Février 2024
Numéro 16

LA GAZETTE DU GDR

Sécurité Informatique - GDR2046

Édito de la directrice

Cet edito est l'occasion de féliciter les lauréates de plusieurs prix décernés depuis le dernier numéro : Sandrine Blazy pour la médaille d'argent du CNRS, Anne Canteaut pour le prix Irène Joliot-Curie de la femme scientifique de l'année, Oana Goga pour le prix Lovelace-Babbage ainsi que la médaille de bronze du CNRS, et Nataliia Bielova pour sa reconnaissance comme "étoile montante" par W@Privacy ! ! ! Sandrine et Anne sont interviewées dans ce numéro, et nous espérons pouvoir vous présenter les interviews de Nataliia et Oana prochainement. Vous trouverez également dans ce numéro l'interview de Romain Cayre, accessit au prix de thèse du GDR l'an dernier, et les retours sur les journées nationales, sur l'école d'été, les journées C2, et enfin REDOCS. Merci encore à toutes celles et tous ceux qui se sont investis dans leur organisation. J'espère que ces articles vous rappelleront de bons moments si vous y avez participé, et vous donnerons envie d'assister à ceux qui se profilent : journées MFS en avril, RESSI en mai, Journées Nationales et APVP en juin, école d'été en juillet.

Depuis le dernier numéro l'équipe de direction du GDR s'est élargie et Adeline Roux-Langlois a rejoint le bureau en tant que Directrice Adjointe. Au niveau des responsables de GT il y a aussi eu quelques changements depuis la dernière gazette, avec l'arrivée de Iuliia Tchakenko pour le GT SDM et Estelle Cherrier-Pawlowski pour le GT PVP. Ces changements sont rappelés plus en détail dans les brèves de ce numéro.

L'année 2024 sera une année importante pour le GDR puisque ce sera l'année de son renouvellement. Nous sommes donc en train de travailler au projet qui nous engagera sur la nouvelle mandature. Si vous souhaitez proposer des idées, des coups de mains, etc. n'hésitez pas à nous contacter Adeline ou moi.

Très bonne lecture et à très bientôt !

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 MFS, *Oléron, France, 3-5 avril 2024,* https://gtmfs2024.sciencesconf.org/

RESSI (GT SSLR), *Eppe-Sauvage, France, 15-17 mai 2024,* https://ressi2024.sciencesconf.org/

Journées Nationales du GDR, *Rennes, France, 10-12 juin 2024*

Ecole d'été du GDR, Cyber in Berry 2.0, *Bourges, France, 15-19 juillet 2024,* https://cyberinberry2.sciencesconf.org/

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

Africacrypt 2024, *Douala, Cameroon, 10-12 juillet 2024*

GRASEC 2024 : The 5th International Workshop on Graph-based Approaches for CyberSecurity to be held in conjunction with the 19th International Conference on Availability, Reliability and Security, *Vienne, Autriche, 30 juillet - 2 août*

C&ESAR 2024 : the 31st Computer & Electronics Security Application Rendezvous, *Rennes, France, 19-20 novembre 2024*

Le coin prospectif

Sandrine Blazy

La gazette interviewe Sandrine Blazy, professeure à l'université de Rennes, directrice adjointe de l'IRISA, et spécialiste des compilateurs et des logiciels sûrs. Elle a développé avec Xavier Leroy, CompCert, le premier compilateur pour le langage C vérifié à l'aide de l'assistant à la démonstration Coq. Elle poursuit ses travaux pour doter CompCert de davantage de possibilités de compilation, et offrir des garanties supplémentaires en termes de sécurité logicielle. Elle vient de recevoir la médaille d'argent du CNRS.

Félicitations pour cette médaille d'argent ! Peux-tu présenter rapidement tes activités, en particulier celles qui ont conduit à l'obtention de ce prix ?

