UMR IRISA

Activity Report 2019

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

Ludovic Mé [Inria, Advanced Research position, HDR]
Emmanuelle Anceaume [CNRS, Researcher, HDR]
Michel Hurfin [Inria, Researcher, HDR]
Jean-Louis Lanet [Inria, Researcher, HDR]

Faculty Members

Christophe Bidan [Centrale-Supélec, Professor, HDR]
Valérie Viet Triem Tong [Team leader, Centrale-Supélec, Associate Professor, HDR]
Gilles Guette [Univ de Rennes I, Associate Professor]

Guillaume Hiet [Centrale-Supélec, Associate Professor]
Jean-Francois Lalande [Centrale-Supélec, Professor, HDR]
Guillaume Piolle [Centrale-Supélec, Associate Professor]
Sam Thomas [Centrale-Supélec, Associate Professor, from Jun 2019 until Nov 2019]
Eric Totel [Centrale-Supélec, Professor, until Sep 2019, HDR]
Frédéric Tronel [Centrale-Supélec, Associate Professor]
Pierre Wilke [Centrale-Supélec, Associate Professor]

Post-Doctoral Fellows

Ludovic Claudepierre [Inria until Oct 2019,Univ de Rennes I since Nov 2019]
Jerome Fellus [Univ de Rennes I, until Jun 2019]
Mouad Lemoudden [Inria]
Frédérique Robin [Inria, from Oct 2019]

PhD Students

Nicolas Bellec [Inria, from Oct 2019]
Aimad Berady [from Nov 2018]
Sebanjila Bukasa [Inria, until Mar 2019]
Vasile Cazacu [CNRS]
Ronny Chevalier [HP France]
Tomas Javier Concepcion Miranda [Centrale-Supélec, from Oct 2019]
Alexandre Dey [Airbus]
Aurélien Dupin [Thales, until Jan 2019]
Mathieu Escouteloup [Inria]
Benoit Fournier [Univ de Rennes I]
Cyprien Gottstein [Orange Labs]
Pierre Graux [Inria]
Cedric Herzog [Inria]
David Lanoé [Inria, until Sep 2019]
Kevin Le Bon [Inria]
Laetitia Leichtnam [Ministère de la Défense, until Sep 2019]
Leopold Ouairy [Inria]
Aurelien Palisse [Inria, until Jan 2019]
Charles Arya Xosanavongsa [Thales, until Nov 2019]

Technical staff

Mohamed Alsamman [Inria, Engineer, from Sep 2019]

Interns and Apprentices

Yassir Anouar [Inria, from Apr 2019 until Sep 2019]
Nicolas Bailluet [ENS Rennes, from May 2019 until Jul 2019]
Thomas Furet [Inria, from May 2019 until Aug 2019]
Francois Jullion [Centrale-Supélec, Jun 2019]
Hugo Kermabon-Bobinnec [IMT Atlantique, from Feb 2019 until Mar 2019]
Stephane Kui [Centrale-Supélec, from Feb 2019 until Jun 2019]
Romain Laurent [Univ de Rennes I, from Jun 2019 until Jul 2019]
Yassine Lemmou [Inria, from Mar 2019 until Apr 2019]
Arnaud Van Straaten [Inria, from May 2019 until Aug 2019]
Nadim Zemmouri [Centrale-Supélec, from May 2019 until Jul 2019]

Administrative Assistants

Lydie Mabil [Inria]
Alexandre Dang [Centrale-Supélec, from Oct 2019]

External Collaborator

Frédéric Majorczyk [DGA]

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

An attack on a computer system begins with the exploitation of one or more vulnerabilities of that system. Generally speaking, a vulnerability can be a software bug or a misconfiguration that can be exploited by the attacker to perform unauthorized actions. Exploiting a vulnerability leads to a use of the system according to a case not foreseen in its specification, implementation or configuration. This puts the system in an inconsistent state allowing the attacker to divert the use of the system in his or her own interest.

The systems we use are large, interconnected, constantly evolving and, therefore, are likely to retain many vulnerabilities; their security depends on our ability to update them quickly when new threats are discovered. It is thus necessary to understand how the attacker has compromised the system: what vulnerabilities he has exploited, what actions he has conducted, where he is located in the system. It is essential to study statically the malicious code used by the attacker. It is also important to be able to study it dynamically to be able to replay attacks on demand.

Ideally, we should be ahead of the attacker and therefore imagine new ways to attack. In addition, we believe it is necessary to improve the feedback to the expert by allowing him to quickly understand the progress of an attack. The first step before being able to offer secure systems is to understand and measure the real capabilities of the attacker.

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

In this context, we are particularly interested in

- **highlighting attacks** on the micro-architecture 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 is generally composed of several steps. During a first approach step the attacker enters the system, locates the target and makes itself persistent. Then, in a second step, the payload of the attack is effectively launched, leading to a violation of the security policy (attacks against confidentiality, integrity, or availability of OS, applications, services, or data).

The objective of intrusion detection is to be able to detect the attacker, ideally during the first step of the attack. To do this, intrusion detection systems (IDS) are based on probes that continuously monitor the system. These probes report events to a core engine that decide whether or not to alert the expert.

Intrusion detection systems are important for all systems handling sensitive data that may be accessible to a malicious agent. They are especially crucial for low-level systems that provide essential support services to other systems. They are essential in inter-connected systems that are designed to last a long time and are difficult to update.

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:

- deceptive security
- malicious behavior tolerance

In the notion of *deceptive security* we group together all the approaches that aim to mislead the active attacker in a system in order to deceive him on the exact nature of his target. These approaches can slow down the attacker or lead him to abandon his attack.

Finally, we contribute to the design of architectures or services relying on the collaboration of entities that is not affected by the minority presence of malicious entities. These architectures or services are based on the collaboration of a set of nodes that are not affected by the presence in minority of malicious nodes.

4. Highlights of the Year

4.1. Highlights of the Year

This year we highlight two key events in the team's life:

- We have organized the SILM semester on the Security of Software/Hardware Interfaces. The goal of this semester is to promote the scientific, teaching and industrial transfer activities on the security of software/hardware interfaces. This semester is supported by DGA.
- We have concluded the transfer of a license to use GroddDroid our Android malware analysis framework.

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. 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.

