Activity Report 2018

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 Scientist

Jérôme François [Deputy team leader, Inria, Researcher]

Faculty Members

Laurent Andrey [Univ de Lorraine, Associate Professor]
Rémi Badonnel [Univ de Lorraine, Associate Professor]
Raouf Boutaba [Waterloo Univ, Inria, Univ de Lorraine (LUE), Professor, HDR]
Thibault Cholez [Univ de Lorraine, Associate Professor]
Isabelle Chrisment [Team Leader, Univ de Lorraine, Professor, HDR]
Olivier Festor [Univ de Lorraine, Professor, HDR]
Abdelkader Lahmadi [Univ de Lorraine, Associate Professor]
Lucas Nussbaum [Univ de Lorraine, Associate Professor]

Post-Doctoral Fellow
Quang Vinh Dang [Inria, from Feb 2018 until May 2018]

PhD Students
Ahmad Abboud [Cynapsys, granted by CIFRE, from Aug 2018]
Pierre-Olivier Brissaud [Thales, granted by CIFRE]
Paul Chaignon [Orange Labs, granted by CIFRE]
Maxime Compastié [Orange Labs, granted by CIFRE]
Giulia de Santis [Inria]
Adrien Hemmer [Inria, from Apr 2018]
Pierre Marie Junges [Univ de Lorraine, from Oct 2018]
Daishi Kondo [CNRS]
Abir Laraba [Univ de Lorraine (LUE), from Oct 2018]
Mingxiao Ma [CNRS]
Xavier Marchal [CNRS]
Abdulqawi Saif [Xilopix/Qwant, from Dec 2015, then Univ de Lorraine, from Sep 2018]
Nicolas Schnepf [Inria]
Salvatore Signorello [Univ de Luxembourg, until June 2018]

Technical staff
Soline Blanc [Inria]
Antoine Chemardin [CNRS, from Nov 2018]
Florent Didier [Inria, until May 2018]
Thomas Lacour [Inria]
Alexandre Merlin [Inria]
Loic Rouch [Inria, until Aug 2018]

Interns
Anthony Anthony [Inria, from Jun 2018 until Aug 2018]
Guillaume Bressan [Ecole Normale Supérieure Paris, from Jun 2018 until Aug 2018]
Shihabur Rahman Chowdhury [Inria, from Jun 2018 until Aug 2018]
Olivier Dautricourt [Inria, from Jun 2018 until Aug 2018]
Benoit Frapiccini [CNRS, from Jun 2018 until Aug 2018]
Mohamed Said Frikha [Univ de Lorraine, from Apr 2018 until Sep 2018]
Gaby Portelli [Inria, from Jun 2018 until Jul 2018]

Administrative Assistants
Isabelle Herlich [Inria]
Annick Jacquot [CNRS, from Jul 2018]

Visiting Scientist
Sara El Alaoui [University of Nebraska Lincoln, from May 2018 until Aug 2018]

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 [36], [33]. 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) [38] 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, which must also be addressed. 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 ambitions 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.

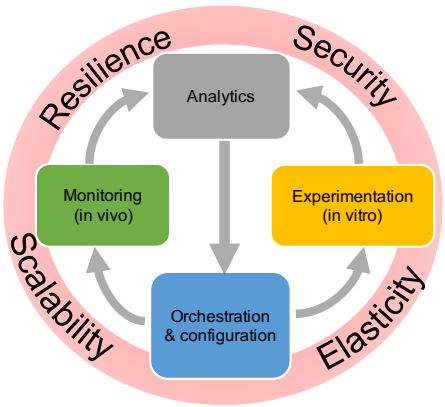

Figure 1. The Resist project

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 [34] 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 [37] 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 [35].

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 resillience, 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

- Raouf Boutaba gave his inaugural conference as Inria Internationale Chair and Professor@Lorraine about *Convergence of telecommunications and information technologies: towards programmable, intelligent and resilient networks*.
- The team (Jérôme François and Isabelle Chrisment) organized the RESSI'18 (Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information).

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 experimental platform
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, including Lyon. 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 first joint FIT-Grid'5000 school, and various improvements (update to Debian 9, several new clusters, 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: Frédéric Desprez
- URL: https://www.grid5000.fr/

6.3. HTTP-NDN gateway

A gateway to transport HTTP over NDN
KEYWORDS: Internet protocols - Interoperability - Named Data Networking - Web - Network gateway
FUNCTIONAL DESCRIPTION: In order to creat an NDN island using our HTTP over NDN architecture, we propose two kinds of gateways: (1) an ingress gateway (iGW), which converts HTTP user requests into NDN messages and converts requested NDN messages into HTTP responses sent to the end-users, and (2) an egress gateway (eGW), the counterpart of the first one, which converts requested NDN messages into HTTP requests towards web sites and converts HTTP responses into NDN messages.

The whole thing can be considered as an HTTP proxy for the outsiders of the NDN network because the gateways represent the input(s) and output(s) of the NDN network island which can store the HTTP responses passing through. The gateway also features intelligent naming and cache management of web contents passing through the NDN network to better use the NDN architecture. Native NDN clients and NDN web servers can be present inside this NDN network, and they can communicate with the same mapping protocol used by the gateways to communicate with regular HTTP/IP clients or servers.

NEWS OF THE YEAR: First release

- Partner: Orange Labs
- Contact: Thibault Cholez
- URL: https://github.com/DOCTOR-ANR/NDN-HTTP-Gateway

6.4. micro-NDN

microservices for NDN
KEYWORDS: Named Data Networking - Network Function Virtualization - Microservices
FUNCTIONAL DESCRIPTION: micro-NDN proposes to split the main functions of an NDN (Named-Data Networking) router into multiple microservices and to orchestrate them. Currently, it implements seven microservices: five are usual functions of an NDN router as in the NFD forwarding deamon (http://named-data.net/doc/NFD/current), and two are proposed to improve security: - Name Router (NR): Route Interest packets to producers that have registered a prefix of the name of the packet, it is like the Forwarding Information Base (FIB) in an NDN router, - Backward Router (BR): Route back Data packets to the consumers that have asked for it, it is like the Pending Interest Table (PIT) in an NDN router, - Packet Dispatcher (PD): Select the right pipeline for each kind of packet, - Content Store (CS): Aims to store Data packets to reuse them later when reasked, like the Content Store (CS) in an NDN router, - Strategy Forwarder (SF): A more general way to apply strategy (fail-over, round-robin, etc.), - Signature Verifier (SV): Verify the signature of the NDN packet based on the trusted keys, - Name Filter (NF): Drop packets based on their name.

