Loïc Miller

loic.miller@irisa.fr Scholar HAL ORCID
https://loicmiller.com/

Education

2018 – 2022 **PhD – University of Strasbourg**, Computer Science, Strasbourg.
Securing Workflows: On the Use of Microservices and Metagraphs to Prevent Data Exposures. Supervised by Prof. Cristel Pelsser and Prof. Antoine Gallais. Co-supervised by Associate Prof. Pascal Mérindol. Thesis carried out in the Networks team of the ICube laboratory (UMR7357), and defended on April 22, 2022 before the following jury:

- *Cristel Pelsser*, Professor at the Catholic University of Louvain,
- *Antoine Gallais*, Professor at INSA Hauts-de-France,
- *Géraldine Texier*, Professor at IMT Atlantique (chair and reviewer),
- *Etienne Rivière*, Professor at the Catholic University of Louvain (reviewer),
- *Sébastien Tixeuil*, Professor at Sorbonne University,
- *Gregory Blanc*, Associate Professor at Télécom SudParis,
- External guest: *Matthew Roughan*, Professor at the University of Adelaide

2016 – 2018 **MSc in computer science – Computer networks and embedded systems**, University of Strasbourg.
Analysis of the BGP protocol leading to several new attack vectors, and implementation of a detection tool. Supervised by Prof. Cristel Pelsser and Associate Prof. Stéphane Cateloin. Graduated with honors.

Experience

2025 – · · · · **Associate Professor**, CentraleSupélec, Rennes.
Blockchain scalability for the design of digital currencies.

2023 – 2025 **Postdoctoral Researcher**, IMT Atlantique, Rennes
Design and implementation of non-interactive proofs of proof-of-work in a variable difficulty environment for blockchain scalability. Supervised by Associate Prof. Romaric Ludinard (IMT Atlantique, IRISA) and Prof. Emmanuelle Anceaume (CNRS, IRISA).

2022 – 2023 **Postdoctoral Researcher**, IMT Atlantique, Rennes
Study on the use of blockchain in collaborative cybersecurity systems. Supervised by Prof. Marc-Oliver Pahl (Cybersecurity for Critical Networked Infrastructures Chair – Cyber CNI).

2018 – 2022 **PhD Student**, University of Strasbourg, Strasbourg
Securing Workflows: On the Use of Microservices and Metagraphs to Prevent Data Exposures.

Teaching

2024 – 2025
- **Internet Network Administration**, ISTIC, Master 2 – 3h Lecture.
- **Blockchain and Consensus**, IMT Atlantique, 2nd-3rd year – 3h Lecture.
- **Blockchain Principles and Applications**, ISTIC, Master 2 – 3h Tutorial.
- **Network Routing**, ESIR, 2nd year – 16.5h Lec., 3h Tut., 22.5h Lab.
- **Network Security**, ISTIC, Master 2 – 18h Lab.

2023 – 2024
- **Internet Network Administration**, ISTIC, Master 2 – 3h Lecture.

Teaching (continued)

2021 – 2022
- **Inter-Domain Routing**, Univ. of Strasbourg, Master 1 – 14h Lab.

2019 – 2020
- **Data Structures and Algorithms 1**, Univ. of Strasbourg, Bachelor 2 – 22h Tutorial.
- **Computer Architecture Basics**, Univ. of Strasbourg, Bachelor 1 – 10h Tut., 24h Lab.

2018 – 2019
- **Data Structures and Algorithms 2**, Univ. of Strasbourg, Bachelor 2 – 24h Tutorial.
- **Computer Culture and Practice**, Univ. of Strasbourg, Bachelor 1 – 28h Lab.

Tutoring

2024 – · · · ·
- **Dorian Pacaud**, *Towards blockchain frugality.*
  IMT Atlantique, PhD. Supervised with Romaric Ludinard (IMT Atlantique) and Emmanuelle Anceaume (CNRS, IRISA).

2023 – 2024
- **Nathanaël Derousseaux**, *Implementation of non-interactive proofs of proof-of-work in a dynamic setting.*
  Univ. of Strasbourg, Master 2 end-of-study internship. Supervised with Romaric Ludinard (IMT Atlantique) and Emmanuelle Anceaume (CNRS, IRISA).
- **Dorian Pacaud**, *Blockchain scalability.*
  Univ. Rennes 1, Master 2 end-of-study internship. Supervised with Romaric Ludinard (IMT Atlantique) and Emmanuelle Anceaume (CNRS, IRISA).

