

Colloque IMT

« Entrons-nous dans une nouvelle ère de la Cyber-sécurité ? »

Etat de l'art de la menace : retour sur les attaques en Ukraine

Romain Françoise - CTO

Sentryo

romain.francoise@sentryo.net



Diplômé de l'INSA de Lyon en 2003, Romain débute sa carrière chez Arkoon Network Security et travaille pendant plus de 10 ans sur la cybersécurité des réseaux IT. En 2014, Romain est invité à participer à une nouvelle aventure : Sentryo. Il est depuis CTO de Sentryo, un pionnier de la cybersécurité de l'internet industriel. Il est également contributeur au logiciel libre, dans les projets Debian et GNU.

Combiner attaques logicielles et matérielles : Exemple des lampes connectées Philips Hue

Olivier Potin - Maître-Assistant

Département "Systèmes et Architectures Sécurisées",

Mines St Etienne

olivier.potin@emse.fr



Olivier Potin est Maître-Assistant à Mines Saint-Etienne dans le département "Systèmes et Architectures Sécurisées" au Centre de Microélectronique de Provence de Gardanne depuis 2014. Ses domaines de recherches concernent les attaques par canaux cachés et le développement de contre-mesures matérielles/logicielles. Il a collaboré avec le CEA sur la compilation dynamique pour la sécurité, Gemalto sur le développement d'attaques et de contre-mesures sur TrustZone, STMicroelectronics sur le développement d'un capteur pour la détection d'attaques LASER sur ASIC,... dans le cadre de projets ANR et FUI. Auparavant il a été cofondateur et responsable technique d'ORIDAO (Développement d'un algorithme cryptographique pour la traçabilité RFID et la lutte contre la contrefaçon) et obtenu un doctorat au Laboratoire d'Informatique, Robotique et Microélectronique de Montpellier (LIRMM) en 1996 et un Master "Administration des Entreprises" à l'Université de Montpellier en 2008.

Détection des attaques contre les systèmes cyber-physiques industriels

Joaquin Garcia-Alfaro - Enseignant-chercheur

Département Réseaux et Services de Télécom (RST),

Télécom Sud Paris

joaquin.garcia_alfaro@Télécom-sudparis.eu



Joaquin Garcia-Alfaro est professeur à Télécom SudParis, département RST. Il est ingénieur et docteur en informatique ; et habilité à diriger des recherches. Il est membre senior de l'IEEE et de l'ACM. Ses principaux thèmes de recherche se concentrent sur les problèmes de sécurité réseau, la gestion des politiques de sécurité, l'analyse des vulnérabilités et la proposition des contre-mesures. Il a été chercheur invité à l'Université Carleton (Ottawa, Canada), Université Concordia (Montréal, Canada), Université Ryerson (Toronto, Canada), Université Ouverte de Catalogne (Barcelone, Espagne) et Université Autonome de Barcelone (Bellaterra, Espagne). Il est co-auteur de plus de 100 articles dans des revues et des conférences internationales à comité de lecture. Il a fait partie de nombreux comités de programme de conférences nationales et internationales. Il a été organisateur et président des comités de programme des conférences ATC 2017, RAID 2016, FPS 2015, AIDP 2014, DPM 2013, FPS 2012, SETOP 2011. Il est le référent Télécom SudParis pour la chaire CNI (Cybersécurité des infrastructures critiques) de l'Institut Mines-Télécom.

Approches matérielles pour contrer les attaques logicielles

Jean-Luc Danger - Enseignant-chercheur

Dépt. Communications et Electronique (COMELEC)

Télécom ParisTech

jean-luc.danger@Télécom-paristech.fr



Jean-Luc Danger is full Professor at Télécom ParisTech (www.Télécom-paristech.fr/). He is the head of the digital electronic system research group where research topics are about of security / safety for embedded systems, configurable architectures, implementation of complex algorithms in ASICs or FPGAs. Jean-Luc authored more than 200 scientific publications and 20 patents in architectures of embedded systems and security, and is co-founder of the company Secure-IC (www.secure-ic.com). He received his engineering degree in Electrical Engineering from Ecole Supérieure d'Electricité in 1981. After 12 years in industrial laboratories (PHILIPS,NOKIA), he joined Télécom ParisTech in 1993 where he became full professor in 2002. His personal research interests are trusted computing, cyber-security, random number generation, protected implementations in novel technologies.

