RESEARCH CENTRE

**Nancy - Grand Est**

**IN PARTNERSHIP WITH:**

**CNRS, Université de Lorraine**

# 2020 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: 2018 January 01*

## Keywords

### Computer sciences and digital sciences

A1.1.8. – Security of architectures

A1.1.13. – Virtualization

A1.2. – Networks

A1.3. – Distributed Systems

A1.5.2. – Communicating systems

A2.3.2. – Cyber-physical 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

B9.8. – Reproducibility

# 1 Team members, visitors, external collaborators

## Research Scientists

- Raouf Boutaba [Inria, International Chair, Advanced Research Position]
- Jérôme François [Inria, Researcher]

## Faculty Members

- Isabelle Chrisment [Team leader, Univ de Lorraine, Professor, HDR]
- Laurent Andrey [Univ de Lorraine, Associate Professor]
- Rémi Badonnel [Telecom Nancy, Associate Professor]
- Christophe Bianco [Telecom Nancy, Associate Professor]
- Thibault Cholez [Univ de Lorraine, Associate Professor]
- Olivier Festor [Univ de Lorraine, Professor, HDR]
- Abdelkader Lahmadi [Univ de Lorraine, Associate Professor]
- Lucas Nussbaum [Univ de Lorraine, Associate Professor]
- Abdulqawi Saif [Univ de Lorraine, ATER, until Aug 2020]

## Post-Doctoral Fellows

- Luke Bertot [Inria]
- Lama Sleem [Univ de Lorraine]

## PhD Students

- Ahmad Abboud [Numeryx Technologies, CIFRE]
- Pierre-Olivier Brissaud [Inria, until Apr 2020]
- Jean-Philippe Eisenbarth [Univ de Lorraine]
- Philippe Graff [CNRS, from Sep 2020]
- Adrien Hemmer [Inria]
- Matthiews Jose [Orange Labs, CIFRE]
- Pierre Marie Junges [Univ de Lorraine]
- Abir Laraba [Univ de Lorraine]
- Mingxiao Ma [CNRS]
- Mohamed Oulaaffart [Univ de Lorraine]
- Mehdi Zakroum [Univ de Lorraine]

### Technical Staff

- Mohamed Abderrahim [Inria, Engineer]
- Soline Blanc [Univ de Lorraine, Engineer]
- Antoine Chemardin [Inria, Engineer]
- Thomas Lacour [Inria, Engineer]
- Alexandre Merlin [Inria, Engineer]
- Nicolas Perrin [Inria, Engineer]

### Interns and Apprentices

- Benoit Chauvière [Univ de Lorraine, from Apr 2020 until Sep 2020]
- Mohamed Said Frikha [Univ de Lorraine, from Oct 2020]
- Remi Garcia [Inria, from Mar 2020 until Aug 2020]
- Philippe Graff [Inria, until Aug 2020]
- Alexis Gueguen [Univ de Lorraine, from Apr 2020 until Sep 2020]
- Juuso Haavisto [Univ de Lorraine, from Mar 2020 until Jul 2020]
- Ramzi Hadrich [Univ de Lorraine, from Mar 2020 until Jul 2020]
- Amine Kadi [Inria, from Jul 2020 until Sep 2020]
- Itzel Andrea Villanueva Ortega [Inria, from Jun 2020 until Jul 2020]

### Administrative Assistant

- 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 [1] which contributes to traffic opacity.

[1] http://www.arcep.fr/uploads/tx_gsavis/15-0832.pdf, accessed on 08/02/2021

### 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[30, 26]. 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) [32] 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.

**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

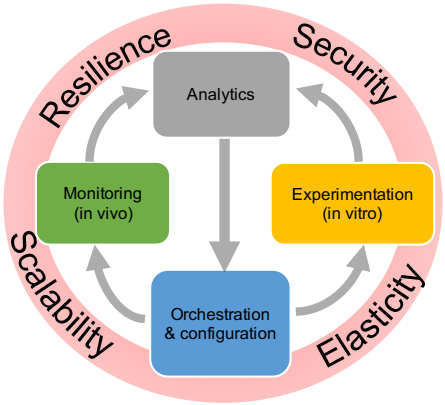


Figure 1: The Resist project

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.

We are playing a central role in the development of the Grid'5000 testbed [27] and our objective is to reinforce our collaborations with other testbeds, towards a **testbed federation** in order to enable experiments to scale to multiple testbeds, providing a diverse environment reflecting the Internet itself.

Moreover, our research focuses on extending the infrastructure virtualization capabilities of our Distem [31] emulator, which provides a flexible software-based experimental environment.

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 [29].

### 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[2] 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.

[2] https://lhs.loria.fr

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

Since January 2020, Abdelkader Lahmadi has been nominated as the scientific head of the HSL (High Security Lab) platform, hosted at LORIA and Inria Nancy Grand Est.

After years of research work in security, a startup is going to be created mid-2021. In 2020, this objective was a clear target with major actions performed including presentations of an ML-guided threat assessment PoC in industry events and to cyber-security companies. Most notably, this startup project was accepted to be in the phase of incubation (guided pre-startup creation phase) by the *Incubateur Lorrain*, which is labelled as incubator of excellence. In parallel, a patent has been filled to protect our technology and a first market study has been realized by a professional marketing company.

Although the joint team with University of Waterloo has ended last year, the collaboration was fruitful with important joint contributions at IFIP Networking [17] (core-A), IEEE Transactions on Cloud Computing [1] and an accepted article at IEEE Transactions on Network and System Management published in Janurary 2021.

# 6 New software and platforms

## 6.1 New platforms

**CPS Security Assessment Platform**

**Participants** Abdelkader Lahmadi *(contact)*, Frédéric Beck, Thomas Lacour, Jérôme François.

NEWS OF THE YEAR:

During 2020, we have extended our IoT (Internet of Things) and CPS (Cyber-Physical Systems) security assessment platform with more off-the-shelf IoT devices. The platform is used for several demonstrations and it is extensively used for the development carried on the SCUBA tool suite to automate the assessment of the security of IoT and SCADA systems by using ML/AI methods. So a major release of the SCUBA tool suite will be achieve on 2021.

# 7 New results

## 7.1 Monitoring

### 7.1.1 Adaptive monitoring of Low-Power IoT Networks

**Participants** Abdelkader Lahmadi, Laurent Andrey, Mohamed-Said Frikha *(ENSI/CRISTAL, Tunisia)*.

Low-power Internet of Things (IoT) networks are widely deployed in various environments with resource constrained devices, making their state monitoring particularly challenging. We proposed an adaptive monitoring mechanism for low-power IoT devices, by using a Reinforcement Learning (RL) method to automatically adapt the polling frequencies of the collected attributes [20]. Our goal is to minimize the number of monitoring packets while keeping accurate and timely detection of threshold crossings associated to supervised attributes. Our results show that our approach converges to optimal polling frequencies and outperforms static periodic notification-based methods by reducing the number of monitoring packets, with a percentage of correctly detected threshold crossings exceeding 80%.

### 7.1.2 Programmable Network Monitoring

**Participants** Jérôme François, Isabelle Chrisment, Abir Laraba, Raouf Boutaba, Shihab Chowdhury *(University of Waterloo)*.

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. Advantage of EFSM over widely used formalisms in SDN (like flow based rules) is to be stateful and so able to track multi-step attacks. Our mapping method can be leveraged to monitor any protocol or its misuse. We demonstrated its effectiveness against TCP protocol attacks. First, in our initial work [17], the misuse of ECN (Explicit Congestion Notification) mechanism has been considered in a simple scenario. Second, we extended this work with a more realistic setup assuming AQM (Adaptive Queue Management) and also with optimistic ACK attack. In all cases, our solution enforces a fair bandwidth share between flows even in case of non-cooperative or misbehaving flows. This extended work has been accepted for publication in IEEE TNSM Transactions on Network and Service Management in 2021.

### 7.1.3 Encrypted Traffic Analysis

**Participants** Jérôme François, Pierre-Olivier Brissaud, Isabelle Chrisment, Thibault Cholez, Olivier François, Olivier Bettan *(Thales)*.

We pursued our research on HTTP/2 traffic analysis by demonstrating the robustness of our classifier (H2Classifier), regarding its ability to be leveraged for diverse services (+3000 websites tested) and to remain performant over time (four months) assuming a regular model update [10]. The results highlight that an off-the-shelf machine-learning method to classify HTTP/2 traffic is applicable to many websites but a weekly training may be needed to keep the model accurate.

