RESEARCH CENTRE

Rennes - Bretagne Atlantique

IN PARTNERSHIP WITH:

CNRS, Université Rennes 1, CentraleSupélec

2021

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]
- Lily Blanleuil [Centrale-Supélec, Researcher, from Oct 2021]
- Yufei Han [Inria, Advanced Research Position, from Feb 2021]
- Michel Hurfin [Inria, Researcher, HDR]
- Ludovic Mé [Inria, Advanced Research Position, HDR]
- Salwa Souaf [Centrale-Supélec, Researcher, until Nov 2021]

Faculty Members

- Valérie Viet Triem Tong [Team leader, Centrale-Supélec, Professor, HDR]
- Christophe Bidan [Centrale-Supélec, Professor, HDR]
- Pierre Francois Gimenez [Centrale-Supélec, Chair]
- Gilles Guette [Univ de Rennes I, Associate Professor]
- Guillaume Hiet [Centrale-Supélec, Associate Professor, HDR]
- Jean-Francois Lalande [Centrale-Supélec, Professor, HDR]
- Guillaume Piolle [Centrale-Supélec, Associate Professor]
- Frédéric Tronel [Centrale-Supélec, Associate Professor]
- Pierre Wilke [Centrale-Supélec, Associate Professor]

PhD Students

- Matthieu Baty [Inria]
- Aimad Berady [Ministère des armées, until Nov 2021]
- Pierre Victor Besson [Centrale-Supélec]
- Romain Brisse [Centrale-Supélec]
- Tomas Javier Concepcion Miranda [Centrale-Supélec]
- Severine Delaplace [Inria]
- Aimen Djari [CEA]
- Mathieu Escouteloup [Inria, until Sep 2021]
- Benoit Fournier [Univ de Rennes I, until Jul 2021]
- Cyprien Gottstein [Orange Labs, CIFRE]
- Cedric Herzog [Inria]
- Maxime Lanvin [Centrale-Supélec, from Oct 2021]
- Helene Orsini [Centrale-Supélec, from Oct 2021]
- Vincent Raulin [Inria, from Oct 2021]
- Adrien Schoen [Inria, from Oct 2021]
- Natan Talon [Hackuity, from Dec 2021]

Technical Staff

- Mohamed Alsamman [Inria, Engineer, until Jun 2021]
- Ludovic Claudepierre [Univ de Rennes I, Engineer, until Nov 2021]
- Pascal Greliche [Centrale-Supélec, Engineer, from Apr 2021]
- Leopold Ouairy [Inria, Engineer, until Nov 2021]

Interns and Apprentices

- Erwan Fasquel [Centrale-Supélec, from Feb 2021 until Jul 2021]
- Damien Gourbeyre [Centrale-Supélec, from May 2021 until Aug 2021]
- Pierre Jamelot [Inria, from May 2021 until Jun 2021]
- Maxime Lanvin [Inria, from Apr 2021 until Aug 2021]
- Benjamin Loison [Inria, from Jun 2021 until Jul 2021]
- Sergio Nobrega Gonçalves [Centrale-Supélec, until Mar 2021]
- Sebastien Poeydomenge [Univ de Rennes I, from Mar 2021 until Aug 2021]
- Vincent Raulin [Centrale-Supélec, from Mar 2021 until Sep 2021]
- Thibault Reynaldo [CNRS, from Mar 2021 until Aug 2021]
- Adrien Schoen [Centrale-Supélec, from Feb 2021 until Jul 2021]

Administrative Assistant

- Lydie Mabil [Inria]

External Collaborators

- Erwan Abgrall [Ministère des armées, from Sep 2021]
- Frédéric Majorczyk [DGA, until Aug 2021]

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 Cidre 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 New software and platforms

The new software are detailed in the next section.

5.1 New software

5.1.1 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 2021, 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

Contact: Valerie Viet Triem Tong

Participants: Pierre Wilke, Valerie Viet Triem Tong, Frédéric Tronel, Alexandre Sanchez, Jean-François Lalande, Laurent Georget, Guillaume Hiet, Christophe Hauser, Radoniaina Andriatsimandefitra Ratsisahan

Partner: CentraleSupélec

5.1.2 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

Release Contributions: - Increase of the speed of the static analysis - New language for targeting the suspicious code - New strategy for discovering the GUI using the Manifest and the layout files - Visualization of the bytecode events on a new timeline - Integration tests have been created

News of the Year: In 2021, we have created integration tests, corrected a large number of bugs and improved the visualization of the bytecode. We continue to migrate AndroBlare on more recent versions of Android.

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, Valerie Viet Triem Tong, Pierre Wilke

Contact: Jean-François Lalande

Partners: CentraleSupélec, Insa Centre Val-de-Loire

5.1.3 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: The code has been released using an open source license.

Publication: hal-02877815

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

Contact: Pierre Graux

5.1.4 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

5.1.5 TEMPO

Name: The Evasive Malware PlatfOrm

Keyword: Malware

Functional Description: This platform enables reseachers to label Windows malware and download a list of evasive samples.

URL: https://tempo.irisa.fr

Contact: Cédric Herzog

5.1.6 GUI-Mimic

Keywords: Malware, Software testing

Functional Description: GUI-Mimic is a software that automates the use of graphical software through short recorded sequences. Indeed, there is no tool that allows to easily generate varied and randomized sequences that stimulate many components of the same software. GUI-Mimic was developed for malware analysis.

URL: https://gitlab.inria.fr/vraulin/GUI-Mimic

Publication: hal-03449827

Contact: Vincent Raulin

6 New results

6.1 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 the 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: Mathieu Escouteloup, Romain Brisse, Ludovic Claudepierre, Yufei Han, Jean-François Lalande, Valérie Viet Triem Tong.

