



IMT Atlantique

Bretagne-Pays de la Loire
École Mines-Télécom

UNE GRANDE ÉCOLE D'INGÉNIEURS
GÉNÉRALISTES RECONNUE
INTERNATIONALEMENT POUR
L'EXCELLENCE DE SA RECHERCHE
www.imt-atlantique.fr

Une recherche d'excellence pour la sécurité
des systèmes complexes, de l'industrie
du futur et des infrastructures critiques



Forum International
de la Cybersecrité

SECURITY AND PRIVACY BY DESIGN

Europe ticks off!



IMT Atlantique au FIC 2019

Une recherche d'excellence pour la sécurité des systèmes complexes de l'industrie du futur et des infrastructures critiques



Pavillon « Bretagne-Pôle d'excellence cyber »

Stand D12

Sommaire

Nos experts au FIC	page 2
Les rendez-vous d'IMT Atlantique au FIC	page 3
Rencontrez les start-up issues de l'incubateur	page 4
La chaire cyberdéfense des systèmes navales	page 5
La chaire Cyber CNI	page 7
À propos d'IMT Atlantique	page 9

Nos experts au FIC 2019



Jean Le Traon

Directeur du campus de Rennes

Administrateur du **Pôle d'excellence cyber**



Gilles Coppin

Directeur du laboratoire CNRS Lab-STICC

**#intelligence #artificielle #industrie
#aéronautique #interaction Homme-Machine**



Yvon Kermarrec

Professeur

Directeur de la **Chaire Cyber défense des systèmes navals**

#naval #informatique #cyber attaque #cyber résilience



Frédéric Cuppens

Professeur au département Systèmes Réseaux, Cybersécurité et Droit du numérique

Porteur de la **Chaire Cyber CNI**

#Sécurité des systèmes #détection d'intrusion #FireWall



Gouenou Coatrieux

Professeur au département Image et traitement de l'information

**#cryptage #chiffrement de données d'imagerie
médicale partagées #tatouage de données**



Nora Cuppens

Directrice de recherche au département Systèmes Réseaux, Cybersécurité et Droit du numérique

#cyber sécurité #cyber défense #cyber résilience

Les rendez-vous d'IMT Atlantique au FIC

> *Pavillon Bretagne /Pôle excellence cyber – Stand D12*

Mardi 22 janvier à 14h00

Signature du renouvellement de la Chaire Cyber CNI

Après trois années de fonctionnement, la Chaire dédiée à la Cybersécurité des Infrastructures Critiques (Cyber CNI) est renouvelée pour une période équivalente grâce à l'engagement de ses partenaires académiques et industriels. Chaire de l'Institut Mines-Télécom, portée par IMT Atlantique, elle s'appuie sur le partenariat des écoles Télécom ParisTech et Télécom SudParis et bénéficie, dans le cadre du Pôle d'excellence cyber, du soutien du Conseil Régional de Bretagne, un territoire à la pointe de la cybersécurité. Cinq partenaires industriels s'engagent pour cette nouvelle période : AIRBUS, AMOSSYS, BNP Paribas, EDF et NOKIA.

Mercredi 23 janvier 2019 11h00

Master class spéciale FIC " **Towards a Secure Internet of Things: case of a German-French collaboration**" avec la participation de Frédéric Cuppens et Nora Cuppens, chercheurs à IMT Atlantique - Thématique : **Sécurité de l'internet des objets** (uniquement en anglais)

Mardi 22 et mercredi 23 janvier

La Chaire Cyberdéfense des systèmes navals recrute des doctorants ! À cette occasion le directeur de la chaire répond à toutes vos questions.

La Chaire Cyberdéfense des systèmes navals est une chaire de recherche (2014 à 2020) dans le domaine de la cyberdéfense des systèmes navals avec l'École Navale, Naval Group et Thalès comme partenaires.

Cryptage et tatouage pour protéger les données de santé.