### 7.1.4 Predictive Security Monitoring for Large-Scale Internet-of-Things

**Participants** Jérôme François, Rémi Badonnel, Abdelkader Lahmadi, Isabelle Chrisment, 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 2020, we pursued our efforts on this topic by performing a comparative analysis of process mining for supporting IoT predictive security, as presented in the IEEE TNSM journal [4]. We have first formalized and integrated into our architecture four other categories of commonly-used detection methods, including elliptic envelope, support-vector machine, local outlier factor and isolation forest techniques, that serve as a support to this analysis. We have then performed extensive sets of experiments with three different industrial datasets (connected cars, industry 4.0, and robot networks), in order to comparatively evaluate our process mining solution, by considering the influence of the time splitting, the influence of the clustering techniques, and the overall detection performance according to multiple criteria. Moreover, we have tested how our approach reacts against noisy or missing data. The experiments have clearly shown the benefits of jointly using process mining and data pre-processing, in particular clustering techniques. The data pre-processing permits to identify and minimize the states characterizing the IoT-based system, so that the process mining is not facing a state explosion. As future work, we are interested in elaborating an ensemble-learning solution capable to efficiently combine different learning techniques to detect misbehaviors and potential attacks in these environments.
This work has been achieved in the context of the H2020 SecureIoT project (section 9.2.1).

### 7.1.5 Monitoring of Blockchains' Networking Infrastructure

**Participants** Thibault Cholez, Jean-Philippe Eisenbarth, Olivier Perrin.

In 2020, we built an open dataset[3] composed of snapshots of the Bitcoin network and we made a comprehensive analysis of it. During one month, we performed daily crawls on the nodes composing the network and gathered information about them. Our dataset and all related tools, more precisely the crawler and the scripts to analyze the data are also open source[4], thus making our study fully reproducible and extensible, by opposition to previous studies in the domain. We highlighted some metrics that characterize the network. Among these metrics, we analyzed a few classical ones like the size of the network, the geographical localization of peers and the churn to get fresh results, but also new ones, in particular the popularity of peers, and the inventory of software vulnerabilities that affect clients' versions and their distribution among the deployed nodes. We showed that the size of the p2p Bitcoin network is very stable. The peers composing the network are well balanced throughout the world and show little churn. But the network also exhibits more concerning properties like the fact that a significant part of the network tends to update the client version slowly, and the unbalanced popularity of peers, even among the reachable ones. The first part of these results will be presented as a poster in IFIP/IEEE IM 2021.

### 7.1.6 Quality of Experience Monitoring

**Participants** Isabelle Chrisment, Antoine Chemardin, Frédéric Beck, Lakhdar Meftah *(University of Lille)*, Romain Rouvoy *(University of Lille)*.

In 2020, we carried on our collaboration with the SPIRALS team (Inria/Université de Lille). Even though mobile crowdsourcing allows industrial and research communities to build realistic datasets, it can also be used to track participants' activity and to collect insightful reports from the user environment. Most of existing crowdsourced datasets systematically tag data samples with metadata (e.g., time and location stamps), which may lead to user privacy leaks. We proposed a software library that empowers legacy mobile crowdsourcing apps to increase user privacy without compromising the overall quality of the crowdsourced datasets. By introducing an a priori data anonymization process, we showed that our decentralized crowdsourcing approach, named Fougere, defeats state-of-the-art location-based privacy attacks with little impact on the quality of crowdsourced datasets [5]

To address indoor environments, we also used WiFi places to capture the user context in a privacy-friendly way. In particular, we defined a WiFi places recognition algorithm based on WiFi scans data and we showed how this WiFi places data can be shared between users, while preserving their privacy. This contribution has been published at the IFIP DAIS'2020 conference [19].

In the context of both ANR BottleNet (section 9.3.1) and IPL BetterNet (section 9.3.5) projects, we also continued to work on our open measurement platform for the quality of mobile Internet access (i.e., setup and manage the backend infrastructure for data collection and analysis). This platform is hosted by the High Security Laboratory [5] located at Inria Nancy Grand-Est. After consolidating our backend infrastructure and after an agreement of Inria's ethics committee (COERLE), we were able to run experimentations with real users with the help of INSEAD, a management school running a behavioral lab to provide users for various experiments. We conducted from April 2020 to July 2020 a measurement campaign involving 60 users, over a three-month period per user. Even if such campaigns were very complex to perform, we have now at our disposal a huge amount of collected data, which is valuable for our observatory.

[3] http://concordia-btc-p2p.lhs.loria.fr/index.html
[4] https://github.com/jpeisenbarth/bitnodes/tree/add_statistics
[5] https://lhs.loria.fr

## 7.2 Experimentation

### 7.2.1 Grid'5000 Design and Evolutions

**Participants** Lucas Nussbaum, Benjamin Berard *(SED)*, Luke Bertot, Alexandre Merlin, Nicolas Perrin, Patrice Ringot *(SISR LORIA)*, Teddy Valette *(SED)*.

The team was again heavily involved in the evolutions and the governance of the Grid'5000 testbed. Since the beginning of 2017, Lucas Nussbaum serves as the *directeur technique* (CTO) of Grid'5000 in charge of managing the global technical team (10 FTE). He is also a member of the *Bureau* of the GIS Grid'5000.

**The SILECS project.** It aims at creating a new infrastructure on top of the foundations of Grid'5000 and FIT[6] in order to meet the experimental research needs of the distributed computing and networking communities. In 2020, we submitted an ESR/EQUIPEX+ proposal, which unfortunately was not selected. We are exploring other solutions to fund this future flagship testbed.

**The SLICES project.** It aims at build a European-scale infrastructure (of which SILECS will be the French node). We submitted the ESFRI[7] proposal in September 2020. Also in September 2020, the SLICES-DS H2020 project started and will work on the SLICES *design study*.

**The Fed4FIRE+ project.** We made important progress on the federation of the Grid'5000 testbed (cf. section 9.2.1). We achieved full support for standard usage through the federation's tools, solving a number of challenges and drawing interesting lessons [9].

### 7.2.2 Distributing Connectivity Management in Cloud-Edge infrastructures

**Participants** Lucas Nussbaum.

In the context of David Espinel's PhD (CIFRE Orange, co-supervised with Adrien Lebre and Abdelhadi Chari), we worked on distributing connectivity management in Cloud-Edge infrastructures. In 2020, we finalized a survey on that topic [23] which was recently accepted for publication in *IEEE Communications Surveys & Tutorials*. Then, we designed DIMINET, a module able to interconnect independent networking resources in an automatized and transparent manner in the context of Edge infrastructures [11].

## 7.3 Analytics

### 7.3.1 CPS Security Analytics

**Participants** Abdelkader Lahmadi, Mingxiao Ma, Isabelle Chrisment.

With the increasing penetration of inverter-based distributed generators (DG) into low-voltage distribution micro-grid systems, it is of great importance to guarantee their safe and reliable operations. These systems leverage communication networks to implement a distributed and cooperative control structure. However, the detection of stealthy attacks with a large impact and weak detection signals on such distributed control systems is rarely studied. We addressed the problem of detecting a stealthy attack, named MaR (Measurement as Reference), that we designed in a previous work, targeting the communication network of a microgrid while an attacker modifies the voltage measurement with the

[6] https://fit-equipex.fr/
[7] https://www.esfri.eu/

reference values [18]. We collect datasets from a hardware platform modeled after a simplified microgrid and running the MaR attack performed with a Man-in-the-Middle (MitM) technique. We use the collected datasets to compare different attack detection algorithms based on multiple categories of machine learning algorithms. Our results show that the Random Forest algorithm outperforms the others to detect suspicious packets modified by a MitM attacker with an accuracy close to 97%.

#### 7.3.2 Efficient distribution of security filtering rules in SDN

**Participants** Abdelkader Lahmadi, Ahmad Abboud, Michael Rusinowitch *(Pesto team)*, Adel Bouhoula *(Numeryx)*.

Software Defined Networks administrators can specify and smoothly deploy abstract network-wide policies, and then the controller acting as a central authority implements them in the flow tables of the network switches. The rule sets of these policies are specified in the forwarding tables, which are usually accessed using very expensive and power-hungry ternary content-addressable memory (TCAM). Consequently, a given table can only contain a limited number of rules. However, various applications need large rule sets to perform filtering on diverse flows. We proposed several algorithms [7, 25] for decomposing and distributing a rule set on network switches of limited flow table size, while preserving the network policy semantics. Through experiments on several rule sets with single and multiple dimensions, we evaluate and analyse the performance of our rule placement techniques. Our results show that our proposals are efficient in practice.

