Activity Report 2019

Team RESIST

Resilience and Elasticity for Security and ScalabiliTy of dynamic networked systems

Inria teams are typically groups of researchers working on the definition of a common project, and objectives, with the goal to arrive at the creation of a project-team. Such project-teams may include other partners (universities or research institutions).

RESEARCH CENTER
Nancy - Grand Est

THEME
Networks and Telecommunications

Table of contents

Team RESIST

Creation of the Team: 2018 January 01

Keywords:

Computer Science and Digital Science:

A1.1.4. - High performance computing
A1.1.8. - Security of architectures
A1.1.13. - Virtualization
A1.2. - Networks
A1.3. - Distributed 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
A4.9. - Security supervision

Other Research Topics and Application Domains:

B5. - Industry of the future
B6.3.2. - Network protocols
B6.3.3. - Network Management
B6.4. - Internet of things
B6.5. - Information systems
B6.6. - Embedded systems
B9.8. - Reproducibility

1. Team, Visitors, External Collaborators

Research Scientists

Raouf Boutaba [Waterloo Univ, Inria, Univ de Lorraine (LUE), Inria Internationale Chair and Professor]
Jérôme François [Inria, Researcher]

Faculty Members

Isabelle Chrisment [Team leader, Univ de Lorraine, Professor, HDR]
Laurent Andrey [Univ de Lorraine, Associate Professor]
Rémi Badonnel [Univ de Lorraine, Associate Professor]
Thibault Cholez [Univ de Lorraine, Associate Professor]
Abdelkader Lahmadi [Univ de Lorraine, Associate Professor]
Olivier Festor [Univ de Lorraine, Professor, HDR]
Lucas Nussbaum [Univ de Lorraine, Associate Professor]

Post-Doctoral Fellows
Cherifa Dad [Univ de Lorraine, ATER, until Aug 2019]
Luke Bertot [Inria, from Oct 2019]

PhD Students
Abdulqawi Saif [Univ de Lorraine, ATER]
Ahmad Abboud [Numeryx Technologies, granted by CIFRE]
Pierre-Olivier Brissaud [Thales, granted by CIFRE until Jun 2019, Inria from Jul 2019]
Paul Chaignon [Orange Labs, until Jan 2019]
Jean-Philippe Eisenbarth [Univ de Lorraine, from May 2019]
Adrien Hemmer [Inria]
Matthews Jose [Orange Labs, granted by CIFRE, from Jan 2019]
Pierre-Marie Junges [Univ de Lorraine]
Abir Laraba [Univ de Lorraine]
Mingxiao Ma [CNRS]
Xavier Marchal [CNRS, until Jul 2019]
Nicolas Schnepf [Inria, until Sep 2019]
Mehdi Zakroum [Univ de Lorraine, from Oct 2019]

Technical staff
Mohamed Abderrahim [Inria, from Jun 2019]
Soline Blanc [Inria]
Antoine Chemardin [Inria]
Thomas Lacour [Inria]
Alexandre Merlin [Inria]
Nicolas Perrin [Inria, Engineer, from Oct 2019]

Interns and Apprentices
Samer Abou Jaoude [Inria, from Mar 2019 until May 2019]
Leila Dada [Inria, from Mar 2019 until Jul 2019]
Tristan de Paola [Univ de Lorraine, from Jun 2019 until Aug 2019]
Jean Francois Elhadji Diame [Inria, from Jun 2019 until Aug 2019]
Mohamed Said Frikha [Univ de Lorraine, from Apr 2019 until Nov 2019]
Philippe Graff [Inria, from Sep 2019]
Clement Guidi [Univ de Lorraine, from Jun 2019 until Jul 2019]
Tarek Nsiri [Univ de Lorraine, from Jun 2019 until Sep 2019]

Administrative Assistants
Isabelle Herlich [Inria]
Sylvie Musili [Univ. Lorraine]

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 loosing control to other stakeholders, particularly to Over-the-Top (OTT) content and service providers. Therefore, the delivery of Internet services has increased in complexity to mainly cope with the diversity and exponential growth of network traffic both at the core and at the edge. Intermediate players are multiplying and each of them has been proposing solutions to enhance service access performance.

In the Internet landscape, no single entity can claim a complete view of Internet topology and resources. Similarly, a single authority cannot control all interconnection networks and cloud data centers to effectively manage them and **provide reliable and secure services** to end users and devices at scale. The **lack of clear visibility into Internet operations** is exacerbated by the increasing use of encryption solutions [1] which contributes to traffic opacity.

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 [46], [43]. Scalability must be ensured across multiple dimensions to face of order of magnitude: more users, devices, contents and applications.

- **Security:** Security has gained a lot of popularity 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) [48] 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.

[1] http://www.arcep.fr/uploads/tx_gsavis/15-0832.pdf, accessed on 09/06/2017

- **Resilience** refers to the ability of a system to **adapt itself when facing challenging situations**. It is reasonable to assume that any system may face an attack for which protection mechanisms may fail. A comprehensive approach to resilience that considers not only the network and system resources but also the supported users and applications brings both benefits and challenges since users and applications can be very diverse, ephemeral and mobile. Applications are also deployed in dynamic environments like cloud platforms and are frequently reconfigured.

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

3. Research Program

3.1. Overview

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

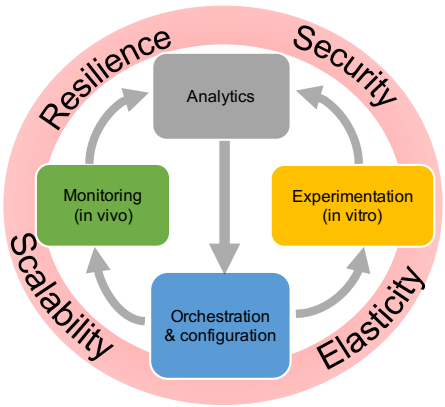

Figure 1. The Resist project

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

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

3.2. Monitoring

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

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

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

Crowd-sourcing and third-party involvement are gaining in popularity, paving the way for massively distributed and collaborative monitoring. We thus investigate opportunistic mobile crowdsensing in order to collect user activity logs along with contextual information (social, demographic, professional) to effectively measure end-users' **Quality of Experience**. However, collaborative monitoring raises serious concerns regarding trust and sensitive data sharing (open data). Data anonymization and sanitization need to be carefully addressed.

3.3. Experimentation

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

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

We are playing a central role in the development of the Grid'5000 testbed [44] and our objective is to reinforce our collaborations with other testbeds, towards a **testbed federation** in order to enable experiments to scale to multiple testbeds, providing a diverse environment reflecting the Internet itself.

Moreover, our research focuses on extending the infrastructure virtualization capabilities of our Distem [47] emulator, which provides a flexible software-based experimental environment.

Finally, methodological aspects are also important for ensuring **trustworthy and reproducible experiments**, and raises many challenges regarding testbed design, experiment description and orchestration, along with automated or assisted provenance data collection [45].

3.4. Analytics

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

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

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

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

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

3.5. Orchestration

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

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

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

4. Application Domains

4.1. Internet

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

From a security perspective, **monitoring and analysing Internet traffic is an important part of threat prevention and predictive security**. Indeed, large network telescopes like the one we use in the High Security Laboratory[2] allow detecting world-wide campaigns of attacks which target a specific exploit in some applications. Moreover the monitoring of the Internet traffic at the **edge** is the best way to quickly detect distributed attacks like DDoS and to mitigate them before they become effective. However, the Internet traffic analysis is made much more complicated since the **massive shift towards encryption** that happened few years ago, which requires new traffic classification methods.

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

4.2. SDN and Data-Center Networks

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

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**.

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

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 guarentee 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 embed 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

5.1. Highlights of the Year

The impact of the RESIST team in network and service management community has been highly recognized and awarded this year in recognition of their exceptional contributions and leadership in this research area.

- R. Badonnel has been elected as the chair of the IFIP (International Federation for Information Processing) WG6.6 (Working Group 6.6).
- J. François has been appointed as co-chair of NMRG (Network Management Research Group) of IRTF (Internet Research Task Force).
- T. Cholez gets involved in the new H2020 European project Concordia (section 9.3.1.4).

5.1.1. Awards

- O. Festor has received the *Dan Stokesberry award*.
- J. François has received the *IEEE Young Professional in Network and Service Management award*.

6. New Software and Platforms

6.1. Distem

KEYWORDS: Large scale - Experimentation - Virtualization - Emulation

FUNCTIONAL DESCRIPTION: Distem is a distributed systems emulator. When conducting research on Cloud, P2P, High Performance Computing or Grid systems, it can be used to transform an homogenenous cluster (composed of identical nodes) into an experimental platform where nodes have different performance, and are linked together through a complex network topology, making it the ideal tool to benchmark applications targetting such environments, or aiming at tolerating performance degradations or variations which are frequent in the Cloud or in other applications distributed at large scale (P2P for example).

RELEASE FUNCTIONAL DESCRIPTION: New features in Distem 1.3 include: (1) New network emulation parameters: loss, duplication, corruption, reordering and jitter, (2) Support for Debian Stretch, (3) Added many tests, (4) Moved project from GForge to GitHub (https://github.com/madynes/distem).

NEWS OF THE YEAR: New version 1.3

- Participants: Luc Sarzyniec, Lucas Nussbaum and Tomasz Buchert
- Partners: CNRS - Université de Lorraine - Loria - Grid'5000 - Inria
- Contact: Lucas Nussbaum
- URL: http://distem.gforge.inria.fr

6.2. Grid'5000

Grid'5000 testbed

KEYWORDS: HPC - Cloud - Big data - Testbeds

FUNCTIONAL DESCRIPTION: The Grid'5000 experimental platform is a scientific instrument to support computer science research related to distributed systems, including parallel processing, high performance computing, cloud computing, operating systems, peer-to-peer systems and networks. It is distributed on 10 sites in France and Luxembourg. Grid'5000 is a unique platform as it offers to researchers many and varied hardware resources and a complete software stack to conduct complex experiments, ensure reproducibility and ease understanding of results.

