RESEARCH CENTRE

Inria Nancy - Grand Est Center

IN PARTNERSHIP WITH:

Université de Lorraine, CNRS

2022

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

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

A1.3.5. – Cloud

A1.3.6. – Fog, Edge

A1.5.2. – Communicating systems

A2.6. – Infrastructure software

A3.1.1. – Modeling, representation

A3.1.3. – Distributed data

A3.1.8. – Big data (production, storage, transfer)

A3.2.2. – Knowledge extraction, cleaning

A3.2.3. – Inference

A3.3. – Data and knowledge analysis

A3.4. – Machine learning and statistics

A4.1. – Threat analysis

A4.4. – Security of equipment and software

A4.7. – Access control

A4.9. – Security supervision

Other research topics and application domains

B5. – Industry of the future

B6.2.1. – Wired technologies

B6.2.2. – Radio technology

B6.3.2. – Network protocols

B6.3.3. – Network Management

B6.4. – Internet of things

B6.5. – Information systems

B6.6. – Embedded systems

B8.2. – Connected city

B9.2.3. – Video games

1 Team members, visitors, external collaborators

Research Scientists

- Isabelle Chrisment [Team leader, Inria, on secondment from Univ. de Lorraine, HDR]
- Raouf Boutaba [INRIA, Advanced Research Position, until Jun 2022, HDR]
- Jerome François [INRIA, Researcher]
- Nicolas Schnepf [INRIA, Researcher]

Faculty Members

- Laurent Andrey [Univ. de Lorraine, Associate Professor]
- Rémi Badonnel [Univ. de Lorraine, Professor, from Sep 2022]
- Thibault Cholez [Univ. de Lorraine, Associate Professor]
- Olivier Festor [Univ. de Lorraine, Professor, from Mar 2022, HDR]
- Abdelkader Lahmadi [Univ. de Lorraine, Associate Professor]

Post-Doctoral Fellows

- Xavier Marchal [CNRS]
- Lama Sleem [Univ. de Lorraine]

PhD Students

- Omar Anser [INRIA]
- Enzo D'Andrea [INRIA]
- Jean-Philippe Eisenbarth [Univ. de Lorraine]
- Philippe Graff [CNRS]
- Adrien Hemmer [Univ. de Lorraine, ATER, until Sep 2022]
- Joel Ky [ORANGE]
- Abir Laraba [Univ. de Lorraine]
- Mohamed Oulaaffart [Univ. de Lorraine]
- Mehdi Zakroum [Univ. de Lorraine]

Technical Staff

- Karim Baccar [INRIA, Engineer, from Feb 2022]
- Matthews Jose [ORANGE LABS, Engineer, from Feb 2022]
- Alexandre Merlin [INRIA, Engineer]

Interns and Apprentices

- Mohamed Baccour [INRIA, Intern, from May 2022 until Oct 2022]
- Paul Cambon [Univ. de Lorraine, Intern, from Sep 2022]
- Katsuki Isobe [UNIV OSAKA PREFECTURE, Intern, from Aug 2022]
- Thomas Pacorel [INRIA, Intern, from Apr 2022 until Sep 2022]
- Clément Rault [INRIA, Intern, from Jun 2022 until Aug 2022]

Administrative Assistants

- Nathalie Fritz [Univ. de Lorraine]
- Isabelle Herlich [INRIA]

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 (link accessed on 08/02/2021) 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. Several experts warn about major Internet blackouts in the coming years[24, 21]. 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) [25] 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.

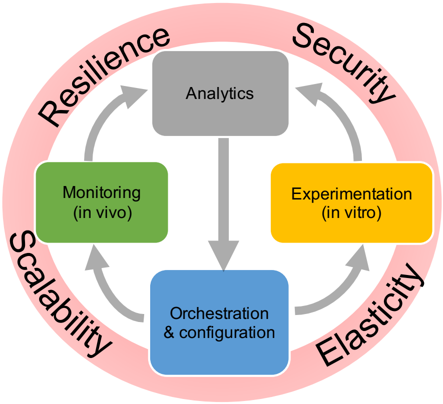

Figure 1: The Resist project

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 [23].

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 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 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 Highlights of the year

Rémi Badonnel defended his HDR (*Habilitation à diriger les recherches*) on March 9, 2022 [16]. He got a full-professor position at Télécom Nancy since september 2022.

The startup CYBI with Abdelkader Lahmadi and Jérôme François as co-founders has been created in May 2022. CYBI exploits and industrials the patented technology SCUBA [20] dedicated to the management of attack paths.

6 New software and platforms

6.1 New platforms

5G Security Assessment Platform

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

During 2022, we developed a novel platform 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). Ir 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. First prototypes of these tool are already and integrated in the platform to generate and inject them on the fly 5G packets. This platform is restricted to be used by the RESIST team.

7 New results

7.1 Monitoring

7.1.1 Programmable Network Monitoring

Participants: Jérôme François *(contact)*, Raouf Boutaba, Isabelle Chrisment, Abir Laraba.

We proposed a systematic method to map Extended Finite State Machine (EFSM) models into a P4 switch in order to embed detection of complex behaviors within the dataplane. The advantage of EFSM over the other widely used formalisms in SDN (like flow-based rules) is to be stateful and so able to track multi-step attacks.

We have further extended this work by combining our EFSM scheme with a Petri net, whose main advantage is to be easily represented and so implemented with reconfigurable match tables. As a result, an attack detector can be recomposed at run-time from a set of EFSM models which are synchronized with a Petri net. We thus proposed a method to automatically map a Petri Net into P4 abstractions which can be then compiled to a P4 programmable dataplane. Our approach has been demonstrated to be effective on sophisticated attacks, *e.g.* a DNS poisoning attack involving multiple stages. This work has been presented at IFIP/IEEE NOMS 2022 (Network Operations and Management Symposium) [11].

7.1.2 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 2022 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.

7.1.3 Monitoring and exploitation of Blockchains' Networking Infrastructure

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

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 of public P2P networks.

