RESEARCH CENTRE

Inria Centre at Rennes University

IN PARTNERSHIP WITH:

CNRS, CentraleSupélec, Université de Rennes

2023

ACTIVITY REPORT

Team

CIDRE

Confidentialité, Intégrité, Disponibilité et Répartition

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

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

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Security and Confidentiality

Inria

Contents

Team CIDRE 1

1 Team members, visitors, external collaborators 2

2 Overall objectives 4
2.1 CIDRE in Brief . . . 4

3 Research program 4
3.1 Our perspective . . . 4

4 Application domains 4

5 Highlights of the year 4
5.1 Awards . . . 4

6 New software, platforms, open data 4
6.1 New software . . . 4
6.1.1 OATs'inside . . . 4
6.1.2 MoM . . . 5
6.1.3 DaViz . . . 5
6.1.4 Koika-LLR . . . 6
6.1.5 URSID . . . 6
6.2 Open data . . . 6

7 New results 6
7.1 Axis 1 : Attack comprehension . . . 6
7.2 Axis 2 : Attack detection . . . 9
7.3 Axis 3 : Attack resistance . . . 9

8 Bilateral contracts and grants with industry 11
8.1 Bilateral contracts with industry . . . 11
8.2 Bilateral grants with industry . . . 11

9 Partnerships and cooperations 13
9.1 International initiatives . . . 13
9.1.1 Visits to international teams . . . 13
9.2 National initiatives . . . 13
9.3 Regional initiatives . . . 16

10 Dissemination 16
10.1 Promoting scientific activities . . . 17
10.1.1 Scientific events: organisation . . . 17
10.1.2 Scientific events: selection . . . 17
10.1.3 Invited talks . . . 17
10.1.4 Scientific expertise . . . 18
10.1.5 Research administration . . . 18
10.2 Teaching - Supervision - Juries . . . 18
10.2.1 Teaching . . . 18
10.2.2 Supervision(Ongoing Phd thesis) . . . 18
10.2.3 Juries . . . 20
10.3 Popularization . . . 21
10.3.1 Articles and contents . . . 21
10.3.2 Education . . . 21
10.3.3 Interventions . . . 21

11 Scientific production **21**
11.1 Major publications 21
11.2 Publications of the year 22
11.3 Cited publications 24

Team CIDRE

Creation of the Team: 2023 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]
- Yufei Han [INRIA, Advanced Research Position]
- Michel Hurfin [INRIA, Researcher, HDR]
- Ludovic Me [INRIA, Senior Researcher, HDR]

Faculty Members

- Valerie Viet Triem Tong [Team leader, CENTRALESUPELEC, Professor, HDR]
- Kevin Allix [CENTRALESUPELEC, Associate Professor, until Jun 2023]
- Christophe Bidan [CENTRALESUPELEC, Professor, HDR]
- Pierre-Francois Gimenez [CENTRALESUPELEC, Associate Professor]
- Gilles Guette [UNIV RENNES, Associate Professor]
- Guillaume Hiet [CENTRALESUPELEC, Professor, HDR]
- Jean-François Lalande [CENTRALESUPELEC, Professor, HDR]
- Alessandro Palumbo [CENTRALESUPELEC, Associate Professor, from Nov 2023]
- Rubén Salvador Perea [CENTRALESUPELEC, Associate Professor, from Mar 2023]
- Frédéric Tronel [CENTRALESUPELEC, Associate Professor]
- Yaëlle Vinçont [ENS RENNES, Professor, from Sep 2023]
- Pierre Wilke [CENTRALESUPELEC, Associate Professor]

Post-Doctoral Fellow

- Anatolii Khalin [CENTRALESUPELEC, Post-Doctoral Fellow, from Nov 2023]

PhD Students

- Lucas Aubard [INRIA]
- Matthieu Baty [INRIA]
- Nicolas Bellec [CENTRALESUPELEC, ATER, until Nov 2023]
- Pierre-Victor Besson [CENTRALESUPELEC, until Aug 2023]
- Pierre-Victor Besson [UNIV RENNES, ATER, from Sep 2023]
- Romain Brisse [MALIZEN]
- Séverine Delaplace [UNIV LUXEMBOURG]
- Fanny Dijoud [INRIA, from Nov 2023]
- Lionel Hemmerle [CENTRALESUPELEC]
- Maxime Lanvin [CENTRALESUPELEC]

- Pierre Lledo [DGA-MI, from Dec 2023]
- Jean-Marie Mineau [CENTRALESUPELEC]
- Hélène Orsini [CENTRALESUPELEC]
- Manuel Poisson [AMOSSYS, CIFRE, from Mar 2023]
- Vincent Raulin [INRIA]
- Adrien Schoen [INRIA]
- Natan Talon [HACKUITY, CIFRE]

Technical Staff

- Sébastien Kilian [CENTRALESUPELEC, Engineer, from Nov 2023 until Nov 2023]
- Manuel Poisson [UNIV RENNES, Engineer, until Jan 2023]
- Manuel Poisson [INRIA, Engineer, from Feb 2023 until Mar 2023]

Interns and Apprentices

- Lucien Audebert [CENTRALESUPELEC, from Apr 2023 until Jul 2023]
- Fanny Dijoud [CENTRALESUPELEC, from Apr 2023 until Sep 2023]
- Aymane El Otmani [CENTRALESUPELEC, from Apr 2023 until Aug 2023]
- Thibault Guerinel [CENTRALESUPELEC, from Jun 2023 until Jun 2023]
- Ayman Houna [CENTRALESUPELEC, from Mar 2023 until Jul 2023]
- Sinan Ismaila [INRIA, from May 2023 until Jul 2023]
- Sebastien Kilian [UNIV RENNES, from Feb 2023 until Jul 2023]
- Marius Le Douarin [CENTRALESUPELEC, from Jun 2023 until Sep 2023]
- Clara Moy [UNIV RENNES, from Jun 2023 until Jul 2023]
- Seydina Oumar Niang [CENTRALESUPELEC, from Apr 2023 until Jun 2023]
- Lomig Piette [CENTRALESUPELEC, from May 2023 until Jul 2023]
- Grégor Quetel [CENTRALESUPELEC, from Feb 2023 until Jul 2023]
- Thomas Sericola [UNIV RENNES, from Jun 2023 until Jun 2023]

Administrative Assistant

- Lydie Mabil [INRIA]

Visiting Scientist

- Joscha Cüppers [CISPA, from Jul 2023 until Sep 2023]

External Collaborators

- Erwan Abgrall [MINISTERE DES ARMEES, until Aug 2023]
- Frederic Majorczyk [DGA-MI]
- Louis Rilling [DGA-MI, from Dec 2023]

2 Overall objectives

2.1 CIDRE in Brief

The Cidre team is interested in with security issues that weaken machines, networks and organizations. 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 Cidre team are naturally system security. 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

5.1 Awards

Aimad Berady has received the "Special Jury Prize at the Prix de la gendarmerie nationale 2023 - Research and Strategic Thinking" for his Ph.D. thesis.

6 New software, platforms, open data

6.1 New software

6.1.1 OATs'inside

Keywords: Android, Malware, Reverse engineering, Code analysis

Scientific Description: OATs'inside is an analysis tool that handles native Android applications. The system uses a hybrid approach based on dynamic monitoring and trace-based symbolic execution to output control flow graphs for each method of the analyzed application.

Functional Description: OATs'inside is an Android reverse engineering tool that try to handle some native based 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.

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

Publication: hal-02877815

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

Contact: Jean-François Lalande

6.1.2 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

Contact: Valerie Viet Triem Tong

Partner: DGA-MI

6.1.3 DaViz

Name: Dataset Vizulisation

Keywords: Visualization, Android

Scientific Description: With millions of Android malware samples available, researchers have a large amount of data to perform malware detection and classification, specially with the help of machine learning. Thus far, visualization tools focus on single samples or one-to-many comparison, but not a many-to-many approach. Daviz is a web frontend/backend that aids to compare and explore Android application datasets. With the aid of multiple chart types and a system of interactive sample filtering, users can get a better understanding of the datasets at hand.

