LA GAZETTE DU GDR Sécurité informatique- En direct des Labos (LAAS-CNRS)

Mohamed Kaâniche

Juillet 2023
Numéro 15

LA GAZETTE DU GDR

Sécurité Informatique - GDR2046

Édito de la directrice

Les journées nationales et l'école d'été viennent de s'achever. Ce sont des temps forts mêlant l'ensemble des thématiques du GDR, et nous vous en reparlerons dans le prochain numéro de l'automne. Ce numéro estival sera consacré aux autres événements organisés durant le printemps : journées résidentielles du GT MFS en mars, RESSI pour le GT SSLR ainsi qu'une journée du GT SDM en mai, et enfin APVP pour le GT PVP en juin.

Et notre tour de France des laboratoires se poursuit : nous partons pour Toulouse au LAAS pour découvrir ses activités en cybersécurité. Et nous ferons un petit détour par le FIC organisé à Lille en avril.

Un grand merci à celles et ceux qui ont partagé leur passion et leur enthousiasme, et qui ont organisé les événements de ce printemps. Si vous souhaitez vous aussi partager une expérience originale et enrichissante, n'hésitez pas à nous contacter.

Bonne lecture, bel été et bonnes vacances !

Caroline Fontaine,

Directrice du GDR Sécurité Informatique

Rubriques

Événements

(Evénements organisés ou labellisés par le GDR, https://gdr-securite.irisa.fr/lagenda/)

Journées du GT C2, *Najac, Aveyron France, 15-20 octobre 2023*

(Autres événements, repris en partie du forum du GDR)

Ecole d'été ARTificial Intelligence in Secure Applicatio Ns (ARTISAN), *Vienne, Autriche, 17-20 juillet 2023*

Workshop on Deconstructing Gamified Approaches to Security and Privacy (DGASP 2023), *co-organisé avec SOUPS 2023, Anaheim, Californie, Etats-Unis, 6 août 2023*

18th International Conference on Availability, Reliability and Security (ARES 2023) et 4th International Workshop on Graph-based Approaches for CyberSecurity (GRASEC 2023), *Bénévent, Italie, 29 août - 1 septembre 2023*

Cryptographic Hardware and Embedded Systems conference (CHES 2023), *Prague, République Tchèque, 10-14 septembre 2023*

3rd International Workshop on Designing and Measuring security in Software Architecture (DeMeSSA 2023), *co-organisé avec ECSA 2023, Istanbul, Turquie, 18-22 septembre 2023*

18th International Workshop on Data Privacy Management (DPM 2023) et 7th International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2023), *coorganisé avec ESORICS 2023, The Hague, Pays Bas, 25-29 septembre 2023*

Journée thématique sur les Attaques par Injection de Fautes (JAIF), *Gardanne, France, 28 septembre 2023*

5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2023), *Paris, France, 11-13 octobre 2023*

12th Workshop on Programming Languages and Operating Systems (PLOS 2023), *coorganisé avec SOSP 2023, Koblenz, Allemagne, 23 octobre 2023*

8th International Conference on Mobile, Secure and Programmable Networking (MSPN 2023), *Paris, France, 26-27 octobre 2023*

30th Computer & Electronics Security Application Rendezvous (C&ESAR 2023), *Rennes, France, 21-22 novembre 2023*

ACM CCS Workshop on Recent Advances in Resilient and Trustworthy ML Systems in Autonomous Networks (ARTMAN 2023), *Copenhague, Danemark, 30 novembre 2023*

IEEE Global Communications Conference (GLOBECOM 2023), *Kuala Lumpur, Malaisie, 4-8 décembre 2023*

18th International Conference on Risks and Security of Internet and Systems (CRiSIS 2023), *Rabat, Maroc, 6-8 décembre 2023*

Retour sur les journées du GT MFS

Jannik Dreier

Depuis deux ans, les journées du GT MFS (Groupe de Travail sur les Méthodes Formelles pour la Sécurité) ont pris un format de *workshop* de trois jours destiné à rassembler les membres de la communauté scientifique (principalement française, même si nous avons pu comptabiliser cette année des participants et participantes venant du Canada, de l'Angleterre, de l'Allemagne, de Belgique, ...) des méthodes formelles pour la sécurité. Cette édition, organisée par Charlie Jacomme et Joseph Lallemand, s'est déroulée à la station biologique de Roscoff du CNRS, dans un décor extraordinaire, du 28 au 30 mars 2023, avec une bonne cinquantaine de participants et participantes.

