Octobre 2021
Numéro 10

LA GAZETTE DU GDR

Sécurité Informatique - GDR2046

Édito de la directrice

C'est la reprise ! Enfin nous commençons à reprendre une vie plus normale, et si les journées nationales 2021 ont eu lieu en distanciel, de plus en plus d'événements reprennent en présentiel pour la plus grande joie de nous retrouver.

C'est aussi mon premier édito, puisque j'ai pris la direction du GDR le 1er juillet dernier. Je souhaite avant tout remercier de tout cœur Gildas Avoine, qui a monté le GDR en 2016 et en a assuré la direction jusqu'à l'été dernier, ainsi que Marc-Olivier Killijian qui l'a épaulé comme directeur-adjoint de 2016 à 2020, pour l'énergie et le dynamisme qu'ils ont insufflés au GDR ! Et je n'oublie pas Aurélie Patier, gestionnaire à l'IRISA, pour son aide constante sur les aspects administratifs durant ces années, ni Marie-France Grandisson qui prend le relais à mes côtés au LMF. L'équipe de la gazette a elle aussi passé le relais. Un grand merci à Patrick Bas qui a été son rédacteur en chef depuis sa création, ainsi qu'à Annelie Hauser qui l'a secondé. Et merci à Céline Chevalier d'avoir accepté de devenir la nouvelle rédactrice en chef, et à Pauline Puteaux qui la rejoint à partir de ce numéro.

Vous trouverez dans ce nouveau numéro une interview de Teddy Furon sur la sécurité de l'apprentissage automatique, ainsi que la présentation du laboratoire EURECOM. Comme dans les précédents numéros, nous vous proposons également des témoignages et retours sur des événements récents : APVP organisé en juin en distanciel, l'école d'été du GDR organisée en juillet à Toulouse, et le Forum International de la Cybersécurité qui a eu lieu à Lille en septembre. Pas d'article faute de place sur les Journées Nationales, malgré un très beau programme, mais vous verrez dans les brèves que vous pouvez récupérer les présentations qui vous intéressent. Et bien sûr comme toujours des annonces d'événements, d'offres de postes/stages tirés du forum.

Bonne lecture à toutes et à tous !

Caroline Fontaine,
Directrice du GDR Sécurité Informatique

Rubriques

Événements

(Repris en partie du forum du GDR)

Journée thématique (GT SSLR en partenariat avec le GDR GPL) génie logiciel et sécurité *CNAM, Paris, 9 novembre 2021*

Journée thématique (GT SSM) : Algorithmes de chiffrement post-quantiques et sécurité matérielle *LIP6, Paris, 10 novembre 2021*

20th Smart Card Research and Advanced Application Conference (CARDIS 2021) et Fall School on Nano-Electronics for Secure Systems (NESSY) *Lübeck, Allemagne, et en ligne, 10-12 novembre 2021*

13th IEEE International Workshop on Information Forensics and Security (WIFS 2021) *Montpellier, 7-10 décembre 2021*

14th International Symposium on Foundations & Practice of Security (FPS 2021) *Paris, 8-10 décembre 2021*

17th International Conference on Ubiquitous Security (UbiSec 2021) *Guangzhou, Chine, et en ligne, 28-31 décembre 2021*

Le coin prospectif

Teddy Furon

La gazette interviewe Teddy Furon, chercheur à l'Inria dans l'équipe projet LinkMedia au Centre Inria Rennes Bretagne Atlantique. Spécialiste en sécurité des contenus multimédia, Teddy est lauréat de la chaire IA/sécurité SAIDA. La gazette a décidé de le questionner sur son domaine de recherche, notamment sur ses activités en lien avec la sécurité de l'apprentissage automatique.

Bonjour Teddy, peux-tu présenter rapidement tes activités ?

Bonjour Céline et Pauline. Je suis chercheur dans l'équipe projet LinkMedia au Centre Inria Rennes Bretagne Atlantique. Je fais partie de la communauté « sécurité des contenus » (en anglais « *Information Forensics & Security* »), une niche dans le grand paysage de la cybersécurité. Mon travail consiste à évaluer des niveaux de sécurité de primitives de traitement du signal et des images. Les applications portent des noms exotiques comme le tatouage, le traçage de traîtres, la recherche des plus proches voisins... un peu de *differential privacy* et de stéganographie aussi.

Teddy Furon.

Tu viens d'obtenir la chaire IA/sécurité SAIDA, félicitations ! Pourrais-tu nous parler plus en détails de ce projet, quels sont les défis que tu souhaites relever ?

