RESEARCH CENTRE

Inria Center at Rennes University

IN PARTNERSHIP WITH:

CNRS, Université Rennes 1, CentraleSupélec

2022

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

Inria

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]
- Yufei Han [INRIA, Advanced Research Position]
- Michel Hurfin [INRIA, Researcher, HDR]
- Ludovic Mé [INRIA, Senior Researcher, HDR]

Faculty Members

- Valérie Viet Triem Tong [Team leader, CENTRALESUPELEC, Professor, HDR]
- Kevin Allix [CENTRALESUPELEC, Associate Professor, from Oct 2022]
- Christophe Bidan [CENTRALESUPELEC, Professor, HDR]
- Pierre-Francois Gimenez [CENTRALESUPELEC, Associate Professor, & Chair/SRP Inria]
- Gilles Guette [UNIV RENNES, Associate Professor]
- Guillaume Hiet [CENTRALESUPELEC, Professor, HDR]
- Jean-François Lalande [CENTRALESUPELEC, Professor, HDR]
- Guillaume Piolle [CENTRALESUPELEC, until Aug 2022]
- Frédéric Tronel [CENTRALESUPELEC, Associate Professor]
- Pierre Wilke [CENTRALESUPELEC, Associate Professor]

PhD Students

- Lucas Aubard [CENTRALESUPELEC, from Oct 2022]
- Matthieu Baty [INRIA]
- Nicolas Bellec [CENTRALESUPELEC, ATER, from Dec 2022]
- Pierre-Victor Besson [CENTRALESUPELEC]
- Romain Brisse [CENTRALESUPELEC]
- Tomas Concepcion Miranda [CENTRALESUPELEC]
- Séverine Delaplace [UNIVERSITE LUXEMBOURG, from Jun 2022]
- Lionel Hemmerle [CENTRALESUPELEC, from Nov 2022]
- Maxime Lanvin [CENTRALESUPELEC]
- Jean-Marie Mineau [CENTRALESUPELEC, from Oct 2022]
- Hélène Orsini [CENTRALESUPELEC]
- Vincent Raulin [INRIA]
- Adrien Schoen [INRIA]
- Natan Talon [HACKUITY, CIFRE]

Technical Staff

- Pascal Greliche [CENTRALESUPELEC, Engineer, until Oct 2022]
- Manuel Poisson [UNIVERSITE RENNES, Engineer, from Oct 2022]

Interns and Apprentices

- Damien Armillon [CENTRALESUPELEC, Intern, from Apr 2022 until Sep 2022]
- Lucas Aubard [CENTRALESUPELEC, Intern, from Feb 2022 until Jul 2022]
- Lionel Hemmerlé [CENTRALESUPELEC, Intern, from Apr 2022 until Sep 2022]
- Romain Ninot [CENTRALESUPELEC, Intern, from Apr 2022 until Sep 2022]
- Manuel Poisson [CENTRALESUPELEC, Intern, from Feb 2022 until Jul 2022]

Administrative Assistant

- Lydie Mabil [INRIA]

External Collaborators

- Erwan Abgral [MINISTERE DES ARMEES/CENTRALESUPELEC, from Aug 2022]
- Frederic Majorczyk [DGA/CENTRALESUPELEC]

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 Highlights of the year

This year, several works carried out in the team were published in the best conferences of our field. Among them, we would like to highlight the following publications:

- **RT-DFI: Optimizing Data-Flow Integrity for Real-Time Systems[15].** Published and presented at 34th Euromicro Conference on Real-Time Systems. This article received an outstanding paper award as detailed in 5.1.
- **Debiasing Android Malware Datasets: How Can I Trust Your Results If Your Dataset Is Biased ?** [4] Published in Transactions on Information Forensics and Security. This work focuses on the quality assessment of malware datasets.
- **Cerberus: Exploring Federated Prediction of Security Events [15].** Published and presented at the ACM SIGSAC Conference on Computer and Communications Security. This article focuses on Federated AI for intrusion detection.

5.1 Awards

We were very proud to receive an outstanding paper award at 34th Euromicro Conference on Real-Time Systems (ECRTS 2022) for the article entitled "RT-DFI: Optimizing Data-Flow Integrity for Real-Time Systems". This work is the result of a fruitful collaboration between Nicolas Bellec and Isabelle Puaut from the INRIA PACAP research team, Simon Rokicki from the INRIA TARAN research team, Guillaume Hiet and Frédéric Tronel from CentraleSupélec/INRIA CIDRE research team.

6 New software and platforms

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.

News of the Year: The full source code have been published and documented. New experiments have been released in september 2022 that enhance the results for more complex applications.

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.

News of the Year: A first version is in production in the LHS.

Contact: Jean-François Lalande

Participants: Tomas Concepcion Miranda, Leopold Ouairy, Damien Gourbeyre

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 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: Kevin Allix, Aimad Berady, Romain Brisse, Pierre-François Gimenez, Gilles Guette, Yufei Han, Maxime Lanvin, Jean-François Lalande, Tomas Concepcion Miranda, Frédéric Majorczyk, Valérie Viet Triem Tong, Pierre Wilke.

Data and model to help the understanding of advanced attack campaigns. Advanced Persistent Threat (APT) attacks are surgically targeted attacks led by advanced attackers, who constantly adapt their Tactics, Techniques, and Procedures (TTP).Identifying patterns in the modus operandi of attackers is an essential requirement in the study of Advanced Persistent Threats. Our community is hampered both by the lack of formalism helping to precisely describe these attacks and by the lack of accurate, relevant, and representative datasets of these current threats. In [2] we propose a formal model of an attacker's tactical progression during the network propagation phase. This formalization allows to describe the PWNJUTSU experiment unequivocally. In this experiment, 22 Red Teamers attacked a vulnerable infrastructure to compromise machines and steal secret flags. we had three distinct goals in this experiment. A first goal was to observe how professionals attackers progress in such an infrastructure. A second goal was to build a dataset of various attacks targeting the same infrastructure. A last goal was to test the relevance of our model of a whole attack campaign. The resulting dataset is available online on here. It contains all participants' event logs (system and network), including the reference environment's event logs. A search engine is also provided to peek into the dataset.

