Les Rencontres Cybersécurité & Défense de l'Institut Polytechnique de Paris

21 octobre 2025

INSTITUT POLYTECHNIQUE DE PARIS | ENSTA | ENSAE | TELECOM Paris | TELECOM SudParis

En partenariat avec

CIEDS CENTRE INTERDISCIPLINAIRE D'ÉTUDES POUR LA DÉFENSE ET LA SÉCURITÉ

CHAIRE CYBER GOUVERNANCE NUMÉRIQUE IHEDN

LE MOT DU COMITÉ SCIENTIFIQUE

Le 21 octobre 2025, l'Institut Polytechnique de Paris organise la première édition de ses Rencontres Cybersécurité et Défense. Industriels ainsi que chercheurs civils et de la défense échangeront autour de cette thématique sensible, à la pointe des enjeux nationaux et européens.

Dans un contexte géopolitique en tension, d'ubiquité du numérique et de variété des voies d'accès au numérique, les intérêts français et européens se trouvent menacés. Les Etats et les entreprises doivent faire face à de nouveaux dangers au nom desquels les cyberattaques organisées à grande échelle par certaines nations et leurs affiliés ou pour des motivations pécuniaires.

Face à ces enjeux, il devient essentiel de penser conjointement cybersécurité et défense des intérêts nationaux et européens.

C'est à ce double défi que Les Rencontres Cybersécurité et Défense de l'Institut Polytechnique de Paris souhaitent apporter des éléments de réponse.

L'évènement est organisé en partenariat avec le Centre Interdisciplinaire d'Études pour la Défense et la Sécurité (CIEDS), soutenu par le ministère des Armées, l'Agence de l'Innovation Défense) et avec le soutien de la chaire Cyber et souveraineté numérique - IHEDN, rattachée à l'Institut des Hautes Études de Défense Nationale (IHEDN) par son Fonds de dotations.

Composition du comité scientifique

Sébastien Canard,
Professeur, LTCI, Télécom Paris

Hervé Debar,
Professeur, SAMOVAR, Télécom SudParis

David Filliat,
Professeur, U2IS, ENSTA,
directeur scientifique du CIEDS

Jean Leneutre,
Maître de conférences, LTCI,
Télécom Paris

François Morain,
Professeur, LIX, École polytechnique

Jean Peeters,
Professeur, Université Bretagne
Sud, titulaire de la Chaire Cyber et
souveraineté numérique - IHEDN

PROGRAMME

9:00

Mots de bienvenue

Laura Chaubard,
Directrice générale
et présidente par intérim
de l'École polytechnique

Patrick Olivier,
Directeur de Télécom Paris

9:30 - 10:00

Conférence

Benjamin Morin
Coordinateur de la stratégie nationale pour la cybersécurité au Secrétariat général pour l'investissement (SGPI)

10:00 - 10:45

Conférence

Bart Preneel,
Professeur à la Katholieke Universiteit Leuven (Belgique), directeur du groupe COSIC (Computer Security and Industrial Cryptography), Cryptologue

10:45 - 11h15 PAUSE

11:15 - 12:15

Table ronde
IA & Cybersécurité

Corentin Larroche,
Expert technique en science des données et détection d'intrusion à l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Michel Combot,
Directeur des technologies, de l'innovation et de l'intelligence artificielle à la Commission nationale de l'informatique et des libertés (CNIL)

Sonia Vanier,
Professeure au département d'Informatique de l'École polytechnique, Responsable de la chaire IA de Confiance, Responsable X Crédit Agricole, Responsable de la chaire IA et Optimisation pour les Mobilités X-SNCF

Katarzyna Kapusta-Dedieu,
Docteur en informatique, Responsable de l'équipe Friendly hackers chez Thales

Thomas Le Goff,
Maître de conférences en droit et régulation du numérique à Télécom Paris

Gregory Blanc,
Maître de conférences en réseaux et sécurité à Télécom SudParis

12:15 - 13:15

Déjeuner
& Session Posters

13:45 - 14:00

Allocution du
général de corps d'armée
Hervé de COURRÈGES
IHEDN

14:00 - 14:30

Conférence

Benoît Chatelain,
Directeur Défense & Sécurité
chez Sopra Steria

14:30 - 15:15

Conférence

Valérie Viet Triem Tong,
Professeure à CentraleSupelec,
Responsable de l'équipe
de recherche PIRAT
CentraleSupelec/CNRS/INRIA/
Univ. Rennes IRISA Lab

15:15 - 15:45 PAUSE

15:45 - 17:05

Présentation
de chercheurs de l'Institut Polytechnique de Paris, mettant en perspectives leurs travaux de recherche récents en lien direct avec ces enjeux de cybersécurité.