Depuis 20 ans, je m'intéresse à la compilation vérifiée, c'est-à-dire à la vérification déductive appliquée aux compilateurs. La vérification déductive permet d'avoir des garanties très fortes sur l'absence d'erreur dans les logiciels. La compilation vérifiée fournit une démonstration établissant que le compilateur n'introduit pas de bug. Pour des logiciels réalistes tels qu'un compilateur du langage C, cette preuve est nécessairement vérifiée par ordinateur, à l'aide d'un assistant à la démonstration, un logiciel qui automatise une partie du raisonnement, s'assure que la démonstration est complète et respecte les lois de la logique mathématique. Avec Xavier Leroy, dès 2003, nous avons développé CompCert, qui est le premier compilateur optimisant ciblant plusieurs architectures et utilisé dans l'industrie, et qui est doté d'une preuve mathématique de correction vérifiée par ordinateur. Depuis mon arrivée à Rennes en 2009, j'utilise CompCert dans mes recherches afin de le doter de davantage de possibilités de compilation, mais aussi d'offrir des garanties supplémentaires, notamment en termes de sécurité logicielle. C'est l'ensemble de ces travaux qui a été récompensé.

Sandrine Blazy
(Jean-Claude MOSCHETTI / CNRS Images)

Peux-tu nous en dire un peu plus sur cette propriété de correction ?

La propriété de correction garantie par CompCert exprime une préservation sémantique : tout programme compilé se comporte comme le programme source dont il est issu. Elle se fonde sur les sémantiques formelles des langages source et cible du compilateur, en l'occurrence le langage C et différents langages assembleur. Une difficulté a été de définir une sémantique opérationnelle de C réaliste, ainsi qu'un principe de raisonnement associé, applicable à tous les programmes C modélisés, c'est-à-dire non seulement ceux dont l'exécution termine mais aussi ceux dont l'exécution diverge (ce qui est le cas par exemple d'un logiciel de commandes de vol d'un avion). Une contrainte supplémentaire a été la nécessité de valider notre sémantique du C (n'ayant pas de sémantique de référence), et de permettre aux utilisateurs d'exécuter cette sémantique afin de tester que leurs programmes sont exempts de comportements indéfinis.

« La propriété de correction garantie par CompCert exprime une préservation sémantique : tout programme compilé se comporte comme le programme source dont il est issu. »

Vois-tu d'autres difficultés ?

Un compilateur vérifié comprend un logiciel, le compilateur, ainsi que sa preuve de correction. Développer un compilateur vérifié nécessite à la fois de programmer le logiciel en utilisant le langage de programmation de l'assistant de preuve (en l'occurrence Coq) afin qu'il génère des programmes efficaces, et de définir un modèle sémantique et des abstractions sur lesquelles raisonner, afin de mener la preuve. Cette co-conception logiciel/preuve est un véritable défi scientifique. En effet, bien que ces deux objectifs soient étroitement liés (la preuve utilise directement le code du logiciel, en plus des notions sémantiques sur lesquelles le raisonnement est effectué), ils sont aussi parfois antagonistes (par exemple, soit la preuve a besoin de calculer des structures de données supplémentaires, qui facilitent le raisonnement mais ralentissent également l'exécution des programmes compilés, soit le logiciel utilise des structures de données fonctionnelles mais moins efficaces).

Qu'en est-il de CompCert aujourd'hui ?

CompCert a été conçu pour compiler des logiciels embarqués critiques, domaines où la fiabilité logicielle est primordiale. CompCert est commercialisé par la société allemande AbsInt ; il a été utilisé dans l'industrie avionique et le nucléaire. Dans ces domaines, le principal intérêt pour CompCert a été l'amélioration des performances du code produit tout en respectant les exigences de traçabilité imposées par les processus de qualification, ce que CompCert a effectivement permis. CompCert est aussi une infrastructure ouverte de recherche. Plusieurs projets en cours réutilisent CompCert

afin de l'étendre à d'autres langages, soit en développant un nouveau *front-end*, soit un nouveau *back-end*. Par exemple, les compilateurs Velus et L2C pour les langages synchrones ciblent le langage Clight de CompCert. Un autre exemple est le *back-end* Kalray KVX. D'autres projets tels que VST réutilisent la sémantique de Clight afin de définir une logique de programme pour prouver le plus automatiquement possible des programmes C, ce qui garantit grâce à CompCert que la propriété établie au niveau source reste valable sur les programmes compilés.

(Jean-Claude MOSCHETTI / IRISA / CNRS Images)

Selon toi, quels sont les défis à relever en compilation vérifiée ?