2022 – 2023
- **Benjamin Loison**, *Design and implementation of non-interactive proofs of proof-of-work in a dynamic setting.*
  ENS Paris-Saclay, Master 2 end-of-study internship. Supervised with Romaric Ludinard (IMT Atlantique) and Emmanuelle Anceaume (CNRS, IRISA).

2019 – 2020
- **Lucas Braun**, *Internet routing security.*
  Developed a BGP attack detection tool. Univ. of Strasbourg, Master 1 research project. Supervised with Jean-Romain Luttringer (Univ. of Strasbourg).
- **Philippe Chevalier**, *Internet routing security.*
  Explored inter-domain routing security. Univ. of Strasbourg, Master 1 research project. Supervised with Jean-Romain Luttringer (Univ. of Strasbourg).

Research coordination

Organization
- Web chair IMC'22.
  Member of the organizing committee for AlgoTel/CoRes'24.
  Logistical support for RESSI'25 – reception, guidance, and assistance.
  Management of the SOTERN (IRISA) team website.
  Assistance in organizing the CyberCNI chair for European Cyber Week (ECW'23).
  Moderation of roundtable discussions with CyberCNI industrial partners.
  CyberCNI Talks (moderation of online presentations).
  Workshops of the Networks team (ICube).

Outreach
- Talk "Blockchain and its use in collaborative cybersecurity systems" at the 2023 Spring school of EUR CyberSchool.

Reviews
- PAM'19, IMC'19, CoNEXT'19, BRAINS'24, JNSM'24-25, NCA'24, ICDCIT'24, CNSM'25.

Publications

Peer-reviewed international journals

1. R. Gil-Pons, M. Ward, and **L. Miller**, "Finding (s,d)-hypernetworks in f-hypergraphs is np-hard," *Information Processing Letters*, vol. 184, p. 106 433, 2024, ISSN: 0020-0190. DOI: `https://doi.org/10.1016/j.ipl.2023.106433`.

2. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “Securing workflows using microservices and metagraphs,” *Electronics*, vol. 10, no. 24, p. 3087, 2021.

Peer-reviewed international conferences

1. **L. Miller**, D. Pacaud, N. Derousseaux, E. Anceaume, and R. Ludinard, “Mining in logarithmic space with variable difficulty,” in *ACM Conference on Computer and Communications Security (CCS)*, CORE rank: **A***, 2025.
2. B. Loison, “Mining in logarithmic space with variable difficulty,” in *2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 2023, pp. 1–4. 🔗 DOI: 10.1109/BRAINS59668.2023.10317023.
3. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “Towards secure and leak-free workflows using microservice isolation,” in *2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)*, IEEE, 2021, pp. 1–5. 🔗 DOI: 10.1109/HPSR52026.2021.9481820.
4. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “Verification of cloud security policies,” in *2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)*, IEEE, 2021, pp. 1–5. 🔗 DOI: 10.1109/HPSR52026.2021.9481870.
5. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “Securing workflows using the microservices architecture,” in *Proceedings of the Network Traffic Measurement and Analysis Conference (TMA)*, Poster, Paris, France: TMA, Jun. 2019.
6. **L. Miller** and C. Pelsser, “A taxonomy of attacks using bgp blackholing,” in *European Symposium on Research in Computer Security*, CORE rank: **A**, Springer, 2019, pp. 107–127.

Peer-reviewed national conferences

1. D. Pacaud, **L. Miller**, E. Anceaume, and R. Ludinard, “Preuves non-interactives : La nouvelle ère des chaînes compressées,” in *ALGOTEL 2025—27èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications*, 2025.
2. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “De l’utilisation des métagraphes pour la vérification de politiques de sécurité,” in *ALGOTEL 2021—23èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications*, 2021.
3. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “Protection contre les fuites de données: Un environnement micro-services sécurisé,” in *CORES 2021–6ème Rencontres Francophones sur la Conception de Protocoles, l’Évaluation de Performance et l’Expérimentation des Réseaux de Communication*, 2021.

Other publications

1. **L. Miller** and M.-O. Pahl, *Collaborative cybersecurity using blockchain: A survey*, 2024. arXiv: 2403.04410 [cs.CR]. 🔗 URL: https://arxiv.org/abs/2403.04410.