Anamaria Costache,
Professeure invitée
à l'École polytechnique

Pascal Cotret,
Maître de conférences à l'ENSTA

Olivier Rioul,
Professeur à Télécom Paris

Stefano Zacchiroli,
Professeur à Télécom Paris

Olivier Levillain,
Maître de conférences
à Télécom SudParis

17:05 - 17:20

Conclusion

Annick Rimlinger,
Directrice Sûreté-Sécurité,
Cyber & Data Protection
chez Aéma Groupe

Mot de clôture par
le comité scientifique

LES CONFÉRENCIERS DE LA PREMIÈRE ÉDITION

Benjamin Morin

Il rejoint le secrétariat général pour l'investissement (SGPI) en février 2025, en qualité de coordinateur de la stratégie nationale pour la cybersécurité. Son parcours long de 25 années dans le secteur de la cybersécurité est jalonné d'expériences dans les domaines de la recherche, de l'expertise, du management et de la cyberdéfense.

Bart Preneel

Professeur à la KU Leuven, où il dirige le groupe de recherche de renommée internationale COSIC. Ses domaines d'expertise couvrent la cryptographie appliquée, la cybersécurité et la protection de la vie privée. Il a donné plus de 150 conférences invitées dans 50 pays et a reçu plusieurs distinctions prestigieuses, dont le RSA Award for Excellence in Mathematics (2014), le ESORICS Outstanding Research Award (2017) et le titre de Personnalité ICT de l'année en Belgique (2025).

Il intervient régulièrement en tant que consultant auprès de l'industrie et des pouvoirs publics sur les questions de cybersécurité et de protection de la vie privée, et a été auditionné à plusieurs reprises par les Parlements belge et européen.

Benoît Chatelain

Directeur Défense & Sécurité de Sopra Steria. Cela comprend l'ensemble des activités sur le marché européen, ainsi que celles au bénéfice de l'Union Européenne, l'OTAN et l'industrie militaire et spatiale. Il est ingénieur en télécommunications et diplômé de Télécom Paris. Il est également diplômé de l'ESSEC. Il est Auditeur de la 70ème Session Nationale Politique de Défense de l'Institut des Hautes Études de Défense Nationale (IHEDN). Il est Président du Comité de Pilotage de la Chaire Cyber et Souveraineté Numérique de l'IHEDN. Il est Chevalier de l'ordre national du Mérite.

Valérie Viet Triem Tong

Professeure à CentraleSupélec en informatique et cybersécurité. Ses travaux portent sur les attaques contre les systèmes d'information, avec une expertise particulière sur l'analyse des malwares, la compréhension et la mitigation des menaces persistantes avancées en cybersécurité. Elle dirige l'équipe de recherche PIRAT affiliée à CentraleSupélec, Inria, l'Université de Rennes et le CNRS de l'IRISA.

Général de corps d'armée Hervé de Courrèges

Par décret présidentiel du 19 juin 2024, le général de corps d'armée Hervé de Courrèges a été nommé directeur de l'IHEDN et de l'Enseignement militaire supérieur, à compter du 1er août.

Promu général en 2018, il est nommé commandant en second du renseignement des forces terrestres à Strasbourg. Puis en 2021, il est promu général de division et nommé commandant de l'Académie militaire de Saint-Cyr Coëtquidan.

Membre du comité d'éthique de la défense, le général de Courrèges est officier de la légion d'honneur, commandeur de l'ordre national du mérite et titulaire de la croix de la valeur militaire.

Annick Rimlinger

Spécialiste reconnue de la maîtrise des risques, justifiant de plus de 20 ans d'expérience dans la création et la direction de services complexes, tant au sein du secteur public que de grands groupes privés. Actuellement Directrice Sûreté-sécurité, Cyber & Data protection au sein d'Aéma Groupe, le 4ème assureur français, elle y dirige une équipe opérationnelle incluant notamment le directeur cyber et data, ainsi que le RSSI.

