RESEARCH CENTRE

Rennes - Bretagne Atlantique

IN PARTNERSHIP WITH:

CNRS, CentraleSupélec, Université Rennes 1

2020

ACTIVITY REPORT

Project-Team CIDRE

Confidentialité, Intégrité, Disponibilité et Répartition

IN COLLABORATION WITH: Institut de recherche en informatique et systèmes aléatoires (IRISA)

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Security and Confidentiality

Contents

Project-Team CIDRE

Creation of the Project-Team: 2011 July 01

Keywords

Computer sciences and digital sciences

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
A9.2. – Machine learning

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 members, visitors, external collaborators

Research Scientists

- Emmanuelle Anceaume [CNRS, Senior Researcher, HDR]
- Michel Hurfin [Inria, Researcher, HDR]
- Jean-Louis Lanet [Inria, Researcher, until Oct 2020, HDR]
- Ludovic Mé [Inria, Advanced Research Position, HDR]

Faculty Members

- Valérie Viet Triem Tong [Team leader, CentraleSupélec, Professor, HDR]
- Christophe Bidan [CentraleSupélec, Professor, HDR]
- Alexandre Dang [CentraleSupélec, ATER, until Sep 2020]
- Pierre Francois Gimenez [CentraleSupélec, Chair, from Oct 2020]
- Gilles Guette [Univ de Rennes I, Associate Professor]
- Guillaume Hiet [CentraleSupélec, Associate Professor, Inria delegation from September 2020 to August 2021]
- Jean-Francois Lalande [CentraleSupélec, Professor, HDR]
- Guillaume Piolle [CentraleSupélec, Associate Professor]
- Salwa Souaf [CentraleSupélec, ATER, from Oct 2020]
- Frédéric Tronel [CentraleSupelec, Associate Professor]
- Pierre Wilke [CentraleSupélec, Associate Professor]

Post-Doctoral Fellows

- Ludovic Claudepierre [Univ de Rennes I]
- Mouad Lemoudden [Inria, until Mar 2020]
- Frédérique Robin [Inria, until Sep 2020]

PhD Students

- Matthieu Baty [Inria, from Oct 2020]
- Aimad Berady [Ministère des armées]
- PierreVictor Besson [CentraleSupélec, from Nov 2020]
- Romain Brisse [Inria, from Oct 2020]
- Vasile Cazacu [CNRS, until May 2020]
- Ronny Chevalier [Hewlet Packard France, CIFRE, until Mar 2020]
- Tomas Javier Concepcion Miranda [CentraleSupélec]
- Severine Delaplace [Inria, from Dec 2020]
- Aimen Djari [CEA, from Oct 2020]

- Mathieu Escouteloup [Inria]
- Benoit Fournier [Univ de Rennes I]
- Cyprien Gottstein [Orange Labs, CIFRE]
- Pierre Graux [Inria]
- Cedric Herzog [Inria]
- Leopold Ouairy [Inria, until Sep 2020]

Technical Staff

- Mohamed Alsamman [Inria, Engineer]
- David Lanoé [Inria, Engineer, from Mar 2020 until Sep 2020]
- Leopold Ouairy [Inria, Engineer, from Dec 2020]

Interns and Apprentices

- Clement Bigarnet [CentraleSupélec, from May 2020 until Jul 2020]
- Severine Delaplace [CentraleSupélec, from Mar 2020 until Sep 2020]
- Sergio Nobrega Gonçalves [Centrale-Supélec, from Oct 2020]
- Khalil Said [CentraleSupélec, from May 2020 until Jul 2020]
- Oscar Salmon-Legagneur [CentraleSupélec, from May 2020 until Jul 2020]

Administrative Assistants

- Lydie Mabil [Inria, from Nov 2020]
- Caroline Tanguy [Inria, from Feb 2020]

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

In 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.

4 Application domains

The fields of application of the Cider team are naturally the security of the systems. The algorithms and tools produced in the team are regularly transferred to the industry through our various collaborations such as Cifre, Start-up or Inria License.

5 Highlights of the year

The start-up Malizen founded by former members of CIDRE, has been officially created in January 2020. Malizen is developing ZeroKit, a tool for supervizing the security of information systems.

6 New software and platforms

6.1 New software

6.1.1 Blare

Name: Blare, an information flow monitor

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 is an information flow monitor that opérates at the OS level. Blare relies on tainting techniques to monitor information flow between files, processes, sockets and memory pages. Blare allows to identify how a (malicious) application contaminates the OS.

News of the Year: In 2020, we have worked on porting Blare to new recent versions of the Linux kernel. In particular, we started to work on kernels 4.x that are used on mobile phone in order to be able to build AndroBlare, a modified version of Android based on Android 9 or 10.

URL: `http://www.blare-ids.org`

Publications: hal-01535949, hal-01535862, hal-00268408, hal-00356441, hal-00356484, hal-00420117, hal-00875211, hal-00840338, hal-00909400, hal-00862468, hal-00736045, hal-00736034, hal-00647116, hal-00647170, hal-00736045

Contacts: Valérie Viet Triem Tong, Alexandre Sanchez, Frédéric Tronel

Partner: CentraleSupélec

6.1.2 GroddDroid

Name: 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 - automates the execution of a malware or a regular Android application

News of the Year: In 2020, we have optimized the static analysis part, based on the soot framework. We have also implemented a new strategy to trigger UI elements on an analyzed application that runs into a smartphone.

