RESEARCH CENTRE

Nancy - Grand Est

IN PARTNERSHIP WITH:

Université de Lorraine, CNRS

2021

ACTIVITY REPORT

Project-Team

RESIST

Resilience and elasticity for security and scalability of dynamic networked systems

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

DOMAIN

Networks, Systems and Services, Distributed Computing

THEME

Networks and Telecommunications

Contents

Project-Team RESIST

Creation of the Project-Team: 2020 December 01

Keywords

Computer sciences and digital sciences

A1.1.8. – Security of architectures

A1.1.13. – 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

- Isabelle Chrisment [Team leader, Inria, Senior Researcher, from Sep 2021, HDR]
- Raouf Boutaba [Inria, International Chair, Advanced Research Position]
- Jérôme François [Inria, Researcher]
- Nicolas Schnepf [Inria, Researcher, from Oct 2021]

Faculty Members

- Isabelle Chrisment [Team leader, Univ de Lorraine, Professor, until Aug 2021, HDR]
- Laurent Andrey [Univ de Lorraine, Associate Professor]
- Rémi Badonnel [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]

Post-Doctoral Fellows

- Luke Bertot [Inria, until Sep 2021]
- Xavier Marchal [CNRS, from Feb 2021]
- Lama Sleem [Univ de Lorraine]

PhD Students

- Ahmad Abboud [NUMERYX TECHNOLOGIES, CIFRE, until Nov 2021]
- Omar Anser [Inria, from June 2021]
- Enzo D'andrea [Inria, from Oct 2021]
- Jean-Philippe Eisenbarth [Univ de Lorraine]
- Philippe Graff [CNRS]
- Adrien Hemmer [Inria - Université de Lorraine, Inria until Aug 2021, Université de Lorraine (ATER) from Sep 2021]
- Matthiews Jose [Orange Labs, CIFRE]
- Pierre Marie Junges [Univ de Lorraine]
- Joel Roman Ky [Orange, CIFRE, from Oct 2021]
- Abir Laraba [Univ de Lorraine, ATER, from Sep 2021]
- Mingxiao Ma [CNRS, until Apr 2021]
- Mohamed Oulaaffart [Univ de Lorraine]
- Mehdi Zakroum [Univ de Lorraine]

Technical Staff

- Mohamed Abderrahim [Inria, Engineer, until Jun 2021]
- Antoine Chemardin [Inria, Engineer, until Mar 2021]
- Thomas Lacour [Inria, Engineer, until Dec 2021]
- Alexandre Merlin [Inria, Engineer]
- Nicolas Perrin [Inria, Engineer]
- Jonathan Proietto-Stallone [Inria, Engineer, from Sep 2021]

Interns and Apprentices

- Salima Ait-Alla [Inria, from Mar 2021 until Sep 2021]
- Karim Baccar [Inria, from Feb 2021 until May 2021]
- Gabriel Branco Frizzo [Univ de Lorraine, from Jun 2021 until Aug 2021]
- Louise Bulone [Univ de Lorraine, from Apr 2021 until Sep 2021]
- Enzo D'andrea [Univ de Lorraine, from Mar 2021 until Sep 2021]
- Omar Kassmi [Univ de Lorraine, from Jun 2021 until Aug 2021]
- Antoine Petit [Inria, from Sep 2021]
- Ambroise Sander [Univ de Lorraine, from May 2021 until Aug 2021]

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 (link accessed on 08/02/2021) which contributes to traffic opacity.

2.2 Challenges

In this context two main challenges stand out:

- **Scalability**: As mentioned above, the Internet ecosystem is continuously expanding in both size and heterogeneity. Scalability was already a challenge in the last decade but solutions mainly focused on scaling one dimension at a time, e.g. increasing the capacity of network links or that of compute resources in order to face peak demand, even if it is infrequent. Such **over-provisioning** however wastes significant resources and **cannot cope with future demand** at a reasonable cost. Several experts warn about major Internet blackouts in the coming years[30, 27]. 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) [31] 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

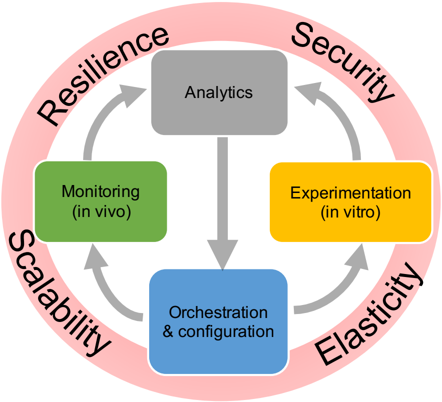

Figure 1: The Resist project

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.

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 allow detecting world-wide campaigns of attacks which target a specific exploit in some applications. Moreover the monitoring of the Internet traffic at the **edge** is the best way to quickly detect distributed attacks like DDoS and to mitigate them before they become effective. However, the Internet traffic analysis is made much more complicated since the **massive shift towards encryption** that happened few years ago, which requires new traffic classification methods.

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

4.2 SDN and Data-Center Networks

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

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

4.3 Fog and Cloud computing

Cloud computing has largely evolved in the last years including new networking capabilities as highlighted in the previous section towards the model of XaaS or **everything-as-a-service**. Moreover, cloud computing continues to be more distributed and aims at integrating more heterogeneous resources. One particular example is **fog computing** that consists of a massively distributed number of different resources, including low-performance ones. Large network operators have a great interest in fog computing because they already operate such an infrastructure (e.g. a national operator with regional clouds and setup boxes in end users' homes). Softwarization or virtualization of all functions and services will help them to be competitive by reducing their costs. In general, intelligent orchestration of massively distributed resources will be investigated in various application domains, including **federated cloud infrastructures, fog computing, 5G networks, IoT and big data infrastructures**.

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

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

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

4.4 Cyber-Physical Systems

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

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

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

5 Highlights of the year

Since January 2021, Isabelle Chrisment is Deputy Scientific Director at Inria in charge of the national scientific domain "Networks, Systems and Services, Distributed Computing".

5.1 Awards

Pierre-Marie Junges received the best student paper award at 17th International Conference on Network and Service Management (CNSM) for his work on predicting credentials and software composition of embedded devices [15].

6 New software and platforms

This year two new software tools appear in the project catalog. Our IoT testing platform got some new devices for assessment.