- Authors: Mourad Leslous, Adrien Abraham, Pierre Graux, Jean François Lalande, Valérie Viet Triem Tong and Pierre Wilke
- 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

5.3. 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

5.4. GroddViewer

KEYWORDS: Android - Detection - Malware

FUNCTIONAL DESCRIPTION: To visualise data from GroddDroid

- Authors: Jean-François Lalande, Valérie Viet Triem Tong, Sébastien Campion, Mathieu Simon and Pierre Wilke
- Contact: Valérie Viet Triem Tong

5.5. Survivor

KEYWORDS: Intrusion Response - Intrusion Recovery - Survivability - Resiliency - Linux - Checkpoint/Restore - Threat Mitigation

FUNCTIONAL DESCRIPTION: Survivor is a set of low-level components to design a Linux-based operating system able to withstand ongoing intrusions and to allow business continuity despite the presence of an active adversary. Survivor provides an Intrusion Response System (IRS) with the low-level components and interfaces needed to orchestrate a per-service checkpoint, recovery, and mitigation actions. It recovers infected services (i.e., their processes and their associated files) to a previous safe state and it protects their state by applying a set of mitigations (e.g., privilege restrictions and resource quotas) aimed at withstanding further reinfections.

- Participants: Ronny Chevalier, Guillaume Hiet, David Plaquin and Chris Dalton
- Partners: CentraleSupélec - HP Labs
- Contact: Ronny Chevalier

5.6. PyMaO

Python Malware Orchestrator

KEYWORDS: Android - Malware

FUNCTIONAL DESCRIPTION: PyMaO chains several analyses that are part of an experiment. An analysis is most of the time, a call to an external tool that returns a result, for example apktool, grep, Androguard, Apkid. An experiment is a collection of analyses that are run one by one, chained, if some conditions hold. For example, if the unpacking of an application with Apktool succeeds, then you can grep the code for searching a string.

PyMaO has a nice old-fashion graphical interface (ncurses).

RELEASE FUNCTIONAL DESCRIPTION: Initial release corresponding to the demo presented at MASCOTS 2019.

NEWS OF THE YEAR: A demo has been presented at the MASCOTS 2019 conference: https://hal-centralesupelec.archives-ouvertes.fr/hal-02305473

- Authors: Jean-François Lalande, Pierre Graux and Tomas Javier Concepcion Miranda
- Contact: Jean-François Lalande
- URL: https://gitlab.inria.fr/cidre-public/pymao

5.7. OATs'inside

KEYWORDS: Android - Malware - Reverse engineering - Code analysis

FUNCTIONAL DESCRIPTION: OATs'inside is a Android reverse engineering tool that handles all native obfuscation techniques. This tool uses a hybrid approach based on dynamic monitoring and trace-based symbolic execution to output control flow graphs (CFGs) for each method of the analyzed application. These CFGs spare users the need to dive into low-level instructions, which are difficult to reverse engineer.

- Participants: Pierre Graux, Jean-François Lalande, Valérie Viet Triem Tong and Pierre Wilke
- Contact: Pierre Graux

6. New Results

6.1. Axis 1 : Attack comprehension

6.1.1. Fault injection

Electromagnetic injection is a non-invasive way to attack a chip. The large number of parameters that require to be properly tuned for such an attack limits its efficiency. In [30] we propose several ways to improve the success rate of fault injection by electromagnetic radiation. We show that software execution is altered at targeted instructions if the radiating probe is located above the phase-locked loop device driving the clock tree. We identify the phase-locked loop as a sensitive part of the chip. We reduce the preferential location for the electromagnetic injection to a small area in the vicinity of the analog power supply feeding the phase-locked loop. We also explore the influence of the frequency of the injected electromagnetic wave. We compute the optimal fault rate in a bandwidth of $15MHz$, in the upper limit of the chip bandwidth. Our experiments show that for an optimal frequency a precision of $5ns$, we succeed to reach the best fault rate. With this electromagnetic injection technique, the achieved success rate reaches 15 to 20%. Such a fault can be used to retrieve the key of a cryptographic algorithm (for an Advanced Encryption Standard application for example).

6.1.2. Malware analysis

About Android malware analysis, we have started investigations with specific malware that hide their behavior using obfuscation techniques [10]. As these malware are difficult to find in the wild, we have also started to analyze both datasets of the literature and large collection of applications captured from different repositories such as the Play Store. This huge amount of applications to analyze (currently more than 100,000) makes difficult to build reliable experiments [20]. We have designed a new tool, called PyMaO, that helps to orchestrate experiments. This tool is published as an open source tool under GPL v3. We have also revisited the historical datasets of malware of the literature and introduce a more up-to-date malware and goodware dataset [26].

6.1.3. Focus on doxware

A doxware is a particular type of ransomware that threatens to release personal or sensitive data to the public if the user does not pay the ransom. The term comes from the hacker term "doxing," or releasing confidential information over the internet. The only difference between a classical ransomware and a doxware resides in a *valuable files hunting* followed by an exfiltration of these data. In [34], we have explored how an attacker may be able to quickly localized valuable assets of a machine using an analysis of the content and the vocabulary of its files.

6.1.4. Attack scenario reconstruction

In order to supervise the security of a large infrastructure, the administrator deploys multiple sensors and intrusion detection systems on several critical places in the system. It is easier to explain and detect attacks if more events are logged. Starting from a suspicious event (appearing as a log entry), the administrator can start his investigation by manually building the set of previous events that are linked to this event of interest. Accordingly, the administrator attempts to identify links among the logged events in order to retrieve those that correspond to the traces of the attacker's actions in the supervised system; previous work is aimed at building these connections. In practice, however, this type of link is not trivial to define and discover. Hence, there is a real necessity to describe and define formally the semantics of these links in literature. In In order to supervise the security of a large infrastructure, the administrator deploys multiple sensors and intrusion detection systems on several critical places in the system. It is easier to explain and detect attacks if more events are logged. Starting from a suspicious event (appearing as a log entry), the administrator can start his investigation by manually building the set of previous events that are linked to this event of interest. Accordingly, the administrator attempts to identify links among the logged events in order to retrieve those that correspond to the traces of the attacker's actions in the supervised system; previous work is aimed at building these connections. In practice, however, this type of link is not trivial to define and discover. Hence, there is a real necessity to describe and define formally the semantics of these links in literature. In this paper, a clear definition of this relationship, called contextual event causal dependency, is introduced and proposed. The work presented in this paper aims at defining a formal model that would ideally unify previous work on causal dependencies among heterogeneous events. We define a relationship among events that enables the discovery of all events, which can be considered as the cause (in the past) or the effect (in the future) of an event of interest (e.g., an indicator of compromise, produced by an attacker action). In [36], we have proposed a clear definition of this relationship, called contextual event causal dependency. The work presented in [36] aims at defining a formal model that would ideally unify previous work on causal dependencies among heterogeneous events. We define a relationship among events that enables the discovery of all events, which can be considered as the cause (in the past) or the effect (in the future) of an event of interest (e.g., an indicator of compromise, produced by an attacker action).