URL: http://kharon.gforge.inria.fr/grodddroid.html

Publications: hal-01311917, hal-01201743, hal-01584989, hal-01535678

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

Contacts: Valérie Viet Triem Tong, Jean-François Lalande

Partners: CentraleSupélec, Insa Centre Val-de-Loire

6.1.3 PyMaO

Name: Python Malware Orchestrator

Keywords: Android, Malware

Scientific Description: PyMaO (Python Malware Orhestrator) is a tool that helps to orchestrate experiments involving applications such as Android apps run on a smartphone or external devices. 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).

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 Contributions: Initial release corresponding to the demo presented at MASCOTS 2019.

News of the Year: PyMao has been heavily refactored for handling experiments that are not related to Android. In particular we added the support of external devices that are handled by ssh commands.

URL: https://gitlab.inria.fr/cidre-public/pymao

Publication: hal-02305473

Authors: Jean-François Lalande, Pierre Graux, Tomas Javier Concepcion Miranda, Benoit Fournier

Contact: Jean-François Lalande

6.1.4 OATs'inside

Keywords: Android, Malware, Reverse engineering, Code analysis

Functional Description: OATs'inside is an 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.

News of the Year: Initial release of the code.

Publication: hal-02877815

Authors: Pierre Graux, Jean-François Lalande, Valérie Viet Triem Tong, Pierre Wilke

Contact: Pierre Graux

6.1.5 Tata

Name: Taint Analysis for Transient Analysis

Keywords: Cybersecurity, Android

Scientific Description: TATA (Taint Analysis for Transient Analysis) is a tool that automatically detects, at compilation time, missing transient keywords directly from Android applications' source code. The analysis focuses on applications composed of Dalvik bytecode and C/C++ native code.

Functional Description: Tata searches a particular vulnerability in the source code of an Android application.

Release Contributions: First release of the prototype.

News of the Year: Initial release of the code.

URL: https://gitlab.inria.fr/cidre-public/tata/tata-release

Publication: hal-03066847

Contacts: Pierre Graux, Jean-François Lalande, Valérie Viet Triem Tong, Pierre Wilke

6.1.6 MoM

Name: Malware-O-Matic

Keywords: Malware, Cybersecurity, Ransomware

Functional Description: MoM is an automated platform for conducting dynamic malware scans running on Windows. MoM is a bare-metal, non-virtualized platform on which user activity is simulated.

Release Contributions: Refactoring allowing greater flexibility in its deployment and use. Monitoring of experiments.

URL: https://lhs-pec.inria.fr/hosting/

Publication: hal-01405636

Contacts: Valérie Viet Triem Tong, Alexandre Sanchez, Leopold Ouairy

Partner: DGA-MI

7 New results

7.1 Axis 1 : Attack comprehension

To fully understand attack means, we are interested on the one hand in giving the security expert the tools to quickly have the knowledge of the scope of an attack in progress. On the other hand, we are interested in researching new attack means.

Visualization and monitoring Visualization attacks for better understanding of a live attack or for forensic purpose is also of primary interest to the team. We got new results for visualizing Android malware [14] that is built on top of the tools developed the last couple of years.

Evaluation of the evasion techniques used by Windows malware in the wild An evasive malware is a malware carrying an environment-aware payload that aims at remaining invisible to any protection system. In [13] we evaluate the evasion techniques used by Windows malware in the wild. First, we evaluate how common AVs cope both with unknown malware and well-known evasion techniques. To this end, we develop and use Nuky, a ransomware targeting Windows, and implementing several evasion techniques. Second, we design and evaluate a countermeasure that reproduces the presence of the artifacts on computers by instrumenting the Windows API in order to force malware to evade. The purpose of this countermeasure is to limit the infection's spread and not to replace malware detection.

Attacks against Android smartphones We continued to study the possible ways of attacking an Android smartphone by building new attacks. In particular we focused on the attack surface offered by native code that may be embedded in Android applications. We discovered two new ways for obfuscating an attack [12] that would be very difficult to detect with current analysis tools that only focus on the Java bytecode of an Android application. A first attack bypasses the JNI interface between the native code and the objects stored in the heap. A second attack obfuscates the bytecode by removing it from a fully compiled (native) version of an application. This last attack would be usable for a smartphone vendor that would pre-install a compiled application on a smartphone.

How to attack NOP The fault model of the *virtual NOP* considers that with a fault injection, an instruction can be replaced by a NOP (or an instruction with no effect on the program). By considering that we can inject several faults, in [18] we prove that we can then rewrite the program in execution by letting it execute only the instructions we are interested in. This is called NOP-oriented programming and we show that this method is Turing-complete. An extension of Gem5 has been developed with the aim of being able, through simulation, to predict the fault injections to be made to carry out a NOP-oriented attack.

7.2 Axis 2 : Attack detection

Vulnerability detection In [17] we propose a novel approach to automatically detect vulnerabilities in java source codes. First, a Natural Language Processing technique is used in order to represent code's functions in Bag-of-words. This is achieved by extracting meaningful information from each function. Then, the k-Nearest-Neighbors' Machine-Learning algorithm is used to cluster similars functions. Finally, it is possible to automatically detect vulnerabilities in each cluster, by comparing tests and method calls performed by each function in the cluster.

Network Attack Detection Based on Novelty Detection on Graph Structured Data In [16], we introduce a representation of log files of various types in a unified and unique graph representation. This representation mixes and links events of different kinds to constitute a rich description of the activities to be analyzed. To detect anomalies in these graphs, we also propose an unsupervised learning approach based on an auto-encoder. Applying this approach to the CICIDS 2017 dataset, we show that although our approach is unsupervised, its detection results are as good, and even better or much better, than those obtained by many supervised approaches.