Cybersécurité des infrastructures critiques

Simon Foley - Enseignant-chercheur

Département Systèmes Réseaux, Cybersécurité et Droit du numérique (SRCD)

IMT Atlantique

simon.foley@imt-atlantique.fr



Simon Foley est Directeur de Recherche (Cybersécurité) à l'Institut Mines-Télécom / IMT Atlantique (anciennement Télécom Bretagne) à Rennes. Auparavant, il était chargé de cours statutaire en informatique à University College Cork en Irlande.

Ses intérêts de recherche incluent les contrôles d'accès distribués / réseau, la confiance, l'analyse de sécurité, la gestion des risques de sécurité et la sécurité des infrastructures critiques. Ses recherches portent sur la conception et l'analyse des systèmes de sécurité technologique. Il est membre des comités de rédaction du Journal of Computer Security et de la International Journal of Information Privacy, Security and Integrity ; Coprésident du PC pour le Symposium européen sur la recherche en sécurité informatique et ancien président de la NSPW et de la CSF.

Activités de la chaire de cyber défense des systèmes navals

Yvon Kermarrec - Enseignant-chercheur

Département Logique des Usages - Sciences Sociales de l'Information (LUSSI)

IMT Atlantique

yvon.kermarrec@imt-atlantique.fr



Yvon Kermarrec est Professeur en informatique à IMT Atlantique et fut responsable du département de recherche LUSSI (Logiques d'utilisation, sciences sociales et sciences de l'information). Ses activités de recherche et d'enseignement sont en lien avec les systèmes distribués, le génie logiciel, la fiabilité et la sécurité. Il a été chercheur à Courant Institute de New York University, architecte logiciel avec Raytheon (Vancouver) avant de rejoindre Télécom ParisTech et Télécom Bretagne.

Il est actuellement détaché auprès de l'école Navale, où il coordonne les activités de recherche de la chaire de cyber défense des systèmes navals en lien avec les partenaires (l'école Navale, IMT Atlantique, Thales, Naval Group, et la Région Bretagne).

"Comment enclencher réellement la mise en mouvement des organisations en Sécurité Opérationnelle"

Gérard Gaudin - Consultant

gerard.gaudin2@wanadoo.fr



Gérard Gaudin est Consultant international indépendant G²C et Président du Club R2GS. Gérard GAUDIN est ingénieur diplômé de l'École Supérieure d'Électricité (Supelec 79). Après un passage dans 2 multinationales françaises du secteur des technologies de l'information, il a exercé au sein de CS en tant que cadre dirigeant de nombreuses responsabilités de management de centres de profit importants, dans divers domaines relatifs à l'IT et à la SSI (correspondant à des tailles d'équipe allant jusqu'à 300 ingénieurs et des chiffres d'affaires jusqu'à 40 M€). Depuis 2003, il mène en tant que consultant international indépendant (G²C) des missions dans le domaine SSI, avec un accent particulier sur la Cyber Défense et le SIEM. Dans ce contexte, il a créé à la fin de l'année 2008 le Club R2GS (Réflexion et Recherche en Gestion opérationnelle de la Sécurité), dont il est le Président et qui regroupe plus de 250 personnes (dont nombre de RSSI) appartenant à plus de 50 grandes entreprises et organisations parmi les plus avancées en France sur les thèmes Cyber Défense et SIEM. Ce club a un prolongement en Europe avec la constitution progressive d'un réseau complet de chapitres ou d'associations « clones » (Royaume-Uni, Allemagne, Italie, Belgique, Luxembourg) coordonnés par le Club R2GS Europe, association qu'il préside également. De plus, il est l'initiateur et le Président au sein de l'ETSI (Un des principaux organismes de standardisation internationaux dans le domaine IT) d'une entité dénommée ISG ISI (Information Security Indicators), dédiée à l'ensemble des aspects de détection des événements de sécurité (dont indicateurs opérationnels, modèle de classification, échelle de maturité et procédures de tests), qui se positionne au cœur de réglementations ou de lois, comme la LPM volet Cyber, la Directive NIS ou le règlement RGPD.