#### 7.3.3 Anomaly Detection

**Participants** Jérôme François, Abdelkader Lahmadi, Rémi Badonnel, Isabelle Chrisment, Adrien Hemmer, Mohamed Abderrahim.

In [16], we demonstrated a Man-in-the-Middle (MitM) attack against Bluetooth Low Energy (BLE) devices while collecting datasets of network traffic data exchange with and without the attack. We studied the use of machine learning to detect this attack by combining unsupervised and supervised techniques. We compared two unsupervised techniques based on autoencoders (Long Short-Term Memory: LSTM, Temporal Convolutional Network: TCN) to reconstruct the model of BLE communications and detect suspicious data batches. Our results show that a TCN approach is more accurate and provides higher temporal memory effect since our datasets are of small size. We then applied a classification method based on Text-CNN technique to classify packets as normal or attack inside each suspicious batch. Our model reconstruction results show that we are able to discriminate normal and attack models with high precision and our classification method achieves high accuracy ($\approx 0.99$) and low false positive rate ($\approx 0.03$).

#### 7.3.4 Support for Programmable In-Network Analytics

**Participants** Jérôme François, Olivier Festor, Kahina Lazri *(Orange Labs)*, Matthews Jose.

In the context of the M. Jose's PhD thesis, our research aimed at increasing the support of in-network analytics. Although several papers claim for adding analytic capabilities in switch, especially to support machine learning functions, current capabilities of hardware switches are not satisfactory even with the recent dataplane programming paradigm. Although switch architectures are well tailored for performing matching and forwarding operations, they have not been designed to run computations such as arithmetic. Some works have proposed solutions for fixed point operations with all inherent limitations in terms of accuracy. Assuming the commonly accepted Reconfigurable Match Table (RMT) model, we were the first to add support for floating point arithmetic in programmable hardware switches using

P4 (accepted at IFIP/IEEE IM 2021). Native integer addition is the limited capability that exists in such hardware. However, P4 switches also include match-action tables that can be leveraged for designing lookup tables to perform floating point operations. We are the first to do so in an efficient way. The first step consisted in defining a computational pipeline using a lookup table and native operators for each elementary operation (division, log,...). In a second step, optimization techniques have been proposed to combine efficiently these elementary operations to apply a compound function. These optimizations include the analysis of function inputs and domains of operations to restrict the lookup table range to limit their size and/or improve the operation accuracy. Parallelization of operations was also necessary to reduce the number of stages in the processing pipeline which is drastically limited in real hardware. Finally, we have showcased our prototype on real hardware (Tofino) by applying different operations including a logistic regression to highlight a practical use case.

## 7.4 Orchestration

### 7.4.1 Scheduling and Offloading Mechanisms

**Participants** Jérôme François, Raouf Boutaba, Shihab Chowdhury *(University of Waterloo)*, Anthony Anthony *(University of Waterloo)*.

The simple programming model and very low-overhead I/O capabilities of emerging packet processing techniques leveraging kernel-bypass I/O and poll-mode processing are gaining significant popularity for building high performance software middleboxes (aka Virtual Network Functions (VNFs)). However, existing OS schedulers fall short in rightsizing CPU allocation to poll-mode VNFs due to the schedulers' shortcoming in capturing the actual processing cost of these VNFs. The state-of-the-art VNF schedulers proposed as an alternative to OS schedulers are intrusive, requiring the VNFs to be built with scheduler specific libraries or having carefully selected scheduling checkpoints. Unlike existing approaches, we proposed UNiS that is non-intrusive, i.e., does not require VNF modifications and treats poll-mode VNFs as black boxes. UNiS is also workflow-aware, i.e., takes Service Function Chaining (SFC) processing order into account while scheduling VNFs. Testbed experiments show that UNiS is able to achieve a throughput within 90% and 98% of that achievable using an intrusive cooperative scheduler for synthetic and real data center traffic, respectively. While this work started before 2020, it has been extended in [1]. We have considered alternative implementations of the scheduler and included additional illustrative examples. The overhead of the scheduler was also investigated deeply by evaluating the number of context switches and cache misses.

### 7.4.2 Program Encoding and Processing into IP packets.

**Participants** Jérôme François, Alexander Clemm *(Futurewei)*, Vivien Maintenant *(Telecom Nancy)*, Sébastien Tabor *(Telecom Nancy)*.

New IP/BPP (Big Packet Protocol) is a proposed protocol and framework to allow the behavior of packets and flows to be programmed from the edge by being encoded into the packet itself. New IP/BPP is very flexible and can rely on various variables or conditions. In [12], we investigated the feasibility of such kind of protocols with a platform-agnostic approach using P4. Our study reveals large gaps between these two but shows that, under reasonable assumptions, it is possible to process in-network packets based on their own programs.

### 7.4.3 Vulkan for NFV

**Participants** Thibault Cholez, Juuso Haavisto.

In the context of the MOSAICO ANR project, we wanted to design a high-performance NFV architecture that can easily use GPU processing. The use-case envisioned was to implement as a GPU-accelerated network function an existing software able to identify in real time encrypted network flows thanks to a random-forest classifier (cf section 7.1.3). We proposed to use APL (Array-processing language) as a high-level domain specific language for developers who want to write network processing algorithms that can be efficiently executed on a GPU. We rewrote the core of the random forest algorithm from the Python implementation in scikit-learn to this language. Then, we developed a first compiler to translate APL programs to the SPIR-V intermediate language for parallel computing with the aim to efficiently execute the latter on any GPU supporting the Vulkan API. Finally, we also proposed a configuration for OpenStack and the orchestrator Kubernetes to automatically deploy the network classifier program on GPUs available in the cloud. The implementation of the architecture demonstrated its soundness. The classifier is currently being rewritten to better take advantage of the high level of concurrency in GPUs and limit the bottleneck to write network packets into the VRAM.

#### 7.4.4 Software-Defined Security for Clouds

**Participants** Rémi Badonnel, Olivier Festor, Maxime Compastié, 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.

In the context of the efforts done with Orange Labs on software-defined security for clouds, we published a survey on virtualization models for supporting cloud protection in the Elsevier Journal of Computers and Security [3]. We described and compared different virtualization models, in order to establish a reference architecture of cloud infrastructures. We then analyzed the security issues related to these models from the reference architecture, by considering related vulnerabilities and attacks. Finally, we pointed out different recommendations with respect to the exploitation of these models for supporting cloud protection. Within the H2020 Concordia project, we also recently started the PhD thesis of Mohamed Oulaaffart who will investigate new security automation mechanisms for cloud composite services, with a particular focus on migration issues. The objective is to automate security enhancement for cloud services and their resources in order to maintain safe configurations when migrations occur. We consider exploiting orchestration language extensibility to enable the specification of security enhancements, according to different orchestrated security levels. We are then interested in designing a dedicated framework with specific algorithms for supporting the security of cloud services during the migration phase, by taking into account configuration changes and dependencies amongst resources. We are also considering the complementarity of endogenous and exogenous security mechanisms with that respect.

This word has been achieved in the context of the Inria-Orange joint lab (section 9.3.2) and the H2020 EU Concordia project.

# 8 Bilateral contracts and grants with industry

## 8.1 Bilateral grants with industry

- Thales (Palaiseau, France):
  - CIFRE PhD (Pierre-Olivier Brissaud, supervised by Isabelle Chrisment and Jérôme François)
  - Encrypted network traffic analysis (HTTP2 over TLS)
- Orange Labs (Issy-Les-Moulineaux, France):
  - CIFRE PhD (Matthews Jose, supervised by Olivier Festor and Jérôme François)
  - Complex arithmetic operation for in-network computing using hardware dataplanes

- Numeryx Technologies (Paris, France):
  - CIFRE PhD (Ahmad Abboud, supervised by Michael Rusinowitch, Abdelkader Lahmadi and Adel Bouhoula)
  - Compressed and Verifiable Filtering Rules in Software-defined Networking

# 9 Partnerships and cooperations

## 9.1 International initiatives

### 9.1.1 Inria associate team not involved in an IIL

**NetMSS**

**Title:** NETwork Monitoring and Service orchestration for Softwarized networks

**Duration:** 2018 - 2020

**Coordinator:** Jérôme François

**Partners:**

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

**Inria contact:** Jérôme François

**Summary:** Evolution towards softwarized networks are greatly changing the landscape in networking. In the last years, the effort was focused on how to integrate network elements in cloud-based models. This leads to the advent of network function virtualization primarily relying on regular virtualization technologies and on some advances in network programmability. Several architectural models have been thus proposed and, even if no full consensus is reached yet, they highlight the major components. Among them, monitoring and orchestration are vital elements in order to ensure a proper assessment of the network conditions (network monitoring) serving as the support for the decision when deploying services (orchestration). With softwarization of networks, these elements can benefit from a higher flexibility but the latter requires new methods to be efficiently handled. For example, monitoring softwarized network requires collecting heterogeneous information, regarding the network but also cloud resources, from many locations. Targeting such a holistic monitoring will then support better decision algorithms, to be applied in a scalable and efficient manner, taking advantage of the advanced capabilities in terms of network configuration and programmability. In addition, real-time constraints in networking are very strong due to the transient nature of network traffic and are faced with high throughputs, especially in data-center networks where softwarization primarily takes place. Therefore, the associate team promotes (1) line-rate and accurate monitoring and (2) efficient resource uses for service orchestration leveraging micro-services.