Forensic Analysis of Network Attacks In [15] we propose an approach to treat automatically network events to provide the security analyst with a new way to determine the subset of information related to a given Indice of Compromise (IoC). This approach also relies, as the one of the previous section, on the generation of graphs that are built from the logged network events. The automatic processing of these graphs thanks to the Louvain algorithm allows then to isolate communities around.

7.3 Axis 3 : Attack resistance

Intrusion Survivability for Commodity Operating Systems We propose a novel intrusion survivability approach [2] 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.

This article is an extension of our conference paper from ACSAC'19. We give more details about our cost-sensitive response selection process, the results of our experiments and we extended the discussion regarding the limitations of our work. We also give more context regarding the concepts our work is based on and a more detailed comparison with related works. This work has been done in the context of the PhD of Ronny Chevalier, in collaboration with HP Labs.

Modular verification of software/hardware security mechanisms Modern computing systems have grown in complexity, and 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. Inconsistencies between components' assumptions on the rest of the system can have significant repercussions on this system, and may ultimately lead to safety or security issues. In [4], we introduce FreeSpec, a formalism built upon the key idea that components can be modeled as programs with algebraic effects to be realized by other components. FreeSpec allows for the modular modeling 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.

This article is an extension of our conference paper from FM'2018. It gives an updated introduction to our formalism, which reduce the size of FreeSpec proofs. It also describes how FreeSpec can be used to reason about a component which is being used by more than one component. This composition pattern was not considered previously, although it is ubiquitous in practice. This work has been done in the context of the PhD of Thomas Letan, in collaboration with the ANSSI and Yann Régis-Gianas from Inria PI.R2 team.

Threat Hunting Threat hunting is the process of searching through a compromised network to isolate an active attacker. The efficiency of this process depends on the defender's ability to effectively identify the traces left by the attacker in the network. In [1], we formalize both defensive processes and the attacker's offensive approaches, allowing for confronting their respective perceptions during the same attack campaign. The attacker's perception of the campaign is built from the execution of his attack procedures, his exposed resources and the compromised components. The defender's perception of the attack is built from the collected traces on the targeted information system. This model leads to the construction of two persistent graphs on a common set of objects and components allowing for (1) an omniscient actor to compare, for both defender and attacker, the gap in knowledge and perceptions; (2) the attacker to become aware of the traces left on the targeted network; (3) the defender to improve the quality of Threat Hunting by identifying false-positives and adapting logging policy to be oriented for investigations.

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 as 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 [6] 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 $O(n)$ per process, when the number f of Byzantine processes verifies $f = O(1)$. We have improve upon this result by showing that the problem cannot be solved if $f = n/3$ or more processes are Byzantine. We have proposed a novel algorithm that works in a synchronous system model with signatures (i.e., the authenticated message model), tolerates up to f Byzantine failures (where $f < n/3$) and that terminates in $O(log\, f)$ rounds [7].

Blockchain in adversarial environments We are pursuing our efforts dedicated to the theoretical aspects of blockchains. There exists many forms of Blockchain finality conditions, from deterministic to probabilistic terminations. To favor availability against consistency in the face of partitions, most blockchains only offer probabilistic eventual finality: blocks may be revoked after being appended to the blockchain, yet with decreasing probability as they sink deeper into the chain. Other blockchains favor consistency by leveraging the immediate finality of Consensus -a block appended is never revoked- at the cost of additional synchronizations. In this paper, we focus on necessary and sufficient conditions to implement a blockchain with deterministic eventual finality, which ensures that selected main chains at different processes share a common increasing prefix. This is a much weaker form of finality that allows us to provide a solution in an asynchronous system subject to unlimited number of byzantine failures. We study stronger forms of eventual finality as well and show that it is unfortunately impossible to provide a bounded displacement. By bounded displacement we mean that the (unknown) number of blocks that can be revoked from the current blockchain is bounded. This problem reduces to consensus or eventual consensus depending on whether the bound is known or not. We also show that the classical selection mechanism, such as in Bitcoin, that appends blocks at the longest chain is not compliant with a solution to eventual finality [26].

In parallel to this work, we have proposed the design of a scalable permissionless blockchain in the proof-of-stake setting, called StakeCube. 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 an adaptive adversary, and makes no synchrony assumption beyond what is required for the byzantine agreement. We have instantiated and evaluated StakeCube, and experimentally studied and assessed its performance, especially regarding scalability. We were successfully able to run StakeCube with up to 5,000 participants,

confirming up to 1,100 bytes/s of transaction, with a confirmation time starting at 200 seconds. Finally, we have used StakeCube in a large scale energy marketplace application, and show that a node running on a Raspberry Pi Zero is able to handle the load without issues [8]. We have also proposed a consensus algorithm whose objective is to decide on the same union of proposed values, such that with high probability all the values proposed by the honest nodes belong to the decision. Our algorithm has been designed to cope with an asynchronous and permissionless system. By relying on a proof-of-eligibility, our algorithm is tolerant to an adversary capable of instantaneously corrupting entities. A straightforward application of our algorithm is the design of permissionless distributed ledgers [19].

USB filtering The project is to do filtering in "man-in-the-middle" mode between a Device and a USB Host. The underlying idea is to be able to block any possible attack via USB (BadUSB in particular) and to lock/restrict the use of a USB port on the Host (allow a limited number of devices vendors/classes, limit the types of commands that can be used...). Positioning in cut-off on the USB link allows to observe all the possible data circulating between Device and Host and also to have an OS-independent filtering method (which is particularly interesting to prevent attacks that take place before the OS starts up) To do this, we chose an FPGA (arty 7) programming linked to 2 USB PHY (USB3300 mounted on board by waveshare). This USB PHY allows to exchange USB packets via an ULPI interface (8 Data pins and 4 operating pins). The first objective is to be just a "pass-through" between the Host and the Device. With our set-up, we are currently able to:

- capture all USB packets for low-speed devices
- detect and block specific class and vendor ID
- detect and block keyboard if some keys are pressed
- detect and block keyboard if the keyboard typong speed is too high (BadUSB attack)

The next step is to handle full-speed devices and mass storage.