Assessing the opportunity of combining state-of-the-art Android malware detectors Research on Android malware detection based on Machine learning has been prolific in recent years. In [5], in collaboration with the TruX team at the University of Luxembourg we detail a large-scale evaluation of four state-of-the-art approaches that their achieved performance fluctuates when applied to different datasets. Combining existing approaches appears as an appealing method to stabilise performance. We therefore proceed to empirically investigate the effect of such combinations on the overall detection performance. In our study, we evaluated 22 methods to combine feature sets or predictions from the state-of-the-art approaches. Our results showed that no method has significantly enhanced the detection performance reported by the state-of-the-art malware detectors. Nevertheless, the performance achieved is on par with the best individual classifiers for all settings. Overall, we conduct extensive experiments on the opportunity to combine state-of-the-art detectors. Our main conclusion is that combining state-of-the-art malware detectors leads to a stabilization of the detection performance, and a research agenda on how they should be combined effectively is required to boost malware detection. All artifacts of this study form a dataset of $\tilde{0}.5$ million apks and all extracted features. These artifacts are made available for replicability here.

Quality of Android malware datasets. Android security has received a lot of attention over the last decade, especially when working on malware analysis. The CIDRE team have also a long past work on malware analysis. When presenting our contributions in conferences or discussing with other researchers of the community we had the feelings that the datasets that are used in the literature were of low quality: if the datasets are outdated or not representative of the studied population, the conclusions may be flawed. In [4], we have investigated the irregularities of datasets used in experiments, questioning the validity of the performances reported in the literature. We have developed a new method for debiasing datasets. With this method we have rebuilt new dataset, more up-to-date and with less bias than in the literature. This dataset has been released on the artifact repository of IEEE, as an independent contribution for ensuring the reproducibilty of our experiments and to serve as new start point for future works. In particular, this dataset can be used by other reasearchers contributing in Android malware detection or classification with machine learning algorithms.

Imbalanced Classification with TPG Genetic Programming: Impact of Problem Imbalance and Selection Mechanisms [19]

Model Stealing Attacks Against Inductive Graph Neural Networks [18]

7.2 Axis 2 : Attack detection

Participants: Kevin Allix, Yufei Han, Guillaume Hiet, Michel Hurfin, Jean-François Lalande, Maxime Lanvin, Frédéric Majorczyk, Ludovic Mé, Helene Orsini, Adrien Schoen, Valérie Viet Triem Tong.

Errors in the CICIDS2017 dataset and the significant differences in detection performances it makes. [25]

Among the difficulties encountered in building datasets to evaluate intrusion detection tools, a tricky part is the process of labelling the events into malicious and benign classes. The labelling correctness is paramount for the quality of the evaluation of intrusion detection systems but is often considered as the ground truth by practitioners and is rarely verified. Another difficulty lies in the correct capture of the network packets. If it is not the case, the characteristics of the network flows generated from the capture could be modified and lead to false results.

In this paper, we present several flaws we identified in the labelling of the CICIDS2017 dataset and in the traffic capture, such as packet misorder, packet duplication and attack that were performed but not correctly labelled. We also assess the impact of these different corrections on the evaluation of supervised intrusion detection approaches.

Detecting APT through graph anomaly detection. [22]

Despite fruitful achievements made by unsupervised machine learning-based anomaly detection for network intrusion detection systems, they are still prone to the issue of high false alarm rates, and it is still difficult to reach very high recalls. In 2020, our team proposed (Leichtnam' PhD thesis) Sec2graph, an unsupervised approach applied to security objects graphs that exhibited interesting results on single-step attacks. The graph representation and the embedding allowed for better detection since it creates qualitative features.

In this paper, we present new experiments to assess the performances of this approach for detecting APT attacks. We achieve better detection performances than the original work's baseline detection methods on the DAPT2020 dataset.

Towards generic quality assessment of synthetic traffic for evaluating intrusion detection systems. [24]

Network Intrusion Detection Systems (NIDSes) evaluation requires background traffic. However, real background traffic is hard to collect. We hence rely on synthetic traffic generated especially for this task. The quality of the generated traffic has to be evaluated according to some clearly defined criteria.

In this paper, we show how to adapt the quality assessment solutions proposed for different fields of data generation such as image or text generation to network traffic. We discuss the criteria that allow evaluation of the quality of a generated network traffic and propose functions to evaluate these criteria.

Cross-domain Alert Correlation methodology for Industrial Control Systems Alert correlation is a set of techniques used to process alerts raised by various intrusion detection systems in order to a eliminate redundant alerts, reduce the number of false alerts, and reconstruct attack scenarios. In Industrial Control Systems, the presence of a physical process and the associated specific threats has led to the heterogeneity of alerts due to the development of multi-domain detection techniques. Some detection approaches rely solely on observations at the level of the cyber domain while other approaches monitor the physical process. The two approaches are complementary but the information carried by the two types of alerts are different. In [6], we combine the alerts from physical domain intrusion detection with more classical cyber-domain intrusion detection alerts. We develop an alert correlation approach using an alert enrichment that allows mapping physical domain alerts into the cyber domain. We also propose a specific alert selection for correlation that adapts to the state of the physical process by dynamically adjusting the size of the selected alert window. We publicly released all the datasets generated and used in our results.

Intrusion Detection through Lightweight Tangled Program Graphs The fast improvement of Machine-Learning (ML) methods gives rise to new attacks in Information System (IS). Simultaneously, ML also creates new opportunities for network intrusion detection. Early network intrusion detection is a valuable asset for IS security, as it fosters early deployment of countermeasures and reduces the impact of attacks on system availability. In [8] we propose and study an anomaly-based Network Intrusion Detection System (NIDS) based on Tangled Program Graph (TPG) ML. Secure-GEGELATI learns how to detect intrusions from IS-produced traces and is optimised to fit the requirements of intrusion detection. The study evaluates the capacity of Secure-Gegelati to act as a continuously learning, real-time, and low energy NIDS when executed in an embedded network probe. We show that a TPG is capable of switching between training and inference phases, new training phases enriching the probe knowledge with limited degradation of previous intrusion detection capabilities. The Secure-GEGELATI software reaches 8x the energy efficiency of an optimised Random Forests (RF)-based Intrusion Detection System (IDS) on the same platform. It is capable of processing 13.2 k connections/seconds with a peak power of less than 3.3 Watts on an embedded platform, and is processing in real-time the CIC-IDS 2017 dataset while detecting 84% of intrusions and raising less than 0.2% of false alarms.

