UMR IRISA

Activity Report 2018

Team CIDRE

Confidentiality, Integrity, Availability and Repartition

Joint team with Inria Rennes – Bretagne Atlantique

D1 – Large Scale Systems

Table of contents

Project-Team CIDRE

Creation of the Project-Team: 2011 July 01

Keywords:

Computer Science and Digital Science:

A1.1.8. - Security of architectures
A1.2.3. - Routing
A1.2.8. - Network security
A1.3. - Distributed Systems
A1.3.3. - Blockchain
A1.3.4. - Peer to peer
A1.3.5. - Cloud
A2.3.1. - Embedded systems
A3.1.5. - Control access, privacy
A3.3.1. - On-line analytical processing
A3.4.1. - Supervised learning
A3.4.2. - Unsupervised learning
A3.5.2. - Recommendation systems
A4.1. - Threat analysis
A4.1.1. - Malware analysis
A4.1.2. - Hardware attacks
A4.4. - Security of equipment and software
A4.5. - Formal methods for security
A4.8. - Privacy-enhancing technologies
A4.9.1. - Intrusion detection
A4.9.2. - Alert correlation

Other Research Topics and Application Domains:

B6.3.3. - Network Management
B6.5. - Information systems
B9.6.2. - Juridical science
B9.10. - Privacy

1. Team, Visitors, External Collaborators

Research Scientists

Emmanuelle Anceaume [CNRS, Researcher]
Michel Hurfin [Inria, Researcher, HDR]
Jean-Louis Lanet [Inria, Senior Researcher, from May 2018, HDR]
Ludovic Mé [Inria,Senior Researcher, HDR]

Faculty Members

Christophe Bidan [CentraleSupelec, Professor, HDR]
Gilles Guette [Univ de Rennes I, Associate Professor]
Guillaume Hiet [CentraleSupelec, Associate Professor]

Jean-Francois Lalande [CentraleSupelec, Associate Professor, HDR]
Guillaume Piolle [CentraleSupelec, Associate Professor]
Eric Totel [CentraleSupelec, Professor, HDR]
Frédéric Tronel [CentraleSupelec, Associate Professor]
Valérie Viet Triem Tong [Team leader, CentraleSupelec, Associate Professor, HDR]
Pierre Wilke [CentraleSupelec, Associate Professor,from september 2018]

Post-Doctoral Fellows

Ludovic Claudepierre [Inria, from May 2018]
Jerome Fellus [Univ de Rennes I, from Sep 2018]
Mouad Lemoudden [Inria, from Apr 2018]

PhD Students

Aimad Berady [Ministère des Armées, from Nov 2018]
Sebanjila Bukasa [Inria, from May 2018]
Vasile Cazacu [CNRS]
Ronny Chevalier [Hewlet Packard France]
Damien Crémilleux [CentraleSupelec, until Sep 2018]
Aurélien Dupin [Thales]
Mathieu Escouteloup [Inria, from Oct 2018]
Benoit Fournier [Univ de Rennes I, from Nov 2018]
Cyprien Gottstein [Orange Labs, from Oct 2018]
Pierre Graux [Inria]
Cedric Herzog [Inria, from Nov 2018]
David Lanoé [Inria]
Laetitia Leichtnam [Ministère de la Défense]
Mourad Leslous [Inria, until Aug 2018]
Pernelle Mensah [Bell Labs (Alcatel)]
Ruta Moussaileb [IMT Atlantique, from May 2018]
Mounir Nasr Allah [CentraleSupelec, until Nov 2018]
Leopold Ouairy [Inria, from May 2018]
Thomas Letan [ANSSI, until November 2018]
Aurelien Palisse [Inria, from May 2018]
Aurélien Trulla [Inria, until Aug 2018]
Charles Arya Xosanavongsa [Thales]

Technical staff

Antoine Guellier [CNRS, until Feb 2018]
Souhir Laribi [Inria, from Nov 2018]

Interns

Samuel Pipet [CentraleSupelec, from Jun 2018 until Jul 2018]
Raj Krishnan Vijayaraj [CentraleSupelec, from May 2018 until Jul 2018]

Administrative Assistant

Lydie Mabil [Inria]

Visiting Scientist

Carlos Alberto Maziero [Professor at Federal University of Parana (Curitiba, Brazil)]

External Collaborators

Frédéric Majorczyk [DGA]
Sébastien Gambs [UQAM, HDR]

2. Overall Objectives

2.1. CIDRE in Brief

The Cidre team is concerned with security and privacy issues. Our long-term ambition is to contribute to the construction of widely used systems that are trustworthy and respectful of privacy, even when parts of the system are targeted by attackers.

With this objective in mind, the CIDRE team focuses mainly on the three following topics:

- **Attack comprehension**
- **Attack detection**
- **Attack resistance**

3. Research Program

3.1. Our perspective

For many aspects of our daily lives, we rely heavily on computer systems, many of which are based on massively interconnected devices that support a population of interacting and cooperating entities. As these systems become more open and complex, accidental and intentional failures become much more frequent and serious. We believe that the purpose of attacks against these systems is expressed at a high level (compromise of sensitive data, unavailability of services). However, these attacks are often carried out at a very low level (exploitation of vulnerabilities by malicious code, hardware attacks).

The CIDRE team is specialized in the defense of computer systems. We argue that to properly protect these systems we must have a complete understanding of the attacker's concrete capabilities. In other words, **to defend properly we must understand the attack**.

The CIDRE team therefore strives to have a global expertise in information systems: from hardware to distributed architectures. Our objective is to highlight security issues and propose preventive or reactive countermeasures in widely used and privacy-friendly systems.

3.2. Attack Comprehension

The first step before being able to offer secure systems is to understand and measure the real capabilities of the attacker. It's a cat and mouse game and in this game, the attacker is always one step ahead of the defender. The attacker is able to exploit for his own benefit all the services, machines, codes that are accessible to him, even on systems that seem highly protected.

Our first research axis therefore aims at highlighting both the effective attacker's means and the way an attack unfolds and spreads.

This knowledge is valuable for security experts who must react quickly during an attack. They need effective ways to understand how their systems may have been compromised.

The main scientific challenge is to be able to adapt to all the attacker's protections against automatic analysis that the attacker could imagine.

In this context, we are particularly interested in

- **highlighting attacks** on hardware that affect software security
- **providing expert support**
  - to analyze malicious code
  - to quickly investigate an intrusion on a system monitored by an intrusion detection system

3.3. Attack Detection

An attack has several phases. A first major phase is the approach phase, during which the attacker enters the system, locates the target and makes himself persistent, the attack is at this point a simple intrusion. In a second phase, the attack is actually launched.

The main objective of intrusion detection is to be able to detect the attacker during the first approach phase. For that purpose, an intrusion detection system (IDS) is based on probes that continuously monitor the system. These probes generate low level alerts (warnings) for any observation of an event that could be a sign of an intrusion. These low-level alerts are very numerous and their semantic value is low. In other words, an IDS generates a huge amount of low-level alerts that bring only few information and overwhelm the security analyst. In addition, many of these alerts are actually false positives, *i.e.* alerts raised when there is no real intrusion.

However, these low-level alerts can themselves be considered as security events by a higher-level IDS: an alert correlation system. These higher-level IDS seek to exploit known relationships between low-level alerts to generate meta-alerts with greater semantic value, *i.e.* with higher-level meaning. An alert correlation system allows to reduce the number of alerts (and especially, false positives) and to return to the security analysts a higher level analysis of the situation.

There are mainly two approaches to detect intrusions. The misuse-based detection and the anomaly-based detection. A misuse-based detection is actually a signature-based detection approach: it allows to detect only the attacks whose signature is available. From our point of view, while useful in practice, misuse-detection is intrinsically limited. Indeed, it requires to continuously update the database of signatures. We follow the alternative approach, namely the anomaly approach, which consists in detecting any deviation from a reference behavior. The main difficulty is thus to compute a model of this reference behavior. Such a model is only useful if it is sufficiently accurate. Otherwise, if the model is an over-approximation, it will be a source of false negatives, *i.e.* real intrusions not detected. If the model is a under-approximation, it will be a source of false positives, *i.e.* normal behaviors seen as intrusions.

In this context, our contributions in intrusion detection systems follow two separate axes: anomaly-based IDS and alert correlation systems. Our contribution in anomaly-based intrusion detection relies on:

- **Illegal Information Flow Detection:** we have proposed to detect information flows in the monitored system (either a node or a set of trusted nodes) that are allowed by the access control mechanism, but are illegal from the security policy point of view. This approach is particularly appealing to detect intrusions in a standalone node.
- **Anomaly-Based Detection in Distributed Applications:** our goal is to specify the normal behavior based on either a formal specification of the distributed application, or previous executions. This approach is particularly appealing to detect intrusions in industrial control systems since these systems exhibit well-defined behaviors at different levels: network level (network communication patterns, protocol specifications, etc.), control level (continuous and discrete process control laws), or even the state of the local resources (memory or CPU).
- **Online data analytics:** our goal is to estimate on the fly different statistics or metrics on distributed input streams to detect abnormal behavior with respect to a well-defined criterion such as the distance between different streams, their correlation or their entropy.

3.4. Attack Resistance

The first two axes of the team allowed us to measure the concrete technical means of the attacker. We claim that the attacker can always avoid the measures put in place to secure a system. We believe that another way to offer more secure systems is to take into account from the design phase that these systems will operate in the presence of an omnipotent attacker. The last research axis of the CIDRE team is focused on offering systems that are resistant to attackers, *i.e.* they can provide the expected services even in the presence of an attacker.

To achieve this goal, we explore two approaches:

- be able to take into account all possible actions of the attacker
- provide services based on the collaboration of a set of nodes that are not affected by the presence in minority of malicious nodes

We are interested in massively-used systems that are essential building blocks of security or privacy.