CompCert a montré qu'il est désormais possible de raisonner sur des objets aussi complexes que des compilateurs. Ce n'est qu'un jalon et il y a encore beaucoup à faire. Il serait intéressant d'ajouter des optimisations utiles pour d'autres domaines d'utilisation, notamment les optimisations de boucles particulièrement difficiles à prouver. Une autre piste de recherche est la concurrence en mémoire partagée dans un modèle de mémoire faiblement cohérent, tel que standardisé dans C 2011. La sémantique opérationnelle des programmes concurrents en C 2011 est extrêmement complexe ; son utilisation pour prouver la correction d'une transformation de programme est une question ouverte. Concernant les assistants de preuve, des travaux sont nécessaires pour permettre davantage de raisonnement automatique, et également proposer de meilleurs outils logiciels pour manipuler des sémantiques opérationnelles. Enfin, un domaine actif de recherche est la compilation sécurisée, qui étend la compilation vérifiée pour garantir des propriétés de sécurité utilisées notamment en cryptographie telles que l'absence de canaux cachés, et des premiers résultats ont été obtenus avec les compilateurs vérifiés CompCert et Jasmin.

« Un domaine actif de recherche est la compilation sécurisée, qui étend la compilation vérifiée pour garantir des propriétés de sécurité utilisées notamment en cryptographie. »

Quels conseils peux-tu donner aux jeunes chercheurs et chercheuses intéressés par la compilation vérifiée ?

Tout d'abord, lire et manipuler les outils du domaine pour se forger sans cesse une culture scientifique et trouver des sujets qui nous passionnent, qui vont nous accaparer pendant longtemps. Plus généralement, ne pas hésiter à élargir son horizon, être curieux de ce que font les collègues et aller discuter avec eux.

Et puis, ne pas sous-estimer le hasard des rencontres. Ma vie scientifique est faite de rencontres enrichissantes. Par exemple, j'ai rencontré Andrew Appel lors de son congé sabbatique en France, alors qu'il commençait à formaliser en Coq une logique de programme (devenue par la suite VST) et que je cherchais à établir l'équivalence entre différents styles sémantiques pour le langage Clight de CompCert. Nous avons fini par proposer un nouveau style sémantique qui est devenu celui utilisé par CompCert.

Merci Sandrine, et encore bravo !

Article rédigé par Sandrine Blazy (Inria, Univ Rennes, CNRS, IRISA) et Céline Chevalier, contact : sandrine.blazy@irisa.fr

Brèves

Les candidatures pour le prix de thèse 2024 sont désormais closes. Rendez-vous début avril 2024 pour les résultats ! Plus d'informations à l'adresse https://gdr-securite.irisa.fr/prix-de-these/.

Le projet Sciences des éditions ISTE vient de s'enrichir de plusieurs nouveautés sur le thème de la cryptographie et de la sécurité des données (dont le responsable est Damien Vergnaud), coordonnées d'une part par David Pointcheval (cryptographie asymétrique) et d'autre part par Christina Boura et María Naya-Plasencia (cryptographie symétrique, en deux tomes) : https://www.istegroup.com/fr/theme/cryptographie-securite-des-donnees/.

Le coin prospectif

Anne Canteaut

La gazette interviewe Anne Canteaut, directrice de recherche dans l'équipe-projet COSMIQ, au centre Inria de Paris et présidente entre 2019 et 2023 de la Commission d'Évaluation de l'Inria. Anne est lauréate 2023 du prix Irène Joliot-Curie de la femme scientifique de l'année, attribué par l'Académie des Sciences et l'Académie des Technologies. Elle est spécialiste de cryptographie symétrique et s'intéresse à la fois à la cryptanalyse et à la conception de nouveaux chiffrements et fonctions de hachage.

Peux-tu présenter rapidement tes activités, en particulier celles qui ont conduit à l'obtention de ce prix ?

Je m'intéresse aux primitives cryptographiques symétriques, tels l'AES ou les fonctions de hachage. La cryptanalyse joue donc un rôle important dans mes travaux, puisque que, contrairement aux protocoles dont la sécurité peut être démontrée en idéalisant les primitives sous-jacentes, la seule manière de garantir qu'une primitive possède le niveau de sécurité attendu est de tenter de la « casser ». Ce constat s'applique d'ailleurs également aux primitives asymétriques, même lorsqu'elles reposent sur un problème difficile, car ce qui importe en cryptographie, c'est le coût de résolution du problème en dimension fixée.

Dans ce contexte, j'essaie de faire en sorte que la recherche sur les primitives cryptographiques ne se résume pas à une incessante partie de ping-pong entre concepteurs et cryptanalystes. Ce qui m'intéresse est donc de formaliser les attaques dédiées à des primitives spécifiques afin de mettre en évidence les propriétés qui les rendent opérationnelles. Le but est de définir de nouveaux critères de conception et de construire des objets qui permettent de résister à ces attaques de manière certaine.

