

Loïc Miller

✉ loic.miller@irisa.fr
🌐 <https://loicmiller.com/>

🏠 Scholar

🌐 HAL

🆔 ORCID



Formation universitaire

- 2018 – 2022 **Doctorat – Université de Strasbourg**, Spécialité Informatique, Strasbourg.
Sécuriser les workflows : de l'usage des microservices et des métagraphes pour prévenir les fuites de données. Sous la direction de Cristel Pelsser et Antoine Gallais. Co-encadré par Pascal Mérindol, MCF à l'Université de Strasbourg. Thèse effectuée dans l'équipe Réseaux du laboratoire ICube (UMR7357), et soutenue le 22 avril 2022 devant le jury suivant:
- Cristel Pelsser, Professeure à l'Université Catholique de Louvain,
 - Antoine Gallais, Professeur à l'INSA Hauts-de-France,
 - Géraldine Texier, Professeure chez IMT Atlantique (présidente et rapporteuse),
 - Etienne Rivière, Professeur à l'Université Catholique de Louvain (rapporteur),
 - Sébastien Tixeul, Professeur à Sorbonne Université,
 - Gregory Blanc, Maître de conférences à Télécom SudParis,
 - Invité hors jury : Matthew Roughan, Professeur à l'Université d'Adelaide
- 2016 – 2018 **Master d'informatique – Réseaux informatiques et systèmes embarqués**, Université de Strasbourg.
Manipulation du protocole BGP débouchant sur plusieurs nouveaux vecteurs d'attaque et implémentation d'un outil pour les détecter. Encadré par Cristel Pelsser et Stéphane Cateloin, MCF à l'Université de Strasbourg. Mention bien.

Expérience professionnelle

- 2023 – 2025 **Chercheur post-doctoral**, IMT Atlantique, Rennes.
Conception et implémentation de preuves de travail non-interactives dans un environnement dynamique, pour le passage à l'échelle des blockchains. Sous la supervision de Romaric Ludinard (IMT Atlantique, IRISA) et Emmanuelle Anceaume (CNRS, IRISA).
- 2022 – 2023 **Chercheur post-doctoral**, IMT Atlantique, Rennes.
Étude sur l'utilisation de la blockchain dans les systèmes de cybersécurité collaboratifs. Sous la supervision de Marc-Oliver Pahl (Chaire Cybersécurité des infrastructures critiques – Cyber CNI).
- 2018 – 2022 **Doctorant**, Université de Strasbourg, Strasbourg.
Sécuriser les workflows : de l'usage des microservices et des métagraphes pour prévenir les fuites de données.

Enseignement

- 2024 – 2025 **Administration des Réseaux Internet**, ISTIC, Master 2 – 3h CM.
 Blockchain et Consensus, IMT Atlantique, 2^e-3^e année – 3h CM.
 Blockchain Principles and Applications, ISTIC, Master 2 – 3h TD.
 Routage dans les Réseaux, ESIR, 2^e année – 16,5h CM, 3h TD, 22,5h TP.
 Sécurité des Réseaux Informatiques, ISTIC, Master 2 – 18h TP.
- 2023 – 2024 **Administration des Réseaux Internet**, ISTIC, Master 2 – 3h CM.
- 2021 – 2022 **Routage Inter-Domaine**, Univ. de Strasbourg, Master 1 – 14h TP.

Enseignement (suite)

- 2019 – 2020
- **Structures de Données et Algorithmes 1**, Univ. de Strasbourg, Licence 2 – 22h TD.
 - **Bases de l'architecture informatique**, Univ. de Strasbourg, Licence 1 – 10h TD, 24h TP.
- 2018 – 2019
- **Structures de Données et Algorithmes 2**, Univ. de Strasbourg, Licence 2 – 24h TP.
 - **Culture et Pratique de l'Informatique**, Univ. de Strasbourg, Licence 1 – 28h TP.

Encadrement de la recherche


- 2024 –
- **Dorian Pacaud**, *Passage à l'échelle de la blockchain*.
IMT Atlantique, Doctorat. Encadré avec Romaric Ludinard (IMT Atlantique) et Emmanuelle Anceaume (CNRS, IRISA).
- 2023 – 2024
- **Nathanaël Deroousseaux**, *Implémentation de preuves de preuve de travail non-interactives dans un environnement dynamique*.
Univ. de Strasbourg, stage de fin d'étude, Master 2. Encadré avec Romaric Ludinard (IMT Atlantique) et Emmanuelle Anceaume (CNRS, IRISA).
 - **Dorian Pacaud**, *Passage à l'échelle de la blockchain*.
Univ. Rennes 1, stage de fin d'étude, Master 2. Encadré avec Romaric Ludinard (IMT Atlantique) et Emmanuelle Anceaume (CNRS, IRISA).
- 2022 – 2023
- **Benjamin Loison**, *Conception et implémentation de preuves de preuve de travail non-interactives dans un environnement dynamique*.
ENS Paris-Saclay, stage de fin d'étude, Master 2. Encadré avec Romaric Ludinard (IMT Atlantique) et Emmanuelle Anceaume (CNRS, IRISA).
- 2019 – 2020
- **Lucas Braun**, *Sécurité du routage Internet*.
Réalisation d'un outil de détection d'attaques BGP. Univ. de Strasbourg, travail d'étude et de recherche, Master 1. Encadré avec Jean-Romain Luttringer (Univ. de Strasbourg).
 - **Philippe Chevalier**, *Sécurité du routage Internet*.
Découverte de la sécurité du routage inter-domaine. Univ. de Strasbourg, travail d'étude et de recherche, Master 1. Encadré avec Jean-Romain Luttringer (Univ. de Strasbourg).