We also provide a central manager that can monitor and orchestrate all the microservices. It provides a web-based GUI and a REST API to dynamically manipulate the topology (spawn a microservice, link them, etc.). It can also trigger actions based on predefined rules, for example to scale-up a bottleneck component.
NEWS OF THE YEAR: First release

- Contact: Thibault Cholez
- URL: https://github.com/DOCTOR-ANR/NDN-microservices

6.5. ndnperf

tool for server-side evaluation of NDN throughput
KEYWORDS: Named Data Networking - Performance measure
FUNCTIONAL DESCRIPTION: NDNperf is a tool for NDN server-side performance evaluation and sizing purposes, in order to have an idea of the throughput a server can achieve when it has to generate and transmit NDN Data packets. It is very similar to iPerf and also needs a client and a server to perform the measurements while minimizing the number of instructions between Interest reception and Data emission. It exists in two flavors (Java and C++) and has the following features: - Periodic performance report: end-to-end throughput, latency, processing time, - Multi-threaded (one main thread for event lookup and N threads for NDN Data generation), - Able to use all the available signatures implemented in the NDN library, choose the size of the key, and the transmission size of Data packets, - Message broker implementation (Java version only, currently no update is scheduled).

NDNperf features many options regarding the signing process because we identified it as the main bottleneck of application performances.
NEWS OF THE YEAR: First release

- Contact: Thibault Cholez
- URL: https://github.com/DOCTOR-ANR/ndnperf

6.6. 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

6.7. Platforms

6.7.1. CPS Security Assessment Platform

During 2018, we have extended our Cyber-Physical systems security assessment platform with new hardware components including multiple types of Programmable Logic Controllers (PLCs), a small scale distribution and sorting testbed, and an experimental system modelled after a microgrid system. The physical platform is also extended with several IoT devices dedicated to residential networks (heating control, lightning system, home gateways, etc). The platform will be mainly used for building security assessment and evaluation experimentation on the available devices to identify and validate their associated attack patterns and discover new vulnerabilities. This platform is used as a testbed for the development carried on the SCUBA (see 6.6) tool suite to assess the security of IoT and SCADA systems.

7. New Results

7.1. Monitoring

7.1.1. HTTPS traffic monitoring

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

While privacy is empowered by encrypted communications such as through the HTTPS protocol, it is also legitimated to allow network monitoring of HTTPS traffic. To be compliant with privacy, we proposed a transparent and passive technique that only detects if an HTTPS request is related to a previously defined action [7]. Our technique is able to detect forbidden searches over a web service such as Google Images. It differs from related work that either focuses on detecting the type of traffic or the used web service. To achieve a high accuracy, our technique relies on learning stage where keywords to be monitored are crawled before we leverage KDE (Kernel Density Estimation). KDE allows us to construct a signature summarizing the sizes of the loaded objects on a page, which strongly depend on the user action or search.

7.1.2. Monitoring Programmable Networks

Participants: Jérôme François [contact], Olivier Festor, Paul Chaignon [Orange Labs], Kahina Lazri [Orange Labs], Thibault Delmas [Orange Labs].

SDN-based monitoring allows us to gather more valuable indicators by specifying or programming the monitoring with a fine granularity. We proposed to use eBPF (extended Berkeley Packet Filter) to apply fine-grained filtering in comparison to OpenFlow. It brings safety guarantees regarding program execution and allows stateful programs. In order to limit the impact on the throughput, we integrated our solution within the regular packet processing pipeline of Open vSwitch, a major software switch for OpenFlow, by extending the cache mechanisms [8].

7.1.3. 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 the last decade, many IoT architectures have been proposed. However, security cannot be guaranteed without failure or by-design. In that context, we are currently investigating predictive security monitoring strategies for large-scale Internet-of-Things. In particular, we are considering the building of behavioral models characterizing such complex networks. The objective is to support both the detection of malicious activities, as well as the selection of security counter-measures.

7.1.4. Quality of Experience Monitoring

Participants: Isabelle Chrisment [contact], Thibault Cholez, Antoine Chemardin, Vassili Rivron [University of Caen], Lakhdar Meftah [University of Lille].

We have pursued our work on smartphone usage monitoring with the SPIRALS team (Inria/Université de Lille) and more specifically on proposing new methods to help measure the QoE and to protect the user's privacy when collecting such data.

In the context of the BottleNet project, to build an adequate instrumented investigation system (mobile applications combining measurements and questionnaires), we decomposed, with a group of students, the network quality concept and the perception of the services in several different approaches. These students worked on bibliographic research, on the smartphone usage and on the perception of the Internet. Structured debates on social issues associated with mobile connectivity were organized. The following topics were dealt: Quality of Service/Quality of Experience; rhythms of life and routines; privacy: diversity of practices and ethical issues; advertising and free: volume, exposure, perception, third-party and cost; quantified self-*: relation to self-quantification; online cultural consumption; information practices on mobile; communication practices.

In the context of the IPL BetterNet project, we continued to work on federating Inria's monitoring tools (APISENSE®, Fathom, Hostview, ACQUA) in a common measurement platform. A first test campaign has been performed with a small set of volunteer users to evaluate the full data collection system built from all these tools.

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: Florent Didier, Alexandre Merlin, Lucas Nussbaum [contact], Olivier Demengeon [SED], 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 (9 FTE).

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. Since 2018, SILECS has been listed as part of the French National Roadmap for Very Large Research Infrastructures (TGIR program).
Grid'5000/FIT school We had a central role in the organization of the Grid'5000/FIT school that took place in Sophia-Antipolis in April 2018, gathering 93 participants. Lucas Nussbaum delivered a keynote talk presenting Grid'5000 and its recent evolutions [28]. A successful evaluation of Grid'5000 by its Scientific Advisory Board also took place during the school.
Storage manager A contribution from the team was the design and development of a new storage access manager that allows secure access to NFS home directories, thus closing a widely-spread security vulnerability.

7.2.2. I/O emulation support in Distem

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

Distem had a new release (version 1.3) at the beginning of 2018. This release mainly focused on bringing it up-to-date in terms of software quality (newer dependencies, added tests) and added some network emulation features that were previously missing.

The emulator was then featured in a tutorial during the Grid'5000/FIT school.

There is ongoing work on adding I/O emulation support in Distem, in order to experiment how Big Data solution can handle degraded situations. This is still pending completion and publication.

7.2.3. I/O access patterns analysis with eBPF

Participants: Abdulqawi Saif, Lucas Nussbaum [contact], Ye-Qiong Song.