6.2. Axis 2 : Attack detection

6.2.1. Vulnerabilities detection in Java

In a prior work, we have focused on adapting a machine-learning tool (ChuckyJava) aiming at automatically detect vulnerabilities in Java. ChuckyJava is able to detect vulnerabilities by performing in two steps: the neighborhood discovery and the anomaly detection. The neighborhood discovery is the ability for the tool to detect method of similar semantics: neighbors. In [25], we mitigate many ChuckyJava's limitations by developing JavaNeighbors that improves the neighborhood discovery. JavaNeighbors represents methods by terms and using a method based on a Natural Language Processing technique, JavaNeighbors computes the distance between all representations of methods. Finally, according to the distance, each method has a neighbor list from the closest to the most distant ones. JavaNeighbors has enabled ChuckyJava to detect vulnerabilities with more accuracy.

6.2.2. Ransomware detection

A ransomware attacks mostly begins with social engineering methods to install payloads on victims' computers, followed by a communication with command and control servers for data exchange. To enable an early detection and thus scale down these attacks, we propose in [35] a detection model based on the collected system and network logs from a computer. The analysis is performed on various ransomware families with a high detection rate. Packet level detection is performed to grant the best use case scenario. This work intends to provide an independent third-party procedure that is able to distinguish between a benign software and a malicious ransomware based on network activity. Furthermore, it is not limited to only identify ransomware but could be utilized to inspect different malware.

6.2.3. Intrusion detection using logs of distributed application

Although security issues are now addressed during the development process of distributed applications, an attack may still affect the provided services or allow access to confidential data. To detect intrusions [22], we consider an anomaly detection mechanism which relies on a model of the monitored application's normal behavior. During a model construction phase, the application is run multiple times to observe some of its correct behaviors. Each gathered trace enables the identification of significant events and their causality relationships, without requiring the existence of a global clock. The constructed model is dual: an automaton plus a list of likely invariants. The redundancy between the two sub-models decreases when generalization techniques are applied on the automaton. Solutions already proposed suffer from scalability issues. In particular, the time needed to build the model is important and its size impacts the duration of the detection phase. The proposed solutions address these problems, while keeping a good accuracy during the detection phase, in terms of false positive and false negative rates. To evaluate them, a real distributed application and several attacks against the service have been considered. One of our goal is to identify redundancies and complementarities between the proposed models.

6.3. Axis 3 : Attack resistance

6.3.1. Attacker Life cycle

We have been witnessing for years the awareness of the existence of a so-called Advanced Persistent Threat (APT). These attacks, regularly target or involving nation-states and large companies, were first defined in 2011. Ad Advanced Persistent Threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. In [13], we have proposed a model providing an operational reading of the attackers' lifecycle in a compromised network. This model allows to express possible regressions in the attack and introduces the concept of a waiting state, which is essential for long-term actions. In this article we have also proposed a confrontation between our model and two recent examples of attacks whose progression has been publicly described: the Equifax breach (2017) and the TV5Monde sabotage (2015).

6.3.2. OS-level intrusion survivability

Despite the deployment of preventive security mechanisms to protect the assets and computing platforms of users, intrusions eventually occur. In [17], we have proposed a novel intrusion survivability approach to withstand ongoing intrusions. Our approach relies on an orchestration of fine-grained recovery and per-service responses (e.g., privileges removal). Such an approach may put the system into a degraded mode. This degraded mode prevents attackers to reinfect the system or to achieve their goals if they managed to reinfect it. It maintains the availability of core functions while waiting for patches to be deployed. We devised a cost-sensitive response selection process to ensure that while the service is in a degraded mode, its core functions are still operating. We built a Linux-based prototype and evaluated the effectiveness of our approach against different types of intrusions. The results show that our solution removes the effects of the intrusions, that it can select appropriate responses, and that it allows services to survive when reinfected. In terms of performance overhead, in most cases, we observed a small overhead, except in the rare case of services that write many small files asynchronously in a burst, where we observed a higher but acceptable overhead.

6.3.3. Secure routing in drones swarms

Unmanned aerial vehicle (UAV) applications and development have increased over the past few years as this technology has become more accessible and less expensive. On a single UAV scenario, communication is a keystone to transmit commands and retrieve data from UAV sensors. It is even more critical in swarm where cooperation and inter messaging is fundamental. The communication between the nodes of a swarm is based on a suitable routing algorithm. The routing must allow each node to send messages to each other, by successive hops between different neighbors. A UAV swarm is a particular mobile ad-hoc networks where nodes run independently but form a cooperative communication network. UAV swarm shares com- mon characteristics with VANET (vehicular ad hoc network), sensors network or mobile phone network but also strongly differs on specific points (mobility model, instability, limited infrastructure access). Any computation on a UAV is a permanent trade off between volume, weight and power consumption, with no infrastructure access. In [31], we have proposed a secured routing protocol designed for UAV swarm networks. SEER4US is the first protocol providing integrity of routing messages and authentication of their sender with low energy consumption for battery preservation.

6.3.4. Securing the control flow of smartcard C programs

Results obtained several years ago about securing the control flow of C programs have been extended and published in the journal Computers and Security [7]. This extended version of our work focuses on the formal verification of the introduced countermeasures. We prove that any possible attack that would skip more than one C instruction is detected by our countermeasures. We also extended the experimental results on a benchmark software dedicated to smartcards. This work has been achieved in cooperation with Karine Heydemann from the LIP6 laboratory (Sorbonne Université).

6.3.5. A secure implementation of the replicated state machine

State machine replication (RSM) is today the foundation of many cloud-based highly-available products: it allows some service to be deployed such to guarantee its correct functioning despite possible faults. In RSM, clients issue operation requests to a set of distributed processes implementing the replicated service, that, in turn, run a protocol to decide the order of execution of incoming operations and provide clients with outputs. Faults can be accidental (e.g. a computer crashing due to a loss of power) or have a malicious intent (e.g. a compromised server). Whichever is the chosen fault model, RSM has proven to be a reliable and effective solution for the deployment of dependable services. RSM is usually built on top of a distributed Consensus primitive that is used by processes to agree on the order of execution of requests concurrently issued by clients. The main problem with this approach is that Consensus is impossible to achieve deterministically in a distributed settings if the system is asynchronous and even just a single process may fail by crashing. This led the research community to study and develop alternative solutions based on the relaxation of some of the constraints, to allow agreement to be reached in partially synchronous systems with faulty processes by trading off consistency with availability. An alternative approach consists in imposing constraints on the set of operations that can be issued by clients, i.e. imposing updates that commute. In particular, commutative replicated data types (CRDTs) can be implemented with an RSM approach in asynchronous settings using the monotonic growth of a join semilattice, i.e., a partially ordered set that defines a join (least upper bound) for all element pairs. In [18] we have proposed an algorithm that solves Generalized Lattice Agreement in a Byzantine fault model. To the best of our knowledge this is the first solution for Byzantine lattice agreement that works on any possible lattice, and it is the first work proposing a Byzantine tolerant RSM built on it. The algorithm is wait-free, i.e., every process completes its execution of the algorithm within a bounded number of steps, regardless of the execution of other processes. We have also sketch the main lines of a signature-based version of our algorithms which take advantage of digital signatures to reduce the message complexity to $\mathcal{O}(n)$ per process, when the number f of Byzantine processes verifies $f = \mathcal{O}(1)$.