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

- **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 publicly datasets 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

8.2 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 focusing 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: 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 attacks. The approach is based on AI to automaticallydesign a model use for the oracle. It uses machine learning to search in a corpus of applicatons methods having the same semantics. Then in a second step, after converting the source code into a vector, it computes 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 her PhD thesis in November 2016 in the context of a contract between CentraleSupelec and the French Ministry of Defence. Her work consists in presenting events appearing in heterogeneous logs as a dependency graph between the lines of logs. This allows the administrator to investigate easily the logs to discover the different steps that an attack has performed 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.

- **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.

- **CEA: Etude du potentiel des approches à base de graphes et de preuves d'enjeux pour les cryptomonnaies avec ou sans permission** Mohamed-Aimen Djari has started his PhD thesis in October 2019 in the context of a contract between the CNRS and the CEA. His work consists in evaluating security and scalability of permissionless crypto-currency blockchains. The main objective of this thesis is to implement a proof-of-stake permissionless blockchain with suitable incentive mechanisms, and robust mechanisms to defend the system against Sybil attacks.

- **ANSSI: Formalisation de mécanismes de sécurité pour l'architecture de processeurs RISC-V** Matthieu Baty started his PhD in October 2020 in the context of a collaboration between Inria and the ANSSI. In this project, we want to formally specify hardware-based security mechanisms of a RISC-V processor to prove that they satisfy a well-defined security policy. In particular, we would like to use the Coq proof assistant to formally specify and verify the processor. Our goal is also to extract an HDL description of that certified processor, that could be used to synthetize the processor on an FPGA board.

9 Partnerships and cooperations

9.1 European initiatives

9.1.1 FP7 & H2020 Projects

SPARTA

Title: Special projects for advanced research and technology in Europe

Duration: February 2019 - January 2022

Coordinator: CEA (Commissariat à l'énergie atomique et aux énergies alternatives)

Partners: (only those that are directly related to task T6.4 of Programm HAII-T)

- SnT, University of Luxembourg (Luxembourg)
- ITTI SP ZOO (Poland)
- Institut Mines-Télécom (France)

Inria contact: Thomas Jensen (Celtique team)

Summary: SPARTA is a Cybersecurity Competence Network supported by the EU's H2020 program (Grantagreement ID: 830892) and led by CEA. This 3 years project started in February 2019. It aims at coordinating and developing 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 at developing 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.

- **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. Our goal is 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.

- **ANR Project: Byblos (2021-2025)**

  Byblos is a collaborative ANR project involving Rennes university, IRISA (CIDRE and WIDE research teams), Nantes university (GDD research team), and Insa Lyon, LIRIS (DRIM research team). This project aims at overcoming performance and scalability issues of blockchains, that are inherent to the total order that blockchain algorithms seek to achieve in their operations, which implies in turn a Byzantine-tolerant agreement. To overcome these limitations, this project aims at taking a step aside, and exploiting the fact that many applications – including cryptocurrencies – do not require full Byzantine agreement, and can be implemented with much lighter, and hence more scalable and efficient, guarantees. This project further argues that these novel Byzantine-tolerant applications have the potential to power large-scale multi-user online systems, and that in addition to Byzantine Fault Tolerance, these systems should also provide strong privacy protection mechanisms, that are designed from the ground up to exploit implicit synergies with Byzantine mechanisms.

- **FUI Project: SECEF (2020-2023)**

  SECEF (Security Exchange Format) is a collaborative project involving industrial (CS, IMS Networks, techlib', Cyber Test Systems) and academic (CentraleSupélec, Télécom SudParis) partners. The goal of this project is to promote format standardization in cybersecurity. More precisely, we want to address the limitation of the IDMEF format and to propose a new RFC for a standard security event exchange format. In this project, the CIDRE team is involved in studying the state of the art in security event formats and specifying a new security event format and its corresponding transport protocol. We will also participate in the standardisation effort.

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

General chair, scientific chair Emmanuelle Anceaume has co-organized with Christophe Bisière, Matthieu Bouvard, Quentin Bramas and Catherine Casamatta TOKENOMICS 2020: International Conference on Blockchain Economics, Security and Protocols. This hybrid event took place in Toulouse, 26-27 May 2020 [23].

Guillaume Hiet was the chair holder of the SILM thematic semester [1] on the security of software/hardware interfaces. The goal of this semester was to promote the scientific, teaching and industrial transfer activities on the security of software/hardware interfaces. Our objective was also to identify scientific and technological challenges in that field and to propose a strategic action plan. To that end, we organized different events in 2020:

- A master class, a demonstration and a presentation of the semester at International Cybersecurity Forum (FIC 2020), in January 2020, Lille, France;
- The second edition of the SILM workshop [2], in September 2020 (online event);
- A regular seminar [3] at Inria, Rennes, France.

We also wrote a white-paper on that topic that has been delivered to the DGA. This technical report is currently under review and will be publicly released in 2021.

Guillaume Hiet and Frédéric Tronel have co-organized SILM 2020: the second Workshop on the Security of the Software/Hardware Interfaces. This online event was co-localized with the IEEE Euro S&P conference, June 19 2020 [24].