Privacy Stealing Attacks Against Inductive Graph Neural Networks. Graph Neural Networks (GNNs) are a variant of machine learning techniques that can be applied to exploit topological information contained by graph-structured data. In [1], we unveil how these graph learning models are prone to the privacy-motivated attacks. Such privacy-stealing efforts can clone the decision behaviors of the target graph learning models via merely querying the output of the models. Such privacy stealing efforts can facilitate downstream data privacy reserve engineering attacks as a stepping stone, like membership inference and model inversion attacks.

Our study defines a threat model to characterize an adversary's background knowledge along two dimensions. We establishes six different attack scenarios based on this threat model. Finally we extensively evaluate our proposition on a six benchmark graph datasets and demonstrate the efficacy of these attacks. Interestingly, we unveil that the model privacy stealing can be achived by simply querying the classification output of the target graph learning models. It indicates that it is paramount to consider model/data privacy protection in applying Machine Learning-as-a-Service in real-world privacy-critical applications.

Visualization and monitoring Romain Brisse started his PhD thesis in the Malizen company, which is a start-up that originated in the CIDRE team. Malizen develops the ZeroKit tool that aims to investigate complex attacks by using a visual tool offering interactive views of logs (system, network). During his first year, Romain proposed a new recommender system that helps the analyst to choose among proposals for his next step of investigation [9]. These recommendations increase the efficiency of the investigator. These recommendations are computed using the knowledge extracted from the MITRE ATT&CK (real world adversary knowledge) and scored by algorithms that manipulate the investigated logs. Experiments have been conducted with experts in log analysis on the dataset TC3 from the DARPA in order to show the usefulness of the recommendations.

Effect of electromagnetic fault injection on micro-architecture In [7], we demonstrate that complex CPUs are vulnerable to fault injection attacks. In particular, the memory hierarchy and the MMU can be changed, which creates a mismatch between hardware behavior and software expectations. In this work, we highlight several new fault effects at the micro-architectural level, in particular in the memory hierarchy: On the L1 instruction cache, on the memory management, on the L2 cache.

Low-Cost Evaluation Platform for Multifault Injection Fault injection using laser beams or electromagnetic injection (EMI) are used in the literature to hijack control flow or to change a register value. Experiments in this domain requires expensive experiments due to the cost of EMI benches or laser probes. In [10], we propose TRAITOR, a low-cost evaluation platform to precisely inject numerous faults by clock glitch. With a low-cost FPGA, we produce our own faulty clock signal to replace the one of the targeted board. The platform makes the injection more controllable and easily reproducible. It provides the ability to inject consecutive faults and to realize complex attacks inducing several bursts of faults.

6.2 Axis 2 : Attack detection

Participants: Mathieu Escouteloup
, Yufei Han, Jean-François Lalande, Valérie Viet Triem Tong.

Vulnerability detection The results obtained during the PhD thesis of Pierre Graux led to investigate attacks that use both the Java bytecode and the native code to flaw some sensitive data in an Android application. Such attack would be possible if a developer misuse the "transient" keyword on a sensitive field that would be serializable. We proposed an automatic detection of such vulnerability by combining static analysis and symbolic execution [12]. Our approach was applied on the Telegram source code and we found non-exploitable flows hidden within Telegram's code base.

Stalkerware detection Stalkerware enables adversaries to conduct surveillance and remote control on a targeted person's device. The Android devices are a particularly fertile ground for stalkerware, most of which spy on a single communication channel, sensor, or category of private data, though 27% of stalkerware surveil multiple private data sources. In [18], we propose DOSMELT, a stalkerware detection system with nuanced warnings that precisely characterize the types of surveillance functionalities conducted by Android stalkerware. The goal of DOSMELT is to provide in-time alerts to victims of stalkerwares. They can then take appropriate mitigating actions. Furthermore, we introduce active learning techniques into the design of DOSMELT, to promote effective data-driven security analysis even with few manually annotated apps.

6.3 Axis 3 : Attack resistance

Participants: Emmanuelle Anceaume, Aimad Berady, Mathieu Escouteloup, Gilles Guette , -NoValue--NoValue- -NoValue- *(-NoValue-)*YufeiHan , Guillaume Hiet, Camille Le Bon, Frédéric Tronel, Valérie Viet Triem Tong.

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 [3], 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.

Preventing hardware timing information leakage. Since Spectre and Meltdown attacks were published in 2018, numerous attacks target the whole microarchitecture to extract information from timing variations. In [11], we propose and implement a process to build cores without microarchitectural timing leakage. We outline new generic design rules based on first principles to prevent timing information leakage, and build whole cores immune to them.

Injecting protections at runtime using Dynamic Binary Instrumentation. Memory corruption attacks have been a significant issue in software security for over two decades and are still one of the most dangerous and widespread types of attacks nowadays. In [13], we propose an approach to protect applications against memory corruption attacks at runtime. We developed DAMAS, a framework capable of deploying such protections on running applications. Our solution does not require recompiling the application and uses runtime information to optimize the protections during the process execution. We implemented a Control-Data Isolation protection using our framework and evaluated its impact on performance.