À quel type d'attaques t'intéresses-tu plus particulièrement ?

Un des sujets qui m'intéresse plus particulièrement est de comprendre si certaines propriétés algébriques des composants d'une primitive, typiquement des propriétés de leur représentation polynomiale, peuvent être exploitées dans une attaque. En effet, les concepteurs choisissent souvent des composants optimaux selon divers critères, soit pour leur implémentation soit pour leur résistance à certaines attaques connues. Or, cette optimalité va souvent de pair avec des structures mathématiques particulières, susceptibles d'introduire des faiblesses inattendues. Avec mes collègues, nous avons par exemple mis en évidence les faiblesses induites par l'utilisation d'une fonction non-linéaire ayant un faible degré multivarié, ou représentée par un simple monôme sur un corps fini.

> « Ce qui m'intéresse est donc de formaliser les attaques dédiées à des primitives spécifiques afin de mettre en évidence les propriétés qui les rendent opérationnelles. »

La recherche sur les primitives symétriques est-elle toujours d'actualité, malgré l'adoption de standards bien établis comme l'AES ou SHA-3 ?

Oui car, même si l'AES ou SHA-3 sont des primitives solides, elles ne peuvent pas servir de couteau suisse, et il y a des applications auxquelles elles ne sont pas adaptées. C'est par exemple ce qui a motivé la compétition « *lightweight* » du NIST qui vient de s'achever par le choix du chiffrement authentifié ASCON. La diversification des applications, par exemple les preuves *zero-knowledge* qui nécessitent des fonctions de hachage ayant des propriétés très inhabituelles, induit également une profusion de nouvelles propositions. Nous avons donc besoin de nouveaux outils, mathématiques et algorithmiques, pour évaluer de manière précise leur niveau de sécurité. Par ailleurs, il est indispensable de continuer à analyser des standards bien établis comme l'AES, de tenter d'améliorer les attaques existantes et de mieux comprendre leur sécurité. C'est à la fois nécessaire pour que l'on puisse continuer à faire confiance aux primitives que nous utilisons, et pour que l'on dispose de fondements solides permettant d'étayer les futures constructions.

Anne Canteaut

Pourquoi avoir choisi ce domaine de recherche ?

En fait, ma thèse a principalement porté sur un tout autre sujet : la cryptographie à clef publique à base de codes, notamment le système de McEliece. C'est un des principaux volets de la cryptographie post-quantique, mais à l'époque, même si l'on savait déjà qu'un éventuel ordinateur quantique remettrait en cause la sécurité de nos principaux systèmes asymétriques, comme le RSA ou ceux reposant sur la difficulté du log discret, ce sujet

n'était pas du tout au goût du jour. Ces systèmes alternatifs à ceux qui étaient bien établis étaient vus comme une lubie de quelques mathématiciens. À la fin de ma thèse, la plupart des collègues m'ont incitée à m'orienter vers un autre domaine de la cryptographie, ce qui était indéniablement un bon conseil. J'avais commencé quelques travaux en cryptographie symétrique à la fin de ma thèse, et j'ai donc naturellement poursuivi lors de mon postdoc à l'ETH Zürich dans l'équipe de Jim Massey.

J'aime beaucoup raconter cette histoire, qui fait sourire quand on sait que la cryptographie post-quantique est un sujet actuellement hyper médiatisé et que les collègues, que l'on a incités à abandonner ces recherches il y a 20 ans, reçoivent désormais de multiples sollicitations et financements. Si ces collègues n'avaient pas eu le courage et l'énergie de continuer à travailler dans cette voie, nous aurions perdu collectivement l'expertise sur ce sujet, et nous n'aurions jamais été capables de proposer des primitives post-quantiques efficaces à base de codes car leur sécurité repose sur des travaux qui ont nécessité un effort de longue haleine.

Cet épisode, puis mon mandat de présidente de la Commission d'Évaluation de l'Inria, m'ont beaucoup appris sur la politique de la recherche et la manière de définir les orientations scientifiques, à l'échelle d'un institut, d'une université, d'un pays ou d'une communauté. Je crois tout d'abord qu'il n'y a pas de grand visionnaire capable de déterminer les directions de recherche qui auront des répercussions majeures dans 10 ou 20 ans. Croire que cela serait possible est même dangereux parce que cela conduit à se fermer des portes, à abandonner des sujets qui auraient pu avoir des conséquences importantes. La définition des orientations scientifiques doit au contraire être une décision collégiale, et résulter d'une discussion. Par ailleurs, il me semble que l'essentiel est de préserver la diversité des thèmes de recherche, et de ne pas céder aux phénomènes de modes, comme on a tendance à le faire en ce moment, sans quoi on assèche certains domaines.