NEWS OF THE YEAR: This year's highlights include the TILECS workshop, and various improvements (update to Debian 10, several new clusters including the addition of 72 GPUs, etc.). More information on https://www.grid5000.fr/w/News

- Participants: Christian Pérez, David Loup, Frédéric Desprez, Laurent Lefèvre, Laurent Pouilloux, Marc Pinhède, Simon Delamare, Lucas Nussbaum, Teddy Valette and Alexandre Merlin
- Contact: Lucas Nussbaum
- URL: https://www.grid5000.fr/

6.3. SCUBA

A Tool Suite for the automated security assessment of IoT environments

KEYWORDS: Cybersecurity - Internet of things - Machine learning - Artificial intelligence

FUNCTIONAL DESCRIPTION: IoT devices are used in different fields of application, not only for the general public, but also in industrial environments. SCUBA is tool suite for the security assessment of industrial and general public IoT devices. It mainly relies on collected information through passive and active scanning of a running IoT device in its exploitation environment to build its Security Knowledge Base (SKB). The knowledge base contains all relevant information of the device regarding its network communications extracted from PCAP files, the enumeration of its used hardware and software represented in the CPE (Common Platform Enumeration) format, the list of its known vulnerabilities in the CVE (Common Vulnerabilities and Exposures) format associated to their CWE (Common Weakness Enumeration) and CAPEC (Common Attack Pattern Enumeration and Classification) descriptions. The SKB is used by SCUBA to predict the intrusion chains associated to an IoT device and its environment. SCUBA tries to be as automated as possible to face the large scale and the great heterogeneity of IoT networks.

NEWS OF THE YEAR: First release

- Participants: Abdelkader Lahmadi, Frédéric Beck, Thomas Lacour and Jérôme François
- Contact: Abdelkader Lahmadi

6.4. Platforms

6.4.1. CPS Security Assessment Platform

NEWS OF THE YEAR :

During 2019, we have extended our IoT (Internet of Things) and CPS (Cyber-Physical Systems) security assessment platform with more IoT devices dedicated to home networks (Alexa and Google Home voice assistants, smart door bell, smart door lock, alarm system). The platform is used for several demonstrations and it is extensively used for the development carried on the SCUBA (see 6.3) tool suite to automate the assessment of the security of IoT and SCADA systems by using ML/AI methods.

- Participants: Abdelkader Lahmadi, Frédéric Beck, Thomas Lacour and Jérôme François
- Contact: Abdelkader Lahmadi

7. New Results

7.1. Monitoring

7.1.1. Encrypted Traffic Analysis

Participants: Jérôme François [contact], Pierre-Olivier Brissaud, Pierre-Marie Junges, Isabelle Chrisment, Thibault Cholez, Olivier François, Olivier Bettan [Thales].

Nowadays, most of Web services are accessed through HTTPS. While preserving user privacy is important, it is also mandatory to monitor and detect specific users' actions, for instance, according to a security policy. Our paper [4] presents a solution to monitor HTTP/2 traffic over TLS. It highly differs from HTTP/1.1 over TLS traffic what makes existing monitoring techniques obsolete. Our solution, H2Classifier, aims at detecting if a user performs an action that has been previously defined over a monitored Web service, but without using any decryption. It is thus only based on passive traffic analysis and relies on random forest classifier. A challenge is to extract representative values of the loaded content associated to a Web page, which is actually customized based on the user action. Extensive evaluations with five top used Web services demonstrate the viability of our technique with an accuracy between 94% and 99%.

We were also interested by Internet of Things (IoT) as related devices become widely used and their control is often provided through a cloud-based web service that interacts with an IoT gateway, in particular for individual users and home automation. Therefore, we propose a technique demonstrating that is possible to infer private user information, i.e., actions performed, by considering a vantage point outside the end-user local IoT network. By learning the relationships between the user actions and the traffic sent by the web service to the gateway, we have been able to establish elementary signatures, one for each possible action, which can be then composed to discover compound actions in encrypted traffic. We evaluated the efficiency of our approach on one IoT gateway interacting with up to 16 IoT devices and showed that a passive attacker can infer user activities with an accuracy above 90%. This work has been published in [16] and is related to the H2020 SecureIoT project (section 9.3.1.2).

7.1.2. Predictive Security Monitoring for Large-Scale Internet-of-Things

Participants: Jérôme François [contact], Rémi Badonnel, Abdelkader Lahmadi, Isabelle Chrisment, Adrien Hemmer.

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

In that context, we have proposed a process mining approach, that is capable to cope with a variety of devices and protocols, for supporting IoT predictive security [14]. We have described the underlying architecture and its components, and have formalized the different phases related to this solution, from the building of behavioral models to the detection of misbehaviors and potential attacks. The pre-processing identifies the states characterizing the IoT-based system, while process mining methods elaborate behavioral models that are compatible with the heterogeneity of protocols and devices [26]. These models are then exploited to analyze monitoring data at runtime and detect misbehaviors and potential attacks preventively. Based on a proof-of-concept prototype, we have quantified the detection performances, as well as the influence of time splitting and clustering techniques. The experimental results clearly show the benefits of our solution combining process mining and clustering techniques. As future work, we are interested in comparing it to other alternative learning techniques, as well as in evaluating to what extent the generated alerts can be exploited to drive the activation of counter-measures.

This work has been achieved in the context of the H2020 SecureIoT project (section 9.3.1.2).

7.1.3. Monitoring of Blockchains' Networking Infrastructure

Participants: Thibault Cholez [contact], Jean-Philippe Eisenbarth, Olivier Perrin.

With the raise of blockchains, their networking infrastructure becomes a critical asset as more and more money and services are made on top of them. However, they are largely undocumented and may be prone to performance issues and severe attacks so that the question of the resiliency of their overlay network arises. With regard to the state of the art on P2P networks security, the fact that a service infrastructure is distributed is not sufficient to assess its reliability, as many bias (for instance, if nodes are concentrated in a given geographical location) and attacks (eclipse, Sybil or partition attacks) are still possible and may severely disturb the network.

Overall, according to the scientific literature, the security provided by the proof of work consensus and the huge size of the main public blockchains seem to protect them well from large scale attacks (51% attack, selfish mining attack, etc.) whose cost to be successful becomes prohibitive and often exceeds the expected gain. However, rather than only focusing on the application level, an attacker could rather try to disturb the underlying P2P network to weaken the consensus in some specific parts of the blockchain network to gain advantage. Our current work uses a third-party crawler to get an accurate view of the Bitcoin overlay network. We are currently analyzing the data with graph theory metrics to identify possible anomalies or flaws that could be exploited by attackers.

7.1.4. Quality of Experience Monitoring

Participants: Isabelle Chrisment [contact], Antoine Chemardin, Frédéric Beck, Lakhdar Meftah [University of Lille], Romain Rouvoy [University of Lille].

We carried on our collaboration with the SPIRALS team (Inria/Université de Lille). Even though mobile crowdsourcing allows industrial and research communities to build realistic datasets, it can also be used to track participants' activity and to collect insightful reports from the environment (e.g., air quality, network quality). While data anonymization for mobile crowdsourcing is commonly achieved *a posteriori* on the server side, we have proposed a decentralized approach, named Fougere [19], which introduces an *a priori* data anonymization process. In order to validate our privacy preserving proposal, two testing frameworks (ANDROFLEET and PEERFLEET [20]) have been designed and implemented. They allows developers to automate reproducible testing of nearby peer-to-peer (P2P) communications.

In the context of both ANR BottleNet (section 9.2.1.1) and IPL BetterNet (section 9.2.5.1) projects, we continued to work on our open measurement platform for the quality of mobile Internet access (i.e., setup and manage the backend infrastructure for data collection and analysis). This platform is hosted by the High Security Laboratory [3] located at Inria Nancy Grand-Est. A collect campaign has been performed with a small set of volunteer users selected by the INSEAD-Sorbonne Université Behavioural Lab [4].

7.2. Experimentation

This section covers our work on experimentation on testbeds (mainly Grid'5000), on emulation (mainly around the Distem emulator), and on Reproducible Research.

7.2.1. Grid'5000 Design and Evolutions

Participants: Benjamin Berard [SED], Luke Bertot, Alexandre Merlin, Lucas Nussbaum [contact], Nicolas Perrin, Patrice Ringot [SISR LORIA], Teddy Valette [SED].

The team was again heavily involved in the evolutions and the governance of the Grid'5000 testbed.
Technical team management. Since the beginning of 2017, Lucas Nussbaum serves as the *directeur technique* (CTO) of Grid'5000 in charge of managing the global technical team (10 FTE). He is also a member of the *Bureau* of the GIS Grid'5000.
SILECS project. We are also heavily involved in the ongoing SILECS project, that aims to create a new infrastructure on top of the foundations of Grid'5000 and FIT in order to meet the experimental research needs of the distributed computing and networking communities.
SLICES ESFRI proposal. At the European level, we are involved in a ESFRI proposal submission. We submitted a *Design Study* project in November 2019, and are in the final stages of submitting the ESFRI proposal itself in early 2020.
TILECS workshop. We participated in the organization of the TILECS workshop. TILECS (*Towards an Infrastructure for Large-Scale Experimental Computer Science*, https://www.silecs.net/tilecs-2019/) gathered about 80 members (mostly faculty) of the testbeds designers and users community in France, to discuss the future plans for research infrastructures in the networking and distributed computing fields. During that workshop, Lucas Nussbaum presented Grid'5000 [32].
Group storage. A technical contribution from the team is the addition of a *group storage* service that allows groups of users to share data, with improved security and performance compared to what was previously available.
Support for Debian 10. Another notable technical contribution from the team is the work of Teddy Valette on supporting Debian 10 in the set of Grid'5000 system environments made available to users.

[3] https://lhs.loria.fr
[4] https://www.insead.edu/centres/insead-sorbonne-universite-lab-en

New clusters available in Nancy: graffiti, gros, grue. Finally, the team was also heavily involved in the purchase and installation of several new clusters in the Nancy site, gathering funding from CPER LCHN, CPER Entreprises, MULTISPEECH team, LARSEN team. This greatly increases the resources available locally, both for GPUs (graffiti and grue), and for large-scale experiments (gros).

7.2.2. Involvement in the Fed4FIRE Testbeds Federation

Participants: Luke Bertot, Lucas Nussbaum [contact].

In the context of the Fed4FIRE+ project (section 9.3.1.1), Grid'5000 was officially added to the Fed4FIRE federation at the beginning of 2019. In 2019, we implemented on-demand *stitching* between Grid'5000 experiments and other testbeds of the federation (through VLANs provided by GEANT and RENATER), allowing experiments that combine resources from Grid'5000 and other testbeds [27]. We are also improving our implementation of an SFA Aggregate Manager in order to allow the use of Grid'5000 through Fed4FIRE tools, such as the jFed GUI.
We also worked on the issue of classifying and presenting the set of testbeds available in the federation. This was the subject of a presentation at the GEFI collaboration workshop [31].

7.2.3. I/O Emulation Support in Distem

Participants: Alexandre Merlin, Abdulqawi Saif, Lucas Nussbaum [contact].