Blockchain in adversarial environments. We are pursuing our efforts dedicated to the theoretical aspects of blockchains in adversarial environments. This work, which started last year, aims at formally characterizing what a user can expect from blockchains in presence of adversarial environments. We argue that such an expectation can be fully characterized by the notion of « finality ». The notion of finality refers to the time when it becomes impossible to remove a block that has previously been appended to the blockchain. Blockchain finality can be deterministic or probabilistic, immediate or eventual. Informally, immediate finality guarantees, as its name suggests, that when a block is appended to a local copy, it is immediately finalized and thus will never be revoked in the future. Most of the permissionned blockchains satisfy the deterministic form of immediate consistency, including Red Belly blockchain

and Hyperledger Fabric blockchain, while the probabilistic form of immediate consistency is typically achieved by permissionless pure proof-of-stake blockchains such as Algorand, or StateCube. Designing blockchains with immediate finality favors consistency against availability in presence of transient partitions of the system. It leverages the properties of Consensus (i.e a decision value is unique and agreed by everyone), at the cost of synchronization constraints.

On the other hand eventual finality ensures that all local copies of the blockchain share a common increasing prefix, and thus finality of their blocks increases as more blocks are appended to the blockchain. The majority of cryptoassets blockchains, with Bitcoin and Ethereum as celebrated examples, guarantee eventual finality with some probability: blocks may be revoked after being appended to the blockchain, yet with decreasing probability as they sink deeper into the chain.

While probabilistic eventual finality has been widely studied in the context of Bitcoin, some few studies have started to lay the foundations of the computation power of blockchains with deterministic eventual finality consistency.

We reinvestigate the definition of (deterministic) eventual prefix consistency introduced in [20] to fit both the context in which an infinite number of blocks are appended to the blockchain. We introduce the notion of bounded displacement, which informally says that the number of blocks that can be revoked from the current blockchain is bounded. Specifically, we show that known bounded displacement eventual prefix consistency is equivalent to Consensus, that unknown bounded displacement eventual prefix consistency is equivalent to eventual strong prefix consistency, and eventual strong prefix consistency is stronger than Eventual Consensus. We provide an algorithm that guarantees eventual prefix consistency in an asynchronous environment with an unbounded number of Byzantine processes. We also show that it is impossible to build a blockchain that guarantees eventual prefix consistency based on the longest chain rule. Finally, we discuss impossibilities and possibilities of unbounded displacement eventual prefix consistency. In particular, we propose an algorithm that solves unknown bounded displacement eventual prefix in an eventually synchronous environment in presence of less than a majority of Byzantine processes. To summarize, we close the gap between eventual prefix and strong prefix consistencies. More details appear in [8].

Uniform node sampling in adversarial environments. This work considers the problem of achieving uniform node sampling in large scale systems in presence of Byzantine nodes. The uniform node sampling service offers to applications using it a single simple primitive that returns, upon invocation, the identifier of a random node that belongs to the system. We first propose an omniscient strategy that processes on the fly an unbounded and arbitrarily biased input stream made of node identifiers exchanged within the system, and outputs a stream that preserves the uniformity property. Informally, uniformity states that any node in the system should have the same probability to appear in the sample of any correct node of the system. We show through a Markov chain analysis that this property holds despite any arbitrary bias introduced by the adversary. We then propose a strategy based on a sketch data structure that is capable of approximating the omniscient strategy without requiring any prior knowledge on the composition of the input stream. We show through both theoretical analysis and extensive simulations that this "knowledge-free" strategy accurately approximates the omniscient one. We evaluate the resilience of the knowledge-free strategy by studying two representative attacks (flooding and targeted attacks). We quantify the minimum number of identifiers that Byzantine nodes must insert in the input stream to prevent uniformity. Finally, we propose a new construction that processes each input stream with sketches put in series that allows to both increase the accuracy of a single sketch and decrease the time to converge to a uniform output stream. To our knowledge, such a work has never been proposed before. More details appear in [2].

Stochastic analysis of rumor spreading. The long term objective of this work is a deep analysis of rumor spreading in large-scale and open networks in presence of adversarial behaviors. So far, we have proposed and analyzed a new asynchronous rumor spreading protocol to deliver a rumor to all the nodes of a large-scale distributed network. This spreading protocol relies on what we call a k-pull operation for any value of k. Specifically a k-pull operation consists, for an uninformed node s, in contacting k-1 other nodes at random in the network, and if at least one of them knows the rumor, then node *s* learns it. We have performed a thorough study of the total number of k-pull operations needed for all the n nodes of

the system to learn the rumor, for any value of n. All these results appear in [6, 14]. The second step of this work will be to take into account the multiplicity of the recipients of the pull operations to design Byzantine-tolerant pull operations.

Stochastic analysis of algorithms for collecting longitudinal data. This work proposes and analyses the performance and the vulnerability to attacks of three algorithms for collecting longitudinal data in a large scale system. A monitoring device is in charge of continuously collecting measurements from end-devices. The communication graph is connected but not necessarily complete. For scalability reasons, at each collect, a single end-device is randomly selected among all the end-devices to send the content of its local buffer of data to the monitoring device. Once sent, the end device resets its buffer, and resumes its measurement process. Two of the three algorithms are randomized algorithms while the third one is deterministic. The difference between the randomized algorithms stems from the random choice policy: in the first algorithm, choice is uniform while in the second one the random choice is weighted by the current amount of measurements at end-devices. The third algorithm is deterministic. End-devices are successively chosen in a round robin way. We study the transient and stationary maximum load distribution at end-devices when collects are made using the first and third algorithm, and by providing bounds via a coupling argument when the second algorithm is used. While the third algorithm provides the best performance, it is highly vulnerable to attacks. Details of this line of research is described in [15].