Selon toi, quels sont les défis à relever en cryptographie symétrique ?

De manière générale, un des défis majeurs est de faire évoluer les primitives cryptographiques, symétriques et asymétriques, vers une plus grande simplicité. Je crois en effet que les primitives que nous proposons actuellement sont trop complexes pour devenir des outils classiques, indispensables et bien maîtrisés par les développeurs. Cette « complexité » est dissuasive et entrave parfois le déploiement de la cryptographie. Le fait qu'il soit encore difficile de motiver certains choix de conception dans les spécifications de nos standards (par exemple, le cadencement de clef dans les chiffrements par blocs) est problématique, car il est difficile d'implémenter sans erreur un algorithme dont les principes nous échappent comme de recopier sans faute un texte écrit dans une langue qui nous est complètement étrangère. Cette situation est par ailleurs la source de suspicions, parfois légitimes. Enfin, cette complexité s'avère parfois coûteuse, notamment en énergie, ce qui est rédhibitoire pour certaines applications. Il me semble donc important de réussir à faire reposer nos primitives sur quelques principes de conception simples qui régissent le choix de l'ensemble des composants du système et d'aboutir à des conceptions minimalistes et épurées.

Quels conseils peux-tu donner aux jeunes chercheurs et chercheuses intéressés par la recherche en cryptographie ?

Se méfier des modes dans lesquelles tout le monde s'engouffre. Il y a des sujets essentiels et passionnants en informatique au-delà de l'IA et du quantique, et il est important qu'on ne les délaisse pas. Il faut donc tenter, autant que faire se peut, de ne pas se faire dicter ses choix en recherche par la mode, mais par sa curiosité et par ce qui nous intéresse.

Un deuxième conseil est de prendre conscience que la recherche est une activité très exigeante intellectuellement, comme toute activité créatrice, et peut donc parfois être difficile à vivre. Pour ma part, c'est la dimension collective de ce travail qui m'a toujours motivée, et m'a permis de surmonter des moments de doute. C'est par la discussion, la confrontation des points de vue qu'on fait avancer les choses.

Merci Anne pour ces éclairages très intéressants sur ta discipline et la recherche en général, et encore bravo pour ton prix !

Article rédigé par Anne Canteaut (COSMIQ, Inria Paris) et Céline Chevalier, contact : anne.canteaut@inria.fr

Arrivées et départs du bureau du GDR

Depuis le dernier numéro de la gazette, deux responsables de GT ont passé le relai. Benjamin Nguyen a été remplacé par Estelle Cherrier-Pawlowski en tant que co-responsable du GT PVP, aux côtés de Mathieu Cunche. Philippe Carré a été remplacé par Iuliia Tkachenko en tant que co-responsable du GT SDM, aux côtés de William Puech. L'équipe de direction s'est quant à elle agrandie avec l'arrivée d'Adeline Roux-Langlois en tant que directrice adjointe. Merci à vous cinq pour votre investissement et votre enthousiasme ! Si vous ne la connaissez pas, la composition complète du bureau du GDR est disponible ici : https://gdr-securite.irisa.fr/bureau/.

Le coin prospectif

Romain Cayre

La gazette interviewe Romain Cayre, accessit du Prix de thèse du GDR en 2023, pour sa thèse intitulée « Offensive and defensive approaches for wireless communication protocols security in IoT» qui a été effectuée au Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS) sous la direction de Guillaume Auriol et de Mohamed Kaâniche. Romain est actuellement en post-doc à EURECOM au sein du groupe de recherche Sécurité numérique, avec Aurélien Francillon, et collabore régulièrement avec Damien Cauquil, responsable R&D à Quarkslab. La gazette a décidé d'interroger Romain sur son domaine de recherche en général et sur ses travaux en particulier.

Bonjour Romain, félicitations pour ton accessit ! Tu as soutenu ta thèse à la fin de l'année 2022. Peux-tu nous en dire un peu plus sur tes principales contributions ?