We finished the work on adding I/O emulation support in Distem, in order to experiment how Big Data solution can handle degraded situations [22].

7.2.4. Distributing Connectivity Management in Cloud-Edge infrastructures

Participant: Lucas Nussbaum [contact].

In the context of David Espinel's PhD (CIFRE Orange, co-supervised with Adrien Lebre and Abdelhadi Chari), we worked on distributing connectivity management in Cloud-Edge infrastructures [38]. The classic approach of deploying large data centers to provide Cloud services is being challenged by the emerging needs of Internet of Things applications, Network Function Virtualization services or Mobile edge computing. A massively distributed Cloud-Edge architecture could better fit the requirements and constraints of these new trends by deploying on-demand Infrastructure as a Service in different locations of the Internet backbone (i.e, network point of presences). A key requirement in this context is the establishment of connectivity among several virtual infrastructure managers in charge of operating each site. In this work, we analyzed the requirements and challenges raised by the inter-site connectivity management in a Cloud-Edge infrastructure.

7.2.5. NDN Experimentation

Participants: Thibault Cholez [contact], Xavier Marchal, Olivier Festor.

While ICN is a promising technology, we currently lack experiments carrying real user traffic. This also highlights the difficulty of making the link between the new NDN world and the current IP world. To address this issue, we designed and implemented an HTTP/NDN gateway (composed of ingress and egress gateways) that can seamlessly transport the traffic of regular web users over an NDN island, making them benefit from the good properties of the protocol to deliver content (request mutualization, caching, etc.). The gateway itself is part of a wider architecture that aims to use NFV to deploy NDN and benefit from its orchestration capability to address performance and security issues inherent to new network architectures.

To validate the whole architecture, a testbed involving real users was made. The gateway was used by dozens of users for a few weeks to prove that running a NDN network over NFV is a viable solution to address the transition between both worlds. Users accessed many websites through the NDN network in a very satisfying way. The results have been published in IEEE Communications Magazine [5].

7.3. Analytics

7.3.1. CPS Security Analytics

Participants: Abdelkader Lahmadi [contact], Mingxiao Ma, Isabelle Chrisment.

During 2019, we evaluated a novel type of attack, named Measurement as Reference attack (MaR), on the cooperative control and communication layers in microgrids, where the attacker targets the communication links between distributed generators (DGs) and manipulates the reference voltage data exchanged by their controllers. We assessed its impact on reference voltage synchronization at the different control layers of a microgrid. Results and the development of an experimental platform are presented in [18] to demonstrate this attack, in particular the maximum voltage deviation and inaccurate reference voltage synchronization it causes in a microgrid. ML algorithms are also applied on the collected datasets from this platform for the detection of this attack.

7.3.2. Optimal and Verifiable Packet Filtering in Software-Defined Networks

Participants: Abdelkader Lahmadi [contact], Ahmad Abboud, Michael Rusinowitch [Pesto team], Miguel Couceiro [Orpailleur team], Adel Bouhoula [Numeryx].

Packet filtering is widely used in multiple networking appliances and applications, in particular, to block malicious traffic (protection of network infrastructures through firewalls and intrusion detection systems). It is also widely deployed on routers, switches and load balancers for packet classification. This mechanism relies on the packet's header fields to filter such traffic by using range rules of IP addresses or ports. However, the set of packet filters has to handle a growing number of connected nodes and many of them are compromised and used as sources of attacks. For instance, IP filter sets available in blacklists may reach several millions of entries, and may require large memory space for their storage in filtering appliances. In [40], [39], we proposed a new method based on a double mask IP prefix representation together with a linear transformation algorithm to build a minimized set of range rules. We have formally defined the double mask representation over range rules and proved that the number of required masks for any range is at most $2w-4$, where w is the length of a field. This representation makes the network more secure, reliable and easier to maintain and configure. We show empirically that the proposed method achieves an average compression ratio of 11% on real-life blacklists and up to 74% on synthetic range rule sets. Finally, we add support of double mask into a real SDN network.

7.3.3. Port Scans Analysis

Participants: Jérôme François [contact], Frederic Beck, Sofiane Lagraa [University of Luxembourg], Yutian Chen [Telecom Nancy], Laurent Evrard [University of Namur], Jean-Noël Colin [University of Namur].

TCP/UDP port scanning or sweeping is one of the most common technique used by attackers to discover accessible and potentially vulnerable hosts and applications. Although extracting and distinguishing different port scanning strategies is a challenging task, the identification of dependencies among probed ports is primordial for profiling attacker behaviors, with as a final goal to better mitigate them. In [6], we proposed an approach that allows us to track port scanning behavior patterns among multiple probed ports and identify intrinsic properties of observed group of ports. Our method is fully automated and based on graph modeling and data mining techniques including text mining. It provides to security analysts and operators relevant information about services that are jointly targeted by attackers. This is helpful to assess the strategy of the attacker, such that understanding the types of applications or environment she targets. We applied our method to data collected through a large Internet telescope (or Darknet).

In addition, we decided to leverage this knowledge for improving data analysis techniques applied to network traffic monitoring. Network traffic monitoring is primordial for network operations and management for many purposes such as Quality-of-Service or security. However, one major difficulty when dealing with network traffic data (packets, flows...) is the poor semantic of individual attributes (number of bytes, packets, IP addresses, protocol, TCP/UDP port number...). Many attributes can be represented as numerical values but cannot be mapped to a meaningful metric space. Most notably are application port numbers. They are numerical but comparing them as integers is meaningless. In [13], [12], we propose a fine grained attacker behavior-based network port similarity metric allowing traffic analysis to take into account semantic relations between port numbers. The behavior of attackers is derived from passive observation of a Darknet or telescope, aggregated in a graph model, from which a semantic dissimilarity function is defined. We demonstrated the veracity of this function with real world network data in order to pro-actively block 99% of TCP scans.

7.4. Orchestration

7.4.1. Mutualization of Monitoring Functions in Edge Computing

Participants: Jérôme François [contact], Mohamed Abderrahim [Orange Labs], Meryem Ouzzif [Orange Labs], Karine Guillouard [Orange Labs], Adrien Lebre [STACK Inria team, IMT Atlantique], Charles Prud'Homme [IMT Atlantique], Xavier Lorca [IMT Mines Albi, France].

By relying on small sized and massively distributed infrastructures, the edge computing paradigm aims at supporting the low latency and high bandwidth requirements of the next generation services that will leverage IoT devices (e.g., video cameras, sensors). To favor the advent of this paradigm, management services, similar to the ones that made the success of cloud computing platforms, should be proposed. However, they should be designed in order to cope with the limited capabilities of the resources that are located at the edge. In that sense, they should mitigate as much as possible their footprint. Among the different management services that need to be revisited, we investigated in [10] the monitoring one. Monitoring functions tend to become compute-, storage-and network-intensive, in particular because they will be used by a large part of applications that rely on real-time data. To reduce as much as possible the footprint of the whole monitoring service, we proposed to mutualize identical processing functions among different tenants while ensuring their quality-of-service (QoS) expectations. We formalized our approach as a constraint satisfaction problem and show through micro-benchmarks its relevance to mitigate compute and network footprints.

This work has been achieved in the context of the Inria-Orange joint lab (section 9.2.2.1).

7.4.2. Software-Defined Security for Clouds

Participants: Rémi Badonnel [contact], Olivier Festor, Maxime Compastié.

Cloud infrastructures provide new facilities to build elaborated added-value services by composing and configuring a large variety of computing resources, from virtualized hardware devices to software products. They are however further exposed to security attacks than traditional environments. We have pursued our efforts on a software-defined security strategy based on the TOSCA language, in order to support the protection of cloud resources using unikernel techniques [11]. This language enables the specification of cloud services and their orchestration. We have extended it to drive the integration and configuration of security mechanisms within cloud resources, at the design and operation phases, according to different security levels. We rely on unikernel techniques to elaborate cloud resources using a minimal set of libraries, in order to reduce the attack surface. We have designed a framework to interpret this extended language and to generate and configure protected unikernel virtual machines, in accordance with contextual changes. The adaptation is typically performed through the regeneration of protected unikernel virtual machines in a dynamic manner. We have quantified the benefits and limits of this approach through extensive series of experiments. As future work, we are interested in investigating security issues specifically related to cloud resource migrations, and evaluating to what extent our hardening techniques can be complemented by security chains.

This word has been achieved in the context of the Inria-Orange joint lab (section 9.2.2.1).

7.4.3. Chaining of Security Functions

Participants: Rémi Badonnel [contact], Abdelkader Lahmadi, Stephan Merz, 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 continued our efforts on the orchestration and verification of security chains, in collaboration with Stephan Merz from the VeriDis project-team at Inria Nancy, and concretized with the PhD defense of Nicolas Schnepf in September 2019 [3]. In particular, we have proposed this year an approach for automating the merging of security chains in software-defined networks [24]. This method complements the inference-based generation techniques that we proposed in [9]. The merging algorithms are designed to compose several security chains into a single one, in order to minimize the number of security functions and rules, while preserving the semantics of the

initial chains. The algorithms have been implemented in Python and have been integrated into a proof-of-concept prototype that also contains the learning and inference components [23]. The performance of this implementation has been evaluated through extensive experiments. In particular, we have compared different approaches to merging security chains in terms of the complexity of the resulting chains, their accuracy, and the overhead incurred in computing the combined chains. The proposed solution is able to minimize the number of security functions and rules. It also facilitates the building of security chains at runtime, through a decoupling from the generation of individual chains.

7.4.4. Software-Defined Traffic Engineering to Absorb Influx of Network Traffic

Participants: Jérôme François [contact], Abdelkader Lahmadi, Romain Azais [MOSAIC team], Benoit Henry [IMT Lille Douai], Shihabur Chowdhury [University of Waterloo], Raouf Boutaba [University of Waterloo].