Safe artificial intelligence for trust-critical Machine-Learning-as-a-Service system. With dramatic advance of Deep Learning (DL) techniques during the past decade, various DL algorithms have achieved impressive human-level classification and notable success in domains from computer vision to natural language processing. Increasingly deployed in various real-world trust-critical systems, safety of DL techniques becomes a leading research priority and is as important as the focus on accuracy, speed, and scalability. The stakeholders of DL services often have the safety concern and ask how they can trust the DL-enabled systems in the cost-sensitive decision-making process. In this proposal, our study is concretized to three trust-critical applications with categorical input data including 1) malware detection and intrusion detection [17], 2) graph-based social network analysis [1] and 3) automated medical diagnosis using electronic health records. Compared to continuous data, like images, establishing the safety guarantees on categorical inputs against various adversarial attacks raises a unique challenge: the adversarial attacks on categorical data are intrinsically NP-hard Mixed-Integer Non-Linear Programming problems. Our study thus aims to provide both theoretical and practical answers to assess and mitigate the adversarial vulnerability of Deep Learning techniques on categorical data, in order to deliver safety-guaranteed learning in trust-critical applications.

7 Bilateral contracts and grants with industry

7.1 Bilateral contracts with industry

- **DGA (2019-2021)**

  Participants: Ludovic Claudepierre, Gilles Guette.

  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

- **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.

- **DGA**. The engineer Leopold Ouairy was affected to the MoM malware analysis platform. He notably refactored the platform to make it more easy to maintain and expand and added new features required by the work of Vincent Raulin.

7.2 Bilateral grants with industry

- **Ministry of Defence: Characterization of an attacker**

  Participants: Aimad Berady, Gilles Guette, Valérie Viet Triem Tong.

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**

  Participants: Michel Hurfin.

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. For example, in [4], we propose and evaluate a solution which uses a space filling curve to partition wide area geometric graphs.

- **CEA:**

  Participants: Emmanuelle Anceaume.

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.

- **DGA:**

  Participants: Jean-François Lalande, Valérie Viet Triem Tong, Pierre Wilke.

Tomas Concepcion Miranda is financed notably by the DGA though the Pôle d'Excellence Cyber (PEC) since October 2021. Tomas works on Android malware dataset characterisation and associated visualization tools.

- **ANSSI:**

  Participants: 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.

- **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 work on the automatic generation of attack scenario to design deceptive honeynet.

- **Malizen:**

  Participants: Romain Brisse, Jean-François Lalande.

Romain Brisse's thesis is financed by Malizen, an Inria start-up from the CIDRE team since January 2021. His thesis focuses on recommendation system for visual investigation software.

- **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, Ludovic Me.

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

- **DGA:**

Participants: Pierre-François Gimenez, Ludovic Me.

Adrien Schoen is financed notably 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 autoencoder.

- **DGA:**

Participants: Pierre-François Gimenez, Yufei Han, Valérie Viet Triem Tong.

Helene Orsini's thesis is financed by DGA since October 2021. Her thesis project focuses on adversarially robust and interpretable Machine Leanring pipeline for network intrusion detection systems. She will study how to automatize 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.

8 Partnerships and cooperations

8.1 European initiatives

8.1.1 FP7 & H2020 projects

H2020 Project: SOTERIA (2021-2024).

Participants: Guillaume Piolle.

The SOTERIA project aims to develop a citizen-driven and citizen-centric, cost-effective, marketable identity management service, to enable citizens to control their personal data easily and securely. This project will develop a framework combining a high-level identification tool with a decentralized secured data storage platform, to enable all citizens to fully protect and control their personal data while also gaining enhanced awareness on potential privacy risks.

The SOTERIA solution will be tested and validated through 3 real-world large-scale use-cases, involving 6,500 European citizens, targeting 3 applications which usefulness has been highlighted during COVID-19 pandemic: e-learning, e-voting and e-health. This 3-year transdisciplinary project from both SSH and technology angles, will develop an innovative solution based on: a secured access interface relying on high-level identification, a smart platform processing data to transmit only the minimum personal data required, a secured data storage platform (decentralized architecture) under the full control of the citizen, an educational tool to raise awareness of citizens developed using a citizen-driven and citizen-centric approach.

CIDRE and WIDE team members are collaborating together in this project. The participation of CIDRE focuses on security and privacy properties in distributed identity management frameworks, in the context of the PhD of Mathieu Gestin (WIDE).

H2020 Project: SPARTA (2019-2022).

Participants: Michel Hurfin, Ludovic Me.

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

8.1.2 Other european programs/initiatives

Participants: Jean-François Lalande, Valérie Viet Triem Tong, Pierre Wilke.

The CIDRE team is co-supervizing the phd thesis of Séverine Delaplace with the TruX research group of the University of Luxembourg. The work of Severine is focused on malware analysis that interact with a remote server. A contract for this thesis in "co-tutelle" states the conditions for a double diploma at the end of the thesis.

8.2 National initiatives

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: TrustGW (2021-2025).

Participants: Guillaume Hiet, Frédéric Tronel, Pierre Wilke.

TrustGW is a collaborative ANR project involving the CIDRE team from IRISA, the ARCAD team from Lab-STICC, and the SYSCOM team from IETR. This project aims to develop a dynamically reconfigurable and trusted heterogeneous software-hardware gateway architecture for the Internet of Things. We consider a generic architecture composed of several RISC-V processors (baseband, generic) and FPGA components. The hypervisor allows virtualizing these resources and allocating them to the different virtual machines. 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 all the resources and (3) to secure the applications running on the gateway. In the framework of this project, the contribution of the CIDRE team will mainly focus on the last challenge.

PHC AURORA Project: SECUTRACE (2020-2021).

Participants: Guillaume Hiet.