6.3.6. Blockchain in adversarial environments

We are pursuing our efforts dedicated to the theoretical aspects of blockchains. In particular, we have recently proposed to specify blockchains as a composition of abstract data types all together with a hierarchy of

consistency criteria that formally characterizes the histories admissible for distributed programs that use them. Our work is based on an original oracle-based construction that, along with new consistency definitions, captures the eventual convergence process in blockchain systems. This study allows us to focus on the implementability of the presented abstractions and a mapping of representative existing blockchains from both academia and industry in our framework. It is already known that some blockchain implementations solve eventual consistency of an append-only queue using Consensus. However the question about the consistency criterion of blockchains as Bitcoin and Ethereum that technically do not solve Consensus, and their relation with Consensus in general was not studied. We have also proposed a specification of distributed ledger register that matches the Lamport hierarchy from safe to atomic. Moreover, we propose implementations of distributed ledger registers with safe, regular and atomic guaranties in a model of communication specific to distributed ledgers technology that we also formalize. Then, we propose an implementation of a distributed ledger register that satisfies the atomic specification and the k-consistency property that characterizes the permissionless distributed blockchains such as Bitcoin and Ethereum. Preliminary results appear in [41].

In parallel to this work, we have proposed the design of a scalable permissionless blockchain in the proof-of-stake setting. In particular, we use a distributed hash table as a building block to set up randomized shards, and then leverage the sharded architecture to validate blocks in an efficient manner. We combine verifiable Byzantine agreements run by shards of stakeholders and a block validation protocol to guarantee that forks occur with negligible probability. We impose induced churn to make shards robust to eclipse attacks, and we rely on the UTXO coin model to guarantee that any stake-holder action is securely verifiable by anyone. Our protocol works against adaptive adversary, and makes no synchrony assumption beyond what is required for the byzantine agreement. This work has been published in [19].

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- **HP (2013-2019): Embedded Systems Security** One of the main activities of HP Inc. is to develop and manufacture computing platforms (such as laptops, printers, etc). These platforms consist of hardware and embedded software (usually referred to as firmware). Such embedded software is typically required for the proper functioning of the hardware and relied upon by high level operating system, application or solution software. One of the research tracks of this collaboration consists in enhancing the security level of low-level software components (firmware and OS) in future computing platforms. The final objective is to provide a more resilient and trustworthy platform to the end-user. This work is carried out in the context of the PhD of Ronny Chevalier.
- **DGA (2018-2020)** Traditionally, IDSes are evaluated based on their detection ability against a labeled dataset that contains normal and abnormal network traffic. Upon inspection, it is clear that datasets publicly available are usually obsolete in the span of a couple years in both anomaly types and background, benign Internet traffic. They also suffer from a lack of volume and diversity in traffic, and ultimately, lack of representativeness and realism. In this context, the goal of this project is to come up with an evolutive platform for IDS evaluation that solves many of the issues that exist in the state of the art methods. In order to create such an evolutive platform, there is a need for dynamic infrastructure that allows continuous and automatic change. Here are a number of design principles that we followed for our platform: reproducibility (it is possible to rebuild the infrastructure of the platform or any element of it); repeatability (any action carried out on the infrastructure tested in the platform is repeatable); live evaluation (while traditional IDS evaluation is carried out using a static benchmark dataset, we propose an environment that resembles what IDS does in real life); realism (in terms of traffic generation, real world attack representativeness, and system setup. This will surely be a continuous and evolutive effort to try to approach real world conditions as best as can be); automatization (scripts allow a complete description of the system in which an IDS is tested, and of normal/malicious activity generation inside this system).

  This work is carried out in the context of the postdoc of Mouad Lemoudden.

- **DGA (2019-2021)** DGA and its industrial partners have to regularly implement filters applied to standard or proprietary protocols on communication interfaces or directly in products. In order to allow administrators to easily adapt these filters to the specific context of the various devices, filtering languages specific to the different filtering policies applicable to the different devices should be developed. Even for simple static filters, the definition of such languages is a complex task. A methodological approach that would simplify this task for higher level abstraction filtering languages (and therefore simpler to use) would be to allow the definition of higher level abstraction filtering languages by relying on a single language of lower level of abstraction. This would make it possible to define high-level abstraction and easy-to-use languages in a recursive way by progressively increasing the levels of abstraction (and specificity). In addition, this approach would improve reusability. Indeed, it would be possible to rely on a filtering language, previously developed for another project, in order to more easily develop a more specific (and easy to use) language for another project.

  This work is carried out in the context of the postdoc of Ludovic Claudepierre

7.2. Bilateral Grants with Industry

- **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.
- **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

- **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

- **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. Research Stays Abroad

Emmanuelle Anceaume has been invited by the University of La Sapienza (Italy) from the 1st to the 30th of September 2019. During this stay, she collaborated with Profs Leonardo Querzony and Giuseppe A. Di Luna. Their collaboration gave rise to an implementation of the Replicated State Machine, which is resilient to Byzantine behaviors in asynchronous environments [18] (will appear at IPDPS in 2020).

8.4. European Initiatives

8.4.1. H2020 Projects

- **SPARTA (2019-2022) - https://www.sparta.eu/**

  SPARTA is a Cybersecurity Competence Network supported by the EU's H2020 program (Grant agreement ID: 830892) and led by CEA. This 3 years project started in February 2019. It aims to coordinate and develop the implementation of high-level research and innovation in digital security, in order to strengthen the strategic autonomy of the European Union.The CIDRE team is involved both in the workpackage 2 (SPARTA Roadmap) that aims to develop an ambitious Cybersecurity Research and Innovation Roadmap and the workpackage 6 (SPARTA Program HAII-T) that will develop a foundation for secure-by-design Intelligent infrastructures. More precisely, in the context of a task dedicated to resilience-by-design, we design an intrusion detection mechanism that combines both signature-based and anomaly-based approaches.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events: Organisation

9.1.1.1. General Chair, Scientific Chair

- Ludovic Mé served as general chair of the conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information), May 2019, Erquy, France.
- Guillaume Hiet is the chair holder of the SILM thematic semester. He served as general chair of the SILM workshop, November 2019, Rennes, France.