Functional Description: Daviz is a web frontend and backend for the interactive visualization of large scale dataset of Android applications.

Contact: Jean-François Lalande

Participants: Tomas Concepcion Miranda, Leopold Ouairy, Damien Gourbeyre

6.1.4 Koika-LLR

Name: Koika-LLR

Keywords: Proof, Hardware platform

Functional Description: This is the development associated with CSF'23 paper, aiming at proving properties about Kôika circuits.

CSF23: A generic framework to develop and verify security mechanisms at the microarchitectural level: application to control-flow integrity

URL: https://gitlab.inria.fr/cidre-public/koika-llr

Contact: Matthieu Baty

6.1.5 URSID

Keywords: Cybersecurity, Cyber attack, Virtual Machine, Cyber Range

Functional Description: URSID makes it possible to deploy multiple variants of vulnerable virtual architectures from a single attack scenario description. These architectures can be used to train security teams or students, or as a honeypot for learning and analyzing attack techniques used in the field.

Authors: Pierre-Victor Besson, Gireg Maury, Gilles Guette, Valerie Viet Triem Tong, Alexandre Monroche

Contact: Pierre-Victor Besson

6.2 Open data

We have released a dataset containing a red team exercise of 13 participants with the publication [9]. The CERBERE projectis both a reproducible attack-defense exercise and a labelled dataset usable for research purposes. The attack-defense exercise is first composed of an exercise for red teamers automatically deployed with variable attack scenarios. Second, an exercise for blue teamers can be operated using the system and network logs generated during the attack phase. We provide with this article, the software to rebuild the infrastructure for red teamers. We share a labelled dataset where we spot the ground truth, i.e. the log lines that have been involved in the attacker's actionsThe dataset contains system and network logs related to the intrusion of a red teamer attacking a small infrastructure. The originality of the dataset is that all infrastructures contain different vulnerabilities which grealty enrich the dataset in terms of variability. The dataset is available on https://gitlab.inria.fr/cidre-public/cerbere-dataset/

7 New results

7.1 Axis 1 : Attack comprehension

To fully understand various methodologies of cyber attacks, our study is organized with a two-fold focus. On one hand, we are interested in providing security analysts the tools for quickly capturing the knowledge of the scope of an attack in progress. On the other hand, we are interested with investigating new horizons of emerging threats.

Participants: Erwan Abgrall, Kevin Allix, Romain Brisse, Pierre-François Gimenez, Gilles Guette, Yufei Han, Maxime Lanvin, Jean-François Lalande, Frédéric Majorczyk, Manuel Poisson, Vincent Raulin, Ruben Salvador, Valérie Viet Triem Tong, Pierre Wilke.

Attacking at non-harmonic frequencies in screaming-channel attacks Screaming-channel attacks enable Electromagnetic (EM) Side-Channel Attacks (SCAs) at larger distances due to higher EM leakage energies than traditional SCAs, relaxing the requirement of close access to the victim. This attack can be mounted on devices integrating Radio Frequency (RF) modules on the same die as digital circuits, where the RF can unintentionally capture, modulate, amplify, and transmit the leakage along with legitimate signals. Leakage results from digital switching activity, so the hypothesis of previous works was that this leakage would appear at multiples of the digital clock frequency, i.e., harmonics. Our work [14] demonstrates that compromising signals appear not only at the harmonics and that leakage at non-harmonics can be exploited for successful attacks. Indeed, the transformations undergone by the leaked signal are complex due to propagation effects through the substrate and power and ground planes, so the leakage also appears at other frequencies. We first propose two methodologies to locate frequencies that contain leakage and demonstrate that it appears at non-harmonic frequencies. Then, our experimental results show that screaming-channel attacks at non-harmonic frequencies can be as successful as at harmonics when retrieving a 16-byte AES key. As the RF spectrum is polluted by interfering signals, we run experiments and show successful attacks in a more realistic, noisy environment where harmonic frequencies are contaminated by multi-path fading and interference. These attacks at non-harmonic frequencies increase the attack surface by providing attackers with an increased number of potential frequencies where attacks can succeed.

High-Level Synthesis-Based On-board Payload Data Processing considering the Roofline Model On-board payload data processing can be performed by developing space-qualified heterogeneous Multi-processor Systemon-Chips (MPSoCs). We present in [19] key compute-intensive payload algorithms, based on a survey with space science researchers, including the two-dimensional Fast Fourier Transform (2-D FFT). Also, we propose to perform design space exploration by combining the roofline performance model with High-Level Synthesis (HLS) for hardware accelerator architecture design. The roofline model visualizes the limits of a given architecture regarding Input/Output (I/O) bandwidth and computational performance, along with the achieved performance for different implementations. HLS is an interesting option in developing FPGA-based onboard processing applications for payload teams that need to adjust architecture specifications through design reviews and have limited expertise in Hardware Description Languages (HDLs). In this paper, we focus on an FPGA-based MPSoC thanks to recently released radiation-hardened heterogeneous embedded platforms.

Retrieving Object Behaviors From Native-based Obfuscated Android Applications Analyzing Android applications is essential to review proprietary code and to understand malware behaviors. However, Android applications use obfuscation techniques to slow down this process. These obfuscation techniques are increasingly based on native code. In [6], we propose OATs'inside, a new analysis tool that focuses on high-level behaviors to circumvent native obfuscation techniques transparently. The targeted high-level behaviors are object-level behaviors, i.e., actions performed on Java objects (e.g., field accesses, method calls), regardless of whether these actions are performed using Java or native code. Our system 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. CFGs are composed of Java-like actions enriched with condition expressions and dataflows between actions, giving an understandable representation of any code, even those fully native. OATs'inside spares users the need to dive into low-level instructions, which are difficult to reverse engineer. We extensively compare OATs'inside functionalities against state-of-the-art tools to highlight the benefit when observing native operations. Our experiments are conducted on a real smartphone: We discuss the performance impact of OATs'inside, and we demonstrate its practical use on applications containing anti-debugging techniques provided by the OWASP foundation. We also evaluate the robustness of OATs'inside using obfuscated unit tests using the Tigress obfuscator.

BAGUETTE: Hunting for Evidence of Malicious Behavior in Dynamic Analysis Reports Malware analysis consists of studying a sample of suspicious code to understand it and producing a representation or explanation of this code that can be used by a human expert or a clustering/classification/detection tool. The analysis can be static (only the code is studied) or dynamic (only the interaction between the

code and its host during one or more executions is studied). The quality of the interpretation of a code and its later detection depends on the quality of the information contained in this representation. To date, many analyses produce voluminous reports that are difficult to handle quickly. In [23], we present BAGUETTE, a graph-based representation of the interactions of a sample and the resources offered by the host system during one execution. We explain how BAGUETTE helps automatically search for specific behaviors in a malware database and how it efficiently assists the expert in analyzing samples.

Humans vs. Machines in Malware Classification Today, the classification of a file as either benign or malicious is performed by a combination of deterministic indicators (such as antivirus rules), machine learning classifiers, and, more importantly, the judgment of human experts. However, to compare the difference between human and machine intelligence in malware analysis, it is first necessary to understand how human subjects approach malware classification. In this direction, we present in [7] the first experimental study designed to capture which 'features' of a suspicious program (e.g., static properties or runtime behaviors) are prioritized for malware classification according to humans and machines intelligence. For this purpose, we created a malware classification game where 110 human players worldwide and with different seniority levels (72 novices and 38 experts) have competed to classify the highest number of unknown samples based on detailed sandbox reports. Surprisingly, we discovered that both experts and novices base their decisions on approximately the same features, even if there are clear differences between the two expertise classes. Furthermore, we implemented two state-of-the-art Machine Learning models for malware classification and evaluated their performances on the same set of samples. The comparative analysis of the results unveiled a common set of features preferred by both Machine Learning models and helped better understand the difference in the feature extraction. This work reflects the difference in the decision-making process of humans and computer algorithms and the different ways they extract information from the same data. Its findings serve multiple purposes, from training better malware analysts to improving feature encoding.