In 2022, we pursued our work on the Ethereum P2P network. We noticed that, on the one hand, the Ethereum P2P network based on a distributed hash table (DHT) is largely unexploited, as no data is stored in the DHT, and on the other hand, the storage of the blockchain data is only growing (which will eventually be problematic as fewer nodes will be able to afford the storage costs). We studied in a second time the data storage of the main client of Ethereum (Geth) and its way of synchronizing the state of the blockchain between the peers. We designed a new distributed storage architecture for Ethereum taking full advantage of the DHT, that is backward compatible with current clients and able to reduce the disk space used for long-term storage by 95% (58% of the total storage of a node), without impacting the guarantees or the performance of the Ethereum blockchain.

However, storing data on the DHT makes it more prone to attacks, especially to localized Sybil attacks. We therefore analyzed Ethereum peers looking for patterns that could prove that Sybil attacks are possible. More precisely, we looked for peers that: 1) are too close to each other in the DHT ID space, or 2) are from the same /24 subnetwork, or 3) share the same IP address. We showed the existence of thousands of suspicious nodes grouping many identifiers for a single IP address (up to 10.000/IP) which clearly proves that the threat of a Sybil attack on Ethereum's DHT is real.

We finally designed and implemented a protection architecture against Sybil attacks to avoid suspicious nodes to grow in number with time and conduct a large scale attack able to disrupt the Etherum blockchain. It is based on a a global monitoring system that detects suspicious nodes in real time, a Smart Contract structuring the resulting list of nodes and propagating it to all peers, and finally a fully-distributed revocation system, where each peer must check individually if the report is accurate and remove its connections to suspicious peers. The revocation is currently based on an external tool using the RPC API of the Geth client but could be later directly integrated in the main client. The deployment of all these mechanisms on Ethereum's test network has shown the effectiveness of the proposed architecture. This work was published in Springer's Journal of Network and Systems Management [3] in 2022.

7.1.4 Monitoring Internet-wide threat with a network telescope

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

We introduced a framework [5] for an improved and efficient monitoring of the probing activities targeting network telescopes. Particularly, we model the probing rates which are a good indicator for measuring the cyber-security risk targeting network services. Sequences of probing rates targeting similar ports are used as inputs to stacked Long Short-Term Memory (LSTM) neural networks to predict probing rates 1 hour and 1 day in advance. It serves to compute monitoring indicators to infer anomalous probing traffic and to raise early threat warnings.

7.2 Experimentation

7.2.1 Understanding Cloud Gaming Network Traffic and optimizing its transport

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

In the context of the ANR MOSAICO project, we selected cloud gaming (CG) as the use case to test the future low-latency network functions the project will propose. Indeed, with the recent technological evolutions in networks and increased deployment of multi-tier clouds, cloud gaming is gaining renewed interest and is expected to become a major Internet service in the upcoming years. Many companies have launched powerful platforms such as Google Stadia, Nvidia GeForce Now, Microsoft xCloud, Sony PlayStation Now among others, to attract players. However, for all end-users to fully enjoy their gaming sessions over the wide range of network access qualities, CG platforms must adapt their traffic.

In 2022, we pursued our work to characterize CG traffic and evaluate the ability of the platforms to adapt their traffic to cope with network constraints. We extended our work with new measurements on the platforms through emulated cellular network conditions and refined our analysis of the delivered QoS by platforms. This extension is accepted with minor revision in Springer Journal of Network and System Management (JNSM) and the corresponding dataset is available for the community.

To improve the delivery of such low-latency applications, new Active Queue Management architectures like L4S (Low Latency, Low Loss, Scalable Throughput) are proposed. Currently, traffic is routed to a low-latency queue only based on the presence of the ECN (Explicit Congestion Notification) bit in the IP header, but this is too restrictive and can be easily manipulated. Instead, we aim at analyzing and detecting CG traffic based on its inherent characteristics, so as to forward the packets in the low-latency queue. We designed a decision trees based ML model to efficiently detect CG traffic based on flow-level features among other high-bitrate applications transported over UDP. The evaluation proves that our model achieves good results (98.5% accuracy) and can be realistically deployed as a Virtualized Network Function at the edge, handling more than 10Gb/s of medium-sized flows on a low-end server. This work is accepted for publication as a full paper in IFIP/IEEE NOMS 2023.

Finally, we extended the cloud-gaming use case to cloud-Virtual Reality. While VR headsets are progressively popularized, they still need an expensive 3D-capable computer to render appealing virtual environments. A potential solution to further generalize VR lies in the development of cloud-VR where the rendering is performed on a distant server. However, this raises new challenges for the network that is not yet ready to transport such high-bandwidth and ultra-low latency flows. We conducted an analysis of the network traffic generated by the Air-Link protocol of a Meta Quest 2 headset. We give its characteristics and show that it is resilient to concurrent Wi-Fi traffic. We list the main challenges to enable the transport of VR flows on WAN and give promising research directions in particular in the area of network management.

7.2.2 Benchmarking of lightweight cryptographic algorithms for wireless IoT networks

Participants: Abdelkader Lahmadi *(contact)*, Lama Sleem.

Cryptographic algorithms that can provide both encryption and authentication are increasingly required in modern security architectures and protocols (e.g. TLS v1.3). Many authenticated encryption systems have been proposed in the past few years, which has resulted in several cryptanalysis research work. In this same direction, the National Institute of Standards and Technology (NIST) is coordinating a large effort to find a new standard authenticated encryption algorithm to be used by resource-constrained and limited devices.

In [2], we evaluate on a real IoT test-bed 12 algorithms of the 33 candidates of the Round 2 phase from NIST competition. We ported the 12 algorithms to different hardware platforms (an x86_64 PC, an AVR ATmega128, an MSP430F1611 and the IoT-LAB platform) and make a fair comparison between their performance. We adapted these algorithms to the Contiki operating system to evaluate the latency and efficiency of each algorithm on IoT applications deployed on a national experimental platform which is IoT-LAB.

7.3 Analytics

7.3.1 Efficient Distribution of Security Filtering Rules in SDN

Participants: Abdelkader Lahmadi *(contact)*.