Gouenou Coatrieux, expert en sécurité de l'imagerie et des données médicales vous parle des dernières évolutions scientifiques du domaine.

Le tatouage de données pourrait bien être la meilleure technique de traçabilité des données de santé dans un avenir proche. Elle revient à inscrire des informations cachées dans les images médicales, pour assurer sécurité et confidentialité aux patients et aux professionnels de santé.

Rencontrez les starts-up issues de l'incubateur d'IMT Atlantique !

WaToo

« Lutter contre le détournement et la fuite de données sensibles par des utilisateurs autorisés. »

WaToo est une société issue de la recherche spécialisée dans la lutte contre la fuite, le détournement et la falsification de données et de documents sensibles par des utilisateurs autorisés (p.e. des personnels, des collaborateurs). Elle propose notamment la solution WaTrack qui permet de protéger des bases de données ou des documents mises à disposition de collaborateurs ou vendues sous licence. Il identifiera le partenaire ou le client peu scrupuleux qui aura fuité ou revendu illégalement l'information. www.watoo.tech

Acklio

Acklio développe des logiciels visant à faciliter et sécuriser le développement, l'intégration et l'exploitation des déploiements IoT. Créée à Rennes en 2016, la start-up est à l'origine d'une technologie qui permet l'utilisation d'IP aux réseaux émergents de l'internet des objets. Cette technologie, aujourd'hui exclusivité d'Acklio, est en passe d'être reconnue comme standard international par l'IETF. www.ackl.io

Secure IC

« Fournisseur de technologies de protection des systèmes électroniques embarqués vis-à-vis d'attaques malveillantes et de menaces cyber. »

Les produits et services de Secure IC : Technologies de protection des systèmes électroniques embarqués contre la modification et la falsification, Cryptographie propriétaire, Technologies de génération et de protection de clés secrètes, Génération d'aléa, Évaluation de la sécurité pré-silicium, Évaluation de la sécurité post-silicium, Protection des contenu multimédia, Cryptographie post-quantique, Consulting/ Expertise, Tutoriels/Training, Projets spéciaux, Projets collaboratifs, Standardisation. www.secure-ic.com

Yagaan

« L'analyse de vulnérabilité du code source s'adapte à votre contexte et à votre métier. »

Si les vulnérabilités élémentaires sont universelles, chaque métier, chaque usage (applications, objets connectés, produits ou systèmes) a aussi ses propres risques et ses propres besoins de sécurité. Pour tenir compte des spécificités de chaque métier, Yagaan a conçu YAG Suite : la première solution qui combine l'analyse statique de code au machine learning pour qualifier intelligemment les alertes selon le contexte. www.yagaan.com

Woleet

« Fournisseur de vérité numérique »

La plateforme Woleet ancre vos données dans la blockchain Bitcoin pour créer une preuve d'existence horodatée, universelle et interopérable et garantir leur intégrité.

Deux avantages pour l'utilisateur : la possibilité de vérifier la preuve déclarée sans passer par un tiers de confiance (format de preuve ouvert) ni que le propriétaire de la donnée n'ait à la divulguer. www.woleet.io



Des partenaires engagés au service de la sécurité numérique des systèmes navals

La cyberdéfense a été érigée au rang de priorité nationale par le Livre blanc de la défense et la sécurité nationale de 2013. En créant en octobre 2014 la chaire de cyberdéfense des systèmes navals, l'École navale, l'ENSTA Bretagne, IMT Atlantique, Naval Group et Thales couvrent la composante navale de la cyberdéfense. Le projet est soutenu par la région Bretagne et le Pôle d'Excellence Cyber.

Les partenaires (leaders industriels de leur secteur) et les enseignants-chercheurs (experts scientifiques en cyberdéfense) confortent l'expertise cyber de la chaire.