4. Application Domains

4.1. Security is required everywhere

With the infiltration of computers and software in almost all aspects of our modern life, security can nowadays be seen as an absolutely general concern. As such, the results of the research targeted by CIDRE apply to a wide range of domains. It is clear that critical systems, in which security (and safety) is a major concern, can benefit from ideas such as dynamic security policy monitoring. On the other hand, systems used by the general public (basically, the internet and services such as web or cloud services, social networks, location-based services, etc.) can also benefit from the results obtained by CIDRE, in particular to solve some of the privacy issues raised by these systems that manipulate huge amounts of personal data. In addition, systems are getting more and more complex, decentralized, distributed, or spontaneous. Cloud computing, in particular, brings many challenges that could benefit from ideas, approaches and solutions studied by CIDRE in the context of distributed systems.

Industrial Control Systems (ICS) and in particular Supervisory Control and Data Acquisition are also new application domains for intrusion detection. The Stuxnet attack has emphasized the vulnerability of such critical systems which are not totally isolated anymore. Securing ICS is challenging since modifications of the systems, for example to patch them, are often not possible. High availability requirements also often conflict with preventive approaches. In this case, security monitoring is appealing to protect such systems against malicious activities. Intrusion detection in ICS is not fundamentally different from traditional approaches. However, new hypotheses and constraints need to be taken into account, which also bring interesting new research challenges.

5. New Software and Platforms

5.1. Blare

To detect intrusion using information flows
KEYWORDS: Cybersecurity - Intrusion Detection Systems (IDS) - Data Leakage Protection
SCIENTIFIC DESCRIPTION: Blare implements our approach of illegal information flow detection for a single node (Android and Linux kernel, JVM) and a set of nodes (monitoring of flows between linux machines).
FUNCTIONAL DESCRIPTION: Blare IDS is a set of tools that implements our approach to illegal information flow detection for a single node and a set of nodes.

NEWS OF THE YEAR: During this year, Laurent Georget has modified the implementation of Blare in order to correctly monitor the kernel system calls with LSM hooks. He add also ported this new version of Blare to the Lollipop Android emulator.

- Partner: CentraleSupélec
- Contact: Frédéric Tronel
- Publications: Information Flow Tracking for Linux Handling Concurrent System Calls and Shared Memory - Verifying the Reliability of Operating System-Level Information Flow Control Systems in Linux - Monitoring both OS and program level information flows to detect intrusions against network servers - Experimenting a Policy-Based HIDS Based on an Information Flow Control Model - Introducing reference flow control for intrusion detection at the OS level - Blare Tools: A Policy-Based Intrusion Detection System Automatically Set by the Security Policy - Diagnosing intrusions in Android operating system using system flow graph - Intrusion detection in distributed systems, an approach based on taint marking - BSPL: A Language to Specify and Compose Fine-grained Information Flow Policies - Information Flow Policies vs Malware - A taint marking approach to confidentiality violation detection - Designing information flow policies for Android's operating system - Information Flow Control for Intrusion Detection derived from MAC Policy - Flow based interpretation of access control: Detection of illegal information flows - A taint marking approach to confidentiality violation detection
- URL: http://www.blare-ids.org

5.2. GNG

Security Supervision by Alert Correlation
KEYWORDS: Intrusion Detection Systems (IDS) - SIEM
SCIENTIFIC DESCRIPTION: GNG is an intrusion detection system that correlates different sources (such as different logs) in order to identify attacks against the system. The attack scenarios are defined using the Attack Description Langage (ADeLe) proposed by our team, and are internally translated to attack recognition automatons. GNG intends to define time efficient algorithms based on these automatons to recognize complex attack scenarios.

- Partner: CentraleSupélec
- Contact: Eric Totel
- Publication: A Language Driven Intrusion Detection System for Events and Alerts Correlation
- URL: http://www.rennes.supelec.fr/ren/perso/etotel/GNG/index.html

5.3. GroddDroid

KEYWORDS: Android - Detection - Malware
SCIENTIFIC DESCRIPTION: GroddDroid automates the dynamic analysis of a malware. When a piece of suspicious code is detected, groddDroid interacts with the user interface and eventually forces the execution of the identified code. Using Blare (Information Flow Monitor), GroddDroid monitors how an execution contaminates the operating system. The output of GroddDroid can be visualized in an web browser. GroddDroid is used by the Kharon software.
FUNCTIONAL DESCRIPTION: GroddDroid 1 - locates suspicious code in Android application 2 - computes execution paths towards suspicious code 3 - forces executions of suspicious code 4 - automate the execution of a malware or a regular Android application

NEWS OF THE YEAR: In 2017, GroddDroid has integrated the work of Mourad Leslous, who have implemented GFinder. GPFinder improves the computation of control flow paths by taking into account the Android framework. The end of the year has been used to clean the code and to improves the graphical interface.

- Partners: CentraleSupélec - Insa Centre Val-de-Loire
- Contact: Valérie Viet Triem Tong
- Publications: Kharon dataset: Android malware under a microscope - GroddDroid: a Gorilla for Triggering Malicious Behaviors - GPFinder: Tracking the Invisible in Android Malware - Information flows at OS level unmask sophisticated Android malware
- URL: http://kharon.gforge.inria.fr/grodddroid.html

5.4. Kharon

KEYWORDS: Android - Malware - Dynamic Analysis
FUNCTIONAL DESCRIPTION: Kharon is a software for managing Android application analysis. Kharon uses the results of the GroddDroid software. The user can submit one or several applications to Kharon and get a graph of the innformation flows that occured at system level and that have been caused by the application.

Kharon is used in the Kharon platform for the analysis of malicious applications. This platform is deployed at the high security laboratory (LHS) of Rennes.

- Author: Sébastien Campion
- Partners: CentraleSupélec - Insa Centre Val-de-Loire
- Contact: Valérie Viet Triem Tong
- URL: http://kharon.gforge.inria.fr/

5.5. StarLord

KEYWORDS: Security - SIEM
FUNCTIONAL DESCRIPTION: In the domain of security event visualisation, we have developed a prototype called StarLord. Basically, this software is able to parse heterogeneous logs, and to extract from each line of logs a set of security objects. Moreover, some of these objects appears in several lines of different logs. These lines are thus linked by the sharing of one or more security objects. When we analyse the lines of logs, we are thus able to generate graphs that represents the links between the different objects discovered in the logs. These graphs are thus displayed in 3D in order for the administrator to investigate easily the relations between the logs and the relations between the logs and some particular indicators of compromission. The tool permits to discover visually the activity of an attacker on the supervised system.

- Authors: Ludovic Mé, Eric Totel, Nicolas Prigent and Laetitia Leichtnam
- Contact: Eric Totel
- Publication: STARLORD: Linked Security Data Exploration in a 3D Graph

5.6. SpecCert

KEYWORDS: Formal methods - Coq
FUNCTIONAL DESCRIPTION: SpecCert is a framework for specifying and verifying Hardware-based Security Enforcement (HSE) mechanisms against hardware architecture models. HSE mechanisms form a class of security enforcement mechanism such that a set of trusted software components relies on hardware functions to enforce a security policy.

- Participant: Thomas Letan
- Partners: ANSSI - CentraleSupélec
- Contact: Guillaume Hiet
- Publications: SpecCert: Specifying and Verifying Hardware-based Security Enforcement - SpecCert: Specifying and Verifying Hardware-based Software Enforcement
- URL: https://github.com/lethom/speccert

5.7. HardBlare

KEYWORDS: Intrusion Detection Systems (IDS) - FPGA - Static analysis
FUNCTIONAL DESCRIPTION: HardBlare is a hardware/software framework to implement hardware DIFC on Xilinx Zynq Platform. HardBlare consists of three components : 1) the VHDL code of the coprocessor, 2) a modified LLVM compiler to compute the static analysis, and 3) a dedicated Linux kernel. This last component is a specific version of the Blare monitor.

- Partners: CentraleSupélec - Lab-STICC
- Contact: Guillaume Hiet
- Publications: ARMHEx: A hardware extension for DIFT on ARM-based SoCs - ARMHEx: a framework for efficient DIFT in real-world SoCs - ARMHEx: embedded security through hardware-enhanced information flow tracking - HardBlare: a Hardware-Assisted Approach for Dynamic Information Flow Tracking - A portable approach for SoC-based Dynamic Information Flow Tracking implementations - Towards a hardware-assisted information flow tracking ecosystem for ARM processors - HardBlare: an efficient hardware-assisted DIFC for non-modified embedded processors

5.8. Conductor

KEYWORDS: Intrusion Detection Systems (IDS) - Static analysis - Instrumentation
FUNCTIONAL DESCRIPTION: Conductor contains three main components: a static analysis to extract the expected behavior of the target, an instrumentation module to add instructions to the target's code in order to send messages to the co-processor, and an intrusion detection engine executed on the co-processor. The latter processes the messages sent by the instrumented target, describing its current behavior. This behavior is then compared against the expected behavior previously extracted by the static analysis.

- Participants: Ronny Chevalier, Guillaume Hiet, Maugan Villatel and David Plaquin
- Partners: CentraleSupélec - HP Labs
- Contact: Ronny Chevalier
- Publication: Co-processor-based Behavior Monitoring: Application to the Detection of Attacks Against the System Management Mode

5.9. Platforms

5.9.1. Kharon platform

The Kharon platform is under development in the LHS of Rennes and should be ready to use in the beginning of 2018. This experimental platform aims to analyze Android malware using a set of software developed by the CIDRE team. Software that are involved are:

- The Blare IDS http://www.blare-ids.org/, and in particular the AndroBlare version, for tracking information flows of malware;
- The GroddDroid software http://kharon.gforge.inria.fr/grodddroid.html, for manipulating the malware statically and dynamically;
- The GPFinder software http://kharon.gforge.inria.fr/gpfinder.html, for computing paths in the malware's control flow;
- The kharon software that handles the orchestration of a bunch of malware, the server and a set of smartphones.

The Kharon platform will be used for analysing malware as soon as they appear in the wild. The analysis results will be stored for further experiments and statistics.