Merci ! Tout d'abord la chaire porte une certaine vision de la sécurité de l'apprentissage automatique. L'apprentissage manipule trois types de « contenus » qu'il faut sécuriser : les données d'entraînement, le modèle appris et les données de test. Il faut protéger en particulier trois valeurs classiques en sécurité des contenus : confidentialité, intégrité et propriété. À partir de ce canevas, des scénarios émergent naturellement : la confidentialité des données de test revient à pouvoir inférer (appliquer un modèle appris) sur des données chiffrées.

La confidentialité des données d'entraînement revient à mesurer la quantité d'information relative à ces données qui fuit du modèle. Leur intégrité pose la question de leur manipulation pour biaiser l'apprentissage (*poisoning* ou *backdoor* en anglais). Enfin, constituer un jeu de données d'entraînement de qualité et apprendre un modèle est coûteux. Est-il possible de prouver que tel modèle m'appartient ? Est-il possible de montrer que tel modèle a été appris sur mes données ? Ces questions se posent pour tout type de données, mais aussi tout cadre d'apprentissage (supervisé, non supervisé, profond, renforcé, fédéré, frugal, méta, auto... bref tout *X-learning*). Voici en quelques lignes les enjeux de la sécurité du *machine learning*.

> « Les exemples adverses ne sont pas une menace mais un avertissement. »

En quoi les exemples adverses (*adversarial examples*) sont-ils une menace pour la cybersécurité ?

Les exemples adverses ne sont pas une menace mais un avertissement. Comme dans beaucoup d'autres domaines, le *machine learning* envahit actuellement la cybersécurité. Ses capacités de généralisation (s'acquitter d'une tâche sur des données non observées à l'entraînement) et de robustesse (sur des données bruitées) sont extraordinaires. Mais ces qualités nous donnent un faux sentiment de sécurité. Les exemples adverses nous avertissent que robustesse et sécurité sont deux concepts différents (chose connue depuis longtemps en sécurité des contenus). En classification d'images, il faut ajouter une quantité de bruit énorme pour que le modèle se trompe tant il est robuste.

> « Avant d'utiliser l'apprentissage automatique en sécurité, il serait bon d'étudier la sécurité intrinsèque de l'apprentissage automatique. »

Et pourtant, il est très vulnérable : un attaquant disposant de certaines informations leurre le modèle avec une perturbation adverse imperceptible à l'œil nu. Cela montre qu'avant d'utiliser l'apprentissage automatique en sécurité, il serait bon d'étudier la sécurité intrinsèque de l'apprentissage automatique.

Quels conseils peux-tu donner aux jeunes chercheurs intéressés par la sécurité des données multimédia ?

1. Arrêter d'utiliser les mots « traitement du signal » ou « sécurité des contenus » comme le fait le vieux dinosaure que je suis, « *machine learning* » voire « *artificial intelligence* » c'est plus vendeur !
2. Avoir une lecture adverse de la littérature des exemples adverses. Le sujet est difficile car très à la mode : il y a plus de 3000 papiers parus ces 4 dernières années rien qu'en exemples

adverses. L'ultra compétition n'aide pas la recherche. La littérature est souvent peu reproductible avec des revendications parfois survendues sans aucune auto-évaluation.

3. Bien connaître les us et coutumes (souvent implicites) des conférences / journaux où l'on veut publier. Comme l'a dit une fois un éditeur associé au jeune chercheur dépité d'un rejet que j'étais : « si tu veux jouer à ce jeu, tu dois en suivre les règles ».

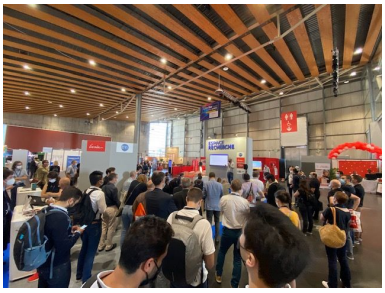
Merci Teddy pour ces réponses très intéressantes et pour tes conseils. Nous sommes impatients de découvrir tes avancées dans le cadre de la chaire SAIDA !

Article rédigé par Teddy Furon (Centre Inria Rennes – Bretagne Atlantique), Céline Chevalier et Pauline Puteaux, Contact : teddy.furon@inria.fr

Retour sur le FIC 2021

Caroline Fontaine

Le Forum International de la Cybersécurité, organisé habituellement tous les ans à Lille au mois de janvier n'avait pu se tenir depuis l'édition de janvier 2020. Il s'est finalement tenu en cette rentrée, les 7-8-9 septembre. 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'ingénieurs et universités proposant des formations en cyber ; associations diverses de la sécurité et du logiciel libre ; éditeurs de revues et magazines ; étudiants prospectant pour des stages ou des formations ; sans oublier les acteurs académiques.



