks

Participants: Abdelkader Lahmadi *(contact)*, Raouf Boutaba, 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). While promising remarkable performance compared to manual or threshold-based detection, 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.

In [1], we developed a comprehensive evaluation of eight unsupervised ML models selected from different classes of ML algorithms and applied to AD in the context of cloud gaming applications. We collected cloud gaming Key Performance Indicators (KPIs) time-series datasets in real-world network conditions, and we evaluate and compare the selected ML models using the same methodology, and assess their robustness to data contamination, their efficiency and computational complexity. Our proposed methodology relies on window-based anomaly detection techniques as they are more useful for network operators compared to single point detection approaches. However, we found most existing window-based approaches lack in accuracy and may under or overestimate a model's performance. Therefore, we proposed a novel Window Anomaly Decision (WAD) approach that overcomes these drawbacks.

8.3.3 Support for Programmable In-Network Analytics

Participants: Jérôme François *(contact)*, Olivier Festor, Matthews Jose.

In the context of the Matthews Jose's PhD thesis, our research aimed at increasing the support of in-network analytics. Although several papers claim to add analytic capabilities in switches, especially to support machine learning functions, current capabilities of hardware switches are not satisfactory even with the recent dataplane programming paradigm. Native integer addition is the limited capability that exists in such hardware. However, P4 switches also include match-action tables that can be leveraged for designing lookup tables to perform floating point operations.

We proposed to add support for real-value operations on the switch. This was achieved by leveraging mathematical lookup tables for building pipelines to compute real-value functions. We developed procedures for computing basic elementary operations, keeping in mind the constraints and limitations of a programmable switch. Our prototype on Barefoot Tofino switch shows the efficiency of our system for in-network computation of different types of operations and its application for in-network logistic regression models used for classification problems and time series functions such as ARIMA for DDoS detection [17].

8.3.4 Security Analysis of Embedded Devices

Participants: Jérôme François *(contact)*, Olivier Festor, Pierre-Marie Junges.

The growth of embedded devices like IoT or networking devices makes them major targets for attackers in the Internet. They are known to face security issues because of their bad design and/or configuration.

To observe and analyze attackers' behaviors, we developed HiFipot [13], a high fidelity honeypot which is capable to mimic an IoT device by emulating its firmware with, as a priority, to attract sophisticated and/or human attackers since most of current techniques only monitor commons and automated attacks. The main challenges were to ensure the proper emulation and the obfuscation of the emulation processes from the attacker point-of-view. We were able to outperform the state-of-the-art emulation-based honeypots in regard to the number of possible emulated devices.

8.3.5 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. However, these techniques require a strong expertise to be configured properly. AutoML brings techniques to automatically find the best suitable hyper-parameters. However, the use of these conventional methods are resource intensive and lead to significant costs in terms of computation and time as they solve the configuration optimization problem. Moreover, a ML-based NIDS, once built, is only effectively applicable in a similar network context that includes the network topology, services and applications running on computers, applications or types of attacks from which the data was obtained for its initial generation.

In [6], we defined a new technique based on meta-learning. From previous experiences of auto-tuning of hyper-parameters, it learns a model capable to directly infer a configuration from the description of a new dataset where the IDS must be applied. The results demonstrate an acceptable degradation of detection accuracy while the configuration is in average 9 times faster.

8.4 Orchestration

8.4.1 Software-Defined Security for Clouds

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

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 have proposed in [3] an inter-cloud trusted third-party approach, called C3S-TTP, for supporting configuration security in cloud composite services. This third-party entity serves as an intermediary between the cloud tenant and the cloud provider, and is responsible for collecting configuration information and preventing configuration vulnerabilities before performing the migration of cloud resources. We have first described the considered architecture and its main building blocks. We have specified an extension of the TOSCA orchestration language to support the interactions amongst the trusted third party, the cloud tenant, and the cloud provider. We have formalized the assessment process performed by the trusted third party by considering vulnerability descriptions extracted from the official OVAL repository. We have developed a proof-of-concept prototype of this architecture, implemented on top of our SMT-based assessment framework. Finally, we have performed an extensive series of experiments in order to quantify the benefits and limits of our approach in comparison to a baseline solution without a trusted third party. In particular, we have shown to what extent the observability enabled by the trusted third party contributes to increase the performance of vulnerability prevention and to minimize risks related to vulnerable configurations.

We have also started to work on the design of a moving target defense strategy that couples artificial intelligence with verification techniques. We have specified the considered framework which consists in two main blocks. A learning block based on reinforcement learning algorithms automates the selection of movements according to the rewards. These rewards are calculated based on the results of a verifier block, which exploits configuration verification techniques to assess the movements chosen by the artificial intelligence. We have also mathematically formalized our solution by considering our previous modelling. The objective of our moving target defense strategy is to have an approach which makes the movements hard to predict for the attackers, while minimizing the risk of reaching vulnerable configurations in a cloud composite services. We have conducted a first serie of experiments based on a proof-of-concept prototype, in order to evaluate the performance of our solution. In that context, we have compared our approach to a baseline strategy, and taken into account the severity scores of vulnerabilities provided by a CVSS repository. The experimental results show that our strategy reduces the exposure to severe security attacks, while the overhead due to the assessment time is very limited.