We explored the relevance of an emerging instrumentation technology for the Linux kernel, eBPF, and used it to analyze I/O access patterns such as non-sequential accesses, which are particularly harmful on non-SSD drives. We designed a tool to help with such analysis, and applied it to two popular NoSQL databases, MongoDB and Cassandra, outlining severe performance problems [19] with MongoDB, where a workload that should have resulted in sequential accesses was in fact turned into lots of random accesses.

7.2.4. Experiment Monitoring

Participants: Abdulqawi Saif, Alexandre Merlin, Lucas Nussbaum [contact], Ye-Qiong Song.

Most computer experiments include a phase where metrics are gathered from and about various kinds of resources. This phase is often done via manual, non-reproducible and error-prone steps. We designed an experiment monitoring framework called MonEx, built on top of infrastructure monitoring solutions and supporting various monitoring approaches. MonEx fully integrates into the experiment workflow by encompassing all steps from data acquisition to producing publishable figures [18], [29].

7.2.5. Testbed federation and collaborations in the testbeds community

Participant: Lucas Nussbaum [contact].

The Fed4FIRE+ H2020 project started in January 2017 and will run until the end of September 2021. This project aims at consolidating the federation of testbeds in Europe of which Grid'5000 is a member. In 2018, we focused on various aspects related to experiment reproducibility.

We are also active in the GEFI initiative that aims at building links between the US testbeds community (GENI) and their European (FIRE), Japanese and Brazilian counterparts. We participated in the annual GEFI meeting where we chaired two sessions on *Experiment reproducibility* and *Networking experiments*, respectively, and gave one talk on Experiment data management, outlining the recent work that was done on Grid'5000 on disk reservation [27].

7.2.6. Blockchain experimentation

Participants: Jérôme François [Contact], Wazen Shbair [University of Luxembourg, Luxembourg], Radu State [University of Luxembourg, Luxembourg], Mathis Steichen [University of Luxembourg, Luxembourg].

The experimentation of distributed applications like blockchains needs a highly reconfigurable and controllable environment for fine-tuning blockchain and network parameters in different scenarios. Therefore, there might be significant manual operations which lead to human errors and make it hard to reproduce experiments. We proposed an easy to use orchestration framework over the Grid'5000 platform [23]. Our tool can fine-tune blockchain and network parameters before and between experiments. The proposed framework offers insights for private and consortium blockchain developers to identify performance bottlenecks and to assess the behavior of their applications in different circumstances.

7.2.7. 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 transport the traffic of regular web users over an NDN island. Users just need to configure the ingress gateway as a standard web proxy that will be the entry point to the virtualized NDN island, and their traffic is seamlessly transported over NDN, thus benefiting from the good properties of the protocol to deliver content (request mutualization, caching, etc.). HTTP requests/responses are converted into NDN Interest/Data and the answer can either come from the island, or from the web through the egress gateway. Our first functional experimental results of an initial testbed deployment exhibit the capability of our global infrastructure to retrieve the top-1000 most popular web sites without difficulty [17]. This opens the way to wider and more realistic experiments of NDN with real traffic. In particular, the gateway was used to perform QoE experiments involving real users from Nancy and Troyes. They accessed many websites through the NDN network in a very satisfying way.

7.3. Analytics

7.3.1. CPS Security analytics

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

During 2018, we designed and 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 analyzed the control-theoretic and detectability properties of this attack to assess its impact on reference voltage synchronization at the different control layers of a microgrid. Results from numerical simulation are presented in [15] and demonstrate this attack, in particular the maximum voltage deviation and inaccurate reference voltage synchronization it causes in the microgrid.

7.3.2. Analysis of Internet-wide attacks

Participants: Abdelkader Lahmadi [contact], Giulia de Santis, Jérôme François, Olivier Festor.

Internet-wide scanners are heavily used for malicious activities. In [13], we developed models based on HMMs (Hidden Markov Models) and finite mixture models to identify network scanners from the packets received by a darknet. We used data collected by the darknet hosted in the High Security Lab of Inria Nancy - Grand Est to build these models by characterizing the spatial and temporal movements of the studied scanners (Zmap and Shodan). Our models are able to recognize the scanner with an accuracy of 95% when using spatial movements, and of 98% when using temporal movements.

Under the umbrella of the ThreatPredict project with the International University of Rabat, we have performed preliminary exploratory analysis of Inria darknet data that consists of examining time series of scan activities and the scanning behavior of different attackers [24]. We performed experiments on the clustering of darknet data to extract threat patterns including scanning and DDoS activities. We are still extending the technique with more features and developing Hololens based visualization of the obtained graphs. Based on our experience, traffic analysis faces a major challenge when using machine learning or data-mining techniques due to data which cannot be represented in a meaningful metric space. One major case is TCP or UDP ports. We thus proposed a new semantic based metric between port numbers that does not follow a regular numeric distance but relies on observed attacks of the past.

7.3.3. Cyber Threat Intelligence

Participants: Jérôme François, Abdelkader Lahmadi [contact], Quang Vinh Dang.

We are exploring and validating techniques for learning correlations between vulnerabilities and attack patterns from Cyber threat intelligence data sources including CVE (Common Vulnerabilities and Exposures), CAPEC (Common Attack Pattern Enumeration and Classification) and CWE (Common Weaknesses Enumeration) documents. While there already exist some relations between them, they have been defined manually and so are quite incomplete. Finding these relations is a cumbersome and tedious task and our objective is to guide or even automatically detect relations or correlations between documents. This will ease a better understanding and mitigation of threats. Our work relies on leveraging NLP (Natural Language Processing Techniques) with several techniques such as graph-based or recommendation-based mining. The first results show the ability of our technique to automatically discover missing relations between attack patterns and vulnerability descriptions in the context of SDN [12]. We also consider word and document embedding to identify correlations between them.

7.4. Orchestration

7.4.1. Programming of network functions

Participants: Thibault Cholez [contact], Diane Adjavon [Orange Labs], Anthony Anthony, Raouf Boutaba, Paul Chaignon, Shihabur Rahman Chowdhury, Olivier Festor, Jérôme François, Kahina Lazri [Orange Labs], Xavier Marchal.

NFV is a key technology for the successful deployment of new network protocol stacks like Named Data Networking (NDN). Instead of trying to oddly couple IP and new Information-Centric Networking protocols, one should rather deploy them in different network slices and ensure their isolation. We proposed a complete NFV architecture composed of several Virtual Network Functions (VNF) designed for NDN and orchestrated so that they can dynamically adapt the topology to react against issues such as an ongoing attack [25].