Teaching in detail

Status	Year	Institution	Audience	Level	Subject	HETD	Class size	Format
Adjunct	2024 – 2025	ISTIC	Master	M2	Internet Network Administration	4.5h	~10	Lecture
Adjunct	2024 – 2025	IMT Atlantique	Master	M2	Blockchain and Consensus	4.5h	23	Lecture
Adjunct	2024 – 2025	ISTIC	Master	M2	Blockchain Principles and Applications	3h	23	Tutorial
Adjunct	2024 – 2025	ESIR	Master	M1	Network Routing	42.75h	12	Lec.,Tut.,Lab
Adjunct	2024 – 2025	ISTIC	Master	M2	Network Security	12h	22	Lab
Adjunct	2023 – 2024	ISTIC	Master	M2	Internet Network Administration	4.5h	~10	Lecture
Adjunct	2021 – 2022	Univ. of Strasbourg	Master	M1	Inter-Domain Routing	9.33h	13	Lab
Adjunct	2019 – 2020	Univ. of Strasbourg	Bachelor	L2	Data Structures and Algorithms 1	22h	52	Tutorial
Adjunct	2019 – 2020	Univ. of Strasbourg	Bachelor	L1	Computer Architecture Basics	26h	30 (~300+)	Tut.,Lab
Adjunct	2018 – 2019	Univ. of Strasbourg	Bachelor	L2	Data Structures and Algorithms 2	16h	~30	Lab
Adjunct	2018 – 2019	Univ. of Strasbourg	Bachelor	L1	Computer Culture and Practice	18.67h	41	Lab
Adjunct	2018 – 2025			L1-M2		163.25h	10-300	Lec.,Tut.,Lab

2024 – 2025

- **Blockchain and Consensus**, IMT Atlantique, 2nd-3rd year – 3h Lec. – 23 students.
  The module "Blockchain and Consensus" is aimed at 2nd and 3rd year students from all engineering tracks at the Rennes campus, in particular the "Digital platforms: technologies and markets" specialization. This training program aims to train engineers on the technical (networks, virtualization, cloud), economic, and legal aspects of digital platforms. The module also welcomes students from the specialized master's degree in cybersecurity, co-organized by IMT Atlantique and CentraleSupélec. More specifically, this module presents the fundamental concepts of blockchains – the principles of distributed systems (processes, communication, failures), consensus mechanisms, as well as smart contract development with the Solidity language.
  In this module, I delivered a 3h lecture on the topic of sharding in blockchains, for which I created the course materials. The content was designed with a heterogeneous audience in mind, accessible to 2nd-year students while offering a deeper level for 3rd-year students. I first presented the issues of blockchain scalability (e.g. throughput), the metrics and trade-offs associated with these issues, then the concept of sharding and its variants. I also detailed several solutions (Elastico, RapidChain) and presented forms of sharding in different contexts (public/private blockchains, permissioned or not).
- **Blockchain Principles and Applications**, ISTIC, Master 2 – 3h Tut. – 23 students.
  The module "Blockchain Principles and Applications" is intended for M2-level students following the "Hardware and software security" track of the Cybersecurity master's program offered by the CyberSchool, a graduate school in cybersecurity. The aim of this module is to present blockchain technology as well as its main applications, to give students the necessary elements to understand the differences between blockchain variants, understand their strengths and weaknesses, and finally decide whether one of these variants is relevant to solve a given problem. The first part of the course focuses on applications, e.g. digital currency, distributed ledger, smart contracts, while the second part focuses on the components of blockchain, e.g. cryptography, consensus algorithms.
  As part of this module, I substituted for Romaric Ludinard, one of the instructors of this course, for the duration of a 3h tutorial. The tutorial aimed to lead students to reflect on how to specify and implement a self-managed system for coffee management at IMT Atlantique.