Decoding the Secrets of Machine Learning in Windows Malware Classification: A Deep Dive into Datasets, Features, and Model Performance Many studies have proposed machine-learning (ML) models for malware detection and classification, reporting an almost-perfect performance. However, they assemble ground-truth in different ways, use diverse static-and dynamic-analysis techniques for feature extraction, and even differ on what they consider a malware family. As a consequence, our community still lacks an understanding of malware classification results: whether they are tied to the nature and distribution of the collected dataset, to what extent the number of families and samples in the training dataset influence performance, and how well static and dynamic features complement each other. The article [12] sheds light on those open questions by investigating the impact of datasets, features, and classifiers on ML-based malware detection and classification. For this, we collect the largest balanced malware dataset so far with 67k samples from 670 families (100 samples each), and train state-of-the-art models for malware detection and family classification using our dataset. Our results reveal that static features perform better than dynamic features, and that combining both only provides marginal improvement over static features. We discover no correlation between packing and classification accuracy, and that missing behaviors in dynamically-extracted features highly penalise their performance. We also demonstrate how a larger number of families to classify makes the classification harder, while a higher number of samples per family increases accuracy. Finally, we find that models trained on a uniform distribution of samples per family better generalize on unseen data.

BadVFL: Backdoor Attacks in Vertical Federated Learning Federated learning (FL) enables multiple parties to collaboratively train a machine learning model without sharing their data; rather, they train their own model locally and send updates to a central server for aggregation. Depending on how the data is distributed among the participants, FL can be classified into Horizontal (HFL) and Vertical (VFL). In VFL, the participants share the same set of training instances but only host a different and non-overlapping subset of the whole feature space. Whereas in HFL, each participant shares the same set of features while the training set is split into locally owned training data subsets. VFL is increasingly used in applications like financial fraud detection; nonetheless, very little work has analyzed its security. In [20], we focus on robustness in VFL, in particular, on backdoor attacks, whereby an adversary attempts to manipulate the

aggregate model during the training process to trigger misclassifications. Performing backdoor attacks in VFL is more challenging than in HFL, as the adversary i) does not have access to the labels during training and ii) cannot change the labels as she only has access to the feature embeddings. We present a first-of-its-kind clean-label backdoor attack in VFL, which consists of two phases: a label inference and a backdoor phase. We demonstrate the effectiveness of the attack on three different datasets, investigate the factors involved in its success, and discuss countermeasures to mitigate its impact.

Unveiling stealth attack paths in Windows Environments using AWARE When an attacker targets a system, he aims to remain undetected as long as possible. He must therefore avoid performing actions that are characteristic of an identified malicious behavior. One way to avoid detection is to only perform actions on the system that appear legitimate. That is, actions that are allowed because of the system configuration or actions that are possible by diverting the use of legitimate services. In [21], we present and experiment with AWARE (Attacks in Windows Architectures REvealed), a defensive tool able to query a Windows system and build a directed graph highlighting possible stealthy attack paths that an attacker could use during the propagation phase of an attack campaign. These attack paths only rely on legitimate system actions and the use of Living-Off-The-Land binaries. AWARE also proposes a range of corrective measures to prevent these attack paths.

CVE representation to build attack positions graphs In cybersecurity, CVEs (Common Vulnerabilities and Exposures) are publicly disclosed hardware or software vulnerabilities. These vulnerabilities are documented and listed in the NVD database maintained by the NIST. Knowledge of the CVEs impacting an information system provides a measure of its level of security. In [22] we point out that these vulnerabilities should be described in greater detail to understand how they could be chained together in a complete attack scenario. This article presents the first proposal for the CAPG format, which is a method for representing a CVE vulnerability, a corresponding exploit, and associated attack positions.

7.2 Axis 2 : Attack detection

Participants: Pierre-Francois Gimenez, Yufei Han, Maxime Lanvin, Frédéric Majorczyk, Ludovic Mé, Adrien Schoen.

Towards Understanding Alerts raised by Unsupervised Network Intrusion Detection Systems The use of machine learning for anomaly detection in cyber security-critical applications, such as intrusion detection systems, has been hindered by the lack of explainability. Without understanding the reason behind anomaly alerts, it is too expensive or impossible for human analysts to verify and identify cyber-attacks. Our research addresses this challenge and focuses on unsupervised network intrusion detection, where only benign network traffic is available for training the detection model. In [18], we propose a novel post-hoc explanation method, called AE-pvalues, which is based on the p-values of the reconstruction errors produced by an Auto-Encoder-based anomaly detection method. Our work identifies the most informative network traffic features associated with an anomaly alert, providing interpretations for the generated alerts. We conduct an empirical study using a large-scale network intrusion dataset, CICIDS2017, to compare the proposed AE-pvalues method with two state-of-the-art baselines applied in the unsupervised anomaly detection task. Our experimental results show that the AE-pvalues method accurately identifies abnormal influential network traffic features. Furthermore, our study demonstrates that the explanation outputs can help identify different types of network attacks in the detected anomalies, enabling human security analysts to understand the root cause of the anomalies and take prompt action to strengthen security measures.

7.3 Axis 3 : Attack resistance

Participants: Emmanuelle Anceaume, Erwan Abgrall, Matthieu Baty, Pierre-Victor Besson, Gilles Guette, Yufei Han, Guillaume Hiet, Sebastien Kilian, Frédéric Tronel, Pierre Wilke.

A generic framework to develop and verify security mechanisms at the microarchitectural level: application to control-flow integrity In recent years, the disclosure of several significant security vulnerabilities has revealed the trust put in some presumed security properties of commonplace hardware to be misplaced. We propose to design hardware systems with security mechanisms, together with a formal statement of the security properties obtained, and a machine-checked proof that the hardware security mechanisms indeed implement the sought-for security property. Formally proving security properties about hardware systems might seem prohibitively complex and expensive. In [8], we tackle this concern by designing a realistic and accessible methodology on top of the Kôika Hardware Description Language [27] for specifying and proving security properties during hardware development. Our methodology is centered around a verified compiler from high-level and inefficient to work with Kôika models to an equivalent lower-level representation where side effects are made explicit and reasoning is convenient. We apply this methodology to a concrete example: the formal specification and implementation of a shadow stack mechanism on an RV32I processor. We prove that this security mechanism is correct, i.e., any illegal modification of a return address does indeed result in the termination of the whole system. Furthermore, we show that this modification of the processor does not impact its behaviour in other, unexpected ways.

Stochastic analysis of rumor spreading with multiple pull operations in presence of non-cooperative nodes The recent rise of interest in distributed applications has highlighted the importance of effective information dissemination. The challenge lies in the fact that nodes in a distributed system are not necessarily synchronized, and may fail at any time. This has led to the emergence of randomized rumor spreading protocols, such as push and pull protocols, which have been studied extensively. The k-pull operation, which allows an uninformed node to ask for the rumor from a fixed number of other nodes in parallel, has been proposed to improve the pull algorithm's effectiveness. In [16], we present and study the performance of the k-pull operation in the presence of a certain fraction f of non-cooperative nodes. Our goal is to understand the impact of k on the propagation of the rumor despite the presence of a fraction f of non-collaborative nodes.

Automatically Refining a Single Attack Scenario into Multiple Cyber Range Architectures Contrary to intuition, insecure computer network architectures are valuable assets in IT security. Indeed, such architectures (referred to as cyber-ranges) are commonly used to train red teams and test security solutions, in particular the ones related to supervision security. Unfortunately, the design and deployment of these cyber-ranges is costly, as they require designing an attack scenario from scratch and then implementing it in an architecture on a case-by-case basis, through manual choices of machines/users, OS versions, available services and configuration choices. The article [10] presents URSID, a framework for automatic deployment of cyber-ranges based on the formal description of attack scenarios. The scenario is described at the technical attack level according to the MITRE nomenclature, refined into several variations (instances) at the procedural level and then deployed in virtual multiple architectures. URSID thus automates costly manual tasks and allows to have several instances of the same scenario on architectures with different OS, software or account configurations. URSID has been successfully tested in an academic cyber attack and defense training exercise as detailed in Section 10.3.2.