To push even further the possibilities of NFV, we applied the microservice architecture inherited from the software world to design atomic and flexible functions that must be combined to process NDN traffic. The proposed architecture, described in μNDN [16], includes seven orchestrated microservices. Some of them are components extracted from the monolithic and heavy-burden NDN router while others are new on-path functions that can perform specific processing on the traffic like a signature-verification module or a name-filtering module. The evaluation through two realistic scenarios proved the ability of our manager to dynamically scale-up bottleneck functions and mitigate ongoing attacks on the NDN network. We also refined our countermeasure against information leakage attacks in NDN [4].

In [8], we proposed to offload part of the processing of VNF to the programmable switches. The problem resides in guaranteeing a fair scheduling at the switch level assuming the required run-to-completion execution. We thus defined a token-based scheduling approach. In [6], we defined a new scheduler for VNFs that integrates a CPU cycle estimator and a heuristic to avoid wasting idle CPU cycles.

7.4.2. Software-defined security for clouds

Participants: Rémi Badonnel [contact], Olivier Festor, Maxime Compastié, He Ruan [Orange Labs].

We have pursued our work on a software-defined security framework for enabling the enforcement of security policies in distributed clouds. This framework aims at dynamically integrating and configuring security mechanisms for protecting cloud services that are distributed over multi-cloud and multi-tenant environments. In that context, we have described in [11] generation mechanisms for building protected cloud resources based on unikernels in an on-the-fly manner. These unikernels integrate security mechanisms at an early stage, and are characterized by highly-constrained configurations, in order to reduce the attack surface. A demonstration of this work has been showcased during the IFIP/IEEE NOMS 2018 international conference [10]. We have also investigated the exploitation of the TOSCA orchestration language to drive the generation of these unikernels. This language supports the specification of cloud services in the form of topologies and their orchestrations. The objective was to extend this language to both describe the generation of unikernel ressources, and specify different levels of security to be orchestrated. We have designed a framework to interpret this extended language, and to generate and configure protected resources according to these levels. We have evaluated the performance of generation mechanisms through extensive experiments. This generation can be performed in a proactive manner with respect to security levels, in accordance with elasticity and on-demand cloud properties.

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 elaboraboration 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. In particular, we have formalized and extended our approach for generating SDN policies to protect Android applications [21], [22]. We have introduced a system based on inference rules for automating the generation of such chains [20], taking into account both their networking behavior and the OS-level permissions that they request. By using first-order predicates for classifying network traffic observed in flow traces, the composition and factorization of security chains to be applied for several applications becomes straightforward. Our system infers a high-level representation of the security functions, which can be translated into an concrete implementation in the Pyretic language for programming software-defined networks. We showed that the generated chains satisfy several desirable properties such as the absence of black holes or loops, shadowing freedom, and that they are consistent with the underlying security policy. We are currently working on optimizing and improving the parameterization of the security chains that are generated by our inference system.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- RED ALERT LABS (Paris, France)
  - Verification of the security requirements of an IoT device (a connected doorbell) using the SCUBA tool suite.
  - An extension of SCUBA (see 6.6) is developed to verify the security requirements provided in Common Criteria format by the industrial partner. The verification uses the information of the Security Knowledge Bases (SKB) built by the SCUBA tool suite.

8.2. Bilateral Grants with Industry

- Thales (Palaiseau, France):
  - CIFRE PhD (Pierre-Olivier Brissaud, supervised by Isabelle Chrisment and Jérôme François)

  - Anomaly detection in encrypted network traffic
- Orange Labs (Issy-Les-Moulineaux, France):
  - CIFRE PhD (Maxime Compastie, supervised by Olivier Festor and Rémi Badonnel)
  - Software-Defined Security for Distributed Cloud Infrastructures
- Orange Labs (Issy-Les-Moulineaux, France):
  - CIFRE PhD (Paul Chaignon, supervised by Olivier Festor and Jérôme François)
  - Monitoring of Software-Defined Networks
- Xilopix then Qwant (Épinal, France):
  - CIFRE PhD (Abdulqawi Saif, supervised by Ye-Qiong Song and Lucas Nussbaum)
  - Open Science for the scalability of a new generation search technology
- 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. National Initiatives

9.1.1. ANR

9.1.1.1. ANR BottleNet

Participants: Isabelle Chrisment [contact], Thibault Cholez, Vassili Rivron.

- Acronym: BottleNet
- Title: Comprendre et diagnostiquer les dégradations des communications de bout en bout dans l'Internet
- Coordinator: Inria
- Duration: October 2015- March 2018
- 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.

9.1.1.2. ANR Doctor

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

- Acronym: DOCTOR
- Title: DeplOyment and seCurisaTion of new functiOnalities in virtualized networking enviRonments
- Coordinator: Orange Labs (Bertrand Matthieu)
- Duration: December 2014-December 2018
- Partners: Orange Labs, Thales, Montimage, UTT and LORIA
- Site: http://www.doctor-project.org
- Abstract: The DOCTOR project is an applied research project that advocates the use of virtualized network equipment (Network Functions Virtualization), to enable the co-existence of new Information-Centric Networking stacks (e.g.: Named-Data Networking) with IP, and the progressive migration of traffic from one stack to another while guaranteeing the good security and manageability of the network. Therefore in DOCTOR, the main goals of the project are: (1) the efficient deployment of NDN as a virtualized networking environment; (2) the monitoring and security of this virtualized NDN stack.

9.1.1.3. 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-January 2020
- Others Partners: 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 a duration of 4 years. It includes 14 academic partners (engineering schools including Telecom Nancy), industrial partners (Airbus, Orange), innovative startups (the MOOC agency, and Isograd), as well as professional or scientific societies (Syntec Numérique, Unetel, SEE). 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. We have also performed the maintenance of the different contents of the MOOC, in preparation of the second session, which will start January 2019.

9.1.1.4. Inria-Orange Joint Lab

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

9.1.2. Technological Development Action (ADT)

9.1.2.1. ADT SCUBA

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

- Acronym: CUBA
- 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.

9.1.3. FUI

9.1.3.1. 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.

9.1.3.2. FUI HUMA

Participants: Jérôme François [contact], Soline Blanc, Isabelle Chrisment, Quang Vinh Dang, Abdelkader Lahmadi, Giulia de Santis.