Au programme de cette année, trois *keynotes* sur des sujets clés des méthodes formelles, par Tamara Rezk (sur l'application des méthodes formelles pour la sécurité du JavaScript), Stéphanie Delaune (sur la vérification de la non-traçabilité dans les protocoles cryptographiques), et David Monniaux (sur la compilation vérifiée formellement), un panel de présentations par les participants et participantes de leurs travaux récents, et une session de présentation des outils du domaine et de nombreuses occasions de rencontrer et de discuter avec les autres permanents et permanentes, ainsi que (post-)doctorants et (post-)doctorantes. Ces rencontres informelles, parfois prolongées tard le soir, ont été bien appréciées par les participants et participantes – l'occasion de faire des rencontres, de discuter, et de découvrir la diversité des personnes présentes. La variété des sujets présentés a également permis de faire un tour des différents versants des méthodes formelles, de la vérification formelle de protocoles à la vérification de programmes, en passant par l'implémentation des primitives cryptographiques, l'analyse statique, la logique, la compilation préservant la propriété de temps constant et la sécurité matérielle.

Le *social event* de cette édition était une promenade en bateau dans la Baie de Morlaix, suivie par une découverte de l'Île de Batz en autonomie. Même une météo ventée et pluvieuse n'a pas empêché la bonne humeur et la continuation des discussions. Certains et certaines se seraient même baignés un soir dans la mer, pourtant encore très fraîche.

Un grand merci aux organisateurs !

Jannik Dreier (Université de Lorraine, TELECOM Nancy, LORIA, Nancy), contact : jannik.dreier@loria.fr

Retour sur RESSI 2023

Arthur Tran Van et Adam-Oumar Abdel-Rahman

L'édition 2023 de RESSI s'est tenue dans le village de vacances de Neuvy-sur-Barangeon, en Sologne. Cédric Eichler et Benjamin Nguyen, responsables du comité d'organisation, ont réalisé un travail remarquable en mettant en place une organisation minutieuse. Au programme de cette édition, nous avons eu des sessions de rejeu de papiers, des keynotes, des sessions projets, des sessions enseignement et une session doctorants accompagnés de posters. Il convient de mentionner la présentation captivante de Charles Bouillaguet sur une plateforme d'apprentissage dédiée à la cryptographie, qui a véritablement conquis le public.

Lors de cette édition, nous avons remarqué une forte participation des doctorants. Les plus jeunes se sont particulièrement distingués en motivant les participants à venir découvrir leurs posters en seulement 3 minutes de présentation.

RESSI 2023 était une occasion de partager, découvrir et échanger avec ses pairs dans une atmosphère conviviale. Parmi les activités proposées, nous pouvons relever le choix d'un challenge surprenant, axé sur l'anonymisation. Cette thématique a permis aux participants d'explorer un domaine qui leur était souvent peu familier et qui s'éloignait des CTF classiques.

Notre souhait est que cette édition suscite un enthousiasme généralisé en vue de la prochaine édition qui se déroulera à Lille. Cet événement sera organisé par Michaël Hauspie et Thomas Vantroys de l'Université de Lille, qui ont élaboré le programme pour l'édition de 2023.

Vivement 2024 !

Arthur Tran Van et Adam-Oumar Abdel-Rahman, Télécom SudParis, Samovar, Institut Polytechnique de Paris, contact : atran-van@telecom-sudparis.eu, adam_oumar.abdel_rahman@telecom-sudparis.eu

Déchiffrement d'une lettre de Charles Quint (suite)

La gazette a interviewé dans son précédent numéro Cécile Pierrot, Pierrick Gaudry et Paul Zimmermann (Université de Lorraine, CNRS, Inria, LORIA) au sujet d'un travail pour le moins original, débuté par hasard : le déchiffrement d'une lettre écrite par Charles Quint. Si vous avez aimé ce travail, nous vous proposons ici quelques éléments complémentaires qu'ils nous ont communiqués.

Tout d'abord, ce travail a depuis fait l'objet d'une publication dans les actes de la conférence internationale Histocrypt 2023 : https://ecp.ep.liu.se/index.php/histocrypt/article/view/704/610. Pour les fans, l'intégralité des actes d'Histocrypt 2023 est disponible ici : https://ecp.ep.liu.se/index.php/histocrypt/issue/view/77/80.