### 9.1.2 Inria international partners

**Declared Inria international partners** The team is actively involved in the international program of LUE (Lorraine Université d'Excellence):

- Prof. Raouf Boutaba (University of Waterloo): Inria International Chair and Professor@Lorraine[8]
- Abir Laraba: international PhD grant in cooperation with University of Waterloo
- Mehdi Zakroum: international PhD grant in cooperation with International University of Rabat.

[8] http://lue.univ-lorraine.fr/en/node/30

**Informal international partners** Since 2019, we have started a collaboration with Sonia Mettali from the CRISTAL Lab at the ENSI engineering school (Tunisia) on the development of reinforcement learning methods for the monitoring of IoT. The work is done in the context of the PhD of Mohamed Said Frikha, jointly co-supervised by Sonia Mettali and Abdelkader Lahmadi.

#### 9.1.3 Participation in other international programs

**ThreatPredict**

**Title:** ThreatPredict, From Global Social and Technical Big Data to Cyber Threat Forecast

**Coordinator:** Inria

**Duration:** December 2017 - December 2020

**Others Partners:** International University of Rabat (IUR), Carnegie Mellon University

**Funding:** North Atlantic Treaty Organization

**Summary:** Predicting attacks can help to prevent them or at least reduce their impact. Nowadays, existing attack prediction methods make accurate predictions only hours in advance or cannot predict geo-politically motivated attacks. ThreatPredict aims to predict different attack types days in advance. It develops machine-learning algorithms that capture the spatio-temporal dynamics of cyber-attacks and global social, geo-political and technical events. Various sources of information are collected, enriched and correlated such as honeypot data, darknet, GDELT, Twitter, and vulnerability databases. In addition to warning about attacks, this project will improve our understanding of the effect of global events on cyber-security.

### 9.2 European initiatives

#### 9.2.1 FP7 & H2020 Projects

**Fed4Fire+**

**Title:** Federation for FIRE Plus

**Program:** H2020

**Duration:** January 2017 - December 2021

**Coordinator:** Interuniversitair Micro-Electronica centrum Imec VZW

**Url:** https://www.fed4fire.eu

**Partners:** 20 Partners (please see https://www.fed4fire.eu/the-consortium/)

**Inria contact:** David Margery (for RESIST: Lucas Nussbaum)

**Summary:** Fed4FIRE+ is a successor project to Fed4FIRE. In Fed4FIRE+, we more directly integrate Grid'5000 into the wider eco-system of experimental platforms in Europe and beyond using results we developped in Fed4FIRE. We will also provide a generalized proxy mechanism to allow users with Fed4FIRE identities to interact with services giving access to different testbeds but not designed to support Fed4FIRE identities. Finally, we will work on orchestration of experiments in a federation context.

**SecureIoT**

**Title:** Predictive Security for IoT Platforms and Networks of Smart Objects

**Duration:** December 2017 - December 2020

**Coordinator:** INTRASOFT International SA

**Partners:**

- Fujitsu Technology Solutions GMBH
- Atos Spain S.A
- Siemens SRL
- Singularlogic S.A.
- Automotive Technology SA
- P@SSPORT Holland B.V.
- UBITECH LIMITED
- Sprint Sprl;
- Germany Rechtsanwaltsgesellschaft mbH
- LuxAI S.A.
- Institut National de Recherche en Informatique et automatique
- OWL Clustermanagement GmbH
- Research and Education Laboratory in Information Technologies – Athens Information Technology (AIT)

**Inria contact:** Jérôme François

**Url:** http://secureiot.eu

**Summary:** SecureIoT is a a joint effort of global leaders in IoT services and IoT cybersecurity to secure the next generation of dynamic, decentralized IoT systems, that span multiple IoT platforms and networks of smart objects, through implementing a range of predictive IoT security services. SecureIoT will integrate its security services in three different application scenarios in the areas of digital automation in manufacturing (industry 4.0), socially assistive robots for coaching and healthcare and connected cars and autonomous driving.

Emerging cross-platform interactions and interactions across networks of smart objects require more dynamic, scalable, decentralized and intelligent IoT security mechanisms. Such mechanisms are highly demanded by the industry in order to secure a whole new range of IoT applications that transcend the boundaries of multiple IoT platforms, while involving autonomous interactions between intelligent CPS systems and networks of smart objects. In this direction, the main objectives of the project are to predict and anticipate the behavior of IoT systems, facilitate compliance to security and privacy regulations and provide APIs and tools for trustworthy IoT solutions.

**SPARTA**

**Title:** Special projects for advanced research and technology in Europe

**Duration:** February 2019 - January 2022

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

**Partners:** see web site

**Inria contact:** Jérôme François

**Url:** http://www.sparta.eu/

**Summary:** Cybersecurity is an urgent and major societal challenge. In correlation with the digitization of our societies, cyberthreats are having an increasing impact on our lives: it is essential to ensure digital security and strategic autonomy of the EU by strengthening its cybersecurity capacities. This challenge requires the coordination of Europe's best competences, along with strong international cooperations, towards common research and innovation goals.

SPARTA is a novel cybersecurity competence network, with the objective to collaboratively develop and implement top-tier research and innovation actions. Strongly guided by concrete challenges forming an ambitious Cybersecurity Research & Innovation Roadmap, SPARTA tackles hard innovation challenges, leading the way in building transformative capabilities and forming a worldleading cybersecurity competence network across the EU. Four initial research and innovation programs push the boundaries to deliver advanced solutions to cover emerging issues, with applications from basic human needs to economic activities, technologies, and sovereignty.

**CONCORDIA**

**Acronym:** CONCORDIA

**Title:** Cyber security cOmpeteNCe fOr Research anD InnovAtion

**Program:** H2020

**Duration:** January 2019 - January 2022

**Coordinator:** Research Institute CODE (Munich, Germany)

**Partners:** 52 partners, 26 academic and 26 industrial, from 19 countries (please see https://www.concordia-h2020.eu/consortium)

**Inria contact:** Thibault Cholez

**Url:** https://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 research program to develop next-generation cybersecurity solutions by taking a holistic end-to-end data-driven approach from data acquisition, data transport and data usage, and addressing device-centric, network-centric, software-centric, system-centric, data-centric and user-centric security. The solutions will be integrated in sector-specific (vertical) and cross-sector (horizontal) industrial pilots with building incubators. Vertical pilots include Telecom, Finance, e-Health, Defence and e-Mobility, while horizontal pilots are about two European-scale federated platforms that are the DDoS clearing house and the Threat Intelligence platform. CONCORDIA also develops a CONCORDIA ecosystem by providing lab infrastructures, platforms, tools as "Living Labs" as well as advanced cybersecurity courses on cyber-ranges.

The team is mainly involved in three tasks (research, education and European dimension). On the research side, we work on blockchain monitoring 7.1.5 and cloud security automation 7.4.4. Regarding the education in cybersecurity, we contributed to the creation of a MOOC on Coursera entitled "Becoming Cybersecurity Consultant" whose first session will be launched in Q2 2021. We also participated in the "Teach the teachers" activity by launching a survey on the cybersecurity awareness of European high-school students. Finally, we pursue the development of content for the cyberrange of TELECOM Nancy.

### 9.2.2 Collaborations in European programs, except FP7 and H2020

**ERASMUS+ REWIRE**

**Acronym:** REWIRE

**Title:** Cybersecurity Skills Alliance: a new Vision for Europe

**Program:** ERASMUS+

**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

**Inria 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 will bring together lessons learned from other initiatives including the four pilot projects, and will be 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 will 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.