Participation in Organizing Comittees Jean-Francois Lalande has been the local organizer of EICC 2020: European Interdisciplinary Cybersecurity Conference, Rennes, november 18th 2020 (ACM).

10.1.2 Scientific events: selection

Chair of conference program committees Jean-Francois Lalande was part of the program chair of IWSMR 2020: 2nd International Workshop on Information Security Methodology and Replication Studies.

Emmanuelle Anceaume was part of the program chair with Quentin Bramas of TOKENOMICS 2020.

Emmanuelle Anceaume was part of the program chair of the Fault tolerance, Security, and Privacy track of SSS 2020: 22nd International Symposium on Stabilization, Safety, and Security of Distributed Systems.

Guillaume Hiet and Frédéric Tronel have been the programm co-chairs of SILM 2020.

[1] https://silm.inria.fr/
[2] https://silm-workshop-2020.inria.fr/
[3] https://semestres-cyber.inria.fr/en/silm-seminar/

Members of Conference Program Comittees Jean-Francois Lalande served for the technical program committee of:

- Conferences:
  - SecITC 2020: International Conference on Information Technology and Communications
  - SSTIC 2020: Symposium sur la sécurité des technologies de l'information et des communications
- Workshops:
  - CUING 2020: International Workshop on Criminal Use of Information Hiding
  - WTMC 2020: International Workshop on Traffic Measurements for Cybersecurity
  - IWCC 2020: International Workshop on Cyber Crime
  - SPCLOUD 2020: International Workshop on Security, Privacy and Performance in Cloud

Emmanuelle Anceaume served for the technical program committee of:

- ICDCS 2020: 40th IEEE International Conference on Distributed Computing Systems ()
- TrustCom 2020: 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications ()
- SSS 2020: 22nd International Symposium on Stabilization, Safety, and Security of Distributed Systems ()
- NCA 2020: 19th IEEE International Symposium on Network Computing and Applications ()
- BRAINS 2020: 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services ()
- Algotel 2020: 22èmes rencontres francophones sur les aspects algorithmiques des télecommunications ()

Pierre Wilke served for the technical program committee of the SILM 2020 workshop (Sécurité de l'Interface Logiciel/Matériel).

Ludovic Mé served

- the Scientific Committee of FIC 2020.
- the Program Committee of CARI 2020.

Michel Hurfin served for the technical program committee of :

- CARI 2020: African Conference on Research in Computer Science and Applied Mathematics
- SSS 2020: 22nd International Symposium on Stabilization, Safety, and Security of Distributed Systems

Gilles Guette served for the technical program committee of:

- ISNCC 2020: IEEE International Symposium on Networks, Computers and Communications ()
- ICISSP 2020: International Conference on Information Systems Security and Privacy ()

Reviewers Valérie Viet Triem Tong served as a reviewer for the International Conference on Availability, Reliability and Security (ARES 2020)

Valérie Viet Triem Tong served as a reviewer for the International Conference on Information Technology and Communications (SecITC 2020)

Pierre Wilke served as a reviewer for the International Workshop on Cyber Crime (IWCC 2020)

10.1.3 Journals

Members of the editorial boards Jean-Francois Lalande was guest editor of Journal of Universal Computer Science for the special issue "Information Security Methodology, Replication Studies and Information Security Education" [25]

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

Reviewers - reviewing activities Jean-Francois Lalande was external reviewer for the journals:

- Computers and Security, Elsevier.
- IEEE Transactions on Reliability.
- Annals of Telecommunications, Springer.
- International Journal on Advances in Security, IARIA.

Guillaume Hiet was external reviewer for the journals:

- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems
- ACM Transactions on Privacy and Security
- IEEE Access

Ludovic Mé was external reviewer for the journal of the ACM Transactions on Embedded Computing Systems.

Michel Hurfin was external reviewer for the journal IEEE Transactions on Cloud Computing. Gilles Guette was external reviewer for The International Journal of Computer and Telecommunications Networking, Elsevier.

10.1.4 Scientific expertise

Jean-Francois Lalande is member of the advisory board of the SIMARGL H2020 project: Secure Intelligent Methods for Advanced Recognition of Malware and Stegomalware.

Emmanuelle Anceaume is member of the Task Force blockchain working group of the Ministry of Economics and Finance.

Ludovic Mé serves:

- the Scientific Council of the LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées);
- the Expert Council of the DSTN (Digital Science and Technology Network);
- the “Bureau du GT sécurité des systèmes logiciels” du GDR Sécurité;
- as a pilot for expert group for the evaluation of French research entities (UMRs and EAs) relatively to the protection of scientific and technological properties (PPST).

10.1.5 Research administration

Ludovic Mé, Guillaume Piolle, and Valérie Viet Triem Tong were members of a recruitment committee for an Inria chair in cybersecurity position at CentraleSupelec.

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

Ludovic Mé was member of a recruitment committee for a full Professor in cyber security at IMT Atlantique.

Ludovic Mé is deputy scientific director of Inria, in charge of the cybersecurity domain.

	Licence level	Master level	CS†	Univ. Rennes 1	Initial education	Continuing education	2019 -2020
Emmanuelle Anceaume		✓		✓	✓		10
Christophe Bidan	✓	✓	✓		✓	✓	-
Gilles Guette	✓	✓		✓	✓		400
Guillaume Hiet	✓	✓	✓		✓	✓	132
Jean-François Lalande	✓	✓	✓		✓	✓	282 +36*
Guillaume Piolle	✓	✓	✓	✓	✓	✓	209
Frédéric Tronel	✓	✓	✓	✓	✓	✓	287 ??*
Valérie Viet Triem Tong	✓	✓	✓	✓	✓	✓	125 105*

Table 1: Summary of teaching effort (eqTD) – †: CentraleSupélec – *: outside courses

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

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

In these institutions,

- Gilles Guette is the 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.