Bonjour, et merci ! Mes thématiques de recherche portent sur la sécurité des protocoles de communication sans fil déployés dans le contexte de l'Internet des Objets. Ces dernières années, on a en effet pu assister à l'émergence des objets connectés dans divers domaines de la vie quotidienne, ce qui a entraîné le déploiement de nombreuses technologies de communication sans fil concurrentes visant à répondre aux enjeux spécifiques (faible consommation, mobilité, etc) liés à ces nouveaux systèmes. Ces technologies posent de nouveaux défis du point de vue de la sécurité, notamment liés à leur hétérogénéité, ainsi qu'à la nature dynamique et décentralisée des réseaux de l'Internet des Objets. L'objectif de mes travaux consiste à évaluer, détecter et prévenir les nouvelles menaces liées au déploiement de ces protocoles de communications sans fil. Les contributions de ma thèse s'organisent selon deux axes complémentaires : un axe offensif, visant à explorer les nouvelles menaces liées à ce contexte, ainsi qu'un axe défensif, principalement dédié à la détection et à la prévention de celles-ci.

> « L'objectif de mes travaux consiste à évaluer, détecter et prévenir les nouvelles menaces liées au déploiement de ces protocoles de communications sans fil. »

Mes contributions offensives s'orientent principalement sur l'analyse de menaces inhérentes à la spécification des protocoles, avec un intérêt particulier sur les couches basses. J'ai notamment développé un *framework* offensif nommé Mirage, facilitant l'implémentation et l'automatisation d'attaques visant les protocoles sans fil de l'Internet des Objets. Cette première contribution a permis le développement de divers outils, permettant d'analyser en profondeur la couche physique et la couche liaison de divers protocoles tels que *Bluetooth Low Energy* et Zigbee. Cela a notamment rendu possible la seconde contribution offensive de ma thèse, consistant en une stratégie d'attaque nommée InjectaBLE, qui permet à un attaquant d'injecter du trafic arbitraire au sein d'une connexion *Bluetooth Low Energy*. Elle repose sur l'exploitation d'une situation de compétition visant un mécanisme de la couche liaison destiné à compenser un potentiel décalage entre les horloges des équipements cibles, et permet la mise en place de stratégies d'attaque de type usurpation d'identité ou Homme du Milieu. La troisième contribution offensive met en évidence un nouveau type d'attaques, liées à la coexistence de technologies sans fil hétérogènes dans les mêmes bandes de fréquence : les attaques pivots inter-protocolaires. Il est en effet possible de détourner certains mécanismes radios bas niveau de la pile protocolaire *Bluetooth Low Energy* pour communiquer avec des protocoles sans fil non supportés nativement, tels que le protocole ZigBee, et potentiellement mener des attaques sans fil visant ces derniers. Cette situation ouvre une nouvelle surface d'attaque difficile à anticiper, et s'avère particulièrement problématique dans un contexte de déploiement massif de la technologie *Bluetooth Low Energy* (*smartphones*, objets connectés, ordinateurs...).

Romain Cayre

Sur le plan défensif, je me suis concentré sur le développement d'approches de détection et de prévention d'intrusion adaptées au contexte de l'Internet des Objets. J'ai notamment proposé OASIS, un *framework* de détection d'intrusion permettant d'embarquer des modules de détection au sein des contrôleurs *Bluetooth Low Energy*. Le *framework* permet de générer un logiciel de détection embarqué instrumentant le *firmware* du contrôleur afin de collecter des métriques pertinentes pour la détection, et d'exécuter des modules défensifs

de façon générique, indépendamment de l'implémentation du contrôleur. J'ai également proposé une approche de filtrage du trafic destinée à la prévention d'intrusion pour les protocoles sans fil pair à pair, reposant sur l'utilisation d'une stratégie de brouillage réactif, technique généralement utilisée dans un contexte offensif, à des fins défensives.

Peux-tu nous décrire le fonctionnement de Mirage, le framework Python offensif ciblant les communications sans fil utilisées dans l'IoT que tu as développé ?

Le développement de cet outil a principalement été motivé par la très grande diversité des outils matériels et logiciels destinés à la mise en œuvre pratique d'attaques sans fil, l'utilisation de bibliothèques haut niveau peu adaptées au développement d'outils offensifs, et la difficulté de coordonner ces outils entre eux. Le *framework* Mirage, développé en Python et publié sous licence libre (MIT), fournit une architecture logicielle destinée au développement d'attaques sans fil, unifiée, modulaire et générique. Il implémente nativement le support de nombreux outils matériels offensifs, fournit sept piles protocolaires majeures ainsi que de nombreux modules d'attaques, et peut être facilement étendu à de nouveaux protocoles ou de nouveaux outils matériels.