## 9.3 National initiatives

### 9.3.1 ANR

**ANR BottleNet**

**Participants** Isabelle Chrisment *(contact)*, Antoine Chemardin, Thibault Cholez.

**Acronym:** BottleNet

**Title:** Understanding and Diagnosing End-to-End Communication Bottlenecks of the Internet

**Coordinator:** Inria

**Duration:** October 2015 - extended to September 2020

**Partners:** Inria Muse, Inria Diana, Lille1 University, Telecom Sud-Paris, Orange, IP-Label.

**Summary** : The Quality of Experience (QoE) when accessing the Internet, on which more and more human activities depend on, is a key factor for today's society. The complexity of Internet services and of users' local connectivity has grown dramatically in the last years with the proliferation of proxies and caches at the core and access technologies at the edge (home wireless and 3G/4G access), making it difficult to diagnose the root causes of performance bottlenecks. The objective of BottleNet is to deliver methods, algorithms, and software systems to measure end-to-end Internet QoE and to diagnose the cause of the experienced issues. The result can then be used by users, network and service operators or regulators to improve the QoE.

**ANR FLIRT**

**Participants** Rémi Badonnel *(contact)*, Olivier Festor, Thibault Cholez, Jérôme François, Abdelkader Lahmadi, Laurent Andrey.

**Acronym:** FLIRT

**Title:** Formations Libres et Innovantes Réseaux et Télécoms

**Coordinator:** Institut Mines-Télécom (Pierre Rolin)

**Duration:** January 2016-Décembre 2020

**Partners:** TELECOM Nancy, Institut Mines-Télécom, Airbus, Orange, the MOOC Agency, Isograd

**Url:** http://flirtmooc.wixsite.com/flirt-mooc-telecom

**Summary:** FLIRT (Formations Libres et Innovantes Réseaux & Télécom) is an applied research project led by Institut Mines-Télécom which includes 14 academic partners (engineering schools including Telecom Nancy), industrial partners (Airbus, Orange) and innovative startups (the MOOC agency, and Isograd). The project has resulted in a collection of 10 MOOCs (Massive Open Online Courses) in the area of networks and telecommunications, three training programmes based on this collection, as well as several innovations related to pedagogical efficiency (such as virtualization of practical labs, management of student cohorts, and adaptative assessment). The RESIST team has led a working group dedicated to the building and operation of a MOOC on network and service management. This MOOC covers the fundamental concepts, architectures and protocols of the domain, as well as their evolution in the context of future Internet (e.g. network programming, flow monitoring). It has been operated so far during three sessions on the FUN MOOC plateform, and has also been made available to other curriculums in the context of the covid-19 pandemic.

**ANR MOSAICO**

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

**Acronym:** MOSAICO

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

**Coordinator:** Orange Labs

**Start:** 01/12/2019

**Duration:** 4 years

**Partners:** Orange Labs, Montimage, ICD-UTT

**Summary:** For several years, programmability has become increasingly important in network architectures. The last trend is to finely split services 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 possibilities for operators and management facilities through orchestration. As a consequence, it appears that network functions, such as routing, filtering, etc. can be split in several micro-services, implemented through different means, according to the software environments, and at different topological locations, thus opening the way to fully end-to-end programmable networks. 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), while preserving end-to-end security. The MOSAICO project proposes to design, implement and validate a global and multi-layer orchestration solution, 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 in several steps including the definition of the micro-services and of the global architecture, some synthetic benchmarking, the design of orchestration rules and the evaluation against the project use-case of a low latency network application.

**ANR PRESTO**

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

**Acronym:** PRESTO

**Title:** PRocessing Encrypted Streams for Traffic Oversight

**Coordinator:** ENS Paris (David Pointcheval)

**Duration:** 01/2020 - 12/2023

**Partners:** Institut Mines-Telecom, Orange Labs, 6cure

**Summary:** While GDPR (General Data Protection Regulation) imposes some privacy constraints, growing threats against 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 kick-off of the project took place in Paris the 27/01/2020. This year we were the main editor of the first deliverable "D1.1: Description of the use cases" which was submitted in December. In particular, we defined the functional and non-functional requirements of the use-case "Content Filtering" and we refined it for enterprise and home networks.

### 9.3.2 Inria joint Labs

**Inria-Orange Joint Lab**

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

**Acronym:** IOLab

**Title:** Inria - Orange Joint Laboratory

**Duration:** September 2015 - August 2020

**Summary:** The challenges addressed by the Inria-Orange joint laboratory relate to the virtualization of communication networks, the convergence between cloud computing and communication networks, and the underlying software-defined infrastructures. Our work concerns in particular monitoring methods for software-defined infrastructures, and management strategies for supporting software-defined security in multi-tenant cloud environments.

#### 9.3.3 Technological Development Action (ADT)

**ADT SCUBA**

**Participants** Abdelkader Lahmadi *(Contact)*, Jérôme François, Thomas Lacour, Frédéric Beck.

**Acronym:** SCUBA

**Duration:** January 2018-January 2020

**Summary:** The goal of this ADT was to develop a tool suite to evaluate the security of industrial and general public IoT devices in their exploitation environment. The Tool suite relies on a set of security probes to collect information through passive and active scanning of a running IoT device in its exploitation environment to build its Security Knowledge Base (SKB). The knowledge base contains all relevant information of the device regarding its network communications, the enumeration of its used hardware and software, the list of its known vulnerabilities in the CVE format associated to their Common Weakness Enumeration (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC) descriptions. The collected information is used to evaluate the devices associated with their usage scenarios and to identify intrusion chains in an automated way.

#### 9.3.4 FUI

**FUI PACLIDO**

**Participants** Abdelkader Lahmadi *(contact)*, Mingxiao Ma, Isabelle Chrisment, Jérôme François.

**Acronym:** PACLIDO

**Title:** Lightweight Cryptography Protocols and Algorithms for IoT (Protocoles et Algorithmes Cryptographiques Légers pour l'Internet des Objets)

**Coordinator:** ADS (Airbus Defence and Space)

**Duration:** September 2017- August 2020

**Partners:** Sophia Conseil, Université de Limoges, Cea tech, Trusted Objects, Rtone, Saint Quentin En Yvelines.

**Summary:** The goal of PACLIDO was to propose and develop lightweight cryptography protocols and algorithms to secure IoT communications between devices and servers. The implemented algorithms and protocols have been evaluated in multiple use cases including smart home and smart city applications.

#### 9.3.5 Inria Project Lab

**IPL BetterNet**

**Participants** Isabelle Chrisment *(contact)*, Antoine Chemardin, Frederic Beck, Thibault Cholez.

**Acronym:** BetterNet

**Coordinator:** RESIST (Isabelle Chrisment)

**Duration:** October 2016-August 2020

**Partners:** Inria MiMove, Inria Diana, Inria Spirals, Inria Dionysos, ENS-ERST and IP-Label

**Url:** https://project.inria.fr/betternet

**Summary:** BetterNet's goal was to build and deliver a scientific and technical collaborative observatory to measure and improve the Internet service access as perceived by users. We have proposed new user-centered measurement methods, which associate social sciences to better understand Internet usage and the quality of services and networks. Tools, models and algorithms have been provided to collect data.

.

# 10 Dissemination

## 10.1 Promoting scientific activities

### 10.1.1 Scientific events: organisation

**General Chair, Scientific Chair:**
Isabelle Chrisment: IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2020), general chair.
Thibault Cholez: IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2020), general co-chair.
Olivier Festor: IEEE International Symposium on Integrated Network Management (IM 2021), general co-chair and member of the NOMS/IM Conferences Steering Committee (NISC).

**Member of the Organizing Committees:**
Laurent Andrey: IEEE International Symposium on Integrated Network Management (IM 2021), web chair.
Rémi Badonnel: IFIP IFIP International Conference on Networking (Networking 2020); IEEE/IFIP Network Operations and Management Symposium (NOMS 2020); IEEE International Symposium on Integrated Network Management (IM 2021); IEEE/IFIP International Conference on Network and Service Management (CNSM 2021).
Isabelle Chrisment: Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2020), member of the steering committee; IEEE International Symposium on Integrated Network Management (IM 2021), tutorial co-chair.
Olivier Festor: IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), tutorial co-chair
Abdelkader Lahmadi: IEEE International Conference on Cloud Networking (CloudNet 2020) keynote co-chair
Jérôme François: IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), publication co-chair; IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2020), member of the steering committee; Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2020), member of the steering committee.