Extending The Boundaries and Exploring The Limits Of Blockchain Compression The long-term feasibility of blockchain technology is hindered by the inability of existing blockchain protocols to prune the consensus data leading to constantly growing storage and communication requirements. Kiayias et al. have proposed Non-Interactive-Proofs-of-Proof-of-Works (NIPoPoWs) as a mechanism to reduce the storage and communication complexity of blockchains to O(poly log(n)). However, their protocol is only resilient to an adversary that may control strictly less than a third of the total computational power, which

is a reduction from the security guaranteed by Bitcoin and other existing Proof-ofbased blockchains. In [15], we present an improvement to the Kiayias et al. proposal, which is resilient against an adversary that may control less than half of the total computational power while operating in O(poly log(n)) storage and communication complexity. Additionally, we present a novel proof that establishes a lower bound of O(log(n)) on the storage and communication complexity of any PoW-based blockchain protocol.

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

- **DGA (2021-2024)**

  Participants: Yufei Han, Pierre-François Gimenez, Vincent Raulin, Leopold Ouairy, Alexandre Sanchez, Valérie Viet Triem Tong.

  Vincent Raulin's PhD focuses on using machine learning approaches to boost malware detection/classification based on dynamic analysis traces by extracting feature representations with the knowledge of malware analysis experts. This representation aims at capturing the semantics of the program (i.e., what resources it accesses, what operations it performs on them) in a plateform-independent fashion, by replacing the implementation particularities (system call number 2) with higher-level operation (opening a file). This representation could notably provide semantic explanation of malware activity and deliver explainable malware detection/malware family classification.

8.2 Bilateral grants with industry

- **AMOSSYS:**

  Participants: Erwan Abgrall, Gilles Guette, Manuel Poisson, Valerie Viet Triem Tong.

  Manuel Poisson has started a thesis in collaboration with Amossys. Manuel Poisson is interested in identifying operational attack scenarios in an information system.

- **ANSSI:**

  Participants: Matthieu Baty, Guillaume Hiet, Frédéric Tronel, Pierre Wilke.

  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.

- **ANSSI:**

  Participants: Lucas Aubard, Gilles Guette, Ludovic Mé.

Lucas Aubard started his PhD in October 2022 in the context of a collaboration between Inria and the ANSSI. The objective of this thesis is to improve the existing knowledge on reassembly policies, to design mechanisms to automate IDS configuration and to improve the application of these policies within IDS/IPS to increase their detection capabilities in specific contexts such as cloud computing.

- **DGA:**

  Participants: Pierre-Victor Besson, Gilles Guette, Guillaume Piolle, Valérie Viet Triem Tong.

  Pierre-Victor Besson is financed by a DGA-PEC grant since October 2020. Pierre-Victor Besson works on the automatic generation of attack scenario to design deceptive honeynet.

- **DGA:**

  Participants: Fanny Dijoud, Michel Hurfin, Pierre-François Gimenez, Frederic Majorczyk.

  Fanny Dijoud PhD Thesis is funded by a DGA-PEC grant since November 2023. Fanny Dijoud works on system and network supervision through AI-based methods.

- **Malizen:**

  Participants: Romain Brisse, Jean-François Lalande.

  Romain Brisse's PdD thesis is financed by Malizen, an Inria start-up from the CIDRE team since January 2021. During the year 2023, Romain has developed a new recommendation system based on the recorded user's actions of blue teamers.

- **Hackuity:**

  Participants: Natan Talon, Gilles Guette, Yufei Han, Valérie Viet Triem Tong.

  Natan Talon started his PhD in October 2021 in the context of a collaboration with the company Hackuity. The main objective of this thesis is to be able to assess whether an information system is likely to be vulnerable to an attack. This attack may have been observed in the past or inferred automatically from other attacks.

- **DGA:**

  Participants: Pierre-François Gimenez, Yufei Han, Maxime Lanvin, Ludovic Mé.

  Maxime Lanvin is financed by the DGA through the Pôle d'Excellence Cyber (PEC) since October 2021. Maxime works on behavorial intrusion detection based on machine learning techniques. His work focuses on the analysis of time series to detect APT attacks.

- **DGA:**

Participants: Pierre-François Gimenez, Yufei Han, Ludovic Mé, Adrien Schoen.

Adrien Schoen is financed by the DGA though the Pôle d'Excellence Cyber (PEC) since October 2021. Adrien works on the generation of synthetic network dataset to better evaluate intrusion detection systems. This work is based on various deep learning models such as generative adversarial network and variational auto-encoder.

- **DGA:**

Participants: Yufei Han, Hélène Orsini, Valérie Viet Triem Tong.

Helene Orsini's PdD thesis is financed by DGA since October 2021. Her thesis project focuses on adversarially robust and interpretable machine learring pipeline for network intrusion detection systems. She will study how to automate the feature engineering phase to extract informative features from non-structured, categorical and imperfect security reports / logs. Furthermore, she will investigate how to make the machine learning pipeline resilient to intentional evading techniques in network intrusion behaviors.

9 Partnerships and cooperations

9.1 International initiatives

Associated team SecGen with CISPA We started, in 2023, the associated team "SecGen" with two professors at CISPA, Jilles Vreeken and Mario Fritz, on the subject of network traffic generation and network anomaly detection. Machine learning has been successfully applied to intrusion detection, but it needs training data. This training data generally comes from datasets, but their diversity is questionable, and their aging is problematic. Synthetic data generation is a solution to these problems. In the context of SecGen, we hosted a PhD student from CISPA, Joscha Cuppers, for 2 months, and a PhD student of CIDRE, Adrien Schoen, went to CISPA in 2023 for 2 months.

9.1.1 Visits to international teams

Research stays abroad Adrien Schoen stayed at CISPA from October 16th, 2023 to December 15th, 2023 in the team of Jilles Vreeken to work on the topic of generating temporal sequences networks flows. During this stay, he worked with Joscha Cüppers, PhD at CISPA. This visit has led to interesting scientific results that will be submitted to an international venue in 2024.

9.2 National initiatives

PEPR CyberSecurity project: DefMal (2022-2028)

Participants: Kevin Allix, Pierre-François Gimenez, Yufei Han, Jean-François Lalande, Valérie Viet Triem Tong.

PEPR DefMal is a collaborative ANR project involving CentraleSupélec, Rennes University, Lorraine University, Sorbonne Paris Nord University, CEA, CNRS, Inria and Eurecom. Malware is affecting government systems, critical infrastructures, businesses, and citizens alike, and regularly makes headlines in the press. Malware extorts money (ransomware), steals data (banking, medical), destroys information systems, or disrupts the operation of industrial systems. The fight against malware is a national and European security issue that requires scientific advances to design new responses and anticipate future

attack methods. The aim of the project DefMal is to study malicious programs, whether they are malware, ransomware, botnet, etc. The first objective is to develop new approaches to analyze malicious programs. This objective covers the three aspects of the fight against malware: (i) Understanding (ii) Detection and (iii) Forensics. The second objective of the project is the global understanding of the malware ecosystem (modes of organization, diffusion, etc.) in an interdisciplinary approach involving all the actors concerned.

PEPR Cybersecurity project: SecureEval(2022-2028)

Participants: Guillaume Hiet, Frédéric Tronel, Pierre Wilke.

The security assessment of digital systems relies on compliance and vulnerability analyses to provide recognized cybersecurity assurances. The SECUREVAL project of PEPR Cybersecurity aims to design new tools around new digital technologies to verify the absence of hardware and software vulnerabilities and achieve the required compliance proofs. These developments are based on a double approach, first theoretical and founded on the French school of symbolic reasoning, then applied and anchored in the practice of tool development and security assessment techniques. In addition, by exploring new techniques for security assessments, this project will also allow France to remain at the top of the world in assessment capabilities by anticipating the evolution of international certification schemes. Within this project's framework, our contribution concerns tasks 4.4 Formal analysis and models at the software-hardware boundary (led by Guillaume Hiet) and 3.2 Vulnerability analysis tools in binary codes (led by Frédéric Tronel). Two Ph.D. and one postdoc funded by this project will start between 2023 and 2025.