6.1 New software

6.1.1 SKB

Name: Security Knowledge Base

Keywords: Cybersecurity, Knowledge database, Vulnerability

Functional Description: This project holds all information and tools related to the Security Knowledge Base (SKB) from the SCUBA project and its components such as:

* CPE, Common Platform, Enumeration, URIs to identify hardware platforms, operating systems, applications/softwares,

* CVE, Common Vulnerability and Exposure, publicly known cybersecurity vulnerabilities,

* CWE, Common Weakness Enumeration, list of common software security weaknesses,

* CAPEC, Common Attack Pattern Enumeration and Classification, dictionary and classification taxonomy of known attacks,

* ExploitDB, ExploitDB dictionary,

* Metasploit, Metasploit dictionary,

* Nessus Plugin, Nessus Plugin dictionary,

* Mitre Matrix techniques, Mitre techniques dictionary.

It is based on an OrientDB graph database with the Tinkerpop computing framework, and a MongoDB as documents database.

The graph database is constructed based on cve-search from CIRCL and our own correlation algorithms and methods.

News of the Year: First release

Contact: Abdelkader Lahmadi

Participants: Abdelkader Lahmadi, Jerôme François, Thomas Lacour, Frederic Beck

6.1.2 Crawleth

Keywords: Peer-to-peer, Peer-to-peer., Distributed systems, Distributed networks, Blockchain

Scientific Description: Crawleth works at the Node Discovery protocol level. Its goal is to find all the nodes regardless of the protocol used above: it can find the nodes of the Ethereum's mainnet and testnet, along with the nodes that participate in other blockchain systems built on top of the Ethereum's Node Discovery layer. The crawling methodology is as follows. First, Crawleth tests the connectivity of the bootstrap nodes (whose IP addresses and Node IDs are retrieved from the Geth client source code where they are hardcoded) by sending a PING packet and waiting for the PONG response. Then, for each responding node, it sends a FINDNODE packet with the target parameter being the bootstrap Node ID itself. The FINDNODE requests used by our crawler are always centered on the contacted Node ID, where its routing table has the highest precision because the buckets are the deepest (more contacts are known). Each recipient will answer with a NEIGHBOR packet containing sixteen close nodes to itself, in terms of Node ID XOR distance. Crawleth will carry on this strategy on the newly discovered nodes until there is no new nodes to discover, which means that it went all around the DHT. When a crawl is finished, it exports the information of the discovered up nodes (IP address, UDP port, Node ID, geolocalization) and starts a new crawl.

Functional Description: The goal of Crawleth is to find all the nodes following Ethereum's Node Discovery protocol. At the end of a crawl, it exports the information of the discovered nodes.

URL: `https://gitlab.inria.fr/jeisenba/Crawleth`

Contact: Jean-Philippe Eisenbarth

Participants: Jean-Philippe Eisenbarth, Thibault Cholez, Olivier Perrin, Ambroise Sander, Christophe Belleut, Florent Caspar

6.2 New platforms

CPS Security Assessment Platform

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

During 2021, 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. In 2022, we will extend this platform with a small scale 5G testbed to evaluate the security of devices relying on this networking technology.

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 [3]. In 2021, we pursued our work on adaptive monitoring mechanisms for low-power IoT devices, by using a Deep Reinforcement Learning (DRL) method coupled with an Unsupervised Learning reward technique to automatically adapt the polling frequencies of a set of dynamically selected attributes [19]. Our goal is to minimize the number of monitoring packets while keeping accurate and timely detection of anomalies reported by the supervised attributes.

7.1.2 Programmable Network Monitoring

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

We proposed a systematic method to map Extended Finite State Machine (EFSM) models into a P4 switch in order to embed detection of complex behaviors within the dataplane. The Advantage of EFSM over the other widely used formalisms in SDN (like flow based rules) is to be stateful and so able to track multi-step attacks. Our mapping method can be leveraged to monitor any protocol or its misuse. We demonstrated its effectiveness against TCP protocol attacks: optimistic acknowledgments and ECN protocol misuse in [5]. In order to provide a valid scenario, our setup based on mininet considers AQM (Adaptive Queue Management). In all cases, our solution enforces a fair bandwidth share between flows even in case of non-cooperative or misbehaving flows. We have further extended this work by combining our EFSM scheme with a Petri net, whose main advantage is to be easily represented and so implemented with reconfigurable match tables. As a result, an attack detector can be recomposed at run-time from a set of EFSM models which are synchronized with a Petri net.

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

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

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

After having performed a comparative analysis of the performance of detection methods definitively included in the IEEE TNSM journal [4], we pursued in 2021 our efforts by proposing an ensemble learning-based architecture for supporting an early detection of multi-phase attacks in IoT infrastructures [12]. The architecture leverages the performance of five major detection methods, namely process mining, elliptic envelope, one class support vector machine, local outlier factor and isolation forest. We have described the main components of this architecture, their operations and the interactions amongst them. In particular, we have specified the building of dependency graphs using a cross-correlation of data sources, to automate the identification of different phases and their relationships based on the structure and behavior of the IoT systems. We have formalized our detection solution by considering four ensemble learning-based scoring methods, that serve as a support to combine the results of the five considered detection methods to increase the overall detection performance, the different detection methods being executed in parallel. We have developed a proof-of-concept prototype based on the ProM and Scikit-learn libraries, and evaluated the performance of our proposed approach through a large set of experiments based on industrial datasets.
This work has been achieved in the context of the H2020 SecureIoT project (see section 9.3.1).

7.1.4 Monitoring of Blockchains' Networking Infrastructure

Participants: Thibault Cholez *(contact)*, Jean-Philippe Eisenbarth, Olivier Perrin *(Coast team)*.

In 2021, we pursued our work on blockchain monitoring in the Concordia project. We successfully published [9, 10] our previous work on the monitoring of the Bitcoin P2P network. As a reminder, we improved an open source Bitcoin P2P crawler, made an open Bitcoin P2P dataset over several months listing all the peers constituting the Bitcoin P2P network and conducted an analysis of the data with a focus on metrics that can impact the resiliency of the network.

After Bitcoin, Ethereum is the second most popular Blockchain with a total market capitalization over 400 Billion euros in November 2021. But the technical value of Ethereum lies in its ability to execute Smart Contracts that allow automated payments when predefined rules are validated by consensus. In 2021, we conducted a study on the Ethereum P2P network. We developed an Ethereum crawler to explore the

Ethereum P2P network and built a Ethereum dataset made of several months of continuous measurement. Both are released in open source.

Beyond global statistics on the network, our results show that a few nodes may be considered suspicious for several reasons: 1) they are too close to each other in the DHT ID space, or 2) a /24 subnetwork runs a large number of nodes, or 3) because an IP address exhibits many different IDs (Sybil attack).