Anomaly-based Intrusion Detection using POSET In the context of the European SPARTA project, we have proposed an anomaly-based intrusion detection tool where the normal behavior of an application is described using models based on automata and invariants. First, the solution was evaluated using a distributed application (XtreemFS, a distributed file system). In this case, the events observed on different machines form a partially ordered set (POSET), which is the ideal target of our solution. Then, the tool was adapted to analyze network traffics (both Pcap and CSV files). Here observed events are totally ordered. Results of these evaluations are summarized in the published SPARTA deliverables.

Exploring Federated Prediction of Security Events Prior works in industrial intrusion detection practices follow the general approach to build AI-driven predicative models to learn from historical data. Such models characterize previous attack events and use this knowledge to predict future ones. These systems typically require collecting events from different industrial organizations and storing them in a centralized AI-as-a-Service (AIaaS) platform to train an AI-driven prediction model. However, these records often include privacy-sensitive metadata, including machine ID, event description, timestamp, system hardening actions taken, etc. Moreover, disclosing them can reveal sensitive information about security policies and security postures. Confidentiality concerns of industrial customers hence make it unrealistic to deploy such a centralized learning process of AI-based security event prediction methods. In [15], we investigate the feasibility of using privacy-friendly collaborative learning to benefit from participating organizations' knowledge without requiring data disclosure. In particular, we turn to employ Federated Learning to train AI models collaboratively by first locally training AI models per participating organization and then aggregating the local model updates. This Federated AI-based intrusion detection method is tested using real-world network attack attack data stored in a distributed way by 20 different industrial participants. We analyze the detection performance of this Federated AI system in practices, including measuring the detection performances and communication / computational cost of the Federated AI system. Furthermore, we discuss how the distribution drift of the attack behaviors across different industrial users affect the accuracy of the Federated AI system. We demonstrate how to measure the contribution of different participating organizations in the system to the collectively trained intrusion detection model and evaluate the benefits of each organization gained from joining the federation network. Finally, we unveil that distributed data poisoning attacks against the Federated AI system are effective at undermining robustness and decreasing the attack detection precision by a significant amount. While the state-of-the-art countermeasures are claimed to be effective, we demonstrate that carefully tuned data poisoning attacks can easily bypass the defense measures and injects decision bias to the Federated AI system without triggering any alerts of the hygiene check. Besides, we show that data reconstruction attacks can be performed against the participating organizations of the Federated AI system by leaking the statistical profiles of their privately owned attack data used for AI model training. Efficient as the Federated AI system is, our study also raises a severe concern over the potential risk of system integrity and data privacy leaks inside this Federated AI system.

AdvCat: Domain-Agnostic Robustness Assessment for Cyber security-Critical Applications with Categorical Inputs Machine Learning-as-a-Service systems (MLaaS) have been largely developed for cyber security-critical applications, such as detecting network intrusions and fake news campaigns. Despite effectiveness, their robustness against adversarial attacks is one of the key trust concerns for MLaaS deployment. Our work [16] are thus motivated to assess the adversarial robustness of the Machine Learning models residing at the core of these security-critical applications with categorical inputs. Previous research efforts on accessing model robustness against manipulation of categorical inputs are specific to use cases and heavily depend on domain knowledge, or require white-box access to the target ML model. Such limitations prevent the robustness assessment from being as a domain-agnostic service provided to various real-world applications. We propose a provably optimal yet computationally highly efficient adversarial robustness assessment protocol for a wide band of ML-driven cyber security-critical applications. We demonstrate the use of the domain-agnostic robustness assessment method with substantial experimental study on fake news detection and intrusion detection problems. ——

7.3 Axis 3 : Attack resistance

Participants: Emmanuelle Anceaume, Aimen Djari, Guillaume Piolle, Yufei Han, Guillaume Hiet, Frédéric Tronel.

Identity Management Systems allow users to prove characteristics about themselves to multiple service providers. IMS evolved from impractical, site-by-site authentication, to versatile, privacy enhancing Self Sovereign Identity (SSI) Frameworks. SSI frameworks often use Anonymous Credential schemes to provide user privacy, and more precisely unlinkability between uses of these credentials. However, these schemes imply the disclosure of the identity of the Issuer of a given credential to any service provider. This can lead to information leaks. In [3], we have proposed a new Anonymous Credential scheme that allows a user to hide the Issuer of a credential, while being able to convince the service providers that they can trust the credential, in the absence of a trusted setup. We proved this new scheme secure under the Computational Diffie Hellman assumption, and Decisional Diffie Hellman assumption, in the Random Oracle Model. We show that this scheme is efficient enough to be used with laptops, and to be integrated into SSI frameworks or any other IMS.

Boundaries Extending The Boundaries and Exploring The Limits Of Blockchain Compression Blockchain technology aims to replace traditional banking systems and manage the world's economic data. However, 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 a blockchain protocol based on superblock Non-InteractiveProofs-of-Proof-of-Work (NIPoPoWs) as a mechanism to reduce the storage and communication complexity of blockchains to $O(polylog(n))$. However, their protocol is only resilient to an adversary that may control strictly less than 1/3rd of the total computational power, which is a reduction from the security guaranteed by Bitcoin and other existing blockchain protocols that guarantee security against an adversary that may control strictly less than 1/2 of the total computational power. We present an improvement to the Kiayias et al. proposal termed Gems-scheme, which is resilient against an adversary that may control less than 1/2 of the total computational power while operating in $O(polylog(n))$ 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 [29].

Stochastic analysis of rumor spreading with multiple pull operations We propose and analyze a new asynchronous rumor spreading protocol to deliver a rumor to all the nodes of a large-scale distributed network [7]. This spreading protocol relies on what we call a k-pull operation, with $k \geq 2$. 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 perform a thorough study of the total number $T_{k,n}$ of k-pull operations needed for all the n nodes to learn the rumor. We compute

the expected value and the variance of $T_{k,n}$, together with their limiting values when n tends to infinity. We also analyze the limiting distribution of $(T_{k,n} - E(T_{k,n}))/2$ and prove that it has a double exponential distribution when n tends to infinity. Finally, we show that when $k > 2$, our new protocol requires less operations than the traditional 2-push-pull and 2-push protocols by using stochastic dominance arguments. All these results generalize the standard case $k = 2$.