L'« espace recherche », partagé par les membres de l'alliance Allistène (CNRS, INRIA, CEA, Université et Écoles), avait été entièrement repensé cette année, et était bien plus visible et attractif que les années précédentes. En particulier, finis les petits pupitres individuels avec démos, qui attiraient finalement assez peu de monde. L'espace disposait cette année d'une vraie scène sonorisée sur laquelle ont été présentés des travaux de recherche variés, qui ont attiré un public nombreux et intéressé (plus de 70 personnes en continu lors des exposés). Les conférences étaient regroupées en sessions thématiques, qui figuraient au programme officiel du FIC, si bien que les participants les avaient repérées d'avance et n'étaient pas là par hasard. Au programme : « protection des données personnelles », « sécurité matérielle », « sécurité réseau et systèmes distribués » ou encore « sécurité des données ». S'en sont suivies beaucoup de discussions riches et intéressantes pour tous : académiques, industriels ou étatiques.

Le GDR a été représenté sur le stand du CNRS de l'« espace recherche » durant les 3 jours, par sa directrice ainsi que Jean-Yves Marion (président du conseil scientifique du GDR) et le soutien de l'INS2I : Olivier Cappé (directeur-adjoint scientifique de l'INS2I en charge de la cybersécurité), Estelle Hutschka (chargée de communication) et Mandack Gueye (responsable de la valorisation). L'ambiance de l'« espace recherche » était collégiale et la mutualisation de l'espace et de la scène vraiment agréable, finalement dans l'esprit du GDR puisque nous étions tous présents ensemble en tant que communauté. Une belle édition donc ! J'en profite pour remercier toutes celles et tous ceux qui ont participé à l'animation de l'espace, en particulier sur scène, car les exposés étaient passionnants. Rendez-vous lors du prochain FIC (peut-être en juin 2022)...

Merci Caroline pour ton retour. Cette nouvelle version du FIC semble avoir tenu ses promesses et rencontré beaucoup de succès !

Article rédigé par Caroline Fontaine, Contact : caroline.fontaine@lsv.fr

Compte rendu de APVP 21

Benjamin Nguyen et Mathieu Cunche

Après l'annulation de l'édition de 2020, le 11e Atelier sur la Protection de la Vie Privée s'est déroulé exceptionnellement en ligne (plateforme BBB) du 15 au 17 juin dernier, organisé par Mathieu Cunche et Benjamin Nguyen, les deux co-responsables du GT *Protection de la Vie Privée*. Cet événement annuel cherche à regrouper la communauté francophone pluridisciplinaire s'intéressant aux problèmes de vie privée. Compte tenu de son déroulement en distanciel total, un format plus court a été adopté, avec une conférence plénière, des ateliers collaboratifs, des présentations de résultats de doctorants afin de leur permettre de faire connaître leurs recherches auprès de la communauté, une présentation par la Commission Nationale Informatique et Libertés (CNIL) de ses activités en 2020/2021, une table ronde pluridisciplinaire, et une compétition d'anonymisation et réidentification. Un nombre record de 61 participants a été atteint pour cette édition, démontrant un intérêt toujours croissant pour les thèmes portés par le groupe de travail PVP.

Conférence plénière. Yves Poullet, Professeur émérite à l'Université de Namur (Belgique), fondateur du *Centre de Recherches Informatique et Droit* (CRID), a été l'un des pionniers de la collaboration entre ces deux disciplines. Au cours d'une conférence passionnante, Yves Poullet a présenté son expérience des 40 dernières années à travailler sur la question de la protection de la vie privée, en insistant bien entendu sur le RGPD, ainsi que sa vision pour le futur de ce domaine de recherche. L'intégralité de sa conférence est à retrouver à l'adresse https://www.youtube.com/watch?v=zNyZpHwy7Xg.

Ateliers collaboratifs. Afin de proposer des activités interactives, nous avons organisé deux sessions d'ateliers sous la forme de questions suggérées par les participants. Chaque participant a pu ainsi débattre au cours de deux ateliers, parmi les suivants :

- A1- Le RGPD moralise-t-il l'économie des données personnelles ?
- A2- La recherche sur le traçage de contacts est-elle encore d'actualité ?
- A3- Recherche en vie privée, quel impact pour les citoyens ?
- B1- Quel impact ont les protocoles de l'IETF (internet) sur la protection de la vie privée ?
- B2- Quels modèles formels pour modéliser les propriétés de *privacy* ?
- B3- Quels enjeux PVP pour le traitement des données médicales et textuelles ?