Teaching in detail (continued)

- **Network Routing**, ESIR, 2nd year – 16.5h Lec., 3h Tut., 22.5h Lab – 12 students.
  The module "Network Routing" is aimed at 2nd-year ESIR students, specializing in Digital Systems and Networks (equiv. M1). It aims to provide students with knowledge and practice of routing technologies. In particular, this module first covers graph theory (Bellman-Ford, Dijkstra). It then covers intra-domain routing protocols (RIP, OSPF), and operator networks (BGP, MPLS, BGP/MPLS VPNs). The module is completed with a treatment of BGP security, multicast routing, and ad hoc network routing.
  For this module, I delivered 16.5 hours of lectures, 3 hours of tutorials, and 22.5 hours of lab work. As part of the labs, I once again set up the mini-Internet infrastructure from ETH Zurich (see 2021–2022 Inter-Domain Routing for more details). In short, the mini-Internet is a virtual teaching platform that reproduces the practical functioning of the Internet on a reduced scale. I was able to make this platform available to students thanks to the generous support of Mathieu Goessens and the ISTIC-ESIR administration team. The supporting material for the labs can be found here. The module covers the RIP, OSPF, BGP, and MPLS protocols, with a particular focus on BGP security and BGP/MPLS VPNs. We also cover multicast routing. Assessment was based on a final lab report, which I prepared by combining the ETH assignment with one I had previously created for the University of Strasbourg. The module was also evaluated with a final exam, which I fully designed, organized and graded.
- **Network Security**, ISTIC, Master 2 – 18h Lab – 22 students.
  The module "Network Security" is aimed at M2-level students in information mathematics and cryptography. It is designed to provide students with advanced skills in network security. The course combines elements of cybersecurity and cryptography, with a particular focus on securing communications and analyzing threats in computer networks. Students are introduced to concepts such as VLAN management, IPsec, IDS/IPS, as well as the use of tools like nmap, Burp Suite, and Pfsense. The labs allow students to explore practical scenarios, such as securing routers and switches, implementing IPsec and VPNs, and performing network vulnerability analysis.
  I contributed to this module by supervising a lab group, creating lab materials, and conducting assessment through two graded lab sessions.

2023 – 2025

- **Internet Network Administration**, ISTIC, Master 2 – 3h Lec. – ~10 students.
  The module "Internet Network Administration" covers the essential protocols for network administration, with a particular focus on TCP/IP protocols, routing (RIP, OSPF, BGP), as well as other protocols such as DHCP and LDAP. Students are introduced to the principles of dynamic routing and the algorithms for computing optimal paths. The objective is to provide them with a deep understanding of the mechanisms underlying network operation and the protocols used for management and communication.
  In this module, I delivered 3 hours of lectures covering routing protocols (RIP, OSPF, BGP) and path calculation algorithms (Bellman-Ford, Dijkstra), finishing with a section on BGP attacks. I also prepared the lecture materials for this course.

Teaching in detail (continued)

2021 – 2022 **Inter-Domain Routing**, Univ. of Strasbourg, Master 1 – 14h Lab – 13 students.

The module “Inter-Domain Routing” is aimed at M1-level networking students preparing for careers in network administration or design. It covers the essential mechanisms underlying Internet operation, including the BGP protocol used between autonomous systems, as well as traffic engineering techniques such as MPLS, SR, and BGP/MPLS VPNs. The goal is to enable students to configure basic operator network services, diagnose issues in complex inter-networks, and implement traffic engineering strategies. This module has a strong practical component through the use of emulated equipment on a software platform (mini-Internet) to study real-world scenarios.

In this module, I supervised a lab group. I designed the lab sessions in collaboration with Jean-Romain Luttringer. Together, we carried out the first adaptation of the mini-Internet for the University of Strasbourg, replacing the labs previously based on GNS3. Originally developed at ETH Zurich, the mini-Internet is a virtual teaching platform that reproduces the practical functioning of the Internet on a reduced scale. Hosted on a single server, it simulates a complete network composed of routers, switches, and hosts distributed across multiple autonomous systems (AS). Each component runs in a Linux container accessible remotely via SSH. This setup allows students to manage their own AS and collaborate to establish global Internet connectivity, providing a practical and realistic approach that deepens their understanding of Internet infrastructure operations and challenges.

To adapt the mini-Internet for Strasbourg, we handled deployment of the platform, designed the lab sessions, and created a project (network topology, exercises, grading, etc.) tailored to our students. The sessions covered BGP, MPLS, and BGP-MPLS VPNs. Additionally, we created a section on BGP hijacks used for the graded lab, and a section on DDoS and BGP poisoning for the substitute graded lab. Some of the supporting materials are available online here. During the lab sessions, my group and I also provided explanations of theoretical concepts and protocols (BGP, MPLS) and conducted the evaluation of graded labs and projects in coordination with Jean-Romain’s group. The mini-Internet platform and the supervision were highly appreciated by the students.