PEPR Cybersecurity project: SuperviZ (2022-2028)

Participants: Pierre-François Gimenez, Gilles Guette, Yufei Han, Ludovic Mé.

PEPR SuperviZ is a collaborative ANR project involving CentraleSupélec, Eurecom, Institut Mines-Télécom, Institut Polytechnique de Grenoble, Rennes University, Lorraine University, CEA, CNRS and Inria. The digitalization of all infrastructures makes it almost impossible today to secure all systems *a priori*, as it is too complex and too expensive. Supervision seeks to reinforce preventive security mechanisms and to compensate for their inadequacies. Supervision is fundamental in the general context of enterprise systems and networks, and is just as important for the security of cyber-physical systems. Indeed, with the ever growing number of connections between objects, the attack surface of systems has become frighteningly wide. This makes security even more difficult to implement. The increase in the number of components to be monitored, as well as the growing heterogeneity of the capacity of these objects in terms of communication, storage and computation, makes security supervision more complex.

PEPR Cybersecurity project: REV (2023-2028)

Participants: Pierre-François Gimenez.

PEPR REV is a project about vulnerability research and exploitation. A notable characteristic of complex targets is that they can generally no longer be attacked using a single technique or exploiting a single vulnerability, due to the deployment of numerous protections. For this reason, the REV project is tackling this problematic at multiple levels by addressing all layers, hardware, software and communication interfaces (web and IoT). In this purpose, one of the project's objectives is to combine several tools and approaches simultaneously: for example, memory analysis will benefit from advances in hardware attacks, and will be used to develop exploits. This broad-spectrum analysis is fundamental today: as an illustration, hardware attacks can be combined with software attacks, software attacks can be based on

weaknesses in the micro-architecture or require advanced network interactions. Moreover, the impact of attacks and exploits nowadays goes far beyond malicious use, allowing for instance to forensically investigate complex systems such as smartphones. The question also arises from an ethical and legal point of view, and this is a major societal issue: to which extent is it possible to use these techniques, in particular for law enforcement, from an ethical or legal point of view. What is the possible use of these attacks, when should they be corrected ("responsible disclosure") or used, and in what legal framework?

ANR Project: Byblos (2021-2025).

Participants: Emmanuelle Anceaume.

Byblos is a collaborative ANR project involving Rennes university and 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.

ANR Project: BC4SSi (2023-2027)

Participants: Emmanuelle Anceaume.

BC4SSI is a JCJC ANR project led by Romaric Ludinard (SOTERN), involving the SOTERN and CIDRE research teams. Self-sovereign identities (SSI) are digital identities that are managed in a decentralized manner. This technology allows users to self-manage their digital identities without depending on third-party providers to store and centrally manage the data, including the creation of new identities. Implementing SSI requires a lot of care since identities are more than simple identifiers: they need to be checked by the service provider via, for instance, verifiable claims. Such requirements make blockchain technology a prime candidate for deploying SSI and storing verifiable claims. BC4SSI aims at studying the weakest synchrony assumptions enabling SSI deployment in a public Blockchain. Among the different existing challenges, BC4SSI will address the following scientific locks: alternatives to PoW security proofs, lightweight replication, scalability and energy consumption.

CominLabs project: Priceless (2021-2025)

Participants: Emmanuelle Anceaume.

Priceless is a collaborative CominLabs project involving Rennes University with IRISA (CIDRE and WIDE research teams), and IODE (Institut de l'ouest: droit et Europe), and Nantes university (GDD research team). Promoters of blockchain-based systems such as cryptocurrencies have often advocated for the anonymity these provide as a pledge of privacy protection, and blockchains have consequently been envisioned as a way to safely and securely store data. Unfortunately, the decentralized, fully-replicated and unalterable nature of the blockchain clashes with both French and European legal requirements on the storage of personal data, on several aspects such as the right of rectification and the preservation of consent. This project aims to establish a cross-disciplinary partnership between Computer Science and Law researchers to understand and address the legal and technical challenges associated with data storage in a blockchain context.

ANR Project: TrustGW (2021-2025).

Participants: Guillaume Hiet, Frédéric Tronel, Pierre Wilke.

In the ANR TrustGW project, we consider a system composed of IoT objects connected to a gateway. This gateway is, in turn, connected to one or more cloud servers. The architecture of the gateway, which is at the heart of the project, is heterogeneous (software-hardware), composed of a baseband processor, an application processor, and hardware accelerators implemented on an FPGA. A hypervisor allows sharing these resources and allocating them to different virtual machines. TrustGW is a collaborative project between the ARCAD team from Lab-STICC, the ASIC team from IETR, and the CIDRE team from IRISA. The project addresses three main challenges: (1) to define a heterogeneous, dynamically configurable and trusted gateway architecture, (2) to propose a trusted hypervisor allowing to deploy virtual machines on a heterogeneous software-hardware architecture with virtualization of the whole resources and (3) to secure the applications running on the gateway. Within this project's framework, the CIDRE team's contribution focuses mainly on the last challenge, particularly through the PhD of Lionel Hemmerlé (2022-2025). Guillaume Hiet is the director of this PhD, co-supervised by Frédéric Tronel, Pierre Wilke and Jean-Christophe Prévotet. We will also explore hardware-assisted Dynamic Information Flow Tracking approaches for hybrid applications, which offload part of their computation to an FPGA.

CominLabs project: SCRATCHS (2021-2024)

Participants: Pierre Wilke, Guillaume Hiet.

SCRATCHS is a collaboration between researchers in the fields of formal methods (EPICURE, Inria Rennes), security (CIDRE, CentraleSupélec Rennes), and hardware design (Lab-STICC). Our goal is to co-design a RISC-V processor and a compiler toolchain to ensure by construction that a security-sensitive code is immune to timing side-channel attacks while running at maximal speed. We claim that a co-design is essential for end-to-end security: cooperation between the compiler and hardware is necessary to avoid time leaks due to the micro-architecture with minimal overhead. In the context of this project, Guillaume Hiet is the director of the Ph.D. of Jean-Loup Houdot, co-supervised by Pierre Wilke and Frederic Besson, on security-enhancing compilation against side-channel attacks.

9.3 Regional initiatives

Smart and Secure Room project

Participants: Jean-Francois Lalande, Anatolii Khalin.

Anatolii Khalin started in November as a post-doctoral researcher in the team, co-supervized with the AUT team from IETR. His work focuses on detecting cyberattacks that could target a cyberphysical system. In particular, smart buildings taking autonomous decisions about energy production and consumption could be the target of an attacker. We plan to design new estimators used to predict the different physical measures of a smart building. These estimators could be used to raise alerts when a deviation from the expected prediction is detected, for example, because of a compromised device in the building.

10 Dissemination

Participants: Matthieu Baty, Christophe Bidan, Pierre-Victor Besson, Romain Brisse, Pierre-François Gimenez, Gilles Guette, Yufei Han, Guillaume Hiet, Michel Hurfin, Jean-François Lalande, Ludovic Me, Helene Orsini, Alexandre Sanchez, Natan Talon, Frédéric Tronel, Valérie Viet Triem Tong.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

General chair, scientific chair Guillaume Hiet was the General Chair of the SILM 2023 workshop, co-localized with IEEE Euro S&P

Member of the organizing committees Ludovic Mé was a member of the organizing committee of JSI 2023 (Journées Scientifiques Inria, Bordeaux, August 30th to September 1rst) and of the 8th Franco-Japanese Cybersecurity Workshop (Bordeaux, November 29th to December 1st, 2023). He also served the steering committee of RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information).