Existing shortest path-based routing in wide area networks or equal cost multi-path routing in data center networks do not consider the load on the links while taking routing decisions. As a consequence, an influx of network traffic stemming from events such as distributed link flooding attacks and data shuffle during large scale analytics can congest network links despite the network having sufficient capacity on alternate paths to absorb the traffic. This can have several negative consequences, service unavailability, delayed flow completion, packet losses, among others. In this regard and under the context of NetMSS associate team (section 9.4.1.1), we proposed SPONGE [15], a traffic engineering mechanism for handling sudden influx of network traffic. SPONGE models the network as a stochastic process, takes the switch queue occupancy and traffic rate as inputs, and leverages the multiple available paths in the network to route traffic in a way that minimizes the overall packet loss in the network. We demonstrated the practicality of SPONGE through an OpenFlow based implementation, where we periodically and pro-actively reroute network traffic to the routes computed by SPONGE. Mininet emulations using real network topologies show that SPONGE is capable of reducing packet drops by 20% on average even when the network is highly loaded because of an ongoing link flooding attack.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

- Thales (Palaiseau, France):
  - CIFRE PhD (Pierre-Olivier Brissaud, supervised by Isabelle Chrisment and Jérôme François)
  - Encrypted network traffic analysis (HTTP2 over TLS)
- Orange Labs (Issy-Les-Moulineaux, France):
  - CIFRE PhD (Paul Chaignon, supervised by Olivier Festor and Jérôme François)
  - Software Datapaths for Multi-Tenant Packet Processing
- Orange Labs (Issy-Les-Moulineaux, France):
  - CIFRE PhD (Matthews Jose, supervised by Olivier Festor and Jérôme François)
  - Complex arithmetic operation for in-network computing using hardware dataplanes
- Numeryx Technologies (Paris, France):
  - CIFRE PhD (Ahmad Abboud, supervised by Michael Rusinowitch, Abdelkader Lahmadi and Adel Bouhoula)
  - Compressed and Verifiable Filtering Rules in Software-defined Networking

9. Partnerships and Cooperations

9.1. Regional Initiatives

Olivier Festor is leading the Grand Est PACTE initiative on cyber-security. This initiative led to a total funding of 400 K€ to acquire, develop and operate the first Cyber Range in the Grand Est. This unique equipment is deployed at TELECOM Nancy and serves as the main platform for cyber-security training in the Grand Est region for both civil and military staff.

9.2. National Initiatives

9.2.1. ANR

9.2.1.1. ANR BottleNet

Participants: Isabelle Chrisment [contact], Antoine Chemardin, Thibault Cholez.

- Acronym: BottleNet
- Title: Understanding and Diagnosing End-to-End Communication Bottlenecks of the Internet
- Coordinator: Inria
- Duration: October 2015 - extended to September 2020
- Others Partners: Inria Muse, Inria Diana, Lille1 University, Telecom Sud-Paris, Orange, IP-Label.
- Abstract: The Quality of Experience (QoE) when accessing the Internet, on which more and more human activities depend on, is a key factor for today's society. The complexity of Internet services and of users' local connectivity has grown dramatically in the last years with the proliferation of proxies and caches at the core and access technologies at the edge (home wireless and 3G/4G access), making it difficult to diagnose the root causes of performance bottlenecks. The objective of BottleNet is to deliver methods, algorithms, and software systems to measure end-to-end Internet QoE and to diagnose the cause of the experienced issues. The result can then be used by users, network and service operators or regulators to improve the QoE.

9.2.1.2. ANR FLIRT

Participants: Rémi Badonnel [contact], Olivier Festor, Thibault Cholez, Jérôme François, Abdelkader Lahmadi, Laurent Andrey.

- Acronym: FLIRT
- Title: Formations Libres et Innovantes Réseaux et Télécoms
- Coordinator: Institut Mines-Télécom (Pierre Rolin)
- Duration: January 2016-Décembre 2020
- Others Partners: TELECOM Nancy, Institut Mines-Télécom, Airbus, Orange, the MOOC Agency, Isograd
- Site: http://flirtmooc.wixsite.com/flirt-mooc-telecom
- Abstract: FLIRT (Formations Libres et Innovantes Réseaux & Télécom) is an applied research project leaded by the Institut Mines-Télécom, for an (extended) duration of 5 years. It includes 14 academic partners (engineering schools including Telecom Nancy), industrial partners (Airbus, Orange) and innovative startups (the MOOC agency, and Isograd). The project is to build a collection of 10 MOOCs (Massive Open Online Courses) in the area of networks and telecommunications, three training programmes based on this collection, as well as several innovations related to pedagogical efficiency (such as virtualization of practical labs, management of student cohorts, and adaptative assessment). The RESIST team is leading a working group dedicated to the building and operation of a MOOC on network and service management. This MOOC covers the fundamental concepts, architectures and protocols of the domain, as well as their evolution in the context of future Internet (e.g. network programming, flow monitoring). It corresponds to a training program of 5 weeks. The main targeted skills are to understand the challenges of network and service management, to know the key methods and techniques related to this area, and to get familiar with the usage and parameterization of network management solutions.

9.2.1.3. ANR MOSAICO

Participants: Thibault Cholez [contact], Olivier Festor.

- Acronym: MOSAICO
- Title: Multi-layer Orchestration for Secured and low lAtency applICatiOns
- Coordinator: Orange Labs
- Start: 01/12/2019
- Duration: 4 years
- Others Partners: Orange Labs, Montimage, ICD-UTT
- Abstract:

  For several years, programmability has become increasingly important in network architectures. The last trend is to finely split services into micro-services. The expected benefits relies on an easier development and maintenance, better quality, scalability and responsiveness to new scenarios than monolithic approaches, while offering more possibilities for operators and management facilities through orchestration. As a consequence, it appears that network functions, such as routing, filtering, etc. can be split in several micro-services, implemented through different means, according to the software environments, and at different topological locations, thus opening the way to fully end-to-end programmable networks. This need for multi-level and multi-technology orchestration is even more important with the emergence of new services, such as immersive services, which exhibit very strong quality of service constraints (i.e. latency cannot exceed a few milliseconds), while preserving end-to-end security. The MOSAICO project proposes to design, implement and validate a global and multi-layer orchestration solution, able to control several underlying network programmability technologies (SDN, NFV, P4) to compose micro-services forming the overall network service. To reach this objective, the project will follow an experimental research methodology in several steps including the definition of the micro-services and of the global architecture, some synthetic benchmarking, the design of orchestration rules and the evaluation against the project use-case of a low latency network application.

  The kick-off meeting of MOSAICO took place the 03/12/2019 in Orange Gardens. Our current work consists in surveying the latest technologies around NFV and Open Networking.

9.2.2. Inria joint Labs

9.2.2.1. Inria-Orange Joint Lab

Participants: Jérôme François [contact], Olivier Festor, Matthews Jose, Paul Chaignon.

- Acronym: IOLab
- Title: Inria - Orange Joint Laboratory
- Duration: September 2015 - August 2020
- Abstract: The challenges addressed by the Inria-Orange joint laboratory relate to the virtualization of communication networks, the convergence between cloud computing and communication networks, and the underlying software-defined infrastructures. Our work concerns in particular monitoring methods for software-defined infrastructures, and management strategies for supporting software-defined security in multi-tenant cloud environnements.

9.2.3. Technological Development Action (ADT)

9.2.3.1. ADT SCUBA

Participants: Abdelkader Lahmadi [Contact], Jérôme François, Thomas Lacour, Frédéric Beck.

- Acronym: SCUBA
- Duration: January 2018-January 2020

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

9.2.4. FUI

9.2.4.1. FUI PACLIDO

Participants: Abdelkader Lahmadi [contact], Mingxiao Ma, Isabelle Chrisment, Jérôme François.

- Acronym: PACLIDO
- Title: Lightweight Cryptography Protocols and Algorithms for IoT (Protocoles et Algorithmes Cryptographiques Légers pour l'Internet des Objets)
- Coordinator: ADS (Airbus Defence and Space)
- Duration: September 2017- August 2020
- Others Partners: Sophia Conseil, Université de Limoges, Cea tech, Trusted Objects, Rtone, Saint Quentin En Yvelines.
- Abstract: The goal of PACLIDO is to propose and develop lightweight cryptography protocols and algorithms to secure IoT communications between devices and servers. The implemented algorithms and protocols will be evaluated in multiple use cases including smart home and smart city applications. PACLIDO develops in addition an advanced security monitoring layer using machine learning methods to detect anomalies and attacks while traffic is encrypted using the proposed algorithms.

9.2.5. Inria Project Lab

9.2.5.1. IPL BetterNet

Participants: Isabelle Chrisment [contact], Antoine Chemardin, Frederic Beck, Thibault Cholez.

- Acronym: BetterNet
- Coordinator: RESIST (Isabelle Chrisment)
- Duration: October 2016-August 2020
- Others Partners: Inria MiMove, Inria Diana, Inria Spirals, Inria Dionysos, ENS-ERST and IP-Label
- Site: https://project.inria.fr/betternet
- Abstract: BetterNet's goal is to build and deliver a scientific and technical collaborative observatory to measure and improve the Internet service access as perceived by users. We will propose new user-centered measurement methods, which will associate social sciences to better understand Internet usage and the quality of services and networks. Tools, models and algorithms will be provided to collect data that will be shared and analyzed to offer valuable service to scientists, stakeholders and the civil society.

9.2.5.2. IPL Discovery

Participant: Lucas Nussbaum [contact].

- Coordinator: Adrien Lebre (STACK)
- End: June 2019
- Site: http://beyondtheclouds.github.io
- Others Partners: Orange, RENATER
- Abstract: To accommodate the ever-increasing demand for Utility Computing (UC) resources, while taking into account both energy and economical issues, the current trend consists in building larger and larger Data Centers in a few strategic locations. Although such an approach enables UC providers to cope with the actual demand while continuing to operate UC resources through a centralized software system, it is far from delivering sustainable and efficient UC infrastructures for future needs.

The DISCOVERY initiative aims at exploring a new way of operating Utility Computing (UC) resources by leveraging any facilities available through the Internet in order to deliver widely distributed platforms that can better match the geographical spread of users as well as the ever increasing demand. Critical to the emergence of such locality-based UC (also referred as Fog/Edge Computing) platforms is the availability of appropriate operating mechanisms. The main objective of DISCOVERY is to design, implement, demonstrate and promote a new kind of Cloud Operating System (OS) that will enable the management of such a large-scale and widely distributed infrastructure in an unified and friendly manner.

9.3. European Initiatives

9.3.1. H2020 Projects

9.3.1.1. Fed4Fire+ (2017-2022)

Title: Federation for FIRE Plus

Program: H2020

Duration: January 2017 - December 2021

Coordinator: Interuniversitair Micro-Electronica centrum Imec VZW

Partners:
Universidad de Malaga; National Technical University of Athens - NTUA; The Provost, Fellows, Foundation Scholars & the other members of board of the College of the Holy & Undivided Trinity of Queen Elizabeth Near Dublin; Ethniko Kentro Erevnas Kai Technologikis Anaptyxis; GEANT LImited; Institut Jozef Stefan; Mandat International Alias Fondation Pour la Cooperation Internationale; Universite Pierre et Marie Curie - Paris 6; Universidad De Cantabria; Fundacio Privada I2CAT, Internet I Innovacio Digital A Catalunya; EURESCOM-European Institute For Research And Strategic Studies in Telecommunications GMBH; Nordunet A/S; Technische Universitaet Berlin; Instytut Chemii Bioorganicznej Polskiej Akademii Nauk; Fraunhofer Gesellschaft zur Foerderung Der Angewandten Forschung E.V.; Universiteit Van Amsterdam; University of Southampton; Martel GMBH; Atos Spain SA; Institut National de Recherche en Informatique et automatique.