De l'analyse morphologique à Cyber-Detect : valorisons les virus !

Jean-Yves Marion – Directeur du LORIA

Mines Nancy

jean-yves.marion@mines-nancy.univ-lorraine.fr



Jean-Yves Marion is director of Loria (cnrs, Inria, université de Lorraine) and member of Institut Universitaire de France. Jean-Yves Marion got a Ph.D. in Computer Science from Paris 7 University in 1991. He had a Post Doctoral Research position at Indiana University in 1992 and in 1993. From 1995 to 2002, he was Assistant Professor (maître de conférences) at Nancy 2 University (IUT Charlemagne in the computer science dept). He obtained an "Habilitation à diriger les Recherches" (HDR) in 2000. He is one of the co-founders of High Security Lab (LHS).

Fraude dans la téléphonie

Aurélien Francillon – Maître de Conférences

Sécurité numérique

Eurecom

Aurelien.Francillon@eurecom.fr



Aurélien Francillon est actuellement Maître de conférences au sein du département Sécurité numérique d'Eurecom où il enseigne la sécurité système et réseaux. Ses principaux intérêts de recherche concernent la sécurité des systèmes embarqués, des microcontrôleurs aux smartphones. Pour étudier la sécurité de ces systèmes et leurs applications, une approche holistique est nécessaire de leur conception à leur déploiement.

Il s'intéresse aussi à plusieurs thèmes tels que la sécurité logicielle, le support matériel pour la sécurité logicielle, la sécurité des réseaux sans fil ainsi que plus récemment à la fraude dans la téléphonie.

Fuite d'information - Identification de l'origine par le tatouage des données

Gouenou Coatrieux - Professeur

Département Image et Traitement de l'Information (ITI)

IMT Atlantique

gouenou.coatrieux@imt-atlantique.fr



He is currently a full professor with the Information and Image Processing Department, IMT Atlantique, Brest. He conducts his research in the Laboratory of Medical Information Processing, Inserm UMR1101, Brest, where he leads the research axis METIS (multimedia medical information analysis, protection and secondary use). He is also the head of the joint laboratory SePEMeD (Security and Processing of Externalized Medical Image Data).

His primary research interests concern watermarking (images and databases), crypto-watermarking, secure processing of outsourced data & big health data, information system security, digital forensics. He is a member of the International Federation for Medical and Biological Engineering "Global Citizen Safety and Security Working Group" and the European Federation for Medical Informatics "Security, Safety, and Ethics Working Group," and has contributed to the Technical Committee of "Information Technology for Health" of the IEEE Emb Society. He is an Associate Editor of the Innovation and Research in Bio-Medical and past associate editor of Engineering and of the IEEE Journal on Biomedical and Health Informatics, Digital Signal Processing.

Leverage SDN and NFV to achieve software-defined security

Zonghua Zhang – Enseignant-chercheur

Dépt Informatique et Réseaux (DEPT/IR)

IMT Lille Douai

zonghua.zhang@Télécom-lille.fr



Zonghua Zhang est un enseignant-chercheur à l'IMT Lille Douai, Institut Mines-Télécom. Auparavant, il a occupé le poste de chercheur au NICT (Japon), à l'INRIA et l'Université de Waterloo (Canada). Il est titulaire d'un diplôme de doctorat (JAIST, Japon), et a obtenu une HDR (UPMC, France) en informatique. Il possède une expérience de plus de 17 ans dans le domaine de la sécurité de l'information et des réseaux et a contribué à plus d'une douzaine de projets collaboratifs nationaux et internationaux dans ce domaine. Ses sujets de recherche couvrent la détection d'anomalies, la gestion de réputation et de confiance, ainsi que les protocoles de sécurité. Ses intérêts actuels incluent les technologies Software-Defined Networking (SDN) et Network Functions Virtualization (NFV), ainsi que les systèmes cyber-physiques (CPS) (santé connectée et systèmes de transports intelligents (ITS)). Il est membre du comité de rédaction des quatre revues internationale.