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 rules updates in a fast and efficient way to avoid a security breach or to meet a service needs.

In [6], we extend our previous work on network management rules distribution by introducing an efficient update strategy. Through extensive experiments on several rule sets with single and multiple path topologies, we evaluate and analyze the performance of our strategy. The obtained results show a reduction of up to 90% in update time.

7.3.2 Characterization and troubleshooting of cloud gaming applications on mobile networks

Participants: Abdelkader Lahmadi *(contact)*, Isabelle Chrisment, Raouf Boutaba, Joël Ky.

In the context of the Joel Ky's PhD thesis, our aim is to develop novel solutions for automatically - leveraging AI techniques - characterizing, classifying and troubleshooting cloud gaming applications [19]. These Low-latency applications have soared with the rapid evolution of Internet. Current network capacities (especially time-varying capacity networks like 4G/5G networks) struggle to ensure user QoE (Quality of Experience). There is therefore a need to collect, identify and analyze metrics specific to low-latency applications in network equipment (switches, base stations, UEs...) for efficient troubleshooting of user QoE degradation purposes.

In [10] we investigate unsupervised ML approaches (PCA, OC-SVM, Isolation Forest, Auto-Encoder, LSTM-VAE) to understand their performance and their robustness. Our dataset consists of game sessions played on the public Google Stadia Cloud Gaming servers. The game sessions are played using a 4G network emulation replicating the capacity variations sampled on a commercial 4G network. We compare different models ranging from traditional approaches to deep learning and we evaluate their default performance while varying the level of contamination in their training datasets. Our experiments show that Auto-Encoder models achieve the best performance without contamination while the OC-SVM and the Isolation Forest are the most robust to data contamination.

7.3.3 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.

In previous years, we introduced a framework, InREC, to compute floating point arithmetic with P4-capable Tofino programmable switches. Our solution heavily relied on lookup-tables fiulled with pre-computed operations. This framework was extend in 2022 with NetREC [4, 9] that adds further support. In [4], our main contribution was focused on adding the support for stateful function. In [9], we first introduced a new real number fixed point representation that is aligned with switch capabilities. By doing so, exchanging real number representations among multiple switches was more convenient and efficient. It paved the way for distributed computation of sophisticated functions on multiple switches. This however requires to deal with constraints related to switch resources and packet forwarding. All of them are resolved thanks to a MILP (Mixed-integer linear programming) formulation and resolution. Besides, support for recursive or time-based functions was added.

7.3.4 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.

In order to observe attackers, we defined a new honeypot called HiFiPot. It is capable of creating a high-interaction honeypot on-the-fly with a high fidelity, *i.e.* from a firmware image. Our technique improves the most recent state-of-the-art solution to emulate an IoT device without scarifying the furtiveness. It is based on an iterative learning procedure to automatically correct emulation errors and to ensure Internet connectivity while maintaining these corrections invisible to the attackers. Out of the 1,000 firmware images tested, 443 (44,3%) can be deployed as honeypot. More than 500 instances of were deployed in the wild, and received about 1,900 HTTP traversal attacks, and downloaded 31 distinct malware binaries (out of 909) among which eight were unknown.

This work concludes the PhD thesis of P.-M. Junges [17] and is accepted for publications in IEEE/IFIP NOMS 2023.

7.3.5 Analysis of network resiliency

Participants: Nicolas Schnepf *(contact)*.

To meet their stringent requirements in terms of performance and dependability, communication networks should be “well connected”. While classic connectivity measures typically revolve around topological properties, e.g., related to cuts, these measures may not reflect well the degree to which a network is actually dependable. In [7] we introduced a more refined measure for network connectivity, the *hazard value*, which is developed to meet the needs of a real network operator. It accounts for crucial aspects affecting the dependability experienced in practice, including actual traffic patterns, distribution of failure probabilities, routing constraints, and alternatives for services with preferences therein. We analytically showed that the hazard value fulfills several fundamental desirable properties that make it suitable for comparing different network topologies with one another, and for reasoning about how to efficiently enhance the robustness of a given network. We also presented an optimised algorithm to compute the hazard value and an experimental evaluation against networks from the Internet Topology Zoo and classical datacenter topologies, such as fat trees and BCubes. This evaluation showed that the algorithm computes the hazard value within minutes for realistic networks, making it practically usable for network designers.

7.4 Orchestration

7.4.1 Vulkan for NFV

Participants: Thibault Cholez.

In the scope of the MOSAICO ANR project, we finished in 2022 a cooperation with the University of Oulu initiated with the 2020 internship in Resist of Juuso Haavisto on the design of an open NFV architecture that can easily use GPGPU processing with heterogeneous devices. In fact, recent studies have focused on integrated graphics units and various performance optimizations to address bottlenecks such as latency. However, these approaches tend to produce architecture-specific binaries and lack the orchestration of functions. A complementary effort would be a GPGPU architecture based on standard and open components, which allows the creation of interoperable and orchestrable network functions.

Our architecture is based on a combination of open and standardized technologies, namely SPIR-V, Vulkan, and Kubernetes. We described our architecture and provided design guidelines to use it. We proved its applicability with an actual use case performing traffic classification with random forest inference. This VNF was deployed successfully by Kubernetes on different GPU hardware and executed with better performance than the Cython counterpart on CPU. Our contribution is supported by a software made available for the community and the corresponding full paper was accepted for publication at IFIP/IEEE NOMS 2022 [8].

7.4.2 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.

Within the H2020 Concordia project, we have pursued investigating a security automation strategy for cloud services, with a focus on issues related to resource migration. This strategy argues in favor of exploiting service descriptions as an important knowledge source to drive security enhancement. The first pillar of this work consists in extending an orchestration language for specifying different orchestrated security levels and supporting security automation. The second pillar concerns the design of a framework with selection algorithms to determine the security mechanisms to be activated for protecting a whole cloud service during the migration of one or several of its resources.