The SILM thematic semester [1] is dedicated to the security of software/hardware interfaces and focus more particularly on the three following axes:

1. Analyzing the behavior and the state of hardware components using, e.g. trace mechanisms, fuzzing, reverse-engineering techniques, or side channel analyses;
2. Studying the hardware vulnerabilities and the software attacks that can exploit them: e.g. side-channels, fault injections, or exploitation of unspecified behavior;
3. Detecting and preventing software attacks using dedicated hardware components. Proposing software countermeasures to protect from hardware vulnerabilities.

The goal of this semester is to promote the scientific, teaching and industrial transfer activities on the security of software/hardware interfaces. Our objective is also to identify scientific and technological challenges in that field and to propose a strategic action plan. To that end, we organized different events:

- The SILM summer school (in collaboration with the GDR "Sécurité Informatique") [2], in July 2019, Rennes, France.
- The SILM workshop [3], in Novembre 2019, Rennes, France
- A regular seminar [4] at Inria, Rennes, France.

We will also animate a working group and publish a white-paper on that topic.

9.1.1.2. Member of the Organizing Committees

Christophe Bidan served as a member of the organization committee of C&ESAR 2019 (26rd Computers & Electronics Security Applications Rendez-vous), November 2019, Rennes, France.

Eric Totel served as a member of the organization committee of the conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information), May 2019, Erquy, France.

Gilles Guette served as a member of the organization committee of the conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information), May 2019, Erquy, France.

Frédéric Tronel served as a member of the organization committee of SSTIC 2019 (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.

Frédéric served as a member of the organisation committee of SILM Summer School and SILM workshop.

9.1.2. Scientific Events: Selection

9.1.2.1. Chair of Conference Program Committees

Jean-François Lalande was the program co-chair of HPCS 2019 (The 2019 International Conference on High Performance Computing & Simulation), July 2019, Dublin, Ireland, IEEE Computer Society.

Jean-François Lalande was the program co-chair of CECC 2019 (Central European Cybersecurity Conference), November 2019, Munich, Germany, ACM Press.

[1] https://silm.inria.fr/
[2] https://silm-school.inria.fr/
[3] https://silm-workshop.inria.fr/
[4] https://semestres-cyber.inria.fr/en/silm-seminar/

Jean-François Lalande was the program co-chair of IWSMR 2019 workshop (1st International Workshop on Information Security Methodology and Replication Studies), August 2019, Dublin, Ireland, ACM Press.

9.1.2.2. Member of the Conference Program Committees

Ludovic Mé served the Scientific Committee of the FIC 2020.

Frédéric Tronel and Valérie Viet Triem Tong served as a member of the program committee of SSTIC 2019 (Symposium sur la sécurité des technologies de l'information et des communications) June 2019, Rennes, France.

Jean-François Lalande served as a member of the program committee of the international conferences CECC 2019, SecITC 2019, and of international workshops IWCC 2019, CUING 2019, SHPCS 2019, WTMC 2019.

Gilles Guette served as a member of the program committee of the international conferences ICISSP 2019, ISNCC 2019, ITSC 2019.

Guillaume Piolle served as a member of the program committee of the APVP 2019 workshop.

Emmanuelle Anceaume served as a member of the program committee of NCA 2019, EDCC 2019, ICDCS 2019, DEBS 2019, TrustCom 2019, BSCT 2019 and Tokenomics 2019.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

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

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

9.1.3.2. Reviewer - Reviewing Activities

Michel Hurfin served as a reviewer for the International Journal of Control , the Journal on Discrete Event Dynamic Systems - Theory and Applications, and IEEE Transactions on Dependable and Secure Computing.

Jean-François Lalande served as a reviewer for the following international journals: Journal of Cyber Security and Mobility, IEEE Transactions on Reliability, Journal Elsevier FGCS, IEEE Transactions on Industrial Informatics, MDPI Applied Sciences, Journal of Universal Computer Science.

Eric Totel served as a reviewer for the European Congress of Embedded Real Time Software and Systems.

Pierre Wilke served as a reviewer for the 12th International Conference on Security for Information Technology and Communications (SecITC 2019).

Guillaume Hiet served as a reviewer for the Journal of Computer Security and IEEE Design & Test

9.1.4. Invited Talks

Ludovic Mé. *Cyber security: current challenges*. LIRIMA Franco-African webinar. Sept. 2019.

Jean-François Lalande: *Obfuscated Android Application Development*, CECC 2019, Munich.

Emmanuelle Anceaume: *Abstractions for permissionless distributed systems*, SSL seminar, Nancy, 5 December 2019.

Emmanuelle Anceaume: *Can we safely adapt the construction of permissionless blockchains to user demand ?*, *Journées Futur & Rupture*, ParisTech, 31 March 2019.

Emmanuelle Anceaume: *Beyond the block: a lego blockumentary*, SecDays, 9-10 January 2019.

Emmanuelle Anceaume: *Round table at the "Future & Rupture day"* with Mr Ronan Le Gleut (Sénateur), Mr. Gérard Memmi (Télécom ParisTech), Mr. Nicolas KozaKiewicz (Atos Worldline) - moderator Patrick Duvaut, February, 28 2019.

9.1.5. Scientific Expertise

- Ludovic Mé served the HCERES evaluation committee of the LAAS-CNRS research lab.
- Ludovic Mé has served the Scientific Council of the LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées).
- Valérie Viet Triem Tong has participated in the scientific evaluation comity *Global Security and Cybersecurity* (CES 39) of the French Research Agency (ANR).
- Jean-François Lalande is part of the advisory board of the starting european project "SIMARGL" (H2020 project): Secure Intelligent Methods for Advanced Recognition of Malware and Stegomalware.

9.1.6. Research Administration

- Christophe Bidan was a member of a recruitment committee for an assistant professor position at CentraleSupélec, Rennes.
- Ludovic Mé is deputy scientific director of Inria, in charge of the cyber security domain.
- Valérie Viet Triem Tong was a member of 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 IMT, Brest.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Team members are involved in initial and continuing education in CentraleSupélec, a french institute of research and higher education in engineering and science and ESIR (Ecole Supérieure d'Ingénieur de Rennes) the graduate engineering school of the University of Rennes 1.

In these institutions,

- Gilles Guette is director of corporate relations at ESIR;
- Jean-François Lalande is responsible of the major program dedicated to information systems security and the special track Infosec of CentraleSupélec ;
- Frédéric Tronel and Valérie Viet Triem Tong share the responsability of the *mastère spécialisé* (post-graduate specialization degree) in Cybersecurity. This education was awarded **best French master degree** in the category "Master Cybersecurity masters and Security of systems" in the Eduniversal master ranking 2019.