En associant formation et recherche, la chaire occupe une place privilégiée et spécifique dans le secteur de la cyberdéfense. Cette spécificité est valorisée et légitimée par un choix de partenaires solides et reconnus du secteur occupe une place de tout premier rang : la chaire correspond pleinement aux besoins actuels en termes de formations d'experts en cybersécurité, de développement de nouveaux outils et d'approches stratégiques afin de protéger les systèmes d'information de plus en plus complexes.

Enfin, la dualité du domaine civil et militaire maritime fera bénéficier à l'ensemble des acteurs des avancées de cette chaire.

La formation et la sensibilisation

- Former les futurs acteurs des systèmes d'information à la cybersécurité, et leur permettre ainsi de connaître les points de vigilance et les pistes de solutions.
- Sensibiliser les acteurs actuels et leur permettre d'anticiper la gestion des prochaines attaques et d'y réagir le plus efficacement possible via des plateformes et autres exercices : intégration de cours en cybersécurité dans le cursus de formation des officiers de la Marine Nationale.
- Former des experts en cyber sécurité dans le milieu maritime via les études doctorales.

La recherche

- Garantir un enseignement supérieur de qualité, un haut niveau de compétences et le développement d'un tissu industriel de pointe.
- Explorer et proposer de nouvelles approches et outils afin de protéger ces systèmes complexes.

Les thématiques scientifiques

- La protection des informations sensibles embarquées,
- L'analyse de la fiabilité et de l'intégrité des informations collectées par les capteurs et utilisées par les systèmes d'information des navires,
- L'analyse des failles de sécurité et intrusions affectant ces derniers,
- Le déploiement de correctifs logiciels adaptés en cas de besoin, ainsi que toute autre réaction nécessaire au rétablissement de la sécurité des systèmes,
- L'aide à la prise de décisions en situations critiques.

La chaire de Cyberdéfense des systèmes navals recrute des doctorants

La cybersécurité est avant tout une question de souveraineté nationale. La sécurité numérique est une clé de la maîtrise de tout système qui demain sera en réseau et sécurisé au bon niveau ou ne « sera pas » !

La chaire de cyberdéfense des systèmes navals s'inscrit ainsi au cœur d'un écosystème très sensible et éminemment stratégique porté par des problématiques croissantes d'attaques maritimes et d'activités criminelles.

La chaire recrute des doctorants afin de former des experts en cybersécurité dans le milieu maritime.

L'équipe au 1er janvier 2019 : 10 doctorants, 4 nouveaux docteurs, 15 enseignants chercheurs, 10 experts Naval Group et Thales, 1 automaticien, 1 chargée de communication.

www.chaire-cyber-navale.fr



Renouvellement de la Chaire Cyber CNI Signature par les partenaires lors du FIC 2019, le 22 janvier à Lille

Après trois années de fonctionnement, la Chaire dédiée à la Cybersécurité des Infrastructures Critiques (Cyber CNI) est renouvelée pour une période équivalente grâce à l'engagement de ses partenaires académiques et industriels. Chaire de l'Institut Mines-Télécom, portée par IMT Atlantique, elle s'appuie sur le partenariat des écoles Télécom ParisTech et Télécom SudParis et bénéficie, dans le cadre du Pôle d'excellence cyber, du soutien du Conseil Régional de Bretagne, un territoire à la pointe de la cybersécurité.

Cinq partenaires industriels s'engagent pour cette nouvelle période : AIRBUS, AMOSSYS, BNP Paribas, EDF et NOKIA. La signature de renouvellement de la Chaire aura lieu lors du FIC (Forum International de la Cybersécurité) à Lille le 22 janvier 2019 à 14h.

Inaugurée en janvier 2016, la Chaire Cyber CNI conduit depuis des travaux de recherche et participe à la formation dans son domaine de spécialité, la cybersécurité des infrastructures critiques (réseaux d'énergie, processus industriels, usines de production d'eau, systèmes financiers, ...). Cette discipline scientifique récente est rapidement devenue un sujet inévitable pour bon nombre d'entreprises et d'organisations.