10.1.2 Scientific events: selection

Member of the conference program committees

- Ludovic Mé served the Scientific Committee of FIC 2023 (Forum International de la Cybersécurité) and the Program Committee of JSI 2022 (Journées Scientifiques Inria).
- Gilles Guette served the Scientific Committee of ICISSP 2023 (International Conference on Information Systems Security and Privacy).
- Jean-Francois Lalande was part of the program committees of the conferences EICC 2023, SSTIC 2023 and the workshops IWCC 2023 and CUING 2023.
- Guillaume Hiet was part of the program committees of the following conferences: SILM 2023, EAI SecureComm 2023, NSS 2023, VERDI@DSN 2023.

Reviewer Michel Hurfin served as reviewer for the conference Sirocco 2023.

Member of the editorial boards Jean-Francois Lalande was part of the editorial board of IARIA International Journal on Advances in Security.

Reviewer - reviewing activities

- Jean-Francois Lalande served as reviewer for IEEE Transactions on Reliability.
- Michel Hurfin served as reviewer for ARIMA (Revue Africaine de Recherche en Informatique et Mathématiques Appliquées.)
- Guillaume Hiet served as an external reviewer for the book Guide to Software Verification with Frama-C.

10.1.3 Invited talks

Ludovic Mé was panelist for a round table organized by EDIH Bretagne and dedicated to the role of research in such a program (Nov. 2023, 22nd).

Ludovic Mé gave an invited talk on offensive aspects of AI at the CESIN congress (Dec. 2023, 6th).

Pierre-François Gimenez was a panelist for a round table at the event "La Cyber au rendez-vous de l'IA de confiance" organized by the PTCC at Campus Cyber (Jun. 2023, 20th)

10.1.4 Scientific expertise

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” of the GDR “sécurité” ;
- the technical committee of the PTCC (Programme de Transfert au Campus Cyber).

Guillaume Hiet is the co-chair of the Systems, Software and Network Security working group of the GDR Sécurité Informatique.

Jean-Francois Lalande was a reviewer for the PhD grants of Normandie University.

Valérie Viet Triem Tong was vice-President of the ANR project evaluation committee: Specific Topics in Artificial Intelligence (TSIA) CyberSecurity

Valérie Viet Triem Tong chaired the recruitment committee (selection and audition) for the Nancy researchers’ recruitment process (CRCN and ISFP).

10.1.5 Research administration

- Ludovic Mé is deputy scientific director of Inria, in charge of the cyber security area.
- Valérie Viet Triem Tong was in charge of cybersecurity activities in the CominLabs Laboratory of Excellence, which involves research teams from Brittany to Nantes.

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

Several 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,

- Christophe Bidan is the head of the Rennes campus of CentraleSupélec;
- Gilles Guette is the director of corporate relations at ESIR (until august 2023);
- Jean-François Lalande is responsible of the major program dedicated to information systems security and the special track Infosec of CentraleSupélec engineering education; He is also involved in the organization committee of EUR CyberSchool and in the computer science master degree (SIF and Cyber tracks).
- 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 2022.

The teaching duties are summed up in table 1.

10.2.2 Supervision(Ongoing Phd thesis)

PhD:

- Nicolas Bellec, Security in real-time embedded systems, defended May 2023, supervised by Isabelle Puaut from PACAP (50%), Guillaume Hiet (25%) and Frédéric Tronel (25%).

	Licence level	Master level	CS†	Univ. Rennes	Initial education	Continuing education	2021 -2022
Emmanuelle Anceaume		✔	✔	✔	✔		20h
Christophe Bidan	✔	✔	✔	✔	✔	✔	-h
Pierre-François Gimenez		✔	✔		✔	✔	120h
Gilles Guette	✔	✔		✔	✔		460h
Guillaume Hiet	✔	✔	✔		✔	✔	266h
Michel Hurfin		✔	✔	✔	✔		6h
Jean-François Lalande	✔	✔	✔	✔	✔	✔	110† +14h*
Guillaume Piolle	✔	✔	✔	✔	✔	✔	186h
Ruben Salvador	✔	✔	✔	✔	✔	✔	250h
Frédéric Tronel	✔	✔	✔	✔	✔	✔	287h
Valérie Viet Triem Tong	✔	✔	✔	✔	✔	✔	105h† 105h*
Pierre Wilke	✔	✔	✔		✔	✔	120h

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

PhD in progress:

- Pierre Lledo, On intrusion detection, started December 2023, supervised by Jean-François Lalande (50%) and Frederic Majorczyk (50%).
- Lucas Aubard, Ambiguïtés de recouvrement de données dans les protocoles d'Internet et supervision reseau, started October 2022, supervised by Pierre Chifflier (25%), Gilles Guette (25%), Johan Mazel (25%) and Ludovic Mé (25%).
- Matthieu Baty, 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%).
- Pierre-Victor Besson, CHOUCHEN : Complete HOneynet with User Copycat on Hypervisor with Emulated Network, started November 2020, supervised by Valérie Viet Triem Tong (25%), Gilles Guette (25%), Guillaume Piolle (25%) and Erwan Abgrall (25%).
- Romain Brisse, Exploration recommendations for the investigation of security incidents, started december 2020, co-supervised with Frédéric Majorczyk (50%) and Simon Boche (50%).
- Séverine Delaplace, Analyzing Android malware communicating with a remote server, started december 2020, supervised by Jean-Francois Lalande (25%), Jacques Klein (25%, University of Luxembourg), Pierre Wilke (25%) and Kévin Allix (25%, University of Luxembourg) (International co-advised thesis). Ended in december 2023.
- Fanny Dijoud, Détection d'intrusions au niveau système d'informations : détection d'anomalies par traitement IA dans des graphes dynamiques hétérogènes représentant l'activité du système, started november 2023, supervised by Michel Hurfin (25%), Pierre-François Gimenez (25%), Frédéric Majorczyk (25%) et Barbara Pilastre (25%, DGA).
- Lionel Hemmerlé, Conception et implémentation d'un langage dédié à l'introspection de machine virtuelle, started November 2022, supervised by Guillaume Hiet (25%), Pierre Wilke (25%), Frédéric Tronel (25%), and Jean-Christophe Prévotet (25%)

- Maxime Lanvin, Tacking efficiently the time into account when using machine learning techniques for the analysis of heterogeneous log files, started October 2021, supervised by Christophe Bidan (25%), Ludovic Mé (25%), Pierre-François Gimenez (25%), and Eric Totel (25%).
- Jean-Marie Mineau, Android Malware Manipulation for Improved Investigations, started November 2022, supervised by Jean-Francois Lalande (75%), Valérie Viet Triem Tong (25%).
- Hélène Orsini, IA based supervision, started October 2021, supervised by Yufei Han (50%) Valérie Viet Triem Tong (25%), David Lubicz (25%)
- Manuel Poisson, Évaluation automatisée du niveau de sécurité d'un système d'information, started March 2023, supervised by Valérie Viet Triem Tong (25%), Gilles Guette (25%), Frédéric Guihéry (25%) and Damien Crémilleux (25%).
- Vincent Raulin, IA-based classification of malware, started October 2021, supervised by Valérie Viet Triem Tong (25%), Yufei Han (25%), Pierre-François Gimenez (50%).
- Adrien Schoen, Generation of realistic activities for Intrusion Detection Systems evaluation, started October 2021, supervised by Ludovic Mé (25%), Gregory Blanc (25%),Yufei Han (25%), and Frédéric Majorczyk (25%).
- Natan Talon, Rejeu et apprentissage de scénarios d'attaques, started December 2021, supervised by Mathieu Jaume (25%), Gilles Guette (25%), Yufei Han (25%) and Valérie Viet Triem Tong (25%).
- Grégor Quetel, Détection d'anomalie et création d'une sonde d'inférence sémantique, started Octobre 2023, supervised by Pierre-François Gimenez (25%), Eric Alata (25%), Thomas Robert (25%) and Laurent Pautet (25%).