Sycomore++ The arrival of Bitcoin drove the shift to decentralized ecosystems through the exchange of transactions without intermediary. However, one of the main challenges that need to face permissionless blockchains are scalability and security. Sycomore++ is a permissionless graph-based distributed ledger whose main feature is to dynamically self-adapt the number of created blocks to the current number of submitted transactions [9, 13]. We have conducted a performance evaluation of Sycomore++ and have compared it with the ones of Bitcoin and Sycomore, a graph-based distributed ledger. Our evaluation relies on agentbased simulations to evaluate the capability of these distributed ledgers to address the aforementioned challenges, within different execution contexts. One of the main lessons drawn from these intensive simulations is the capability of Sycomore++ to drastically reduce transaction confirmation time with respect to the other two ledgers, to quickly react to any sudden variation of the transaction submission rate, to minimize the computational power waste w.r.t. PoW-based permissionless distributed ledgers, and to surpass Bitcoin in terms of resilience to a network adversarial environment. We also study resilience to adversarial miners that want to endanger the quality of the graph showing that, as in Bitcoin, the adversary is limited by its computational power[12].

Towards understanding the robustness against evasion attack on categorical inputs Characterizing and assessing the adversarial vulnerability of classification models with categorical input has been a practically important, while rarely explored research problem. Categorical data exist widely in cyber security applications. For example, dynamic and static features of malware samples contain many categorical run-time and static signatures attributes, such as the types of API calls, files / processes visited or created and generated network traffics. Adversarial attacks against ML-based security incident detection systems raise a severe concern over the trustworthiness of ML-based detection. Therefore, exploring the origin of adversarial risk over categorical data can deepen our understanding about the feasibility of adversarial threats against real-world cyber security applications.

Our work [10] echoes the challenge by first unveiling the impact factors of adversarial vulnerability of classification models with categorical data based on an information-theoretic adversarial risk analysis about the targeted classifier. Though certifying the robustness of such classification models is intrinsically an NP-hard combinatorial problem, our study shows that the robustness certification can be solved via an efficient greedy exploration of the discrete attack space for any measurable classifiers with a mild smoothness constraint. Our proposed robustness certification framework is instantiated with deep neural network models applied on real-world safety-critic data sources. Our empirical observations confirm the impact of the key adversarial risk factors with categorical input.

Finding MNEMON: Reviving Memories of Node Embeddings In this work [17], we focus on exploring the potential data privacy leaks while deploying graph-based machine learning over the privately owned data, such as molecules invented to develop new medicines and social networks. Unveiling the privacy information about the training data directly violate the intellectual property policy of any entity using the Machine Learning service.

Previous security research efforts orbiting around graphs have been exclusively focusing on either (de-)anonymizing the graphs or understanding the security and privacy issues of graph neural networks. Little attention has been paid to understand the privacy risks of integrating the output from graph embedding models (e.g., node embeddings) with complex downstream machine learning pipelines. In this paper, we fill this gap and propose a novel model-agnostic graph recovery attack that exploits the implicit graph structural information preserved in the embeddings of graph nodes. We show that an adversary can recover edges with decent accuracy by only gaining access to the node embedding matrix of the original graph without interactions with the node embedding models. We demonstrate the effectiveness and applicability of our graph recovery attack through extensive experiments.

RT-DFI: Optimizing Data-Flow Integrity for Real-Time Systems The emergence of Real-Time Systems with increased connections to their environment has led to a greater demand in security for these systems. Memory corruption attacks, which modify the memory to trigger unexpected executions, are a significant threat against applications written in low-level languages. Data-Flow Integrity (DFI) is a protection that verifies that only a trusted source has written any loaded data. The overhead of such a security mechanism remains a major issue that limits its adoption. In [11], we presents RT-DFI, a new approach that optimizes the Data-Flow Integrity to reduce its overhead on the Worst-Case Execution Time. We model the number and order of the checks and use an Integer Linear Programming solver to optimize the protection on the Worst-Case Execution Path. Our approach protects the program against many memory-corruption attacks, including Return-Oriented Programming and Data-Only attacks. Moreover, our experimental results show that our optimization reduces the overhead by 7% on average compared to a state-of-the-art implementation.

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

- **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.

- **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.

- **ANSSI:**

Participants: 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 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 Mé.

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 Mé.

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.

9 Partnerships and cooperations

9.1 International research visitors

9.1.1 Visits of international scientists

Anurag Jain Anurag Jain from the International Institute of Information Technology, Hyderabad, India has visited the team from the 1st of May to the 31st of May. During this stay, with Emmanuelle Anceaume they have managed to identify and improve the Non-Interactive-Proofs-of-Proof-of-Work (NIPoPoWs) mechanism to achieve security against a Byzantine adversary that may control up to half of the total computational power, matching that of the non-NIPoPoW-protocols.

9.1.2 Visits to international teams

Research stays abroad Pierre-François Gimenez stayed for three months at CISPA Helmholtz Center for Information Security in Saarbrücken, Germany. During this stay, Pierre-François worked with Pr. Mario Fritz on malware analysis with machine learning. More specifically, this project is interested in the robustness of malware detectors based on machine learning against adversarial attacks. Mario Fritz brings his experience and knowledge of robust machine-learning-based detectors and certifiable machine learning. Pierre-François brings his expertise on malware analysis.

9.1.3 H2020 projects

SPARTA

Participants: Michel Hurfin, Ludovic Mé.

SPARTA project on cordis.europa.eu

Title: Strategic programs for advanced research and technology in Europe

Duration: From February 1, 2019 to June 30, 2022

Partners:

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France
- CESNET ZAJMOVE SDRUZENI PRAVNICKYCH OSOB (CESNET), Czechia
- JOANNEUM RESEARCH FORSCHUNGSGESELLSCHAFT MBH (JOANNEUM RESEARCH), Austria
- NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY (NASK), Poland
- TARTU ULIKOOL (UNIVERSITY OF TARTU), Estonia
- MYKOLO ROMERIO UNIVERSITETAS (MYKOLAROMERIS UNIVERSITY), Lithuania
- LATVIJAS MOBILAIS TELEFONS SIA, Latvia
- SECURITY MADE IN LETZEBUERG (SMILE), Luxembourg
- FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV (FHG), Germany
- FUNDACION TECNALIA RESEARCH & INNOVATION (TECNALIA), Spain
- TECHNISCHE UNIVERSITAET MUENCHEN (TUM), Germany
- THALES SIX GTS FRANCE SAS (THALES SIX GTS France), France
- COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA), France
- STOWARZYSZENIE POLSKA PLATFORMA BEZPIECZENSTWA WEWNETRZNEGO (PPBW), Poland
- INSTITUT NATIONAL DES SCIENCES APPLIQUEES DE LYON (INSA LYON), France
- SAP SE, Germany
- FORTISS GMBH, Germany
- LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY (LIST), Luxembourg
- VYSOKE UCENI TECHNICKE V BRNE (BRNO UNIVERSITY OF TECHNOLOGY), Czechia
- FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH (VICOM), Spain
- INDRA SISTEMAS SA (INDRA), Spain
- INSTITUT MINES-TELECOM, France
- RHEINISCHE FRIEDRICH-WILHELMS-UNIVERSITAT BONN, Germany
- UNIVERSITE DU LUXEMBOURG (uni.lu), Luxembourg
- CONSIGLIO NAZIONALE DELLE RICERCHE (CNR), Italy
- "NATIONAL CENTER FOR SCIENTIFIC RESEARCH ""DEMOKRITOS""" ("NCSR ""D"""), Greece

- LIETUVOS KIBERNETINIU NUSIKALTIMU KOMPETENCIJU IR TYRIMU CENTRAS (LITHUANIAN CYBERCRIME CENTER OF EXCELLENCE FOR TRAINING RESEARCH & EDUCATIO), Lithuania
- KENTRO MELETON ASFALEIAS (CENTER FORSECURITY STUDIES CENTRE D'ETUDES DE SECURITE), Greece
- INDRA FACTORIA TECNOLOGICA SL, Spain
- UNIVERSITAT KONSTANZ (UKON), Germany
- LEONARDO - SOCIETA PER AZIONI (LEONARDO), Italy
- KAUNO TECHNOLOGIJOS UNIVERSITETAS (UNIVERSITY OF TECHNOLOGY, KAUNAS), Lithuania
- TECHNIKON FORSCHUNGS- UND PLANUNGSGESELLSCHAFT MBH (TECHNIKON), Austria
- ITTI SP ZOO (ITTI), Poland
- DIREZIONE GENERALE PER LE TECNOLOGIE DELLE COMUNICAZIONI E LA SICUREZZA INFORMATICA - ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE (DG TCSI-ISCOM), Italy
- GENEROLO JONO ZEMAICIO LIETUVOS KARO AKADEMIJA (GENERAL JONAS ZEMAITISMILITARY ACADEMY OF LITHUANIA), Lithuania
- FUNDACIO EURECAT (EURECAT), Spain
- CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI (CNIT), Italy
- CENTRALESUPELEC (CentraleSupélec), France
- YES WE HACK (YWH), France
- INSTITUTO SUPERIOR TECNICO (IST), Portugal
- SECRETARIAT GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE (SGDSN), France
- UNIVERSITE DE NAMUR ASBL (UNamur), Belgium
- INOV INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES INOVACAO (INOV), Portugal
- CENTRE D'EXCELLENCE EN TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (CETIC), Belgium
- CZ.NIC, ZSPO (CZ.NIC), Czechia
- CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI), Italy

Inria contact: Thomas Jensen

Coordinator:

Summary: In the domain of Cybersecurity Research and innovation, European scientists hold pioneering positions in fields such as cryptography, formal methods, or secure components. Yet this excellence on focused domains does not translate into larger-scale, system-level advantages. Too often, scattered and small teams fall short of critical mass capabilities, despite demonstrating world-class talent and results. Europe's strength is in its diversity, but that strength is only materialised if we cooperate, combine, and develop common lines of research. Given today's societal challenges, this has become more than an advantage – an urgent necessity. Various approaches are being developed to enhance collaboration at many levels. Europe's framework programs have sprung projects in cybersecurity over the past thirty years, encouraging international cooperation and funding support actions. More recently, the Cybersecurity PPP has brought together public institutions and industrial actors around common roadmaps and projects. While encouraging, these efforts have highlighted the need to break the mould, to step up investments and intensify coordination. The SPARTA proposal brings together a unique set of actors at the intersection of

scientific excellence, technological innovation, and societal sciences in cybersecurity. Strongly guided by concrete and risky challenges, it will setup unique collaboration means, leading the way in building transformative capabilities and forming world-leading expertise centres. Through innovative governance, ambitious demonstration cases, and active community engagement, SPARTA aims at re-thinking the way cybersecurity research is performed in Europe across domains and expertise, from foundations to applications, in academia and industry.

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 "objects" that should eventually be all, or almost all, connected, the attack surface increases significantly. 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.

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 many 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 Guillaume Hiet, 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.

PHC AURORA Project: SECUTRACE (2020-2022).

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.

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 Guillaume Hiet, Pierre Wilke and Frederic Besson, on security-enhancing compilation against side-channel attacks.

10 Dissemination

Participants: Kevin Allix, Emmanuelle Anceaume, Pierre-François Gimenez, Gilles Guette, Yufei Han, Guillaume Hiet, Michel Hurfin, Jean-François Lalande, Ludovic Mé, Valérie Viet Triem Tong, Pierre Wilke.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

General chair, scientific chair

- Guillaume Hiet was the General Chair of the SILM 2022 workshop, co-localized with IEEE Euro S&P

Member of the organizing committees

- Ludovic Mé was a member of the organizing committee of JSI 2022 (Journées Scientifiques Inria) and 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

- Emmanuelle Anceaume was part of the program committees of the following conferences: IEEE/IFIP DSN 2022, OPODIS 2022, IEEE NCA 2022, IEEE BRAINs 2022, and FAB 2022.
- Michel Hurfin was part of the program committee of CARI 2022 (African Conference on Research in Computer Science and Applied Mathematics).
- Jean-Francois Lalande was part of the program committees of the conferences EICC 2022, SSTIC 2022 and the workshops WTMC 2022, CUING 2022, IWCC 2022.
- Ludovic Mé served the Scientific Committee of FIC 2022 (Forum International de la Cybersécurité), the Program Committee of JSI 2022 (Journées Scientifiques Inria), and the Program Committee of CARI 2022 (African Conference on Research in Computer Science and Applied Mathematics).
- Valérie Viet Triem Tong was part of the program committees of the following conferences: FPS 2023.
- Guillaume Hiet was part of the program committees of the following conferences: SILM 2022, EAI SecureComm 2022.