### 10.1.2 Scientific events: selection

**Chair of Conference Program Committees:**
Rémi Badonnel: IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), experience program committee co-chair; IEEE International Symposium on Integrated Network Management (IM 2021), experience program committee co-chair.
Abdelkader Lahmadi: Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2020), program committee co-chair; IEEE International Conference on Mobility, Sensing and Networking (MSN 2020) track co-chair
IFIP IFIP International Conference on Networking (Networking 2020), demo track co-chair.

**Member of the conference program committees**
Laurent Andrey: IEEE Conference on Network Softwarization (NetSoft 2021).
Rémi Badonnel: IEEE International Conference on Communications (ICC 2020), IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), IEEE International Conference on Networks of the Future (NoF 2020), IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2020), IEEE Conference on Network Softwarization (NetSoft 2020), IEEE Conference on Cloud and Internet of Things (CIoT 2020), Cyber Security in Networking Conference (CSNet 2020), IEEE International Symposium on Integrated Network Management (IM 2021), IEEE/IFIP International Conference on Network and Service Management (CNSM 2021), IEEE/IFIP International Workshop on Internet of Things Management (Manage-IoT 2021).
Thibault Cholez: IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2020), Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2020), IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), IEEE International Symposium on Integrated Network Management (IM 2021), IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2020), IEEE International Conference on Cloud Networking (CloudNet 2020).
Isabelle Chrisment: IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2020), IFIP Network Traffic Measurement and Analysis Conference (TMA 2020), ACM/IEEE International Conference on Internet of Things Design and Implementation (IoTDI 2020), IEEE/IFIP International Conference on Network and Service Management (CNSM 2020), Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication (CoRes 2020), IEEE International Symposium on Integrated Network Management (IM 2021).
Olivier Festor: IEEE/IFIP Network Operations and Management Symposium (NOMS 2020),IEEE/IFIP International Conference on Network and Service Management (CNSM 2020),IEEE Conference on Network Softwarization (NetSoft 2020), IEEE International Conference on Networks of the Future (NoF 2020)
Abdelkader Lahmadi: IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2020), Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2020), IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), IEEE International Symposium on Integrated Network Management (IM 2021), IEEE/IFIP International Conference on Network and Service Management (CNSM 2021), IEEE Conference on Network Softwarization (NetSoft 2020), Cyber Security in Networking Conference (CSNet 2020), IEEE/IFIP International Workshop on Internet of Things Management (Manage-IoT 2021).
Lucas Nussbaum: CloudCom 2020, WETICE 2020, CNERT 2021, WOSC 20, ICC 2020, CSNet 2020, MSR Mining Challenge 2020, OSS 2021.
Jérôme François: IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), IEEE Conference on Network Softwarization (NetSoft 2020), IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2020) Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2020), Conference on Innovations in Clouds, Internet and Networks (ICIN 2020), Cyber Security in Networking Conference (CSNet 2020), IEEE International Conference on Communications (ICC 2020), International Workshop on Network Intelligence (INFOCOM) (NI 2020)

### 10.1.3 Journal

**Member of the editorial boards**
Rémi Badonnel: Associate Editor for Wiley International Journal of Network Management (IJNM), Associate Editor for the Springer Journal of Network and System Management (JNSM), Associate Editor for the IEEE Transactions on Network and Service Management (TNSM), Lead Guest Editor for the Special Issue on Cybersecurity of the IEEE Transactions on Network and Service Management (TNSM).
Isabelle Chrisment: Associate Editor for Wiley International Journal of Network Management (IJNM)
Abdelkader Lahmadi: Associate Editor for Wiley International Journal of Network Management (IJNM), Guest Editor for a Special Issue on Intelligent and Trustworthy Internet Edge of the Springer Journal of Network and System Management (JNSM)
Jérôme François: Associate Editor-in-Chief for IJNM

**Reviewer - reviewing activities**
Laurent Andrey: IEEE Transactions on Network and Service Management (TNSM), Springer Journal of Network and System Management (JNSM) and Wiley International Journal of Network Management (IJNM).
Rémi Badonnel: IEEE Transactions on Network and Service Management (TNSM), Springer Journal of Network and System Management (JNSM), IEEE Communications Magazine (COMMAG), Wiley International Journal of Network Management (IJNM) and Elsevier Journal of Industrial Information Integration (JIII).
Thibault Cholez: IEEE Transactions on Network and Service Management (TNSM), Wiley International Journal of Network Management (IJNM), Elsevier Journal on Computer Networks (COMNET), Elsevier Journal on Computers & Security (COSE)and IEEE/ACM Transactions on Networking (ToN).
Isabelle Chrisment: IEEE Transactions on Network and Service Management (TNSM) and Elsevier Pervasive and Mobile Computing (PMC).
Lucas Nussbaum: SIGCOMM CCR.
Abdelkader Lahmadi: IEEE Transactions on Network and Service Management (TNSM), Springer Journal of Network and System Management (JNSM), IEEE Communications Magazine (COMMAG), Wiley International Journal of Network Management (IJNM)
Jérôme François: IEEE Transactions on Network and Service Management (TNSM), Springer Journal of Network and System Management (JNSM), Wiley International Journal of Network Management (IJNM).

#### 10.1.4 Invited talks

Olivier Festor gave a keynote at IEEE/IFIP NOMS'2020 entitled: Micro-Servicing NDN and its value for improved security, scalability and integration, April 2020.

#### 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.
Isabelle Chrisment served as a co-chair of the Allistene cybersecurity working group, whose main goal is to help drive the French cybersecurity. research and innovation.
Jérôme François is co-chair of NMRG (Network Management Research Group) of IRTF (Internet Research Task Force).

#### 10.1.6 Scientific expertise

Isabelle Chrisment was as a member of the GDR RSD/ASF selection committee for the thesis award. She is also a member of the AFNIC's Scientific Council. She also served as a reviewer for the Luxembourg National Research Fund.
Jérôme François serves as a reviewer for PhD grant of Région Aquitaine and is in the advisory board of the Interreg TERMINAL project (2019-2021).
Olivier Festor is member of the Scientific Council of Orange. In 2020, he was also President of the HCERES evaluation committee of the CITI/Insa de Lyon lab as well as member of the evaluation committee of the CNAM lab project on global security.

#### 10.1.7 Research administration

Thibault Cholez is a member of the executive council of the Digitrust project (I-Site project of the Université de Lorraine to foster research on trust and security in IT).
Isabelle Chrisment is an elected member of the scientific pole AM2I (Automatique, Mathématiques, Informatique et leurs Interaction) at Université de Lorraine. She is also a member of the COMIPERS at Inria Nancy Grand Est.
Lucas Nussbaum is an elected member of the LORIA laboratory council at Université de Lorraine.
Abdelkader Lahmadi is the scientific head of the High Security Lab.

## 10.2 Teaching - Supervision - Juries

### 10.2.1 Teaching

Olivier Festor is the Director of the TELECOM Nancy Engineering School.
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.
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** 290 hours - L3, M1, M2 - Computer Networks, Object-Oriented Programming, Network Services, Constraint development on small Connected Objects, Mobile applications and Internet of Things, IT tools for Project Management - TELECOM Nancy, Université de Lorraine
- **Isabelle Chrisment** 220 hours -L3, M1, M2 -C and Shell Programming, Computer Networking, Operating Systems, Network Security. - TELECOM Nancy, Université de Lorraine
- **Jérôme François** 70 hours - M1, M2 - Network security, network management, big data - 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
- **Abdelkader Lahmadi** 280 hours - L3, M1, M2 - Real time and Embedded Systems Programming, Distributed Systems and Algorithms, Green IT, Algorithms and Advanced Programming, Security of Cyber Physical Systems - ENSEM Engineering School, Université de Lorraine
- **Lucas Nussbaum** 200 hours - L2, Licence Pro (L3), M1 - several courses about systems administration, monitoring, virtualization, configuration management, networking, operating systems. - IUT Nancy-Charlemagne

#### E-learning

- **MOOC** *Supervision de Réseaux et Services (Session 2)*, FUN Project, Université de Lorraine, Ingénieur, formation initiale et continue, Thibault Cholez, Rémi Badonnel, Laurent Andrey, Olivier Festor, Abdelkader Lahmadi, Jérôme François, January-March 2020, over 6000 from 77 countries, and 347 certificates of achievement. The third session of this MOOC has been extended to August 2020 (as an open archive) in the context of the Covid-19 pandemic situation.
- **MOOC** *Sécurité des Réseaux Informatiques (Session 1)*, FUN Project, IMT, Inria (Jérôme François), Université de Lorraine (Isabelle Chrisment). 11000 registered users from October to December 2020 and 342 certificates of achievement.