So, we proposed a revocation mechanism to avoid these few suspicious nodes to grow and conduct a large scale attack able to disrupt the blockchain. It is based on a global monitoring system that detects suspicious nodes and list them in a specific Smart Contract leveraging event logs to store data at a reasonable cost. Nodes of the Ethereum network can then check individually if the report is accurate and cut their own connections to suspicious peers (and blacklist them). The revocation is currently based on an external tool using the RPC API but could be later directly integrated in the official client.

7.1.5 Accuracy-adaptive and Lightweight In-band Network Telemetry

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

In-band Network Telemetry (INT) has recently emerged as a means of achieving per-packet near real-time visibility into the network. INT capable network devices can directly embed device internal states such as packet processing time, queue occupancy and link utilization information in each passing packet. INT piggybacks telemetry information on user data traffic and can significantly increase packet size. A direct consequence of increasing packet size for carrying telemetry data is a substantial drop in network goodput. This paper aims at striking a balance between reducing INT data plane overhead and the accuracy of network view constructed from telemetry data. To this end, we proposed LINT [7], an accuracy-adaptive and Lightweight INT mechanism that can be implemented on commodity programmable devices. The core idea is to identify and filter the less interesting observations of telemetry data directly in the data plane without negatively impacting the quality of the collected telemetry data.

7.2 Experimentation

7.2.1 Distributing Connectivity Management in Cloud-Edge Infrastructures

Participants: Lucas Nussbaum.

In 2021 we continued our work on distributing connectivity management in Cloud-Edge infrastructures and we published a survey on that topic [2] in *IEEE Communications Surveys & Tutorials*. This work has been achieved even though Lucas Nussbaum who was a full member of Resist until 2020 is currently on Inria secondment on a non-research position.

7.2.2 Understanding Cloud Gaming Network Traffic

Participants: Thibault Cholez, Olivier Festor, Philippe Graff, Xavier Marchal.

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

In a first work, we tried to characterize CG traffic and the ability of the platforms to cope with network constraints. We conducted real-life measurements performed between April and July 2021 on the four aforementioned CG platforms, configuring different network constraints like packet loss, throughput decrease, latency increase and jitter variation to observe the behaviour of these CG platforms under extreme network conditions. Our findings show that the four platforms exhibit different adaptation behaviors. Moreover, many cases result in a degraded QoS, leaving room for further improvements at both application and/or network levels. This work was published [11] and the corresponding dataset is available for the community.

7.3 Analytics

7.3.1 CPS Security Analytics

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

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. In [25], we designed a novel attack named "measurement-as-reference" (MaR) attack and used it as a typical stealthy attack example to analyze the theoretical impact on the microgrid system and used numerical simulation results to verify the analysis. We provided mathematical models of possible false data injection (FDI) and denial of service (DoS) attacks in a representative distributed and cooperative controlled microgrid system. We proposed a secure control framework with an attack detection module based on machine learning techniques. To validate the effectiveness of this framework, we implemented two typical attacks, MaR attack and delay injection attack, on a hardware platform modeled after a microgrid system. We collected datasets from the platform and validated the performance of multiple categories of machine learning algorithms to detect such attacks. Our results show that tree-based classifiers (Decision Tree, Random Forest and AdaBoost) outperform other algorithms and achieve excellent performance in detecting normal behavior, delay injection and false data attacks.

7.3.2 Efficient Distribution of Security Filtering Rules in SDN

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

SDN 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. In [24], we developed a simple representation of filtering rules in SDN that enables more compact rule tables and thus are easier to manage while keeping their semantics unchanged. We proposed and evaluated new techniques to decompose and distribute filtering rule sets over a given network topology. We also introduced an update strategy to handle the changes in network policy and topology. In addition, we also exploited the structure of a series-parallel graph to efficiently resolve the rule placement problem for all-sized networks with an acceptable time.

7.3.3 Support for Programmable In-Network Analytics

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

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 to add analytic capabilities in switches, especially to support machine learning functions, current capabilities of hardware switches are not satisfactory even with the recent dataplane programming paradigm. Native integer addition is the limited capability that exists in such hardware. However, P4 switches also include match-action tables that can be leveraged for designing lookup tables to perform floating point operations. In [13], we introduced *InRec*, a framework which can generate the P4 code to be instantiated on a Tofino switch from a real number computational function definition. The process is automated through several steps of refinement and optimization to select an appropriate representation of the operations using adjusted lookup tables, for example based on the domains and ranges of variables. This prototype has been showcased on real hardware and used to apply a logistic regression model for fingerprinting IoT devices [14].

To go beyond a single function to be computed on a single switch, we extended our approach by (1) merging multiple computational pipelines (real functions) into one assuming some optimization such as parallelization of operations and (2) distributing the process onto multiple devices based on available resources using mixed-integer linear programming. In addition, we added support to stateful operations such as recursive ones.

7.3.4 Security Analysis of Embedded Devices

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

The growth of embedded devices like IoT or networking devices makes them major targets for attackers in the Internet. They are known to face security issues because of their bad design and/or configuration. In [16], we proposed a systematic method to evaluate the security of an embedded device. We retrieved a large list of device firmware over ten years and analyzed their software composition in regards to the number of services they provide or the number of vulnerable and old software. We thus evaluate their security by assessing their exposure to threats over Internet and also investigate if vendors have changed their firmware design over a decade.

Thanks to this work, we built a large database from publicly available firmware programs. We thus decided to investigate wether an attacker could exploit this information when looking for potential hosts to attack in Internet. In [15], we defined a method based on a random forest classifier to reconstruct precise information about an IoT device configuration (brand name, usernames, passwords, software components) from partial knowledge such as open ports revealed by a TCP scan. Using our dataset of 6935 embedded devices, the HTTP, SSH or DNS software names can be predicted with a precision higher than 80% with a limited knowledge. The correct HTTP, SSH or DNS versions can be inferred in more than 95% of the cases after 1.4 trials on average. Similarly, our technique also predicts the password of at least one valid user in more than 97% of the cases after 1.15 trials on average.

7.4 Orchestration

7.4.1 Vulkan for NFV

Participants: Thibault Cholez.

In the scope of the MOSAICO ANR project, we pursued in 2021 a cooperation with the University of Oulu initiated with the 2020 internship in Resist of Juuso Haavisto on the design of an open NFV architecture that can easily use GPGPU processing with heterogeneous devices. In fact, recent studies have focused on integrated graphics units and various performance optimizations to address bottlenecks such as latency. However, these approaches tend to produce architecture-specific binaries and lack the orchestration of functions. A complementary effort would be a GPGPU architecture based on standard and open components, which allows the creation of interoperable and orchestrable network functions.