8.4.2 Vulnerability Prevention in 5G Networks

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

Effective management of software updates on network equipment like firewalls or routers 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.

We have started to work in collaboration with TU Berlin (Prof. Stefan Schmid), Aalborg University (Prof. Jiří Srba) and INRIA DIANA team (Damien Saucez) on vulnerability and congestion-aware software update synthesis in 5G networks. In particular, we have investigated the synthesis of software updates in emerging virtualized and programmable networks, such as the 5G network infrastructure, aiming to ensure vulnerability avoidance and congestion freedom at any time during the update. A network configuration may be vulnerable if it contains a certain combination of software versions. Fixing such vulnerabilities requires update procedures that are aware of compatibility constraints by *e.g.* querying OVAL vulnerability descriptions. In addition, the resulting update schedule must ensure that also during the update, no vulnerability (violation of compatibility) is encountered, yet maintaining performance such as avoiding congestion. We have formalized the problem and proposed a solution that exploits formal methods and in particular mixed integer linear programming to achieve optimal solutions, taking into account both vulnerability and congestion constraints. We have exemplified our framework considering a 5G architecture, as the one described in the etsi5123 standard. We have evaluated our solution on a large range of realistic ISP topologies from the topology zoo dataset as well as on a real 5G network where we physically execute the software update sequences generated by our tool.

9 Bilateral contracts and grants with industry

9.1 Bilateral grants with industry

Numeryx Technologies (Paris, France)

Participants: Abdelkader Lahmadi *(contact)*, Wafik Zahwa.

- CIFRE PhD Wafik Zahwa is supervised by Michael Rusinowitch (INRIA Pesto team), Abdelkader Lahmadi and Mondher Ayadi (NUMERYX) on *Building Self-Driven Network Functions* [15]. Since October 2022.

Orange Lab (Issy-Les-Moulineaux and Lannion, France)

Participants: Abdelkader Lahmadi *(contact)*, Raouf Boutaba.

- CIFRE PhD (Joël Ky, supervised by Abdelkader Lahmadi, Raouf Boutaba and Bertrand Mathieu (Orange) on *Automatic characterization, classification and troubleshooting of cloud gaming applications* [1, 2]. Since October 2021.

10 Partnerships and cooperations

10.1 International initiatives

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

NetMSS

Participants: Abdelkader Lahmadi *(contact)*, Jérôme François, Enzo D'Andrea, Joël Ky.

Title: NETwork Monitoring and Service orchestration for Softwarized networks

Duration: 2022 to 2025

Coordinator: Raouf Boutaba (University of Waterloo)

Partners:

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

CyberGenAI

Participants: Isabelle Chrisment *(contact)*, Jérôme François, Omar Anser, Thibault Cholez, Nicolas Schnepf.

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

Duration: 2022 to 2024

Coordinator: Isabelle Chrisment

Partners:

- DFKI (German Research Center for Artificial Intelligence), Germany
- Osaka Metropolitan University, Japan

Inria contact: Isabelle Chrisment

Summary: Anomaly Detection can be applied on many domains like predictive maintenance, fraud prevention as well as intrusion detection with different approaches, *e.g.* using statistical tools, graphs, Machine Learning (ML), neural networks or deception technology. ML algorithms suffer from their complexity which results into highly customized techniques (centric to a use case and even a dataset). Most precisely, they suffer from their difficult configurations with many hyper-parameters to tune or also the algorithm to be chosen.

The main objective of the associate team is to make robust ML techniques when they will face new types of attacks or when deployed within new environments despite the lack of large and comprehensive datasets. In particular, we want to investigate and adapt techniques such as parameter optimization or dataset augmentation in order to enhance attack prediction.

10.2 International research visitors

10.2.1 Visits of international scientists

Other international visits to the team

Ruslan Bondaruc

Status PhD Student

Institution of origin: Universita degli Studi di Milano

Country: Italy

Dates: From July 1, 2023 until December 31, 2023

Context of the visit: Collaboration on security orchestration, in particular focused on the deployment of service compositions in the edge-cloud continuum

Mobility program/type of mobility: Erasmus+ Program

Christian Camilo Garzón

Status Master Student

Institution of origin: Universidad de Antioquia

Country: Colombia

Dates: From May 1, 2023 until October 30, 2023

Context of the visit: Collaboration on self-driven security systems in SDN and P4 programmable networks.