Auditrice du 58ème cycle « Intelligence économique et stratégique » de l'IHEDN, de la 20ème session nationale de l'INHES, et est Lieutenant-Colonel de la Réserve Citoyenne de la Gendarmerie Nationale.

LES ORATEURS DE LA TABLE RONDE IA & CYBERSÉCURITÉ

Michel Combot

Directeur des technologies et de l'innovation de la Commission nationale de l'Informatique et des Libertés (CNIL). Diplômé de l'École polytechnique et de Télécom Paris, Michel Combot bénéficie de 26 ans d'expérience dans les domaines de l'économie numérique, des télécoms et des médias.

Sonia Vanier

Professeure au Département d'Informatique de l'École polytechnique (DIX), Directrice de l'équipe ORAILIX du Laboratoire d'Informatique le LIX. Responsable de la chaire «IA de Confiance et Responsable», de la chaire «IA et Optimisation pour les Mobilités».

Ses thèmes de recherche portent principalement sur le développement d'outils d'aide à la décision pour des problèmes industriels complexes, l'Intelligence Artificielle (IA), la Recherche Opérationnelle (RO), l'Optimisation des Réseaux, l'optimisation sous incertitude, les approches hybrides entre l'IA et la RO pour les futurs systèmes d'IA étiques, sécurisés, durables et de confiance.

Corentin Larroche

Il a obtenu son doctorat en mathématiques aux interfaces à Télécom Paris en 2021. Il est expert technique en science des données et détection d'intrusion à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) depuis 2017.

Katarzyna Kapusta-Dedieu

Chercheuse en cybersécurité de l'IA au sein du laboratoire cortAIx Labs de Thales. Elle pilote l'équipe transverse « AI Friendly Hackers » dont l'objectif est de développer des contremesures contre les attaques spécifiques à l'IA, notamment celles visant à détourner l'usage d'une IA ou de voler les données d'apprentissage. Elle intervient en tant qu'experte technique sur le sujet de la cybersécurité de l'IA dans les projets de recherches collaboratifs et dans les groupes de standardisation européens, tels que ETSI TC Securing Artificial Intelligence. Elle a obtenu un doctorat en informatique à Télécom Paris en 2018 où elle continue d'enseigner. Elle est l'autrice de plusieurs articles publiés dans des revues et conférences, ainsi que des brevets.

Thomas Le Goff

Maître de conférences en droit et régulation du numérique à Télécom Paris (laboratoire i3, CNRS), où il enseigne et mène des recherches sur les règlementations relatives aux technologies numériques, aux données, à la cybersécurité et à l'IA. Avant d'entrer dans le monde académique, il a travaillé comme juriste d'entreprise chez Électricité de France (EDF), au sein du pôle propriété intellectuelle, données et numérique de la Direction Juridique, où il avait la charge de l'expertise en matière de protection des données et de régulation numérique.

Grégory Blanc

Il a obtenu un doctorat en sécurité informatique du Nara Institute of Science and Technologie (Japon) dans le domaine de l'analyse des scripts malveillants dans les navigateurs Web, en 2012. Il a ensuite rejoint le laboratoire SAMOVAR de Télécom SudParis en tant que chercheur postdoctoral et a contribué au montage et au pilotage de projets collaboratifs européens tels que NECOMA (projet européen-japonais). Depuis 2015, il est maître de conférences en sécurité et réseaux à Télécom SudParis où il coordonne la spécialisation en sécurité des systèmes et réseaux. Récemment, il coordonne le projet ANR GRIFIN dans lequel il explore les apports de l'apprentissage automatique pour rendre la boucle de sécurité autonomique afin d'améliorer la résilience des réseaux du futur : monitoring, détection, sélection de contremesures, déploiement des politiques de sécurité.

PRÉSENTATION DE CHERCHEURS DE L'INSTITUT POLYTECHNIQUE DE PARIS

Pascal Cotret

Enseignant-chercheur au Laboratoire des Sciences et Techniques de l'information de la Communication et de la Connaissance (Lab-STICC) de l'ENSTA (campus de Brest) sur le campus de Brest depuis 2019. Son expertise porte sur la sécurité à la frontière logiciel/matériel et les systèmes embarqués. Il s'intéresse également à l'adéquation algorithme-architecture de mécanismes de sécurité.