10.2.2 Supervision

PhD defended in 2020:

- 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%);
- Leopold Ouairy, *Analyse des vulnérabilités dans des systèmes embarqué face à des attaques par fuzzing*, started in 2017, supervised by Jean-Louis Lanet and Helene Le Bouder (IMT-A);
- 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%);
- David Lanoë, *Construction d'un multi-modèle d'application répartie pour la détection d'intrusion*, started in October 2016, supervised by Michel Hurfin (50%) and Eric Totel (50%);

- Pierre Graux, *Défis pour les Applications Android Natives : Obfuscation et Vulnérabilités.*, started in October 2017, supervised by Valérie Viet Triem Tong (50%) and Jean-François Lalande (50%);

- Laetitia Leichtnam, *Détection et visualisation d'anomalies dans des événements réseaux hétérogènes : modélisation des événements sous forme de graphes et détection de communautés et de nouveautés grâce à l'apprentissage automatique*, started in October 2016, supervised by Eric Totel (40%), Nicolas Prigent (30%) and Ludovic Mé (30%);

PhD in progress :

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

- 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%);

- Camille Le Bon, *Security enhancement in embedded hard real-time systems*, started in October 2018, supervised by Erven Rohou (PACAP) (30%), Guillaume Hiet (35%), Frédéric Tronel (35%)

- 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%);

- 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%);

- 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%);

- 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%).

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

- Pierre-Victor Besson, *Complete HOneynet with User Copycat on Hypervisor with Emulated Network* , started in November 2020, supervised by Valérie Viet Triem Tong (25%);, Gilles Guette (25%), Guillaume Piolle(25%), Erwan Abgrall (25%).

- Séverine Delaplace, *Analyse de malware Android communicant avec des serveurs distants*, started in November 2020, supervised by Jean-François Lalande (25%), Jacques Klein (25%), Pierre Wilke (25%) and Tegawendé Bissyande (25%).

- Romain Brisse, *Recommandation d'Explorations dans le cadre d'Investigations d'Incidents de Sécurité*, started in November 2020, supervised by Jean-François Lalande (50%), Frederic Majorczyk (50%)

- Mohammed-Aimen Djari, *Etude du potentiel des approches à base de graphes et de preuves d'enjeux pour les crypto monnaies avec ou sans permission* , started October 2019, supervised by Emmanuelle Anceaume and Sara Tucci (CEA).

- Matthieu Batty, *Formalisation de mécanismes de sécurité pour l'architecture de processeurs RISC-V*, started October 2020, supervised by Guillaume Hiet (37%), Pierre Wilke (38%) and Ludovic Mé (25%).

10.2.3 Juries

Valérie Viet Triem Tong has been the reviewer of the following PhD manuscript:

- Fabien Charmet, *Security Characterization of SDN Virtual Network migration: Formal Approach and Resource Optimization*, supervised by Abdallah M'Hamed et de Christophe Kiennert, Telecom Sud Paris, February 2020.

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

- Aliénor Damien, *Sécurité par analyse comportementale de fonctions embarquées sur plateformes avioniques modulaires intégrées*, supervised by Vincent Nicomette, Eric Alata, Nathalie Feyt, Université Fédérale de Toulouse Midi-Pyrénées, délivré par l'INSA de Toulouse, June 2020.

Ludovic Mé was reviewer for the following PhD manuscript:

- Jonathan Roux, "Détection d'intrusion dans des environnements sans-fil par l'analyse des activités radio.", supervised by Vincent Nicomette, Université Fédérale de Toulouse Midi-Pyrénées, délivré par l'INSA de Toulouse, February 2020.

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

- Renzo Navas, "Improving the Resilience of the Constrained Internet of Things", supervized by Laurent Toutain, IMT Atlantique, December 2020.

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

- Riad Ladjel, *Secure Distributed Computations for the Personal Cloud*, supervised by Nicolas Anciaux, Université Paris-Saclay, préparée à l'Université de Versailles Saint-Quentin-en-Yvelines, December 2020.

Jean-Francois Lalande was reviewer of the following PhD manuscript:

- Quentin Ricard, *Détection autonome de trafic malveillant dans les réseaux véhiculaires*, supervized by Philippe Owezarski, Université Fédérale Toulouse Midi-Pyrénées, september 24th 2020.

Emmanuelle Anceaume was the reviewer and member of the PhD committee for the following PhD thesis:

- Yackolley Amoussou-Guenou, *Governing the commons on Blockchain*. PhD thesis delivered by Sorbonne Université, supervised by Maria Potop-Butucaru and Sara Tucci.

Emmanuelle Anceaume was member of the PhD committee for the following PhD thesis:

- Adam Shimi, *On the Power of Rounds: Explorations of the Heard-Of Model*. TPhD thesis delivered by l'INPT de Toulouse and supervised by Aurélie Hurault and Philippe Queinnec.
- Hoang Long Nguyen, *Blockchain based transparency system*. Thèse délivrée par l'Université de Lorraine, Laboratoire Lorrain de Recherche en Informatique et ses Applications, UMR 7503. PhD thesis supervised by Olivier Perrin.

10.3 Popularization

10.3.1 Articles and contents

We published several articles related to security in Blog binaire of Le Monde:

- "Des codes malveillants jusque dans la poche", Jean-François Lalande & Valérie Viet Triem Tong
- "Snowden : d'Orwell à La Boétie", Jean-Louis Lanet
- "Le divulgâcheur du bureau des légendes", Ludovic Mé

10.3.2 Education

CIDRE has won the special price "Open access 2020" of the HALathon 2020 event, organized internally by CentraleSupélec.