Présentations de résultats de recherche par des doctorants. Avec l'organisation de nombreux événements en ligne à cause de la Covid, beaucoup de doctorants ont des difficultés à présenter leurs résultats de recherche, se faire connaître, et constituer leur réseau de collaborations. Nous avons donc conservé deux sessions de présentations d'articles de recherche où un doctorant était premier auteur. 10 présentations ont pu être réalisées lors de l'atelier, en laissant une part raisonnable de temps de discussion. Deux thèmes (géolocalisation et impact de la PVP dans l'IA) étaient plus particulièrement représentés cette année.

Session CNIL. Cette année, la CNIL a souhaité s'associer plus fortement à APVP *via* l'organisation d'une table ronde pluridisciplinaire sur le thème de la lutte au quotidien contre la surcollecte et le traitement de données, animée par Félicen Vallet (CNIL), avec comme panélistes Esther Onfroy (Fondatrice d'Exodus Privacy et du Defensive Lab Agency), Ksenia Ermoshina (sociologue au CNRS, au Centre Internet & Société) et Antoine Courmont (sociologue LINC/CNIL). Félicien Vallet et Antoine Courmont ont également présenté une sélection des activités de la CNIL pour l'année 2020/2021, en revenant sur un certain nombre de plaintes, ainsi que sur la question du *contact tracing*. Après de très bons retours de la part des participants à l'atelier, le partenariat avec la CNIL devrait se poursuivre dans les années à venir.

Compétition d'anonymisation et réidentification (DARC). Pour la première fois, APVP a choisi d'organiser une compétition liée à une problématique de protection des données : l'anonymisation et la réidentification des données. La compétition était organisée en deux phases : une première phase où les équipes participantes devaient anonymiser un jeu de données de géolocalisation, tout en maximisant l'utilité du jeu de données anonymes, et une deuxième phase où il fallait *attaquer* (réidentifier) les jeux de données des autres équipes. La première phase s'est déroulée du 1er au 15 juin, et la 2e phase s'est déroulée au cours de l'atelier, se terminant le 17 juin en fin d'après-midi pour la clôture. 5 équipes ont participé. Au final, c'est l'équipe de l'Université du Québec à Montréal (UQAM) qui s'est imposée sur les deux défis, devant les équipes de FemtoST/Orange et de l'INSA de Lyon. La compétition a donné lieu au mois de juillet à un atelier spécifique du GT PVP de retour d'expérience et présentation des techniques utilisées. Nous remercions et félicitons l'ensemble des participants. Suite à ce succès, nous prévoyons d'organiser un challenge similaire l'année prochaine.

Retour d'expérience. Selon les retours que nous avons eus, la formule particulière d'APVP21 a été appréciée par l'ensemble des participants. En effet, l'in-

teractivité dans les débats et les présentations, parfois difficile pour un événement en ligne, a pu être préservée.

Merci Benjamin et Mathieu pour votre retour sur ce 11e Atelier. Apparemment, vous avez réussi à le rendre très vivant malgré la distance ! Les participants auront hâte de vous retrouver l'année prochaine.

Article rédigé par Benjamin Nguyen (INSA Centre Val de Loire, LIFO) et Mathieu Cunche (INSA Lyon - CITI, Inria - Privatics), Contact : benjamin.nguyen@insa-cvl.fr, mathieu.cunche@insa-lyon.fr

Brèves

- Deux ouvrages sur la sécurité multimédia, intitulés *Authentication et insertion de données cachées* et *Biométrie, protection et chiffrement multimédia*, viennent de paraître (coordinateur : William Puech, ISTE Editions).
- *Slides des Journées Nationales 2021* : disponibles sur le site https://gdr-secu-jn2021.sciencesconf.org/resource/page/id/2
- *Save the date* : Les « Journées C2 » auront lieu du 10 au 15 avril 2022 à Hendaye.

Retour sur l'école d'été CYBER In Toulouse

Vincent Nicomette

Cette année, l'école d'été du GDR Sécurité Informatique a pu se tenir dans les locaux de l'INSA de Toulouse, en présentiel, du 19 au 23 juillet (« CYBER in Toulouse »). Deux thématiques principales étaient au menu de cette école : la sécurité des objets connectés (les deux premiers jours) et la sécurité des systèmes embarqués critiques (les trois derniers jours).