Cette première phase de la chaire a permis des avancées significatives pour améliorer la sécurité et la résilience des infrastructures, notamment dans les domaines de la détection de comportements malveillants en utilisant des techniques d'apprentissage automatique, de la visualisation 3D d'événements de sécurité ou du diagnostic des causes accidentelles ou malveillantes d'un incident de sécurité.

Si la thématique principale reste la cybersécurité des infrastructures critiques, la Chaire Cyber CNI élargit, dans sa phase 2, son domaine d'expertise et de recherche : le renforcement des actions concernant l'application de l'intelligence artificielle (IA) à la cybersécurité, le partage et la mutualisation des renseignements sur la menace (*Threat Intelligence*), les applications industrielles des objets connectés (*Industrial IoT*), la blockchain... figurent ainsi parmi ses nouvelles thématiques de recherche.



IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

De nouvelles thèses porteront ces objectifs, en complément de celles déjà ouvertes. En parallèle, la phase 2 de la Chaire Cyber CNI prévoit un renforcement des actions de communication, des événements de promotion, et *in fine*, de la valorisation des travaux réalisés.

« La Chaire Cyber CNI, portée par IMT Atlantique, est historiquement une des premières traitant de cybersécurité à ce niveau majeur de compétence et d'innovation sur le sujet complexe des infrastructures critiques. Le travail effectué ces dernières années, déjà remarquable, va se poursuivre par un engagement réitéré de tous, académiques, industriels, partenaires, étudiants, doctorants, dans la seconde phase du processus, autour de nouveaux sujets primordiaux. Le renouvellement de la chaire est donc à ce titre d'une importance cruciale, que justifient des nouveaux axes de recherche, des enjeux toujours croissants, mais aussi une attente importante des contributeurs dont les besoins sont toujours et justement plus prégnants. », Serge Maurice, Airbus & président du Comité de pilotage de la Chaire Cyber CNI.

www.chairecyber-cni.org

À propos d'IMT Atlantique

IMT Atlantique est une grande école d'ingénieurs généralistes (parmi les 400 premières universités du monde du THE World University Ranking 2019, en 3ème position des écoles d'ingénieur de France), reconnue internationalement pour sa recherche (présente dans 4 thématiques du classement de Shanghai). Elle appartient à l'Institut Mines-Télécom et dépend du ministère en charge de l'industrie et du numérique.

Les formations d'IMT Atlantique s'appuient sur une recherche de pointe, au sein de 6 unités mixtes de recherche (avec le CNRS, l'INRIA, l'INSERM, des universités ou écoles d'ingénieur), dont elle est tutelle : GEPEA, IRISA, LATIM, LABSTICC, LS2N et SUBATECH. L'école s'appuie sur son excellence en recherche dans ses domaines phares (énergie et numérique, cybersécurité, environnement et numérique, industrie du futur, nucléaire, santé et numérique, risques et interactions) et en couplant les domaines scientifiques pour répondre aux défis de demain : transition numérique, transition environnementale, transition industrielle, transition énergétique, santé du futur et recherche fondamentale.

IMT Atlantique est labellisée Carnot pour la qualité de sa recherche partenariale, en tant que composante du Carnot Télécom & Société Numérique (TSN) et du Carnot M.I.N.E.S. (Méthodes Innovantes pour l'Entreprise et la Société).

www.imt-atlantique.fr

Contacts presse

IMT Atlantique Bretagne-Pays de la Loire

Pricillia Creach
Responsable du pôle médias et promotion
Tél. 06 30 51 38 30
priscillia.creach@imt-atlantique.fr
www.imt-atlantique.fr

Green Lemon Communication

Laurence Le Masle
Tél. 06 13 56 23 98
l.lemasle@greenlemoncommunication.com
www.greenlemoncommunication.com
[@greenlemoncom](https://twitter.com/greenlemoncom)