Mobility program/type of mobility: LUE Graduate School Program - ORION

Claudia Lanza

Status Researcher

Institution of origin: Università della Calabria

Country: Italy

Dates: From June 18, 2023 until December 15, 2023

Context of the visit: Collaboration on the semantic analysis of cyber threat intelligence data and their classification.

Mobility program/type of mobility: research stay

Satou Aurélie Kpoze

Status PhD Student

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

Country: Bénin

Dates: From February 2, 2023 until September 6, 2023

Context of the visit: Collaboration on attack mitigation in industrial control systems (SCADA).

Mobility program/type of mobility: internship

10.2.2 Visits to international teams

Research stays abroad

Nicolas Schnepf and Omar Anser

Visited institution: Osaka Metropolitan University (OMU)

Country: Japan

Dates: From November 11, 2023 until November 24, 2023

Context of the visit: Cooperation in the context of the CyberGenAI associate team

Mobility program/type of mobility: research stay in the context of the Net NSS join team in order to strengthen the collaboration with associated researchers, especially Daishi Kondo: deployment of honeypots within all partner institutions (OMU, DFKI and Inria) involved in CyberGenAI and management of real-time applications in edge networks within an 5G environment. We have also started a new axis of collaboration about the use of formal methods to facilitate the allocation of paths in optical networks with Ideki Tode.

10.3 European initiatives

10.3.1 H2020 projects

AI@EDGE

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

Title: A secure and reusable Artificial Intelligence platform for Edge computing in beyond 5G Networks

Url: AIatEDGE project on cordis.europa.eu

Duration: 2021 to 2023

Partners: 20 participants from 8 countries (please see the full consortium description)

Inria contact: Jérôme François

Coordinator: Fondazione Bruno Kessler

Summary: Artificial Intelligence has become a major innovative force and it is one of the pillars of the fourth industrial revolution. This trend has been acknowledged also by the European Commission that has already pointed out how high-performance, intelligent, and secure networks are fundamental for the development and evolution of the multi-service Next Generation Internet (NGI). While great progress has been done during the last years with respect to the accuracy and performance of AI-enabled platforms, their integration in potentially autonomous decision-making systems or even critical infrastructures requires end-to-end quality assurance.

AI@EDGE addresses the challenges harnessing the concept of "reusable, secure, and trustworthy AI for network automation". In AI@EDGE European industries, academics and innovative SMEs commit to achieve an EU-wide impact on industry-relevant aspects of the AI-for-networks and networks-for-AI paradigms in beyond 5G systems. Cooperative perception for vehicular networks, secure, multi-stakeholder AI for IIoT, aerial infrastructure inspections, and in-flight entertainment are the uses cases targeted by AI@EDGE to maximise the commercial, societal, and environmental impact.

To achieve the goal, AI@EDGE targets significant breakthroughs in two fields: (i) general-purpose frameworks for closed-loop network automation capable of supporting flexible and programmable

pipelines for the creation, utilization, and adaptation of the secure, reusable, and trustworthy AI/ML models; and (ii) converged connect-compute platform for creating and managing resilient, elastic, and secure end-to-end slices capable of supporting a diverse range of AI-enabled network applications.

In this project, we developed automated configuration methods for intrusion detectors using meta-learning and investigated data augmentation techniques for network traffic. We were particularily involved in one of the use case related to industry4.0 with 5G connectivity where we evaluated the solutions we developped.

CONCORDIA

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

Title: Cyber security cOmpeteNCe fOr Research anD InnovAtion

Duration: 2019 to 2023

Coordinator: Research Institute CODE (Munich, Germany)

Partners: 56 partners, 28 academic and 28 industrial, from 19 countries (please see the full consortium description)

Local contact: Thibault Cholez

Url: www.concordia-h2020.eu

Summary: CONCORDIA is one of the 4 pilot projects whose goal is to structure and develop a network of cybersecurity competences across Europe. CONCORDIA has a holistic research program addressing the security of devices, networks, software, systems, data and users. The solutions were integrated in 5 sector-specific pilots (Telecom, Finance, e-Health, Defence and e-Mobility), and two horizontal pilots that are European-scale federated platforms (DDoS clearing house and the Threat Intelligence platform). CONCORDIA also develops an ecosystem by providing lab infrastructures, platforms and cybersecurity courses.

On the research side, we finalized our contributions on blockchain monitoring (see details in Section 8.1.2) and cloud security automation (see details in Section 8.4.1). Regarding the education in cybersecurity, we contributed to the fourth session of a MOOC on Coursera entitled "Becoming Cybersecurity Consultant", including an interactive webinar with practical live exercises over the KYPO cyber-range. Finally, we contributed to the redaction of the last deliverables and to the final review by the European Comission.