La sécurité des objets connectés a donné lieu à une présentation introductive de Marc Dacier, qui a poursuivi par une analyse de la sécurité des protocoles « *Zero Conf* ». Matthieu Cunche a, quant à lui, conclu la première journée en nous présentant ses travaux sur les problèmes de protection de la vie privée dans les protocoles de communication sans fil (en particulier le Bluetooth). Le second jour a été consacré à une matinée de présentations/démonstrations, par Romain Cayre (APSYS/LAAS-CNRS) et Florent Galtier (LAAS-CNRS), visant à illustrer concrètement des problèmes de sécurité dans les protocoles de communications de nombreux objets connectés (soit des protocoles propriétaires, soit des protocoles standards comme le BLE). Diverses attaques et *reverse engineering* étaient au programme. Les démonstrations ont été faites en direct avec de nombreux objets connectés du commerce ainsi que du matériel de SDR (*Software Defined Radio*). Enfin l'après-midi du second jour était consacré à une présentation suivie d'un TP visant à illustrer les attaques de type canaux de fuite sur des systèmes embarqués. Florent Bruguier (LIRMM), ainsi que Vincent Migliore (INSA Toulouse/LAAS-CNRS) étaient aux commandes. Il a fallu jongler avec du matériel et de la crypto.

La seconde partie de l'école d'été était donc consacrée aux problématiques de sécurité des systèmes embarqués critiques, et avait un format un peu original puisqu'elle incluait un challenge de sécurité occupant les participants pendant la dernière journée et demie. Avant ce challenge, des présentations concernant les problématiques de sécurité dans différents systèmes embarqués critiques ont été proposées (automobile, avionique et espace). Chaque intervenant (Guillaume Lussier pour Renault, Bertrand Leconte pour Airbus et Benoit Tranier pour Thales) nous a fait part des problématiques de sécurité spécifiques à son domaine et des principaux verrous actuels. Ensuite, l'école s'est donc terminée par un petit challenge de sécurité, spécifiquement conçu pour systèmes embarqués, sous la houlette de trois intervenants spécialistes du domaine : Stéphane Duverger (Airbus), Benoit Camredon (Airbus) et Benoit Morgan (ENSEEIHT/IRIT).

À noter également que cette année, l'école comportait une rump session le mercredi soir, qui a permis à tout participant volontaire de faire une présentation de son choix sur un sujet, bien sûr en rapport avec la cybersécurité. Seule contrainte : faire la présentation en 5 minutes maximum. Cette session était intéressante, les volontaires ont présenté soit leur sujet de thèse, soit un sujet qui leur tenait à cœur, le tout dans une bonne ambiance.

Les gagnants et les trois enseignants qui ont organisé le challenge.

Quelques témoignages des participants :

« J'ai énormément apprécié l'excellent challenge Airbus en conclusion de la semaine, ça permet de s'essayer à un vrai cas pratique dans une bonne ambiance de CTF. »

« C'était bien de pouvoir voir et échanger avec d'autres doctorants en présentiel, devant la table de déjeuner ou pause-café. »

« Les TP, typiquement le challenge guidé par les enseignants, étaient très intéressants et m'ont permis d'apprendre plein de choses. »

« J'ai beaucoup apprécié la pédagogie de Stéphane Duverger. J'en ai presque oublié le challenge de sécurité pendant son One-Man-Show. *»*

« J'ai spécialement aimé les démos faits par Romain Cayre et Florent Galtier, ça montre de manière très visuelle des vulnérabilités de communication sans fil des objets connectés. »

« On a découvert plein de vulnérabilités sur les protocoles sans fil ! Le challenge de sécurité était trop bien, aussi. Merci les organisateurs ! »

Merci Vincent pour ton retour sur cette école d'été, et merci aux participants pour vos témoignages enthousiastes !

Article rédigé par Vincent Nicomette (INSA Toulouse, CNRS - LAAS), Contact : vincent.nicomette@laas.fr

Une nouvelle directrice

Caroline Fontaine

La Gazette interviewe Caroline Fontaine, chercheuse CNRS au LMF (Paris-Saclay) et nouvelle directrice du GDR.

Bonjour Caroline, peux-tu nous rappeler ton parcours et tes activités de recherche actuelles ?

Bonjour, j'ai eu un parcours un peu atypique, puisque j'ai été maîtresse de conférences avant d'être recrutée au CNRS, que j'ai changé plusieurs fois de laboratoires comme de régions, et que cela m'a permis peu à peu d'enrichir mes thématiques de recherche.

J'ai commencé par faire une thèse à l'INRIA à Rocquencourt en cryptographie et codes correcteurs algébriques, thèse au cours de laquelle j'ai également été confrontée aux techniques de tatouage d'images, qui relèvent du traitement d'images, domaine qui était complètement nouveau pour moi. Après un court passage au LRI à Orsay en tant qu'ATER dans l'équipe d'algorithmique, j'ai été recrutée comme maîtresse de conférences à Lille au LIFL (ancêtre du laboratoire CRIStAL), dans une équipe travaillant sur les systèmes d'exploitation pour cartes à puces et les techniques de routage dans les réseaux ad-hoc. C'est durant cette période que j'ai été recrutée au CNRS. En 2005, j'ai rejoint l'IRISA à Rennes dans une équipe de traitement d'images et de codage de source, puis en 2009 j'ai migré encore plus à l'ouest au Lab-STICC, à Brest, dans une équipe de sécurité à forte coloration maritime. Il y a trois ans je suis revenue en région parisienne au sein du LSV, laboratoire historique en méthodes formelles pour la sécurité, qui depuis a fusionné avec l'équipe VALS du LRI pour donner naissance au LMF.