Animation de la recherche

- Organisation
- Web chair IMC'22.
Membre du comité d'organisation AlgoTel/CoRes'24.
Aide logistique pour RESSI'25 – accueil, orientation et accompagnement.
Gestion du site web de l'équipe SOTERN (IRISA).
Aide à l'organisation de la chaire CyberCNI pour l'European Cyber Week (ECW'23).
Animation de table ronde avec les partenaires industriels CyberCNI.
CyberCNI Talks (modération de présentations en ligne).
Workshops de l'équipe Réseaux (ICube) pour la présentation et discussion d'articles.
- Diffusion
- Talk "Blockchain and its use in collaborative cybersecurity systems" à l'école de Printemps 2023 de l'EUR CyberSchool.
- Reviews
- PAM'19, IMC'19, CoNEXT'19, BRAINS'24, JNSM'24, NCA'24, ICDCIT'24.

Publications

Revue internationale avec comité de lecture

- 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.

Conférences internationales avec comité de lecture

- 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](https://doi.org/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](https://doi.org/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](https://doi.org/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.

Conférences nationales avec comité de lecture

- 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.

Autres

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

Détail des enseignements

Statut	Année	Établissement	Public	Niveau	Matière	HETD	Effectifs	Nature
Vacataire	2024 – 2025	ISTIC	Master	M2	Administration des Réseaux Internet	4.5h	~10	CM
Vacataire	2024 – 2025	IMT Atlantique	Master	M2	Blockchain et Consensus	4.5h	23	CM
Vacataire	2024 – 2025	ISTIC	Master	M2	Blockchain Principles and Applications	3h	23	TD
Vacataire	2024 – 2025	ESIR	Master	M1	Routage dans les Réseaux	42.75h	12	CM,TD,TP
Vacataire	2024 – 2025	ISTIC	Master	M2	Sécurité des Réseaux Informatiques	12h	22	TP
Vacataire	2023 – 2024	ISTIC	Master	M2	Administration des Réseaux Internet	4.5h	~10	CM
Vacataire	2021 – 2022	Univ. de Strasbourg	Master	M1	Routage Inter-Domaine	9.33h	13	TP
Vacataire	2019 – 2020	Univ. de Strasbourg	Licence	L2	Structures de Données et Algorithmes 1	22h	52	TD
Vacataire	2019 – 2020	Univ. de Strasbourg	Licence	L1	Bases de l'Architecture Informatique	26h	30 (~300+)	TD,TP
Vacataire	2018 – 2019	Univ. de Strasbourg	Licence	L2	Structures de Données et Algorithmes 2	16h	~30	TP
Vacataire	2018 – 2019	Univ. de Strasbourg	Licence	L1	Culture et Pratique de l'Informatique	18.67h	41	TP
Vacataire	2018 – 2025			L1-M2		163.25h	10-300	CM,TD,TP

2024 – 2025

■ **Blockchain et Consensus**, IMT Atlantique, 2^e-3^e année – 3h CM – 23 étudiants.

Le module “Blockchain et Consensus” s’adresse aux étudiants en 2^e et 3^e année de toutes les spécialités de parcours ingénieur du campus de Rennes, en particulier la spécialité “Plateformes numériques : technologies et marchés”. Cette formation vise à former des ingénieurs sur les aspects techniques (réseaux, virtualisation, cloud), économiques et juridiques des plateformes numériques. Le module accueille également des étudiants du mastère spécialisé en cybersécurité, co-organisé par IMT Atlantique et CentraleSupélec. Plus particulièrement, ce module présente les concepts fondamentaux aux blockchains – les principes des systèmes distribués (processus, communication, défaillances), les mécanismes de consensus ainsi que le développement de smart contracts avec le langage Solidity.

Dans le cadre de ce module, je suis intervenu pour 3h de CM sur la thématique du sharding dans les blockchains, dont j’ai réalisé le support de cours. Le contenu a été conçu en prenant en compte un public hétérogène, accessible aux 2^e années tout en offrant un niveau d’approfondissement adapté aux 3^e années. J’ai d’abord présenté les problèmes de passage à l’échelle des blockchains (e.g. débit), les métriques et compromis associés à ces problèmes, puis dans un deuxième temps le concept de sharding et ses variantes. J’ai aussi détaillé plusieurs solutions (Elastico, RapidChain) et présenté les formes de sharding dans différents contextes (blockchains publiques/privées, permissionnées ou non).

■ **Blockchain Principles and Applications**, ISTIC, Master 2 – 3h TD – 23 étudiants.