The SECUTRACE research project aims to contribute to the dependability and cyber-security of systems by exploiting the trace generation mechanisms available in most consumer hardware platforms. These mechanisms are, for example, available in embedded systems using ARM processors (CoreSight technology) and on computers using Intel processors (Intel PT technology). SECUTRACE is a collaborative project between the CIDRE team at CentraleSupélec/Inria (France) and Volker Stolz's team at Western Norway University of Applied Sciences (HVL). This work should ultimately reduce the defect rate in software, mitigate the effects of programming errors, and provide new ways to detect intrusions.

8.3 Regional initiatives

CominLabs project: Priceless (2021-2025).

Participants: Emmanuelle Anceaume.

Priceless is a collabortive 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.

CominLabs project: SCRATCHS (2021-2024).

Participants: Guillaume Hiet, Frédéric Tronel, Pierre Wilke.

SCRATCHS is a collaboration between researchers in the fields of formal methods (Celtique, Inria Rennes), security (Cidre, CentraleSupélec Rennes) and hardware design (Lab-STICC). Co-design is essential to get end-to-end security: cooperation between the compiler and hardware is necessary to avoid time leaks due to the micro-architecture with minimal overhead. This project aims 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.

FUI project: SECEF (2020-2022).

Participants: Guillaume Hiet.

SECEF (Security Exchange Format) is a FUI collaborative project involving industrial partners (CS, IMS Networks, techlib, Cyber Test Systems) and academics (CentraleSupélec, Télécom SudParis). This project aims to promote the standardization of formats in the field of cybersecurity. More precisely, we want to address the limitations of the IDMEF format and propose a new RFC for a standard format for security events exchange. In this project, the CIDRE team is involved in studying the state of the art of security event formats and the specification of a new security event format. We will also participate in the standardization effort. In the framework of this project, we have recruited Pascal Greliche as a research engineer for two years (2021-2023).

9 Dissemination

9.1 Promoting scientific activities

9.1.1 Scientific events: organisation

Seminar "Hands-on Machine Learning for Security", sponsored by the GDR Sécurité Informatique, organised by Pierre-François Gimenez and Yufei Han. This seminar was an in-person event and broadcasted on Youtube (link).

General chair, scientific chair Guillaume Hiet organized (SILM 2021): the third Workshop on the Security of the Software/Hardware Interfaces. This online event was co-localized with the IEEE Euro S&P conference, September 6th, 2021.

Member of the organizing committees Ludovic Mé

- was a member of the organizing committee of JSI 2021 (Journées Scientifiques Inria) ;
- organized a special one-day event on the C3 project in the context of the 2021 European Cyber Week in Rennes ;
- serves the steering committee of RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information).

9.1.2 Scientific events: selection

Chair of conference program committees.

- Guillaume Hiet was the Program Committee chair of SILM 2021.
- Jean-Francois Lalande was the Program co-chair of the IWSMR 2021 workshop.

Member of the conference program committees.

- Emmanuelle Anceaume was part of the program committee of IEEE DSN 2021, OPODIS 2021, IEEE TrustCom 2021, and Tokenomics 2021.
- Pierre-François Gimenez was part of the program committee of AAAI-22.
- Yufei Han served as a part of the program committee of IJCAI 2021, ICML 2021, KDD 2021, NeurIPS 2021, ICLR 2021, AAAI 2021 and SDM 2021.
- Guillaume Hiet was part of the program committee of EAI SecureComm 2021.

- Jean-Francois Lalande was part of the program committee of EICC 2021, SecITC 2021, IWSMR 2021, WTMC 2021, CUING 2021, IWCC 2021, SSTIC 2021.
- Ludovic Mé served the Scientific Committee of FIC 2021 (Forum International de la Cybersécurité, Lille) and the Program Committee of JSI 2021 (Journées Scientifiques Inria).
- Gilles Guette served the program Committee of ICISSP 2021.

Reviewer

- Yufei Han served as a reviewer of RAID 2021.

9.1.3 Journal

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

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

Reviewer - reviewing activities

- Yufei Han served as a reviewer of IEEE Transactions on Dependable and Secured Computing (IEEE Trans on TDSC). He also served as a reviewer for NeuralComputing (Elsevier) and Cyber Security (Elsevier).
- Pierre-François Gimenez served as a reviewer of IEEE Transactions on Computers.
- Jean-Francois Lalande served as a reviewer of MDPI Electronics, IEEE Transactions on Reliability, IEEE TIFS, Elsevier FGCS.

9.1.4 Invited talks

Guillaume Hiet gave an invited talk at the (COEMS Forsterk Seminar) on Hardblare – heterogeneous solution for embedded software security.

Ludovic Mé was panelist for round tables dedicated to the interaction between cyber security and AI, in the context of:

- the conference CAID 2021 (Conference on Artificial Intelligence for Defense) ;
- the Atos Cyber Day.

9.1.5 Scientific expertise

Jean-Francois Lalande was a reviewer for the phD grants in IA for the "HAISCoDe" program of Normandie University.

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 the expert group for the evaluation of French research entities (UMRs and EAs) relatively to the protection of scientific and technological properties (PPST)

9.1.6 Research administration

Emmanuelle Anceaume was member of a recruitment committee for a Maitre de conférence position at the University of Rennes 1.

Guillaume Hiet and Valérie Viet Triem Tong were members of a recruitment committee for a Maitre de conférence position at *CentraleSupelec*.

Ludovic Mé was member of a recruitment committee for a Professor position at the University of Rennes 1, and for a Starting Reseach Position at Inria.

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

Valérie Viet Triem Tong was member of a recruitment committee for a Maitre de conférence position at the University of Lille.