In particular, we have proposed in [12] an automated SMT-based security framework for supporting the migration of resources in these cloud services, and preventing the occurrence of new configuration vulnerabilities. We have formalized the underlying security automation based on SMT solver, in order to assess the migrated resources and select adequate countermeasures, considering both endogenous and exogenous security mechanisms. We have then evaluated its benefits and limits through large series of experiments based on a proof-of-concept prototype implemented over the CVC4 commonly-used open-source solver[22]. These experiments show a minimal overhead with regular operating systems deployed in cloud environments. The prototype has been showcased during an international conference [13], where we have illustrated its operation through two main scenarios related to the detection of vulnerable configurations prior to resource migrations, and related to the suggestion of corrective operations for remediating them.

Furthermore, we have started to work on an inter-cloud trusted third-party approach, called C3S-TTP, for supporting such configuration security. Vulnerability prevention is challenged by the reluctance of stakeholders, namely the cloud tenant and the cloud provider, to share precise configuration information regarding respectively their cloud composite services and their cloud infrastructures, this information disclosure posing also security issues. Our third-party entity serves as an intermediate between the cloud tenant and the cloud provider, and is responsible for collecting configuration information and preventing configuration vulnerabilities before the migration of cloud resources. 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 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.

8 Bilateral contracts and grants with industry

8.1 Bilateral grants with industry

Numeryx Technologies (Paris, France)

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

- CIFRE PhD in collaboration with PESTO team (Wafik Zahwa, supervised by Michael Rusinowitch, Abdelkader Lahmadi and Mondher Ayadi) on *Building Self-Driven Network Functions*. Since October 2022.

Orange Lab (Issy-Les-Moulineaux, France)

Participants: Jérôme François *(contact)*, Olivier Festor, Matthews Jose, Joël Ky, Bertrand Mathieu *(Orange)*, Kahina Lazri *(Orange)*.

- CIFRE PhD (Joël Ky , supervised by Isabelle Chrisment, Abdelkader Lahmadi, Raouf Boutaba and Bertrand Mathieu) on *Automatic characterization, classification and troubleshooting of cloud gaming applications* [10, 19]. Since October 2021.
- CIFRE PhD (Matthews Jose, supervised by Olivier Festor, Jérôme François and Kahina Lazri) on *Complex arithmetic operation for in-network computing using hardware dataplanes* [4, 9]. Since January 2019.

9 Partnerships and cooperations

9.1 International initiatives

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

CyberGenAI

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

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

Duration: 2022 - 2024

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

Partners:

- DFKI (German Research Center for Artificial Intelligence) and Osaka Prefecture University (Japan)

Summary: Prediction techniques have gained in performance thanks to Artificial Intelligence (AI) which became the unavoidable enabler for building the new cyber-security solutions to detect, forecast and mitigate threats. On top of the methods used, ML (Machine Learning) is the widely adopted, for example for intrusion detection. While these techniques are good to recognize previously observed attacks or malicious behaviors, they suffer from their ability to generalize their knowledge with a good accuracy and anticipate new types of attacks. ML algorithms actually suffer from their complexity which results in too much tailored techniques. Most precisely, they suffer from their difficult configurations with many hyper-parameters to tune and even the algorithm to choose. Furthermore, over-fitting during the learning phase prevents the model to be robust against noisy data or generalized against new data, i.e. new type of attackers' action.

Therefore, our main objective is to make robust ML techniques when they will face new types of attacks or intrusion to detect or when deployed within new environment despite the lack of large and comprehensive datasets.

NetMSS

Participants: Jérôme François *(contact)*, Raouf Boutaba, Joël Ky, Abdelkader Lahmadi.

Title: NETwork Monitoring and Service orchestration for Softwarized networks

Duration: 2019 - 2024

Coordinator: Raouf Boutaba (rboutaba@uwaterloo.ca)

Partners:

- Team of Prof. Raouf Boutaba, David R. Cheriton School of Computer Science, University of Waterloo (Canada)

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

The focus on the associate team 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.

9.1.2 STIC/MATH/CLIMAT AmSud projects

ANGEL

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

Title: Angel: IoT e-Health Platform to Monitor and Improve Quality of Life

Program: STIC-AmSud

Duration: January 1, 2021 – December 31, 2022

Partners:

- Federal University of Ceará, Brazil
- San Agustin National University Arequipa (UNSA), Peru
- Federal University of Piauí, Brazil
- Federal University of São Paulo, Brazil
- University of Valparaíso, Chile
- Engineering School of Digital Technologies, France
- University of La Rochelle, France
- Institut Mines-Télécom - Télécom Sud-Paris (IMT-TSP), France

Summary: ANGEL aims to provide a robust Internet of Things (IoT) platform to Ambient Assisted Living, offering support to the improvement of Quality of Life (QoL), especially for persons with chronic diseases, elderly people and persons with acute diseases under medical monitoring. The idea is to use the Internet of Things (IoT) to obtain and enrich environmental data to infer QoL level, monitor health vital signs and identify atypical situations such as falls, nocturia, and the other problems related to the gait pattern. To support these health services, this project will also study data enrichment for smart health systems, infrastructure and connectivity, and, transversely, runtime testing techniques as well as data privacy and security.

- Prof. Raouf Boutaba (University of Waterloo): Inria International Chair and Professor@Lorraine

Other international visits to the team

9.2 European initiatives

9.2.1 H2020 projects

AI@EDGE

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

AIatEDGE project on cordis.europa.eu

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

Duration: From January 1, 2021 to December 31, 2023

Partners:

- Institut National de Recherche En Informatique et Automatique (INRIA), France
- Universite de Lorraine (UL), France
- Lunds Universitet, Sweden
- BETA TLC SPA, Italy
- Centro Ricerche Fiat Scpa (Centro Ricerche Fiat), Italy
- Rise Research Institutes of Sweden AB (RISE), Sweden
- Deutsches Forschungszentrum fur Kunstliche Intelligenz GMBH (DFKI), Germany
- ATOS Spain SA, Spain
- Software Radio Systems Limited (SRS), Ireland
- Ericsson AB (EAB), Sweden
- Universitat Politecnica de Catalunya (UPC), Spain
- Fondazione Bruno Kessler (FBK), Italy