Le module “Blockchain Principles and Applications” s’adresse aux étudiants de niveau M2 suivant le parcours “Sécurité logicielle et matérielle” du master Cybersécurité proposé par la CyberSchool, une école universitaire de recherche en cybersécurité. L’objectif de ce module est de présenter la technologie blockchain ainsi que ses applications principales, afin de donner aux étudiants les éléments nécessaires pour comprendre les différences entre les variantes de blockchain, comprendre leurs forces et leurs faiblesses, et enfin décider si une de ces variantes est pertinente pour résoudre un problème donné. La première partie du cours se concentre sur les applications, e.g. monnaie numérique, livre de compte distribué, smart contracts, tandis que la deuxième partie se concentre sur les éléments constitutifs de la blockchain, e.g. cryptographie, algorithmes de consensus.

Dans le cadre de ce module, j’ai remplacé Romaric Ludinard, un des enseignants de ce module, pour la durée d’un TD de 3h. Le TD avait pour but d’amener les étudiants à réfléchir sur la façon de spécifier et d’implémenter un système auto-géré pour la gestion du café à IMT Atlantique.

Détail des enseignements (suite)

- **Routage dans les Réseaux**, ESIR, 2^e année – 16.5h CM, 3h TD, 22.5h TP – 12 étudiants.
Le module “Routage dans les Réseaux” s’adresse aux étudiants de 2^e année de l’ESIR, spécialité Systèmes Numériques et Réseaux (équival. M1). Il vise à fournir aux étudiants une connaissance et une pratique des technologies autour du routage. En particulier, ce module traite en première partie de la théorie des graphes (Bellman-Ford, Dijkstra). Il traite ensuite les protocoles de routage intra-domaine (RIP, OSPF), puis des réseaux d’opérateurs (BGP, MPLS, VPN BGP/MPLS). Le module est complété par un traitement de la sécurité BGP, du routage multicast, et du routage dans les réseaux ad hoc.

Pour ce module, j’ai assuré 16.5h de CM, 3h de TD et 22.5h TP. Dans le cadre des TPs, j’ai à nouveau mis en place l’infrastructure mini-internet venant de l’ETH Zurich (cf. 2021-2022 Routage Inter-Domaine pour plus de détails). En bref, le mini-Internet est une plateforme pédagogique virtuelle qui reproduit le fonctionnement pratique de l’Internet à échelle réduite. J’ai pu mettre cette plateforme à disposition des étudiants grâce à l’aide généreuse de Mathieu Goessens et du service admin ISTIC-ESIR. Vous pouvez retrouver les supports d’accompagnement pour les TPs [ici](#). Le module détaille les protocoles RIP, OSPF, BGP et MPLS avec un focus particulier sur la sécurité BGP et les VPNs BGP/MPLS. Nous abordons également le routage multicast. Le module a été évalué avec un compte-rendu final des TPs que j’ai réalisé à partir du compte-rendu demandé par l’ETH ainsi que celui que j’avais conçu pour l’Université de Strasbourg. Le module a aussi été évalué avec un examen final que j’ai rédigé, organisé, et noté complètement.

- **Sécurité des Réseaux Informatiques**, ISTIC, Master 2 – 18h TP – 22 étudiants.
Le module “Sécurité des Réseaux Informatiques” s’adresse aux étudiants de niveau M2 en mathématiques de l’information et cryptographie. Il vise à fournir aux étudiants des compétences avancées en sécurité des réseaux. Le cours combine des éléments de cyber-sécurité et de cryptographie, avec un focus particulier sur la sécurisation des communications et l’analyse des menaces dans les réseaux informatiques. Les étudiants sont initiés à des concepts tels que la gestion de VLANs, IPsec, IDS/IPS, ainsi que l’utilisation d’outils comme nmap, Burp Suite, et Pfsense. Les TPs permettent d’explorer des scénarios concrets, tels que la sécurisation des routeurs et commutateurs, l’implémentation d’IPsec et de VPN, ainsi que l’analyse de vulnérabilités réseau.

J’ai participé à ce module en encadrant un groupe de TP, en réalisant les supports de TP et assuré l’évaluation avec deux TP notés.

2023 – 2025

- **Administration des Réseaux Internet**, ISTIC, Master 2 – 3h CM – ~10 étudiants.
Le module “Administration des réseaux Internet” aborde les protocoles essentiels dans l’administration des réseaux, avec un accent particulier sur les protocoles TCP/IP, le routage (RIP, OSPF, BGP), ainsi que d’autres protocoles comme DHCP et LDAP. Les étudiants sont initiés aux principes de routage dynamique et aux algorithmes de calcul de chemins optimaux. L’objectif est de leur fournir une compréhension approfondie des mécanismes sous-jacents au fonctionnement des réseaux et des protocoles utilisés pour leur gestion et leur communication.

Lors de ce module, j’ai assuré 3 heures de cours magistraux concernant les protocoles de routage (RIP, OSPF, BGP) et le calcul des chemins (Bellman-Ford, Dijkstra), en finissant par une partie sur les attaques BGP. J’ai réalisé les supports pour ce cours.

Détail des enseignements (suite)

2021 – 2022

■ **Routage Inter-Domaine**, Univ. de Strasbourg, Master 1 – 14h TP – 13 étudiants.