10.1.3 Journal

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:
  - Special issue "Fighting Cybersecurity Risks from a Multidisciplinary Perspective" with the Journal of Universal Computer Science
  - Journal of Universal Computer Science
  - MDPI Electronics
- Pierre-François served as reviewer for:
  - Journal of Computer Security
  - International Journal of Information Security
  - International Journal of Information Technology
- Guillaume Hiet served as reviewer for: Elsevier Computers & Security

10.1.4 Invited talks

- Ludovic Mé was panelist for a round table organized by BNP-Paribas and dedicated to the interaction between cyber security and AI (April 2022, 14th).
- Emmanuelle Anceaume was invited to give a talk at BRAINS 2022
- Pierre-François Gimenez was invited to give a talk at SUPSEC
- Guillaume Hiet and Pierre Wilke were invited to give talks at the COEMS Forsterk Seminar 2022

10.1.5 Scientific expertise

Jean-Francois Lalande was a reviewer for the phD grants “RIN Doctorants” of Normandie University and for the call for projects IRGA 2022 of Grenoble Alpes University.

Ludovic Mé serves:

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

Guillaume Hiet served as a reviewer for an ANR project.

Since October 2022, Guillaume Hiet is the co-chair of the Systems, Software and Network Security working group of the GDR Sécurité Informatique.

10.1.6 Research administration

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

The team participated to several recruitment committees:

- Ludovic Mé was member of the recruitment committees for a Professor position and for an Assistant Professor position at Télécom-Paris.
- Valérie Viet Triem Tong was member of the recruitment committees for a Professor position at University of Lorraine.
- Valérie Viet Triem Tong was member of the recruitment committees for a Professor position at IMT.
- Valérie Viet Triem Tong was member of the recruitment committees for an Assistant Professor position at CentraleSupélec.
- Valérie Viet Triem Tong was member of the recruitment committees for a Professor position at CentraleSupélec.
- Emmanuelle Anceaume was member of the recruitment committees for a Professor position at ESIR.
- Emmanuelle Anceaume was member of the recruitment committees for a Maitre de Conférence position at ISTIC.
- Jean-François Lalande was member of the recruitment committees for an Assistant Professor position at CentraleSupélec.
- Jean-François Lalande was member of the recruitment committees for a Professor position at CentraleSupélec.
- Guillaume Hiet was member of the recruitment committees for an Assistant Professor position at CentraleSupélec.

	Licence level	Master level	CS†	Univ. Rennes 1	Initial education	Continuing education	2021 -2022
Emmanuelle Anceaume		✓	✓	✓	✓		20
Christophe Bidan	✓	✓	✓		✓	✓	-
Gilles Guette	✓	✓		✓	✓		460
Michel Hurfin		✓	✓		✓		6
Jean-François Lalande	✓	✓	✓		✓	✓	252 +56*
Guillaume Piolle	✓	✓	✓	✓	✓	✓	186
Frédéric Tronel	✓	✓	✓	✓	✓	✓	287
Valérie Viet Triem Tong	✓	✓	✓	✓	✓	✓	105 105*

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

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;
- 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.

10.2.2 Supervision

Emmanuelle Anceaume co-supervises the following PhD students:

- Mohamed Aimen Djari, *Etude du potentiel des approches à base de graphe et de preuves de possession pour les cryptomonnaies avec ou sans permission.* Co-supervised by Emmanuelle Anceaume (50%) and Sara Tucci, CEA (50%). PhD Defended on December 2022.
- Arthur Rauch, *Stockage frugal pour la blockchain du futur.* Co-supervised by Emmanuelle Anceaume (50%) and Davide Frey (50%). Started Oct. 2021
- Vincent Kowalski, *Transition de systèmes fermés à systèmes ouverts pour des abstractions de type Byzantine-FT.* Co-supervised by Emmanuelle Anceaume (33%), Achour Mostefaoui (33%), and Matthieu Perrin (33%). Started Nov. 2021.

Guillaume Hiet co-supervises the following PhD students:

- Lionel Hemmerlé , Conception et implémentation d'un langage dédié à l'introspection d'une machine virtuelle au sein d'un hyperviseur, started November 2022, supervised by Guillaume Hiet (25%), Pierre Wilke (25%), Frédéric Tronel (25%) and Jean-Christophe Prévotet (25%).

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

- 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%).

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

Jean-François Lalande co-supervises the following PhD students:

- 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).

- Jean-Marie Mineau, Android Malware Manipulation for Improved Investigations, supervised by Jean-Francois Lalande (75%), Valérie Viet Triem Tong (25%).

Ludovic Mé co-supervises the following PhD students:

- 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%).

- 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%).

- 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%).

Valérie Viet Triem Tong co-supervises the following PhD students:

- 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%). Tomas Conception Miranda defended his Phd at the end of 2022.

- Aimad Berady, characterization of an advanced attacker, co-supervised with Gilles Guette. Aimad Berady defended his Phd at the end of 2022.

- Vincent Raulin, Machine Learning approaches to boost malware detection/classification supervised by Yufei Han (25%), Valérie Viet Triem Tong (25%), Pierre-François Gimenez (33%).

- Pierre-Victor Besson, automatic design of vulnerable architectures, started in october 2020, supervised by Erwan Abgrall (33%), Valérie Viet Triem Tong (33%), Gilles Guette (33%), Guillaume Piolle(33%) .
- Helene Orsini, Adversarially robust and interpretable Machine Leanring pipeline for network intrusion detection systems, supervised by Yufei Han (50%), Valérie Viet Triem Tong (25%), David Lubicz (25%).
- Natan Talon, Towards automatic pentesting with the help of re-enforcement learning. supervised by Valérie Viet Triem Tong (33%), Gilles Guette (33%), Yufei Han (33%), Mathieu Jaume (33%).
- Jean-Marie Mineau, Android Malware Manipulation for Improved Investigations, supervised by Jean-Francois Lalande (75%), Valérie Viet Triem Tong (25%).