- Conservatoire National des Arts et Metiers (CNAM), France
- Politecnico di Milano (POLIMI), Italy
- Universita Politecnica delle Marche (UNIVPM), Italy
- Eight Bells Ltd (Eight Bells Ltd), Cyprus
- Atos IT Solutions and Services Iberia SL (ATOS IT), Spain
- Telecom Italia SPA (TIM), Italy
- Erevnitiko Panepistiliako Institouto Systimation Epikoinonias Kai Ypologiston-Emp (Research University Institute Communication and Computer SYSTEMS), Greece
- Aerotools UAV SL, Spain
- SAFRAN Passenger Innovations Germany GMBH (SPI), Germany
- Fundacio Privada I2cat, Internet i Innovacio Digital a Catalunya (CERCA - i2CAT), Spain
- ATHONET SRL, Italy

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.

CONCORDIA

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

Title: Cyber security cOmpeteNCe fOr Research anD InnovAtion

Duration: 01/2019 - 03/2023

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 will be 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 work on blockchain monitoring 7.1.3 and cloud security automation 7.4.2. Regarding the education in cybersecurity, we contributed to the third session of a MOOC on Coursera entitled "Becoming Cybersecurity Consultant", including an interactive webinar with practical live exercises over the KYPO cyber-range. We also contributed to provide highschool teachers with contents to help them raise awareness among students on the cybersecurity threats. On another topic, we helped with the the definition of a cybersecurity skill framework. Finally, we also contributed to the integration efforts regarding an open exchange format for cyber-ranges, and pursued the organization of cyber-security events (Capture-The-Flag, Cybersecurity Hackathon) in the TELECOM Nancy premises.

ERASMUS+ REWIRE

Participants: Rémi Badonnel.

Title: Cybersecurity Skills Alliance: a new Vision for Europe

Duration: November 2020 - October 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 second year of the project, the efforts have been mainly centered on working on the elaboration of the cyber skills framework and on the design of a blueprint for the cybersecurity sector, together with an analysis of job adverts for cybersecurity skills needs evaluation, whose results were published in [14].

SPARTA

Participants: Jérôme François.

SPARTA project on cordis.europa.eu

Title: Strategic programs for advanced research and technology in Europe

Duration: From February 1, 2019 to June 30, 2022

Partners:

Partners: 45 partners. See web site for a full list.

Inria contact: Thomas Jensen

Coordinator: Commissariat à l'Energie Atomique et aux Energies Alternatives

Summary: In the domain of Cybersecurity Research and innovation, European scientists hold pioneering positions in fields such as cryptography, formal methods, or secure components. Yet this excellence on focused domains does not translate into larger-scale, system-level advantages. Too often, scattered and small teams fall short of critical mass capabilities, despite demonstrating world-class talent and results. Europe's strength is in its diversity, but that strength is only materialised if we cooperate, combine, and develop common lines of research. Given today's societal challenges, this has become more than an advantage – an urgent necessity. Various approaches are being developed to enhance collaboration at many levels. Europe's framework programs have sprung projects in cybersecurity over the past thirty years, encouraging international cooperation and funding support actions. More recently, the Cybersecurity PPP has brought together public institutions and industrial actors around common roadmaps and projects. While encouraging, these efforts have highlighted the need to break the mould, to step up investments and intensify coordination. The SPARTA proposal brings together a unique set of actors at the intersection of scientific excellence, technological innovation, and societal sciences in cybersecurity. Strongly guided by concrete and risky challenges, it will setup unique collaboration means, leading the way in building transformative capabilities and forming world-leading expertise centres. Through innovative governance, ambitious demonstration cases, and active community engagement, SPARTA aims at re-thinking the way cybersecurity research is performed in Europe across domains and expertise, from foundations to applications, in academia and industry.

9.3 National initiatives

9.3.1 ANR

ANR MOSAICO

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

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

Coordinator: Orange Labs

Duration: 12/2019-11/2023

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 we are in charge of the cloud-gaming use-case. First, we conducted a comprehensive study to characterize this type of traffic and the capacity of modern platforms to adapt their traffic 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. Lastly, we will propose new means to improve the QoS by designing an applying new dedicated network functions in the data plane to enhance low-latency services, in particular by leveraging Active Queue Management algorithms.

ANR PRESTO

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

Title: PRocessing Encrypted Streams for Traffic Oversight

Coordinator: ENS Paris (David Pointcheval)

Duration: 01/2020 - 12/2023

Partners: Institut Mines-Telecom, 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 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. Next, we will help implementing the cryptographic scheme proposed in 2022 by our partners for this use-case and validate it against realistic scenarios.

9.3.2 PEPR

PEPR 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: 07/2022 - 06/2028

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 consider 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.

9.3.3 Inria joint Labs

Inria-Orange Joint Lab

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

Title: Inria - Orange Joint Laboratory

Duration: September 2015 - August 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...

10 Dissemination

Participant: Laurent Andrey, Rémi Badonnel, Raouf Boutaba, Isabelle Chrisment, Thibault Cholez, Olivier Festor, Jérôme François, Abdelkader Lahmadi.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

General chair, scientific chair
Olivier Festor: IEEE/IFIP Network Operations and Management Symposium (NOMS 2023), General co-chair, IEEE/IFIP International Conference on Network and Service Management (CNSM 2022), Steering Committee member.

Member of the organizing committees
Rémi Badonnel: IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), experience track 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 2022), publications co-chair; Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2022), member of the steering committee;

Isabelle Chrisment: Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2022), member of the steering committee;

Abdelkader Lahmadi: IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), publicity co-chair.

10.1.2 Scientific events: selection

Member of the conference program committees
Rémi Badonnel: IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), IEEE International Conference on Cloud Computing (CLOUD 2022), IEEE Conference on Network Softwarization (NetSoft 2022), IEEE/IFIP International Conference on Network and Service Management (CNSM 2022), IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2021), IEEE International Conference on Networks of the Future (NoF 2022), IEEE International Conference on Communications (ICC 2022).