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

7.4.2 Software-Defined Security for Clouds

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

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

Within the H2020 Concordia project, we have pursued investigating a security automation strategy for cloud services, with a focus on issues related to resource migration [17]. This strategy argues in favor of exploiting service descriptions as an important knowledge source to drive security enhancement. The first pillar of this work consists in extending an orchestration language for specifying different orchestrated security levels and supporting security automation. The second pillar concerns the design of a framework with selection algorithms to determine the security mechanisms to be activated for protecting a whole cloud service during the migration of one or several of its resources. Finally, the third pillar is focused on the complementarity of exogenous and endogenous security mechanisms. We have shown through illustrative examples (restriction, proactive restriction and relaxation use cases) to what extent the selection of exogenous and endogenous mechanisms could be supported by risk management algorithms. We have also recently built a framework based on SMT solving for supporting the migration of resources in cloud composite services, and preventing the occurrence of new configuration vulnerabilities. We have evaluated the benefits and limits of this framework through large series of experiments using a proof-of-concept prototype implemented over the CVC4 commonly-used open-source solver[28].

This work has been achieved in the context of the H2020 EU Concordia project.

7.5 Chaining of Security Functions

Participants: Rémi Badonnel *(contact)*, Abdelkader Lahmadi, Stephan Merz *(Veridis team)*, Nicolas Schnepf.

Software-defined networking offers new opportunities for protecting end users and their applications. It enables the elaboration of security chains that combines different security functions, such as firewalls, intrusion detection systems, and services for preventing data leakage. In that context, we have published a book chapter [20] that introduces a method for automating the orchestration of security functions driven by process learning, and illustrates how it could be used for protecting Android devices by relying on software-defined networks. This solution contributes to bridging the gap between learning and verification techniques. Our method addresses four main problems: (i) modeling the specific security needs of applications through process learning techniques, (ii) generating corresponding chains of security functions based on formal synthesis methods, (iii) verifying the correctness properties of these chains, and (iv) optimizing their deployment by merging chains and adapting them to the network infrastructure. We evaluated the performance of the method through extensive series of experiments. The flexibility of SDN infrastructures enables us to synthesize and deploy security chains that are specific to the networking behavior of individual applications running on smart devices. By construction, the

obtained chains ensure certain correctness properties, and specific properties can be formally verified based on SMT solving and model checking. Finally, by applying appropriate optimization methods, the impact of deploying security chains on network performance can be substantially reduced. This work opens several directions for future research, including the exploration of emerging methods from explainable artificial intelligence that could be considered for facilitating the interpretation of automation results, together with the use of more elaborated detection techniques.
This work has been performed in collaboration with the Inria VERIDIS project team.

8 Bilateral contracts and grants with industry

8.1 Bilateral grants with industry

Participants: Jérôme François *(contact)*, Olivier Festor, Matthews Jose, Abdelkader Lahmadi *(contact)*, Ahmad Abboud, Michael Rusinowitch *(Pesto team)*, Adel Bouhoula *(Numeryx)*.

Orange Lab (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 [13, 14]

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 [24]

9 Partnerships and cooperations

9.1 International initiatives

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

NetMSS

Title: NETwork Monitoring and Service orchestration for Softwarized networks

Duration: 01/2018 - 12/2021 (under renewal)

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 is greatly changing the landscape in networking. In the last years, the effort have focused on how to integrate network elements in cloud-based models. This has led 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 has been 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 a new method to be efficiently handled. For example, monitoring softwarized network requires the collect of heterogeneous information, regarding the network but also the 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 STIC/MATH/CLIMAT AmSud project

ANGEL

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

Duration: 01/2021-12/2022

Local supervisor: Jérôme François

Partners:

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

Inria contact: Jérôme François

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

9.1.3 Participation in other International Programs

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.
- Abir Laraba: international PhD grant in cooperation with University of Waterloo
- Mehdi Zakroum: international PhD grant in cooperation with International University of Rabat.

9.2 International research visitors

9.2.1 Visits of international scientists

Inria International Chair

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

9.3 European initiatives

9.3.1 FP7 & H2020 projects

CONCORDIA

Title: Cyber security cOmpeteNCe fOr Research anD InnovAtion

Duration: 01/2019 - 01/2022

Coordinator: Research Institute CODE (Munich, Germany)

Partners: 52 partners, 26 academic and 26 industrial, from 19 countries (please see the full consortium description)

Inria contact: Thibault Cholez

Url: www.concordia-h2020.eu

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

On the research side, we work on blockchain monitoring 7.1.4 and cloud security automation 7.4.2. Regarding the education in cybersecurity, we contributed to the first session of a MOOC on Coursera entitled "Becoming Cybersecurity Consultant", including an interactive webinar with practical exercises over the KYPO cyber-range. We also participated in the seminars of a cybersecurity awareness week organized for high-school students and teachers. Finally, we contributed to the integration efforts regarding an open exchange format for cyber-ranges, and organized two cybersecurity events (Capture-The-Flag, Cybersecurity Hackathon) in the TELECOM Nancy premises.

AI@EDGE

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

Duration: January 2021 - December 2023

Coordinator: Fondazione Bruno Kessler

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: aiatedge.eu

Summary: AI@EDGE will develop a connect-compute fabric – specifically leveraging the serverless paradigm – for creating and managing resilient, elastic, and secure end-to-end slices. Such slices will be capable of supporting a diverse range of AI-enabled applications. Privacy-preserving machine learning and trusted networking techniques will be used to ensure each stakeholder can use the platform without disclosing sensitive information. The AI@EDGE project will focus on six main breakthroughs: (1) AI/ML for closed loop automation; (2) Privacy preserving, machine learning for multi-stakeholder environments; (3) Distributed and decentralized connect-compute platform; (4) Provisioning of AI-enabled applications; (5) Hardware-accelerated serverless platform for AI/ML; (6) Cross-layer, multi-connectivity and disaggregated radio access.

SPARTA

Title: Special projects for advanced research and technology in Europe

Duration: 02/2019 - 01/2022

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

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

Inria contact: Jérôme François

Url: www.sparta.eu

Summary: 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 world leading 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.

Under this context, the team develops a new IoT honeypot based on firmware emulation now deployed at the High Security Lab in Nancy.