Le module “Routage Inter-Domaine” s’adresse aux étudiants en réseaux de niveau M1 qui se préparent à des métiers liés à l’administration ou à la conception de réseaux. Il aborde les mécanismes essentiels au fonctionnement de l’Internet, notamment le protocole BGP utilisé entre systèmes autonomes, ainsi que des techniques d’ingénierie de trafic comme MPLS, SR et les VPN BGP MPLS. L’objectif est de permettre aux étudiants de configurer les services de base d’un réseau d’opérateur, de diagnostiquer des dysfonctionnements dans des inter-réseaux complexes et de mettre en œuvre des stratégies d’ingénierie de trafic. L’enseignement de ce module comporte une forte dimension appliquée grâce à l’utilisation d’équipements émulés sur une plateforme logicielle (mini-internet) pour étudier des cas concrets.

Dans le cadre de ce module, j’ai encadré un groupe de TP. J’ai construit les séances de TP en collaboration avec Jean-Romain Luttringer. Ensemble, nous avons entrepris la première adaptation du mini-Internet à l’Université de Strasbourg, remplaçant ainsi les TPs précédemment basés sur GNS3. Initialement développé à l’ETH Zurich, le mini-Internet est une plateforme pédagogique virtuelle qui reproduit le fonctionnement pratique de l’Internet à échelle réduite. Hébergé sur un serveur unique, il simule un réseau complet composé de routeurs, de commutateurs et d’hôtes répartis dans différents systèmes autonomes (AS). Chaque composant fonctionne dans un conteneur Linux accessible à distance via SSH. Ce projet permet aux étudiants de gérer leur propre AS et de collaborer pour établir une connectivité Internet globale, offrant ainsi une approche pratique et réaliste qui approfondit leur compréhension des opérations et des défis de l’infrastructure Internet.

Pour réaliser l’adaptation du mini-internet à Strasbourg, il nous a fallu nous occuper du déploiement du mini-internet, ainsi que de la réalisation des séances de TP et d’un projet (topologie réseau, questions, barème, ...) pour qu’ils soient adaptés à nos étudiants. Nous avons traité dans les séances BGP, MPLS, ainsi que les VPNs BGP-MPLS. Nous avons créé en plus une section basée sur les hijacks BGP, utilisée pour le TP noté, et une section DDoS et BGP poisoning, utilisée pour le TP de substitution. Vous pourrez trouver une partie du support en ligne [ici](#). J’ai également assuré avec mon groupe pendant les séances de TP une partie explication des concepts théoriques et des protocoles BGP, MPLS, et à la fin l’évaluation des TP notés et des projets harmonisée avec le groupe de Jean-Romain. L’utilisation du mini-internet, ainsi que l’encadrement, ont été très fortement appréciés par les étudiants.

2019 – 2020

■ **Structures de Données et Algorithmes 1**, Univ. de Strasbourg, Licence 2 – 22h TD – 52 étudiants.

Le module “Structures de Données et Algorithmes 1” s’adresse aux étudiants de niveau L2 et a pour objectif de leur fournir une compréhension approfondie des concepts fondamentaux en algorithmique et en structures de données. Il aborde les structures classiques (i.e. tableaux, listes chaînées, piles, files) ainsi que les algorithmes de tri, de recherche et d’optimisation. Ce module permet également d’introduire le concept de complexité algorithmique.

J’ai assuré les séances de TD pour ce module, où il était surtout question de spécification des structures de données classiques et de complexité. J’ai participé à l’évaluation du module, et me suis occupé des rattrapages. J’ai également réalisé les supports pour chaque TD.

Détail des enseignements (suite)

- **Bases de l'architecture informatique**, Univ. de Strasbourg, Licence 1 – 10h TD, 24h TP – 30 (~300+) étudiants.

Le module “Bases de l'Architecture Informatique” s'adresse aux étudiants de niveau L1, et vise à leur fournir les bases essentielles pour comprendre le fonctionnement des systèmes informatiques. Il traite de la représentation des informations, comme le codage des nombres, des caractères et d'autres types de données, ainsi que de leur traitement informatique, qu'il s'agisse d'opérations arithmétiques ou de manipulations associées. Le module explore également les fondements de l'architecture des ordinateurs, notamment l'architecture de Von Neumann, le rôle de l'unité de traitement, la gestion mémoire et les entrées/sorties. Une introduction aux langages machine et assembleur permet de faire le lien entre l'architecture matérielle et la programmation à bas niveau.

J'ai participé à ce module en encadrant deux groupes de TP et un groupe de TD. Les séances de TD et de TP étaient basées sur l'utilisation d'un processeur simple du nom de Cardiac, dont les mécanismes sont les mêmes que ceux des processeurs modernes. Les séances de TD comprenaient des exercices sur une version papier de Cardiac pour explorer la mémoire, l'accumulateur et l'exécution des instructions. Ces séances de TD étaient ensuite suivies de travaux pratiques sur le simulateur logiciel de Cardiac, où les étudiants rédigeaient et exécutaient des programmes en assembleur. Au cours de ce module, j'ai assuré l'évaluation de mes groupes via un TP noté, et j'ai participé à l'évaluation de l'examen final pour toute la promotion de cette année (300+ étudiants). J'ai également réalisé des supports additionnels pour accompagner chaque TD/TP, sous forme de slides.

2018 – 2019

- **Structures de Données et Algorithmes 2**, Univ. de Strasbourg, Licence 2 – 24h TP – ~30 étudiants.