Thibault Cholez: IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), International Workshop on High-Precision, Predictable, and Low-Latency Networking (HiPNet 2022), Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2022).

Isabelle Chrisment: IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2022), ACM/IEEE International Conference on Internet of Things Design and Implementation (IoTDI 2022), IEEE/IFIP International Conference on Network and Service Management (CNSM 2022), Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication (CoRes 2022), International Workshop on Traffic Measurements for Cybersecurity (WTMC 2022).

Olivier Festor: IEEE Conference on Network Softwarization (NetSoft 2022), IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), IEEE International Conference on Networks of the Future (NoF 2022).

Jérôme François: IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), IEEE/IFIP International Conference on Network and Service Management (CNSM 2022), Conference on Innovations in Clouds, Internet and Networks (ICIN 2022), International Workshop on Network Intelligence (Networking).

Reviewer

Rémi Badonnel and Olivier Festor have received Best Reviewer Awards for their contributions to the review process of IEEE/IFIP Network Operations and Management Symposium (NOMS 2022).

10.1.3 Journal

Rémi Badonnel has been selected to serve as Editor-in-Chief for Springer Journal of Network and System Management (JNSM)from January 2023.

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), Associate Editor for Springer Journal of Network and System Management (JNSM), Lead Guest Editor for the Special Issue on Cybersecurity of IEEE Transactions on Network and Service Management (TNSM) [1].

Jérôme François: Associate Editor-in-Chief for Wiley International Journal of Network Management (IJNM).

Abdelkader Lahmadi: Associate Editor for Wiley International Journal of Network Management (IJNM) [15].

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).

Thibault Cholez: Springer Journal of Network and System Management (JNSM).

Jérôme François: IEEE Transactions on Network and Service Management (TNSM), Springer Journal of Network and System Management (JNSM).

10.1.4 Invited talks

Rémi Badonnel gave a talk on Cyberspace Security Management at University of Zurich (Switzerland) in April 2022.

Rémi Badonnel gave a talk on Security Monitoring for the Cyberspace at the DGA Workshop on Security Monitoring (SupSec) organized at Inria Rennes in September 2022.

Rémi Badonnel gave a talk on Managing Security for the Internet at the French-German Workshop organized at CISPA (Germany) in October 2022.

10.1.5 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.

Jérôme François is co-chair of NMRG (Network Management Research Group) of IRTF (Internet Research Task Force).

10.1.6 Scientific expertise

Isabelle Chrisment is a member of the AFNIC's Scientific Council. She is also a member of the SLICES-PP project's general assembly.

Olivier Festor is member of the Scientific Council of Orange. He is also member of the board of the ANR evaluation committee on "Software Science and Engineering, communication Networks and High Performance Infrastructures". He is member of the Strategic Board of the UE project CONCORDIA.

10.1.7 Research administration

Isabelle Chrisment is Deputy Scientific Director at Inria in charge of the national scientific domain “Networks, Systems ans Services, Distributed Computing”. She was also a member of the COMIPERS at Inria Nancy Grand Est.
Abdelkader Lahmadi is the scientific head of the High Security Lab of Nancy.
Thibault Cholez is part of the executive committee of the University of Lorraine’s I-site project Digitrust on cybersecurity and responsible of the axis "Protocols for Secure Networks and Network Monitoring". Digitrust Activity Report.

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

Rémi Badonnel is heading the Internet Systems and Security specialization of the 2nd and 3rd years at the TELECOM Nancy engineering school.
Thibault Cholez is in charge of the organization of professional projects for the three years of TELECOM Nancy students in apprenticeship.
Olivier Festor is the Director of *Lorraine INP* which groups all engineering schools of Université of Lorraine.
Abdelkader Lahmadi is heading the training Engineering of Digial Systems at ENSEM engineering school.
Team members are teaching the following 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** 300 hours - L3, M1, M2 - Computer Networks, Network Services, Constraint development on small Connected Objects, 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 2022 at TELECOM Nancy for students and apprentices.

- **MOOC** *Sécurité des Réseaux Informatiques (Session 3)*, FUN Project, IMT (SudParis et Saint Étienne), Inria (Jérôme François), Université de Lorraine (Isabelle Chrisment). over 6100 registered users from October to December 2022.

- **MOOC** *Becoming a Cyber-Security Consultant (Session 3)*, Concordia Project, Lama Sleem, Rémi Badonnel, and Thibault Cholez, Courses over the coursera MOOC platform, and interactive webinar with practical exercises hosted on the KYPO cyber-range, from October to December 2022.

10.2.2 Supervision

PhD in progress

- Enzo D'Andrea, *Graph-based network data representation for machine learning*, since October 2021, supervised by Olivier Festor & Jérôme François.
- Omar Anser, *Automation of attack mitigations in 5G environments*, since December 2021, supervised by Isabelle Chrisment & Jérôme François.
- Philippe Graff, *Development and orchestration of network micro-services for low-latency and secure applications*, since September 2020, supervised by Olivier Festor and Thibault Cholez.
- Adrien Hemmer, *Predictive Security Monitoring for Large-Scale Internet-of-Things*, since October 2018, supervised by Isabelle Chrisment and Rémi Badonnel.
- Matthews Jose, *Programming model for new flow-based network monitoring*, since January 2019, supervised by Olivier Festor & Jérôme François.
- Joel Ky, *Caractérisation, classification et diagnostic des applications de cloud gaming*, since October 2021, supervised by Raouf Boutaba & Abdelkader Lahmadi.
- Mohamed Oulaaffart, *Automating security enhancement for cloud services*, since January 2020, supervised by Olivier Festor & Rémi Badonnel.
- Mehdi Zakroum, *Forecasting cyberthreats from exogeneous data*, since October 2019, supervised by Isabelle Chrisment & Jérôme François.
- Wafik Zahwa, *Building Self-Driven Network Functions*, since October 2022, supervised by Michael Rusinowitch (PESTO team) & Abdelkader Lahmadi.