6. New Results

6.1. Axis 1 : Attack comprehension

6.1.1. Attacks stay possible even when programs seem not vulnerable

The protection of any software starts at the hardware level. In ,K. Bukasa, L. Claudepierre, J.-L. Lanet, in collaboration with R. Lashermes from SED Inria Rennes – Bretagne Atlantique, explore how Electromagnetic Fault Injection (EMFI) can disturb the behavior of a chip and undermine the security of the information handled by the target. They demonstrate the possibilities to create software vulnerabilities with hardware fault injection (with EM pulses), not against crypto-systems but targeting regular software running on IoT devices. Experimentations are conducted on an ARMv7-M (Cortex-M3) microcontroller, present at the heart of a wide-range of embedded systems, to prove that a fault attack is able to create a vulnerability in a code where there is none in the usual software security meaning. Protecting against vulnerabilities must thus encompass protecting against both software and hardware attacks.

6.2. Axis 2 : Attack detection

6.2.1. Intrusion detection in sequential control systems.

Sophisticated process-aware attacks targeting industrial control systems require adequate detection measures taking into account the physical process. In [20], we propose an approach relying on automatically mined process specifications to detect attacks on sequential control systems. The specifications are synthesized as monitors that read the execution traces and report violations to the operator. In contrast to other approaches, a central aspect of our method consists in reducing the number of mined specifications suffering from redundancies. We evaluate our approach on a hardware-in-the-loop testbed with a complex physical process model and discuss the mining efficiency and attack detection capabilities of our approach.

6.2.2. Hardware-based Information Flow Tracking

The HardBlare project proposes a software/hardware co-design methodology to ensure that security properties are preserved all along the execution of the system but also during files storage. It is based on the Dynamic Information Flow Tracking (DIFT) that generally consists in attaching tags to denote the type of information that are saved or generated within the system. These tags are then propagated when the system evolves and information flow control is performed in order to guarantee the safe execution and storage within the system monitored by security policies.

Existing hardware DIFT approaches have not been widely used neither by research community nor by hardware vendors. It is due to two major reasons: current hardware DIFT solutions lack support for multi-threaded applications and implementations for hardcore processors. In [10] we addresse both issues by introducing an approach with some unique features: DIFT for multi-threaded software, virtual memory protection (rather than physical memory as in related works) and Linux kernel support using an information flow monitor called RFBlare. These goals are accomplished by taking advantage of a notable feature of ARM CoreSight components (context ID) combined with a custom DIFT coprocessor and RFBlare. The communication time overhead, major source of slowdown in total DIFT time overhead, is divided by a factor 3.8 compared to existing solutions with similar software constraints as in this work. The area overhead of this work is lower than 1% and power overhead is 16.2% on a middle-class Xilinx Zynq SoC.

Most of hardware-assisted solutions for software security, program monitoring, and event-checking approaches require instrumentation of the target software, an operation which can be performed using an SBI (Static Binary Instrumentation) or a DBI (Dynamic Binary Instrumentation) framework. Hardware-assisted instrumentation can use one of these two solutions to instrument data to a memory-mapped register. Both these approaches require an in-depth knowledge of frameworks and an important amount of software modifications in order to instrument a whole application. In [11] we propose a novel way to instrument an application, at the source code level, taking advantage of underlying hardware debug components such as CS (CoreSight)

components available on Xilinx Zynq SoCs. As an example, the instrumentation approach proposed in this work is used to detect a double free security attack. Furthermore, it is evaluated in terms of runtime and area overhead.

6.2.3. Alert correlation in intrusion detection.

In distributed systems and in particular in industrial SCADA environments, alert correlation systems are necessary to identify complex multi-step attacks within the huge amount of alerts and events. In [22] we describe an automata-based correlation engine developed in the context of a European project where the main stakeholder was an energy distribution company. The behavior of the engine is extended to fit new requirements. In the proposed solution, a fully automated process generates thousands of correlation rules. Despite this major scalability challenge, the designed correlation engine exhibits good performance. Expected rates of incoming low level alerts approaching several hundreds of elements per second are tolerated. Moreover, the data structures chosen allow to quickly handle dynamic changes of the set of correlation rules. As some attack steps are not observed, the correlation engine can be tuned to raise an alert when all the attack steps except k of them have been detected. To be able to react to an ongoing attack by taking countermeasures, alerts must also be raised as soon as a significant prefix of an attack scenario is recognized. Fulfilling these additional requirements leads to an increase in the memory consumption. Therefore purge mechanisms are also proposed and analyzed. An evaluation of the tool is conducted in the context of a SCADA environment.

6.2.4. Most recent and frequent items in distributed streams for DDoS detection.

The need to analyze in real time large-scale and distributed data streams has recently became tremendously important to detect attacks (DDoS), anomalies or performance issues. In particular the identification of recent heavy-hitters (or hot items) is essential but highly challenging. Actually, this problem has been heavily studied during the last decades with both exact and probabilistic solutions. While simple to state and fundamental for advanced analysis, answering this issue over a sliding time window and among distributed nodes is still an active research field. The distributed detection of frequent items over a sliding time window presents two extra challenging aspects with respect to the centralized detection of frequent items since the inception of the stream: (i) Treat time decaying items as they enter and exit the sliding window; (ii) Produce mergeable local stream summaries in order to obtain a system-wide summary. In [12], we propose a sliding window-based solution of the top k most frequent items based on a deterministic counting of the most over-represented items in the data streams, which are themselves probabilistically identified using a dynamically defined threshold. Performance of our new algorithm are astonishingly good, despite any items order manipulation or distributed execution.

6.2.5. Propagation of information.

Together with Yves Mocquard and Bruno Sericola, we have worked on the well studied dissemination of information in large scale distributed networks through pairwise interactions. The information to be propagated can simply be a bit of information to any code, including viruses. This problem, originally called rumor mongering, and then rumor spreading has mainly been investigated in the synchronous model. This model relies on the assumption that all the nodes of the network act in synchrony, that is, at each round of the protocol, each node is allowed to contact a random neighbor. In this paper, we drop this assumption under the argument that it is not realistic in large scale systems. We thus consider the asynchronous variant, where at random times, nodes successively interact by pairs exchanging their information on the rumor. In a previous paper, we performed a study of the total number of interactions needed for all the nodes of the network to discover the rumor. While most of the existing results involve huge constants that do not allow us to compare different protocols, we provided a thorough analysis of the distribution of this total number of interactions together with its asymptotic behavior [4]. In addition to this study, we have proposed an algorithm that allows, through simple pairwise interactions, each node of the large scale and dynamic system to build a global clock which allows any node to maintain with high probability a common temporal referential [25]. By combining this global clock together with the rumor spreading algorithm, we have proposed a mechanism that allows each node to locally detect that the system has converged to a sought configuration with high probability. We

have also shown the applicability of our convergence detection mechanism to many other pairwise interaction-based protocols. For instance, our construction can be applied to a leader election protocol provided that its convergence time is known with high probability [26].

6.3. Axis 3 : Attack resistance

6.3.1. Connectivity in an inter-MANET network.

New generation radio equipment, used by soldiers and vehicles on the battlefield, form ad hoc networks and specifically, Mobile Ad hoc NETworks (MANET). The battlefields where these equipments are deployed include a majority of coalition communication. Each group on the battleground may communicate with other members of the coalition and establish inter-MANET links. These inter-MANET links are governed by routing policies that can be summarized as Allowed or Denied link. However, if more than two groups form a coalition, blocked multi-hop communications and non-desired transmissions due to these restrictive policies would appear. In [19], we present these blocking cases and theoretically evaluate their apparition frequency. Then, we present two alternatives to extend the binary policies and decrease the number of blocking cases. Finally, we describe an experimental scenario containing a blocking case and evaluate our propositions and their performance.

6.3.2. Permissionless ledgers for decentralized cryptocurrency systems (blockchain).

The goal of decentralized cryptocurrency systems is to offer a medium of exchange secured by cryptography, without the need of a centralized banking authority. An increasing number of distributed cryptocurrency systems are emerging, and among them Bitcoin, which is often designated as the pioneer of this kind of systems. Bitcoin circumvents the absence of a global trusted third-party by relying on a blockchain, an append-only data-structure, publicly readable and writable, in which all the valid transactions ever issued in the system are progressively appended through the creation of cryptographically linked blocks. In [15], we propose a new way to organise both transactions and blocks in a distributed ledger to address the performance issues of permissionless ledgers. In contrast to most of the existing solutions in which the ledger is a chain of blocks extracted from a tree or a graph of chains, we present a distributed ledger whose structure is a balanced directed acyclic graph of blocks. We call this specific graph a SYC-DAG. We show that a SYC-DAG allows us to keep all the remarkable properties of the Bitcoin blockchain in terms of security, immutability, and transparency, while enjoying higher throughput and self-adaptivity to transactions demand.

6.3.3. Modular verification of Programs with Effects and Effect Handlers in Coq

Modern computing systems have grown in complexity, and the attack surface has increased accordingly. Even though system components are generally carefully designed and even verified by different groups of people, the composition of these components is often regarded with less attention. This paves the way for architectural attacks, a class of security vulnerabilities where the attacker is able to threaten the security of the system even if each of its components continues to act as expected. In [24], we introduce FreeSpec, a formalism built upon the key idea that components can be modelled as programs with algebraic effects to be realized by other components. FreeSpec allows for the modular modelling of a complex system, by defining idealized components connected together, and the modular verification of the properties of their composition. In addition, we have implemented a framework for the Coq proof assistant based on FreeSpec.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- **HP (2013-2019): Embedded Systems Security** We aim at researching and prototyping low-level intrusion detection mechanisms in embedded system software. This involves mechanisms in continuation of previous work realized by our team as well as investigating new techniques more directly tied to specific HP device architectures. Our main objective is to monitor low-level software (firmware, OS kernels, hypervisors) thanks to a dedicated external co-processor. Ronny Chevalier is doing is PhD in the context of this project. Being under NDA, details about this research program cannot be provided.