Ce travail a aussi fait l'object d'une vidéo, diffusée sur une chaîne de télévision allemande et disponible ici : https://www.ardmediathek.de/video/wir-im-saarland-grenzenlos/ausgekluegelt-was-in-einem-alten-brief-von-kaiser-karl-v-steht/sr/Y3JpZDovL3NyLW9ubGluZS5kZS9HTC1XSU1TXzEyNTIxMC9zZWN0aW9uLzU

Retour sur le FIC 2023

Olivier Blazy

Le Forum International de la Cybersécurité est organisé tous les ans à Lille. Il s'est tenu cette année du 5 au 7 avril au Grand Palais. La dernière édition avait eu lieu en janvier 2022 (voir la gazette numéro 12).

S'y sont retrouvés tous types d'acteurs de la cybersécurité : entreprises (grands groupes, PME, startups) venues pour faire affaire ; services de l'état cherchant à se faire connaître et accompagner les entreprises et citoyens, mais aussi à recruter ; écoles d'ingénieur et universités proposant des formations en cybersécurité ; associations diverses de la sécurité et du logiciel libre ; délégations étrangères ; éditeurs de revues et magazines ; journalistes spécialisés en cyber ; hommes ou femmes politiques ; *streamers* ; étudiants prospectant pour des stages, thèses, alternances, formations ; sans oublier les acteurs académiques.

L'espace recherche, partagé par les membres de l'alliance Allistène (CNRS, INRIA, CEA, IMT, CDEFI, FU), et le stand du CREOGN continue à prendre de l'ampleur. Il était doté cette année d'un véritable espace de *Masterclass* avec plus de 60 places, les exposés d'Allistène ont couvert des thématiques diverses et fait intervenir des membres de toutes les institutions et de provenances géographiques variées.

Le GDR a été représenté sur le stand du CNRS par Olivier Blazy, Pascal Lafourcade, Jean-Yves Marion et le soutien du staff CNRS : Rapahaëlle Achach, Estelle Hutschka, Mandack Gueye, et Nicolas Porquet.

Les exposés de l'ensemble des *Masterclass* sont disponibles sur la chaine youtube du FIC : https://www.youtube.com/playlist?list=PLsaypbHfNQulAxqozdFK_ikpCnCk3o3dr.

Des présentations courtes des chercheurs en lien avec l'INS2I sont disponibles sur cette page : https://www.ins2i.cnrs.fr/fr/cnrsinfo/le-cnrs-au-forum-international-de-la-cybersecurite-2023.

Olivier Blazy, École Polytechnique, contact : olivier.blazy@polytechnique.edu

Prix de thèse 2023

Le prix de thèse 2023 du GDR Sécurité Informatique a été décerné à Tina Nikoukhah pour sa thèse « La vie secrète des images JPEG : détection de falsification via les traces de compression ». Pour mieux connaître son travail, vous pouvez relire son interview réalisé dans le numéro 14 de la gazette et/ou regarder la vidéo qu'elle nous a envoyée et qui est en ligne sur le site du GDR : https://gdr-securite.irisa.fr/prix-de-these/. Le jury a aussi souhaité décerner un accessit à Romain Cayre, pour sa thèse « Offensive and defensive approaches for wireless communication protocols security in IoT ». Bravo à eux ainsi qu'à toutes celles et ceux qui ont déposé leur candidature, les dossiers étaient d'excellente qualité.

Retour sur la journée du GT SDM

Pauline Puteaux

Le 16 mai 2023 s'est tenue, sur le beau campus Berges du Rhône de l'Université Lumière Lyon 2, une réunion du GT SDM (Groupe de Travail « Sécurité et Données Multimédia »), co-labellisée par le GDR ISIS, autour de l'analyse forensique de données multimédia.

Avec l'essor et la large disponibilité d'outils professionnels d'édition, ainsi que la recrudescence de méthodes s'appuyant sur l'apprentissage profond, falsifier des données multimédia est aujourd'hui relativement aisé et accessible.

L'analyse forensique vise à vérifier l'authenticité et l'intégrité des données multimédia, c'est-à-dire s'assurer qu'elles n'ont pas subi de modifications. Ce domaine de recherche, bien qu'important pour la société, est difficile sur le plan technique.