10.3.3 Interventions

Guillaume Hiet presented a master class on the security of software/hardware interfaces during the International Cybersecurity Forum (FIC 2020).

11 Scientific production

11.1 Publications of the year

International journals

[1] A. Berady, M. Jaume, V. Viet Triem Tong and G. Guette. 'From TTP to IoC: Advanced Persistent Graphs for Threat Hunting'. In: *IEEE Transactions on Network and Service Management*. Latest Developments for Security Management of Networks and Services Special Issue (2021). DOI: 10.1109/TNSM.2021.3056999. URL: https://hal.inria.fr/hal-03131262.

[2] R. Chevalier, D. Plaquin, C. Dalton and G. Hiet. 'Intrusion Survivability for Commodity Operating Systems'. In: *Digital Threats: Research and Practice* 1.4 (Dec. 2020). DOI: 10.1145/34194571. URL: https://hal.inria.fr/hal-03085774.

[3] M. Farhadi, J.-L. Lanet, G. Pierre and D. Miorandi. 'A systematic approach towards security in Fog computing: assets, vulnerabilities, possible countermeasures'. In: *Software: Practice and Experience* 50.6 (2020), pp. 973–997. DOI: 10.1002/spe.2804. URL: https://hal.inria.fr/hal-02441639.

[4] T. Letan, Y. Régis-Gianas, P. Chifflier and G. Hiet. 'Modular verification of programs with effects and effects handlers'. In: *Formal Aspects of Computing* (15th Dec. 2020). DOI: 10.1007/s00165-020-00523-2. URL: https://hal.archives-ouvertes.fr/hal-03107526.

[5] Y. Mocquard, B. Sericola and E. Anceaume. 'Probabilistic Analysis of Rumor Spreading Time'. In: *INFORMS Journal on Computing* 32.1 (1st Oct. 2020). DOI: 10.1287/ijoc.2018.0845. URL: https://hal.archives-ouvertes.fr/hal-01888300.

International peer-reviewed conferences

[6] G. Antonio Di Luna, E. Anceaume and L. Querzoni. 'Byzantine Generalized Lattice Agreement'. In: Proceedings of the 34th IEEE International Parallel and Distributed Processing Symposium (IPDPS). Proceedings of the 34th IEEE International Parallel and Distributed Processing Symposium (IPDPS). New Orleans, United States, 18th May 2020. URL: https://hal.archives-ouvertes.fr/hal-02472207.

[7] G. A. Di Luna, E. Anceaume, S. Bonomi and L. Querzoni. 'Synchronous Byzantine Lattice Agreement in O(log(f)) Rounds'. In: ICDCS 2020 - 40th IEEE International Conference on Distributed Computing Systems. Singapore, Singapore, 8th July 2020, pp. 1–11. URL: https://hal-cnrs.archives-ouvertes.fr/hal-02473843.

[8] A. Durand, G. Hébert, K. Toumi, G. Memmi and E. Anceaume. 'The StakeCube blockchain : Instantiation, Evaluation & Applications'. In: BCCA 2020 - International Conference on Blockchain Computing and Applications. IEEE BCCA 2020 - International Conference on Blockchain Computing and Applications. Virtual, Turkey, 3rd Nov. 2020, pp. 1–8. URL: https://hal.archives-ouvertes.fr/hal-03024408.

[9] M. Escouteloup, R. Lashermes, J.-L. Lanet and J. J.-A. Fournier. 'Recommendations for a radically secure ISA'. In: *Fourth Workshop on Computer Architecture Research with RISC-V*. CARRV 2020 - Workshop on Computer Architecture Research with RISC-V. Valence (virtual), Spain, 29th May 2020, pp. 1–22. URL: https://hal.archives-ouvertes.fr/hal-03128242.

[10] C. Gottstein, P. R. Parvedy, M. Hurfin, T. Hassan and T. Coupaye. 'Inverse Space Filling Curve Partitioning Applied to Wide Area Graphs'. In: DMS 2020 - 11th International conference on Database Management Systems. Zurich, Switzerland, 21st Nov. 2020, pp. 223–241. DOI: 10.5121/csit.2020.101417. URL: https://hal.inria.fr/hal-03137952.

[11] P. Graux, J.-F. Lalande, V. Viet Triem Tong and P. Wilke. 'Preventing Serialization Vulnerabilities through Transient Field Detection'. In: SAC 2021 - The 36th ACM/SIGAPP Symposium On Applied Computing. Gwangju / Virtual, South Korea, 22nd Mar. 2021. URL: https://hal.inria.fr/hal-03066847.

[12] P. Graux, J.-F. Lalande, P. Wilke and V. Viet Triem Tong. 'Abusing Android Runtime for Application Obfuscation'. In: SAD 2020 - Workshop on Software Attacks and Defenses. Genova, Italy, 11th Sept. 2020, pp. 616–624. DOI: 10.1109/EuroSPW51379.2020.00089. URL: https://hal-centralesupelec.archives-ouvertes.fr/hal-02877815.

[13] C. Herzog, V. Viet Triem Tong, P. Wilke, A. Van Straaten and J.-L. Lanet. 'Evasive Windows Malware: Impact on Antiviruses and Possible Countermeasures'. In: SECRYPT 2020 - 17th International Conference on Security and Cryptography. Proceedings of the 17th International Joint Conference on e-Business and Telecommunications - (Volume 3). Lieusaint - Paris, France, 8th July 2020, pp. 302–309. DOI: 10.5220/0009816703020309. URL: https://hal.archives-ouvertes.fr/hal-02949067.