Valérie Viet Triem Tong was member of a recruitment committee for a Maitre de conférence position at the *IUT de Vannes*.

Valérie Viet Triem Tong was member of a recruitment committee for a Professor position at *INSA Centre - Val de Loire*.

Valérie Viet Triem Tong was member of a recruitment committee for a Professor position at *INP ESISAR*.

Gilles Guette was vice-president of a recruitment committee for a Maitre de conférence position at the University of Rennes 1.

9.2 Teaching - Supervision - Juries

9.2.1 Teaching

Team members are involved in initial and continuing education in CentraleSupélec, a french institute of research and higher education in engineering and science, 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 2021.

The teaching duties are summed up in table 1.

9.2.2 Supervision

PhD in progress:

- Aimad Berady, Characterization of an attacker, supervised by Valérie Viet Triem Tong (35%), Gilles Guette (35%), Christophe Bidan (30%).
- Cedric Herzog, E'tude des malware e'vasifs: conception, protection et de'tection, supervised by Valérie Viet Triem Tong (50%),Pierre Wilke (50%), Christophe Bidan (30%).
- Camille Le Bon, Security enhancement in embedded hard real-time systems, started in October 2018, supervised by Erven Rohou (PACAP) (30%), Guillaume Hiet (35%), and Frédéric Tronel (35%)
- 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).

	Licence level	Master level	CS†	Univ. Rennes 1	Initial education	Continuing education	2020 -2021
Emmanuelle Anceaume		✓	✓	✓	✓		20
Christophe Bidan	✓	✓	✓		✓	✓	-
Gilles Guette	✓	✓		✓	✓		460
Michel Hurfin		✓	✓		✓		6
Jean-François Lalande	✓	✓	✓		✓	✓	256 +61*
Guillaume Piolle	✓	✓	✓	✓	✓	✓	186
Frédéric Tronel	✓	✓	✓	✓	✓	✓	287
Valérie Viet Triem Tong	✓	✓	✓	✓	✓	✓	105 105*

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

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

- Cyprien Gottstein, Problématiques de stockage et d'interrogation de très grands graphes répartis dans le contexte de l'Internet des Objets, started October 2018, supervised by Michel Hurfin (50%) and Philippe Raipin Parvedy (50%).

- Arthur Rauch, Stockage frugal et légal pour la Blockchain du futur, started October 2021, supervised by Emmanuelle Anceaume and Davide Frey.

- Vincent Kowalski, Byzantine-FT abstractions from closed to open systems, started October 2021, supervised by Emmanuelle Anceaume, Matthieu Perrin and Achour Mostefaoui.

- Jean-Loup Hatchikian-Houdot, Security-enhancing compiler against side-channel attacks, started October 2021, supervised by Frédéric Besson (50%), Pierre Wilke (25%), and Guillaume Hiet (25%).

- 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%).

- 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%).

- Vincent Raulin, Enhancing malware detection with machine learning by designing a new execution trace representation, started October 2021, supervised by Valérie Viet Triem Tong (33%), Pierre-François Gimenez (33%) and Yufei Han (33%).

- Tomas Concepcion Miranda, profiling and visualization of Android malware dataset, started in october 2019, supervised by Jean-Francois Lalande (33%), Valérie Viet Triem Tong (33%), Pierre Wilke (33%).

- Romain Brisse, recommender system for investigation tools, supervised by Jean-Francois Lalande (50%), Frédéric Majorczyk (50%).

- Séverine Delaplace, Analyzing Android malware communicating with a remote server, 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).
- 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%) and Erwan Abgrall (MINARM, 25%).
- Helene Orsini, Security Incident Detection and Classification with Noisy Structured and Unstructured Data, supervised by Yufei Han (50%), Valérie Viet Triem Tong (25%) and David Lubicz (DGA, 25%).
- Natan Talon, Rejeu et apprentissage de sce'narios d'attaques ,supervised by Mathieu Jaume (25%), Gilles Guette (25%), Yufei Han (25%) and Valérie Viet Triem Tong (25%).

9.2.3 Juries

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*, PhD thesis delivered by l'ENSEEIHT. Jury committee: Reviewers: Emmanuelle Anceaume and Bernadette Charron-Bost. Examiners: Xavier Thirioux and Sébastien Tixeuil.
- Victorien Elvinger, *Réplication sécurisée dans les infrastructures pair-à-pair de collaboration*, PhD thesis delivered by l'Université de Lorraine, supervised by Francois Charoy and Gerald Oster. Jury committee: Reviewers: Emmanuelle Anceaume and Pascal Molli. Examiners: Esther Pacitti and Steve Kremer.
- Marianna Belotti, *Game Theory and Rational Agents*, PhD thesis delivered by CNAM, supervised by Stefano Secci and Maria Potop-Butucaru. Jury committee: Reviewers: Emmanuelle Anceaume and Maurice Herlihy. Examiners: Nicolas Maudet, Julien Pratt and Silvia Bonomi.
- Antoine Durand, *Byzantine consensus and blockchain : Models unification and new protocols*, PhD thesis delivered by Institut Polytechnique de Paris. Jury committee: Reviewers: Maria-Potop Butucaru and Pierre Jouvelet. Examiners: Emmanuelle Anceaume, Joaquim Garcia-Alfaro and Sara Tucci-Piergiovanni.

Pierre-François Gimenez was member of the PhD committee for the following PhD thesis:

- Malcolm Bourdon, *Détection d'intrusion basée sur l'analyse de compteurs matériels pour des objets connectés*, PhD thesis delivered by INSA-Toulouse, supervised by Youssef Laarouchi, Mohamed Kaaniche and Eric Alata.