2019 – 2020 **Data Structures and Algorithms 1**, Univ. of Strasbourg, Bachelor 2 – 22h Tut. – 52 students.

The module “Data Structures and Algorithms 1” is aimed at L2-level students and is designed to provide a deep understanding of fundamental concepts in algorithms and data structures. It covers classic structures (i.e., arrays, linked lists, stacks, queues) as well as sorting, searching, and optimization algorithms. This module also introduces the concept of algorithmic complexity.

I delivered the tutorial sessions for this module, which focused mainly on specifying classic data structures and understanding complexity. I participated in module assessment, handled make-up sessions, and prepared the materials for each tutorial.

Teaching in detail (continued)

Computer Architecture Basics, Univ. of Strasbourg, Bachelor 1 – 10h Tut., 24h Lab – 30 (~300+) students.
The module "Computer Architecture Basics" is aimed at L1-level students and is designed to provide the essential foundations for understanding how computer systems operate. It covers information representation, such as encoding numbers, characters, and other data types, as well as their computational processing, including arithmetic operations and associated manipulations. The module also explores the fundamentals of computer architecture, including the Von Neumann architecture, the role of the processing unit, memory management, and input/output. An introduction to machine and assembly languages bridges the gap between hardware architecture and low-level programming.
I contributed to this module by supervising two lab groups and one tutorial group. The tutorial and lab sessions were based on the use of a simple processor called Cardiac, whose mechanisms mirror those of modern processors. Tutorial sessions included exercises on a paper version of Cardiac to explore memory, the accumulator, and instruction execution. These tutorials were followed by practical sessions on the Cardiac software simulator, where students wrote and executed assembly programs. During this module, I conducted the assessment of my groups through a graded lab and participated in the evaluation of the final exam for the entire cohort (300+ students). I also prepared additional materials to support each tutorial/lab in the form of slides.

2018 – 2019

Data Structures and Algorithms 2, Univ. of Strasbourg, Bachelor 2 – 24h Lab – ~30 students.
The module "Data Structures and Algorithms 2" is aimed at L2-level students and provides an in-depth study of relational data structures, i.e., tables (calculated, associative, hashed addressing), trees (binary, balanced, B-trees), and graphs (directed, undirected, acyclic). The algorithms covered include sorting algorithms as well as graph algorithms such as graph traversal, Warshall's algorithm, and Tarjan's algorithm.
I conducted lab sessions for two groups of approximately fifteen students, in which they implemented various sorting methods, data structures, and graph algorithms using the C programming language.

Computer Culture and Practice, Univ. of Strasbourg, Bachelor 1 – 28h Lab – 41 students.
The module "Computer Culture and Practice" is aimed at L1-level students and is designed to provide basic computing skills, particularly in interacting with the operating system, using the shell, and writing shell scripts. Students learn to navigate a Unix/Linux environment, execute terminal commands, and automate tasks using shell scripts.
I supervised two lab groups, where students explored these concepts through practical exercises, using system commands to manage files, run programs, and automate processes via shell scripts. I also prepared lab materials, graded the exercises, and conducted assessments through two graded lab sessions.

Research activities

In this section, I provide an overview of my research activities since my master's thesis internship. I have addressed various problems, all revolving around the theme of **security in distributed systems**. In particular, I have investigated:

- Securing the Border Gateway Protocol (**BGP**), the de facto inter-domain routing protocol.
- Securing multi-party **workflows** to prevent data leaks.
- The security of **non-interactive proof-of-work proofs** in blockchains.

The rest of this section details these contributions along these three axes.

Research activities (continued)

BGP attacks

These works were carried out during my master's thesis internship. We studied BGP blackholing, a technique commonly used to protect against distributed denial-of-service (DDoS) attacks. Blackholing is triggered by the victim of the DDoS attack, requesting neighboring autonomous systems (ASes) to drop traffic destined for the targeted IP addresses. Although designed as a defensive measure, attackers can abuse it by sending requests for IP addresses they do not own. This misuse turns a protective mechanism into an attack vector. These results were published in [12].