Stefano Zacchiroli

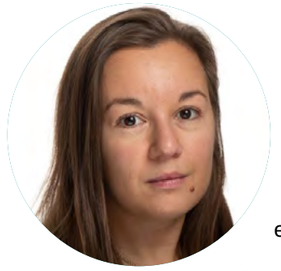
Professeur d'informatique à Télécom Paris. Ses travaux de recherche portent sur les communs numériques, l'ingénierie des logiciels libres, la sécurité informatique et la chaîne d'approvisionnement logicielle. Il est cofondateur et directeur scientifique de Software Heritage, la plus vaste archive publique mondiale du code source. Il a été à trois reprises chef du projet Debian et membre du conseil d'administration de l'Open Source Initiative (OSI). Ses contributions ont été distinguées par le O'Reilly Open Source Award (2015) et le Google Award for Inclusion Research (2022)

Olivier Rioul

Professeur au département Communications et Électronique de Télécom Paris. Ses recherches portent sur les mathématiques appliquées et couvrent divers domaines, parfois non conventionnels, de la théorie de l'information, tels que les inégalités en statistique, la sécurité matérielle et la psychologie expérimentale. Il enseigne la théorie de l'information et les statistiques dans différentes universités depuis une vingtaine d'années et est l'auteur d'un manuel qui est devenu une référence dans ce domaine.

Olivier Levillain

Maître de conférences en cybersécurité à Télécom SudParis. Auparavant, il a dirigé le centre de formation en cybersécurité de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), et a mené des recherches allant des attaques sur les mécanismes matériels bas niveau aux infrastructures de gestion de clés publiques. Ses recherches récentes portent sur les protocoles réseaux sécurisés (en particulier SSL/TLS) ainsi que sur la reproduction de vulnérabilités logicielles.



Anamaria Costache

Professeure invitée au laboratoire d'Informatique (LIX) de l'École polytechnique et professeure associée à l'Université Norvégienne des Sciences et de Technologie (NTNU) depuis 2020. Avant de rejoindre NTNU, elle était chercheuse chez Intel Corporation. Elle a également effectué un postdoctorat au sein du groupe ISG de Royal Holloway, University of London (RHUL), en collaboration avec Martin Albrecht et Rachel Player.

Elle est titulaire d'un doctorat en cryptographie de l'Université de Bristol, où elle a travaillé sous la direction de Nigel Smart. Ses recherches portent principalement sur le chiffrement entièrement homomorphe et, plus largement, sur le calcul sur données chiffrées, l'apprentissage automatique respectueux de la vie privée, ainsi que sur la cryptographie basée sur les réseaux et la cryptographie post-quantique.

QUELQUES TRAVAUX DE RECHERCHE DES CHERCHEURS DE L'INSTITUT POLYTECHNIQUE DE PARIS

Sécurité réseau : de nouvelles façons de chercher l'intrus

Au laboratoire SAMOVAR* de Télécom SudParis, **Gregory Blanc** concentre ses recherches sur la détection d'intrusions dans les réseaux de communication. Avec son équipe, le maître de conférences met au point des techniques fiables et reproductibles de caractérisation de données réseaux et de détections d'anomalies sur ces derniers. Ses recherches trouvent des débouchés dans les milieux industriels et économiques.

https://www.ip-paris.fr/actualites/securite-reseau-de-nouvelles-facons-de-chercher-lintrus

Cybersécurité : à la recherche de la faille matérielle

Pascal Cotret est maître de conférences au Laboratoire des Sciences et Techniques de l'information de la Communication et de la Connaissance (Lab-STICC*) de l'ENSTA. Grâce à ses travaux, il établit des environnements matériels sécurisés pour le développement de logiciels sur des plateformes embarqués. Il décortique pour cela des composants électroniques open source pour mieux les comprendre, en trouver les failles et y apporter d'éventuels correctifs. Il ouvre ainsi la voie à de nombreuses applications industrielles, notamment Défense.

https://www.ip-paris.fr/actualites/cybersecurite-la-recherche-de-la-faille-materielle

L'IA, un outil (fiable) d'aide à la décision

Au laboratoire d'informatique de l'École polytechnique (LIX) et au sein de l'équipe ORAILIX, **Sonia Vanier** associe recherche opérationnelle et intelligence artificielle. Au sein des chaires dont elle est titulaire, elle développe des algorithmes fiables, efficaces et sécurisés offrant une aide à la décision aux entreprises ou industries confrontées à des problèmes complexes à résoudre.