Je suis devenue spécialiste de certains de ces domaines – pas tous – mais les avoir côtoyés au quotidien pendant toutes ces années m'a permis de bien les comprendre tout en traçant mon propre chemin entre cryptographie, protocoles, protection des contenus multimédia, respect de la vie privée et maintenant méthodes formelles. Au passage, j'ai également essayé de tisser des liens entre différents champs disciplinaires, au gré des rencontres, et de favoriser la collaboration. Chaque laboratoire m'a aussi permis de découvrir des environnements de travail différents et très enrichissants.

Qu'est-ce qui t'a motivée pour t'impliquer depuis plusieurs années dans le GDR ?

J'ai été impliquée comme correspondante locale pour les GDR IM et ISIS dès 1999, et j'ai vraiment été très enthousiaste quand le GDR Sécurité a vu le jour en 2016. Les GDR constituent à mes yeux des outils d'animation essentiels pour faire vivre les communautés tout en favorisant les liens entre champs disciplinaires différents (la sécurité, par exemple, regroupe des champs très divers), et en permettant à toutes les personnes qui le souhaitent, quel que soit leur employeur, de se rencontrer, d'échanger, et de ne pas se retrouver isolées. Cela favorise aussi l'émergence de sujets à la frontière des communautés, ce qui est fondamental en particulier en sécurité.

J'ai eu la chance de connaître les premières journées C2 pendant ma thèse et avoir cette opportunité de croiser les autres doctorants de France ainsi que leurs directeurs et directrices de thèse pendant plusieurs jours dans un cadre informel était vraiment une chance incroyable. C'est ce souvenir qui me motive pour permettre aux jeunes d'aujourd'hui de bénéficier d'événements tels que les journées des GT, les journées nationales, REDOCS, l'école d'été, *etc.*, pour un coût modique. J'ai commencé à m'investir dans le GDR Sécurité en 2016 en prenant la coordination du comité de pilotage de l'école d'été, puis en 2017 la co-animation du GT Sécurité et Données Multimédia. En 2021, je suis

d'abord devenue directrice adjointe en janvier, avant de prendre la direction du GDR en juillet.

Quelles sont les missions d'une directrice de GDR selon toi, et que prévois-tu de faire pendant ton mandat ?

Je dirais que ma mission est avant tout de m'assurer que le collectif vit bien, reste actif, de favoriser des échanges pour consolider les communautés et leurs thèmes de recherche, mais aussi faire émerger de nouveaux thèmes et de nouvelles collaborations. C'est aussi faire en sorte que ces liens soient le moins possible affectés par le fait que nous n'avons pas tous le même employeur, que ce soit la science qui nous guide avant tout. Je me sens finalement un peu comme une cheffe d'orchestre : ce n'est pas elle qu'on entend, mais sans elle, cela marcherait beaucoup moins bien. Je me sens avant tout au service des autres.

Le GDR est déjà très actif, et mon objectif est de continuer les activités actuelles et de les enrichir peu à peu avec de nouvelles, mais sans que cela devienne trop lourd à la fois pour le bureau comme pour les membres de la communauté. Car on ne peut pas être sans arrêt sollicités : il faut se garder du temps pour la recherche, comme pour la formation. Il faut donc trouver un équilibre. Parmi les nouvelles actions évoquées au sein du bureau, il y a le développement du club des partenaires pour renforcer les interactions entre académiques et industriels, le développement d'actions vers la société, peut-être la création d'un podcast. En tout cas, toutes les idées sont les bienvenues, c'est ensemble que nous construisons notre univers. Donc si vous avez des idées, ne vous censurez pas et faites-les connaître. De mon côté je me suis aussi personnellement investie depuis plusieurs années dans des interventions en collèges pour faire connaître les métiers de la recherche et de la sécurité aux jeunes, et en particulier leur montrer que toute personne motivée par ces secteurs peut y avoir sa place, filles comme garçons. C'est un sujet qui me tient à cœur, et c'est aussi ce qui a motivé ma participation au projet des « décodeuses du numérique » mené par l'INS2I. Je sais que je ne suis pas la seule à m'investir dans cette voie, et si parmi vous il y en a qui souhaitent que l'on coordonne des actions de plus grande envergure au sein du GDR sur ces questions d'éducation et de parité, j'en serai ravie.