10.3.2 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 is 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 represents 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 aims at providing concrete recommendations and solutions that would lead to the reduction of skill gaps between industry requirements and sectoral training provision and contribute to support growth, innovation and competitiveness in the field of Cybersecurity. The objective is to build a Blueprint for the Cybersecurity industry and a concrete European Cybersecurity Skills Strategy. This strategy brings together lessons learned from other initiatives including the four pilot projects, and is outlined from a holistic approach, identifying political, economical, social, technological, legal and other factors which may be affecting sector skills and training offer. These activities include 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 at least four educational curricula and relevant skills certification schemes for profiles contained in the cybersecurity skills framework.

During the third year of the project, the efforts have been mainly centered on working on the design and implementation of course contents and practical exercises related to identified cybersecurity job profiles, in particular with respect to the penetration tester and the cyber threat intelligence specialist profiles, and on the design of a blueprint for the cybersecurity sector. Project results regarding the analysis of cybersecurity education gaps in Europe were published in [4].

10.4 National initiatives

10.4.1 ANR

ANR MOSAICO

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

Title: Multi-layer Orchestration for Secured and low lAtency applICatiOns

Url: www.mosaico-project.org

Coordinator: Orange Labs

Duration: 2019 to 2023

Partners: Orange Labs, Montimage, ICD-UTT, CNRS-LORIA

Local contact: Thibault Cholez

Summary: For several years, programmability has become increasingly important in network architectures. The last trend is to finely split network function into micro-services. The expected benefits relies on an easier development and maintenance, better quality, scalability and responsiveness to new scenarios than monolithic approaches, while offering more management possibilities for operators through orchestration. As a consequence, it appears that network functions can be split in several micro-services, implemented through different means, according to the software environments and performance requirements in different topological locations. This need for

multi-level and multi-technology orchestration is even more important with the emergence of new services, such as immersive services, which exhibit very strong quality of service constraints (*i.e.* latency cannot exceed a few milliseconds). The MOSAICO project proposes to design, implement and validate a multi-layer architecture, able to control several underlying network programmability technologies (SDN, NFV, P4) to compose micro-services forming the overall network service. To reach this objective, the project will follow an experimental research methodology from the definition of the global architecture and micro-services, to the design of orchestration rules and the evaluation against the project use-case of a low latency network application.

In particular, the team is in charge of the Cloud-Gaming (CG) use-case. First, we conducted a comprehensive study to characterize this type of traffic and the capacity of modern platforms to adapt their trafic when facing bad network conditions (for instance in a cellular network environment). We designed a solution based on machine learning that is able to detect automatically cloud-gaming traffic at line rate (10Gb/s) at the edge of the network with machine learning. We proposed and implemented an hybrid architecture combining both data-plane and control-plane processing thanks to P4 and NFV components. Lastly, we improved the QoS of CG traffic by reducing the latency in case of network congestion (see details in Section 8.2.1).

ANR PRESTO

Participants: Thibault Cholez *(contact)*, Isabelle Chrisment, Jérôme François.

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 is 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. While current tools already work on encrypted streams by analyzing the meta-data only, advanced encryption tools may enrich the analysis by specific researches in the encrypted payload.

The RESIST team is in charge of the use-case addressing the problem of "Content Filtering" applied to encrypted traffic. More precisely we defined the functional and non-functional requirements to enable Content Filtering for both enterprise and home networks. ENS is in charge to define the cryptographic scheme based on KP-ABE and IMT to implement the related cryptographic primitives in a library. Finally, we developed a proof of concept to demonstrate that web contents can be exchanged between a client and a server using KP-ABE to enforce security policies with acceptable performance and without any decryption from the middle box.

10.4.2 PEPR

PEPR CyberSecurity / SuperviZ

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

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 project 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.

RESIST 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, Thibault Cholez, Olivier Festor.

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: Future networks, due to their required openness and their economic value, are prime targets for attackers. The NF-HiSec project designs new methods and tools to secure the networks of the future. More specifically, it 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 aims to protect personal data in the case of lawful interception. The fourth objective aims to model the operation of the security mechanisms of these networks, so as to ensure that the security services provided correspond to the needs of the applications which request them. The fifth objective aims to formalize the link between hardware and software layers on the one hand, and security properties, to ensure the integration of cyber mechanisms in all layers of the network.

RESIST is interested in automating and verifying the building and off-loading of chains of security functions at the edge level, in the context of networks of the future. Depending on contextual changes, such as new security threats, resource degradations and network failures, the security chains may be subject to different off-loading strategies including the transfer, merging and splitting of network functions and their rules. The approach should enable a high level of automation by formally verifying these strategies to make sure that they do not impact on the performance and the security properties of the orchestrated chains, and should take into account the knowledge and experience from the different network edges.

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: TRUSTINCLOUDS project develops solutions for the major cybersecurity challenges specific to Cloud environments, in order to ensure the confidentiality, integrity and availability of data, applications and services. 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. The project will carry out scientific actions on these two main themes, with the objective of developing new methods and tools to secure infrastructures and data. This theoretical work will lead, when relevant, to prototype implementations to prove the concept, considering the shared infrastructure SLICES of the PEPR Cloud for this purpose.