https://www.ip-paris.fr/actualites/lia-un-outil-fiable-daide-la-decision

IA et cybersécurité : optimiser les règles du jeu

L'IA et la cybersécurité, c'est certes une question d'algorithmes et de clefs de chiffrement, mais aussi de réglementation. Et celle-ci n'est pas sans conséquences sur de nombreux secteurs d'activité. **Thomas Le Goff,** maître de conférences au sein du département Sciences économiques et sociales de Télécom Paris et du laboratoire I3*, décortique ce cadre juridique et participe à son amélioration. Ses travaux pluridisciplinaires aident par ailleurs les entreprises à s'y conformer tout en en tirant le meilleur parti technologique.

https://www.ip-paris.fr/actualites/ia-et-cybersecurite-optimiser-les-regles-du-jeu

Podcast [Cybermois 2025] Cybersécurité : pourquoi elle nous concerne tous

https://podcast.ausha.co/sciences-num/cybermois-2025-cybersecurite-pourquoi-elle-nous-concerne-tous

Durant le Cybermois 2025, retrouvez d'autres travaux de recherche sur le site de l'Institut Polytechnique de Paris et/ou ses Écoles membres.

*SAMOVAR : un laboratoire de recherche Télécom SudParis, Institut Polytechnique de Paris, 91120 Palaiseau, France
* Lab- STICC : une unité mixe de recherche CNRS, IMT Atlantique, ENSTA, Université de Bretagne Occidentale, Université Bretagne Sud, École Nationale d'ingénieur de Brest, Institut Polytechnique de Paris, 91120 Palaiseau, France

*LIX : une unité mixte de recherche CNRS, École polytechnique, Institut Polytechnique de Paris, 91120 Palaiseau, France
*I³ : une unité mixte de recherche CNRS, Mines Paris - PSL, Télécom Paris, École polytechnique, Institut Polytechnique de Paris, 91120 Palaiseau, France

SÉLECTION DES TRAVAUX PRÉSENTÉS PAR LES ÉQUIPES DE RECHERCHE

Session posters

Vadim Malvone,
David Cortes,
Axel Oscar
LTCI Télécom Paris

Formal Methods for Dynamic Defense via Strategic Reasoning

Garantir la correction des systèmes logiciels et matériels, en particulier dans des contextes distribués et adversariaux, reste un défi majeur. Les méthodes formelles, telles que la vérification de modèles et les techniques automatiques basées sur les automates, ont évolué pour gérer les interactions multi-agents. Les scénarios de cybersécurité nécessitent un raisonnement sur des processus d'attaque et de défense dynamiques et à plusieurs étapes. Les infrastructures critiques sont confrontées à des menaces adaptatives, tandis que les défenses restent souvent statiques. Les approches existantes se concentrent sur la structure, la probabilité ou le temps, limitant les garanties de bout en bout. Les techniques de Moving Target Defense (MTD) introduisent du dynamisme mais manquent généralement d'un cadre formel reliant les reconfigurations à des garanties de sécurité démontrables.

Karolina Gorna,
LTCI Télécom Paris

Automated Vulnerability Detection in Go Binaries using Concolic Execution

Our work presents Zorya, a specialized concolic execution framework that operates on compiled Go binaries using P-Code intermediate representation. The framework introduces panic-gated exploration techniques that focus analysis effort on failure-relevant code paths, combined with function-level analysis strategies that reduce complexity while maintaining precision. Evaluation demonstrates that Zorya successfully detects various categories of runtime vulnerabilities in Go programs, including theoretical test cases and real-world security issues, where comparable symbolic execution tools are not tailored for Go binaries analysis.

Solal Rapaport,
LTCI Télécom Paris

Altered Histories in Version Control System Repositories: Evidence from the Trenches

Les systèmes de contrôle de version (VCS) comme Git permettent aux développeurs de réécrire localement l'historique enregistré, par exemple pour réordonner et supprimer des commits ou des données spécifiques qu'ils contiennent. Ces modifications ont des cas d'usage légitimes, mais deviennent problématiques lorsqu'elles sont effectuées sur des branches publiques utilisées par des utilisateurs en aval : elles cassent les flux de travail push/pull, remettent en question l'intégrité et la reproductibilité des dépôts, et créent des opportunités pour les attaquants de la chaîne d'approvisionnement d'y introduire des modifications malveillantes. En menant deux études de cas ciblées, nous montrons que les historiques modifiés peuvent changer de manière récurrente les licences rétroactivement, ou sont utilisés pour supprimer des « secrets » (par exemple, des clés privées) commises par erreur.