The teaching duties are summed up in table 1.

9.2.2. Supervision

HdR defended in 2019, Emmanuelle Anceaume, *Abstractions for permissionless systems*.

PhD defended in 2019: Aurélien Dupin, *Secure multi-partie computations*, started February 2016, supervised by Christophe Bidan(40%), David Pointcheval (30% - ENS) and Renaud Dubois (30% - Thales).

PhD defended in 2019: Aurélien Palisse, *Analyse et détection de logiciels de rançon*, started in 2015, supervised by Jean-Louis Lanet, Colas Le Guernic (DGA) and Hélène Le Bouder (IMT Atlantique);

PhD defended in 2019: 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 defended in 2019: Pernelle Mensah, *Generation and Dynamic Update of Attack Graphs in Cloud Providers Infrastructures*, started in January 2016, supervised by Eric Totel (25%), Guillaume Piolle (25%), Christine Morin (25% - Myriads Inria project), and Samuel Dubus (25% - Nokia);

	Licence level	Master level	CS†	Univ. Rennes 1	Initial education	Continuing education	2018 -2019
Emmanuelle Anceaume		✓		✓	✓		10
Christophe Bidan	✓	✓	✓		✓	✓	64
Gilles Guette	✓	✓	✓	✓	✓		400
Guillaume Hiet	✓	✓	✓	✓	✓	✓	328 +34*
Jean-François Lalande	✓	✓	✓		✓	✓	326 +70*
Guillaume Piolle	✓	✓	✓	✓	✓	✓	210
Frédéric Tronel	✓	✓	✓	✓	✓	✓	287
Valérie Viet Triem Tong	✓	✓	✓	✓	✓	✓	229
Pierre Wilke	✓	✓	✓		✓	✓	140

Figure 1.

PhD defended in 2019: Kevin Bukasa, *Vulnerability analysis of embedded systems against physical attacks* , supervised by Jean-Louis Lanet and Ronan Lashermes (SED Inria);

PhD defended in 2019: Ronny Chevalier, *Detecting and Surviving Intrusions - Exploring New Host-Based Intrusion Detection, Recovery, and Response Approaches*, supervised by Guillaume Hiet (50%), David Plaquin (25% - HP) and Ludovic Mé (25%);

PhD in progress: Alexandre Dey, *Continuous Model Learning for Anomaly Detection In the Presence of Highly Adaptative Cyberattacks*, started in November 2019, supervised by Eric Totel (50%) and Ludovic Mé (50%);

PhD in progress: 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: 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: 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: 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: 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%);

PhD in progress: Tomas Conception Miranda, *Profiling and Visualization Android malware*, started in October 2019, supervised by Jean-François Lalande (34%), Valérie Viet Triem Tong (33%), Pierre Wilke (33%).

9.2.2.1. Supervision of external PhD candidates

PhD in progress: Nicolas Bellec, *Security enhancement in embedded hard real-time systems*, started in October 2019, supervised by Isabelle Puaut (50%), Guillaume Hiet (25%), Frédéric Tronel (25%)

PhD in progress: Kevin Le Bon, *Security enhancement in embedded hard real-time systems*, started in October 2018, supervised by Erven Rohu (30%), Guillaume Hiet (35%), Frédéric Tronel (35%)

9.2.3. Juries

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

Amina Saadaoui, *Formal Techniques for Automatic Detection and Resolution of Security Equipment Misconfigurations*, supervised by Adel Bouhoula and Sihem Guemara, University of Carthage, April 2019.

Amir Wonjiga, *User-Centric Security Monitoring in Cloud Environments*, supervised by Christine Morin and Louis Rilling, University of Rennes 1, May 2019.

Ludovic Mé was a member of the committee for the following HDR defense:

Stephane Mocanu, *Cyberdéfense des infrastructures critiques*, University Grenoble Alpes community, January 2019.

Nizar Kheir, *From Cyber-secure to Cyber-resilient Computer Systems: The way forward*, University of Paris-Saclay, May 2019.

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

Xin Ye Model, *Checking Self Modifying Code*, supervised by Tayssir Touili et Jifeng He, University of Paris, Septembre 2019.

Alexandre Dang, *Compilation Sécurisée pour la Protection de la Mémoire*, supervised by Frédéric Besson and Thomas Jensen, University of Rennes 1, December 2019.

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

M. Guillaume Averlant, *Contrôle d'accès dynamique et architecture de sécurité pour la protection des applications sous Android*, Université Fédérale Toulouse Midi- Pyrénées, october 2th 2019.

9.3. Popularization

9.3.1. Articles and contents

- In books/journals for the general public

  Dis, c'est quoi là haut dans le ciel ? C'est un Linux, mon petit ![39], Viet Triem Tong Valérie, Fournier Benoît, Fournier Guillaume, Ouairy Leopold, Cotret Pascal, Guette Gilles, MISC numéro 104, juillet 2019.

- Online publications

  La cybersécurité aux multiples facettes. Steve Kremer, Ludovic Mé, Didier Rémy et Vincent Roca. Blog binaire (https://www.lemonde.fr/blog/binaire/), 4 juillet 2019.

- White Papers - white Papers for Popularization

  Ludovic Mé co-authored (with S. Kremer, D. Rémy and V. Roca) Inria's White Book on Cybersecurity [37].

9.3.2. Interventions

- Valérie Viet Triem Tong has participated to the *Vive la Recherche* event to promote research activities to engineering students at CentraleSupelec
- Valérie Viet Triem Tong has been involved in an artistic performances involving actors and researcher at the Digital Tech Conference, December Rennes, France.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] S. K. BUKASA. *Vulnerability analysis of embedded systems against physical attacks*, Université Rennes 1, July 2019, https://tel.archives-ouvertes.fr/tel-02418822

[2] R. CHEVALIER. *Detecting and Surviving Intrusions: Exploring New Host-Based Intrusion Detection, Recovery, and Response Approaches*, CentraleSupélec, December 2019, https://hal.inria.fr/tel-02417644

[3] P. MENSAH. *Generation and Dynamic Update of Attack Graphs in Cloud Providers Infrastructures*, CentraleSupélec, June 2019, https://hal.inria.fr/tel-02416305

[4] A. PALISSE. *Analysis and detection of ransomware*, Université de Rennes 1 ; Inria, March 2019, https://hal.archives-ouvertes.fr/tel-02415976

Articles in International Peer-Reviewed Journals

[5] F. BESSON, S. BLAZY, P. WILKE. *CompCertS: A Memory-Aware Verified C Compiler using a Pointer as Integer Semantics*, in "Journal of Automated Reasoning", August 2019, vol. 63, n^{o} 2, pp. 369-392 [*DOI :* 10.1007/s10817-018-9496-y], https://hal.inria.fr/hal-02401182