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

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

9.3.1.2. SecureIoT

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

Duration: December 2017 - December 2020

Coordinator: INTRASOFT International SA

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

Inria contact: Jérôme François

Url : http://secureiot.eu

Abstract: SecureIoT is a a joint effort of global leaders in IoT services and IoT cybersecurity to secure the next generation of dynamic, decentralized IoT systems, that span multiple IoT platforms and networks of smart objects, through implementing a range of predictive IoT security services. SecureIoT will integrate its security services in three different application scenarios in the areas of: Digital Automation in Manufacturing (Industry 4.0), Socially assistive robots for coaching and healthcare and Connected cars and Autonomous Driving.

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

9.3.1.3. SPARTA

Title: Strategic programs for advanced research and technology in Europe

Program: H2020

Duration: February 2019 - January 2022

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

Partners: see web site

Inria contact: Jérôme François

Url : http://www.sparta.eu

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

SPARTA is a novel cybersecurity competence network, with the objective to collaboratively develop and implement top-tier research and innovation actions. Strongly guided by concrete challenges forming an ambitious Cybersecurity Research & Innovation Roadmap, SPARTA will tackle 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 will push the boundaries to deliver advanced solutions to cover emerging issues, with applications from basic human needs to economic activities, technologies, and sovereignty.

9.3.1.4. CONCORDIA

Participants: Thibault Cholez [contact], Rémi Badonnel, Olivier Festor.

Acronym: CONCORDIA

Title: Cyber security cOmpeteNCe fOr Research anD InnovAtion

Program: H2020

Start: 01/01/2019

Duration: 4 years

Coordinator: Research Institute CODE (Munich, Germany)

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

Url : https://www.concordia-h2020.eu/

Abstract: CONCORDIA is one of the 4 pilot projects whose goal is to structure and develop a network of cybersecurity competences across Europe. CONCORDIA has a research program to develop next-generation cybersecurity solutions by taking a holistic end-to-end data-driven approach from data acquisition, data transport and data usage, and addressing device-centric, network-centric, software-centric, system-centric, data-centric and user-centric security. The solutions will be integrated in sector-specific (vertical) and cross-sector (horizontal) industrial pilots with building incubators. Vertical pilots include Telecom, Finance, e-Health, Defence and e-Mobility, while horizontal pilots are about two European-scale federated platforms that are the DDoS clearing house and the Threat Intelligence platform . CONCORDIA also develops a CONCORDIA ecosystem by providing lab infrastructures, platforms, tools as "Living Labs" as well as advanced cybersecurity courses on cyber-ranges.

The project kick-off took place in Munich the 28/01/2019. The team is mainly involved in three tasks (research, education and European dimension). On the research side, we begun our work on assessing the reliability of blockchains' networking infrastructure (see section 7.1.3). Regarding the education in cybersecurity, we set up a cyber-range at TELECOM Nancy which was officially launched the 24/09/2019 and is already used by our M1 and M2 students to be trained in cybersecurity. We worked also for the task "Liaison with stakeholders" and were in particular the main editor of the 1st year deliverable of this task.

9.4. International Initiatives

9.4.1. Inria Associate Teams Not Involved in an Inria International Labs

9.4.1.1. NetMSS

Title: NETwork Monitoring and Service orchestration for Softwarized networks

International Partner (Institution - Laboratory - Researcher):

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

Start year: 2018

Duration: 3 years

See also: https://team.inria.fr/netmss/

Evolution towards softwarized networks are greatly changing the landscape in networking. In the last years, effort was focused on how to integrate network elements in cloud-based models. This lead 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 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 new methods to be efficiently handled. For example, monitoring softwarized networks necessitates the collection of heterogeneous information, regarding the network but also cloud resources, from many locations. Targeting such a holistic monitoring will then support better decision algorithms, to be applied in a scalable and efficient manner, taking advantage of the advanced capabilities in terms of network configuration and programmability. In addition, real-time constraints in networking are very strong due to the transient nature of network traffic and are faced with high throughputs, especially in data-center networks where softwarization primarily takes place. Therefore, the associate team will promote (1) line-rate and accurate monitoring and (2) efficient resource uses for service orchestration leveraging micro-services.

9.4.2. Inria International Partners

9.4.2.1. Declared Inria International Partners

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

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

Abir Laraba: international PhD grant in cooperation with University of Waterloo

Mehdi Zakroum: international PhD grant in cooperation with International University of Rabat

9.4.2.2. Informal International Partners

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

9.4.3. Participation in Other International Programs

9.4.3.1. ThreatPredict

- Title: ThreatPredict, From Global Social and Technical Big Data to Cyber Threat Forecast
- Coordinator: Inria
- Duration: December 2017 - November 2020
- Others Partners: International University of Rabat (IUR), Carnegie Mellon University
- Funding: North Atlantic Treaty Organization
- Abstract: Predicting attacks can help to prevent them or at least reduce their impact. Nowadays, existing attack prediction methods make accurate predictions only hours in advance or cannot predict geo-politically motivated attacks. ThreatPredict aims to predict different attack types days in advance. It develops machine-learning algorithms that capture the spatio-temporal dynamics of cyber-attacks and global social, geo-political and technical events. Various sources of information are collected, enriched and correlated such as honeypot data, darknet, GDELT, Twitter, and vulnerability databases. In addition to warning about attacks, this project will improve our understanding of the effect of global events on cyber-security.

9.5. International Research Visitors

9.5.1. Visits of International Scientists

Professor Adel Bouhoula from SUP'COM (Tunisia) from June 2019 until July 2019 in collaboration with PESTO team to develop methods for optimal and verifiable security policies for software-defined networks.

Dashi Kondo, Assistant Professor in Osaka Prefecture University for two weeks in November 2019 to develop new scientific cooperation on network security.

9.5.1.1. Internships

Anthony Samer Abou Jaoude, from March 2019 until May 2019.

Tarek Nsiri, from June 2019 until September 2019.

9.5.2. Visits to International Teams

9.5.2.1. Research Stays Abroad

Abdelkader Lahmadi visited the team of Professor Raouf Boutaba in the University of Waterloo for two weeks during the month of June 2019. During this visit, he provided an IEEE seminar on the topic of Self-Driving Networks.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events: Organisation

10.1.1.1. General Chair, Scientific Chair

Olivier Festor: IEEE Conference on Network Softwarization (NetSoft 2019), general co-chair.

Isabelle Chrisment: IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2020), general co-chair.

10.1.1.2. Member of the Organizing Committees

Laurent Andrey: IEEE Conference on Network Softwarization (NetSoft 2019), web chair.

Rémi Badonnel: IEEE International Symposium on Integrated Network Management (IM 2019); IFIP International Conference on Networking (Networking 2020); IEEE/IFIP Network Operations and Management Symposium (NOMS 2020).

Olivier Festor: IEEE International Symposium on Integrated Network Management (IM 2019), member of the steering committee & Publications co-chair; IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), tutorial co-chair; IFIP International Conference on Networking (Networking 2020), patrons co-chair.

Thibault Cholez: IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2020).

Isabelle Chrisment: Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2019), member of the steering committee.

Jérôme François: Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2019), member of the steering committee; IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2019), demonstration co-chair.

Abdelkader Lahmadi : IEEE International Symposium on Integrated Network Management (IM 2019), co-chair of the workshop HotNSM; IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), publicity co-chair.

Lucas Nussbaum: TILECS workshop.

10.1.2. Scientific Events: Selection

10.1.2.1. Chair of Conference Program Committees

Rémi Badonnel: IEEE/IFIP/In Coop. with ACM SIGCOMM International Conference on Network and Service Management (CNSM 2019), technical program committee co-chair; IEEE International Symposium on Integrated Network Management (IM 2019), experience program committee co-chair; IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), experience program committee co-chair.

Olivier Festor: IEEE International Symposium on Integrated Network Management (IM 2019), Tutorial chair; IEEE Conference on Network Softwarization (NetSoft 2019), Technical Program Committee co-chair; IEEE/IFIP/In Coop. with ACM SIGCOMM International Conference on Network and Service Management (CNSM 2019).

Isabelle Chrisment: IFIP, in-cooperation with ACM SIGCOMM Network Traffic Measurement and Analysis Conference (TMA 2019).

Jérôme François: IEEE International Symposium on Integrated Network Management (IM 2019); IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2019); IEEE Workshop on Emerging Trends in Softwarized Networks (ETSN 2019).

10.1.2.2. Member of the Conference Program Committees

Laurent Andrey: IEEE Conference on Network Softwarization (NetSoft 2019).

Rémi Badonnel: IEEE/IFIP/In Coop. with ACM SIGCOMM International Conference on Network and Service Management (CNSM 2019); IEEE International Symposium on Integrated Network Management (IM 2019); IEEE Conference on Network Softwarization (NetSoft 2019); IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2019); IEEE Global Information Infrastructure and Networking Symposium (GIIS 2019); IEEE International Conference on Communications (ICC 2020); IEEE/IFIP Network Operations and Management Symposium (NOMS 2020).

Isabelle Chrisment: IEEE/IFIP/In Coop. with ACM SIGCOMM International Conference on Network and Service Management (CNSM 2019); IEEE International Symposium on Integrated Network Management (IM 2019); IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2019); Rencontres Francophones sur la Conception de Protocoles, l'Évaluation de Performance et l'Expérimentation des Réseaux de Communication (CoRes 2019); IEEE/IFIP Network Operations and Management Symposium (NOMS 2020); ACM/IEEE International Conference on Internet of Things Design and Implementation (IoTDI 2020);

Thibault Cholez: IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2019); IEEE International Conference on Cloud Networking (CloudNet 2019); IEEE International Symposium on Integrated Network Management (IM 2019); IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2019); IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2block 2019); IEEE/IFIP Network Operations and Management Symposium (NOMS 2020).