Les falsifications continuent de proliférer en partie à cause des limites des technologies de détection des falsifications, à cause des variabilités des supports (images, vidéos, sons) et à cause des traitements très spécifiques (par exemple, les différents niveaux de compression d'images ou les différentes méthodes de compression). Il est devenu trivial pour les contrefacteurs de réaliser des falsifications parfaites (comme les avancées récentes dans la génération des images et vidéos de type *deepfakes*).

Les exposés invités ont été réalisés par Kai Wang (GIPSA-lab, CNRS), sur l'analyse forensique des images par le biais d'approches statistiques ou à l'aide de l'apprentissage profond, et par Luisa Verdoliva (Multimedia Forensics Lab, University Federico II of Naples), sur la détection des *deepfakes*.

Les deux sessions de présentations qui ont eu lieu en début de matinée et dans l'après-midi ont permis d'échanger sur les avancées et les défis dans les domaines des *deepfakes* (sujet à la mode, abordé dans cinq des exposés courts !), de l'adaptation de domaine dans le cadre de l'analyse forensique et de la vérification d'intégrité des documents numériques et imprimés.

La journée a rassemblé une quarantaine de personnes, issues des mondes académique et industriel. Les échanges lors de cette réunion ont été très riches et intéressants. Une vidéo de la présentation invitée de Luisa Verdoliva et l'ensemble des supports de présentations sont disponibles sur le site du GDR ISIS pour ses membres : http://intranet.gdr-isis.fr/index.php?page=compte-rendu&idreunion=494. Nous les ajouterons également sur le site du GDR SI dès que possible.

Pauline Puteaux (CNRS, CRIStAL, Lille), contact : pauline.puteaux@cnrs.fr

Retour sur APVP

Jean-François Couchot

La 13e édition de l'Atelier annuel sur la Protection de la Vie Privée (APVP) s'est déroulée du 12 au 15 juin 2023 à la Saline royale d'Arc-et-Senans en Bourgogne-Franche-Comté.

Cette édition était organisée par le laboratoire FEMTO-ST et l'Université de Franche-Comté. L'atelier a réuni une quarantaine de chercheurs et chercheuses francophones dans le domaine de la protection de la vie privée et des données personnelles, thématique pluridisciplinaire à la croisée de l'informatique, du droit, de l'économie, de la sociologie et des statistiques.

Trois conférences plénières se sont déroulées. Statisticienne à l'INSEE, F. Dupont a présenté le projet de répertoire statistique d'individus et de logements RESIL qui est en cours de construction à horizon 2025. Il s'agit d'un outil interne à l'INSEE qui permettra d'apparier plus facilement des fichiers pour des finalités statistiques exclusivement. Le focus a été mis sur l'approche « *privacy by design* » de ce projet. Professeur au Max Planck Institute, P. Francis a présenté un exposé sur la mitigation des résultats d'attaques permettant d'inférer l'appartenance d'individus dans un modèle d'I.A. ou dans un jeu de données dites anonymisées. Les débats ont permis

d'exprimer une large diversité d'opinions autour de ce sujet au cœur de la communauté. Maître de conférences en Droit à l'Université de Franche-Comté, D. Martin a apporté une analyse approfondie des concepts de vie privée et de données personnelles. Elle a offert un éclairage juridique sur ces notions, en s'appuyant sur une série d'exemples tirés de la jurisprudence. Ces illustrations ont suscité un vif intérêt parmi les participants et ont donné lieu à de multiples interrogations d'ordres technique et juridique sur le sujet.

Une table ronde sur le « Traitement Automatique des Langues et Vie Privée » a été animée par B. Nguyen (LIFO) avec F. Dupont (INSEE), L. Béziaud (IRISA/UQAM), A. Boutet (Inria), G. Berthelier (Inria), J.-F. Couchot (FEMTO-ST). Les panelistes ont échangé sur cette problématique en se concentrant principalement sur les enjeux et les conséquences du partage des décisions de justice, des documents de santé ou des modèles ayant appris sur ceux-ci.