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

- Marzieh Gheisari Amirian, *Secure Identification for the Internet of Things.* PhD thesis delivered by University of Rennes 1 and supervised by Laurent Amsaleg and Teddy Furon.

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

- Etienne Helluy-Lafont, *Sécurité et détection d'intrusion dans les réseaux sans fil*, PhD thesis delivered by University of Lille and supervised by Gilles Grimaud and Michael Hauspie.
- Sylvain Cecchetto, *Analyse du flot de données pour la construction du graphe de flot de contrôle des codes obfusqués.* PhD thesis delivered by University of Lorraine and supervised by Guillaume Bonfante and Jean Yves Marion.
- Frédéric Recoules, *Vérification automatique de code bas niveau : C, assembleur et binaire.* PhD thesis delivered by University Grenoble Alpes and supervised by Marie-Laure Potet and Sébastien Bardin.

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

- Manh-Dung Nguyen, *Binary-level directed fuzzing for complex vulnerabilities.* PhD thesis delivered by University Grenoble Alpes and supervised by Roland Groz and Sébastien Bardin.

Valérie Viet Triem Tong was a member of the HDR committee for the following habilitation:

- Guillaume Hiet, *Security at the Hardware/Software Interface.* Habilitation delivered by University of Rennes 1.

Ludovic Mé was a member of the HDR committee (reviewer) for the following habilitation:

- Guillaume Doyen, *Intégration du Comportement des Entités Terminales dans la Disponibilité des Services à Grande Echelle.* Habilitation delivered by Université de Technologie de Compiègne.

Jean-Francois Lalande was president of the PhD committee for the following PhD thesis:

- Lamine Noureddine, *Packing detection and classification relying on machine learning to stop malware propagation.* PhD thesis delivered by University of Rennes 1.

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

- Fergal Martin Tricot, *Sécurité des données de bout en bout dans un déploiement IdO hétérogène pour l'industrie 4.0*, PhD thesis delivered by INSA Centre Val de Loire.

Guillaume Piolle was member of the PhD committee for the following PhD thesis:

- Supriya Adahtarao, *On GDPR compliant Data Processing*, PhD thesis delivered by University Grenoble Alpes and supervised by Claude Castelluccia and Cédric Lauradoux.

9.3 Popularization

9.3.1 Education

On the Youtube page of the team, many scientific talks are published. Most of them are recordings from the biweekly CIDRE seminars organized by Pierre-François Gimenez. In 2021, 29 videos were published, with about 1400 view in total and about 226 hours of cumulated watch time.

9.3.2 Interventions

Guillaume Piolle has made a scientific mediation and popularization intervention about cybersecurity with the *Blanche de Castille* high school in Nantes, for students following the "digital and computing sciences" (NSI) pathway.

10 Scientific production

10.1 Major publications

[1] Y. Shen, X. He, Y. Han and Y. Zhang. 'Model Stealing Attacks Against Inductive Graph Neural Networks'. In: SP 2022 - 43rd IEEE Symposium on Security and Privacy. San Francisco, United States, 22nd May 2022. URL: https://hal.inria.fr/hal-03482156.

10.2 Publications of the year

International journals

[2] E. Anceaume, Y. Busnel and B. Sericola. 'Byzantine-tolerant Uniform Node Sampling Service in Large-scale Networks'. In: *International Journal of Parallel, Emergent and Distributed Systems* 36.5 (3rd June 2021), pp. 1–28. DOI: 10.1080/17445760.2021.1939873. URL: https://hal-imt-atlantique.archives-ouvertes.fr/hal-03265593.

[3] 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*. Special Issue on Latest Developments for Security Management of Networks and Services 18.2 (2021), pp. 1321–1333. DOI: 10.1109/TNSM.2021.3056999. URL: https://hal.inria.fr/hal-03131262.

[4] C. Gottstein, P. R. Parvedy, M. Hurfin, T. Hassan and T. Coupaye. 'Partitioning Wide Area Graphs Using a Space Filling Curve'. In: *International Journal of Data Mining & Knowledge Management Process* 11.1 (31st Jan. 2021), pp. 13–31. DOI: 10.5121/ijdkp.2021.11102. URL: https://hal.inria.fr/hal-03513456.

[5] Y. Mocquard, B. Sericola, F. Robin and E. Anceaume. 'Stochastic Analysis of Average Based Distributed Algorithms'. In: *Journal of Applied Probability* 58.2 (21st June 2021), pp. 394–410. DOI: 10.1017/jpr.2020.97. URL: https://hal-cnrs.archives-ouvertes.fr/hal-02473856.

[6] F. Robin, B. Sericola, E. Anceaume and Y. Mocquard. 'Stochastic analysis of rumor spreading with k-pull operations'. In: *Methodology and Computing in Applied Probability* (23rd Oct. 2021). URL: https://hal.archives-ouvertes.fr/hal-03128118.

[7] T. Trouchkine, S. K. K. Bukasa, M. Escouteloup, R. Lashermes and G. Bouffard. 'Electromagnetic fault injection against a complex CPU, toward new micro-architectural fault models'. In: *Journal of Cryptographic Engineering* 11.4 (Nov. 2021), pp. 353–367. DOI: 10.1007/s13389-021-00259-6. URL: https://hal.archives-ouvertes.fr/hal-03175704.

International peer-reviewed conferences

[8] E. Anceaume, A. D. Pozzo, T. Rieutord and S. Tucci-Piergiovanni. 'On finality in blockchains'. In: OPODIS 2021 - 25th Conference on Principles of Distributed Systems. Strasbourg, France, 13th Dec. 2021. URL: https://hal-cea.archives-ouvertes.fr/cea-03080029.