Vie Privée: De l'empire des mots à la tyrannie des chiffres, quel chemin choisir ?

Isabelle Landreau – Avocate

SMART LAW FABRIK

isabelle.landreau.avocat@droitdanslemil.fr



Isabelle Landreau est Docteur en droit, avocate spécialisée en droit de la propriété intellectuelle, des nouvelles technologies et des libertés individuelles. Elle a plus de 14 ans d'expérience en tant qu'avocate sur Paris pour des affaires françaises, européennes et internationales. Elle a fondé son propre cabinet SMART LAW FABRIK depuis plus de 7 ans, résolument tourné vers la DATA et l'IA. Elle a commencé sa carrière en tant que professeur associé au Japon, puis juriste d'entreprise en France et aux Etats-Unis. Elle a passé deux ans au Japon pour sa thèse. Elle est formatrice à l'Ecole de Formation du Barreau et chargée de cours dans deux écoles d'ingénieurs sur le cyberdroit.

Elle est aussi médiatrice diplômée depuis 2015 par l'école de formation du Barreau de Paris. Elle donne régulièrement des conférences sur la Data, et est l'auteur de plusieurs articles et ouvrages sur la donnée, les actions de groupe et les marques, en français et en anglais.

Sa pratique d'avocat se concentre sur la protection du citoyen et des PME dans l'utilisation de la data. Elle est aussi vice-Présidente du Cercle des Femmes dans la Cybersécurité (CEFCYS) pour lequel elle anime les colloques et est en charge des partenariats.

Elle est membre de l'association des Avocats Conseil en Entreprises, et de l'ADIJ.

Qui seront les nouveaux fournisseurs de données personnelles

Philippe Jaillon – Enseignant-chercheur

FAYOL - Informatique et systèmes intelligents

Mines St Etienne

philippe.jaillon@mines-stetienne.fr



Philippe Jaillon est enseignant chercheur à l'école des mines de Saint-Etienne. Depuis de nombreuses années il est en charge des enseignements dans les domaines des réseaux de communications et de la sécurité des systèmes d'informations. Ses activités de recherche sont centrées de manière générale sur la sécurité des systèmes d'informations et la sécurité de l'internet des objets. Il s'intéresse aux conséquences de l'exploitation des défauts logiciels et protocolaires sur la vie privée des utilisateurs. Dernièrement il a rejoint l'équipe commune CEA/EMSE SAS (Système et Applications Sécurisés) du centre de Micro-électronique de Provence. Dans ce cadre il s'intéresse aux problèmes que posent les attaques conjointes sur le matériel et le logiciel. Les premiers travaux, initiés avec Télécom Sud-Paris, concernent les réseaux optiques à très haut débit et font l'objet cette année d'un financement dans le cadre de l'inter-Carnot Mines/Télécom.

Données génétiques et vie privée

Mario Südholt – Enseignant-chercheur

Département Automatique Productive Informatique
(DAPI)

IMT Atlantique

mario.sudholt@imt-atlantique.fr



Mario Südholt est professeur titulaire en informatique à l'École des Mines de Nantes, en France, où il occupe la chaire de génie logiciel et de programmation. Il est titulaire d'un MSc de U. Koblenz, Allemagne, d'un doctorat de TU Berlin, Allemagne, et d'une habilitation de l'Université de Nantes, France. Il dirige l'équipe ASCOLA, une équipe conjointe d'EMNantes et d'INRIA qui fait également partie de l'institut LINA (CNRS). Ses intérêts de recherche se concentrent sur les systèmes logiciels à grande échelle, typiquement distribués, leur définition formelle, leurs propriétés compositionnelles, leur mise en œuvre efficace et le support correspondant dans les langages de programmation. Depuis 2011, le professeur Südholt préside l'association internationale de l'AOSD, y compris le comité de pilotage de la conférence de l'AOSD. De plus, il est membre du comité de direction de la conférence internationale sur la composition de logiciels et siège au comité de rédaction de la revue Transactions on AOSD.