Une nouvelle compétition relative à la protection de la vie privée a été présentée cette année, conjointement à l'atelier. Conçue par l'IRISA et l'UQAM, la compétition est ouverte cette année sur l'international. Il s'agit de SNAKE1 (*SaNitization Algorithm under attacK ... ϵ*) qui se concentre spécifiquement sur les attaques d'inférence d'appartenance (*Membership Inférence Attacks* ou MIA) contre des données synthétiques générées par des algorithmes différentiellement privés de l'état de l'art. Étant donné le jeu de données synthétiques produit par l'algorithme attaqué, les participants et participantes doivent inférer la présence/absence d'un ensemble de lignes cibles dans le jeu de données d'entraînement. Un point d'étape préliminaire et de nombreuses discussions entre les participants et les participantes ont eu lieu pendant l'atelier, l'ensemble étant coordonné localement par Louis Béziaud (IRISA/UQAM). La première phase de la compétition est ouverte jusqu'au 31 août. Pour de plus amples informations sur la compétition et pour participer, le site de la compétition est https://www.codabench.org/competitions/879/, ou bien contactez louis.beziaud@irisa.fr.

Sept sessions de présentation d'articles de recherche ont permis d'échanger sur les sujets, notamment l'IA de confiance, l'équité dans l'apprentissage, l'IOT, l'anonymisation et l'assainissement des données, les analyses respectueuses de la vie privée, la cryptographie pour la protection de la vie privée, ainsi que le web et traçage publicitaire.

L'événement social a consisté en la visite de la ville de Besançon et sa citadelle Vauban, classée au patrimoine mondial de l'UNESCO.

Cet événement a été soutenu financièrement par les entités suivantes : GDR Sécurité informatique du CNRS, Orange Business, QWANT, FEMTO-ST, Université de Franche-Comté. Les organisateurs tiennent à les remercier chaleureusement.

De plus amples informations sont disponibles sur le site https://apvp23.sciencesconf.org/ de l'atelier.

Certains participants et participantes ont accepté de participer à la photo de groupe :

Jean-François Couchot, Femto-ST Institute, Univ. Bourg. Franche-Comté, CNRS, contact : jean-francois.couchot@univ-fcomte.fr

REDOCS 2023

La 8e édition des Rencontre Entreprises Doctorants en Sécurité Informatique aura lieu au CIRM à Luminy du 30 octobre 2023 au 4 novembre 2023. Les entreprises participant à cette édition sont : Astran, defants et la Gendarmerie. Les sujets seront mis en ligne sur le site du GDR dès que possible (https://gdr-securite.irisa.fr/redocs/).

Les inscriptions sont maintenant ouvertes : pour cela il vous suffit d'envoyer votre candidature par email à redocs-org@irisa.fr avec un CV académique, un email de votre directeur ou directrice de thèse vous autorisant à participer et confirmant l'établissement d'un ordre de mission ainsi que la prise en charge des frais de déplacements par votre laboratoire.

Nous sommes également à la recherche d'entreprises pour REDOCS 2024. Si vous êtes intéressé pour proposer un sujet, ne pas hésiter à nous contacter par email à redocs-org@irisa.fr.

En direct des labos

La Gazette interviewe Mohamed Kaâniche (DR CNRS), Directeur du Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS-CNRS) et chercheur en sécurité et sûreté de fonctionnement informatique du laboratoire, qui nous présente les recherches en sécurité menées au LAAS-CNRS, situé à Toulouse. L'unité compte environ 600 membres (dont 204 chercheurs et enseignants-chercheurs, 214 doctorants et post-doctorants et 89 ITA et BIATSS permanents). Les activités de recherche du LAAS-CNRS couvrent quatre disciplines : informatique, automatique, robotique et micro/nanosciences et se répartissent au sein de six départements scientifiques. Les recherches en sécurité informatique sont principalement menées au sein du département RISC (réseaux, informatique, systèmes de confiance) avec aussi des collaborations avec le département HOPES (systèmes hyperfréquences et optiques) pour des travaux autour de la sécurité matérielle.

Bonjour, quels sont les axes scientifiques du LAAS-CNRS et, plus précisément, vos objectifs en matière de sécurité informatique ?

Le LAAS-CNRS est un des premiers laboratoires en France à s'être intéressé à la sécurité informatique puisque nos premiers travaux sur ce sujet datent des années 70. Aujourd'hui, les travaux du laboratoire concernent la sécurité des systèmes informatiques et des réseaux (en intégrant à la fois les couches matérielles et logicielles et toutes les couches de communication, depuis la couche physique jusqu'aux couches protocolaires applicatives). Les domaines d'application visés sont très larges et concernent les systèmes informatiques « classiques », mais aussi les systèmes embarqués critiques (en particulier automobiles, avioniques, espace), les systèmes distribués composés d'objets connectés, les systèmes communicants de future génération (5G, 6G, ...), etc.