10.2.3 Juries

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

- Grégoire Menguy, *Black-box code analysis for reverse engineering through constraint acquisition and program synthesis*, Université Paris-Saclay.
- Guillaume Delorme, *Aide à la gestion de l'impact des stratégies IT sur la maîtrise du risque réglementaire*, Université Jean Moulin Lyon 3.

Jean-Francois Lalande was

- a reviewer of the PhD thesis of Florent Galtier, Université Fédérale Toulouse Midi-Pyrénées, the 17th of february 2023: *Sécurité des réseaux sans-fil courte et longue portée basée sur des mécanismes de monitoring de la couche physique.*

Guillaume Hiet was

- a reviewer of the PhD thesis of Soline Ducousso, Université Grenoble Alpes, *Moving code analysis from safety to security: attacker model*

Valérie Viet Triem Tong was

- a reviewer of the PhD thesis of Gregoire Menguy, *Black-box code analysis for reverse engineering through constraint acquisition and program synthesis*, Université Paris-Saclay.
- a member of the PhD committee of Tristan Benoit, *Cartographie des programmes et de leurs interrelations*, Université Lorraine.

Pierre-François Gimenez was

- a member of the PhD committe of Mohamed El Bouazzati, *A Lightweight Host-based Intrusion Detection System using a Hardware-Assisted Monitor to detect Wireless Attacks Targeting Constrained IoT Devices*, Lab-STICC, on December 12th, 2023.

10.3 Popularization

On the Youtube page of the CIDRE team, many scientific talks are published. Most of them are recordings from the biweekly CIDRE seminars organized by Pierre-François Gimenez. In 2023, the channel reached 121 subscribers, and 48 videos were published, with about 5812 views.

10.3.1 Articles and contents

Valérie Viet Triem Tong and Jean-Louis Lanet (previous member of CIDRE and now retired) published in 2023 an article ”Virus numériques” in La Recherche, a monthly French language popular science magazine.

10.3.2 Education

- Jean-François Lalande has participated to the program “1 scientifique - 1 classe: Chiche !” in Lycée Saint Louis of Saumur, for 4 classes in 2023.
- Valérie Viet Triem Tong has participated to the program “1 scientifique - 1 classe: Chiche !” in Lycée Simone Veil at Liffré for 4 classes in 2023.
- Hélène Orsini has participated to the program ”L codent L créent” in Collège des Gayeulles of Rennes for 12 students, in Spring 2023
- Valérie Viet Triem Tong has participated to the program “Immersion Science” presenting cybersecurity and the world of research to high school students in May 2023.
- In 2023, we proposed a Cybersecurity Exercise for the attendees of the Spring Research School organized by the EUR CyberSchool. This training was more than just a traditional Capture-the-Flag (CTF) challenge conceived to train security teams to attack an IT infrastructure. The CERBERE (Red and Blue team Entertainment, REproducibility) exercise is composed of two parts: a first CTF-type exercise in which a player must attack an infrastructure that has been generated in order to guarantee its uniqueness. During this exercise, the player's actions are monitored from three angles: their pentesting activities performed in their web browser, their network activity, and their activity on host operating systems. This data allows a second hunting phase in which a player must reconstruct all the stages of an attack scenario by exploring the logs. In order to adapt to the skills of the players, the CERBERE exercise is derived into several instances for which we control the difficulty. This exercise was built using our tool URSID [10]. The data produced during this exercise helps Romain Brisse, Helene Orsini and Natan Talon's PhD projects. The whole outputs of this exercise have been published in [9].
- Gilles Guette has participated to the program “À la découverte de la recherche” where he presented what is research to Emile Zola college students, for 3 classes, in 2023.

10.3.3 Interventions

- Valérie Viet Triem Tong gave in 2023 an hybrid talk at CentraleSupelec and published online on LinkedIn Café des Sciences: Attaques avancées sur les systèmes informatiques.
- Jean-Francois Lalande was the animator of “Tables rondes métiers de la Cybersécurité" with 10 participants of the industry, the 18th december 2023 at CentraleSupélec.

11 Scientific production

11.1 Major publications

[1] S. Aonzo, Y. Han, A. Mantovani and D. Balzarotti. ‘Humans vs. Machines in Malware Classification’. In: *Proceedings of the 23nd Usenix Security Symposium (USENIX Security '23)*. USENIX Security 2023 - 32nd Usenix Security Symposium. 1145-1162. Anaheim (CA), United States, 2023. URL: https://hal.science/hal-04321950.

[2] M. Baty, P. Wilke, G. Hiet, A. Fontaine and A. Trieu. 'A generic framework to develop and verify security mechanisms at the microarchitectural level: application to control-flow integrity'. In: CSF 2023 - 36th IEEE Computer Security Foundations Symposium. Dubrovnik, France: IEEE, 9th July 2023, pp. 1–16. URL: https://inria.hal.science/hal-04118645.

[3] S. Dambra, Y. Han, S. Aonzo, P. Kotzias, A. Vitale, J. Caballero, D. Balzarotti and L. Bilge. 'Decoding the Secrets of Machine Learning in Windows Malware Classification: A Deep Dive into Datasets, Features, and Model Performance'. In: CCS 2023 - 30th ACM Conference on Computer and Communications Security. Copenhagen, Denmark: ACM, 28th Aug. 2023, pp. 60–74. DOI: 10.1145/3576915.3616589. URL: https://hal.science/hal-04321280.

[4] M. Lanvin, P.-F. Gimenez, Y. Han, F. Majorczyk, L. Mé and E. Totel. 'Towards Understanding Alerts raised by Unsupervised Network Intrusion Detection Systems'. In: *RAID'23: Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses*. RAID 2023: The 26th International Symposium on Research in Attacks, Intrusions and Defenses. Hong Kong China, France: ACM; ACM, Oct. 2023, pp. 135–150. DOI: 10.1145/3607199.3607247. URL: https://hal.science/hal-04172470.

11.2 Publications of the year

International journals

[5] F. Castella, B. Sericola, E. Anceaume and Y. Mocquard. 'Continuous-Time Stochastic Analysis of Rumor Spreading with Multiple Operations'. In: *Methodology and Computing in Applied Probability* 25.4 (23rd Oct. 2023), p. 82. DOI: 10.1007/s11009-023-10058-7. URL: https://cnrs.hal.science/hal-04255487.

[6] P. Graux, J.-F. Lalande, V. Viet Triem Tong and P. Wilke. 'OATs'inside : Retrieving Object Behaviors From Native-based Obfuscated Android Applications'. In: *Digital Threats: Research and Practice* 4.2 (10th Aug. 2023), pp. 1–27. DOI: 10.1145/3584975. URL: https://centralesupelec.hal.science/hal-04279351.

International peer-reviewed conferences

[7] S. Aonzo, Y. Han, A. Mantovani and D. Balzarotti. 'Humans vs. Machines in Malware Classification'. In: *Proceedings of the 23nd Usenix Security Symposium (USENIX Security '23)*. USENIX Security 2023 - 32nd Usenix Security Symposium. 1145-1162. Anaheim (CA), United States, 2023. URL: https://hal.science/hal-04321950.

[8] M. Baty, P. Wilke, G. Hiet, A. Fontaine and A. Trieu. 'A generic framework to develop and verify security mechanisms at the microarchitectural level: application to control-flow integrity'. In: CSF 2023 - 36th IEEE Computer Security Foundations Symposium. Dubrovnik, France: IEEE, 9th July 2023, pp. 1–16. URL: https://inria.hal.science/hal-04118645.

[9] P.-V. Besson, R. Brisse, H. Orsini, N. Talon, J.-F. Lalande, F. Majorczyk, A. Sanchez and V. Viet Triem Tong. 'CERBERE: Cybersecurity Exercise for Red and Blue team Entertainment, REproducibility'. In: CyberHunt 2023 - 6th Annual Workshop on Cyber Threat Intelligence and Hunting. Sorrento, Italy: IEEE Computer Society, 2023, pp. 2980–2988. DOI: 10.1109/BigData59044.2023.10386953. URL: https://centralesupelec.hal.science/hal-04285565.