[9] R. Brisse, S. Boche, F. Majorczyk and J.-F. Lalande. 'KRAKEN: A Knowledge-Based Recommender system for Analysts, to Kick Exploration up a Notch'. In: SECITC 2021 - 14th International Conference on Security for Information Technology and Communications. Virtual, France, 25th Nov. 2021, pp. 1–17. URL: https://hal.inria.fr/hal-03486546.

[10] L. Claudepierre, P.-Y. Péneau, D. Hardy and E. Rohou. 'TRAITOR: A Low-Cost Evaluation Platform for Multifault Injection'. In: ASSS '21: Proceedings of the 2021 International Symposium on Advanced Security on Software and Systems. Virtual Event Hong Kong, Hong Kong SAR China: ACM, 24th May 2021, pp. 51–56. DOI: 10.1145/3457340.3458303. URL: https://hal.inria.fr/hal-03266561.

[11] M. Escouteloup, R. Lashermes, J. Fournier and J.-L. Lanet. 'Under the dome: preventing hardware timing information leakage'. In: CARDIS 2021 - 20th Smart Card Research and Advanced Application Conference. CARDIS: International Conference on Smart Card Research and Advanced Applications. Lübeck, Germany, 10th Nov. 2021, pp. 1–20. URL: https://hal.archives-ouvertes.fr/hal-03351957.

[12] P. Graux, J.-F. Lalande, V. Viet Triem Tong and P. Wilke. 'Preventing Serialization Vulnerabilities through Transient Field Detection'. In: SAC 2021 - 36th ACM/SIGAPP Symposium On Applied Computing. Gwangju / Virtual, South Korea: ACM, 22nd Mar. 2021, pp. 1–9. URL: https://hal.inria.fr/hal-03066847.

[13] C. Le Bon, E. Rohou, F. Tronel and G. Hiet. 'DAMAS: Control-Data Isolation at Runtime through Dynamic Binary Modification'. In: SILM 2021 - Workshop on the Security of Software / Hardware Interfaces. 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). digital event, Austria, 6th Sept. 2021, pp. 86–95. DOI: 10.1109/EuroSPW54576.2021.00016. URL: https://hal.archives-ouvertes.fr/hal-03340008.

[14] Y. Mocquard, B. Sericola and E. Anceaume. 'Analysis of Rumor Spreading with 2-pull or 3-pull Operations'. In: NCA 2021 - 20th IEEE International Symposium on Network Computing and Applications. Online, France: IEEE, 24th Nov. 2021, pp. 1–8. URL: https://hal.archives-ouvertes.fr/hal-03438975.

[15] F. Robin, B. Sericola and E. Anceaume. 'Stochastic analysis of algorithms for collecting longitudinal data'. In: 20th IEEE International Symposium on Network Computing and Applications (NCA 2021). online, France, 23rd Nov. 2021. URL: https://hal.archives-ouvertes.fr/hal-03215515.

[16] Y. Shen, X. He, Y. Han and Y. Zhang. 'Model Stealing Attacks Against Inductive Graph Neural Networks'. In: SP 2022 - 43rd IEEE Symposium on Security and Privacy. San Francisco, United States, 22nd May 2022. URL: https://hal.inria.fr/hal-03482156.

[17] Z. Yang, Y. Han and X. Zhang. 'Attack Transferability Characterization for Adversarially Robust Multi-label Classification'. In: Proceedings of European Conference on Machine Learning (ECML-PKDD) 2021, Part III. Vol. Part III. Bilbao, Spain: Springer, 13th Sept. 2021, pp. 397–413. URL: https://hal.archives-ouvertes.fr/hal-03449837.

Conferences without proceedings

[18] Y. Han, K. A. Roundy and A. Tamersoy. 'Towards Stalkerware Detection with Precise Warnings'. In: ACSAC 2021 - Proceedings of Annual Computer Security Applications Conference. Online, United States, 6th Dec. 2021, pp. 1–13. DOI: 10.1145/3485832.3485901. URL: https://hal.archives-ouvertes.fr/hal-03449857.

[19] V. Raulin, P.-F. Gimenez, Y. Han, V. Viet Triem Tong and L. Ouairy. 'GUI-Mimic, a cross-platform recorder and fuzzer of Graphical User Interface'. In: GreHack 2021 - 9th International Symposium on Research in Grey-Hat Hacking. Grenoble, France, 19th Nov. 2021, pp. 1–7. URL: https://hal.archives-ouvertes.fr/hal-03449827.

Scientific book chapters

[20] E. Anceaume, A. F. Anta, C. Georgiou, N. Nicolaou and M. Potop-Butucaru. 'Formalization of Blockchain Properties'. In: *Principles of Blockchain Systems*. 1st Sept. 2021. URL: https://hal.archives-ouvertes.fr/hal-03439073.

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

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

[22] F. De Vieilleville, S. May, A. Lagrange, A. Dupuis, R. Ruiloba, F. Ngolè Mboula, T. Bitard-Feildel, E. Nogues, C. Larroche, J. Mazel et al., eds. *Proceedings of the Conference on Artificial Intelligence for Defence 2020*. CAID 2020 - Second Conference on Artificial Intelligence for Defence. Rennes, France, Apr. 2021. URL: https://hal.archives-ouvertes.fr/hal-03206297.

Doctoral dissertations and habilitation theses

[23] G. Hiet. 'Security at the Hardware/Software Interface'. Université de Rennes 1, 15th Dec. 2021. URL: https://hal.archives-ouvertes.fr/tel-03511334.