Le module “Structures de données et algorithmes 2” s'adresse aux étudiants de L2 et approfondit l'étude des structures de données relationnelles, i.e. les tables (adressage calculé, associatif, haché), les arbres (binaires, équilibrés, B-arbres) et les graphes (orientés, non orientés, acycliques). Les algorithmes étudiés incluent les algorithmes de tri, ainsi que les algorithmes sur les graphes comme le parcours de graphe, l'algorithme de Warshall et celui de Tarjan.

J'ai assuré les séances de TP pour deux groupes d'une quinzaine d'étudiants, où les étudiants ont implémenté différents types de tris, de structures de données et d'algorithmes sur les graphes en utilisant le langage C.

- **Culture et Pratique de l'Informatique**, Univ. de Strasbourg, Licence 1 – 28h TP – 41 étudiants.

Le module “Culture et Pratique de l'Informatique” s'adresse aux étudiants de niveau L1 et vise à leur fournir des compétences de base en informatique, notamment sur l'interaction avec le système d'exploitation, les bases du shell et les scripts shell. Les étudiants y apprennent à naviguer dans un environnement Unix/Linux, à utiliser des commandes du terminal et à automatiser des tâches à l'aide de scripts shell.

J'ai supervisé deux groupes de TP, où les étudiants ont exploré ces concepts de manière concrète, en utilisant des commandes systèmes pour gérer des fichiers, exécuter des programmes, et automatiser des processus via des scripts shell. J'ai également réalisé les supports pour les TP ainsi que leur correction, et assuré l'évaluation avec deux TP notés.

Activités de recherche

Je développe dans cette section une description de mes activités de recherche depuis mon stage de fin d'étude de master. J'ai traité de différentes problématiques, mais toutes sont rassemblées autour de la notion de **sécurité dans les systèmes distribués**. J'ai en particulier examiné :

- La sécurisation du protocole de routage inter-domaine, Border Gateway Protocol (**BGP**).
- La sécurisation de **workflows** multi-partis, pour éviter les fuites de données.
- La sécurité des **preuves de preuve de travail non-interactives**, dans un contexte blockchain.

La suite de cette section détaille ces contributions en suivant ces trois axes.

Attaques BGP

J'ai réalisé ces travaux durant mon stage de fin d'étude de master. Dans ces travaux, nous étudions le blackholing BGP, une technique fréquemment utilisée pour se protéger des attaques de déni de service distribué (DDoS). Le blackholing est déclenché par la victime du DDoS, qui fait la requête vers les systèmes autonomes (AS) voisins de supprimer le trafic destiné aux adresses IP ciblées par le DDoS. Bien que ce mécanisme soit conçu comme une mesure défensive, il peut être détourné par des attaquants, qui envoient des demandes pour des adresses IP qu'ils ne possèdent pas. Ce détournement transforme une méthode initialement prévue pour la protection en un vecteur d'attaque. Ces travaux ont fait l'objet d'une publication ¹².

Dans ces travaux, nous avons développé une taxonomie des **attaques combinant des détournements de routes (hijacks) et l'utilisation abusive du blackholing**, que nous avons nommées BGP blackjacks, contraction de blackhole hijacks. Nous avons démontré que ces attaques permettent à un attaquant d'obtenir un impact et une portée plus large, ainsi qu'une discrétion accrue par rapport aux hijacks classiques. Nous avons également argumenté l'efficacité de ces attaques en considérant divers environnements de sécurité (RPKI, BG-Psec), en montrant leurs impacts et leur adaptabilité face aux configurations actuelles. Enfin, nous avons étudié les limites de ces mécanismes de sécurité du routage pour BGP, qui se révèlent insuffisants pour contrer certaines de ces attaques. À partir de ces constats, nous avons proposé de nouveaux mécanismes permettant de mieux se protéger ou d'atténuer les effets des blackjacks. Ces travaux ont mis en lumière des menaces émergentes pour l'infrastructure Internet qui n'étaient pas considérées jusqu'alors, et sont destinés aux opérateurs réseau et chercheurs traitant de la sécurité des réseaux. Ils contribuent à renforcer la sécurité du routage inter-domaine.

Plus particulièrement, nous proposons dans ces travaux une classification détaillée des attaques blackjack. Le type d'attaque dépend de la manipulation effectuée sur le chemin BGP, les préfixes affectés et la manière dont le trafic détourné est traité. Ainsi, nous avons défini les "Type-0 blackjacks", qui impliquent la re-origination d'un préfixe légitime de l'AS victime, avec dans le message de re-origination une communauté de blackholing qui va déclencher cette mesure de protection chez un AS ciblé. Faire cela confère deux avantages:

- **Portée** – L'attaquant peut potentiellement supprimer plus de trafic en faisant en sorte qu'un autre AS supprime le trafic, comparativement à la méthode du simple hijack pour attirer le trafic vers son AS pour le supprimer. De surcroît, la communauté qui indique un blackhole possède une précedence en terme de choix sur la longueur de l'AS path, le chemin des AS présent dans les messages BGP. Ainsi, un chemin plus long, mais avec une communauté blackhole, sera préféré à un chemin plus court. En indiquant le numéro de l'AS qui doit supprimer le trafic via blackholing, l'attaquant peut grâce à une communauté spécifique cibler précisément l'AS qui supprimera le trafic de l'AS victime.
- **Furtivité** – Comme l'AS attaquant n'est pas celui qui supprime le trafic, il est plus furtif que par d'autres méthodes de suppression de trafic. On pourrait imaginer retrouver l'attaquant grâce aux messages BGP reçus par les routeurs, mais cela peut être difficile car les routeurs concernés ne sont probablement pas dans le réseau de l'AS victime.