- Acronym: HuMa
- Title: L'HUmain au cœur de l'analyse de données MAssives pour la sécurité
- Coordinator: Intrinsec
- Duration: September 2015-March 2018
- Others Partners: ICube, Idemia, Airbus Defence and Space, Wallix, Sydo.
- Abstract: HuMa targets the analysis of Advanced Persistent Threats. APT are long and complex attacks which thus cannot be captured with standard techniques focused on short time windows and few data sources. Indeed, APTs may be several months long and involve multiple steps with different types of attacks and approaches. The project will address such an issue by leveraging data analytics and visualization techniques to guide human experts, which are the only oned able to analyze APT today, rather than targeting a fully automated approach.

9.1.4. Inria Project Lab

9.1.4.1. IPL BetterNet

Participants: Isabelle Chrisment [contact], Thibault Cholez, Vassili Rivron.

- Acronym: BetterNet
- Coordinator: RESIST (Isabelle Chrisment)
- Duration: October 2018-August 2023
- 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.

9.1.4.2. IPL Discovery

Participant: Lucas Nussbaum [contact].

- 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.

9.2. European Initiatives

9.2.1. Fed4Fire+ (2017-2022)

Title: Federation for FIRE Plus

Program: H2020

Duration: January 2017 - December 2021

Coordinator: Interuniversitair Micro-Electronicacentrum 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)

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.

9.2.2. SecureIoT

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

Duration: 3 years

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

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. International Initiatives

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

9.3.1.1. Masdin

Title: MAnagement of Software-Defined INfrastructure

International Partner (Institution - Laboratory - Researcher):

University of Luxembourg (Luxembourg) - SnT (Interdisciplinary Centre for Security, Reliability and Trust) - Radu State

Start year: 2016

See also: https://project.inria.fr/masdin

Networking is deeply evolving with the rise of programmability and virtualization. The concept of SDI (Software-Defined Infrastructure) has emerged from SDN (Software-Defined Networking) and NFV (Network Function Virtualization) making thus the configuration of the network highly dynamic and adaptable in real-time. However, new methods and tools have to be defined to properly monitor and configure this type of infrastructure. Current works are mainly limited to applying former approaches but do not exploit the novel capabilities offered by SDI. The goal of the associate team is thus to define methodologies taking benefit of them for an efficient monitoring and use of SDI resources while investigating the security issues it brings.

9.3.1.2. 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

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.

9.3.2. Participation in Other International Programs

9.3.2.1. 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.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

9.4.1.1. Internships

- Visit of Anthony (Anthony) Ang in RESIST, Ms Student, from June 4 to August 26 2018, new scheduler for micro-service based VNF [6]
- Visit of Shihabur Chowdhury in RESIST, PhD Student, from June 4 to August 26 2018, new scheduler for micro-service based VNF [6], intelligent traffic engineering

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

Abdelkader Lahmadi: IEEE Conference on Network Softwarization (NetSoft 2018), Workshops co-chair.

Lucas Nussbaum: Grid'5000/FIT School 2018.

Jérôme François: IEEE Conference on Network Softwarization (NetSoft 2018), demonstration co-chair.

Rémi Badonnel: IEEE/IFIP Network Operations and Management Symposium (NOMS 2018), demonstration co-chair; IEEE International Conference on Networks of the Future (NOF 2018), publicity co-chair; IEEE International Symposium on Integrated Network Management (IM 2019), experience track co-chair; IFIP International Conference on Autonomous Infrastructure, Management, Security (AIMS 2018), steering committee member.

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

Rémi Badonnel: IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2018); IEEE/IFIP/In Coop. with ACM SIGCOMM International Conference on Network and Service Management (CNSM 2019).

Isabelle Chrisment: Member of the steering committee for RESSI'18 (Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information); IFIP, in-cooperation with ACM SIGCOMM. Network Traffic Measurement and Analysis Conference (TMA 2019).

Jérôme François: 12th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2018); IEEE/IFIP international workshop on Managing and Managed by Blockchain (Man2block 2018); 5th IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2018); IEEE Workshop on Emerging Trends in Softwarized Networks (ETSN 2018)

Abdelkader Lahmadi: IEEE/IFIP international workshop on Managing and Managed by Blockchain (Man2block 2018), co-chair.

10.1.2.2. Member of the Conference Program Committees

Rémi Badonnel: IEEE/IFIP Network Operations and Management Symposium (NOMS 2018); IEEE Conference on Network Softwarization (NetSoft 2018); IEEE/IFIP/In Assoc. with ACM SIGCOMM International Conference on Network and Service Management (CNSM 2018); IEEE Global Information Infrastructure and Networking Symposium (GIIS 2018); IEEE Global Communications Conference - SAC IoT (GLOBECOM 2018); IEEE International Conference on the Network of the Future (NoF 2018); Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (Algotel 2018).

Thibault Cholez: IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block 2018); IEEE/IFIP International Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2018); IFIP/IEEE International Symposium on Integrated Network Management (IM 2019).

Isabelle Chrisment: IFIP International Conference on Autonomous Infrastructures, Management and Security (IFIP AIMS'18) ; Rencontres Francophones sur la Conception de Protocoles, l'évaluation de Performance et l'Expérimentation Aspects Algorithmiques de Télécommunications (CoResl'18) ; IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2018); IEEE/IFIP Network Operations and Management Symposium (NOMS 2019).

Jérôme François: IEEE/IFIP Network Operations and Management Symposium (NOMS 2018); IEEE Conference on Network Softwarization (IEEE NetSoft 2018); Principles, Systems and Applications of IP Telecommunications (IPTComm'18); 3rd Workshop on MIning DAta for financial applicationS (MIDAS 2018).

Abdelkader Lahmadi: IEEE Conference on Network Softwarization (IEEE NetSoft 2018) ; IEEE/IFIP Network Operations and Management Symposium (NOMS 2018); 2nd Cyber Security in Networking Conference (CSNet 2018); 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2018); IEEE – 13th System of Systems Engineering Conference (SoSE 2018).

Lucas Nussbaum: International Conference on Enabling Technologies: Infrastructure for Collaborative Entreprises (WETICE 2018); European Symposium on Serverless Computing and Applications (ESSCA 2018); 15th International Conference on Mining Software Repositories (MSR 2018 – FOSS award); 10th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2018); 4th International Workshop on Serverless Computing (WoSC 2018); IEEE INFOCOM International Workshop on Computer and Networking Experimental Research Using Testbeds (CNERT 2018).

10.1.2.3. Other selection activities

Rémi Badonnel served as a member of the Selection Committee for the Best Paper Awards of IEEE/IFIP/In Assoc. with ACM SIGCOMM International Conference on Network and Service Management (CNSM 2018).