9.3.2 Other European Programs/Initiatives

ERASMUS+ REWIRE

Title: Cybersecurity Skills Alliance: a new Vision for Europe

Duration: November 2020 - October 2024

Coordinator: Mykolas Romeris University – MRU (Lithuania)

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

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 brings together lessons learned from other initiatives including the four pilot projects, and is outlined from a holistic approach, identifying political, economical, social, technological, legal and other factors which may be affecting sector skills and training offer. These activities include the development of a common methodology for the assessment of the current situation and to anticipate future needs, through identification of existing and emerging skills needs, the creation of a cybersecurity skills framework containing profiles for the needed cybersecurity profiles and their analysis, and the creation of at least four educational curricula and relevant skills certification schemes for profiles contained in the cybersecurity skills framework. During the first year of the project, the efforts have been mainly centered on building the sectorial skill strategy supporting the sectoral cooperation and the blueprint for the cybersecurity industry, including a PESTLE analysis which has been published [18].

9.4 National initiatives

9.4.1 ANR

ANR MOSAICO

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

Coordinator: Orange Labs

Duration: 12/2019-11/2023

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 network function into micro-services. The expected benefits relies on an easier development and maintenance, better quality, scalability and responsiveness to new scenarios than monolithic approaches, while offering more management possibilities for operators through orchestration. As a consequence, it appears that network functions can be split in several micro-services, implemented through different means, according to the software environments and performance requirements in different topological locations. This need for multi-level and multi-technology orchestration is even more important with the emergence of new services, such as immersive services, which exhibit very strong quality of service constraints (i.e. latency cannot exceed a few milliseconds). The MOSAICO project proposes to design, implement and validate a multi-layer architecture, able to control several underlying network programmability technologies (SDN, NFV, P4) to compose micro-services forming the overall network service. To reach this objective, the project will follow an experimental research methodology from the definition of the global architecture and micro-services, to the design of orchestration rules and the evaluation against the project use-case of a low latency network application.

In particular we are in charge of the cloud-gaming use-case. First, we conducted a comprehensive study to characterize this type of traffic and detect it automatically with machine learning. In a second step, we will propose new means to improve the QoS by designing an applying new dedicated network functions in the data plane to enhance low-latency services.

ANR 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 the servers require traffic analysis to detect malicious behaviors. This analysis includes identification of illegitimate connections to mitigate denial of service attacks, content filtering to limit content exposition or content leakage, and log management for later forensic analysis. Security Information and Event Management (SIEM) that deals with internal and external threats should still remain effective under GDPR constraints. Data protection usually means encryption, which in turn heavily limits the traffic analysis capabilities. The main goal of this project is to bridge the gap between these two security and privacy requirements, with advanced cryptographic tools (such as searchable encryption, functional encryption, fully homomorphic encryption, and multi-party computation) in order to provide privacy to the end users while allowing traffic monitoring by the network security manager. While current tools already work on encrypted streams by analyzing the meta-data only, advanced encryption tools may enrich the analysis by specific researches in the encrypted payload.

The team is in charge of the use-case addressing the problem of "Content Filtering" applied to encrypted traffic. More precisely we defined the functional and non-functional requirements to enable Content Filtering for both enterprise and home networks. Next, we will help implementing the cryptographic scheme proposed by our partners for this use-case and validate it against realistic scenarios.

9.4.2 Inria joint Labs

Inria-Orange Joint Lab

Title: Inria - Orange Joint Laboratory

Duration: September 2015 - August 2025

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

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

General chair, scientific chair
Olivier Festor: IEEE International Symposium on Integrated Network Management (IM 2021), general co-chair.
Abdelkader Lahmadi: Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2021), general co-chair.

Member of the organizing committees

Laurent Andrey: IEEE International Symposium on Integrated Network Management (IM 2021), web chair.

Rémi Badonnel: IEEE International Symposium on Integrated Network Management (IM 2021), experience track co-chair; IEEE/IFIP International Conference on Network and Service Management (CNSM 2021), publicity co-chair; IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), experience track co-chair.

Isabelle Chrisment: Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2022), member of the steering committee; IEEE International Symposium on Integrated Network Management (IM 2021), tutorial co-chair.

Jérôme François: IEEE International Symposium on Integrated Network Management (IM 2021), publicity co-chair; Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2021), member of the steering committee; IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2021), member of the steering committee.

Abdelkader Lahmadi: IEEE International Symposium on Integrated Network Management (IM 2021), publication co-chair; co-organizer of the scientific day on network security (GT SSLR, May 2021).

10.1.2 Scientific events: selection

Member of the conference program committees

Laurent Andrey: IEEE Conference on Network Softwarization (NetSoft 2021).

Rémi Badonnel: IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), IEEE International Conference on Communications (ICC 2022), IEEE International Symposium on Integrated Network Management (IM 2021), IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2021), IEEE/IFIP International Conference on Network and Service Management (CNSM 2021), ACM SIGCOMM Workshop on Technologies, Applications, and Uses of a Responsible Internet (TAURIN 2021), Asia-Pacific Network Operations and Management Symposium (APNOMS 2021), IEEE International Mediterranean Conference on Communications and Networking (MeditCom 2021), IEEE International Conference on Networks of the Future (NoF 2021), IEEE Conference on Network Softwarization (NetSoft 2021).

Thibault Cholez: IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), IEEE International Symposium on Integrated Network Management (IM 2021), IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2021), International Workshop on High-Precision, Predictable, and Low-Latency Networking (HiPNet 2021), Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2021), IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2021).

Isabelle Chrisment: IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2022), ACM/IEEE International Conference on Internet of Things Design and Implementation (IoTDI 2021), IEEE/IFIP International Conference on Network and Service Management (CNSM 2021), Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication (CoRes 2021), IEEE International Symposium on Integrated Network Management (IM 2021).

Olivier Festor: IEEE/IFIP International Conference on Network and Service Management (CNSM 2021), IEEE International Symposium on Integrated Network Management (IM 2021), IEEE Conference on Network Softwarization (NetSoft 2021).

Jérôme François: IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), IEEE International Symposium on Integrated Network Management (IM 2021), IEEE/IFIP International Conference on Network and Service Management (CNSM 2021), Cyber Security in Networking Conference (CSNet 2021), Conference on Innovations in Clouds, Internet and Networks (ICIN 2021), IEEE Conference on Network Softwarization (NetSoft 2021), Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2021).

Abdelkader Lahmadi: IEEE/IFIP Network Operations and Management Symposium (NOMS 2022), IEEE International Conference on Communications (ICC 2022), IEEE Annual Consumer Communications & Networking Conference (CCNC 2022), IEEE International Mediterranean Conference on Communications and Networking (MeditCom 2021), IEEE Global Communications Conference (Globecom 2021), IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2021), Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2021), 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 2021).