In that context, RESIST team is planning to investigate different topics related to security management, including multi-domain hardening methods for the configuration of cloud composite services, traceability and configuration audit approaches for cloud services using blockchain techniques, moving target defense methods driven by artificial intelligence for preventing attacks against cloud services, and more generally autonomous security strategies for supporting cloud composite services, in link with the activities developed in the SPIREC project (see paragraph below) also part of the PEPR Cloud.

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.

In that context, RESIST team is planning to investigate methods and techniques for monitoring hardware and software resources in Cloud/Fog/IoT infrastructures, and to address how to dynamically select monitoring attributes and their frequencies according to application needs. 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. Indeed, the increasing complexity of Cloud/Fog/IoT infrastructures, with a continuous generation of a large quantity of unstructured and heterogeneous logs at multiple levels (system, application and network), has made anomaly detection very challenging.

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

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

General chair, scientific chair

- Olivier Festor was general co-chair for IEEE/IFIP Network Operations and Management Symposium (NOMS 2023).

Member of the organizing committees

- Rémi Badonnel: IEEE/IFIP International Conference on Network and Service Management (CNSM 2023), technical program committee co-chair, IEEE/IFIP Network Operations and Management Symposium (NOMS 2023), experience track co-chair.
- Jérôme François: IEEE/IFIP Network Operations and Management Symposium (NOMS 2023), short papers and posters co-chair, Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2023), member of the steering committee.

11.1.2 Scientific events: selection

Chair of conference program committees

- Rémi Badonnel: IEEE/IFIP International Conference on Network and Service Management (CNSM 2023), technical program committee co-chair.

Member of the conference program committees

- Rémi Badonnel: IEEE/IFIP Network Operations and Management Symposium (NOMS 2023), Cyber Security in Networking Conference (CSNet 2023), IEEE/IFIP International Conference on Network and Service Management (CNSM 2023), IEEE/IFIP Network Operations and Management Symposium (NOMS 2024), IEEE Global Information Infrastructure and Networking Symposium (GIIS 2024).
- Thibault Cholez: Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication (CoRes 2023) IEEE/IFIP Network Operations and Management Symposium (NOMS 2023), IEEE Conference on Network Softwarization (NetSoft 2023), Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2023), IEEE/IFIP Network Operations and Management Symposium (NOMS 2024).
- Isabelle Chrisment: IEEE/IFIP Network Operations and Management Symposium (NOMS 2023), IEEE/IFIP International Conference on Network and Service Management (CNSM 2023), IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2023), International Workshop on Traffic Measurements for Cybersecurity (WTMC 2023), IEEE/IFIP Network Operations and Management Symposium (NOMS 2024).
- Abdelkader Lahmadi: IEEE/IFIP Network Operations and Management Symposium (NOMS 2023), Cyber Security in Networking Conference (CSNet 2023), IEEE/IFIP International Conference on Network and Service Management (CNSM 2023), IEEE/IFIP Network Operations and Management Symposium (NOMS 2024), IEEE Conference on Network Softwarization (NetSoft 2023), IEEE International Conference on Communications (ICC 2023) - Cloud Computing, Networking, and Storage Track, IEEE Conference on Standards for Communications (CSCN 2023), IEEE Global Information Infrastructure and Networking Symposium (GIIS 2024).
- Jérôme François: IEEE/IFIP Network Operations and Management Symposium (NOMS 2023), IEEE/IFIP International Conference on Network and Service Management (CNSM 2023), IEEE Conference on Network Softwarization (NetSoft 2023) (PhD symposium), IEEE/IFIP Network Operations and Management Symposium (NOMS 2024).

11.1.3 Journal

Member of the editorial boards

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

Reviewer - reviewing activities

- Laurent Andrey: Springer Journal of Network and System Management (JNSM).
- Rémi Badonnel: IEEE Transactions on Network and Service Management (TNSM), IEEE Communications Magazine (COMMAG), Springer Journal of Network and System Management (JNSM), Wiley International Journal of Network Management (IJNM).
- Isabelle Chrisment: IEEE Transactions on Network and Service Management (TNSM), IEEE Communications Magazine (COMMAG).
- 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), Springer Journal of Network and System Management (JNSM), Wiley International Journal of Network Management (IJNM).

11.1.4 Invited talks

- Matthews Jose gave a talk on the ERASMUS+ REWIRE project at RESSI (*Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*, France) in May 2023. He also gave a talk on the Cybersecurity Skills Gap at the Efvet Securing Cyber Futures: Empowering Skills for Tomorrow, Brussels, Belgium, in November 2023.
- Abdelkader Lahmadi gave a talk on "Experimental Study of Denial-of-Service Attacks on a 5G COTS Server" during the 8th Franco-Japanese Cybersecurity Workshop, Bordeaux, November 2023.