7.2. Bilateral Grants with Industry

- **ANSSI: Security of Low-level Components** Thomas Letan has started his PhD thesis in the context of a contract between CentraleSupelec and the French National Computer Security Agency (ANSSI). His work consists in using formal methods to specify hardware/software security mechanisms and to verify that they correctly enforce some security policies.
- **DGA: Visualization for security events monitoring** Damien Crémilleux has started his PhD thesis in October 2015 in the context of a cooperation with DGA-MI. The subject of the PhD is to define relevant representations to allow front-line security operators to monitors systems from a security perspective. A first proposal was made that led to a tool, VEGAS, that allows to monitor large quantities of alerts in real time and to dispatch these alerts in a relevant way to security analysts.
- **DGA: Intrusion Detection in Distributed Applications** David Lanoé has started his PhD thesis in October 2016 in the context of a cooperation with DGA-MI. His work is focussing on the construction of behavioral models (during a learning phase) and their use to detect intrusions during an execution of the modelled distributed application.
- **DGA: Protection against fuzzing attack** Aurelien Palisse has started his PhD in October 2015 in the context of a cooperation with DGA-MI. The subject of the PhD is to propose a detection mechanism and a mitigation procedure to counter ransomware attacks. He designed a low cost Windows driver that use a Markov chain as a model for an anomaly detection system. The technology has been patented by both Inria and DGA.
- **Idemia: Hardware Security for Embeded Devices** Kevin Bukasa has started his PhD in January 2016 in a bilateral contract between Inria and Idemia. He explored fault injection attacks using EM probes on two different kind of devices: microcontroller (representing IoT) and SoC (representing Smart phone). He demonstrated the vulnerability of both architectures on this kind of attack. On IoT device he has developped an attack allowing to take a full control on the device. He discovered also new fault attacks never described in the litterature.
- **Idemia: Protection against fuzzing attack** Leopold Ouairy has started his PhD in October 2017 in a bilateral contract between Inria and Idemia. The context is related with security testing of Java applications to avoid fuzzing attack. The approach is based on AI to design automatically a model use for the oracle. He used machine learning to serach in a corpus of applicatons methods having the same semantics. Then in a second step, after convertir the source code into a vector he compute a similarity value which is related with absence of conditions evaluation.
- **Ministry of Defence: Visualisation for the characterization of security events** Laetitia Leichtnam has started his PhD thesis in November 2016 in the context of a contract between CentraleSupelec and the French Ministry of Defence. His work consists in presenting events appearing in heterogeneous logs as a dependency graph between the lines of logs. This permits to the administrator to investigate easily the logs to discover the different steps that has performed an attack in the supervised system.
- **Ministry of Defence: Characterization of an attacker** Aïmad Berady has started his PhD thesis in November 2018 in the context of a contract between CentraleSupelec and the French Ministry of Defence. His work is to highlight the characteristics of an attacker performing a targeted and long-term attack on an information system.

- **Nokia: Risk-aware security policies adaptation in modern communication infrastructures** Pernelle Mensah was hired in January 2016 on this CIFRE funding in order to work on unexplored aspects of information security, and in particular response strategies to complex attacks, in the context of cloud computing architectures. The use case proposed by our industrial partner is a multi-tenant cloud computing platform involving software-defined networking in order to provide further flexibility and responsiveness in architecture management. The topic of the thesis is to adapt and improve the current risk-aware reactive response tools, based on attack graphs and adaptive security policies, to this specific environment, taking into account the heterogeneity of actors, platforms, policies and remediation options.
- **Orange LAb's: Storage and query in a massive distributed graph for the web of things** Cyprien Gottstein has started his PhD thesis in October 2018 in the context of a collaboration between Inria and Orange (I/O Lab). In this thesis, we consider storage and query problems that arise when massive distributed graphs are used to represent the web of things. In particular, access to the data and partitioning of the graph are studied to propose efficient geographical services.
- **Thales: Privacy and Secure Multi-party Computation** Aurélien Dupin has started his PhD thesis in January 2016 within the context of a CIFRE contract with Thales. His PhD subject concerns secure multi-party computation. Secure two-party computation provides a way for two parties to compute a function, that depends on the two parties' inputs, while keeping them private. Known since the 1980s, Yao's garbled circuits appear to be a general solution to this problem, in the semi-honest model. Decades of optimizations have made this tool a very practical solution. However, it is well known that a malicious adversary could modify a garbled circuit before submitting it. Many protocols, mostly based on cut-&-choose, have been proposed to secure Yao's garbled circuits in the presence of malicious adversaries. Nevertheless, how much an adversary can modify a circuit and make it still executable have not been studied. In the context of his PhD, Aurélien Dupin is interested by such a question.
- **Thales: Combining Attack Specification and Dynamic Learning from traces for correlation rule generation** Charles Xosanavongsa has started his PhD thesis in December 2016 in the context of a CIFRE with Thales. His work will focus on the construction of correlation rules. In previous work on correlation rule generation, the usual approach is static. It always relies on the description of the supervised system using a knowledge base of the system. The use of correlation trees is an appealing solution because it allows to have a precise description of the attacks and can handle any kind of IDS. But in practice, the behavior of each IDS is quite difficult to predict, in particular for anomaly based IDS. To manage automatically the correlation rules (and adapt them if necessary), we plan to analyze synthetic traces containing both anomaly based and misused based IDS alerts resulting from an attack.

8. Partnerships and Cooperations

8.1. Regional Initiatives

- **Region Bretagne ARED Grant :** the PhD of Mourad Leslous on malicious codes in Android applications is supported by a grant from the Région Bretagne.
- **Labex COMINLABS contract (2014-2018): "Kharon-Security" - http://kharon.gforge.inria.fr**

  Google Play offers more than 800'000 applications (apps), and this number increases every day. Google play users have performed more than 25 billion app downloads. These applications vary from games to music, video, books, tools, etc. Unfortunately, each of these application is an attack vector on Android. The number of malicious applications (pieces of malware) discovered during the first six months of 2013 exceeds the number of pieces of malware discovered during the 2010 to 2012 period, more than 700 thousand malicious and risky applications were found in the wild. In

this context, we propose the Kharon-Security project to stem the progression of Android pieces of malware. We propose to combine static and dynamic monitoring to compute a behavioral signature of Android malware. Behavioral signatures are helpful to understand how malware infect the devices and how they spread information in the Android operating system. Static analysis is essential to understand which particular event or callback triggers malware payload.

In the project we have already developed GroddDroid a tool dedicated to automatic identification and execution of suspicious code. We have also built a dataset of Android malware. In this dataset, all malware are entirely manually reverse and documented. We have also developed an analysis platform. This platform is been deployed at the High Research Laboratory.

- **Labex COMINLABS contract (2015-2018): "HardBlare-Security" - https://hardblare.cominlabs.u-bretagneloire.fr/**

  The general context of the HardBlare project is to address Dynamic Information Flow Tracking (DIFT) that generally consists in attaching marks to denote the type of information that is saved or generated within the system. These marks are then propagated when the system evolves and information flow control is performed in order to guarantee a safe execution and storage within the system. Existing solutions imply a large overhead induced by the monitoring process. Some attempts rely on a hardware-software approach where DIFT operations are delegated to a coprocessor. Nevertheless, such approaches are based on modified processors. Beyond the fact hardware-assisted DIFT is hardly adopted, existing works do not take care of coprocessor security and multicore/multiprocessor embedded systems.

  We plan to implement DIFT mechanisms on boards including a non-modified ARM processor and a FPGA such as those based on the Xilinx Zynq family. The HardBlare project is a multidisciplinary project between CentraleSupélec IETR SCEE research team, CentraleSupélec Inria CIDRE research team and UBS Lab-STICC laboratory. Mounir Nasr Allah is doing his PhD in the context of this project. The main objective of this PhD is to study how hybrid analysis could improve hardware assisted DIFT using static analysis performed at compile-time. Another objective is to manage labels for persistent memory (i.e., files) using a modified OS kernel.

- **Labex COMINLABS contract (2016-2019): "BigClin" - https://bigclin.cominlabs.u-bretagneloire.fr/fr**

  Health Big Data (HBD) is more than just a very large amount of data or a large number of data sources. The data collected or produced during the clinical care process can be exploited at different levels and across different domains, especially concerning questions related to clinical and translational research. To leverage these big, heterogeneous, sensitive and multi-domain clinical data, new infrastructures are arising in most of the academic hospitals, which are intended to integrate, reuse and share data for research.

  Yet, a well-known challenge for secondary use of HBD is that much of detailed patient information is embedded in narrative text, mostly stored as unstructured data. The lack of efficient Natural Language Processing (NLP) resources dedicated to clinical narratives, especially for French, leads to the development of ad-hoc NLP tools with limited targeted purposes. Moreover, the scalability and real-time issues are rarely taken into account for these possibly costly NLP tools, which make them inappropriate in real-world scenarios. Some other today's challenges when reusing Health data are still not resolved: data quality assessment for research purposes, scalability issues when integrating heterogeneous HBD or patient data privacy and data protection. These barriers are completely interwoven with unstructured data reuse and thus constitute an overall issue which must be addressed globally.

  In this project, we plan to develop distributed methods to ensure both the scalability and the online processing of these NLP/IR and data mining techniques; In a second step, we will evaluate the added value of these methods in several real clinical data and on real use-cases, including epidemilology and pharmaco-vigilance, clinical practice assessment and health care quality research, clinical trials.

8.2. National Initiatives

8.2.1. ANR

- **ANR Project: PAMELA (2016-2020) - https://project.inria.fr/pamela/**

  PAMELA is a collaborative ANR project involving Rennes 1 university (ASAP and CIDRE teams in Rennes), Inria Lille (MAGNET team), LIP6 (MLIA team) and two start-ups, Mediego and Snips. It aims at developing machine learning theories and algorithms in order to learn local and personalized models from data distributed over networked infrastructures. The project seeks to provide first answers to modern information systems built by interconnecting many personal devices holding private user data in the search of personalized suggestions and recommendations. More precisely, we will focus on learning in a collaborative way with the help of neighbors in a network. We aim to lay the first blocks of a scientific foundation for these new types of systems, in effect moving from graphs of data to graphs of data and learned models. CIDRE's contribution in this project involves the design of adversary models and privacy metrics suitable to the privacy-related issues of this distributed learning paradigm.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

Carlos Maziero, Professor at the Federal University of Parana (Curitiba, Brazil) has visited our team from January 2018 till December 2018. During his stay, he has worked on models of normal behaviours in distributed applications.