### 10.2.2 Supervision

- PhD in progress: Ahmad Abboud, *Compressed and verifiable filtering rules in Software-defined Networking*, since September 2018, supervised by Michael Rusinowitch, Abdelkader Lahmadi, and Adel Bouhoula.
- PhD in progress: Jean-Philippe Eisenbarth, *Securing the future blockchain-based security services*, since May 2019, supervised by Thibault Cholez and Olivier Perrin (Coast team).

- PhD in progress: David Espinel, *SDN solution for Massively Distributed Cloud Infrastructure*, since February 2018, supervised by Lucas Nussbaum, Adrien Lebre and Abdelhadi Chari.
- PhD in progress: Philippe Graff, *Development and orchestration of network micro-services for low-latency and secure applications*, since September 2020, supervised by Thibault Cholez and Olivier Festor.
- PhD in progress: Adrien Hemmer, *Predictive Security Monitoring for Large-Scale Internet-of-Things*, since October 2018, supervised by Isabelle Chrisment and Rémi Badonnel.
- PhD in progress: Matthews Jose, *Programming model for new flow-based network monitoring*, since January 2019, supervised by Olivier Festor & Jérôme François.
- PhD in progress: Pierre-Marie Junges, *Internet-wide automated assessment of the exposure of the IoT devices to security risks*, since October 2018 supervised by Olivier Festor and Jérôme François.
- PhD in progress: Abir Laraba, *Data-Driven Intelligent Monitoring for Software-Defined Networks*, since October 2018, supervised by Isabelle Chrisment, Raouf Boutaba & Jérôme François.
- PhD in progress: Mingxiao Ma, *Cyber-Physical Systems defense through smart network configuration*, since November 2017, supervised by Isabelle Chrisment, Abdelkader Lahmadi.
- PhD in progress: Mohamed Oulaaffart, *Automating security enhancement for cloud services*, since January 2020, supervised by Olivier Festor & Rémi Badonnel.
- PhD in progress: Mehdi Zakroum, *Forecasting cyberthreats from exogeneous data*, since October 2019, supervised by Isabelle Chrisment & Jérôme François.
- PhD: Pierre-Olivier Brissaud, *HTTPS traffic analysis for user activity monitoring*. Université de Lorraine, 14 December 2020. Supervised by Isabelle Chrisment, Jérôme François, Thibault Cholez and Olivier Bettan (Thales) [28].
- PhD: Abdulqawi Saif, *Experimental Methods for the Evaluation of Big Data Systems*. Université de Lorraine, 17 January 2020. Supervised by Ye-Qiong Song & Lucas Nussbaum [22].

#### 10.2.3 Juries

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

- Charles Xosanavongsa, PhD in Computer Science from Université de Rennes 1, France. Title: Heterogeneous Event Causal Dependency Definition for the Detection and Explanation of Multi-Step Attacks, June 2020 – (Isabelle Chrisment as reviewer).
- Joseph Kamel, PhD in Institut Polytechnique de Paris, France. Title: Misbehavior Detection for Cooperative Intelligent Transport Systems, July 2020 – (Isabelle Chrisment as reviewer).
- Quentin Ricard, PhD in Computer Science from Université Toulouse III, Paul Sabatier, France. Title: Détection autonome de trafic malveillant dans les réseaux véhiculaires, September 2020 – (Isabelle Chrisment as reviewer).
- Mohammed Tayeb Oulad Kouider, PhD in Computer Science from Université de Lorraine. Title: Optimisation de la planification des tournées de véhicules électriques. December 2020 – (Isabelle Chrisment as President).
- Pierre-Olivier Brissaud, PhD in Computer Science from Université de Lorraine. Title: Analyse de trafic HTTPS pour la supervision d'activités utilisateurs, December 2020 – (Isabelle Chrisment as co-supervisor).
- José Rafael Suárez-Varela Maciá, PhD in Computer Science from Universitat Politècnica de Catalunya (Spain). Title: Enabling knowledge-defined networks: Deep reinforcement learning, graph neural networks and network analytics, June – (Jérôme François as defense commitee member)

- Thomas Cledel, PhD in Computer Science from IMT Atlantique Bretagne-Pays de la Loire (France). Title: Cyber-résilience des infrastructures critiques – Analyse préventive des défaillances d'origine malveillante, June 2020 – (Olivier Festor as reviewer)
- Aliénor Damien, PhD in Computer Science from Université Fédérale Toulouse Midi-Pyrénées (France). Title: Sécurité par analyse comportementale de fonctions embarquées sur plateformes avioniques modulaires intégrées, June 2020 – (Olivier Festor as reviewer)
- Edwin Bourget, PhD in Computer Science from IMT Atlantique Bretagne-Pays de la Loire (France). Title: Diagnosing accidental and malicious events in industrial control systems, June 2020 – (Olivier Festor as defense commitee member)

Team members participated to the following Habilitation Degree committees:

- Abbas Bradai, PhD in Automation and Control from Université de Poitiers (France). Title: Contributions to the virtualisation of communication systems: from cellular networks to the Internet of Things, December 2020 – (Olivier Festor as reviewer)

#### 10.2.4 Articles and contents

Abdelkader Lahmadi and Isabelle Chrisment provided an article entitled "Comment évaluer le niveau de sécurité de vos objets connectés ?" in Binaire, Le Monde, June 2020, https://www.lemonde.fr/blog/binaire/2020/06/26/comment-evaluer-le-niveau-de-securite-de-vos-objets-connectes/.

#### 10.2.5 Interventions

Isabelle Chrisment participated in a seminar on cyberdefense and cyberespace at Horizon 2035, CEIS, Paris, October 2020.
Jérôme François was an invited speaker at the *A.I. Now* conference 2020 (Metz, France)

# 11 Scientific production

## 11.1 Publications of the year

**International journals**

[1] A. Anthony, S. R. Chowdhury, T. Bai, R. Boutaba and J. François. 'Non-intrusive and Workflow-aware Virtual Network Function Scheduling in User-space'. In: *IEEE transactions on cloud computing* (15th Sept. 2020). DOI: 10.1109/TCC.2020.3024232. URL: https://hal.inria.fr/hal-02996459.

[2] R. Badonnel, C. Fung, Q. Li and S. Scott-Hayward. 'Guest Editorial: Special Section on Cybersecurity Techniques for Managing Networked Systems'. In: *IEEE Transactions on Network and Service Management* 17.1 (Mar. 2020), pp. 12–14. DOI: 10.1109/TNSM.2020.2972769. URL: https://hal.inria.fr/hal-02957559.

[3] M. Compastié, R. Badonnel, O. Festor and R. He. 'From virtualization security issues to cloud protection opportunities: An in-depth analysis of system virtualization models'. In: *Computers and Security* 97 (Oct. 2020), p. 101905. DOI: 10.1016/j.cose.2020.101905. URL: https://hal.archives-ouvertes.fr/hal-02890270.

[4] A. Hemmer, M. Abderrahim, R. Badonnel, J. François and I. Chrisment. 'Comparative Assessment of Process Mining for Supporting IoT Predictive Security'. In: *IEEE Transactions on Network and Service Management* (Dec. 2020). DOI: 10.1109/TNSM.2020.3038172. URL: https://hal.inria.fr/hal-03019862.

[5] L. Meftah, R. Rouvoy and I. Chrisment. 'Empowering Mobile Crowdsourcing Apps with User Privacy Control'. In: *Journal of Parallel and Distributed Computing* (1st Aug. 2020), p. 15. DOI: 10.1016/j.jpdc.2020.07.011. URL: https://hal.inria.fr/hal-02910246.

[6] D. E. Sarmiento, A. Lebre, L. Nussbaum and A. Chari. 'Decentralized SDN Control Plane for a Distributed Cloud-Edge Infrastructure: A Survey'. In: *Communications Surveys and Tutorials, IEEE Communications Society* (2021). DOI: 10.1109/COMST.2021.3050297. URL: https://hal.archives-ouvertes.fr/hal-03119901.