En particulier, les thèmes sur lesquels nous portons nos efforts actuellement sont :

- la sécurité des réseaux et des protocoles de communication (analyses de sécurité des protocoles sans fil utilisés dans l'IoT, supervision des réseaux basée sur des algorithmes d'apprentissage automatiques explicables, mécanismes matériels de *fingerprinting* d'objets connectés) ;
- la sécurité des systèmes embarqués critiques, notamment dans les domaines de l'automobile, de l'aéronautique, et de l'espace, en proposant des mécanismes de détection embarqués dans ces systèmes ;
- la sécurité du matériel (sécurité de la microarchitecture vis-a-vis d'attaques par canaux auxiliaires notamment, en incluant l'analyse de vulnérabilités mais aussi la conception de mécanismes et architectures de protection assistées par le matériel) et de couches physiques des objets communicants (en faisant converger les nouvelles technologies RF, tel que les RIS (*reconfigurable intelligent surface*) et la cryptographie pour aboutir à des moyens d'authentification sûrs ;
- l'utilisation d'approches formelles permettant d'aider à la construction de langages plus sûrs, notamment vis-à-vis de vulnérabilités d'injection, y compris pour les langages quantiques ;
- la prise en compte de la protection de la vie privée des utilisateurs et de données sensibles dans différents contextes (diffusion de contenus multimédia, remontée d'informations dans le contexte de véhicules connectés, . . .). L'exploration d'algorithmes post-quantiques fait partie de nos sujets d'étude dans ce contexte.

Mohamed Kaâniche

Quelles sont vos collaborations dans ces domaines avec le tissu local, national et international ?

Nous avons de nombreuses collaborations avec des entreprises du tissu local (Airbus, Thalès, Continental, Custocy, ...) ou national (Renault, EDF, ARM), essentiellement dans le cadre de thèses CIFRE ou de projets ANR. Le LAAS est aussi très impliqué dans l'Institut Cybersécurité d'Occitanie, qui se veut un lieu d'échange privilégié entre chercheurs, industriels et collectivités territoriales de la région Occitanie, et qui favorise la recherche amont pluridisciplinaire incluant les sciences humaines et sociales, en finançant des thèses et post-docs, et en soutenant des événements locaux. En particulier des liens étroits se sont créés avec les chercheurs du LIRMM à Montpellier dans ce contexte.

Sur le plan national, le laboratoire est impliqué dans deux projets du PEPR cybersécurité : le projet Superviz, consacré à la supervision des réseaux, et le projet REV consacré à l'analyse de vulnérabilités. Dans le contexte de ces projets notamment, plusieurs liens forts point à point existent avec l'Institut Eurecom, IMT Atlantique, Télécom Sud Paris, Inria, Centrale Supélec, l'Université

Grenoble Alpes, et l'Université de Lorraine. Le LAAS-CNRS est également fortement impliqué dans l'animation scientifique du tissu local via par exemple l'organisation d'événements scientifiques tels que la THCon (https://thcon.party), conférence de recherche attirant environ 300 participants chaque année.

Quels sont les programmes de formation qui sont adossés à vos recherches ?

Les enseignants chercheurs et chercheurs du LAAS-CNRS sont fortement impliqués dans la responsabilité de formations en cybersécurité : la formation ingénieur « TLS-SEC », co-portée par l'INSA, l'ENSEEIHT et l'ENAC (SecNumEdu), le mastère spécialisé « Sécurité Informatique », co-porté par les trois mêmes écoles, mais aussi dans la responsabilité d'unités de formation consacrées à certaines compétences avancées en cybersécurité (sécurité matérielle, sécurité des objets connectés), dispensées à l'INSA de Toulouse notamment.

Pouvez-vous nous présenter rapidement des avancées que vous avez faites dans un domaine donné ?