PhD defended in 2022

- Jean-Philippe Eisenbarth, *Securing the future blockchain-based security services*[1], Université de Lorraine, December 13, 2022, supervised by Thibault Cholez and Olivier Perrin (COAST team).
- Pierre-Marie Junges, *Internet-wide automated assessment of the exposure of the IoT devices to security risks*, Université de Lorraine, July 7, 2022, supervised by Olivier Festor and Jérôme François [17].
- Abir Laraba, *Data-Driven Intelligent Monitoring for Software-Defined Networks*, Université de Lorraine, October 12, 2022, supervised by Isabelle Chrisment, Raouf Boutaba & Jérôme François [18].

10.2.3 Juries

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

- Eder Scheid, PhD in Computer Science from University of Zurich (Switzerland). Title: An Intent-based Blockchain-agnostic Interaction Environment, April 2022 – (Rémi Badonnel as reviewer)
- Manel Smine, PhD in Computer Science from IMT Atlantique Bretagne – Pays de la Loire (France). Title: Software-defined Security for Network Function Virtualization, December 2022 – (Rémi Badonnel as reviewer)
- Laurens Van Hoye, PhD in Computer Science from Ghent University (Belgium). Title: Mitigating Potential Trust Issues in Ad Hoc Collaborations, December 2022 – (Rémi Badonnel as reviewer)
- Antoine Durey, PhD in Computer Science from Université de Lille. Title: Leveraging browser fingerprinting to strengthen web authentication, January 2022 – (Isabelle Chrisment reviewer)

[1] Not fully registred. Final document not yet available.

- Nicolas Sourbier, PhD in Computer Science from INSA Rennes COMUE Université Bretagne Loire. Title: Learning-Based Network Intrusion Detection : an Imbalanced, Constantly Evolving and Timely Problem, September 2022 – (Isabelle Chrisment as reviewer)
- Imane Taibi, PhD in Computer Science from Université Rennes 1. Title: Web-based data driven network monitoring: from performance estimation to anomaly detection. September 2022 – (Isabelle Chrisment as examiner)
- Alexandre Dey, PhD in Computer Science from Ecole Nationale Supérieure Mines-Télécom Atlantique Bretagne Pays-de-la-Loire - IMT Atlantique. Title: Datascience in support of cybersecurity operations. Adaptable, robust and explainable anomaly detection for security analysis. December 2022 – (Isabelle Chrisment as examiner)
- Arnaud Rosay, PhD in Computer Science from Le Mans Université. Title: Détection d'intrusions dans les objets connectés par des techniques d'apprentissage automatique, December 2022 – (Isabelle Chrisment as examiner)
- Zhejiayu Ma, PhD in Computer Science from Université Côte d'Azur. Title: Optimisation basée sur l'apprentissage des systèmes de streaming hybrides cdn/v2v, Decembre 2022 – (Isabelle Chrisment as examiner)
- Aïmad Berady, PhD in Computer Science from Centrale Supélec. Title: Comprendre les menaces sophistiquées, November 2022 – (Jérôme François as examiner)

Team members participated in the following Habilitation Degree committees:

- Eric Alata, HDR in Computer Science from Université de Toulouse, (France). Title: Sécurité système multi-niveaux, des architectures bas-niveaux aux approches formelles orientées langages, November 2022 – (Isabelle Chrisment as president)
- Emmanuel Lavinal, HDR in Computer Science from Université de Toulouse, (France). Title: De la configuration 'a la programmation de réseaux virtuels, December 2022 – (Olivier Festor as reviewer)

International committees:

- Ihsan Ullah, committee for Tenured Associate Professor position, University of Balochistan, Pakistan. October 2022 – (Thibault Cholez as reviewer)

10.3 Popularization

As a part of CONCORDIA's activities, Lama Sleem has contributed to write a guide on the best practices to teach cyber-security in high-school.
Thibault Cholez wrote a blog entry to popularize the team research activity on the evaluation and improvement of public blockchains' P2P networks (CONCORDIA blog entry).

11 Scientific production

11.1 Publications of the year

International journals

[1] R. Badonnel, C. Fung, S. Scott-Hayward, Q. Li, F. Valenza and C. Hesselman. 'Guest Editors Introduction: Special Section on Recent Advances in Network Security Management'. In: *IEEE Transactions on Network and Service Management* 19.3 (Sept. 2022), pp. 2251–2254. DOI: 10.1109/TNSM.2022.3202426. URL: https://hal.inria.fr/hal-03916463.

[2] S. Blanc, A. Lahmadi, K. Le Gouguec, M. Minier and L. Sleem. 'Benchmarking of lightweight cryptographic algorithms for wireless IoT networks'. In: *Wireless Networks* 28.8 (Nov. 2022), pp. 3453–3476. DOI: 10.1007/s11276-022-03046-1. URL: https://hal.inria.fr/hal-03850763.

[3] J.-P. Eisenbarth, T. Cholez and O. Perrin. 'Ethereum's Peer-to-Peer Network Monitoring and Sybil Attack Prevention'. In: *Journal of Network and Systems Management*. Special Issue on Blockchains and Distributed Ledgers in Network and Service Management 30.4 (July 2022), p. 65. DOI: 10.1007/s10922-022-09676-2. URL: https://hal.inria.fr/hal-03777454.

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

[5] M. Zakroum, J. Francois, I. Chrisment and M. Ghogho. 'Monitoring Network Telescopes and Inferring Anomalous Traffic Through the Prediction of Probing Rates'. In: *IEEE Transactions on Network and Service Management* (15th June 2022), pp. 1–1. DOI: 10.1109/TNSM.2022.3183497. URL: https://hal.inria.fr/hal-03933462.

International peer-reviewed conferences

[6] A. Abboud, R. Garcia, A. Lahmadi, M. Rusinowitch, A. Bouhoula and M. Ayadi. 'Automatically Distributing and Updating In-Network Management Rules for Software Defined Networks'. In: NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. Budapest, Hungary: IEEE, 25th Apr. 2022, pp. 1–9. DOI: 10.1109/NOMS54207.2022.9789807. URL: https://hal.inria.fr/hal-03850745.