Activités de recherche (suite)

Nous avons ensuite défini les “Type-N blackjacks”. Dans cette attaque, l’attaquant ne fait pas de re-origination du préfixe ciblé, mais simule un lien (qui n’existe pas dans la réalité) avec l’AS victime. Ainsi, un attaquant qui simule un lien direct avec la victime donnera un blackjack de type 1, un attaquant simulant un lien à 2 sauts de la victime donnera un blackjack de type 2 et ainsi de suite. Cette version de l’attaque est intéressante, car elle annule totalement les bénéfices que pourraient apporter RPKI, une solution de sécurisation de BGP. Plus particulièrement, RPKI permet de vérifier que l’AS d’origine a bien le droit d’annoncer le préfixe associé, bloquant ainsi les blackjacks de type 0. Notez que le déploiement de RPKI dans l’Internet est loin d’être achevé, et les AS qui utilisent ces informations pour filtrer leur routes sont peu nombreux.

Le dernier type défini est le “Type-U blackjack”, qui regroupe les attaques où l’AS de l’attaquant est déjà sur le chemin d’un message d’avertissement BGP légitime. Ainsi, l’attaquant ne modifie pas l’attribut AS path, et ne réalise donc pas à proprement parler un hijack, mais rajoute tout de même la communauté blackhole avec de relayer l’avertissement aux autres AS. Cette version de l’attaque est donc plus furtive que les autres, car on ne manipule pas le chemin.

Nous avons ensuite examiné l’impact de ces attaques en les imaginant dans différents environnements en terme de déploiement de sécurité du routage. Ainsi, nous discutons de l’impact de ces attaques en fonction de ces déploiements:

- **Pas de sécurité** – Les AS n’utilisent ni RPKI ni BGPsec.
- **RPKI (partiel)** – Un sous-ensemble des AS utilise RPKI, mais aucun AS n’utilise BGPsec.
- **RPKI (complet)** – Tous les AS utilisent RPKI, mais aucun AS n’utilise BGPsec.
- **BGPsec (partiel)** – Un sous-ensemble des AS utilise à la fois RPKI et BGPsec. Les autres AS utilisent soit uniquement RPKI, soit aucun mécanisme de sécurité.
- **BGPsec (complet)** – Tous les AS utilisent à la fois RPKI et BGPsec.

Nous notons ensuite pour chaque attaque dans chaque scénario, si le déploiement est résistant ou non à l’attaque, ou bien si cela dépend d’autres facteurs (topologie réseaux, ...). Nous considérons aussi si l’attaque vise le préfixe directement, ou bien un sous-préfixe de la cible qui sera plus désirable. Nous tirons en conclusion que les mécanismes de sécurité actuels pour BGP sont très inadéquats pour les attaques blackjack. RPKI ne protège que l’origine des routes et ne couvre pas toujours les sous-préfixes, tandis que le BGPsec, bien qu’offrant une validation des chemins, ne protège pas l’attribut communautés, reste vulnérable aux attaques de rétrogradation et n’est pas encore déployé.

Pour limiter l’impact des attaques, nous recommandons plusieurs bonnes pratiques : l’ajout de règles de vérification pour les AS directement connectés et la mise en place de filtres pour rejeter les annonces insuffisamment spécifique. Nous proposons également une extension à BGPsec pour intégrer l’authentification des communautés. Ces mesures permettraient non seulement de réduire les abus, mais aussi de retracer l’origine des requêtes de blackholing malveillantes, responsabilisant ainsi les acteurs impliqués.

Sécurisation de workflows multipartis

J’ai réalisé les travaux de cette sous-partie au cours de ma thèse. Dans un contexte où les entreprises adoptent de plus en plus les services cloud pour leurs processus, le transfert et le traitement des données entre multiples acteurs augmentent considérablement les risques d’exposition de données sensibles. Ces travaux proposent de combiner une infrastructure microservices, avec une vérification des politiques de sécurité via une modélisation en métagraphes pour **garantir la confidentialité et le contrôle des données**.

Activités de recherche (suite)

Pour éviter que les acteurs qui ont accès aux données sensibles au cours du workflow puissent les faire fuiter, nous exploitons l'isolation offerte par les **microservices** pour appliquer des politiques d'accès. Cette infrastructure est implémentée dans une preuve de concept où nous testons son efficacité pour garantir le respect des politiques spécifiées, notamment en détectant les violations potentielles du contrôle d'accès. Nous mesurons ensuite les performances de l'infrastructure en intégrant des moteurs de politiques et démontrons que le coût supplémentaire lié à l'autorisation reste raisonnable par rapport aux avantages apportés. Ensuite, nous utilisons une modélisation des politiques de sécurité en métagraphes pour vérifier que la spécification des politiques de sécurité corresponde bien à son implémentation. À notre connaissance, nous sommes les **premiers à utiliser des métagraphes pour la vérification des politiques de contrôle d'accès**. Ces derniers permettent une modélisation précise des politiques, facilitant leur raffinement et la détection d'erreurs d'implémentation. Nous introduisons pour cela une suite d'outils permettant de traduire et de vérifier des politiques, en particulier celles spécifiées pour des workflows. Cette vérification repose sur Rego, un langage déclaratif conçu pour exprimer des politiques complexes. Nous réalisons également une analyse détaillée des performances de cette approche et démontrons que les politiques déployées correspondent bien à leurs spécifications dans un délai très raisonnable, même dans des workflows complexes comportant un grand nombre de règles.