Matthieu Rambaud,
Maryam Munim,
Pascal Urien,
Anaël Messan,
Pirabakaran Thanushan
LTCI Télécom Paris

Transparent cloud data security with lightweight French hardware

Nous présentons une démo qui offre l'interface classique d'un client d'AWS qui stocke sur S3, mais en sous-routine il chiffre et déchiffre les données stockées sur AWS. Ainsi, AWS ne voit pas les données en clair.
La latence est imperceptible par rapport à un usage normal d'AWS. Les clés sont stockées sur 2 ou 3 HSMs (deux sur la table le jour de la démo, un 3e à distance), et le service est assuré même lorsqu'on en met l'un des deux HS.
L'intérêt est que le client de cryptage est open source (il n'utilise pas les tuyaux HYOK/BYOK proposés par AWS), mais reste 100% interfacé avec AWS donc aucune différence pour l'utilisateur.
L'autre point fort est le HSM lui-même, qui est produit par une société française. Il est 10x-100x moins cher et plus léger que les HSMs pour ce même type d'usage.

Montassar Naghmouchi,
SAMOVAR Télécom SudParis

ClinConNet: privacy preserving identity and consent management for clinical trials

ClinConNet proposes a modern, patient-centric solution combining blockchain, Self-Sovereign Identity (SSI), and dynamic consent to manage patient identity and consent in clinical research projects. It utilizes SSI wallets for identity management, and a Blockchain-based Dynamic consent model allowing participants to control their identity and consent data.

Alex Pierron,
SAMOVAR Télécom SudParis

Impact sur la Cybersécurité des techniques d'optimisation basées sur l'IA dans les réseaux B5G

Malgré les avantages apportés par l'adoption généralisée du paradigme de l'IA pour optimiser les opérations dans les réseaux B5G, les résultats sont susceptibles d'introduire de nouveaux vecteurs d'attaque, qui peuvent être utilisés pour mettre en danger des infrastructures critiques. De nouvelles recherches sont nécessaires pour comprendre rapidement le risque et contrer rapidement les activités malveillantes découvertes, afin de réduire des possibles perturbations ou fuites d'information.

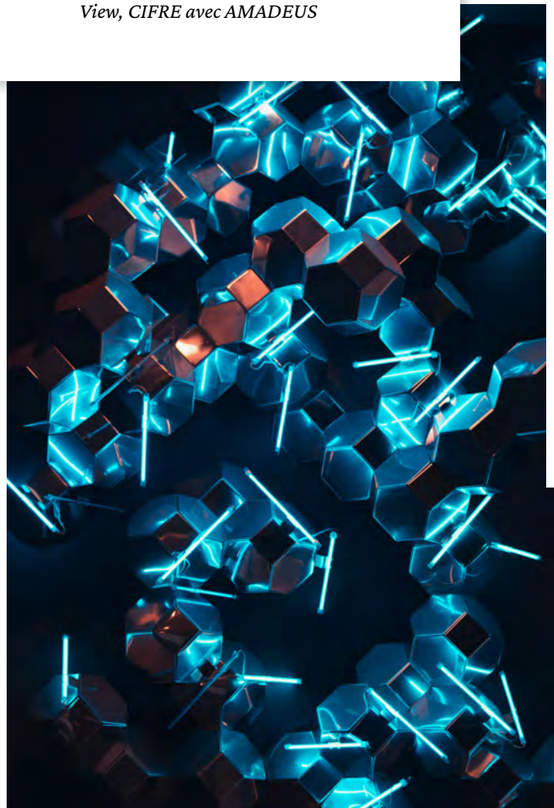
SÉLECTION DES TRAVAUX PRÉSENTÉS PAR LES ÉQUIPES DE RECHERCHE

Session posters

Umberto Fontana,

SAMOVAR Télécom SudParis

The Imitation Game of Functional Abuse — An Industry View, CIFRE avec AMADEUS



Iain Burge,

LTCI Télécom Paris

Quantum Support Vector Machines for Anomaly Detection via Reinforcement Learning

We propose a novel method for implementing quantum reinforcement learning (RL), using quantum SVMs, to detect corrupt quantum network nodes. In particular, we perform tomography - the inference of quantum features, to detect anomalies. SVMs can be trained with a matrix inversion, which is accelerated by the HHL quantum algorithm in certain cases. We expect to avoid the limitations of HHL through the use of RL and synthetic data, which avoids quantum RAM and allows for more control the data matrix structure.