**International peer-reviewed conferences**

[7] A. Abboud, R. Garcia, A. Lahmadi, M. Rusinowitch and A. Bouhoula. 'Efficient Distribution of Security Policy Filtering Rules in Software Defined Networks'. In: NCA 2020 - 19th IEEE International Symposium on Network Computing and Applications. Online conference, France, 24th Nov. 2020. URL: https://hal.inria.fr/hal-03036350.

[8] A. Abboud, A. Lahmadi, M. Rusinowitch, M. Couceiro, A. Bouhoula and M. Ayadi. 'Double Mask: An efficient rule encoding for Software Defined Networking'. In: ICIN 2020 - 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops. 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops, {ICIN} 2020, Paris, France, February 24-27, 2020. Paris, France, 2020, pp. 186–193. URL: https://hal.archives-ouvertes.fr/hal-02547097.

[9] L. Bertot, L. Nussbaum and D. Margery. 'Implementing SFA Support on an Established HPC-flavored Testbed: Lessons Learned'. In: CNERT 2020 - Computer and Networking Experimental Research using Testbeds, in conjunction with IEEE INFOCOM 2020. Toronto, Canada, 6th July 2020, pp. 1–6. URL: https://hal.inria.fr/hal-02962845.

[10] P.-O. Brissaud, J. François, I. Chrisment, T. Cholez and O. Bettan. 'Encrypted HTTP/2 Traffic Monitoring: Standing the Test of Time and Space'. In: WIFS2020 - IEEE International Workshop on Information Forensics and Security. IEEE International Workshop on Information Forensics and Security. New-York/Virtual, United States, 6th Dec. 2020. URL: https://hal.archives-ouvertes.fr/hal-03032578.

[11] D. Espinel Sarmiento, A. Lebre, L. Nussbaum and A. Chari. 'Multi-site Connectivity for Edge Infrastructures DIMINET:DIstributed Module for Inter-site NETworking'. In: CCGRID 2020 - 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing. Melbourne, Australia: http://cloudbus.org/ccgrid2020/, 2020, pp. 1–10. URL: https://hal.archives-ouvertes.fr/hal-02573638.

[12] J. François, A. Clemm, V. Maintenant and S. Tabor. 'BPP over P4: Exploring Frontiers and Limits in Programmable Packet Processing'. In: IEEE Global Communications Conference. IEEE Global Communications Conference 2020. Taipei, Taiwan, 7th Dec. 2020. URL: https://hal.archives-ouvertes.fr/hal-03032566.

[13] A. Hemmer, R. Badonnel and I. Chrisment. 'A Process Mining Approach for Supporting IoT Predictive Security'. In: NOMS 2020 - IEEE/IFIP Network Operations and Management Symposium. Budapest, Hungary: ieee-noms.org, 20th Apr. 2020. URL: https://hal.inria.fr/hal-02402986.

[14] A. Hemmer, R. Badonnel, J. François and I. Chrisment. 'A Process Mining Tool for Supporting IoT Security'. In: NOMS 2020 - IEEE/IFIP Network Operations and Management Symposium. Budapest, Hungary, 20th Apr. 2020. URL: https://hal.inria.fr/hal-02625712.

[15] N. Khan, A. Lahmadi, Z. Kräussl and R. State. 'Management plane for differential privacy preservation through smart contracts'. In: AICCSA 2020 - 17th ACS/IEEE International Conference on Computer Systems and Applications. Antalya / Virtual, Turkey: http://aiccsa.net/AICCSA2020/home, 2nd Nov. 2020. URL: https://hal.inria.fr/hal-03088227.

[16] A. Lahmadi, A. Duque, N. Heraief and J. Francq. 'MitM Attack Detection in BLE Networks using Reconstruction and Classification Machine Learning Techniques'. In: MLCS 2020 - 2nd Workshop on Machine Learning for Cybersecurity. Ghent, Belgium, 14th Sept. 2020, pp. 1–16. URL: https://hal.inria.fr/hal-02948407.

[17] A. Laraba, J. François, I. Chrisment, S. R. Chowdhury and R. Boutaba. 'Defeating Protocol Abuse with P4: Application to Explicit Congestion Notification'. In: 2020 IFIP Networking Conference (Networking). Paris, France, 22nd June 2020. URL: https://hal.inria.fr/hal-02993199.

[18] M. Ma, A. Lahmadi and I. Chrisment. 'Detecting a Stealthy Attack in Distributed Control for Microgrids using Machine Learning Algorithms'. In: 3rd IEEE International Conference on Industrial Cyber-Physical Systems (ICPS). Tampere (online), Finland, 10th June 2020. URL: https://hal.inria.fr/hal-02980115.

[19] L. Meftah, R. Rouvoy and I. Chrisment. 'Capturing Privacy-preserving User Contexts with IndoorHash'. In: DAIS 2020 - 20th IFIP International Conference on Distributed Applications and Interoperable Systems. Vol. 12135. Valletta, Malta: http://www.discotec.org/2020/dais.html, 15th June 2020. DOI: 10.1007/978-3-030-50323-9_2. URL: https://hal.inria.fr/hal-02541391.

[20] M. Said Frikha, A. Lahmadi, S. Mettali Gammar and L. Andrey. 'Leveraging Reinforcement Learning for Adaptive Monitoring of Low-Power IoT Networks'. In: The 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob2020). Thessaloniki (Virtual), Greece, 12th Oct. 2020. URL: https://hal.inria.fr/hal-02980094.

#### Scientific book chapters

[21] J. François, F. Beck, G. Mezzour, K. M. Carley, A. Lahmadi, M. Ghogho, A. Houmz, H. Hammouchi, M. Zakroum, N. Nejjari and O. Cherqi. 'ThreatPredict: From Global Social and Technical Big Data to Cyber Threat Forecast'. In: *Advanced Technologies for Security Applications*. Advanced Technologies for Security Applications. Proceedings of the NATO Science for Peace and Security 'Cluster Workshop on Advanced Technologies. 27th June 2020, pp. 45–54. DOI: 10.1007/978-94-024-2021-0_5. URL: https://hal.inria.fr/hal-03036928.

#### Doctoral dissertations and habilitation theses

[22] A. Saif. 'Experimental Methods for the Evaluation of Big Data Systems'. Université de Lorraine, 17th Jan. 2020. URL: https://hal.univ-lorraine.fr/tel-02499941.

#### Reports & preprints

[23] D. Espinel Sarmiento, A. Lebre, L. Nussbaum and A. Chari. *Decentralized SDN Control Plane for a Distributed Cloud-Edge Infrastructure: A Survey*. INRIA, 15th June 2020, p. 40. URL: https://hal.inria.fr/hal-02868984.

[24] A. Saif, L. Nussbaum and Y.-Q. Song. *On the Impact of I/O Access Patterns on SSD Storage*. Inria, 7th Jan. 2020. URL: https://hal.inria.fr/hal-02430564.

#### Other scientific publications

[25] A. Abboud, R. Garcia, A. Lahmadi, M. Rusinowitch and A. Bouhoula. *R2-D2: Filter Rule set Decomposition and Distribution in Software Defined Networks*. Izmir/Virtual, Turkey, 2nd Nov. 2020. URL: https://hal.inria.fr/hal-03036292.

### 11.2 Cited publications

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

[27] D. Balouek, A. Carpen-Amarie, G. Charrier, F. Desprez, E. Jeannot, E. Jeanvoine, A. Lèbre, D. Margery, N. Niclausse, L. Nussbaum, O. Richard, C. Pérez, F. Quesnel, C. Rohr and L. Sarzyniec. 'Adding Virtualization Capabilities to the Grid'5000 Testbed'. In: *Cloud Computing and Services Science*. Ed. by I. Ivanov, M. Sinderen, F. Leymann and T. Shan. Vol. 367. Communications in Computer and Information Science. Springer International Publishing, 2013, pp. 3–20. DOI: 10.1007/978-3-319-04519-1_1. URL: https://hal.inria.fr/hal-00946971.

[28] P.-O. Brissaud. ' Analyse de trafic HTTPS pour la supervision d'activités utilisateurs'. Not yet registred. Theses. Université de Lorraine, Dec. 2020.

[29] 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.

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

[31] L. Sarzyniec, T. Buchert, E. Jeanvoine and L. Nussbaum. 'Design and Evaluation of a Virtual Experimental Environment for Distributed Systems'. In: *PDP2013 - 21st Euromicro International Conference on Parallel, Distributed and Network-Based Processing*. Belfast, United Kingdom, Feb. 2013. URL: https://hal.inria.fr/hal-00724308.

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