[10] P.-V. Besson, V. Viet Triem Tong, G. Guette, G. Piolle and E. Abgrall. 'URSID: Automatically Refining a Single Attack Scenario into Multiple Cyber Range Architectures'. In: FPS 2023 - 16th International Symposium on Foundations & Practice of Security. Bordeaux, France, 11th Dec. 2023, pp. 1–16. URL: https://inria.hal.science/hal-04317073.

[11] R. Brisse, S. Boche, F. Majorczyk and J.-F. Lalande. 'MIMIR: Modelling user Intentions with Markov chains for Intention Recommendations'. In: *Advances in Digital Forensics*. ICDF 2024 - Twentieth Annual IFIP WG 11.9 International Conference on Digital Forensics. New Delhi, India: IFIP, 2024, pp. 1–23. URL: https://centralesupelec.hal.science/hal-04440805.

[12] S. Dambra, Y. Han, S. Aonzo, P. Kotzias, A. Vitale, J. Caballero, D. Balzarotti and L. Bilge. 'Decoding the Secrets of Machine Learning in Windows Malware Classification: A Deep Dive into Datasets, Features, and Model Performance'. In: CCS 2023 - 30th ACM Conference on Computer and Communications Security. Copenhagen, Denmark: ACM, 28th Aug. 2023, pp. 60–74. DOI: 10.1145/3576915.3616589. URL: https://hal.science/hal-04321280.

[13] N. Gaudin, J.-L. Hatchikian-Houdot, F. Besson, P. Cotret, G. Guy, G. Hiet, V. Lapotre and P. Wilke. 'Work in Progress: Thwarting Timing Attacks in Microcontrollers using Fine-grained Hardware Protections'. In: *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Delft, Netherlands, 3rd July 2023, pp. 1–7. URL: https://hal.science/hal-04155139.

[14] J. Guillaume, M. Pelcat, A. Nafkha and R. Salvador. 'Attacking at non-harmonic frequencies in screaming-channel attacks'. In: *Lecture Notes in Computer Science (LNCS)*. 22nd Smart Card Research and Advanced Application Conference (CARDIS 2023). Lecture Notes in Computer Science (LNCS). Amsterdam, Netherlands: Springer, 15th Nov. 2023, pp. 1–20. URL: https://inria.hal.science/hal-04309083.

[15] A. Jain, E. Anceaume and S. Gujar. 'Extending The Boundaries and Exploring The Limits Of Blockchain Compression'. In: SRDS 2023 - 42nd International Symposium on Reliable Distributed Systems. Marrackech, Morocco, 27th Sept. 2023, pp. 1–11. URL: https://cnrs.hal.science/hal-04166932.

[16] S. Kilian, E. Anceaume and B. Sericola. 'Stochastic analysis of rumor spreading with multiple pull operations in presence of non-cooperative nodes'. In: *The 27th International Conference on Analytical & Stochastic Modelling Techniques & Applications (ASMTA 2023)*. ASMTA 2023 - 27th International Conference on Analytical & Stochastic Modelling Techniques & Applications. Florence, Italy, 20th June 2023, pp. 1–15. URL: https://cnrs.hal.science/hal-04166945.

[17] M. Lanvin, P.-F. Gimenez, Y. Han, F. Majorczyk, L. Mé and E. Totel. 'Errors in the CICIDS2017 dataset and the significant differences in detection performances it makes'. In: *Lecture Notes in Computer Science*. CRiSIS 2022 - 17th International Conference on Risks and Security of Internet and Systems. Vol. 13857. Sousse, Tunisia: Springer, 14th May 2023, pp. 18–33. DOI: 10.1007/978-3-031-31108-6_2. URL: https://hal.science/hal-03775466.

[18] M. Lanvin, P.-F. Gimenez, Y. Han, F. Majorczyk, L. Mé and E. Totel. 'Towards understanding alerts raised by unsupervised network intrusion detection systems'. In: *RAID'23: Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses*. The 26th International Symposium on Research in Attacks, Intrusions and Defenses (RAID). Hong Kong China, France: ACM, Oct. 2023, pp. 135–150. DOI: 10.1145/3607199.3607247. URL: https://hal.science/hal-04172470.

[19] S. Lee, R. Salvador, A. Kritikakou, O. Sentieys, J. Galizzi and E. Casseau. 'High-Level Synthesis-Based On-board Payload Data Processing considering the Roofline Model'. In: *EDHPC 2023 proceedings*. EDHPC 2023 - European Data Handling & Data Processing Conference. Juan-Les-Pins, France, 2nd Oct. 2023, pp. 1–10. URL: https://inria.hal.science/hal-04294305.

[20] M. Naseri, Y. Han and E. de Cristofaro. 'BadVFL: Backdoor Attacks in Vertical Federated Learning'. In: SP 2024 - IEEE Symposium on Security and Privacy. San Francisco, United States, 2024, pp. 1–8. URL: https://hal.science/hal-04321905.

[21] M. Poisson, V. Viet Triem Tong, G. Guette, E. Abgrall, F. Guihéry and D. Crémilleux. 'Unveiling stealth attack paths in Windows Environments using AWARE'. In: *2023 7th Cyber Security in Networking Conference (CSNet)*. CSNet 2023 - 7th Cyber Security in Networking Conference. Montreal, Canada, 16th Oct. 2023, pp. 1–7. URL: https://inria.hal.science/hal-04163780.

[22] M. Poisson, V. Viet Triem Tong, G. Guette, F. Guihéry and D. Crémilleux. 'CVE representation to build attack positions graphs: CAPG format'. In: *2023 6th Annual Workshop on Cyber Threat Intelligence and Hunting (CyberHunt)*. CyberHunt 2023 - 6th Annual Workshop on Cyber Threat Intelligence and Hunting. Sorrento, Italy, 20th Dec. 2023, pp. 1–5. URL: https://inria.hal.science/hal-04317023.

[23] V. Raulin, P.-F. Gimenez, Y. Han and V. Viet Triem Tong. 'BAGUETTE: Hunting for Evidence of Malicious Behavior in Dynamic Analysis Reports'. In: SECRYPT 2023 - 20th International conference on security and cryptography. Rome, Italy, 16th June 2023, pp. 1–8. URL: https://hal.science/hal-04102144.

[24] N. Sourbier, J. Bonnot, K. Desnos, F. Majorczyk, O. Gesny, T. Guyet and M. Pelcat. 'Imbalanced Classification with TPG Genetic Programming: Impact of Problem Imbalance and Selection Mechanisms'. In: GECCO 2022 - Genetic and Evolutionary Computation Conference. GECCO '22: Proceedings of the Genetic and Evolutionary Computation Conference Companion. Boston, United States, 14th June 2023, pp. 1–4. DOI: 10.1145/3520304.3529008. URL: https://hal.science/hal-03699228.

National peer-reviewed Conferences

[25] L. Aubard, J. Mazel, G. Guette, P. Chifflier, O. Levillain, G. Blanc and L. Mé. 'Modélisation et test des ambiguïtés de recouvrement de données pour l'obtention des politiques de ré-assemblage dans les protocoles réseaux'. In: *RESSI 2023 - Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*. RESSI 2023 - Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information. Neuvy-sur-Barangeon, France, 10th May 2023, pp. 1–3. URL: https://hal.science/hal-04165396.

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

[26] Y. Amoussou-Guenou, E. Anceaume, E. Bertin, A. D. Pozzo and A. Küpper, eds. *Proceedings of the 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) - 2023*. IEEE, 2023. DOI: 10.1109/BRAINS59668.2023. URL: https://hal.science/hal-04306801.

11.3 Cited publications

[27] T. Bourgeat, C. Pit-Claudel, A. Chlipala and Arvind. 'The essence of Bluespec: a core language for rule-based hardware design'. In: *Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation*. PLDI 2020. London, UK: Association for Computing Machinery, 2020, pp. 243–257. DOI: 10.1145/3385412.3385965. URL: https://doi.org/10.1145/3385412.3385965.