10.1.3 Journal

Member of the editorial boards

Rémi Badonnel: Associate Editor for IEEE Transactions on Network and Service Management (TNSM), Associate Editor for Wiley International Journal of Network Management (IJNM), Associate Editor for Springer Journal of Network and System Management (JNSM), Lead Guest Editor for the Special Issue on Cybersecurity of IEEE Transactions on Network and Service Management (TNSM).

Isabelle Chrisment: Associate Editor for IEEE Transactions on Network and Service Management (TNSM).

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

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

Reviewer - reviewing activities

Laurent Andrey: IEEE Transactions on Network and Service Management (TNSM).

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).

Thibault Cholez: IEEE Transactions on Network and Service Management (TNSM), Springer Journal of Network and System Management (JNSM), Wiley International Journal of Network Management (IJNM).

Isabelle Chrisment: IEEE Transactions on Network and Service Management (TNSM).

Jérôme François: IEEE Transactions on Network and Service Management (TNSM), Wiley International Journal of Network Management (IJNM).

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).

10.1.4 Invited talks

Abdelkader Lahmadi gave a tutorial at IEEE/IFIP IM'2021 entitled: Practical security analysis of IoT devices [26].

10.1.5 Leadership within the scientific community

Rémi Badonnel is chair of the IFIP (International Federation for Information Processing) WG6.6 (Working Group 6.6) dedicated to the management of networks and distributed systems.

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

10.1.6 Scientific expertise

Isabelle Chrisment is a member of the AFNIC's Scientific Council.

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

Jérôme François serves as a reviewer for ANRT (CIFRE PhD Thess proposal) and MITACS Canada (PhD and postdoc projects)

10.1.7 Research administration

Isabelle Chrisment is Deputy Scientific Director at Inria in charge of the national scientific domain “Networks, Systems ans Services, Distributed Computing”. She 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.
Abdelkader Lahmadi is the scientific head of the High Security Lab of Nancy.

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

Rémi Badonnel is heading the Internet Systems and Security specialization of the 2$^{\text{nd}}$ and 3$^{\text{rd}}$ years at the TELECOM Nancy engineering school.
Thibault Cholez is in charge of the organization of professional projects for the three years of TELECOM Nancy students in apprenticeship.
Olivier Festor is the Director of the TELECOM Nancy Engineering School.
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, Network Services, Constraint development on small Connected Objects, Mobile applications and Internet of Things, Git - TELECOM Nancy, Université de Lorraine

- **Olivier Festor** 128 hours - L3, M1, M2 - Advanced algorithmics and problem solving, Data Structures and Algorithms, Network security, network management, Devops and SCRUM, Project Management – TELECOM Nancy, Université de Lorraine

- **Isabelle Chrisment** 128 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

- **Abdelkader Lahmadi** 280 hours - L3, M1, M2 - Sensor Networks, Distributed Systems and Algorithms, Algorithms and Advanced Programming, Security of Cyber Physical Systems - ENSEM Engineering School, Université de Lorraine

E-learning

- **MOOC** *Supervision de Réseaux et Services (Session 2)*, FUN Project, Université de Lorraine, Ingénieur, formation initiale et continue, Thibault Cholez, Rémi Badonnel, Laurent Andrey, Olivier Festor, Abdelkader Lahmadi, Jérôme François, the content of the MOOC has been opened to other academic curricula through the FUN CAMPUS platform, in the context of the Covid-19 pandemic situation. Two local sessions have also been organized in 2021 at TELECOM Nancy for students and apprentices.

- **MOOC** *Sécurité des Réseaux Informatiques (Session 2)*, FUN Project, IMT (SudParis et Saint Étienne), Inria (Jérôme François), Université de Lorraine (Isabelle Chrisment). over 5700 registered users from November to December 2021.

- **MOOC** *Becoming a Cyber-Security Consultant (Session 2)*, Concordia Project, Lama Sleem, Rémi Badonnel, and Thibault Cholez, Courses over the coursera MOOC platform, and interactive webinar with practical exercises hosted on the KYPO cyber-range, from October to December 2021.

10.2.2 Supervision

PhD in progress

- Enzo D'Andrea, *Graph-based network data representation for machine learning*, since October 2021, supervised by Olivier Festor & Jérôme François.
- Omar Anser, *Automation of attack mitigations in 5G environments*, since December 2021, supervised by Isabelle Chrisment & Jérôme François.
- Jean-Philippe Eisenbarth, *Securing the future blockchain-based security services*, since May 2019, supervised by Thibault Cholez and Olivier Perrin (Coast team).
- 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.
- Adrien Hemmer, *Predictive Security Monitoring for Large-Scale Internet-of-Things*, since October 2018, supervised by Isabelle Chrisment and Rémi Badonnel.
- Matthews Jose, *Programming model for new flow-based network monitoring*, since January 2019, supervised by Olivier Festor & Jérôme François.
- 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.
- Abir Laraba, *Data-Driven Intelligent Monitoring for Software-Defined Networks*, since October 2018, supervised by Isabelle Chrisment, Raouf Boutaba & Jérôme François.
- Mohamed Oulaaffart, *Automating security enhancement for cloud services*, since January 2020, supervised by Olivier Festor & Rémi Badonnel & Christophe Bianco.
- Mehdi Zakroum, *Forecasting cyberthreats from exogeneous data*, since October 2019, supervised by Isabelle Chrisment & Jérôme François.

PhD defended in 2021

- Mingxiao Ma, *Attack Modelling and Detection in Distributed and Cooperative Controlled Microgrid Systems*, Université de Lorraine, 22 April 2021. Supervised by Isabelle Chrisment & Abdelkader Lahmadi [25].
- Ahmad Abboud, *Efficient Rules Management Algorithms in Software Defined Networking*, Université de Lorraine, 9 December 2021. Supervised by Michael Rusinowitch, Abdelkader Lahmadi, and Adel Bouhoula [24].