Les performances de l'infrastructure ont été mesurées à plusieurs niveaux. Le premier test consistait à évaluer l'impact de l'ajout du moteur de politique Open Policy Agent (OPA) sur le temps de démarrage des conteneurs. Pour cette comparaison, nous avons recueilli 130 observations par pod et par déploiement (avec ou sans OPA), donc $N = 1820$ au total. Les résultats ont été obtenus avec un test t pour échantillons indépendants ($t(1818) = 43.19, p < 0.001$). De plus, la taille de l'effet pour cette analyse ($d = 1.985$) a été trouvée supérieure à la convention de Cohen pour un effet large ($d = 0.80$). Une analyse de puissance post hoc montre également une puissance statistique élevée, $1 - \beta > 0.999$. Les tests ont montré une augmentation moyenne du temps de démarrage de 2 secondes par rapport aux déploiements sans OPA, ce qui représente environ 32% de temps supplémentaire.

Pour le second test, la latence des requêtes entre services a été mesurée en fonction du nombre de règles de politique appliquées. Une ANOVA à sens unique entre les groupes a été réalisée pour chaque type de communication (intra-région/inter-région) afin de comparer l'effet de la taille de la politique sur la durée des requêtes dans cinq ordres croissants de taille de politique : sans OPA, tout autoriser, minimale, +100 règles et +1000 règles. Pour chaque ANOVA, nous avons collecté 40 observations par communication autorisée pour chaque niveau de politique ($N = 1600$ au total). Pour les communications intra-région, il existe une différence significative dans la durée des requêtes parmi les cinq scénarios de déploiement des politiques, $F(4, 795) = 364.05, p < 0.001, \eta_p^2 = 0.65$. Pour les communications inter-région, il existe également une différence significative (dans la durée des requêtes) parmi les cinq scénarios de déploiement des politiques, bien que l'effet soit moindre : $F(4, 795) = 15.23, p < 0.001, \eta_p^2 = 0.07$. Les résultats ont montré un **impact sur la latence négligeable**, même lorsque le nombre de règles augmentait de manière significative.

Nous avons ensuite utilisé des **métagraphes** pour modéliser les politiques de contrôle d'accès de manière granulaire. Un métagraphe est une généralisation des graphes, où les sommets représentent des ensembles d'éléments (comme des tâches ou des variables) et les arêtes les relations ou contraintes entre ces ensembles. Cette approche a permis de vérifier si les politiques étaient appliquées correctement et de détecter d'éventuelles incohérences ou redondances dans les règles. Les métagraphes sont particulièrement adaptés à la vérification de grandes quantités de règles, car leur structure permet une gestion efficace des politiques complexes.

Le processus de vérification des politiques s'effectue en plusieurs étapes : d'abord, la politique de sécurité est spécifiée, puis transformée en un métagraphe. L'implémentation réelle de la politique est créée sous forme de règles Rego, puis convertie en un métagraphe d'implémentation. Ces deux métagraphes (spécification et implémentation) sont comparés pour vérifier leur équivalence. Cette méthode permet de détecter les erreurs dans l'implémentation, telles que des règles mal appliquées ou des conflits entre politiques. Pour automatiser ce processus, des outils ont été développés à chaque étape.

Activités de recherche (suite)

La vérification des politiques a été évaluée en générant des workflows aléatoires avec différentes tailles et complexités. Nous avons simulé des erreurs dans les métagraphes pour tester la robustesse de l'algorithme. En tout, 27000 implémentations de politiques ont été générées et comparées à l'aide des métagraphes. Les tests ont montré que l'algorithme de vérification est très efficace, même pour des workflows complexes de grande taille.

Enfin, l'évaluation des performances du processus de vérification a montré que l'algorithme était capable de traiter rapidement même des workflows complexes, avec un temps de vérification inférieur à 2 secondes en moyenne pour des workflows de taille moyenne et 1000 règles. La complexité de l'algorithme est dominée par le tri et la correspondance des arêtes, ce qui lui confère une complexité de $O(m \cdot \log(m))$, où m est le nombre d'arêtes. En conclusion, la méthode de vérification des politiques par métagraphes est non seulement **efficace**, mais **passse à l'échelle** également, ce qui la rend adaptée pour des systèmes à grande échelle.