[6] S. HAMADOUCHE, M. MEZGHICHE, J.-L. LANET. *Hiding a fault enabled virus through code construction*, in "Journal of Computer Virology and Hacking Techniques", 2019, pp. 1-22 [*DOI :* 10.1007/s11416-019-00340-z], https://hal.inria.fr/hal-02416015

[7] K. HEYDEMANN, J.-F. LALANDE, P. BERTHOMÉ. *Formally verified software countermeasures for control-flow integrity of smart card C code*, in "Computers and Security", August 2019, vol. 85, pp. 202-224 [*DOI :* 10.1016/J.COSE.2019.05.004], https://hal.sorbonne-universite.fr/hal-02123836

[8] C. KIRCHNER, L. MÉ. *Défis de la recherche scientifique en cyber-sécurité*, in "Annales des Mines - Enjeux Numériques", December 2019, pp. 1-15, https://hal.inria.fr/hal-02381411

[9] Y. MOCQUARD, B. SERICOLA, E. ANCEAUME. *Probabilistic Analysis of Rumor Spreading Time*, in "INFORMS Journal on Computing", July 2019, pp. 1-20 [*DOI :* 10.1287/IJOC.2018.0845], https://hal.archives-ouvertes.fr/hal-01888300

Invited Conferences

[10] P. GRAUX, J.-F. LALANDE, V. VIET TRIEM TONG. *Obfuscated Android Application Development*, in "CECC 2019 - Central European Cybersecurity Conference", Munich, Germany, ACM Press, November 2019, pp. 1-6 [*DOI :* 10.1145/3360664.3361144], https://hal-centralesupelec.archives-ouvertes.fr/hal-02305924

[11] J.-L. LANET. *Ransomware can always be detected but at which cost ?*, in "JATNA'04", Oujda, Morocco, November 2019, https://hal.inria.fr/hal-02416070

International Conferences with Proceedings

[12] E. ANCEAUME, A. D. POZZO, R. LUDINARD, M. POTOP-BUTUCARU, S. TUCCI-PIERGIOVANNI. *Blockchain Abstract Data Type*, in "SPAA 2019 - 31st ACM Symposium on Parallelism in Algorithms and Architectures", Phoenix, United States, ACM, June 2019, pp. 1-11 [*DOI :* 10.1145/3323165.3323183], https://hal-cnrs.archives-ouvertes.fr/hal-02380364

[13] A. BERADY, V. VIET TRIEM TONG, G. GUETTE, C. BIDAN, G. CARAT. *Modeling the Operational Phases of APT Campaigns*, in "CSCI 2019 - 6th Annual Conf. on Computational Science & Computational Intelligence", Las Vegas, United States, December 2019, pp. 1-6, https://hal.inria.fr/hal-02379869

[14] F. BESSON, S. BLAZY, A. DANG, T. JENSEN, P. WILKE. *Compiling Sandboxes: Formally Verified Software Fault Isolation*, in "ESOP 2019 - 28th European Symposium on Programming", Prague, Czech Republic, LNCS, Springer, April 2019, vol. 11423, pp. 499-524 [*DOI :* 10.1007/978-3-030-17184-1_18], https://hal.inria.fr/hal-02316189

[15] E. BOESPFLUG, R. GOURIER, J.-L. LANET. *Predicting the Effect of Hardware Fault Injection*, in "IWBIS 2019 - 4th IEEE International Workshop on Big Data and Information Security", Bali, Indonesia, IEEE, October 2019, pp. 103-108 [*DOI :* 10.1109/IWBIS.2019.8935864], https://hal.inria.fr/hal-02416062

[16] R. CHEVALIER, S. CRISTALLI, C. HAUSER, Y. SHOSHITAISHVILI, R. WANG, C. KRUEGEL, G. VIGNA, D. BRUSCHI, A. LANZI. *BootKeeper: Validating Software Integrity Properties on Boot Firmware Images*, in "CODASPY 2019 - Conference on Data and Application Security and Privacy", Dallas, United States, ACM Press, March 2019, pp. 1-11, https://arxiv.org/abs/1903.12505 [*DOI :* 10.1145/3292006.3300026], https://hal.inria.fr/hal-02066420

[17] R. CHEVALIER, D. PLAQUIN, C. DALTON, G. HIET. *Survivor: A Fine-Grained Intrusion Response and Recovery Approach for Commodity Operating Systems*, in "ACSAC 2019 - 35th Annual Computer Security Applications Conference", San Juan, Puerto Rico, Proceedings of the 35th Annual Com-

puter Security Applications Conference, December 2019, vol. 2019, https://arxiv.org/abs/1912.06863 [*DOI :* 10.1145/3359789.3359792], https://hal.inria.fr/hal-02289315

[18] G. A. DI LUNA, E. ANCEAUME, L. QUERZONI. *Byzantine Generalized Lattice Agreement*, in "Proceedings of the 34th IEEE International Parallel and Distributed Processing Symposium (IPDPS 2020)", New Orleans, Louisiana, United States, IEEE, May 2020, https://hal-cnrs.archives-ouvertes.fr/hal-02380446

[19] A. DURAND, E. ANCEAUME, R. LUDINARD. *STAKECUBE: Combining Sharding and Proof-of-Stake to build Fork-free Secure Permissionless Distributed Ledgers*, in "International conference on networked systems (NETYS)", Marrakesh, Morocco, June 2019, https://hal.archives-ouvertes.fr/hal-02078072

[20] J.-F. LALANDE, P. GRAUX, T. CONCEPCIÓN MIRANDA. *Orchestrating Android Malware Experiments*, in "MASCOTS 2019 - 27th IEEE International Symposium on the Modeling, Analysis, and Simulation of Computer and Telecommunication Systems", Rennes, France, IEEE Computer societry, October 2019, pp. 1-2, https://hal-centralesupelec.archives-ouvertes.fr/hal-02305473

[21] J.-F. LALANDE, V. VIET TRIEM TONG, P. GRAUX, G. HIET, W. MAZURCZYK, H. CHAOUI, P. BERTHOMÉ. *Teaching Android Mobile Security*, in "SIGCSE '19 - 50th ACM Technical Symposium on Computer Science Education", Minneapolis, United States, Proceedings of the 50th ACM Technical Symposium on Computer Science Education, ACM Press, February 2019, pp. 232-238 [*DOI :* 10.1145/3287324.3287406], https://hal-centralesupelec.archives-ouvertes.fr/hal-01940652