Des travaux notables ont été effectués récemment sur la sécurité des objets connectés, en particulier dans le cadre de la thèse de Romain Cayre (https://hal.laas.fr/tel-03841305). Ces travaux ont permis de révéler plusieurs vulnérabilités et scénarios d'attaques innovants dans le contexte de protocoles de communications de l'IoT (en particulier, *BlueTooth Low Energy* et *Zigbee*), mais également de proposer des mécanismes de détection d'intrusion embarqués. Ces travaux ont donné lieu à la publication d'une CVE et deux publications à la conférence IEEE DSN 2021 notamment, ainsi qu'à un accessit au prix de thèse du GDR Sécurité Informatique. Un autre résultat marquant concerne la proposition par Éric Alata et Cyrius Nugier d'un algorithme de navigation anonyme sur internet résilient aux attaques post-quantiques, QasTor (https://www.occitanie-ouest.cnrs.fr/fr/cnrsinfo/la-navigation-anonyme-sur-internet-sera-t-elle-toujours-possible-lere-post-quantique), une alternative à Tor plus adaptée au *live streaming* de masse, qui fait l'objet d'une maturation par la SATT Toulouse *Tech Transfer*.

Merci Mohamed pour toutes ces informations sur l'organisation du LAAS-CNRS et vos domaines de recherche !

Article rédigé par Mohamed Kaâniche, Directeur du LAAS-CNRS, contact : mohamed.kaaniche@laas.fr

Jobs

Il y a de nombreux postes en sécurité informatique qui sont actuellement ouverts dans la communauté académique française. À toutes fins utiles figure ci-dessous une liste d'annonces parues sur le forum du GDR. Le terme « sécurité » n'apparaît pas systématiquement dans les titres, mais il est contenu dans les fiches de postes de toutes les annonces listées. Si vous souhaitez vous abonner pour les recevoir en temps réel, rendez-vous sur https://gdr-securite.irisa.fr/listes/

Poste d'enseignant-chercheur, EURECOM (Sophia Antipolis)

Sujet : Sécurité numérique : recherche, analyse, exploitation et/ou de la remédiation des vulnérabilités
Aurélien Francillon,
aurelien.francillon@eurecom.fr

Deux postes d'ATER, CentraleSupélec, IRISA (Rennes)

Sujet : Cybersécurité (section 27)
Jean-Francois Lalande,
jean-francois.lalande@irisa.fr

Poste de post-doctorat, ETIS lab (Cergy-Pontoise)

Sujet : Design of short packet wiretap codes for 6G
Durée : 1 an (renouvelable)
Laura Luzzi, laura.luzzi@ensea.fr

Poste de post-doctorat, CEA Paris-Saclay (Saclay)

Sujet : Formal Verification for micro-architectural attacks through efficient speculative symbolic execution
Durée : 3 ans
Sébastien Bardin, sebastien.bardin@cea.fr

Poste de post-doctorat, CEA Paris-Saclay (Saclay)

Sujet : SSA and type-based abstract interpretation for binary code verification
Durée : 3 ans
Matthieu Lemerre, matthieu.lemerre@cea.fr

Poste de post-doctorat, CEA Paris-Saclay (Saclay)

Sujet : Mapping the landscape of complex software vulnerabilities and finding ways to detect them
Durée : 3 ans
Michaël Marcozzi, michael.marcozzi@gmail.com

Deux postes de post-doctorat, CEA Paris-Saclay (Saclay)

Sujets : Automatically infer program annotations to help reverse engineering, code understanding and verification

Automatically simplify highly obfuscated code through black- and white-box reasonning
Durées : 3 ans
Grégoire Menguy, gr.menguy@gmail.com
Sébastien Bardin, sebastien.bardin@cea.fr

Thèse de doctorat, INSA Centre Val de Loire, LIFO (Bourges)

Sujet : Logique et sécurité Zero Trust
Sabine Frittella, sabine.frittella@insa-cvl.fr
Laurent Bobelin, laurent.bobelin@insa-cvl.fr

Thèse de doctorat, INSA Centre Val de Loire, LIFO (Bourges)

Sujet : Signatures assainissables sur des données anonymisables et applications à la protection des données médicales
Xavier Bultel, xavier.bultel@insa-cvl.fr
Benjamin Nguyen,
benjamin.nguyen@insa-cvl.fr

Thèse de doctorat, ETIS (Cergy), A*STAR (Singapour)

Sujet : Trust and trustworthiness for 6G
Arsenia (Ersi) Chorti, arsenia.chorti@ensea.fr

Thèse de doctorat, LTCI, Télécom Paris, Institut Polytechnique de Paris (Palaiseau)

Sujet : Approche ingénierie dirigée par les modèles pour évaluer la sécurité des systèmes Cyber-physiques
Jean Leneutre,
jean.leneutre@telecom-paris.fr