GDPR: for an auditable user consent

Maryline Laurent – Professeur

RST Réseaux et Services de Télécom

Télécom SudParis

maryline.laurent@Télécom-sudparis.eu



Maryline Laurent est professeur au département RST Réseaux et Services de Télécom à Télécom SudParis.

Elle est responsable de l'équipe R3S (Réseaux, Systèmes, Services, Sécurité) du laboratoire CNRS SAMOVAR (UMR5157), co-fondatrice de la chaire Institut-Mines-Télécom Valeurs et politiques des informations personnelles et co-directrice du pôle 2 « Réseaux, Information et Communications » de l'Ecole Doctorale STIC de l'Université Paris-Saclay.

Contrôle des flux sur Android

Nora Cuppens – Directrice de recherche

Département Systèmes Réseaux, Cybersécurité et Droit du numérique (SRCD)

IMT Atlantique

nora.cuppens@imt-atlantique.fr



Nora Cuppens est directrice de recherche à IMT Atlantique de l'Institut Mines-Télécom. Elle est titulaire d'un diplôme d'ingénieur en informatique, d'un doctorat de l'ENSAE (Ecole Nationale Supérieure de l'Aéronautique et de l'Espace - Sup'Aero) et d'un HDR de l'Université de Rennes 1.

Ses intérêts de recherche incluent la formalisation des propriétés et des politiques de sécurité, l'analyse de protocoles cryptographiques, la validation formelle des propriétés de sécurité et l'évaluation des risques de réaction. Ses sujets de recherche actuels comprennent la détection et la réaction aux intrusions, le contrôle et la traçabilité de l'accès et de l'utilisation a posteriori, la préservation de la vie privée par la réécriture des requêtes, la fragmentation des données et l'anonymisation.

Elle a publié plus de 170 articles techniques dans des revues à comité de lecture et des actes de conférences. Elle a été membre de plusieurs comités de programme internationaux dans le domaine du système de sécurité de l'information et présidente du comité de programme de plusieurs conférences et tutoriels.

Elle est responsable du programme transversal Cybersécurité Cyrus de LabSTICC (laboratoire de recherche CNRS de IMT Atlantique), membre de l'équipe de sécurité IRIS de ce laboratoire et la référente IMT Atlantique pour la chaire CyberCNI.

Elle est la représentante française de IFIP TC11 "Information Security", deux IFIP Outstanding Service Awards lui ont été décernés en 2016 et 2017. Elle est membre du groupe de travail Cyber Security d'Allistène au titre de la CDEFI et membre du comité consultatif éditorial du Computer & Security Journal d'Elsevier et de l'International Journal on Advances in Security.

TABLE RONDE

« Les défenseurs peuvent-ils être en avance sur les attaquants »

Aline Richard – Editrice Sciences et Technologies

The Conversation

aline.richard@theconversation.fr



Journaliste scientifique et auteur de livres et documentaires, Aline Richard collabore à Marianne, au Figaro Santé et est chargée de cours à l'Institut Pratique de Journalisme (IPJ Paris-Dauphine). Précédemment, elle a occupé les postes de directrice de la rédaction du magazine La Recherche ; journaliste spécialisée énergie et matières premières à La Tribune, Capital et Infomatin.