[22] D. LANOE, M. HURFIN, E. TOTEL, C. MAZIERO. *An Efficient and Scalable Intrusion Detection System on Logs of Distributed Applications*, in "SEC 2019 - 34th IFIP International Conference on ICT Systems Security and Privacy Protection", Lisbonne, Portugal, Springer, June 2019, pp. 49-63 [*DOI :* 10.1007/978-3-030-22312-0_4], https://hal.inria.fr/hal-02409487

[23] T. LETAN, Y. RÉGIS-GIANAS. *FreeSpec: Specifying, Verifying and Executing Impure Computations in Coq*, in "9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP '20)", Nouvelle-Orléans, United States, January 2020 [*DOI :* 10.1145/3372885.3373812], https://hal.inria.fr/hal-02422273

[24] Y. MOCQUARD, B. SERICOLA, E. ANCEAUME. *Brief: Explicit and Tight Bounds of the Convergence Time of Average-based Population Protocols*, in "SIROCCO 2019 - 26th International Colloquium Structural Information and Communication Complexity", L'Aquila, Italy, Springer, July 2019, pp. 1-4 [*DOI :* 10.1007/978-3-030-24922-9_29], https://hal-cnrs.archives-ouvertes.fr/hal-02380422

[25] L. OUAIRY, H. LE BOUDER, J.-L. LANET. *JavaNeighbors: Improving ChuckyJava's neighborhood discovery algorithm*, in "EUSPN 2019 - 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks", Coimbre, Portugal, November 2019, pp. 1-7, https://hal.inria.fr/hal-01950822

[26] V. VIET TRIEM TONG, C. HERZOG, T. CONCEPCIÓN MIRANDA, P. GRAUX, J.-F. LALANDE, P. WILKE. *Isolating malicious code in Android malware in the wild*, in "MALCON 2019 - 14th International Conference on Malicious and Unwanted Software", Nantucket, United States, MALCON 2019, IEEE Computer society, October 2019, https://hal-centralesupelec.archives-ouvertes.fr/hal-02288116

National Conferences with Proceedings

[27] N. OURDI, A. PALISSE, J.-L. LANET. *Classification of ransomwares using Artificial Neural Networks and Bayesian Networks*, in "Third International Conference on Intelligent Computing in Data Sciences", Marrakech, Morocco, November 2019, https://hal.inria.fr/hal-02416086

Conferences without Proceedings

[28] E. ANCEAUME, Y. BUSNEL, V. CAZACU. *L'art d'extraire des éléments du top-k en temps réel sur des fenêtres glissantes réparties*, in "ALGOTEL 2019 - 21èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications", Saint Laurent de la Cabrerisse, France, June 2019, pp. 1-4, https://hal-imt-atlantique.archives-ouvertes.fr/hal-02118367

[29] E. ANCEAUME, A. GUELLIER, R. LUDINARD, B. SERICOLA. *Sycomore : un registre de transactions distribué et public au débit auto-adaptatif*, in "ALGOTEL 2019 - 21èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications", Saint Laurent de la Cabrerisse, France, June 2019, pp. 1-4, https://hal.archives-ouvertes.fr/hal-02118385

[30] L. CLAUDEPIERRE, P. BESNIER. *Microcontroller Sensitivity to Fault-Injection Induced by Near-Field Electromagnetic Interference*, in "APEMC 2019 - Asia-Pacific International Symposium on Electromagnetic Compatibility", Sapporo, Japan, June 2019, pp. 1-4, https://hal.archives-ouvertes.fr/hal-02313980

[31] B. FOURNIER, G. GUETTE, V. VIET TRIEM TONG, J.-L. LANET. *SEER4US, Secured Energy Efficient Routing for UAV Swarms*, in "WiMob 2019 - 15th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications", Barcelona, France, October 2019, pp. 1-6, https://hal.archives-ouvertes.fr/hal-02294744

[32] K. LE BON, B. HAWKINS, E. ROHOU, G. HIET, F. TRONEL. *Plateforme de protection de binaires configurable et dynamiquement adaptative*, in "RESSI 2019 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information", Erquy, France, May 2019, pp. 1-3, https://hal.inria.fr/hal-02385216

[33] Y. LEMMOU, H. LE BOUDER, J.-L. LANET. *Discriminating Unknown Software Using Distance Model*, in "ICACSIS 2019 - 11th International Conference on Advanced Computer Science and Information Systems", Bali, Indonesia, IEEE, October 2019, https://hal.archives-ouvertes.fr/hal-02352861

[34] R. MOUSSAILEB, C. BERRTI, G. DEBOISDEFFRE, N. CUPPENS, J.-L. LANET. *Watch Out! Doxware on The Way...*, in "CRiSIS 2019 - 14th International Conference on Risks and Security of Internet and Systems", Hammamet, Tunisia, October 2019, https://hal.archives-ouvertes.fr/hal-02313650

[35] R. MOUSSAILEB, N. CUPPENS, J.-L. LANET, H. LE BOUDER. *Ransomware Network Traffic Analysis for Pre-Encryption Alert*, in "FPS 2019 - 12th International Symposium on Foundations & Practice of Security", Toulouse, France, November 2019, https://hal.archives-ouvertes.fr/hal-02313656

[36] C. XOSANAVONGSA, E. TOTEL, O. BETTAN. *Discovering Correlations: A Formal Definition of Causal Dependency Among Heterogeneous Events*, in "EuroS&P 2019 - 4th IEEE European Symposium on Security and Privacy", Stockholm, Sweden, IEEE, June 2019, pp. 340-355 [*DOI :* 10.1109/EUROSP.2019.00033], https://hal-imt-atlantique.archives-ouvertes.fr/hal-02363431

Scientific Books (or Scientific Book chapters)

[37] 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

[38] Y. MOCQUARD, F. ROBIN, B. SERICOLA, E. ANCEAUME. *Average-based Population Protocols : Explicit and Tight Bounds of the Convergence Time*, Irisa, July 2019 [*DOI :* 10.1145/NNNNNNN.NNNNNNN], https://hal.archives-ouvertes.fr/hal-02178618

Scientific Popularization

[39] V. VIET TRIEM TONG, B. FOURNIER, G. FOURNIER, L. OUAIRY, P. COTRET. *Dis, c'est quoi là haut dans le ciel ? C'est un Linux, mon petit*, in "MISC - Le journal de la sécurité informatique", July 2019, https://hal.archives-ouvertes.fr/hal-02380997

Other Publications

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

[41] E. ANCEAUME, M. PAPATRIANTAFILOU, M. POTOP-BUTUCARU, P. TSIGAS. *Distributed Ledger Register: From Safe to Atomic*, July 2019, working paper or preprint, https://hal.archives-ouvertes.fr/hal-02201472