Nous avons également effectué des travaux sur la **suppression de redondances** dans les politiques à l'aide des métagraphes. Plus particulièrement nous avons montré qu'un problème équivalent, à savoir trouver un (s, d) -hyperréseau dans un F-hypergraphes est NP-difficile. Dans ces travaux, nous traitons de la complexité algorithmique liée aux hypergraphes dirigés, une généralisation des graphes où les arcs relient des ensembles de sommets (plutôt que deux sommets uniquement). L'étude se concentre sur le problème des (s, d) -hyperréseaux, c'est-à-dire la sous-structure minimale d'un hypergraphe qui relie un nœud source s à un nœud destination d . Nous examinons en particulier les F-hypergraphes (où chaque arête a une queue de cardinalité 1), où nous concluons que le problème de trouver un (s, d) -hyperréseau dans de tels hypergraphes acycliques est NP-difficile. Ces travaux ont fait l'objet de plusieurs publications [3](#), [6](#), [7](#), [8](#), [9](#), [10](#), [11](#).

Passage à l'échelle de la blockchain

Ces travaux ont été réalisés durant mon postdoc. Dans une première partie, mes travaux ont été réalisés dans le cadre de la chaire industrielle Cybersecurity for Critical Networked Infrastructures (Cyber CNI). Dans ce contexte, j'ai pu échanger avec certains partenaires industriels de la chaire (Airbus, SNCF, BNP Paribas), pour évaluer leurs besoins et leur appréciation de solutions axées autour de la blockchain. J'ai réalisé une revue de la littérature structurée qui aborde le **rôle de la blockchain dans la cybersécurité collaborative**, où le but est d'encourager le partage d'informations entre organisations pour améliorer la sécurité.





La gestion de la confiance dans ces systèmes représente un défi majeur. Les solutions décentralisées, comme la blockchain, sont essentielles pour éliminer les points de défaillance critiques. Pourtant, la littérature existante sur la cybersécurité collaborative basée sur la blockchain est limitée et manque d'analyses approfondies. Je comble cette lacune en étudiant l'évolution de l'utilisation de la blockchain dans la cybersécurité collaborative entre 2016 et 2023. J'explore diverses applications, tendances, et l'évolution de la technologie blockchain, en me concentrant sur le contrôle d'accès, les politiques de validation des données, les technologies sous-jacentes et les mécanismes de consensus. Dans ces travaux [4](#), je souligne que de nombreuses contributions choisissent mal leur protocole de consensus. Pour aider à résoudre ce problème, je propose des lignes directrices pour choisir la blockchain adaptée aux besoins spécifiques de la solution.


Dans un deuxième temps, nous nous sommes intéressés au problème de **passage à l'échelle en stockage**, dans les blockchain à preuve de travail. Ces travaux ont été effectués dans le cadre du projet ANR BC4SSI, qui vise à utiliser la blockchain pour rendre possible un système d'identité numérique auto-souveraine. Il y a en effet une volonté au niveau européen d'assurer une e-identité disponible depuis un smartphone, où chaque individu garderait la maîtrise de ses données d'identité. Niveau recherche, alors que la taille des données applicatives d'une blockchain est variable par nature, les données de consensus, qui assurent l'intégrité de la blockchain, doivent être conservées dans leur intégralité. Cela pose un problème car ces données grandissent de façon linéaire, et l'on compte actuellement, par exemple, 600 Go pour Bitcoin et 1.6 To pour Ethereum.

Activités de recherche (suite)

Dans ces travaux, nous présentons une **construction pour les preuves de preuve de travail non-interactives (NIPoPoW)**, une preuve compacte résumant le travail effectué pour construire une blockchain basée sur la preuve de travail. Plus particulièrement, cette NIPoPoW fonctionne dans des environnements avec une difficulté de minage variable, contrairement aux constructions précédentes qui supposaient une difficulté constante. Cette approche rencontre plusieurs défis, notamment la définition du niveau d'échantillonnage approprié pour les blocs ayant des difficultés de minage différentes et la protection contre les attaques exploitant les blocs de faible difficulté. La construction garantit une sécurité contre un adversaire byzantin contrôlant moins d'un tiers de la puissance de calcul, tout en compressant les données de la blockchain, réduisant le nombre de blocs nécessaires pour la synchronisation. Nous avons travaillé sur des preuves formelles de sécurité ainsi que des résultats expérimentaux montrant que la NIPoPoW proposée réduit de manière exponentielle la taille de la blockchain Bitcoin. L'implémentation de cette construction, et son utilisation sur les données de Bitcoin peut être trouvée en ligne [ici](#).

Dans le cadre de ces travaux, j'ai pu participer à l'encadrement de Benjamin Loison, alors en stage de fin d'études dans le cadre de son Master 2 à l'ENS Saclay. Une version préliminaire des résultats a été publiée à BRAINS'23 ⁵ par Benjamin, dans le cadre d'un article étudiant. La version finale de ces **travaux** a été réalisée en collaboration avec Nathanaël Drousseaux et Dorian Pacaud durant leur stage de fin d'étude de master respectivement à l'Université de Strasbourg et l'Université de Rennes 1. J'ai eu la chance de pouvoir participer à l'encadrement de Nathanaël et Dorian, ce dernier ayant poursuivi en thèse. La version finale de l'article ¹ a été acceptée à la conférence CCS'25. Une version courte a également été acceptée à la conférence AlgoTel'25 ².

- ¹ **L. Miller**, D. Pacaud, N. Drousseaux, 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 \[cs.CR\]](https://arxiv.org/abs/2403.04410).  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](https://doi.org/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](https://doi.org/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](https://doi.org/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.