Abdelkader Lahmadi served as a member of the Selection Committee of the 2018 ComSoc Student Competition "Communications Technology Changing the World".

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).

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

Jérôme François: Associate Editor for the Wiley International Journal of Network Management (IJNM); Guest Editor for a Special Issue on on Security for Emerging Open Networking Technologies in the same journal.

10.1.3.2. Reviewer - Reviewing Activities

Laurent Andrey: Wiley International Journal of Network Management (IJNM); Elsevier Journal on Communication Networks (COMNET).

Rémi Badonnel: IEEE Transactions on Network and Service Management (TNSM); Journal of Intelligent Manufacturing (JIMS); Journal of Network and System Management (JNSM); IEEE Communications Magazine (COMMAG).

Thibault Cholez: Elsevier Journal on Communication Networks (COMNET).

Isabelle Chrisment: Elsevier Journal Computer Communications (COMCOM).

Jérôme François: IEEE Transactions on Network and Service Management (TNSM); IEEE Journal on Selected Areas in Communications (JSAC); Elsevier Journal on Communication Networks (COMNET).

Abdelkader Lahmadi: IEEE Transactions on Network and Service Management (IEEE TNSM); Springer Journal of the Network and Systems Management (JNSM); Wiley International Journal of Network Management (IJNM).

Lucas Nussbaum: International Journal of Grid and Utility Computing (IJGUC); IEEE Transactions on Cloud Computing (TCC); Wiley Software: Practice and Experience (SPE).

10.1.4. Invited Talks

Thibault Cholez:

- SDN DAY 2018, Paris. Une architecture orchestrée de microservices pour les réseaux ICN.

Jérôme François:

- Panelist at IEEE/IFIP NOMS 2018: Cognitive Management versus Privacy in a Cyber World: Collision or Opportunity?
- Inria tech talk at Station-F, Paris. AI Platform for Automated Security Testing of Connected Devices. With Abdelkader Lahmadi, Frédéric Beck and Loïc Rouch.
- ETSI NEW INTERNET FORUM at SDN NFV world congress, Managing the Security of IoT Devices out of your Control.

Abdelkader Lahmadi:

- 12th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2018), Munich, Germany. Security Analysis of Internet of Things Devices [32]. With Frédéric Beck.
- Inria tech talk at Station-F, Paris. AI Platform for Automated Security Testing of Connected Devices. With Jérôme François, Frédéric Beck and Loïc

  .
- SDN DAY 2018, Paris. Toward Self-Driving Networks: A new era of network management.

Xavier Marchal:

- Journées Cloud 2018, Troyes. Une architecture de microservices pour les réseaux ICN.

Lucas Nussbaum:

- dotScale 2018, Paris. Distributions and package management in the containers era.
- Colloque Sciences ouvertes: expériences, enjeux et perspectives, Oct 2018, Vandœuvre-lès-Nancy, France. Table ronde sur les aspects "utilisateurs" : intérêts et retours d'expériences de chercheurs et enseignants-chercheurs du site [26].

10.1.5. Scientific Expertise

Isabelle Chrisment served as a member of the GDR RSD/ASF selection committee for the thesis award.

Olivier Festor jointed Orange scientific council.

Jérôme François serves as reviewer for the program *Etablissement de nouveaux chercheurs et de nouvelles chercheuses universitaires du Fonds de recherche du Québec – Nature et technologies* (FRQNT)

10.1.6. 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 a member of the AFNIC's scientific council. She is also an elected member of the scientific pole AM2I (Automatique, Matheématiques, Informatique et leurs Interaction) at Universiteé de Lorraine. She is a member of the COMIPERS at Inria Nancy Grand Est. She is also involved in Inria's CVP (Cellule de Veille et Prospective) and in the CMI (Commission de la Mention Informatique) board, which is a part of the doctoral school IAEM.

Olivier Festor is member of the Scientific Council of Telecom Sud Paris. He is leading the IFIP TC6 Working Group 6.6 : Network and Service Management.

Jérôme François is a member of the Horizon Startup local committee in Nancy Grand Est.

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 2nd and 3rd 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.

Team members are teaching the following courses:

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

Thibault Cholez 300 hours - L3, M1, M2 - Computer Networks, Object-Oriented Programming, C 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 1)*, FUN Project, Université de Lorraine, Ingénieur, formation initiale et continue, Thibault Cholez, Rémi Badonnel, Laurent Andrey, Olivier Festor, Abdelkader Lahmadi, Jérôme François, de janvier à mars 2018, over 6400 inscriptions from 74 countries, and 370 certificates of achievement. Each MOOC Resist participant contributed to the 2018 maintenance for a second opening on January 2019.

10.2.2. Supervision

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

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

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

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*, supervised by Olivier Festor and Jérôme François.

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

PhD in progress: Xavier Marchal, Secure operation of virtualized Named Data Networks, since December 2015, supervised by Olivier Festor & Thibault Cholez.

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: Nicolas Schnepf, *Orchestration and Verification of Security Functions for Smart Environments*, since October 2016, supervised by Stephan Merz, Rémi Badonnel and Abdelkader Lahmadi.

PhD: Giulia De Santis, Modeling and Recognizing Network Scanning Activities with Finite. Mixture Models and Hidden Markov Models, Université de Lorraine, 20 December 2018, supervised by Olivier Festor and Abdelkader Lahmadi (not yet registred).

PhD: Maxime Compastié, *Software-defined Security for Distributed Clouds*, University of Lorraine, defended on December 18, 2018, supervised by Olivier Festor and Rémi Badonnel (not yet registred).