Olivier Festor: IEEE/IFIP/In Coop. with ACM SIGCOMM International Conference on Network and Service Management (CNSM 2019); IEEE International Symposium on Integrated Network Management (IM 2019); IEEE Conference on Network Softwarization (NetSoft 2019); IEEE/IFIP Network Operations and Management Symposium (NOMS 2020); IEEE/IFIP/In Coop. with ACM SIGCOMM International Conference on Network and Service Management (CNSM 2020); IEEE Conference on Network Softwarization (NetSoft 2020); IFIP International Conference on Networking (Networking 2020).

Jérôme François: IFIP, in-cooperation with ACM SIGCOMM Network Traffic Measurement and Analysis Conference (TMA 2019); IEEE INFOCOM Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2019); Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2019); IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2block 2019).

Abdelkader Lahmadi: IEEE INFOCOM Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2019); IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2block 2019); IEEE/IFIP Network Operations and Management Symposium (NOMS 2020); IEEE International Symposium on Integrated Network Management (IM 2019); IEEE Conference on Network Softwarization (NetSoft 2019); Cyber Security in Networking Conference (CSNet 2019); IEEE Workshop on Emerging Trends in Softwarized Networks (ETSN 2019).

Lucas Nussbaum: International Conference on Enabling Technologies: Infrastructure for Collaborative Entreprises (WETICE 2019); 39th IEEE International Conference on Distributed Computing System (ICDCS 2019); 16th International Conference on Mining Software Repositories (MSR 2019 – FOSS award); 11th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2019). 5th International Workshop on Serverless Computing (WoSC 2019); 54th IEEE International Conference on Communications (ICC) – NGNI Symposium; IEEE Global Information Infrastructure and Networking Symposium (GIIS 2019).

10.1.2.3. Reviewer

The permanent team members made many reviews for the conferences the team is involved in.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

Rémi Badonnel: Associate Editor for the Wiley International Journal of Network Management (IJNM), Associate Editor for the Springer Journal of Network and System Management (JNSM)and guest editor for the IEEE Transactions on Network and Service Management (TNSM).

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

Abdelkader Lahmadi : Associate Editor for the Wiley International Journal of Network Management (IJNM)and Guest Editor for a special issue of Springer Journal of Network and System Management (JNSM).

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

10.1.3.2. Reviewer - Reviewing Activities

Rémi Badonnel: IEEE Transactions on Network and Service Management (TNSM), IEEE Journal on Selected Areas in Communications (JSAC), Springer Journal of Network and System Management (JNSM), IEEE Communications Magazine (COMMAG), Wiley International Journal of Network Management (IJNM) and Elsevier Journal of Industrial Information Integration (JIII).

Thibault Cholez: IEEE Transactions on Network and Service Management (TNSM), IEEE Communications Magazine (COMMAG), Elsevier Journal on Communication Networks (COMNET)and SIGCOMM Computer Communication Review.

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

Laurent Andrey: Springer Journal of Network and System Management (JNSM) and Wiley International Journal of Network Management (IJNM).

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

Abdelkader Lahmadi : IEEE Transactions on Network and Service Management (TNSM), IEEE Journal on Selected Areas in Communications (JSAC), Wiley International Journal of Network Management (IJNM), Springer Journal of Network and System Management (JNSM), IEEE Communications Magazine (COMMAG) and Elsevier Journal Computer Communications (COMCOM).

Lucas Nussbaum: International Journal of Grid and Utility Computing (IJGUC).

10.1.4. Invited Talks

Abdelkader Lahmadi provided a keynote on "Toward Self-driving Networks: Network Management and Security Challenges" in the IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT), 8 April, 2019, Washington D.C., USA.

Isabelle Chrisment provided a talk on "Experimentation in Cybersecurity: from Requirements to Platforms" in the TILECS (Towards an Infrastructure for Large-Scale Experimental Computer Science) workshop, 3-4 July 2019, Grenoble, France.

Olivier Festor gave a keynote on the coupling of Information Centric Networks and Programmable Networks at the Orange Network of the Future workshop in may 2019. He also gave a talk at the Distinguished Experts Panel of IEEE/IFIP IM'2019 in Washington on Intelligent Management and gave a short invited presentation entitled "Opening the Network for More Secure Services" at the SecSoft 2019 workshop in Paris on June 24th, 2019.

10.1.5. Leadership within the Scientific Community

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

Isabelle Chrisment has been a co-chair of the Allistene cybersecurity working group, whose main goal is to help drive the French cybersecurity research and innovation.

Olivier Festor is a member of the IEEE/IFIP NISC (NOMS IM Stering Committee) which manages the set of conferences in the area of network and service management for both IEE and IFIP scientific communities worldwide.

Jérôme François has been appointed as co-chair of NMRG (Network Management Research Group) of IRTF (Internet Research Task Force).

10.1.6. Scientific Expertise

Isabelle Chrisment served as an expert of the HCERES (High Council for Evaluation of Research and Higher Education) committee for the LISTIC Laboratory. She was a member of the GDR RSD/ASF selection committee for the thesis award. She is also a member of the AFNIC's Scientific Council.

Abdelkader Lahmadi served as reviewer for ANRT (CIFRE PhD). Abdelkader Lahmadi has contributed to the writing of a document about the protection of critical infrastructures in transport and energy within the working group "enjeux 2025" of CoFIS (Comité de la Filière industrielle de sécurité).

Olivier Festor is a member of the Scientific Council of Orange and Director of TELECOM Nancy, the graduate Engineering School of Computer Science at the University of Lorraine. He is also contributing to the HCERES national scientific evaluation board.

Jérôme François and Rémi Badonnel serve as reviewers for ANRT (CIFRE PhD). Jérôme François is in the advisory board of the Interreg TERMINAL project (2019-2021).

10.1.7. Research Administration

Thibault Cholez is a member of the executive council of the Digitrust project (I-Site project of the Université de Lorraine to foster research on trust and security in IT).

Isabelle Chrisment is also an elected member of the scientific pole AM2I (Automatique, Mathématiques, Informatique et leurs Interaction) at Université de Lorraine. She is a member of the COMIPERS at Inria Nancy Grand Est. She is also involved in the CMI (Commission de la Mention Informatique) board, which is a part of the doctoral school IAEM.

Abdelkader Lahmadi is a member of the CDT of Inria Nancy Grand Est.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Olivier Festor is the Director of the TELECOM Nancy Engineering School.

Rémi Badonnel is heading the Internet Systems and Security specialization of the 2^{nd} and 3^{rd} years at the TELECOM Nancy engineering school, and is coordinating the Security Pathway Program at the same school, elaborated in the context of the International Master of Science in Security of Computer Systems built with the Mines Nancy school.

Thibault Cholez is in charge of the organization of professional projects for the three years of TELECOM Nancy students in apprenticeship.

Team members are teaching the following courses:

Rémi Badonnel 242 hours - L3, M1, M2 - Networks, Systems and Services, Software Design and Programming, Cloud Computing, Network and Security Management - TELECOM Nancy, Université de Lorraine

Thibault Cholez 290 hours - L3, M1, M2 - Computer Networks, Object-Oriented Programming, Network Services, Constraint development on small Connected Objects, Mobile applications and Internet of Things, IT tools for Project Management - TELECOM Nancy, Université de Lorraine

Isabelle Chrisment 220 hours -L3, M1, M2 -C and Shell Programming, Computer Networking, Operating Systems, Network Security. - TELECOM Nancy, Université de Lorraine

Jérôme François 70 hours - M1, M2 -Network security, Big Data - TELECOM Nancy, Université de Lorraine

Abdelkader Lahmadi 280 hours - L3, M1, M2 - Real time and Embedded Systems Programming, Distributed Systems and Algorithms, Green IT, Algorithms and Advanced Programming, Security of Cyber Physical Systems - ENSEM Engineering School, Université de Lorraine

Lucas Nussbaum 200 hours - L2, Licence Pro (L3), M1 - several courses about systems administration, monitoring, virtualization, configuration management, networking, operating systems. - IUT Nancy-Charlemagne

E-learning

MOOC *Supervision de Réseaux et Services (Session 2)*, FUN Project, Université de Lorraine, Ingénieur, formation initiale et continue, Thibault Cholez, Rémi Badonnel, Laurent Andrey, Olivier Festor, Abdelkader Lahmadi, Jérôme François, January-March 2019, over 6000 from 77 countries, and 347 certificates of achievement. Each MOOC Resist participant contributed to the 2019 maintenance for a third opening on January 2020.

10.2.2. Supervision

PhD in progress: Ahmad Abboud, *Compressed and verifiable filtering rules in Software-defined Networking*, since September 2018, supervised by Michael Rusinowitch, Abdelkader Lahmadi, and Adel Bouhoula.

PhD in progress: Pierre-Olivier Brissaud, *Encrypted traffic analysis*, since July 2016, supervised by Isabelle Chrisment, Jérôme François and Thibault Cholez.

PhD in progress: Jean-Philippe Eisenbarth, *Securing the future blockchain-based security services*, since May 2019, supervised by Thibault Cholez and Olivier Perrin (Coast team).

PhD in progress: David Espinel, *SDN solution for Massively Distributed Cloud Infrastructure*, since February 2018, supervised by Lucas Nussbaum, Adrien Lebre and Abdelhadi Chari.

PhD in progress: Adrien Hemmer, *Predictive Security Monitoring for Large-Scale Internet-of-Things*, since October 2018, supervised by Isabelle Chrisment and Rémi Badonnel.

PhD in progress: Pierre-Marie Junges, *Internet-wide automated assessment of the exposure of the IoT devices to security risks*, since October 2018 supervised by Olivier Festor and Jérôme François.

PhD in progress: Mingxiao Ma, *Cyber-Physical Systems defense through smart network configuration*, since Novemeber 2017, supervised by Isabelle Chrisment, Abdelkader Lahmadi.

PhD in progress: Abdulqawi Saif, *Open Science for the scalability of a new generation search technology*, since December 2015, supervised by Ye-Qiong Song & Lucas Nussbaum.

PhD in progress: Matthews Jose, *Programming model for new flow-based network monitoring*, since January 2019, supervised by Olivier Festor & Jérôme François.

PhD in progress: Data-Driven Intelligent Monitoring for Software-Defined Networks, *Programming model for new flow-based network monitoring*, since October 2018, supervised by Isabelle Chrisment, Raouf Boutaba & Jérôme François.

PhD in progress: Abir Laraba, *Data-Driven Intelligent Monitoring for Software-Defined Networks*, since October 2018, supervised by Isabelle Chrisment, Raouf Boutaba & Jérôme François.

PhD in progress: Mehdi Zakroum, *Forecasting cyberthreats from exogeneous data*, since October 2019, supervised by Isabelle Chrisment & Jérôme François.