We developed a taxonomy of **attacks combining route hijacks and blackholing misuse**, which we called BGP blackjacks, a contraction of blackhole hijacks. We demonstrated that these attacks allow an attacker to achieve wider impact and reach, as well as increased stealth compared to classic hijacks. We also argued the effectiveness of these attacks in different security environments (RPKI, BGPsec), showing their impact and adaptability to current configurations. Finally, we studied the limitations of BGP security mechanisms, which are insufficient against some of these attacks, and proposed new mechanisms to better protect or mitigate the effects of blackjacks. These works highlight emerging threats to Internet infrastructure, intended for network operators and researchers in network security, contributing to stronger inter-domain routing security.

Specifically, we proposed a detailed classification of blackjack attacks. The attack type depends on the manipulation of the BGP path, affected prefixes, and how diverted traffic is handled. We defined "Type-0 blackjacks", which involve re-originating a legitimate prefix of the victim AS, including a blackholing community in the re-originated message that triggers this protection measure in a targeted AS. This provides two advantages:

- **Reach –** The attacker can potentially remove more traffic by causing another AS to drop it, compared to a simple hijack. Moreover, blackhole communities take precedence over AS path length in BGP path selection. By specifying the AS to perform blackholing, the attacker can target the victim's traffic precisely.

- **Stealth –** Since the attacker AS does not drop the traffic directly, it is stealthier than other traffic-removal methods. Detecting the attacker via BGP messages is possible but difficult, as the routers involved are likely outside the victim AS network.

We also defined "Type-N blackjacks", in which the attacker does not re-originate the targeted prefix but simulates a link (that does not exist) with the victim AS. For example, simulating a direct link to the victim yields a Type-1 blackjack; simulating a link two hops away yields Type-2, and so on. This attack is interesting because it completely negates the benefits of RPKI, which verifies that the origin AS is authorized to announce the prefix. Type-0 blackjacks are thus blocked by RPKI. Note that RPKI deployment is far from complete, and few ASes filter routes based on it.

The final type, "Type-U blackjack", involves an attacker AS already present on the path of a legitimate BGP advertisement. The attacker does not modify the AS path and does not strictly hijack the route but still adds the blackhole community when relaying the advertisement. This attack is stealthier than the others since the path is unmodified.

We then evaluated the impact of these attacks in various routing security deployment scenarios:

- **No security –** ASes use neither RPKI nor BGPsec.
- **Partial RPKI –** Some ASes use RPKI, but no AS uses BGPsec.
- **Full RPKI –** All ASes use RPKI, but no AS uses BGPsec.
- **Partial BGPsec –** Some ASes use both RPKI and BGPsec; others use either only RPKI or no security mechanism.
- **Full BGPsec –** All ASes use both RPKI and BGPsec.

For each attack in each scenario, we assessed whether the deployment resisted the attack or whether other factors (network topology, etc.) mattered. We also considered whether the attack targeted the prefix directly or a subprefix of the victim. We concluded that current BGP security mechanisms are highly inadequate against blackjack attacks. RPKI only protects the origin and does not always cover subprefixes, while BGPsec validates paths but does not secure communities, remains vulnerable to downgrade attacks, and is not yet deployed.

Research activities (continued)

To mitigate these attacks, we recommend best practices such as adding verification rules for directly connected ASes and filtering insufficiently specific announcements. We also propose extending BGPsec to authenticate communities. These measures would reduce abuse and allow tracing the origin of malicious blackholing requests, holding responsible actors accountable.

Securing multi-party workflows

These works were conducted during my PhD. As companies increasingly adopt cloud services for their processes, data transfer and processing across multiple parties greatly increase the risk of sensitive data exposure. Our work combines a microservices infrastructure with policy verification via metagraph modeling to **ensure confidentiality and data control**.

To prevent actors with access to sensitive data from leaking it during the workflow, we leverage **microservices** isolation to enforce access policies. This infrastructure is implemented in a proof of concept, testing its effectiveness in enforcing specified policies and detecting potential access violations. We then measure performance by integrating policy engines, showing that the cost overhead of authorization remains reasonable relative to the benefits. We also use metagraph-based policy modeling to verify that policy specifications match their implementation. To our knowledge, we are the **first to use metagraphs for access control policy verification**. This approach allows precise modeling, facilitating refinement and detecting implementation errors. We introduce a toolchain to translate and verify policies, especially workflow policies, using Rego, a declarative language for complex policy expression. Performance analysis demonstrates that deployed policies comply with specifications even in complex workflows with many rules.