10.2.3. Juries

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

- Abdelhadi Azzouni, PhD in Computer Science from Université Pierre et Marie Curie - Sorbonne Universités, France. Title: Smart and Secure Network Softwarization, April 2018 – (Olivier Festor as reviewer).
- Lyes Bayou, Phd in Computer Science from from IMT Atlantique Bretagne-Pays de la Loire, France. Title: Evaluation et mise en oeuvre de la sécurité dans les systèmes SCADA à base de réseaux de capteurs sans fil, June 2018 – (Isabelle Chrisment as reviewer).
- Quang-Vinh Dang, Phd in Computer Science from Université de Lorraine, France. Trust assessment in large-scale collaborative systems, January 2018 – (Isabelle Chrisment as president).
- Pierre-Edouard Fabre, Phd in Computer Science from TELECOM SudParis, France. Title: Utiliser les ressources réseaux pour atténuer les attaques DDoS volumétriques, December 2018 – (Isabelle Chrisment as reviewer).
- Ghada Jaber, PhD in Computer Science from University of Toulouse, France. Title: A Content-Centric Approach for ireless Sensor Networks, December 2018 – (Olivier Festor as reviewer).
- Oualid Koucham, PhD in Automatic Control fromCommunauté Université Grenoble Alpes, France. Title: Détection d'intrusions pour les systèmes de contrôle industriels, November 2018 – (Isabelle Chrisment as reviewer).
- Alassane Samba, Phd in Computer Science from from IMT Atlantique Bretagne-Pays de la Loire, France. Title: Science des données au service des réseaux d'opérateur, October 2018 – (Isabelle Chrisment as reviewer).
- Farah Slim, PhD in Computer Science from IMT Atlantique Bretagne-Pays de la Loire, France. Title: Etude et impléementation d'algorithmes de gestion de ressources pour un système d'exploitation de réseau, March 2018 – (Olivier Festor as examiner).

10.3. Popularization

10.3.1. Interventions

- Débats Grenats, February 2018, Metz, France. Round table on the theme of security over its different forms, including risks induced by cyber-security. Rémi Badonnel.
- Libre sur la place, Nancy. Plongée au cœur des communautés De Debian à l'Open Core. Lucas Nussbaum.

11. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] M. COMPASTIÉ. *Software-defined Security for Distributed Clouds*, Université de Lorraine, December 2018

[2] G. DE SANTIS. *Modeling and Recognizing Network Scanning Activities with Finite Mixture Models and Hidden Markov Models*, Université de Lorraine, December 2018

Articles in International Peer-Reviewed Journals

[3] R. BADONNEL, R. KOCH, M. DRASAR, A. PRAS, V. EISELER, L. STIEMERT, S. SEEBER, D. TUNCER, M. CHARALAMBIDES, G. D. RODOSEK. *Report on the 10th IFIP International Conference on Autonomous Infrastructure, Management, and Security (IFIP AIMS)*, in "Journal of Network and Systems Management", October 2018, vol. 26, n° 4, pp. 1101 - 1109 [*DOI :* 10.1007/s10922-018-9460-5], https://hal.inria.fr/hal-01937234

[4] D. KONDO, T. SILVERSTON, V. VASSILIADES, H. TODE, T. ASAMI. *Name Filter: A Countermeasure against Information Leakage Attacks in Named Data Networking*, in "IEEE Access", October 2018, pp. 65151 - 65170 [*DOI :* 10.1109/ACCESS.2018.2877792], https://hal.archives-ouvertes.fr/hal-01946259

[5] J. VAN DER HOOFT, M. CLAEYS, N. BOUTEN, T. WAUTERS, J. SCHÖNWÄLDER, A. PRAS, B. STILLER, M. CHARALAMBIDES, R. BADONNEL, J. SERRAT, C. R. P. DOS SANTOS, F. DE TURCK. *Updated Taxonomy for the Network and Service Management Research Field*, in "Journal of Network and Systems Management", July 2018, vol. 26, n° 3, pp. 790 - 808 [*DOI :* 10.1007/s10922-017-9443-y], https://hal.inria.fr/hal-01937230

International Conferences with Proceedings

[6] A. ANTHONY, S. R. CHOWDHURY, T. BAI, R. BOUTABA, J. FRANÇOIS. *UNiS: A User-space Non-intrusive Workflow-aware Virtual Network Function Scheduler*, in "CNSM 2018 - 14th International Conference on Network and Service Management", Rome, Italy, November 2018, https://hal.inria.fr/hal-01947552

[7] P.-O. BRISSAUD, J. FRANÇOIS, I. CHRISMENT, T. CHOLEZ, O. BETTAN. *Passive Monitoring of HTTPS Service Use*, in "CNSM'18 - 14th International Conference on Network and Service Management", Rome, Italy, November 2018, 7 p. , https://hal.inria.fr/hal-01943936

[8] P. CHAIGNON, D. ADJAVON, K. LAZRI, J. FRANÇOIS, O. FESTOR. *Offloading Security Services to the Cloud Infrastructure*, in "SecSoN 2018 - SIGCOMM Workshop on Security in Softwarized Networks: Prospects and Challenges", Budapest, Hungary, August 2018, https://hal.inria.fr/hal-01939850

[9] P. CHAIGNON, K. LAZRI, J. FRANÇOIS, T. DELMAS, O. FESTOR. *Oko: Extending Open vSwitch with Stateful Filters*, in "SOSR 2018 - ACM Symposium on SDN Research", Los Angeles, United States, March 2018, pp. 1-13, https://hal.inria.fr/hal-01939857

[10] M. COMPASTIÉ, R. BADONNEL, O. FESTOR, R. HE. *Demo: On-The-Fly Generation of Unikernels for Software-Defined Security in Cloud Infrastructures*, in "NOMS 2018 - IEEE/IFIP Network Operations and Management Symposium", Taipei, Taiwan, April 2018 [*DOI :* 10.1109/NOMS.2018.8406131], https://hal.inria.fr/hal-01798799

[11] M. COMPASTIÉ, R. BADONNEL, O. FESTOR, R. HE, M. KASSI-LAHLOU. *Unikernel-based Approach for Software-Defined Security in Cloud Infrastructures*, in "NOMS 2018 - IEEE/IFIP Network Operations and Management Symposium", Taipei, Taiwan, Proceedings of the IEEE/IFIP Network Operations and Management Symposium, April 2018 [*DOI :* 10.1109/NOMS.2018.8406155], https://hal.inria.fr/hal-01798793

[12] Q.-V. DANG, J. FRANÇOIS. *Utilizing attack enumerations to study SDN/NFV vulnerabilities*, in "IEEE ETSN - International Workshop on Emerging Trends in Softwarized Networks", Montreal, Canada, June 2018, https://hal.inria.fr/hal-01763368

[13] G. DE SANTIS, A. LAHMADI, J. FRANÇOIS, O. FESTOR. *Internet-Wide Scanners Classification using Gaussian Mixture and Hidden Markov Models*, in "NTMS 2018 - 9th IFIP International Conference on New Technologies, Mobility and Security", Paris, France, February 2018, https://hal.inria.fr/hal-01935664

[14] N. KHAN, A. LAHMADI, J. FRANÇOIS, R. STATE. *Towards a management plane for smart contracts: Ethereum case study*, in "NOMS 2018 - IEEE/IFIP Network Operations and Management Symposium", Taipei, Taiwan, April 2018 [*DOI :* 10.1109/NOMS.2018.8406326], https://hal.inria.fr/hal-01935669