8.3.1.1. Research Stays Abroad

Mourad Leslous did an international mobility of three months in the team of Lorenzo Cavallaro in the Information Security Group (ISG) at Royal Holloway, University of London. This mobility was part of the program of EIT Digital Doctoral School, a European institute that promotes entrepreneurship and innovation among PhD students. During this mobility, he worked on control flow and data flow dependencies in order to detect the malicious code inside Android applications.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

Jean-Louis Lanet served as general chair of the 13rd International Conference on Risks and Security of Internet and Systems CRiSIS 2018, Bordeaux France and general chair of the 11th International Conference on Information Technology and Communication Security, Bucharest, Romania,

9.1.1.2. Member of the Organizing Committees

Christophe Bidan served as a member of the organization committee of C&ESAR 2018 (25rd Computers & Electronics Security Applications Rendez-vous), November 2018, Rennes, France.

Frédéric Tronel served as a member of the organization committee of SSTIC 2018 (Symposium sur la sécurité des technologies de l'information et des communications) that took place in Rennes, France in June, where it gathered more than 600 participants.

Gilles Guette served as a member of the organization committee of InOut18, annual event on new mobility that took place in Rennes, France in March.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

Eric Totel chaired the Program Committee of the 2018 French conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information).

9.1.2.2. Member of the Conference Program Committees

Frédéric Tronel and Valérie Viet Triem Tong served as a member of the program committee of SSTIC 2017 (Symposium sur la sécurité des technologies de l'information et des communications) June 2018, Rennes, France.

Valérie Viet Triem Tong served as a member of the program committee of SECITC (International conference on Information Technology and Communications Security), october 2018, Bucharest, Romania.

Jean-François Lalande served as a member of the program committee of the international conferences CECC 2018, IEEE AINS 2018, IEEE HPCS 2018 and of the international workshops SHPCS 2018, IWCC 2018, CUING 2018, BioSTAR 2018, WTMC 2018, DACSW 2018.

Michel Hurfin acts as a member of the program committee of the African Conference on Research in Computer Science and Applied Mathematics (CARI 2018), South Africa, October 2018.

Emmanuelle Anceaume served as a member of the program committee of the following international conferences: ICDCN 2018, NCA 2018 CryBlock 2018, DEBS 2018, PEC 2018, BSCT 2018, and ADSN 2018.

Ludovic Mé served as a member of the 2018 MSPN (International Conference on Mobile, Secure and Programmable Networking) and CARI (Colloque Africain sur la Recherche en Informatique et Mathématiques Appliquées 2018) program Committees.

Guillaume Piolle served as a member of the 2018 APVP (Atelier sur la Protection de la Vie Privée) and EGC-IA (Extraction et Gestion des Connaissances - Intelligence Artificielle) program committees.

Gilles Guette served as a member of the program committee of the International Conference on Information Systems Security and Privacy, ICISSP 2018.

9.1.2.3. Reviewer

Valérie Viet Triem Tong served as a reviewer for the African Conference on Research in Computer Science and Applied Mathematics, October 2018, South Africa, Stellenbosch.

Jean-François Lalande served as a reviewer for ICISSP 2018, APVP 2018.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Jean-François Lalande served as a member of the editorial board of IARIA International Journal on Advances in Security.

Michel Hurfin serves as a member of the editorial board of the JISA Journal (Journal of Internet Services and Applications - Springer).

9.1.3.2. Reviewer - Reviewing Activities

Jean-François Lalande served as a reviewer for Journal of Universal Computer Science, Elsevier FGCS, IEEE TIFS, MDPI Future Internet, MDPI Sensors, Elsevier Computer Commmunications.

Michel Hurfin served as a reviewer for the IEEE TDSC Journal (Transactions on Dependable and Secure Computing), the Springer TOCS Journal (Theory of Computing Systems), and the Taylor & Francis International Journal of Control.

Emmanuelle Anceaume served as a reviewer of the following journals: IEEE TPDS, and ACM TAAS.

Jean Louis Lanet served as reviewer for the Journal of Computer Security.

Guillaume Piolle served as a reviewer for the RIA (Revue d'Intelligence Artificielle) journal.

Guillaume Hiet served as a reviewer for the Journal of Computer Security.

Gilles Guette served as a reviewer for the IEEE JSAC-SI-NETSOFT-ENABLERS and for the IEEE Networking Letters.

9.1.4. Invited Talks

Emmanuelle Anceaume gave several talks:

- *UTXOs as a proof of membership for Byzantine Agreement based Cryptocurrencies* during the National Days of the pre-GDR on security, june 2018.
- *Beyond the block: A lego blockumentary* during "Journées scientifiques de l'Inria".
- *Sycomore, a Directed Acyclic Graph of Blocks*, Chain-in conference, Porto, Portugal, July 2018, [6], also on Youtube "https://www.youtube.com/watch?v=YLW-iHjsWo0".

Valérie Viet Triem Tong gives a talk about *information flow monitoring at the operating system level* during the National Days of the pre-GDR on security, june 2018.

Jean-François Lalande was invited as keynote speaker at SecITC'2018 [7].

Jean-François Lalande was an invited speaker of the workshop SHPCS 2018 [8].

Guillaume Piolle was an invited speaker at the *Surveillance Resilience, & Privacy* conference (Paris, December 2018).

9.1.5. Scientific Expertise

Ludovic Mé has served the Scientific Council of the LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées).

Ludovic Mé has chaired the group of experts dedicated to the evaluation of the security of French computer science research labs (PPST S/C 7).

Ludovic Mé has chaired the Steering Committee of the annual French conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information).

Eric Totel has served the Steering Committee of the annual French conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information).

Valérie Viet Triem Tong has participated in the scientific evaluation comity *Global Security and Cybersecurity* (CES 39) of the French Research Agency (ANR).

9.1.6. Research Administration

Ludovic Mé acts as Scientific Officer for the Rennes - Bretagne Atlantic Inria Research Center. As such, he is also a member of the Evaluation Commission and of the Internal Scientific Council of Inria.

Ludovic Mé was the president of a recruitment committee for an assistant professor position at the CNAM (Conservatoire national des arts et métier, Paris). He also served a recruitment committee for an assistant professor position at CentraleSupélec, Rennes.

Valérie Viet Triem Tong was a member of a recruitment committee for an assistant professor position at CentraleSupélec, Rennes.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: Emmanuelle Anceaume, *Research in Computer Science - Distributed Algorithms*, 20 hours of lecture, M2; Université Rennes 1, France;

Licence: Christophe Bidan, *Algorithms and Data Structures*, 36 hours of lecture including 7.5 hours of lectures, L3 - first year of the engineering degree, CentraleSupélec, France;

Licence: Christophe Bidan, *Software Engineering*, 12 hours, L3 - first year of the engineer degree, CentraleSupélec, France;

Licence: Christophe Bidan, *Supervision of student project*, 1 project, L3 - first year of the engineer degree, CentraleSupélec, France;

Master: Christophe Bidan is responsible for the module *Secured information systems*, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Christophe Bidan, *Applied cryptography*, 6 hours of lecture, M2 - master 2 degree, University of Rennes 1, France;

Master: Christophe Bidan, *Applied cryptography*, 15 hours including 6 hours of lecture, M2 - third year of the engineer degree, CentraleSupélec, France;

Master : Christophe Bidan, *Cryptographic Protocols*, 6 hours of lecture, mastère CS (Cyber Security), CentraleSupélec, France;

Master: Christophe Bidan, *Information systems*, 4.5 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Christophe Bidan, *Supervision of student project*, 2 projects, M1 - second year of the engineer degree, CentraleSupélec, France;

Licence: Gilles Guette, *Algorith and Complexity*, 36 hours, L1 - Licence, ISTIC/University of Rennes, France;

Licence: Gilles Guette, *Network Initiation*, 72 hours, L3 - Licence, ISTIC/University of Rennes, France;

Licence: Gilles Guette, *Network Initiation*, 69 hours, L3 - first year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Network Routing*, 45 hours, M1 - second year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Mobile Network Routing*, 5 hours, M1 - second year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Advanced Network Services*, 13 hours, M1 - second year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Network Project*, 24 hours, M1 - second year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Security*, 46 hours, M1 - second year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Sensors Network*, 28 hours, M2 - Master, ISTIC/University of Rennes, France;

Master: Gilles Guette, *Supervision of student*, Contrat de professionnalisation, M2 - third year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Supervision of student internship*, M2 - ISTIC/University of Rennes, France;

Licence: Guillaume Hiet, *Algorithms and Data Structures*, 12.5 hours, L3 - first year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Hiet, *Computer security and privacy for the engineer*, 8 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Hiet, *Buffer overflow vulnerabilities*, 16 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Hiet, *Buffer overflow vulnerabilities*, 16 hours, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;

Master: Guillaume Hiet, *Pentest*, 19 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Hiet, *Pentest*, 3 hours, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;

Master: Guillaume Hiet, *Introduction to Linux*, 3 hours, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;

Master: Guillaume Hiet, *Java Security*, 4.5 hours, M2 - Mastère Spécialisé CS, CentraleSupélec, France;

Master: Guillaume Hiet, *Linux Security*, 18 hours, M2 - Mastère Spécialisé CS , CentraleSupélec, France;

Master: Guillaume Hiet, *Linux Security*, 7.5 hours, third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Hiet, *LDAP*, 7.5 hours, third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Hiet, *Intrusion Detection*, 15 hours, M2 - Mastère Spécialisé CS, CentraleSupélec, France;

Master: Guillaume Hiet, *Intrusion Detection*, 13.5 hours, M2 - third year of the engineer degree, M2 research degree of University of Rennes 1, CentraleSupélec, France;

Master: Guillaume Hiet, *Security Monitoring*, 3 hours, M2, cycle "Sécurité Numérique", INHESJ, France;

Master: Guillaume Hiet, *Computer Security*, 31.5 hours, M2, Mastère Spécialisé Architecte des Systèmes d'Information, CentraleSupélec, France;

Master: Guillaume Hiet, *Intrusion Detection*, 16 hours, M2, University of Rennes 1, France;

Master: Guillaume Hiet, *Intrusion Detection*, 10 hours, M2 - third year of the engineer degree, ESIR, France;