Vincent Lannurien,
Camélia Slimani,
Louis Morge-Rollet,
Laurent Lemarchand,
David Espes,
Frédéric Le Roy,
Jalil Boukhobza,

Lab-STIIC, ENSTA, Université de Bretagne Occidentale, Brest

A retrospective on DISPEED - Leveraging heterogeneity in a drone swarm for IDS execution.
Financement : projet AID DISPEED

Swarms of drones are gaining more and more autonomy and efficiency during their missions. However, security threats can disrupt their missions' progression. To overcome this problem, Network Intrusion Detection Systems ((N)IDS) are promising solutions to detect malicious behavior on network traffic. However, modern NIDS rely on resource-hungry machine learning techniques, that can be difficult to deploy on a swarm of drones. The goal of the DISPEED project is to leverage the heterogeneity (execution platforms, memory) of the drones composing a swarm to deploy NIDS.

Oussama Elmnaouri,
Pascal Cotret,
Vianney Lapôtre,
Loïc Lagadec,

Lab-STICC, ENSTA,
Université de Bretagne-Sud Lorient

Enhancing Keystone Security Against Cache Timing Attacks: A Modular Approach. Financement ANR SCAMA.

Confidential computing includes various methods to enhance data security, notably by processing sensitive information within Trusted Execution Environments (TEEs). However, TEEs remain vulnerable to Side-Channel Attacks (SCAs), such as cache timing attacks, which exploit timing variations to extract confidential data. Existing TEE designs do not provide sufficient protection against these threats, highlighting the need for stronger security measures. This study focuses on integrating countermeasures specifically targeting timing and cache vulnerabilities within a TEE. The implementation will leverage the RISC-V architecture to explore its potential in mitigating SCA within TEE.

Pierre Garreau,
Pascal Cotret,
Julien Francq,
Jean-Christophe Cexus,
Loïc Lagadec,

Chaire de cyberdéfense des systèmes navals, Ecole Navale, Brest, Lab-STICC, ENSTA, CERT, Naval Group, Ollioules

Priority-Aware Scheduling of Multi-Model, Multi-Precision DNN Inference on Resource-Constrained Embedded Multi-Cores. Financement: Chaire de cyberdéfense des systèmes navals.

Efficient deployment of Deep Learning (DL) models on embedded multi-core platforms remains a significant challenge, especially when multiple models with heterogeneous structures and precision requirements must run concurrently. Existing frameworks offer optimized execution for single-model inference but lack support for multi model scheduling, as well as priority-based resource allocation. In this work, we extend the capabilities of such frameworks by formalizing the problem of multi-model, multi-precision inference scheduling on constrained manycore architectures like PULP.

Liste des formations en cybersécurité

INSTITUT POLYTECHNIQUE DE PARIS

Master 1 Cybersécurité

Master 2 Cybersécurité

ÉCOLE POLYTECHNIQUE

Cycle Ingénieur Parcours d'Approfondissement Informatique, filière Cybersécurité

Bachelor Cybersécurité de l'EPITA-École polytechnique

Master of Science and Technology Cybersecurity

EXECUTIVE EDUCATION :

Executive MSc in Cybersecurity

Cybersécurité des projets IA

Enjeux des nouvelles menaces et des dispositifs électromagnétiques et lasers

Cybersécurité des systèmes embarqués

ENSTA

Cycle Ingénieur 3A Parcours Cybersécurité et architecture des systèmes d'information

TELECOM Paris

Cycle Ingénieur, filière cybersécurité en 2ème année et option en 3ème année

Formation d'ingénieur en apprentissage (FISEA)