10.2.3 Juries

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

- Jean-Yves Zié Diali, *Fast and Scalable Blockchain for Mobile e-payment Solutions*, phD thesis delivered by INSA Centre Val de Loire, supervized by M. Benjamin Nguyen, M. Jérémy Briffaut, M. Ivan Bedini. Jury committee: Reviewers: M. Nicolas Anciaux, M. Jean-François Lalande. Examiners: Mme Chirine Ghedira-Guegan.
- M. Christophe Guerber, delivered by INSA de Toulouse, supervized by Mickaël Royer. Jury commitee: Reviewers: Mme Thi Mai Trang Nguyen, M. Rida Khatoun. Jury commitee: M. Serge Chaumette, M. Jean-François Lalande, M. Vincent Nicomette.

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

- Remi Badonnel, *Managing Security for the Cyber-Space – From Smart Monitoring to Automated Configuration –*. Habilitation delivered by Université de Lorraine.

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

- Arnaud Rossay, *Détection d'intrusions dans les objets connectés par des techniques d'apprentissage automatique*, Le Mans Université.

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

- Pierre-Marie JUNGES, *Evaluation à l'échelle de l'Internet de la Sécurité des Objets Connectés*, phD thesis delivered by Université de Lorraine, supervized by Jerome Francois and Olivier Festor

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

- M. Romain Cayre,*Offensive and defensive approaches for wireless communication protocols security in IoT* delivered by INSA de Toulouse, supervized by Mohamed Kaâniche et de Guillaume Auriol.

Emmanuelle Anceaume was reviewer of the PhD committee for the following PhD theses:

- Zeinab Nehaï, *Formalisation and verification of blockchain systems*, delivered by the University Paris Cité, supervised by Hugues Fauconnier and Francois Bobot.
- Arnaud Favier, *Eventual leader elctions in dynamic networks*, supervised by Pierre Sens.
- Marianna Belotti, *Game theoretical analysis of blockchain users' behaviors*, supervised by Maria Potop Butucaru and Stefano Secci.

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

- Jean-Philippe Eisenbarth, *Analyse, valorisation et protection des réseaux pair-à-pair de blockchains publiques*, supervised by Thibault Cholez and Olivier Perrin.

10.3 Popularization

- Jean-François Lalande has participated to the program "1 scientifique - 1 classe : Chiche !" in Lycée Saint Louis of Saumur, for 5 classes, in March 2022.
- Valérie Viet Triem Tong has participated to the program "1 scientifique - 1 classe : Chiche !" in Lycée Simone Veil of Liffré, for 5 classes, in March 2022 and for 7 classes in November 2022
- Valérie Viet Triem Tong has participated to the program "Girls Can Code" organized at EPITA in November 2022

11 Scientific production

11.1 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.

11.2 Publications of the year

International journals

[2] A. Berady, M. Jaume, V. Viet Triem Tong and G. Guette. 'PWNJUTSU: A dataset and a semantics-driven approach to retrace attack campaigns'. In: *IEEE Transactions on Network and Service Management*. Special Issue on Recent Advances in Network Security Management (2022), pp. 1–13. DOI: 10.1109/TNSM.2022.3183476. URL: https://hal.inria.fr/hal-03694719.

[3] D. Bosk, D. Frey, M. Gestin and G. Piolle. 'Hidden Issuer Anonymous Credential'. In: *Proceedings on Privacy Enhancing Technologies* 2022 (June 2022), pp. 571–607. DOI: 10.56553/popets-2022-0123. URL: https://hal.archives-ouvertes.fr/hal-03789485.

[4] T. Concepción Miranda, P.-F. Gimenez, J.-F. Lalande, V. Viet Triem Tong and P. Wilke. 'Debiasing Android Malware Datasets: How Can I Trust Your Results If Your Dataset Is Biased?' In: *IEEE Transactions on Information Forensics and Security* 17 (3rd June 2022), pp. 2182–2197. DOI: 10.1109/tifs.2022.3180184. URL: https://hal.inria.fr/hal-03700082.

[5] N. Daoudi, K. Allix, T. Bissyandé and J. Klein. 'Assessing the opportunity of combining state-of-the-art Android malware detectors'. In: *Empirical Software Engineering* 28.2 (24th Dec. 2022), p. 22. DOI: 10.1007/s10664-022-10249-9. URL: https://hal.archives-ouvertes.fr/hal-03925375.

[6] O. Koucham, S. Mocanu, G. Hiet, J.-M. Thiriet and F. Majorczyk. 'Cross-domain Alert Correlation methodology for Industrial Control Systems'. In: *Computers and Security* 118.July (29th Apr. 2022), p. 102723. DOI: 10.1016/j.cose.2022.102723. URL: https://hal.archives-ouvertes.fr/hal-03636549.

[7] F. Robin, B. Sericola, E. Anceaume and Y. Mocquard. 'Stochastic analysis of rumor spreading with multiple pull operations'. In: *Methodology and Computing in Applied Probability* 24 (2022), pp. 2195–2211. URL: https://hal.archives-ouvertes.fr/hal-03128118.

[8] N. Sourbier, K. Desnos, T. Guyet, F. Majorczyk, O. Gesny and M. Pelcat. 'SECURE-GEGELATI Always-On Intrusion Detection through GEGELATI Lightweight Tangled Program Graphs'. In: *Journal of Signal Processing Systems* (2022). DOI: 10.1007/s11265-021-01728-1. URL: https://hal.archives-ouvertes.fr/hal-03593545.

International peer-reviewed conferences

[9] E. Anceaume, A. Djari and S. Tucci-Piergiovanni. 'An agent-based simulation study of Sycomore ++ , a scalable and self-adapting graph-based permissionless distributed ledger'. In: The 37th ACM/SIGAPP Symposium On Applied Computing (SAC). Virtual, France, 23rd Apr. 2022. URL: https://hal.archives-ouvertes.fr/hal-03589399.

[10] H. Bao, Y. Han, Y. Zhou, Y. Shen and X. Zhang. 'Towards understanding the robustness against evasion attack on categorical inputs'. In: ICLR 2022 - 10th International Conference on Learning Representations. Virtual Event, France, 25th Apr. 2022. URL: https://hal.inria.fr/hal-03893480.

[11] N. Bellec, G. Hiet, S. Rokicki, F. Tronel and I. Puaut. 'RT-DFI: Optimizing Data-Flow Integrity for Real-Time Systems'. In: ECRTS 2022 - 34th Euromicro Conference on Real-Time Systems. 34. Modène, Italy, 28th June 2022, pp. 1–24. DOI: 10.4230/LIPIcs.ECRTS.2022.18. URL: https://hal.inria.fr/hal-03641576.