Master: Guillaume Hiet, *Intrusion Detection*, 9 hours, M2, Université of Limoges, France;

Master: Guillaume Hiet, *Firewall*, 6 hours, M2, University of Rennes 1, France;

Master: Guillaume Hiet, *Supervision of student project*, 4 projects, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Hiet, *Supervision of student project*, 2 projects, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Hiet, *Supervision of student project*, 2 projects, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;

Licence: Jean-François Lalande, *Algorithms and data structures*, 22 hours, L3 - first year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Computer Sciences*, 13 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Operating System*, 7 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Legal aspects of information security*, 4 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Android mobile development*, 18 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Web development*, 18 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Supervision of student projects*, 7 projects, engineer degree, CentraleSupélec, France;

Licence: Guillaume Piolle, *Software engineering*, 1.5 hours, L3 - first year of the engineering degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Modelling, Algorithms and Programming*, 22 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Computer security and privacy*, 5 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Software project*, 3.5 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Relational databases*, 6 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Computer networks*, 30 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Security Policies*, 4.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Java programming*, 4.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Computer networks*, 9 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Software engineering*, 12 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Network Access Control*, 9 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Web development*, 32 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Privacy protection*, 18 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Computing project*, 60 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Guillaume Piolle, *Legal aspects of information security*, 4.5 hours, M2 - master CyberSecurity, CentraleSupélec, France;

Licence : Eric Totel, *Foundations of computer science, data structures and algorithms*, 9 hours, L3 - first year of the engineer degree, CentraleSupélec, France;

Licence : Eric Totel, *Software Modeling*, 15 hours, L3 - first year of the engineer degree, CentraleSupélec, France;

Master : Eric Totel, *Operating Systems*, 30 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master : Eric Totel, *C language*, 24 hours including 6 hours of lecture, M2 - master CS (Cyber Security), CentraleSupélec, France;

Master : Eric Totel, *C language and C++ language*, 12 hours including 6 hours of lecture, M2 - third year of the engineer degree, CentraleSupélec, France;

Master : Eric Totel, *Dependability* , 9 hours including 7.5 hours of lecture, M2 - third year of the engineer degree and master research, CentraleSupélec, France;

Master : Eric Totel, *Dependability*, 3 hours of lecture, M2 - third year of the engineer degree (ingénierie des systèmes automatisés), CentraleSupelec, France;

Master : Eric Totel, *Dependability*, 4.5 hours of lecture, M2 - post-graduate training (master Architecture des Réseaux de Communication), CentraleSupélec, France;

Master : Eric Totel, *Intrusion Detection*, 6 hours of lecture, M2 - M2 - master CS (Cyber Security), CentraleSupélec, France;

Master : Eric Totel, *Intrusion Detection*, 9 hours of lecture, M2 - master 2 degree, University of Rennes 1, France;

Master : Eric Totel, *Supervision of student project*, 4 projects, M1 - second year of the engineer degree, CentraleSupélec, France;

Master : Eric Totel, *Supervision of student project,* 1 project, M2 - third year of the engineer degree, CentraleSupélec, France;

Licence: Frédéric Tronel, *Software engineering*, 40 hours, L3 - first year of the engineer degree, CentraleSupélec, France;

Licence: Frédéric Tronel, *Operating Systems*, 12 hours, L3 - first year of the engineer degree, CentraleSupélec, France;

Master: Frédéric Tronel, *Operating systems*, 21 hours hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Frédéric Tronel, *Assembly Language*, 6 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Frédéric Tronel, *Buffer overflow vulnerabilities (theory and practice)*, 20.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Frédéric Tronel, *Firewall*, 15 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Frédéric Tronel, *Calculability in distributed systems*, 6 hours, M2, jointly with University of Rennes 1 and CentraleSupélec, France;

Master: Frédéric Tronel, *Computer network*, 8 hours, M2, jointly with University of Rennes 1 and CentraleSupélec, France;

Licence : Valérie Viet Triem Tong, *Algorithms and Data Structures*, 36 hours of lecture including 7 hours of lectures, L3 - first year of the engineering degree, CentraleSupélec, France;

Licence : Valérie Viet Triem Tong, *Supervision of student project*, 2 projects of 2nd year of the engineer degree, CentraleSupélec, France;

Master: Valérie Viet Triem Tong is responsible of the M2 degree in *CyberSecurity* (mastère spécialisé), organized jointly by CentraleSupélec and Institut Mines Télécom (IMT) Atlantique, France;

Master : Valérie Viet Triem Tong, *Formal Methods*, 9 hours, M2 - third year of the engineering degree, CentraleSupélec, France;

Master : Valérie Viet Triem Tong, *Intrusion detection using information flow control*, 9 hours, M2 / third year of the engineering degree, CentraleSupélec, France;

Master : Valérie Viet Triem Tong, , *Compilers*, 18 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master : Valérie Viet Triem Tong, *Supervision of student project*, 2 project, mastere CS (Cyber Security), CentraleSupélec, France;

Master : Valérie Viet Triem Tong, *Supervision of student project,* 1 project, M2 - third year of the engineer degree, CentraleSupélec, France;

Doctorant : Valérie Viet Triem Tong, *Malware analysis*, 6 hours, Research week, ENS Lyon, Lyon, France;

9.2.2. Supervision

9.2.2.1. Thesis defended in 2018

PhD: Thomas Letan, *Contribution à la sécurité des couches basses des systèmes d'information*, novembre 2018, supervised by Guillaume Hiet (50%), Pierre Chifflier (25% - ANSSI), and Ludovic Mé (25%);

PhD: Oualid Koucham, *Détection d'intrusions pour les systèmes de contrôle industriels*, november 2018, supervised by Stéphane Mocanu (50% - Gipsa-lab), Guillaume Hiet (25%), and Jean-Marc Thiriet (25% - Gipsa-lab);

PhD : Mourad Leslous, *Highlighting and executing Android suspicious execution path in Android malware*, 18th december 2018, supervised by Thomas Genet (20% - Celtique Inria project), Jean François Lalande (40% - INSA Centre Val de Loire), and Valérie Viet Triem Tong (40%);

PhD : Yves Mocquard, *Population protocols*, december 2018, supervised by Bruno Sericola (Dyonisos Inria project) and Emmanuelle Anceaume;

PhD : Razika Lounas, *Validation des spécifications formelles de la mise à jour dynamique des applications Java Card*, December 2018, supervised by Jean-Louis Lanet (50%) and Mohamed Mezguiche (50%-Limose, Algerie)

PhD : Abdelhak Mesbah, *Rétroconeption d'application Java Card*, November 2018, supervised by Jean-Louis Lanet (50%) and Mohamed Mezguiche (50%-Limose, Algerie)

9.2.2.2. Theses in progress

PhD in progress (previously in Tamis): Aurélien Palisse, *Detection and early mitigation of ransomware on Windows platforms*, started in 2015, supervised by Jean-Louis Lanet and Hélène Le Bouder (IMT Atlantique);

PhD in progress (previously in Tamis): Kevin Bukasa, *Vulnerability analysis of a Secure Enclave in Embedded Devices*, started in 2016, supervised by Jean-Louis Lanet and Ronan Lashermes (SED Inria);

PhD in progress (previously in Tamis): Leopold Ouairy, *Analyse des vulnérabilités dans des systèmes embarqués*, started in 2017, supervised by Jean-Louis Lanet;

PhD in progress: Mathieu Escouteloup *Micro-architectures Sécurisées*, started in 2018, supervised by Jean-Louis Lanet and Jacques Fournier (CEA);

PhD in progress: Damien Crémilleux, *Visualisation d'évènements de sécurité pour la supervision*, started in October 2015, supervised by Christophe Bidan (30%), Nicolas Prigent (35%), and Frédéric Majorczyk (35% - DGA MI);

PhD in progress: Mounir Nasr Allah, *Contrôle de flux d'information par utilisation conjointe d'analyse statique et d'analyse dynamique accélérée matériellement*, started in November 2015, supervised by Guillaume Hiet (75%) and Ludovic Mé (25%);

PhD in progress: Pernelle Mensah, *Adaptation de la Politique de Sécurité guidée par l'Évaluation du Risque dans les Infrastructures de Communication modernes*, started in January 2016, supervised by Eric Totel (25%), Guillaume Piolle (25%), Christine Morin (25% - Myriad Inria project), and Samuel Dubus (25% - Nokia);

PhD in progress: David Lanoë, *Détection d'intrusion dans les applications distribuées : l'approche comportementale comme alternative à la corrélation d'alertes*, started in october 2016, supervised by Michel Hurfin (50%) and Eric Totel (50%);

PhD in progress : Ronny Chevalier , *Enhanced computer platform security through an intrusion-detection approach*, started in November 2016, supervised by Guillaume Hiet (50%), Boris Balacheff (25% - HP), and Ludovic Mé (25%);

PhD in progress: Laetitia Leichtnam, *Visualisation pour la caractérisation d'événements de sécurité*, started in october 2016, supervised by Eric Totel (40%), Nicolas Prigent (30%) and Ludovic Mé (30%);

PhD in progress : Charles Xosanavongsa, *Combining Attack Specification and Dynamic Learning from traces for correlation rule generation*, started in december 2016, supervised by Eric Totel (50%) and Ludovic Mé (50%);

PhD in progress : Pierre Graux, *Security of Hybrid Mobile Applications*, started in october 2017, supervised by Valérie Viet Triem Tong (50%) and Jean-Francçois Lalande (50%);

PhD in progress : Vasile Cazacu, *Calcul distribué pour la fouille de données cliniques*, started February 2017, supervised by Emmanuelle Anceaume (50%) and Marc Cuggia (50%)

PhD in progress : Aurélien Dupin, *Secure multi-partie computations*, started February 2016, supervised by Christophe Bidan(40%), David Pointchavalm (30% - ENS) and Renaud Dubois (30% - Thales).