Thèse de doctorat, CEA LIST, CentraleSupélec - Université Paris-Saclay (Saclay)

Sujet : Inférence de spécifications d'interaction avec stratégie adversariale
Boutheïna Bannour, boutheina.bannour@cea.fr
Pascale Le Gall,
pascale.legall@centralesupelec.fr

Thèse de doctorat, Telecom Paris, Institut Polytechnique de Paris (Palaiseau)

Sujet : A Model-Based Systems Engineering Approach for Assessing the Security of Cyber-physical Systems
Gregory Blanc,
gregory.blanc@telecom-sudparis.eu
Dominique Blouin,
dominique.blouin@telecom-paris.fr
Jean Leneutre,
jean.leneutre@telecom-paris.fr
Olivier Levillain,
olivier.levillain@telecom-sudparis.eu

Trois thèses de doctorat, Lab-STICC (Brest)

Sujets : Etude d'architectures de processeurs sécurisés contre des attaques physiques
Accélérateurs FPGA en arithmétique RNS pour des isogénies entre courbes elliptiques
Accélérateurs cryptographiques agiles et sécurisés
Arnaud Tisserand, arnaud.tisserand@cnrs.fr

Deux thèses de doctorat, CEA Paris-Saclay (Saclay)

Sujets : Taking the Attacker into Account in Security-oriented Symbolic Execution
Formal Verification for micro-architectural attacks through efficient speculative symbolic execution
Sébastien Bardin, sebastien.bardin@cea.fr

Thèse de doctorat, CEA Paris-Saclay (Saclay)

Sujet : Making fuzzers better at finding software vulnerabilities
Michaël Marcozzi, michael.marcozzi@gmail.com

Deux thèses de doctorat, CEA Paris-Saclay (Saclay)

Sujets : Automatically infer program annotations to help reverse engineering, code understanding and verification
Automatically simplify highly obfuscated code through black- and white-box reasonning
Grégoire Menguy, gr.menguy@gmail.com
Sébastien Bardin, sebastien.bardin@cea.fr

Thèse de doctorat, CEA-LIST Grenoble (Grenoble)

Sujet : Proving that secured programs work as intended
Damien Couroussé, damien.courousse@cea.fr
Frédéric Recoules, frederic.recoules@cea.fr
Sébastien Bardin, sebastien.bardin@cea.fr

Thèse de doctorat, IRT Saint-Exupery de Toulouse, LAAS, CNES (Toulouse)

Sujet : Analyse du risque et mécanismes de sécurité embarqués dans les systèmes spatiaux
Vincent Nicomette, vincent.nicomette@laas.fr

2 thèses de doctorat, Inria, Université de Rennes (Rennes)

Sujets : Modeling, classification, and detection of vulnerabilities and their variants in software code bases using AI
Applying countermeasures to vulnerabilities in code, through AI-driven refactoring and co-evolution
Olivier Barais, Olivier.Barais@irisa.fr
Olivier Zendra, Olivier.Zendra@inria.fr
Paul Temple, Paul.Temple@irisa.fr

Thèse de doctorat, LORIA, Université de Lorraine (Nancy)

Sujet : Taxonomy of Frauds on Crypto-Assets
Abdessamad Imine, abdessamad.imine@loria.fr
Yamina Tadjeddine,
yamina.fourneyron@univ-lorraine.fr

Thèse de doctorat, CryptoExperts (Paris)

Sujet : Generation of Masking Countermeasures Against Side-Channel Attacks
Sonia Belaïd, sonia.belaid@cryptoexperts.com

Thèse de doctorat, SPIE ICS, INSA Lyon (Lyon)

Sujet : Détection d'anomalies par apprentissage par renforcement et contradictoire pour une architecture cyber-sécurité Zero-Trust : application dans le domaine de la santé
Frédéric Le Mouël,
frederic.le-mouel@insa-lyon.fr
Bogdan Stefanescu,
bogdan.stefanescu@spie.com

Thèse de doctorat, IHEDN, Télécom Paris (Institut Polytechnique de Paris), Naval Group

Sujet : Plate-forme de leurrage à haute interactivité pour le renforcement de la cybersécurité des systèmes industriels
Jean Leneutre,
Jean.Leneutre@telecom-paristech.fr
Julien Francq, julien.francq@naval-group.com