Olivier Bettan – Responsable R&D Cyber Security

Thalès

Olivier.bettan@thalesgroup.com



Olivier Bettan is head of the cybersecurity laboratory in a Global Business Unit of Thales dedicated to Critical Information Systems. He is currently a Thales representative at the ECSO cPPP. He has obtained his diploma in Mathematics and Computer Science (DEA in cryptography) from University of Versailles Saint-Quentin (UVSQ) in 2004. Before joining Thales he was responsible of large aeronautic software certification under DO-178B standard. Since 2007, as a Thales R&T projects leader, he managed and contributed to Security related National -ANR, Celtic, FUI, PIA- and European -FP7 & H2020- projects (e.g. PROUV'e, PoSecCo, FIWARE, OPTET, 5GENSURE, HC@WORKS, DOGANA ...).

Florent Kirchner – Chef du laboratoire pour la sécurité et sûreté du logiciel

CEA List

Florent.kirchner@cea.fr



Florent Kirchner leads the Software Safety and Security Laboratory as well as the Cybersecurity Program at CEA LIST. As a senior expert scientist, he has developed and applied several approaches to high-confidence software verification, both as part of academic and industrial projects. He was active in launching and heading collaborative efforts with a wide variety of international partners, including collaborations with Airbus, Bureau Veritas, NASA, and SRI International. As a Head of Laboratory he is responsible for a group of 40 scientists working on the research and development of software analysis techniques, and the associated dissemination and communication activities. He is an active member of several working groups on High-Confidence Software at Systematic, Allistène, GdR, NIS, and ECSO.

Nicolas Lorient – Sr. Expert Cyber Defense

Airbus Defense and Space

nicolas.lorient@airbus.com



Nicolas LORIENT est senior expert en cyber défense dans le groupe Airbus, spécialisé depuis douze ans sur les thématiques de détection et réaction sur incidents de sécurité lors de la mise en place et l'accompagnement de SOC. Il porte un intérêt particulier sur l'adaptation au métier client de la supervision, le facteur humain face aux technologies, les problématiques opérationnelles, et sur l'adaptation continue des systèmes et mesures de détections à la menace. Nicolas a un diplôme d'ingénieur EFREI avec une spécialisation Télécom-Réseau.

Frédéric Cuppens –Professeur

Département Systèmes Réseaux, Cybersécurité et Droit du numérique (SRCD)

IMT Atlantique

frederic.cuppens@imt-atlantique.fr



Frédéric Cuppens est professeur à IMT Atlantique, Campus de Rennes, et responsable de l'équipe IRIS (Sécurité et Résilience des Systèmes) du Lab-STICC. Il est porteur de la chaire Cybersécurité des Infrastructures Critiques et animateur de Club Formation du Pôle d'Excellence Cyber. Il a obtenu un doctorat de l'École Nationale Supérieure de l'Aéronautique et de l'Espace et une Habilitation à Diriger les Recherches de l'Université de Toulouse III. Il mène des travaux de recherche dans le domaine de la sécurité des systèmes d'informations et des systèmes de contrôle industriel (expression, déploiement et validation formelle de politiques de sécurité, détection et réaction aux intrusions). Il a publié plus de 250 articles dans des conférences et des revues internationales. Il a été président du comité de programme des nombreuses conférences en cybersécurité telles que ESORICS, IFIP SEC, DBSEC, CRISIS, FPS ou PST. Il a reçu la médaille Ampère de la SEE en 2015 et un Outstanding Research Award de l'IFIP en 2016.

Hervé Debar – Directeur de département

RST Réseaux et Services de Télécom

Télécom SudParis

herve.debar@Télécom-sudparis.eu



Hervé Debar est professeur à Télécom SudParis, responsable du département Réseaux et Télécommunications et de l'option de 3e année Sécurité des Systèmes et des Réseaux (SSR). Son activité de recherche se concentre depuis 25 ans au domaine de la cybersécurité. Ses centres d'intérêt actuels incluent la protection des systèmes d'information et des réseaux notamment industriels, la détection d'attaques et la réponse à ces attaques. Il est impliqué dans plusieurs projets de recherche internationaux, notamment la coordination du dialogue cybersécurité entre l'Europe et le Japon. Il est vice président académique du comité de pilotage Confiance Numérique et Sécurité du Pole System@tic, et membre élu du partnership board de l'association européenne de cybersécurité (ECISO)