Merci Caroline pour ces informations sur ton parcours, ainsi que pour ton investissement dans le GDR ! Nous te souhaitons bonne continuation dans ta mission de directrice et beaucoup de succès pour les initiatives que tu comptes mettre en œuvre !

Article rédigé par Caroline Fontaine (Laboratoire Méthodes Formelles, CNRS), Céline Chevalier et Pauline Puteaux, Contact : caroline.fontaine@lsv.fr

En direct des labos

Davide Balzarotti et Dora Matzakou

Après Paris et le DIENS dans le numéro précédent, cap sur la côte d'Azur pour cette dixième édition de la Gazette pour aller visiter EURECOM, situé à Sophia Antipolis. EURECOM est un centre de recherche en sciences du numérique regroupant 140 scientifiques (dont 76 doctorants et 26 enseignants-chercheurs). En particulier, il compte un département entièrement dédié à la sécurité informatique, dont nous interrogeons le responsable Davide Balzarotti, Professeur.

Bonjour Davide, quels sont les axes scientifiques d'EURECOM et plus précisément vos objectifs en matière de sécurité informatique ?

EURECOM est divisé en trois départements dont un entièrement dédié à la sécurité numérique. Le département sécurité compte 8 professeurs et plus de 40 doctorants et post-doctorants. Son activité s'organise autour de trois axes de recherche principaux : la sécurité des logiciels et des systèmes, la cryptographie et les technologies de protection de la vie privée, la biométrie et le multimédia.

La sécurité des logiciels et des systèmes étudie tous les aspects de la sécurité système, tels que la découverte de vulnérabilités, l'analyse binaire et de *malwares*, la sécurité sans fil et des communications et la forensique numérique – appliqués à une variété d'environnements différents (tels que les ordinateurs traditionnels, les infrastructures *cloud*, les systèmes embarqués et mobiles, et les technologies Web).

Le deuxième groupe adopte une approche plus fondamentale de la sécurité et de la confidentialité du point de vue de la cryptographie et de la cryptographie appliquée. La recherche dans ce domaine couvre une variété de sujets, tels que les preuves *Zero-Knowledge* et la cryptographie à clé publique, l'analyse des données préservant la confidentialité, la source de confiance distribuée, la sécurité et la confidentialité du ML et de l'IA et la biométrie préservant la confidentialité.

Enfin, le troisième axe se concentre sur l'application des technologies de sécurité et des médias numériques, telles que la surveillance, l'usurpation d'identité, la sécurité et l'explicabilité pour la reconnaissance faciale et vocale basée sur l'IA et la détection *DeepFake*. Le groupe dirige également l'initiative communautaire internationale VoicePrivacy, qui se consacre au développement de solutions de préservation de la vie privée pour la technologie vocale.

Davide Balzarotti.

Quelles sont vos collaborations dans ce domaine avec le tissu local, national et international ?

EURECOM est un consortium (GIE) qui comprend actuellement 11 membres académiques et 6 membres industriels et institutionnels. De plus, tous nos départements sont profondément connectés à l'environnement local de la technopole de Sophia Antipolis, qui héberge les laboratoires de R&D de dizaines d'entreprises nationales et internationales (par exemple, Norton Lifelock, SAP, Renault, Amadeus, pour n'en citer que quelques-uns qui collaborent régulièrement avec le département sécurité numérique). Inria Sophia Antipolis est également un proche collaborateur et un acteur pertinent du territoire actif dans le domaine de la sécurité numérique.

« Le département héberge une chaire 3IA sur l'apprentissage automatique préservant la confidentialité et un projet ERC *consolidator* sur l'analyse des systèmes compromis. »

Au niveau national, le département sécurité numérique fait actuellement partie de dix projets ANR nationaux, trois projets BMBF-MESRI (allemand-français) et quatre projets européens. Le département fait également partie de deux projets financés par les États-Unis, l'un avec la DARPA (programme CHESS) sur la découverte de vulnérabilités assistée par l'Homme et un avec l'US Air Force Research Labs sur l'analyse de *firmware* et plus généralement de la sécurité des systèmes embarqués. Les autres sources de financement du département incluent 15 contrats industriels avec des entreprises situées en France et à l'étranger. Globalement, ces projets assurent un vaste réseau de collaborations avec d'autres équipes de recherche partout dans le monde. En outre, le département héberge une chaire 3IA sur l'apprentissage automatique préservant la confidentialité et un projet ERC *consolidator* sur l'analyse des systèmes compromis.

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

EURECOM propose une large gamme de programmes dédiés à la cybersécurité, notamment une filière d'ingénierie sur la sécurité numérique, un *Master of Science in Digital Security* et un diplôme d'ingénieur de spécialisation en sécurité des systèmes informatiques et des communications.