PhD in progress : Cedric Herzog, *Simulation d'environnement d'observation afin d'éviter le déploiement de malware sur une station de travail*, started in November 2018, supervised by Jean Louis Lanet (50%), Pierre Wilke (25%) and Valérie Viet Triem Tong (25%);

PhD in progress : Benoit Fournier, *Secure routing in drone swarms*, started in november 2018, supervised by Gilles Guette (50%), Jean Louis Lanet (25%) and Valérie Viet Triem Tong (25%);

PhD in progress : Aimad Berady, *Attacker characterization*, started in november 2018, supervised by Christophe Bidan (25%), Guillaume Carat (25%),Gilles Guette (25%), and Valérie Viet Triem Tong (25%);

PhD in progress : Cyprien Gottstein, *Problématiques de stockage et d'interrogation de très grands graphes répartis dans le contexte de l'internet des objets*, started in october 2018, supervised by Michel Hurfin (50%) and Philippe Raipin Parvedy (50%);

9.2.2.3. Supervision of external PhD candidates

LL. D. (Doctor of Laws) in progress: Gustav Malis, *Droit à l'effacement des données mises à disposition par les personnes elles-mêmes*, started in March 2014, supervised by Annie Blandin (80% - IODE) and Guillaume Piolle (20%);

Ruta Moussaileb, in progress, *From Data Signature to Behavior Analysis* started January 2018, supervised by Nora Cuppens (50%-) and Jean-Louis Lanet (50%)

9.2.3. Juries

Valérie Viet Triem Tong has reported the following PhD thesis:

Mickael Salaun, *Inte´gration de l'utilisateur au contro^le d'acce`s: du processus cloisonne´ a` l'interface homme-machine de confiance*, february 2018.

Alicia Filipiak, *Design and formal analysis of security protocols, an application to electronic voting and mobile payment*, march 2018.

Anaël Beaugnon, *Expert-in-the-Loop Supervised Learning for Computer Security Detection Systems*, june 2018.

Steve Muller, *Risk Monitoring and Intrusion Detection for Industrial Control System*, june 2018

Guilia De Santis, *Modeling and Recognizing Network Scanning Activities with Finite Mixture Models and Hidden Markov Models*, december 2018.

Jean-Louis Lanet has reported the following PhD thesis:

Mark Angoustures, December 2018, *Automatic malicious behaviors extraction usable in malware detection*

Damien Marion, December 2018 *Multidimensionality of the Models and the Data in the Side Channel Domain*

Guillaume Hiet was a member of the PhD committee for the following PhD thesis:

Thomas Letan, *Specifying and Verifying Hardware-based Security Enforcement Mechanisms*, October 2018.

Oualid Koucham, *Détection d'intrusions pour les systèmes de contrôle industriels*, November 2018.

Muhammad Abdul WAHAB, *Support matériel pour l'analyse de sécurité du comportement des applications*, December 2018.

Valérie Viet Triem Tong was a member of the PhD committee for the following PhD thesis:

Guillaume Brogi, *Real-time detection of Advanced Persistent Threats using Information Flow Tracking and Hidden Markov Models*, february 2018.

Mourad Leslous, *Highlighting and Executing Suspicious Paths in Android Malwar*, december 2018.

Mark Angoustures, *Extraction automatique de caracte´ristiques malveillantes et me´thode de de´tection de malware dans un environnement re´el*, december 2018.

Jean-François Lalande has reported the following PhD thesis:

Guillaume Brogi, *Détection temps réel de Menaces Persistentes Avancées par Suivi de Flux d'Information et Modèles de Markov Cachés*, april 2018.

Jean-François Lalande was a member of the PhD committee for the following PhD thesis:

Mourad Leslous, *Highlighting and Executing Suspicious Paths in Android Malwar*, december 2018.

Jean-Louis Lanet was a member of the PhD committee for the following PhD thesis:

Khanh Huu The DAM, 2018, *Automatic Learning and Extraction of Malicious Behaviors*

Emmanuelle Anceaume was a member of the grading PhD committee of

Ivan Walulya PhD thesis *On design and applicatins of practical concurrent data structures*, Chalmers University, Sweden, November 2018.

Emmanuelle Anceaume was a member of the PhD committee of

Yves Mocquard, *Analyse probabiliste de protocoles de population* December, 2018.

Ludovic Mé was a member of the PhD committee for the following PhD committee of :

Tan Ngoc Nguyen, *A Security Monitoring Plane for Information Centric Networking: application to Named Data Networking*, Université de Technologie de Troyes, 2018.

9.3. Popularization

9.3.1. Articles and contents

- Emmanuelle Anceaume was interviewed by Jean-Michel Prima. This gave rise to an article: "Améliorer le Bitcoin ... à coup de fourches", Emergences Inria, 2018.
- Jean François Lalande and Valérie Viet Triem Tong were interviewed by Jean-Michel Prima. This gave rise to an article: "Disséquer automatiquement les malware sous Android", Emergences Inria, 2018.
- Emmanuelle Anceaume belonged to the working group “Blockchains challenges” organized by the french governmental group “France Strategie”. This gave rise to a report accessible here: https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-blockchain-21-juin-2018.pdf.

9.3.2. Interventions

Interviews, videos and podcasts :

Emmanuelle Anceaume was interviewed by Joanna Jongwane for a https://interstices.info/le-potentiel-revolutionnaire-de-la-technologie-blockchain/podcast in online Interstice journal, 2018. (Talk is in french).

Emmanuelle Anceaume was interviewed by the Parliamentary Office For Scientific and Technological Assessment (OPECST) in 2018. The OPECST acts as an intermediary between the political world and the world of research. The goal of this interview was to describe the Bitcoin cryptocurrency system and its associated blockchain, and to discuss on the different vulnerabilities Bitcoin is confronted with.

Emmanuelle Anceaume was interviewed by the *mission d'information sur l'usage des blockchains*, by the French National Assembly in 2018.

Demos : Practical results concerning malware analysis issued from the Kharon project were presented during:

Forum International de la Cybersécurité at Lille in 2018

Fête de la science at Inria in 2018

These works also regularly presented during the visits of the *Laboratoire Haute Sécurité* in the Inria Rennes Bretagne Atlantique center.

9.3.3. Internal action

- Emmanuelle Anceaume was invited to join the internal meetings at La Cordée Rennes on "Blockchain focus: Cinéma: Quel potential d'innovation", November the 8th, 2018.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] T. LETAN. *Specifying and Verifying Hardware-based Security Enforcement Mechanisms*, CentraleSupélec, October 2018, https://hal.inria.fr/tel-01989940

Articles in International Peer-Reviewed Journals

[2] E. ANCEAUME, J.-M. PRIMA. *Améliorer le Bitcoin ... à coup de fourches*, in "Emergences Inria", September 2018, https://hal.archives-ouvertes.fr/hal-01888309

[3] A. MESBAH, J.-L. LANET, M. MEZGHICHE. *Reverse engineering Java Card and vulnerability exploitation: a shortcut to ROM,*, in "International Journal of Information Security", February 2018, pp. 1-16 [*DOI :* 10.1007/s10207-018-0401-9], https://hal.inria.fr/hal-01887577

[4] Y. MOCQUARD, B. SERICOLA, E. ANCEAUME. *Probabilistic Analysis of Rumor Spreading Time*, in "INFORMS Journal on Computing", July 2018, pp. 1-20 [*DOI :* 10.1287/xxxx.0000.0000], https://hal.archives-ouvertes.fr/hal-01888300

[5] Y. WANG, P. WILKE, Z. SHAO. *An abstract stack based approach to verified compositional compilation to machine code*, in "Proceedings of the ACM on Programming Languages", January 2019, vol. 3, n^{o} 62, 30 p. , https://hal.archives-ouvertes.fr/hal-02018168

Invited Conferences

[6] E. ANCEAUME. *Sycomore, a Directed Acyclic Graph of Blocks*, in "The International Industrial & Academic Conference on Blockchain Technology - Chain-In", Porto, France, July 2018, Invited talk, https://hal.archives-ouvertes.fr/hal-01888302

[7] J.-F. LALANDE. *Android Malware Analysis: from technical difficulties to scientific challenges*, in "SecITC 2018 - International Conference on Information Technology and Communications Security", Bucharest, Romania, LNCS, November 2018, pp. 1-54, https://hal-centralesupelec.archives-ouvertes.fr/hal-01906318

[8] J.-F. LALANDE, V. VIET TRIEM TONG, M. LESLOUS, P. GRAUX. *Challenges for Reliable and Large Scale Evaluation of Android Malware Analysis*, in "SHPCS 2018 - International Workshop on Security and High Performance Computing Systems", Orléans, France, IEEE Computer Society, July 2018, pp. 1068-1070 [*DOI :* 10.1109/HPCS.2018.00173], https://hal-centralesupelec.archives-ouvertes.fr/hal-01844312

[9] G. PIOLLE. *The robustness of security and privacy properties in decentralized applications*, in "Surveillance, Resilience & Privacy Conference 2018", Paris, France, December 2018, https://hal.inria.fr/hal-01988306

International Conferences with Proceedings

[10] M. ABDUL WAHAB, P. COTRET, M. NASR ALLAH, G. HIET, A. KUMAR BISWAS, V. LAPOTRE, G. GUY. *A small and adaptive coprocessor for information flow tracking in ARM SoCs*, in "ReConFig 2018 - International Conference on Reconfigurable Computing and FPGAs", Cancun, Mexico, Proceedings of the 2018 International Conference on ReConFigurable Computing and FPGAs (ReConFig), December 2018, pp. 1-17, https://hal.archives-ouvertes.fr/hal-01911619

[11] M. ABDUL WAHAB, P. COTRET, M. NASR ALLAH, G. HIET, V. LAPOTRE, G. GUY, A. KUMAR BISWAS. *A novel lightweight hardware-assisted static instrumentation approach for ARM SoC using debug components*, in "AsianHOST 2018 - Asian Hardware Oriented Security and Trust Symposium", Hong Kong, China, Proceedings of the 2018 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), December 2018, pp. 1-13, https://hal.archives-ouvertes.fr/hal-01911621

[12] E. ANCEAUME, Y. BUSNEL, V. CAZACU. *Finding Top-k Most Frequent Items in Distributed Streams in the Time-Sliding Window Model*, in "DSN 2018 - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks", Luxembourg, Luxembourg, IEEE, June 2018, pp. 1-2 [*DOI :* 10.1109/DSN-W.2018.00030], https://hal-imt-atlantique.archives-ouvertes.fr/hal-01839930