[15] M. MA, A. LAHMADI. *On the Impact of Synchronization Attacks on Distributed and Cooperative Control in Microgrid Systems*, in "IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids", Aalborg, Denmark, October 2018, https://hal.inria.fr/hal-01870771

[16] X. MARCHAL, T. CHOLEZ, O. FESTOR. *µNDN: an Orchestrated Microservice Architecture for Named Data Networking*, in "ACM-ICN'18 - 5th ACM Conference on Information-Centric Networking", Boston, United States, September 2018, 12 p. [*DOI :* 10.1145/3267955.3267961], https://hal.inria.fr/hal-01906996

[17] X. MARCHAL, M. EL AOUN, B. MATHIEU, T. CHOLEZ, G. DOYEN, W. MALLOULI, O. FESTOR. *Leveraging NFV for the deployment of NDN: Application to HTTP traffic transport*, in "NOMS 2018 - IEEE/IFIP Network Operations and Management Symposium", Taipei, Taiwan, IEEE, April 2018, 5 p. [*DOI :* 10.1109/NOMS.2018.8406206], https://hal.inria.fr/hal-01906994

[18] A. SAIF, A. MERLIN, L. NUSSBAUM, Y.-Q. SONG. *MonEx: An Integrated Experiment Monitoring Framework Standing on Off-The-Shelf Components*, in "P-RECS 2018: 1st International Workshop on Practical Reproducible Evaluation of Computer Systems", Tempe, AZ, United States, June 2018 [*DOI :* 10.1145/3214239.3214240], https://hal.inria.fr/hal-01793561

[19] A. SAIF, L. NUSSBAUM, Y.-Q. SONG. *IOscope: A Flexible I/O Tracer for Workloads' I/O Pattern Characterization*, in "ISC High Performance 2018 International Workshops - WOPSSS'18", Frankfurt, Germany, June 2018, https://hal.inria.fr/hal-01828249

[20] N. SCHNEPF, R. BADONNEL, A. LAHMADI, S. MERZ. *Generation of SDN policies for protecting Android environments based on automata learning*, in "NOMS 2018 - IEEE/IFIP Network Operations and Management Symposium", Taipei, Taiwan, Proceedings of the IEEE/IFIP Network Operations and Management Symposium (IEEE/IFIP NOMS), IEEE, April 2018 [*DOI :* 10.1109/NOMS.2018.8406153], https://hal.archives-ouvertes.fr/hal-01892390

[21] N. SCHNEPF, R. BADONNEL, A. LAHMADI, S. MERZ. *Rule-Based Synthesis of Chains of Security Functions for Software-Defined Networks*, in "AVOCS 2018 - 18th International Workshop on Automated Verification of Critical Systems", Oxford, United Kingdom, Proceedings of the International Workshop on Automated Verification of Critical Systems, July 2018, https://hal.archives-ouvertes.fr/hal-01892423

[22] N. SCHNEPF, R. BADONNEL, A. LAHMADI, S. MERZ. *Synaptic: A formal checker for SDN-based security policies*, in "NOMS 2018 - IEEE/IFIP Network Operations and Management Symposium", Taipei, Taiwan, IEEE, April 2018 [*DOI :* 10.1109/NOMS.2018.8406122], https://hal.archives-ouvertes.fr/hal-01892397

[23] W. M. SHBAIR, M. STEICHEN, J. FRANÇOIS, R. STATE. *Blockchain orchestration and experimentation framework: A case study of KYC*, in "IEEE/IFIP Man2Block 2018 - IEEE/IFIP Network Operations and Management Symposium", Taipei, Taiwan, April 2018, https://hal.inria.fr/hal-01939865

[24] M. ZAKROUM, A. HOUMZ, M. GHOGHO, G. MEZZOUR, A. LAHMADI, J. FRANÇOIS, M. E. KOUTBI. *Exploratory Data Analysis of a Network Telescope Traffic and Prediction of Port Probing Rates*, in "ISI 2018 - IEEE Intelligence and Security Informatics", Miami, United States, November 2018, https://hal.inria.fr/hal-01947984

Conferences without Proceedings

[25] H. L. MAI, M. AOUADJ, G. DOYEN, D. KONDO, X. MARCHAL, T. CHOLEZ, E. MONTES DE OCA, W. MALLOULI. *Implementation of Content Poisoning Attack Detection and Reaction in Virtualized NDN Networks*, in "ICIN 2018 - 21st Conference on Innovation in Clouds, Internet and Networks", Paris, France, February 2018, 3 p. , https://hal.inria.fr/hal-01907004

[26] X. MANIVAL, L. NUSSBAUM, S. S. DUPLESSIS, E. MONTARGE`S-PELLETIER, P. HUMBERT. *Table ronde sur les aspects "utilisateurs" : intérêts et retours d'expériences de chercheurs et enseignants-chercheurs du site*, in "Colloque Sciences ouvertes : expériences, enjeux et perspectives", Vandœuvre-lès-Nancy, France, Université de Lorraine and Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation, October 2018, https://hal.univ-lorraine.fr/hal-01885979

[27] L. NUSSBAUM. *Experiment Data Management*, in "GEFI 2018 - Global Experimentation for Future Internet", Tokyo, Japan, October 2018, https://hal.inria.fr/hal-01944472

[28] L. NUSSBAUM. *Grid'5000*, in "Grid'5000/FIT School", Sophia-Antipolis, France, April 2018, https://hal.inria.fr/hal-01944478

[29] A. SAIF, A. MERLIN, L. NUSSBAUM, Y.-Q. SONG. *Monitoring Testbed Experiments with MonEx*, in "Grid5000-FIT Spring School", Sophia Antipolis, France, SILECS project, Inria, April 2018, https://hal.inria.fr/hal-01793507

Research Reports

[30] F. BECK, J. FRANÇOIS, T. LACOUR, A. LAHMADI. *Verifying Security Requirements of an IoT device using SCUBA Tool Suite*, Inria Nancy - Grand Est (Villers-lès-Nancy, France) ; In collaboration with Red Alert Labs, November 2018, https://hal.inria.fr/hal-01948512

Other Publications

[31] 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

[32] A. LAHMADI, F. BECK. *Security Analysis of Internet of Things Devices: Hands-on lab*, June 2018, AIMS 2018 - 12th International Conference on Autonomous Infrastructure, Management and Security, https://hal.inria.fr/hal-01943543

References in notes

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

[34] 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

[35] 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

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

[37] 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

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