10.2.3 Juries

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

- Clément El Baz, PhD in Computer Science from Université Rennes 1 (France). Title: Reacting to N-Day Vulnerabilities in Information Systems, October 2021 – (Olivier Festor as reviewer and Rémi Badonnel as examiner)
- Loïck Bonniot, PhD in Computer Science from Université de Rennes 1 (France). Title: Computer Network Modeling and Root Cause Analysis with Statistical Learning, June 2021 – (Isabelle Chrisment as reviewer)
- Malcolm Bourdon, PhD in Computer Science from Université Fédérale Toulouse Midi-Pyrénées (France). Title: Détection d'intrusion basée sur l'analyse de compteurs matériels pour des objets connectés, July 2021 – (Isabelle Chrisment as reviewer)

- Maissa Dammak, PhD in Computer Science from Université Bourgogne Franche-Comté (France) et Université de la Manouba (Tunisie). Title: Authentication and Authorization Security Solutions for the Internet of Things, July 2021 – (Isabelle Chrisment as examiner)
- David Espinel Sarmiento, PhD in Computer Science from IMT Atlantique (France). Title: Distributing connectivity management in Cloud-Edge infrastructures using SDN-based approaches, September 2021 – - (Isabelle Chrisment as examiner)
- Flavia Salutari, PhD in Computer Science from Institut Polytechnique de Paris (France). Title: Longitudinal, large-scale and unbiased Internet measurements: the users, the Web, the models, September 2021 – (Isabelle Chrisment as president and reviewer)
- Corentin Larroche, PhD in Computer Science from Institut Polytechnique de Paris (France). Title: Network-Wide Intrusion Detection through Statistical Analysis of Event Logs: an Interaction-Centric Approach October 2021 – (Isabelle Chrisment as examiner)
- Kevin Dalleau, PhD in Computer Science from Université de Lorraine (France). Title: Une approche stochastique à base d'arbres aléatoires pour le calcul de dissimilarités : application au clustering pour diverses structures de données, November 2021 – (Isabelle Chrisment as president)
- Anis Ahmed Nacer, PhD in Computer Science from Université de Lorraine (France). Title: Composition sure d'API fondée sur des contrats, November 2021 – (Isabelle Chrisment as president)
- Lamine Noureddine, PhD in Computer Science from Université Rennes 1 (France). Title: Packing detection and classification relying on machine learning to stop malware propagation, December 2021 – (Isabelle Chrisment as examiner)

Team members participated in the following Habilitation Degree committees:

- Yassine HADJADJ-AOUL HDR in Computer Science from Université Rennes 1 (France). Title: Contributions to Resource Management in Next-Generation Networks: from congestion control to services' placement, January 2021 – (Isabelle Chrisment as reviewer)
- Claudia Ignat, HDR in Computer Science from Université de Lorraine (France). Title: Large-scale trustworthy distributed collaboration, April 2021 – (Isabelle Chrisment as president)
- Maciej Korczyński, HDR in Computer Science from Université Grenoble Alpes (France). Title: Traffic Measurements and Data Analysis for DNS Security, December 2021 – (Isabelle Chrisment as reviewer)
- Guillaume Doyen, HDR in Computer Science from Université de Technologie de Troyes (France). Title: Intégration du Comportement des Entités Terminales dans la Disponibilité des Services à Grande Echelle, January 2021 – (Olivier Festor as examiner)
- David Espès, HDR in Computer Science from Université de Bretagne Occidentale (France). Title: Cybersécurité de l'Industrie du Futur : vers une industrie plus résiliente, June 2021 – (Olivier Festor as reviewer)

10.3 Popularization

Lama Sleem, Rémi Badonnel, and Thibault Cholez have contributed to the organization of a cybersecurity awareness week for European high-school students in the context of the teach-the-teachers activities of the CONCORDIA H2020 project.
Rémi Badonnel and Olivier Festor have organized an 1G4.0 hackathon day on the security of industrial systems (including an escape game) targeting decision makers from the industry together with student teams, in the context of the "Pacte Grandes Ecoles" framework supported by the Grand Est Region.
Thibault Cholez helped to organize a webconference event for "La Fabrique Défense" and gave a talk entitled "Vers une cybersécurité européenne : le projet CONCORDIA H2020" to explain how Cybercompetence networks promoted by the European Union, and the CONCORDIA project in particular, are expected to foster and enhance cybersecurity in the upcoming years.

Thibault Cholez led a panel about "Diversity & Cybersecurity: Education for Cybersecurity" in the context of the Women in Cyber initiative of the CONCORDIA project.
Thibault Cholez gave an interview to explain the goal and the main contributions of the CONCORDIA project in the Factuel newsletter of the University of Lorraine.

10.3.1 Articles and contents

Abdelkader Lahmadi contributed to an article about AI and cybersecurity, "Que peut l'IA pour la cybersécurité" in Data Analytics Post.
Abdelkader Lahmadi contributed to an article entitled "Le télescope qui surveille le cyberespace", Journal Le Point, 29 July 2021.

10.3.2 Education

Rémi Badonnel was an invited speaker for a *XLM and Co* podcast on cybersecurity curricula and job profiles (Luxembourg).

10.3.3 Interventions

Abdelkader Lahmadi was an invited speaker at the *A.I. Now* conference 2021 (Metz, France).
Abdelkader Lahmadi was an invited speaker at the *GEN* event 2021 (Metz, France).

11 Scientific production

11.1 Publications of the year

International journals

[1] C. Dad, J.-P. Tavella and S. Vialle. 'Synthesis and feedback on the distribution and parallelization of FMI-CS-based co-simulations with the DACCOSIM platform'. In: *Parallel Computing* 106 (Sept. 2021), p. 102802. DOI: 10.1016/j.parco.2021.102802. URL: https://hal.archives-ouvertes.fr/hal-03468312.

[2] D. Espinel 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*. IEEE Communications Surveys & Tutorials 23.1 (25th Feb. 2021), pp. 256–281. DOI: 10.1109/COMST.2021.3050297. URL: https://hal.archives-ouvertes.fr/hal-03119901.

[3] M. S. Frikha, S. M. Gammar, A. Lahmadi and L. Andrey. 'Reinforcement and deep reinforcement learning for wireless Internet of Things: A survey'. In: *Computer Communications* 178 (Oct. 2021), pp. 98–113. DOI: 10.1016/j.comcom.2021.07.014. URL: https://hal.inria.fr/hal-03409798.

[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* 18.1 (Mar. 2021). DOI: 10.1109/TNSM.2020.3038172. URL: https://hal.inria.fr/hal-03019862.

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

International peer-reviewed conferences

[6] F. Beck, A. Lahmadi and J. François. 'HSL: a Cyber Security Research Facility for Sensitive Data Experiments'. In: DISSECT - 7th IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies. Bordeaux, France, 21st May 2021. URL: https://hal.inria.fr/hal-03245054.

[7] S. R. Chowdhury, R. Boutaba and J. François. 'LINT: Accuracy-adaptive and Lightweight In-band Network Telemetry'. In: *IEEE*. IM 2021 - 17th IFIP/IEEE International Symposium on Integrated Network Management. 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). Bordeaux / Virtual, France, 17th May 2021. URL: https://hal.inria.fr/hal-03525026.