PhD: Paul Chaignon, *Software Datapaths for Multi-Tenant Packet Processing*, supervised by Olivier Festor, Jérôme François and Kahina Lazri [1].

PhD: Xavier Marchal, Secure operation of virtualized Named Data Networks, supervised by Olivier Festor & Thibault Cholez [2].

PhD: Nicolas Schnepf, *Orchestration and Verification of Security Functions for Smart Environments*, supervised by Stephan Merz, Rémi Badonnel and Abdelkader Lahmadi [3].

PhD: Lakhdar Meftah, *Towards Privacy-sensitive Mobile Crowdsourcing*, supervised by Romain Rouvoy (University of Lille) and Isabelle Chrisment.

10.2.3. Juries

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

- Damien Crémilleux, PhD in Computer Science from CentraleSupélec, Rennes, France. Title: Visualization for information system security monitoring, February 2019 – (Isabelle Chrisment as president).
- Philippe Pittoli, PhD in Computer Science from the University of Strasbourg, France.Title: Influence d'une architecture de type maître-esclave dans les problématiques de l'Internet des Objets. May 2019 – (Isabelle Chrisment as reviewer).
- Kallol Krishna Karmakar, PhD in Computer Science from the University of Newcastle, Australia. Title: Techniques for Securing Software Defined Networks and Services, June 2019 – (Isabelle Chrisment as reviewer).
- Pierre-Marie Bajan, Phd in Computer Science from Télécom SudParis, France. Title: Simulation d'attaque et d'activité : application à la cyber-défense, July 2019 – (Isabelle Chrisment as examiner).
- Muhammad Jawad Khokhar, PhD in Computer Science from the University of Nice-Sophia Antipolis, France. Title: Modeling Quality of Experience of Internet Video Streaming by Controlled Experimentation and Machine Learning, October 2019 - (Isabelle Chrisment as examiner).
- François Boutigny, Phd in Computer Science from Télécom SudParis, France. Title: Multidomain Virtual Network Embedding under Security-oriented Requirements applied to 5G Networks Slices, November 2019 – (Isabelle Chrisment as examiner).
- Fetia Bannour, PhD in Computer Science and Electrical Engineering from the Paris-Est Créteil University, France. Title: Contributions pour le contrôle distribué dans les réseaux SDN, November 2019 - (Olivier Festor as reviewer).
- Danilo Cerovic, PhD in Computer Science from Sorbonne Université, Paris, France. Title: Architecture réseau résiliente et hautement performante pour les datacenters virtualisés, February 2019 - (Olivier Festor as reviewer).

Team members participated to the following Habilitation Degree committees:

- Nozar Kheir, Habilitation Degree in Computer Science from Université Paris-Saclay, France. Title : From Cyber-secure to Cyber-resilient Computer Systems - The way forward, May 2019 - (Olivier Festor as reviewer).

10.3. Popularization

10.3.1. Articles and contents

Abdelkader Lahmadi and Frédéric Beck provided a podcast about the security of connected devices available at Interstices (https://interstices.info/des-outils-pour-evaluer-la-securite-des-objets-connectes/)

Thibault Cholez gave an interview for the *factuel* (newsletter of the University of Lorraine) to present the H2020 project CONCORDIA (https://factuel.univ-lorraine.fr/node/11394). He also wrote a blog entry entitled "Assessing blockchains' network infrastructure: why it matters for cybersecurity" for the CONCORDIA website (https://www.concordia-h2020.eu/blog-post/assessing-blockchains-network-infrastructure-why-it-matters-for-cybersecurity/).

Isabelle Chrisment contributed to the ARCEP Report entitled "The State of the Internet in France", June 2019, page 19, https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet-2019-270619.pdf (French version) or https://en.arcep.fr/uploads/tx_gspublication/report-state-internet-2019-eng-270619.pdf (English version).

Jérôme François has been interviewed by France 3 Lorraine to present how cyberthreat can be predicted in the context of ThreatPredict (section 9.4.3.1). He also gave an introduction to network security in the context of FAN (https://fan.inria.fr/)

10.3.2. Education

Isabelle Chrisment participated in the SNT (Sciences Numériques et Technologie) MOOC, more especially in the design of a video entitled "Internet IP, a universal protocol?" in the module "Internet and Networks. The SNT MOOC is a FUN Project dedicated to the teachers in high schools to help them within the context of the high school reform.

10.3.3. Internal action

Jérôme François presented ThreatPredict (section 9.4.3.1) at the “Café des Sciences” in Inria Rocquencourt Center.

11. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] P. CHAIGNON. *Software Datapaths for Multi-Tenant Packet Processing*, Université de Lorraine, May 2019, https://hal.univ-lorraine.fr/tel-02315651

[2] X. MARCHAL. *Architectures and advanced functions for a progressive deployment of Information-Centric Networking*, Université de Lorraine, June 2019, https://hal.univ-lorraine.fr/tel-02315611

[3] N. SCHNEPF. *Orchestration and verification of security functions for smart devices*, Université de Lorraine, September 2019, https://hal.univ-lorraine.fr/tel-02351769

Articles in International Peer-Reviewed Journals

[4] P.-O. BRISSAUD, J. FRANÇOIS, I. CHRISMENT, T. CHOLEZ, O. BETTAN. *Transparent and Service-Agnostic Monitoring of Encrypted Web Traffic*, in "IEEE Transactions on Network and Service Management", September 2019, vol. 16, n^{o} 3, pp. 842-856 [*DOI :* 10.1109/TNSM.2019.2933155], https://hal.inria.fr/hal-02316644

[5] G. DOYEN, T. CHOLEZ, W. MALLOULI, B. MATHIEU, H.-L. MAI, X. MARCHAL, D. KONDO, M. AOUADJ, A. PLOIX, E. MONTES DE OCA, O. FESTOR. *An Orchestrated NDN Virtual Infrastructure transporting Web Traffic: Design, Implementation and First Experiments with Real End-Users*, in "IEEE Communications Magazine", June 2019, vol. 57, n^{o} 6 [*DOI :* 10.1109/MCOM.2019.1800730], https://hal.inria.fr/hal-02353861

[6] S. LAGRAA, Y. CHEN, J. FRANÇOIS. *Deep Mining Port Scans from Darknet*, in "International Journal of Network Management", February 2019, https://hal.inria.fr/hal-02403715

[7] D. MARS, S. METTALI GAMMAR, A. LAHMADI, L. AZOUZ SAIDANE. *Using Information Centric Networking in Internet of Things: A Survey*, in "Wireless Personal Communications", March 2019, vol. 105, n^{o} 1, pp. 87-103 [*DOI :* 10.1007/s11277-018-6104-8], https://hal.inria.fr/hal-02393632

[8] T. NGUYEN, H.-L. MAI, R. COGRANNE, G. DOYEN, W. MALLOULI, L. NGUYEN, M. EL AOUN, E. MONTES DE OCA, O. FESTOR. *Reliable Detection of Interest Flooding Attack in Real Deployment of Named Data Networking*, in "IEEE Transactions on Information Forensics and Security", September 2019, vol. 14, n^{o} 9, pp. 2470-2489 [*DOI :* 10.1109/TIFS.2019.2899247], https://hal.archives-ouvertes.fr/hal-02068457

[9] N. SCHNEPF, R. BADONNEL, A. LAHMADI, S. MERZ. *Rule-Based Synthesis of Chains of Security Functions for Software-Defined Networks*, in "Electronic Communications of the EASST", 2019, vol. 076, https://hal.inria.fr/hal-02397981

Invited Conferences

[10] M. ABDERRAHIM, M. OUZZIF, K. GUILLOUARD, J. FRANÇOIS, A. LEBRE, C. PRUD'HOMME, X. LORCA. *Efficient Resource Allocation for Multi-tenant Monitoring of Edge Infrastructures*, in "PDP 2019 - 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing", Pavie, Italy, 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, IEEE, 2019, pp. 1-8 [*DOI :* 10.1109/EMPDP.2019.8671621], https://hal.inria.fr/hal-01987946

International Conferences with Proceedings

[11] M. COMPASTIÉ, R. BADONNEL, O. FESTOR, R. HE. *A TOSCA-Oriented Software-Defined Security Approach for Unikernel-Based Protected Clouds*, in "NetSoft 2019 - IEEE Conference on Network Softwarization", Paris, France, IEEE, June 2019, pp. 151-159 [*DOI :* 10.1109/NETSOFT.2019.8806623], https://hal.archives-ouvertes.fr/hal-02271520

[12] L. EVRARD, J. FRANÇOIS, J.-N. COLIN, F. BECK. *port2dist: Semantic Port Distances for Network Analytics*, in "IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2019) - Demo session", Washington, United States, April 2019, https://hal.inria.fr/hal-02345491

[13] L. EVRARD, J. FRANÇOIS, J.-N. COLIN. *Attacker Behavior-Based Metric for Security Monitoring Applied to Darknet Analysis*, in "IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2019)", Washington, United States, April 2019, https://hal.inria.fr/hal-02345457

[14] A. HEMMER, R. BADONNEL, I. CHRISMENT. *A Process Mining Approach for Supporting IoT Predictive Security*, in "Network Operations and Management Symposium", Budapest, Hungary, April 2020, https://hal.inria.fr/hal-02402986

[15] B. HENRY, S. R. CHOWDHURY, A. LAHMADI, R. AZAÏS, J. FRANÇOIS, R. BOUTABA. *SPONGE: Software-Defined Traffic Engineering to Absorb Influx of Network Traffic*, in "44th IEEE Conference on Local Computer Networks (LCN)", Osnabrück, Germany, October 2019, https://hal.archives-ouvertes.fr/hal-02403616

[16] P.-M. JUNGES, J. FRANCOIS, O. FESTOR. *Passive Inference of User Actions through IoT Gateway Encrypted Traffic Analysis*, in "IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2019) Workshop: 5th International Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2019)", Washington, United States, April 2019, https://hal.inria.fr/hal-02331783

[17] S. LAGRAA, M. CAILAC, S. RIVERA, F. BECK, R. STATE. *Real-time attack detection on robot cameras: A self-driving car application*, in "IEEE IRC 2019 - Third IEEE International Conference on Robotic Computing", Naples, Italy, February 2019, https://hal.inria.fr/hal-02063304

[18] M. MA, A. LAHMADI, I. CHRISMENT. *Demonstration of Synchronization Attacks on Distributed and Cooperative Control in Microgrids*, in "The 16th IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2019)", Washington DC, United States, April 2019, https://hal.archives-ouvertes.fr/hal-02389307