[14] J.-F. Lalande, M. Simon and V. Viet Triem Tong. 'GroDDViewer: Dynamic Dual View of Android Malware'. In: GraMSec 2020 - 7th Seventh International Workshop on Graphical Models for Security. Vol. 12419. LNCS. Virtual Conference, France: https://gramsec.uni.lu, 22nd June 2020, pp. 127–139. DOI: 10.1007/978-3-030-62230-5_7. URL: https://hal-centralesupelec.archives-ouvertes.fr/hal-02913112.

[15] L. Leichtnam, E. Totel, N. Prigent and L. Mé. 'Forensic Analysis of Network Attacks: Restructuring Security Events as Graphs and Identifying Strongly Connected Sub-graphs'. In: WTMC 2020 - International Workshop on Traffic Measurements for Cybersecurity. Genova, Italy, 7th Sept. 2020, pp. 1–9. URL: https://hal.inria.fr/hal-02950490.

[16] L. Leichtnam, E. Totel, N. Prigent and L. Mé. 'Sec2graph: Network Attack Detection Based on Novelty Detection on Graph Structured Data'. In: DIMVA 2020 - 17th Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Lisbon, Portugal, 24th June 2020, pp. 1–20. URL: https://hal.inria.fr/hal-02950489.

[17] L. Ouairy, H. Le Bouder and J.-L. Lanet. 'Confiance: detecting vulnerabilities in Java Card applets'. In: International Conference on Availability, Reliability and Security (ARES). Dublin (effectué en visioconférence), Ireland, 25th Aug. 2020. URL: https://hal.inria.fr/hal-02933668.

[18] P.-Y. Péneau, L. Claudepierre, D. Hardy and E. Rohou. 'NOP-Oriented Programming: Should we Care?' In: Sécurité des Interfaces Logiciel/Matériel. Genoa (virtual), Italy, 11th Sept. 2020. DOI: 10.1109/EuroSPW51379.2020.00100. URL: https://hal.inria.fr/hal-02912301.

[19] G. Saunois, F. Robin, E. Anceaume and B. Sericola. 'Permissionless Consensus based on Proof-of-Eligibility'. In: NCA 2020 - 19th IEEE International Symposium on Network Computing and Applications. Vol. 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA). Boston (virtual venue), United States, 24th Nov. 2020. URL: https://hal.archives-ouvertes.fr/hal-03043681.

[20] Y. Wang, X. Xu, P. Wilke and Z. Shao. 'CompCertELF: Verified Separate Compilation of C Programs into ELF Object Files'. In: Proceedings of the ACM on Programming Languages (PACMPL). Chicago, United States, 16th Nov. 2020. URL: https://hal.archives-ouvertes.fr/hal-03114583.

Conferences without proceedings

[21] C. Herzog, V. Tong, P. Wilke and J.-L. Lanet. 'Malware Windows Evasifs : Impact sur les Antivirus et Possible Contre-mesure'. In: CAID 2020 - Conference on Artificial Intelligence for Defense. Rennes, France, 2020. DOI: 10.5220/0009816703020309. URL: https://hal.inria.fr/hal-03139240.

[22] L. Leichtnam, E. Totel, N. Prigent and L. Mé. 'Novelty detection on graph structured data to detect network intrusions'. In: CAID 2020 - Conference on Artificial Intelligence for Defense. Virtual, France, 15th Dec. 2020. URL: https://hal.inria.fr/hal-03115308.

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

[23] E. Anceaume, C. Bisière, M. Bouvard, Q. Bramas and C. Casamatta, eds. *2nd International Conference on Blockchain Economics, Security and Protocols*. Vol. 82. OASICS. Feb. 2021. DOI: 10.4230/OASIcs.Tokenomics.2020.0. URL: https://hal.archives-ouvertes.fr/hal-03129685.

[24] G. Hiet, F. Tronel and J.-L. Lanet, eds. *Preface of the 2nd Workshop on the Security of Software/Hardware Interfaces (SILM 2020)*. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Genoa, 2020, p. 681. DOI: 10.1109/EuroSPW51379.2020.00097. URL: https://hal.archives-ouvertes.fr/hal-03136790.

[25] S. Wendzel, L. Caviglione, A. Checco, A. Mileva, J.-F. Lalande and W. Mazurczyk. *Information Security Methodology, Replication Studies and Information Security Education*. Vol. 26. Special issue of Journal of Universal Computer Science 7. 28th July 2020, pp. 762–763. URL: https://hal-centralesupelec.archives-ouvertes.fr/hal-02988140.

Reports & preprints

[26] E. Anceaume, A. D. Pozzo, T. Rieutord and S. Tucci-Piergiovanni. *On Finality in Blockchains*. 16th Feb. 2021. URL: https://hal-cea.archives-ouvertes.fr/cea-03080029.

[27] Y. Mocquard, B. Sericola, F. Robin and E. Anceaume. *Stochastic Analysis of Average Based Distributed Algorithms*. 11th Feb. 2020. URL: https://hal-cnrs.archives-ouvertes.fr/hal-02473856.

[28] F. Robin, B. Sericola, E. Anceaume and Y. Mocquard. *Pulling multiple nodes for rumor spreading*. 6th Mar. 2020. URL: https://hal.archives-ouvertes.fr/hal-02500504.

[29] F. Robin, B. Sericola, E. Anceaume and Y. Mocquard. *Stochastic analysis of rumor spreading with k-pull operations*. 2nd Feb. 2021. URL: https://hal.archives-ouvertes.fr/hal-03128118.