[8] S. Delamare and L. Nussbaum. 'Kwollect: Metrics Collection for Experiments at Scale'. In: CNERT 2021 - Workshop on Computer and Networking Experimental Research using Testbeds. Virtual, United States, 10th May 2021, pp. 1–6. URL: https://hal.inria.fr/hal-03236421.

[9] J.-P. Eisenbarth, T. Cholez and O. Perrin. 'A Comprehensive Study of the Bitcoin P2P Network'. In: BRAINS 2021 - 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services. Paris/ Virtuel, France: IEEE, 27th Sept. 2021, p. 8. URL: https://hal.inria.fr/hal-03380595.

[10] J.-P. Eisenbarth, T. Cholez and O. Perrin. 'An open measurement dataset on the Bitcoin P2P Network'. In: IM 2021 - 17th IFIP/IEEE International Symposium on Integrated Network Management. Bordeaux / Virtual, France, 17th May 2021, p. 5. URL: https://hal.inria.fr/hal-03244771.

[11] P. Graff, X. Marchal, T. Cholez, S. Tuffin, B. Mathieu and O. Festor. 'An Analysis of Cloud Gaming Platforms Behavior under Different Network Constraints'. In: HiPNet 2021 - 3rd International Workshop on High-Precision, Predictable, and Low-Latency Networking. Workshops of the 17th International Conference on Network and Service Management (CNSM21). Izmir (Virtual), Turkey: IEEE, 25th Oct. 2021, p. 7. URL: https://hal.inria.fr/hal-03421031.

[12] A. Hemmer, M. Abderrahim, R. Badonnel and I. Chrisment. 'An Ensemble Learning-Based Architecture for Security Detection in IoT Infrastructures'. In: CNSM 2021 - 17th International Conference on Network and Service Management. Izmir (Virtual), Turkey, 25th Oct. 2021. URL: https://hal.inria.fr/hal-03460779.

[13] M. Jose, K. Lazri, J. François and O. Festor. 'InREC: In-network REal Number Computation'. In: *IEEE*. IM 2021 - 17th IFIP/IEEE International Symposium on Integrated Network Management. 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). Bordeaux / Virtual, France, 17th May 2021. URL: https://hal.inria.fr/hal-03525052.

[14] M. Jose, K. Lazri, J. François and O. Festor. 'Leveraging in-network real-value computation for home network device recognition'. In: *IEEE*. IM 2021 - IFIP/IEEE International Symposium on Integrated Network Management (Demo). 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). Bordeaux / Virtual, France, 17th May 2021. URL: https://hal.inria.fr/hal-03525070.

[15] P.-M. Junges, J. François and O. Festor. 'Inferring Software Composition and Credentials of Embedded Devices from Partial Knowledge'. In: CNSM 2021 - 17th International Conference on Network and Service Management. Izmir/virtual, Turkey, 26th Oct. 2021. URL: https://hal.inria.fr/hal-03470012.

[16] P.-M. Junges, J. François and O. Festor. 'Software-based Analysis of the Security by Design in Embedded Devices'. In: IM 2021 - 17th IFIP/IEEE International Symposium on Integrated Network Management. Bordeaux / Virtual, France, 17th May 2021. URL: https://hal.inria.fr/hal-03469993.

[17] M. Oulaaffart, R. Badonnel and O. Festor. 'Towards Automating Security Enhancement for Cloud Services'. In: IM 2021 - 17th IFIP/IEEE International Symposium on Integrated Network Management. Lyon / Virtuel, France, 17th May 2021. URL: https://hal.inria.fr/hal-03454868.

[18] S. Ricci, V. Janout, S. Parker, J. Jerabek, J. Hajny, A. Chatzopoulou and R. Badonnel. 'PESTLE Analysis of Cybersecurity Education'. In: ARES 2021 - 16th International Conference on Availability, Reliability and Security. Vienna, Austria: ACM, 17th Aug. 2021, pp. 1–8. DOI: 10.1145/3465481.3469184. URL: https://hal.inria.fr/hal-03518393.

[19] M. Said Frikha, S. Mettali Gammar and A. Lahmadi. 'Multi-Attribute Monitoring for Anomaly Detection: a Reinforcement Learning Approach based on Unsupervised Reward'. In: PEMWN 2021 - 10th IFIP International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks. Waterloo, Canada, 23rd Nov. 2021. URL: https://hal.inria.fr/hal-03506409.

Scientific book chapters

[20] N. Schnepf, R. Badonnel, A. Lahmadi and S. Merz. 'Automated Orchestration of Security Chains Driven by Process Learning'. In: *Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning*. 1. Wiley, 12th Oct. 2021. DOI: 10.1002/9781119675525.ch12. URL: https://hal.inria.fr/hal-03518390.

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

[21] R. Badonnel, C. Fung, S. Scott-Hayward, Q. Li, J. Zhang and C. Hesselman. *Guest Editors' Introduction: Special Issue on Latest Developments for Security Management of Networks and Services*. Vol. 18. 2. IEEE, June 2021, pp. 1120–1124. DOI: 10.1109/TNSM.2021.3079189. URL: https://hal.inria.fr/hal-03518395.

[22] A. Lahmadi, E. Bertin and R. Li. *BRAINS 2020 special issue: Blockchain research and applications for innovative networks and services*. Wiley, 12th Oct. 2021. DOI: 10.1002/nem.2189. URL: https://hal.inria.fr/hal-03409796.

[23] N. Zincir-Heywood and R. Badonnel. *CNSM 2019 special issue: Embracing the new wave of artificial intelligence*. Vol. 31. 1. Wiley, Jan. 2021. DOI: 10.1002/nem.2149. URL: https://hal.inria.fr/hal-03518397.

Doctoral dissertations and habilitation theses

[24] A. Abboud. 'Efficient Rules Management Algorithms in Software Defined Networking'. Université de Lorraine, 9th Dec. 2021. URL: https://hal.inria.fr/tel-03508140.

[25] M. Ma. 'Attack Modelling and Detection in Distributed and Cooperative Controlled Microgrid Systems'. Université de Lorraine, 22nd Apr. 2021. URL: https://hal.univ-lorraine.fr/tel-03356948.

Other scientific publications

[26] A. Lahmadi and F. Beck. *Practical security analysis of IoT devices*. Bordeaux, France, 17th May 2021. URL: https://hal.inria.fr/hal-03363567.

11.2 Cited publications

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

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

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