Par ailleurs, le département sécurité est également impliqué dans deux programmes de double diplôme : le Master Erasmus Mundus en Sécurité et *Cloud Computing* et le Master EIT DIGITAL en Cybersécurité.

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

Nos professeurs ont publié plus de 40 articles en 2020, dont plusieurs dans les meilleurs conférences de sécurité tels que IEEE Security and Privacy, Usenix Security et NDSS. Ainsi, il est difficile de choisir une seule contribution parmi les nombreux excellents résultats de recherche du département.

« Une ligne récente de travaux qui a été particulièrement réussie se concentre sur la découverte de vulnérabilités par *fuzzing*. »

Juste pour donner un exemple, une ligne récente de travaux qui a été particulièrement réussie se concentre sur la découverte de vulnérabilités par *fuzzing*. Le département travaille dans ce sens avec pour objectif de tester à la fois les logiciels traditionnels et les systèmes embarqués. Par exemple, « Symbolic execution with SymCC » a reçu un *Distinguished Paper Award* à Usenix Security 2020 pour sa nouvelle approche basée sur la compilation de l'exécution symbolique. SymQEMU, suit cette approche en instrumentant la représentation intermédiaire de QEMU (ouvrant la possibilité de l'utiliser pour les logiciels embarqués et les binaires), a été présenté cette année à la conférence NDSS. Le département a également exploré une approche orthogonale qui proposait l'utilisation d'invariants probables au lieu d'une exécution symbolique pour piloter un *fuzzer*. Cette solution a été récemment présentée à Usenix 2021.

Merci Davide pour ces informations très intéressantes et bonne continuation au département et à ses membres pour ces travaux passionnants !

Article rédigé par Davide Balzarotti (EURECOM), Dora Matzakou (EURECOM), Céline Chevalier et Pauline Puteaux, Contact : davide.balzarotti@eurecom.fr, theodora.matzakou@eurecom.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.

Stage, Télécom Paris (Palaiseau) ou Université Clermont Auvergne

Sujet : Validation formelle des requêtes PKI C-ITS
Mounira Msahli,
mounira.msahli@telecom-paris.fr
Pascal Lafourcade,
pascal.lafourcade@uca.fr

Deux postes de post-doctorat, Campus George Charpak Provence (Gardanne)

Sujet 1 : Intégration de primitives cryptographiques post-quantiques sur circuit intégré
Durée : 2 ans
Partenariat avec l'entreprise THALES DIS
Sujet 2 : Résistance aux attaques par observations des cryptosystèmes post-quantiques
Durée : 1 an
Partenariat avec l'entreprise WISEKEY
Nadia El Mrabet,
nadia.el-mrabet@emse.fr

Deux thèses de doctorat, Institut Polytechnique de Paris

Sujet 1 : Modélisation et évaluation de sécurité d'un système complexe
Sujet 2 : Jumeau numérique pour la sécurité de la gestion technique de bâtiment
Grégory Blanc,
gregory.blanc@telecom-sudparis.eu

Poste d'ingénieur plateforme, Institut Polytechnique de Paris

Sujet : Évaluation de sécurité des systèmes d'information industriels complexes
Grégory Blanc,
gregory.blanc@telecom-sudparis.eu

Poste de Professeur, Université du Québec (Montréal)

Sujet : Informatique théorique (cryptographie)
Marc-Olivier Killijian,
killijian.marc-olivier.2@uqam.ca

Poste de post-doctorat, LORIA (Nancy)

Sujet : Privacy Control for Online Social Media
Durée : 12 mois
Maira Nassau,
maira.nassau@loria.fr

Experts CIR pour le MESRI

Expertise scientifique et technique des dossiers de Crédits Impôts Recherche (CIR)
Samia Bouzefrane,
samia.bouzefrane@lecnam.net

Thèse de doctorat, LAMIH/UPHF (Valenciennes)

Sujet : Détection biométrique de mémoire oculaire et applications en cybersécurité
Antoine Gallais,
antoine.gallais@uphf.fr

Poste d'ingénieur R&D, CEA (Grenoble)

Sujet : Logiciel embarqué, compilation, cyber-sécurité
Durée : 18 mois (renouvelables)
Damien Couroussé,
damien.courousse@cea.fr

Responsable de la coopération avec la filière Cybersécurité, CNRS (La Défense - Campus Cybersécurité et Paris 16)

Sujet : Définir et mettre en œuvre une politique de coopération du CNRS avec l'ensemble des acteurs économiques impliqués dans la Cybersécurité
Date limite de candidature : 2 novembre
Durée : 36 mois
Olivier Cappé,
olivier.cappe@cnrs.fr