[7] P. Cuijpers, S. Schmid, N. Schnepf and J. Srba. 'The Hazard Value: A Quantitative Network Connectivity Measure Accounting for Failures'. In: 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Baltimore, United States: IEEE, 27th June 2022, pp. 239–250. DOI: 10.1109/DSN53405.2022.00034. URL: https://hal.inria.fr/hal-03877336.

[8] J. Haavisto, T. Cholez and J. Riekki. 'Unleashing GPUs for Network Function Virtualization: an open architecture based on Vulkan and Kubernetes'. In: 35th IEEE/IFIP Network Operations and Management Symposium (NOMS 2022). Budapest, Hungary: IEEE, 25th Apr. 2022, pp. 1–8. DOI: 10.1109/NOMS54207.2022.9789822. URL: https://hal.inria.fr/hal-03793322.

[9] M. Jose, K. Lazri, J. François and O. Festor. 'NetREC: Network-wide in-network REal-value Computation'. In: IEEE NetSoft 2022 - 8th IEEE International Conference on Network Softwarization. Milan, Italy, 27th June 2022. URL: https://hal.inria.fr/hal-03794892.

[10] J. Ky, B. Mathieu, A. Lahmadi and R. Boutaba. 'Assessing Unsupervised Machine Learning solutions for Anomaly Detection in Cloud Gaming Sessions'. In: *18th International Conference on Network and Service Management (CNSM)*. 2022 18th International Conference on Network and Service Management (CNSM). Thessaloniki, Greece: IEEE, 31st Oct. 2022, pp. 367–373. DOI: 10.23919/CNSM55787.2022.9964533. URL: https://hal.science/hal-03884367.

[11] A. Laraba, J. François, I. Chrisment, S. Rahman Chowdhury and R. Boutaba. 'Detecting Multi-Step Attacks: A Modular Approach for Programmable Data Plane'. In: NOMS2022 - IEEE/IFIP Network Operations and Management Symposium. Budapest, Hungary, 25th Apr. 2022. URL: https://hal.inria.fr/hal-03689476.

[12] M. Oulaaffart, R. Badonnel and C. Bianco. 'An Automated SMT-based Security Framework for Supporting Migrations in Cloud Composite Services'. In: IEEE/IFIP Network Operations and Management Symposium. Budapest, Hungary, 25th Apr. 2022. URL: https://hal.inria.fr/hal-03886057.

[13] M. Oulaaffart, R. Badonnel and O. Festor. 'CMSec: A Vulnerability Prevention Tool for Supporting Migrations in Cloud Composite Services'. In: CloudNet 2022 - IEEE International Conference on Cloud Networking. Paris, France, 7th Nov. 2022. URL: https://hal.inria.fr/hal-03886094.

[14] S. Ricci, M. Sikora, S. Parker, I. Lendak, Y. Danidou, A. Chatzopoulou, R. Badonnel and D. Alksnys. 'Job Adverts Analyzer for Cybersecurity Skills Needs Evaluation'. In: ARES 2022: The 17th International Conference on Availability, Reliability and Security. ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security. Vienna, Austria: ACM, 23rd Aug. 2022, pp. 1–10. DOI: 10.1145/3538969.3543821. URL: https://hal.inria.fr/hal-03916470.

Edition (books, proceedings, special issue of a journal)

[15] *BRAINS 2020 special issue: Blockchain research and applications for innovative networks and services* 32.2 (2022). DOI: 10.1002/nem.2189. URL: https://hal.inria.fr/hal-03409796.

Doctoral dissertations and habilitation theses

[16] R. Badonnel. ‘Managing Security for the Cyber-Space - From Smart Monitoring to Automated Configuration’. Université de Lorraine (UL), 9th Mar. 2022. URL: https://hal.inria.fr/tel-03606329.

[17] P.-M. Junges. ‘Internet-wide automated assessment of the exposure of the IoT devices to security risks’. Université de Lorraine, 7th July 2022. URL: https://hal.univ-lorraine.fr/tel-03765581.

[18] A. Laraba. ‘Protocol Abuse Mitigation In SDN Programmable Data Planes’. Université de Lorraine, 11th Oct. 2022. URL: https://hal.univ-lorraine.fr/tel-03960197.

11.2 Other

Scientific popularization

[19] J. Ky, B. Mathieu, A. Lahmadi and R. Boutaba. ‘Characterization and troubleshooting of cloud gaming applications on mobile networks’. In: Network Traffic Measurement and Analysis Conference (TMA 2022). Enschede, Netherlands, 27th June 2022. URL: https://hal.science/hal-03878114.

Patents

[20] A. Lahmadi, J. François and F. Beck. ‘Computer-implemented method for testing the cybersecurity of a target environment’. WO2022023671A1 (France). 3rd Feb. 2022. URL: https://hal.inria.fr/hal-03902223.

11.3 Cited publications

[21] J. Aron. ‘The internet is almost full’. In: *New Scientist* 226.3022 (2015), p. 20.

[22] C. W. Barrett, C. L. Conway, M. Deters, L. Hadarean, D. Jovanovic, T. King, A. Reynolds and C. Tinelli. ‘CVC4’. In: *Proc. of the International Conference on Computer Aided Verification (CAV)*. Vol. 6806. Lecture Notes in Computer Science. Springer, 2011, pp. 171–177.

[23] T. Buchert, C. Ruiz, L. Nussbaum and O. Richard. ‘A survey of general-purpose experiment management tools for distributed systems’. In: *Future Generation Computer Systems* 45 (2015), pp. 1–12. DOI: 10.1016/j.future.2014.10.007. URL: https://hal.inria.fr/hal-01087519.

[24] D. J. Richardson. ‘Filling the Light Pipe’. In: *Science* 330.6002 (2010), pp. 327–328.

[25] C. Tankard. ‘Advanced Persistent threats and how to monitor and deter them’. In: *Network Security* 2011.8 (2011), pp. 16–19.