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.

11.1.6 Scientific expertise

- Rémi Badonnel is, together with Marine Minier, in charge of the coordination of teaching, research and innovation activities on cybersecurity at the University of Lorraine since November 2023.
- Rémi Badonnel serves as a reviewer for the ANR Generic Call for Proposals 2023. He participates as a member of a recruitment committee (*Comité de Sélection*) at IUT Lannion / IRISA in April 2023.
- Thibault Cholez served as a reviewer for ANRT regarding a CIFRE PhD thesis funding and was a member of a recruitment committee (*Comité de Sélection*) at Université de Toulouse for an assistant professor position in May 2023.
- 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 serves as a reviewer for ANRT and Creach Labs (PhD thesis). She is also the regional scientific coordinator for the Alliage project in the context of the CPER Grand-Est (2021-2027). In 2023, she chaired the CRCN/ISFP recruitment committee at Inria Grenoble.
- Abdelkader Lahmadi serves as a member of the section committee of TSIA (*Intelligence Artificielle et cybersécurité*) ANR specific call 2023. He also serves as a reviewer for the FRHE (*Financement de la Recherche en Hautes Écoles*, Fédération WALLONIE-BRUXELLES) call of projects and he participates as a member of a recruitment committee (*Comité de Sélection*) at École de Mines Nancy in April 2023. Abdelkader Lahmadi serves as a reviewer for the Canadian MITACS Accelerate research proposals 2023.
- Jérôme François is co-chair of NMRG (Network Management Research Group) of IRTF (Internet Research Task Force).

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".

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.
- Thibault Cholez is in charge of the organization of professional projects for the three years of TELECOM Nancy students in apprenticeship and a member of the council of TELECOM Nancy.
- Olivier Festor is the Director of *Lorraine INP* which groups all engineering schools of University of Lorraine.
- 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: 150 hours (half-delegation in CNRS) - L3, M1, M2 - Computer Networks, Network Services, Mobile applications and Internet of Things, Git - TELECOM Nancy, Université de Lorraine
- Olivier Festor: 128 hours - L3, M1, M2 - Advanced algorithmics and problem solving, Data Structures and Algorithms, Network security, network management, 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 2023 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 2023.
- MOOC *Becoming a Cyber-Security Consultant (Session 4)*, Concordia Project, Rémi Badonnel, Thibault Cholez and Lama Sleem, a new session of this course was organized over the Coursera MOOC platform in 2023.

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.
- Enzo d'Andrea, *Graph-based Network Data Representation for Machine Learning*, since October 2021, supervised by Olivier Festor and Jérôme François.
- Joël Ky, *Characterization, Classification and Diagnosis of Cloud Gaming Applications*, since October 2021, supervised by Raouf Boutaba 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.

PhD defended in 2023

- Adrien Hemmer, *Detection Methods for Security of Heterogeneous IoT Systems* [16], defended on 17th January 2023, supervised by Isabelle Chrisment and Rémi Badonnel.
- Matthews Jose, *In-network Real-value Computation on Programmable Switches* [17], defended on 20th March 2023, supervised by Olivier Festor and Jérôme François.
- Mehdi Zakroum, *Machine Learning for the Automation of Cyber-threat Monitoring and Inference* [18], defended on 11th July 2023, supervised by Isabelle Chrisment, Jérôme François and Mounif Ghogho (UIR, Rabat).
- Mohamed Oulaaffart, *Automating Security Enhancement for Cloud Services*, defended on 5th December 2023, supervised by Olivier Festor and Rémi Badonnel and Christophe Bianco.
- Philippe Graff, *Characterization, In-network Identification and Optimization of Low-latency Traffic Transport: the Case of Cloud-Gaming*, defended on 12th December 2023, supervised by Olivier Festor and Thibault Cholez.

11.2.3 Juries

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

- Karel Hynek (PhD in Computer Science from Czech Technical University, Prague, Czech Republic), *The Impact of Encrypted DNS on Network Security*, defended on 10th October 2023 – (Rémi Badonnel as reviewer).
- Hadi Yakan (PhD in Computer Science from Paris Saclay University, France), *Security of V2X Communications in 5G - 3GPP Cellular Networks*, defended on 24th November2023 – (Rémi Badonnel as examiner).
- Benjamin Marais (PhD in Mathematics from Université de Caen Normandie, France), *Améliorations des Outils de Détection de Malware par Analyse Statique grâce à des Mécanismes d'Intelligence Artificielle*, defended on 18th December 2023 – (Rémi Badonnel as reviewer).
- Zhiyuan Yao (PhD in Computer Science from Ecole Polytechnique, France), *Autonomous Service Management in the Cloud*, defended on 17th May 2023 – (Rémi Badonnel as reviewer).
- Olivier Gimenez (PhD in Computer Science, INSA Rennes, France), *Relay Attacks over the Internet: Anomaly Detection using Time Measurement*, defended on 28h February 2023 – (Isabelle Chrisment as reviewer).