[13] E. ANCEAUME, Y. BUSNEL, V. CAZACU. *On the Fly Detection of the Top-k Items in the Distributed Sliding Window Model*, in "NCA 2018 - 17th IEEE International Symposium on Network Computing and Applications", Boston, United States, IEEE, November 2018, pp. 1-8 [*DOI :* 10.1109/NCA.2018.8548097], https://hal.archives-ouvertes.fr/hal-01888298

[14] E. ANCEAUME, A. GUELLIER, R. LUDINARD. *UTXOs as a proof of membership for Byzantine Agreement based Cryptocurrencies*, in "IEEE Symposium on Recent Advances on Blockchain and Its Applications", Halifax, Canada, Proceedings of the 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, IEEE, July 2018, pp. 1-8, https://hal.archives-ouvertes.fr/hal-01768190

[15] E. ANCEAUME, A. GUELLIER, R. LUDINARD, B. SERICOLA. *Sycomore : a Permissionless Distributed Ledger that self-adapts to Transactions Demand*, in "NCA 2018 - 17th IEEE International Symposium on Network Computing and Applications", Boston, United States, IEEE, November 2018, pp. 1-8 [*DOI :* 10.1109/NCA.2018.8548053], https://hal.archives-ouvertes.fr/hal-01888265

[16] S. BUKASA, L. CLAUDEPIERRE, R. LASHERMES, J.-L. LANET. *When fault injection collides with hardware complexity*, in "FPS 2018 - 11th International Symposium on Foundations & Practice of Security", Montréal, Canada, November 2018, pp. 1-16, https://hal.inria.fr/hal-01950931

[17] S. K. BUKASA, R. LASHERMES, J.-L. LANET, A. LEGAY. *Let's shock our IoT's heart: ARMv7-M under (fault) attacks*, in "ARES 2018 - 13th International Conference on Availability, Reliability and Security",

Hambourg, Germany, ACM Press, August 2018, pp. 1-6 [*DOI :* 10.1145/3230833.3230842], https://hal.inria.fr/hal-01950842

[18] D. CRÉMILLEUX, C. BIDAN, F. MAJORCZYK, N. PRIGENT. *Enhancing Collaboration between Security Analysts in Security Operations Centers*, in "CRISIS 2018 - 13th International Conference on Risks and Security of Internet and Systems", Arcachon, France, A. ZEMMARI, M. MOSBAH, N. CUPPENS-BOULAHIA, F. CUPPENS (editors), Proceedings of the 13th International Conference on Risks and Security of Internet and Systems, Springer, October 2018, pp. 1-6, https://hal.inria.fr/hal-01992346

[19] F. GRANDHOMME, G. GUETTE, A. KSENTINI, T. PLESSE. *Alternatives to Binary Routing Policies Applied to a Military MANET Coalition*, in "IWCMC 2018 - 14th International Wireless Communications & Mobile Computing Conference", Limassol, Cyprus, Proceedings of the 14th International Wireless Communications & Mobile Computing Conference, IEEE, June 2018, pp. 1-6 [*DOI :* 10.1109/IWCMC.2018.8450393], https://hal.archives-ouvertes.fr/hal-01851409

[20] O. KOUCHAM, S. MOCANU, G. HIET, J.-M. THIRIET, F. MAJORCZYK. *Efficient Mining of Temporal Safety Properties for Intrusion Detection in Industrial Control Systems*, in "SAFEPROCESS 2018 - 10th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes", Warsaw, Poland, August 2018, pp. 1-8, https://hal.archives-ouvertes.fr/hal-01877109

[21] J.-F. LALANDE, V. VIET TRIEM TONG, P. GRAUX, G. HIET, W. MAZURCZYK, H. CHAOUI, P. BERTHOMÉ. *Teaching Android Mobile Security*, in "50th ACM Technical Symposium on Computer Science Education", Minneapolis, United States, Proceedings of the 50th ACM Technical Symposium on Computer Science Education, March 2019, https://hal-centralesupelec.archives-ouvertes.fr/hal-01940652

[22] D. LANOE, M. HURFIN, E. TOTEL. *A Scalable and Efficient Correlation Engine to Detect Multi-step Attacks in Distributed Systems*, in "SRDS 2018 - 37th IEEE International Symposium on Reliable Distributed Systems", Salvador, Brazil, IEEE, October 2018, pp. 1-10, https://hal.inria.fr/hal-01949183

[23] H. LE BOUDER, G. THOMAS, E. BOURGET, M. GRAA, N. CUPPENS-BOULAHIA, J.-L. LANET. *Theoretical security evaluation of the Human Semantic Authentication protocol*, in "SECRYPT 2018 - 15th International Conference on Security and Cryptography", Porto, Portugal, Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, July 2018, vol. 1, pp. 332-339 [*DOI :* 10.5220/0006841704980505], https://hal-imt-atlantique.archives-ouvertes.fr/hal-01894470

[24] T. LETAN, Y. RÉGIS-GIANAS, P. CHIFFLIER, G. HIET. *Modular Verification of Programs with Effects and Effect Handlers in Coq*, in "FM 2018 - 22nd International Symposium on Formal Methods", Oxford, United Kingdom, LNCS, Springer, July 2018, vol. 10951, pp. 338-354 [*DOI :* 10.1007/978-3-319-95582-7_20], https://hal.inria.fr/hal-01799712

[25] Y. MOCQUARD, B. SERICOLA, E. ANCEAUME. *Balanced allocations and global clock in population protocols: An accurate analysis*, in "SIROCCO 2018 - 25th International Colloquium on Structural Information and Communication Complexity", Ma'ale HaHamisha, Israel, June 2018, https://hal.archives-ouvertes.fr/hal-01888301

[26] Y. MOCQUARD, B. SERICOLA, E. ANCEAUME. *Population Protocols with Convergence Detection*, in "NCA 2018 - 17th IEEE International Symposium on Network Computing and Applications (NCA)", Boston, United States, IEEE, November 2018, pp. 1-8 [*DOI :* 10.1109/NCA.2018.8548344], https://hal.archives-ouvertes.fr/hal-01849441

[27] R. MOUSSAILEB, B. BOUGET, A. PALISSE, H. LE BOUDER, N. CUPPENS-BOULAHIA, J.-L. LANET. *Ransomware's Early Mitigation Mechanisms*, in "ARES 2018 - 13th International Conference on Availability, Reliability and Security", Hambourg, Germany, Proceedings of the 13th International Conference on Availability, Reliability and Security, August 2018 [*DOI :* 10.1145/3230833.3234691], https://hal.archives-ouvertes.fr/hal-01894500

[28] L. OUAIRY, H. LE BOUDER, J.-L. LANET. *Normalization of Java source codes*, in "SECITC 2018 - 11th International Conference on Security for Information Technology and Communications", Bucarest, Romania, November 2018, pp. 1-11, https://hal.inria.fr/hal-01976747

[29] L. OUAIRY, H. LE BOUDER, J.-L. LANET. *Protection of systems against fuzzing attacks*, in "FPS 2018 - 11th International Symposium on Foundations & Practice of Security", Montréal, Canada, November 2018, pp. 1-16, https://hal.inria.fr/hal-01976753

[30] L. OUAIRY, H. LE BOUDER, J.-L. LANET. *Protection of systems against fuzzing attacks*, in "2018 - European Cyber Week", Rennes, France, November 2018, pp. 1-16, https://hal.inria.fr/hal-01950822

Conferences without Proceedings

[31] P. GRAUX, J.-F. LALANDE, V. VIET TRIEM TONG. *Etat de l'Art des Techniques d'Unpacking pour les Applications Android*, in "RESSI 2018 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information", Nancy / La Bresse, France, May 2018, pp. 1-3, https://hal-centralesupelec.archives-ouvertes.fr/hal-01794252

[32] J.-F. LALANDE, V. VIET TRIEM TONG. *Le projet CominLabs Kharon: aidons les malwares à s'exécuter*, in "RESSI 2018 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information", Nancy / La Bresse, France, May 2018, 1 p. , https://hal-centralesupelec.archives-ouvertes.fr/hal-01794223

Scientific Books (or Scientific Book chapters)

[33] S. KREMER, L. MÉ, D. RÉMY, V. ROCA. *Cybersecurity: Current challenges and Inria's research directions*, Inria white book, Inria, January 2019, n^{o} 3, 172 p. , https://hal.inria.fr/hal-01993308

Research Reports

[34] E. ANCEAUME, A. D. POZZO, R. LUDINARD, M. POTOP-BUTUCARU, S. TUCCI-PIERGIOVANNI. *Blockchain Abstract Data Type*, Sorbonne Université, CNRS, Laboratoire d'Informatique de Paris 6, LIP6, Paris, France, February 2018, pp. 1-30, https://arxiv.org/abs/1802.09877 , https://hal.sorbonne-universite.fr/hal-01718480

Scientific Popularization

[35] E. ANCEAUME, J. JONGWANE. *Le potentiel révolutionnaire de la technologie blockchain*, in "Interstices", May 2018, https://hal.inria.fr/hal-01827608

[36] E. ANCEAUME. *Les enjeux des blockchains*, June 2018, Rapport du groupe de travail sur les enjeux de la blockchain. Accessible: https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-blockchain-21-juin-2018.pdf, https://hal.archives-ouvertes.fr/hal-01923502

Other Publications

[37] E. ANCEAUME, A. D. POZZO, R. LUDINARD, M. POTOP-BUTUCARU, S. TUCCI-PIERGIOVANNI. *POSTER: Blockchain Abstract Data Type*, February 2019, pp. 1-2, PPoPP 2019 - 24th ACM SIGPLAN Annual Symposium on Principles and Practice of Parallel Programming, Poster [*DOI :* 10.1145/3293883.3303705], https://hal.archives-ouvertes.fr/hal-01988364

[38] Y. MOCQUARD, B. SERICOLA, E. ANCEAUME. *Balanced allocations and global clock in population protocols: An accurate analysis (Full version)*, May 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01790973