[19] L. MEFTAH, R. ROUVOY, I. CHRISMENT. *FOUGERE: User-Centric Location Privacy in Mobile Crowdsourcing Apps*, in "19th IFIP International Conference on Distributed Applications and Interoperable Systems (DAIS)", Kongens Lyngby, Denmark, J. PEREIRA, L. RICCI (editors), Distributed Applications and Interoperable Systems, Springer International Publishing, 2019, vol. LNCS-11534, pp. 116-132 [*DOI :* 10.1007/978-3-030-22496-7_8], https://hal.inria.fr/hal-02121311

[20] L. MEFTAH, R. ROUVOY, I. CHRISMENT. *Testing Nearby Peer-to-Peer Mobile Apps at Large*, in "MOBILESoft 2019 - 6th IEEE/ACM International Conference on Mobile Software Engineering and Systems", Montréal, Canada, D. POSHYVANYK, I. MALAVOLTA (editors), May 2019, https://hal.inria.fr/hal-02059088

[21] P. ROLIN, D. MOALIC, R. BADONNEL, O. BERGER, J. FOUZAI. *A collection of MOOCs to create digital programs*, in "OOFHEC 2019: the Online, Open and Flexible Higher Education Conference", Madrid, Spain, October 2019, pp. 86-99, https://conference.eadtu.eu/download2527, https://hal.archives-ouvertes.fr/hal-02398007

[22] A. SAIF, A. MERLIN, O. DAUTRICOURT, M. HOUBRE, L. NUSSBAUM, Y.-Q. SONG. *Emulation of Storage Performance in Testbed Experiments with Distem*, in "CNERT 2019 - IEEE INFOCOM International Workshop on Computer and Networking Experimental Research using Testbeds", Paris, France, April 2019, 6 p. , https://hal.inria.fr/hal-02078301

[23] N. SCHNEPF, R. BADONNEL, A. LAHMADI, S. MERZ. *A Tool Suite for the Automated Synthesis of Security Function Chains*, in "IFIP/IEEE IM 2019 - IFIP/IEEE International Symposium on Integrated Network Management", Washington, United States, April 2019, https://hal.inria.fr/hal-02111658

[24] N. SCHNEPF, R. BADONNEL, A. LAHMADI, S. MERZ. *Automated Factorization of Security Chains in Software-Defined Networks*, in "IFIP/IEEE IM 2019 - IFIP/IEEE International Symposium on Integrated Network Management", Washington, United States, April 2019, https://hal.inria.fr/hal-02111656

[25] W. M. SHBAIR, M. STEICHEN, J. FRANÇOIS, R. STATE. *BlockZoom: Large-Scale Blockchain Testbed*, in "2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) - Demo", Seoul, South Korea, IEEE, May 2019, pp. 5-6 [*DOI :* 10.1109/BLOC.2019.8751230], https://hal.inria.fr/hal-02403717

[26] A. VULPE, A. PAIKAN, R. CRACIUNESCU, P. ZIAFATI, S. KYRIAZAKOS, A. HEMMER, R. BADONNEL. *IoT Security Approaches in Social Robots for Ambient Assisted Living Scenarios*, in "The 22nd International Symposium on Wireless Personal Multimedia Communications", Lisbon, Portugal, November 2019, https://hal.inria.fr/hal-02402950

National Conferences with Proceedings

[27] D. DELABROYE, S. DELAMARE, D. LOUP, L. NUSSBAUM. *Remplacer un routeur par un serveur Linux : retour d'expérience des passerelles d'accès à Grid'5000*, in "JRES - Journées Réseaux de l'Enseignement et de la Recherche", Dijon, France, December 2019, https://hal.inria.fr/hal-02401684

Conferences without Proceedings

[28] S. HADDAD-VANIER, C. GICQUEL, L. BOUKHATEM, K. LAZRI, P. CHAIGNON. *Virtual network functions placement for defense against distributed denial of service attacks*, in "8th International Conference on Operations Research and Enterprise Systems ICORES 2019", Praque, Czech Republic, February 2019, https://hal.archives-ouvertes.fr/hal-02421693

[29] M. LAURENT, O. PAUL, G. BLANC, B. CARRON, N. CHARBONNIER, I. CHRISMENT, J. FRANÇOIS, D. HOTZ, P. JAILLON, R. KHATOUN, C. KIENNERT, M. LAZRAG, S. MASMOUDI. *MOOC Sécurité des réseaux: un apprentissage massif de la sécurité par la théorie et la pratique*, in "RESSI 2019: Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information", Erquy, France, RESSI 2019 Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, 2019, pp. 1-4, https://hal.archives-ouvertes.fr/hal-02437172

[30] H.-L. MAI, M. AOUADJ, G. DOYEN, W. MALLOULI, E. MONTES DE OCA, O. FESTOR. *Toward Content-Oriented Orchestration: SDN and NFV as Enabling Technologies for NDN*, in "IM 2019 - IFIP/IEEE Symposium on Integrated Network and Service Management (IM)", Arlington, United States, IEEE, April 2019, https://hal-utt.archives-ouvertes.fr/hal-02274785

[31] L. NUSSBAUM. *An overview of Fed4FIRE testbeds – and beyond?*, in "GEFI - Global Experimentation for Future Internet Workshop", Coimbra, Portugal, November 2019, https://hal.inria.fr/hal-02401738

[32] L. NUSSBAUM. *SILECS/Grid'5000: le volet data-center de SILECS : Présentation et exemples d'expériences*, in "TILECS - Towards an Infrastructure for Large-Scale Experimental Computer Science", Grenoble, France, July 2019, https://hal.inria.fr/hal-02401836

Scientific Books (or Scientific Book chapters)

[33] *5th IEEE Conference on Network Softwarization, NetSoft 2019, Paris, France*, June 2019, https://hal.archives-ouvertes.fr/hal-02296176

[34] *TMA 2019 - Proceedings of the 3rd Network Traffic Measurement and Analysis Conference*, IEEE, Paris, France, June 2019, https://hal.archives-ouvertes.fr/hal-02296177

[35] *Proceedings of the 15th International Conference on Network and Service Management (CNSM 2019)*, October 2019, https://hal.archives-ouvertes.fr/hal-02398019

[36] J. BETSER, C. FUNG, A. CLEMM, J. FRANÇOIS, A. SHINGO, R. BADONNEL, G. M. MOURA. , IEEE (editor) *16th IFIP/IEEE International Symposium on Integrated Network Management (IM 2019) - Experience Session*, IEEE, April 2019, https://hal.archives-ouvertes.fr/hal-02398024

Research Reports

[37] A. SAIF, L. NUSSBAUM, Y.-Q. SONG. *On the Impact of I/O Access Patterns on SSD Storage*, Inria, January 2020, n^{o} RR-9319, https://hal.inria.fr/hal-02430564

Scientific Popularization

[38] D. ESPINEL SARMIENTO, A. LEBRE, L. NUSSBAUM, A. CHARI. *Distributing connectivity management in Cloud-Edge infrastructures : Challenges and approaches*, in "COMPAS 2019 - Conférence d'informatique en Parallélisme, Architecture et Système", Anglet, France, June 2019, pp. 1-7, https://hal.inria.fr/hal-02133606

Other Publications

[39] A. ABBOUD, A. LAHMADI, M. RUSINOWITCH, M. COUCEIRO, A. BOUHOULA. *Minimizing Range Rules for Packet Filtering Using a Double Mask Representation*, May 2019, IFIP Networking 2019, Poster, https://hal.inria.fr/hal-02393008

[40] A. ABBOUD, A. LAHMADI, M. RUSINOWITCH, M. COUCEIRO, A. BOUHOULA, S. E. H. AWAINIA, M. AYADI. *Minimizing Range Rules for Packet Filtering Using Double Mask Representation*, April 2019, working paper or preprint, https://hal.inria.fr/hal-02102225

[41] M. BERMAN, T. FRIEDMAN, A. GOSAIN, K. KEAHEY, R. MCGEER, I. MOERMAN, A. NAKAO, L. NUSSBAUM, K. RAUSCHENBACH, V. SYROTIUK, M. VEERARAGHAVAN, N. YAMANAKA. *Report of the Third Global Experimentation for Future Internet (GEFI 2018) Workshop*, January 2019, https://arxiv.org/abs/1901.02929 - working paper or preprint, https://hal.inria.fr/hal-01978579

[42] D. MARGERY, L. NUSSBAUM. *Estimation of Costs and Pay per Use on a Large-scale Shared Computer Science Testbed: the Grid'5000 Case*, February 2019, working paper or preprint, https://hal.inria.fr/hal-02011425

References in notes

[43] J. ARON. *The internet is almost full*, in "New Scientist", 2015, vol. 226, n^{o} 3022, 20 p.

[44] D. BALOUEK, A. CARPEN-AMARIE, G. CHARRIER, F. DESPREZ, E. JEANNOT, E. JEANVOINE, A. LÈBRE, D. MARGERY, N. NICLAUSSE, L. NUSSBAUM, O. RICHARD, C. PÉREZ, F. QUESNEL, C. ROHR, L. SARZYNIEC. *Adding Virtualization Capabilities to the Grid'5000 Testbed*, in "Cloud Computing and Services Science", I. IVANOV, M. SINDEREN, F. LEYMANN, T. SHAN (editors), Communications in Computer and Information Science, Springer International Publishing, 2013, vol. 367, pp. 3-20 [*DOI :* 10.1007/978-3-319-04519-1_1], https://hal.inria.fr/hal-00946971

[45] T. BUCHERT, C. RUIZ, L. NUSSBAUM, O. RICHARD. *A survey of general-purpose experiment management tools for distributed systems*, in "Future Generation Computer Systems", 2015, vol. 45, pp. 1-12 [*DOI :* 10.1016/J.FUTURE.2014.10.007], https://hal.inria.fr/hal-01087519

[46] D. J. RICHARDSON. *Filling the Light Pipe*, in "Science", 2010, vol. 330, n^{o} 6002, pp. 327–328

[47] L. SARZYNIEC, T. BUCHERT, E. JEANVOINE, L. NUSSBAUM. *Design and Evaluation of a Virtual Experimental Environment for Distributed Systems*, in "PDP2013 - 21st Euromicro International Conference on Parallel, Distributed and Network-Based Processing", Belfast, United Kingdom, February 2013, https://hal.inria.fr/hal-00724308

[48] C. TANKARD. *Advanced Persistent threats and how to monitor and deter them*, in "Network Security", 2011, vol. 2011, n^{o} 8, pp. 16-19