[12] A. Djari, E. Anceaume and S. Tucci-Piergiovanni. 'Simulation study of Sycomore ++ , a self-adapting graph-based permissionless distributed ledger'. In: Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). Paris, France, 27th Sept. 2022. URL: https://hal.archives-ouvertes.fr/hal-03637382.

[13] A. Djari, E. Anceaume and S. Tucci-Piergiovanni. 'Sycomore ++ , un registre distribué orienté graphe auto-adaptatif'. In: AlgoTel 2022 - 24èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications. Saint-Rémy-Lès-Chevreuse, France, 30th May 2022, pp. 1–4. URL: https://hal.archives-ouvertes.fr/hal-03656546.

[14] H. Fargier, P.-F. Gimenez, J. Mengin and B. N. L. Nguyen. 'The complexity of unsupervised learning of lexicographic preferences'. In: MPREF 2022 - 13th Multidisciplinary Workshop on Advances in Preference Handling. Vienne, Austria, 23rd July 2022, pp. 1–8. URL: https://hal.inria.fr/hal-03784693.

[15] M. Naseri, Y. Han, E. Mariconti, Y. Shen, G. Stringhini and E. de Cristofaro. 'Cerberus: Exploring Federated Prediction of Security Events'. In: CCS '22 - ACM SIGSAC Conference on Computer and Communications Security. Los Angeles CA, United States: ACM, 7th Nov. 2022, pp. 2337–2351. DOI: 10.1145/3548606.3560580. URL: https://hal.inria.fr/hal-03893491.

[16] H. Orsini, H. Bao, Y. Zhou, X. Xu, Y. Han, L. Yi, W. Wang, X. Gao and X. Zhang. 'AdvCat: Domain-Agnostic Robustness Assessment for Cybersecurity-Critical Applications with Categorical Inputs'. In: BigData 2022 - IEEE International Conference on Big Data. Osaka, Japan: IEEE, 17th Dec. 2022, pp. 1–13. URL: https://hal.inria.fr/hal-03893496.

[17] Y. Shen, Y. Han, Z. Zhang, M. Chen, T. Yu, M. Backes, Y. Zhang and G. Stringhini. 'Finding MNEMON: Reviving Memories of Node Embeddings'. In: CCS 2022 - ACM SIGSAC Conference on Computer and Communications Security. Los Angeles CA, United States: ACM, 7th Nov. 2022, pp. 2643–2657. DOI: 10.1145/3548606.3559358. URL: https://hal.inria.fr/hal-03893484.

[18] 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: IEEE, 22nd May 2022, pp. 1–22. URL: https://hal.inria.fr/hal-03482156.

[19] N. Sourbier, J. Bonnot, 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, 9th July 2022, pp. 1–4. DOI: 10.1145/3520304.3529008. URL: https://hal.archives-ouvertes.fr/hal-03699228.

National peer-reviewed Conferences

[20] T. Concepción Miranda, J.-F. Lalande, V. Viet Triem Tong and P. Wilke. 'DaViz: Visualization for Android Malware Datasets'. In: RESSI 2022 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information. Chambon-sur-Lac, France, 10th May 2022, pp. 1–3. URL: https://hal.inria.fr/hal-03709062.

Conferences without proceedings

[21] R. Brisse, F. Majorczyk, S. Boche and J.-F. Lalande. 'Enhancing security investigations with exploration recommendation'. In: THCon 2022 - Toulouse Hacking Convention. Toulouse, France, 14th Apr. 2022. URL: https://hal.inria.fr/hal-03648192.

[22] M. Lanvin, P.-F. Gimenez, Y. Han, F. Majorczyk, L. Mé and É. Totel. 'Detecting APT through graph anomaly detection'. In: RESSI 2022 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information. Chambon-sur-Lac, France, 10th May 2022, pp. 1–3. URL: https://hal.science/hal-03675346.

[23] V. Raulin, P.-F. Gimenez, Y. Han and V. Viet Triem Tong. 'Towards a Representation of Malware Execution Traces for Experts and Machine Learning'. In: RESSI 2022 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information. Chambon-sur-Lac, France, 10th May 2022, pp. 1–3. URL: https://hal.archives-ouvertes.fr/hal-03675366.

[24] A. Schoen, G. Blanc, P.-F. Gimenez, Y. Han, F. Majorczyk and L. Mé. 'Towards generic quality assessment of synthetic traffic for evaluating intrusion detection systems'. In: RESSI 2022 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information. Chambon-sur-Lac, France, 10th May 2022, pp. 1–3. URL: https://hal.archives-ouvertes.fr/hal-03675359.

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

[25] M. Lanvin, P.-F. Gimenez, Y. Han, F. Majorczyk, L. Mé and E. Totel, eds. *Errors in the CICIDS2017 dataset and the significant differences in detection performances it makes*. 2023, pp. 1–16. URL: https://hal.science/hal-03775466.

Doctoral dissertations and habilitation theses

[26] A. Berady. 'Understanding sophisticated threats: Intentions, moyens, manières et connaissances convergentes des adversaires'. CentraleSupélec, 10th Nov. 2022. URL: https://theses.hal.science/tel-03861429.

Reports & preprints

[27] F. Castella, B. Sericola, E. Anceaume and Y. Mocquard. *Continuous-time stochastic analysis of rumor spreading with multiple operations*. 30th May 2022. URL: https://hal.archives-ouvertes.fr/hal-03681995.

[28] A. Djari, Y. Amoussou-Guenou, E. Anceaume, S. Tucci Piergiovanni and A. D. Pozzo. *Yggdrasil: Secure State Sharding of Transactions and Smart Contracts that Self-adapts to Transaction Load*. 6th Oct. 2022. URL: https://hal.archives-ouvertes.fr/hal-03793291.

[29] A. Jain, E. Anceaume and S. Gujar. *Extending The Boundaries and Exploring The Limits Of Blockchain Compression*. 2nd May 2022. URL: https://hal-cnrs.archives-ouvertes.fr/hal-03866741.

Other scientific publications

[30] S. Wendzel, L. Caviglione, A. Mileva, J.-F. Lalande and W. Mazurczyk. 'Guest editorial: Information security methodology and replication studies'. In: *Information Technology* (5th Apr. 2022), pp. 1–3. DOI: 10.1515/itit-2022-0016. URL: https://hal.inria.fr/hal-03629524.