Mastère Spécialisé® Cybersécurité et Cyberdéfense

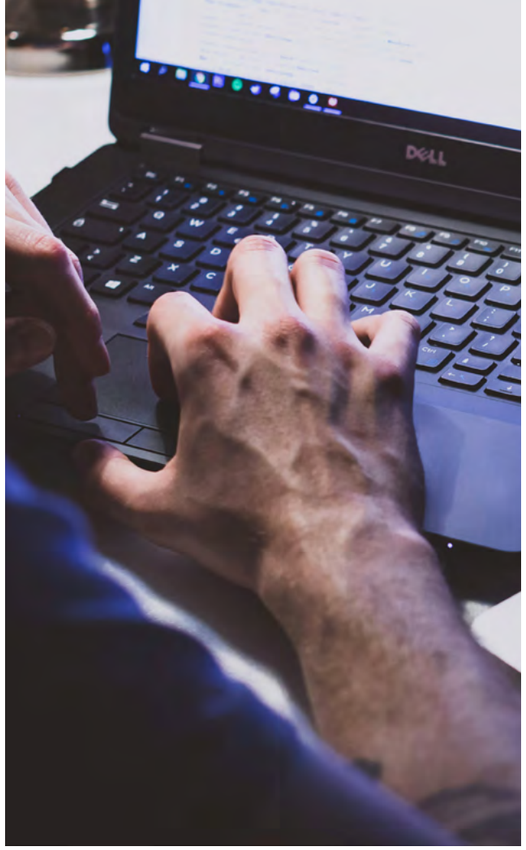
Mastère Spécialisé® Architecte Réseaux et Cybersécurité

Mastère Spécialisé® Expert Cybersécurité des Réseaux et des Systèmes d'information

EXECUTIVE EDUCATION :

Cybersécurité des Données, Réseaux et Systèmes

Architecture en cybersécurité



TELECOM SudParis

Cycle Ingénieur, option en 3ème année (FISE et FISA)

Mastère Spécialisé® Cybersécurité des Infrastructures et des Données

CMA "Train Cyber expert",
porté par Télécom SudParis, dispositif national de formation initiale et continue en cybersécurité, modulable et réutilisable, qui vise à former 10 000 experts d'ici 2030, et qui prépare aux certifications labellisées SecNumEdu par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Institut Polytechnique de Paris

L'Institut Polytechnique de Paris est un établissement public d'enseignement supérieur et de recherche qui fédère six grandes écoles d'ingénieurs françaises : l'École polytechnique, l'ENSTA, l'École nationale des ponts et chaussées (ENPC), l'ENSAE Paris, Télécom Paris et Télécom SudParis. Ensemble, ces écoles conjuguent leurs expertises pour proposer une formation d'excellence et conduire une recherche de haut niveau. Grâce à cet ancrage académique et scientifique unique, IP Paris s'affirme comme un acteur majeur des sciences et technologies en France et à l'international. https://www.ip-paris.fr/

Centre Interdisciplinaire d'Études pour la Défense et la Sécurité - (CIEDS)

L'Institut Polytechnique de Paris a créé le centre interdisciplinaire - CIEDS en 2021 pour imaginer et développer des réponses aux besoins technologiques du secteur de la Défense. Le CIEDS bénéficie d'un soutien fort du ministère des Armées et de l'Agence de l'Innovation de Défense ; il intervient sur les domaines scientifiques clés de l'IP Paris en matière de recherche, de formation et d'innovation pour y promouvoir une large prise en compte des problématiques liées à la Défense.
https://www.ip-paris.fr/cieds

Chaire Cyber et souveraineté numérique – (IHEDN)

La Chaire Cyber et souveraineté numérique – IHEDN s'inscrit dans l'effort de défense des intérêts stratégiques de la France et de sa souveraineté numérique. Elle a pour objectif de contribuer à la réflexion sur la souveraineté numérique et la cybersécurité, grâce à une recherche pluridisciplinaire, au carrefour entre les sciences de l'ingénieur et les sciences humaines et sociales. Elle vise à participer activement à l'effort national pour l'élaboration d'une stratégie de cybersécurité destinée aux entreprises, aux autorités gouvernementales et à la société civile. https://cyber-ihedn.fr/

INSTITUT POLYTECHNIQUE DE PARIS | ENSTA | PONTS | ENSAE | TELECOM Paris | TELECOM SudParis

En partenariat avec

CIEDS CENTRE INTERDISCIPLINAIRE D'ÉTUDES POUR LA DÉFENSE ET LA SÉCURITÉ

CHAIRE CYBER SOUVERAINETÉ NUMÉRIQUE IHEDN