Infrastructure performance was measured at multiple levels. First, we evaluated the impact of adding the Open Policy Agent (OPA) policy engine on container startup time, collecting 130 observations per pod and deployment (with or without OPA), for $N = 1820$ total. Results were analyzed using a t-test for independent samples ($t(1818) = 43.19$, $p < 0.001$). The effect size ($d = 1.985$) exceeds Cohen's convention for a large effect ($d = 0.80$). Post hoc power analysis shows high statistical power, $1 - \beta > 0.999$. On average, startup time increased by 2 seconds with OPA, about 32% more than without.

Second, we measured request latency between services as a function of policy rule count. A one-way ANOVA was conducted for each communication type (intra-region/inter-region) across five policy sizes: no OPA, allow all, minimal, $+100$ rules, $+1000$ rules. We collected 40 observations per authorized communication per policy level ($N = 1600$ total). For intra-region communications, latency differed significantly among the five scenarios, $F(4, 795) = 364.05, p < 0.001, \eta_p^2 = 0.65$. For inter-region, differences were also significant but smaller, $F(4, 795) = 15.23, p < 0.001, \eta_p^2 = 0.07$. Results show a **negligible impact on latency** even with substantially larger policies.

We then used **metagraphs** to model access control policies in a granular manner. A metagraph generalizes graphs: vertices represent sets of elements (tasks, variables), and edges represent relations or constraints between sets. This approach verifies correct policy application and detects inconsistencies or redundancies. Metagraphs scale efficiently for large rule sets.

Policy verification involves several steps: first, the security policy is specified, then transformed into a metagraph. The implemented policy, encoded as Rego rules, is also transformed into a metagraph. Comparing the specification and implementation metagraphs verifies equivalence, detecting misapplied rules or conflicts. We developed tools for automation at each step.

Policy verification was evaluated by generating random workflows of varying size and complexity. Errors were simulated in the metagraphs to test robustness. A total of $27,000$ policy implementations were generated and compared using metagraphs. Tests showed the verification algorithm is highly effective, even for large, complex workflows.

Performance evaluation showed the algorithm handles complex workflows quickly, with average verification time under 2 seconds for medium-size workflows with 1000 rules. Complexity is dominated by edge sorting and matching, giving $O(m \cdot \log(m))$ complexity, where m is the number of edges. In conclusion, metagraph-based policy verification is both **efficient** and **scalable**, suitable for large-scale systems.

Research activities (continued)

We also studied **redundancy elimination** in policies using metagraphs. In particular, we showed that finding an (s, d)-hypernetwork in F-hypergraphs is NP-hard. These works address the algorithmic complexity of directed hypergraphs, where edges connect sets of vertices. The focus is on (s, d)-hypernetworks, i.e., minimal hypergraph substructures connecting a source node s to a destination node d. We specifically examined F-hypergraphs (where each edge has a tail of cardinality 1), and concluded that finding an (s, d)-hypernetwork in such acyclic hypergraphs is NP-hard. These works have been published in several papers [3], [6], [7], [8], [9], [10], [11].

Blockchain scalability

These works were conducted during my postdoctoral research. Initially, my work was carried out within the industrial chair Cybersecurity for Critical Networked Infrastructures (Cyber CNI). In this context, I interacted with several industrial partners of the chair (Airbus, SNCF, BNP Paribas) to evaluate their needs and assess solutions centered around blockchain. I also conducted a structured literature review addressing the **role of blockchain in collaborative cybersecurity**, aiming to encourage information sharing between organizations to improve security.

Trust management in these systems represents a major challenge. Decentralized solutions, such as blockchain, are essential to eliminate critical single points of failure. However, existing literature on blockchain-based collaborative cybersecurity is limited and lacks in-depth analysis. I addressed this gap by studying the evolution of blockchain usage in collaborative cybersecurity between 2016 and 2023. I explored various applications, trends, and technology developments, focusing on access control, data validation policies, underlying technologies, and consensus mechanisms. In these works [4], I highlight that many contributions select their consensus protocols poorly. To address this, I propose guidelines for choosing the blockchain most suitable to specific solution requirements.