- Mohammed Bouchouia (PhD in Computer Science from Institut Polytechnique de Paris , France), *Multi layered Misbehavior Detection for a connected and autonomous vehicle*, defended on 2nd June 2023 – (Isabelle Chrisment as examiner).
- Hassan Chaitou (PhD in Computer Science from Institut Polytechnique de Paris , France), *Optimization of security risk for learning on heterogeneous quality data*, defended on 25th September 2023 – (Isabelle Chrisment as president).
- Farzad Veisi Goshtasb (PhD in Computer Science from University of Strasbourg , France), *Enhancing Industrial Internet of Things through Software-Defined Networking: from building the network to flow management*, defended on 20th November 2023 – (Isabelle Chrisment as president).
- Jan Bayer (PhD in Computer Science from Université Grenoble Alpes, France), *Strengthening Domain Name Abuse Remediation: Domain Classification and Blocklist Enhancement*, defended on 21st December 2023 – (Isabelle Chrisment as reviewer).
- Fernando Kaway Carvalho Ota (PhD in Computer Science from University of Luxembourg), *Secure Architectures for Mobile Financial Applications*, defended on 27th February 27 2023 – (Thibault Cholez as reviewer).
- Fariba Ghaffari (PhD in Computer Science from Télécom SudParis), *A novel Blockchain-based Architecture for Mobile Network Operators: Beyond 5G*, defended on 13th October 2023 – (Abdelkader Lahmadi as examiner).

11.3 Popularization

- Rémi Badonnel gave two interviews respectively on ethical hacking and cyber-range platforms at Radio Campus in January and October 2023.
- Matthews Jose and Rémi Badonnel organized an infoday dedicated to the results of the ERASMUS+ REWIRE project at TELECOM Nancy in November 2023.
- Abdelkader Lahmadi gave an interview organized by Lorraine Université d'Excellence to several national and media about the SCUBA solution for managing attack paths, a technology transferred to the startup Cybi.

11.3.1 Education

- Rémi Badonnel coordinated in 2023 the organization of two Capture The Flag events on cybersecurity which took place at TELECOM Nancy, and participated to the organization of the Cyber Humanum Est cyber wargame week under the umbrella of Lorraine INP and the Defense Base of Nancy.

12 Scientific production

12.1 Publications of the year

International journals

[1] J. R. Ky, B. Mathieu, A. Lahmadi and R. Boutaba. 'ML Models for Detecting QoE Degradation in Low-Latency Applications: A Cloud-Gaming Case Study'. In: *IEEE Transactions on Network and Service Management* (11th July 2023), pp. 1–1. DOI: 10.1109/TNSM.2023.3293806. URL: https://hal.science/hal-04160235.

[2] X. Marchal, P. Graff, J. R. Ky, T. Cholez, S. Tuffin, B. Mathieu and O. Festor. 'An Analysis of Cloud Gaming Platforms Behaviour Under Synthetic Network Constraints and Real Cellular Networks Conditions'. In: *Journal of Network and Systems Management*. Special Issue on High-Precision, Predictable and Low-Latency Networking 31.2 (Jan. 2023), p. 39. DOI: 10.1007/s10922-023-09720-9. URL: https://inria.hal.science/hal-04050288.

[3] M. Oulaaffart, R. Badonnel and O. Festor. 'C3S-TTP: A Trusted Third Party for Configuration Security in TOSCA-based Cloud Services'. In: *Journal of Network and Systems Management* (2023). URL: https://hal.science/hal-04352233.

[4] S. Ricci, S. Parker, J. Jerabek, Y. Danidou, A. Chatzopoulou, R. Badonnel, I. Lendak and V. Janout. 'Understanding Cybersecurity Education Gaps in Europe'. In: *IEEE Transactions on Education* (2023). URL: https://inria.hal.science/hal-04357283.

[5] M. Zakroum, J. François, M. Ghogho and I. Chrisment. 'Self-Supervised Latent Representations of Network Flows and Application to Darknet Traffic Classification'. In: *IEEE Access* 11 (2023), pp. 90749–90765. DOI: 10.1109/ACCESS.2023.3263206. URL: https://inria.hal.science/hal-04396021.

International peer-reviewed conferences

[6] O. Anser, J. François and I. Chrisment. 'Auto-tuning of Hyper-parameters for Detecting Network Intrusions via Meta-learning'. In: *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*. NOMS 2023 - IEEE/IFIP Network Operations and Management Symposium (NOMS) - AnNet workshop. Miami, United States: IEEE, 2023, pp. 1–6. DOI: 10.1109/NOMS56928.2023.10154381. URL: https://inria.hal.science/hal-04180417.