Next, we focused on the problem of **storage scalability** in proof-of-work blockchains. These works were carried out as part of the ANR BC4SSI project, which aims to use blockchain to enable a self-sovereign digital identity system. There is indeed a European-level objective to provide an e-identity accessible from a smartphone, where each individual retains control of their identity data. From a research perspective, while the size of application data in a blockchain is naturally variable, consensus data—which ensures blockchain integrity—must be retained in full. This poses a problem as this data grows linearly, with current sizes around 600 GB for Bitcoin and 1.6 TB for Ethereum.

In this work, we present a **construction for non-interactive proof-of-work proofs (NIPoPoW)**, a compact proof summarizing the work done to build a proof-of-work blockchain. In particular, this NIPoPoW operates in environments with variable mining difficulty, unlike previous constructions assuming constant difficulty. This approach faces several challenges, including defining appropriate sampling levels for blocks of different difficulties and protecting against attacks exploiting low-difficulty blocks. The construction ensures security against a Byzantine adversary controlling less than one-third of computing power, while compressing blockchain data and reducing the number of blocks needed for synchronization. We worked on formal security proofs as well as experimental results showing that the proposed NIPoPoW exponentially reduces the size of the Bitcoin blockchain. The implementation of this construction, and its use on Bitcoin data, can be found online here.

As part of this work, I co-supervised Benjamin Loison during his master's thesis internship at ENS Saclay. A preliminary version of the results was published at BRAINS'23 [5] by Benjamin as part of a student paper. The final version of this work was carried out in collaboration with Nathanaël Derousseaux and Dorian Pacaud during their master's thesis internships at the University of Strasbourg and the University of Rennes 1, respectively. I had the opportunity to supervise Nathanaël and Dorian, the latter continuing into a PhD. The final version of the article [1] was accepted at the CCS'25 conference. A short version was also accepted at the AlgoTel'25 conference [2].

1. **L. Miller**, D. Pacaud, N. Derousseaux, E. Anceaume, and R. Ludinard, “Mining in logarithmic space with variable difficulty,” in *ACM Conference on Computer and Communications Security (CCS)*, CORE rank: **A***, 2025.
2. D. Pacaud, **L. Miller**, E. Anceaume, and R. Ludinard, “Preuves non-interactives : La nouvelle ère des chaînes compressées,” in *ALGOTEL 2025—27èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications*, 2025.
3. R. Gil-Pons, M. Ward, and **L. Miller**, “Finding (s,d)-hypernetworks in f-hypergraphs is np-hard,” *Information Processing Letters*, vol. 184, p. 106 433, 2024, ISSN: 0020-0190. 🔗 DOI: `https://doi.org/10.1016/j.ipl.2023.106433`.
4. **L. Miller** and M.-O. Pahl, *Collaborative cybersecurity using blockchain: A survey*, 2024. arXiv: `2403.04410 [cs.CR]`. 🔗 URL: `https://arxiv.org/abs/2403.04410`.
5. B. Loison, “Mining in logarithmic space with variable difficulty,” in *2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 2023, pp. 1–4. 🔗 DOI: `10.1109/BRAINS59668.2023.10317023`.
6. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “De l’utilisation des métagraphes pour la vérification de politiques de sécurité,” in *ALGOTEL 2021—23èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications*, 2021.
7. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “Protection contre les fuites de données: Un environnement micro-services sécurisé,” in *CORES 2021–6ème Rencontres Francophones sur la Conception de Protocoles, l’Évaluation de Performance et l’Expérimentation des Réseaux de Communication*, 2021.
8. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “Securing workflows using microservices and metagraphs,” *Electronics*, vol. 10, no. 24, p. 3087, 2021.
9. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “Towards secure and leak-free workflows using microservice isolation,” in *2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)*, IEEE, 2021, pp. 1–5. 🔗 DOI: `10.1109/HPSR52026.2021.9481820`.
10. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “Verification of cloud security policies,” in *2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)*, IEEE, 2021, pp. 1–5. 🔗 DOI: `10.1109/HPSR52026.2021.9481870`.
11. **L. Miller**, P. Mérindol, A. Gallais, and C. Pelsser, “Securing workflows using the microservices architecture,” in *Proceedings of the Network Traffic Measurement and Analysis Conference (TMA)*, Poster, Paris, France: TMA, Jun. 2019.
12. **L. Miller** and C. Pelsser, “A taxonomy of attacks using bgp blackholing,” in *European Symposium on Research in Computer Security*, CORE rank: **A**, Springer, 2019, pp. 107–127.