[7] K. Baccar and A. Lahmadi. 'An Experimental Study of Denial of Service Attacks on a 5G COTS Hardware'. In: 2023 7th Cyber Security in Networking Conference (CSNet). Montreal, Canada: IEEE, 16th Oct. 2023, pp. 12–18. DOI: 10.1109/CSNet59123.2023.10339752. URL: https://inria.hal.science/hal-04364309.

[8] K. Baccar and A. Lahmadi. 'An Experimental Testbed for 5G Network Security Assessment'. In: NOMS 2023 IEEE/IFIP Network Operations and Management Symposium. Miami, United States: IEEE, 8th May 2023, pp. 1–6. DOI: 10.1109/NOMS56928.2023.10154283. URL: https://inria.hal.science/hal-04364306.

[9] E. d'Andréa, J. François, O. Festor and M. Zakroum. 'Multi-label Classification of Hosts Observed through a Darknet'. In: *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*. NOMS 2023 - IEEE/IFIP Network Operations and Management Symposium (NOMS) - Experience Session. Miami, United States: IEEE, 2023. DOI: 10.1109/NOMS56928.2023.10154356. URL: https://inria.hal.science/hal-04180419.

[10] J.-P. Eisenbarth, T. Cholez and O. Perrin. 'Avoiding the 1 TB Storage Wall: Leveraging Ethereum's DHT to Reduce Peer Storage Needs'. In: The 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI 2023). Melbourne, Australia, 10th July 2023, p. 10. DOI: 10.1145/3594556.3594625. URL: https://inria.hal.science/hal-04163897.

[11] J.-P. Eisenbarth, T. Cholez and O. Perrin. 'Valorisation de la DHT d'Ethereum pour réduire les besoins de stockage des pairs'. In: CoRes 2023 - 8èmes Rencontres Francophones sur la Conception de protocoles, l'évaluation de performances et l'expérimentation de Réseaux de communication. Cargèse (Corse), France, 22nd May 2023. URL: https://hal.science/hal-04080219.

[12] P. Graff, X. Marchal, T. Cholez, B. Mathieu and O. Festor. 'Efficient Identification of Cloud Gaming Traffic at the Edge'. In: NOMS 2023 - 36th IEEE/IFIP Network Operations and Management Symposium. Miami, United States, 2023, p. 10. DOI: 10.1109/NOMS56928.2023.10154417. URL: https://inria.hal.science/hal-04056607.

[13] P.-M. Junges, J. François and O. Festor. 'HiFiPot: a High-Fidelity Emulation Framework for Internet of Things Honeypots'. In: *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*. NOMS 2023 - IEEE/IFIP Network Operations and Management Symposium (NOMS). Miami, United States: IEEE, 2023. DOI: 10.1109/NOMS56928.2023.10154359. URL: https://inria.hal.science/hal-04180801.

[14] J. R. Ky, P. Graff, B. Mathieu and T. Cholez. 'A Hybrid P4/NFV Architecture for Cloud Gaming Traffic Detection with Unsupervised ML'. In: *IEEE ISCC 2023*. 28th IEEE Symposium on Computers and Communications (ISCC 2023). Gammarth, Tunisia: IEEE, 9th July 2023, pp. 733–738. DOI: 10.1109/ISCC58397.2023.10217863. URL: https://hal.science/hal-04130096.

[15] W. Zahwa, A. Lahmadi, M. Rusinowitch and M. Ayadi. 'Automated Placement of In-Network ACL Rules'. In: *International Conference on Network Softwarization (NetSoft)*. 2023 IEEE 9th International Conference on Network Softwarization (NetSoft). Madrid, Spain: IEEE, 19th June 2023, pp. 486–491. DOI: 10.1109/NetSoft57336.2023.10175436. URL: https://inria.hal.science/hal-04236850.

Doctoral dissertations and habilitation theses

[16] A. Hemmer. 'Detection methods for security of heterogeneous IoT systems'. Université de Lorraine, 17th Jan. 2023. URL: https://hal.univ-lorraine.fr/tel-04158359.

[17] M. Jose. 'In-network real-value computation on programmable switches'. Université de Lorraine, 20th Mar. 2023. URL: https://hal.univ-lorraine.fr/tel-04194968.

[18] M. Zakroum. 'Machine Learning for the Automation of Cyber-threat Monitoring and Inference'. Université de Lorraine; Université Internationale de Rabat, 11th July 2023. URL: https://hal.univ-lorraine.fr/tel-04320557.

Other scientific publications

[19] M. Jose, R. Badonnel, T. Cholez, H. Debar, O. Levillain and G. Blanc. *REWIRE -Cybersecurity skills alliance: a new vision for Europe*. 12th May 2023. URL: https://hal.science/hal-04165397.