Il permet ainsi de réaliser facilement des stratégies d'attaques communes visant divers protocoles sans fil, et fournit une série de mécanismes destinés à faciliter l'automatisation de tâches offensives. Les attaques sont implémentées sous la forme de modules configurables, faciles à développer et à étendre, qui peuvent être combinés entre eux grâce à un mécanisme de *pipeline* pour construire des scénarios plus complexes. Le *framework* a été enrichi tout au long de la thèse, et a été utilisé dans divers contextes, tels que des audits de sécurité ou des travaux de recherche. Il a par exemple été utilisé pour évaluer une méthode de détection d'intrusion générique reposant sur le *monitoring* large bande des communications radio, ou pour évaluer certains mécanismes de sécurité du *Bluetooth Low Energy*.

Tu poursuis en ce moment tes travaux à EURECOM avec Aurélien Francillon. Quels sont les objectifs que tu vises actuellement en matière de recherche ?

Dans le cadre de mon post-doctorat à EURECOM, je continue d'explorer des thématiques de recherche à l'interface entre sécurité embarquée et sécurité sans fil. Dans le cadre d'un projet de recherche en collaboration avec Damien Cauquil (Quarkslab), je me suis intéressé à l'analyse et au détournement de la pile protocolaire *Bluetooth Low Energy* embarquée au sein des systèmes-sur-puces ESP32, et à la façon dont ces derniers peuvent être instrumentés pour mener des attaques sans fil avancées. Je poursuis également mes travaux de recherche autour de la détection d'intrusion, dans l'objectif d'améliorer et de généraliser à d'autres protocoles sans fil l'approche embarquée initiée durant ma thèse avec le *framework* défensif OASIS. Bien que l'instrumentation des piles protocolaires embarquées introduise de nombreux défis techniques, elle permet d'envisager de nombreuses applications innovantes pertinentes pour la sécurité des communications sans fil, tant sur le plan offensif que défensif.

Quels conseils pourrais-tu donner aux doctorants travaillant en sécurité informatique ?

C'est une question difficile ! Je pense que le meilleur conseil qu'on puisse donner à un doctorant est de bien s'entourer et d'échanger dès que possible sur son travail, que ce soit avec ses encadrants, les collègues doctorants ou d'autres chercheurs. Chacun a sa propre sensibilité, ses compétences et sa manière de concevoir la recherche, et ces échanges permettent souvent de développer de nouvelles idées et de prendre du recul sur son sujet. Il faut être particulièrement attentif aux opportunités de collaborer sur un sujet, notamment avec les autres doctorants : il est toujours plus agréable de travailler en coopération, et mes plus beaux souvenirs de thèse sont sans aucun doute les moments d'échange et de partage au sein de l'équipe ! La dimension humaine du travail de recherche ne doit pas être négligée. Pour ceux qui aiment ça, je pense que l'enseignement peut aussi être une composante très enrichissante durant une thèse : cela permet souvent de sortir un peu de son sujet de recherche, de prendre confiance en soi et de se sentir utile aux étudiants. Dans mon cas, j'ai pris beaucoup de plaisir à enseigner durant ma thèse, et je pense que cela a joué un rôle important dans mon travail.

Merci Romain pour toutes ces explications et ces détails très intéressants !

Article rédigé par Romain Cayre (EURECOM, Nice) et Céline Chevalier, contact : romain.cayre@eurecom.fr

Retour sur les Journées Nationales 2023

Brice Colombier

La sixième édition des journées nationales du GDR sécurité informatique s'est déroulée au campus cyber à Paris, du 26 au 28 juin derniers. Cette année, l'organisation était pilotée par Adeline Roux-Langlois et Nicolas Porquet. C'était l'occasion pour l'ensemble de la communauté française de se retrouver, d'échanger sur les travaux en cours ou bien encore de découvrir des sujets de recherche voisins. Le programme, dense et varié, a permis de tisser des liens entre les différentes thématiques de la sécurité.

Ainsi, les journées nationales ont commencé par une *keynote* donnée par Julia Lawall, qui nous a présenté l'outil Coccinelle, qui intéressera sûrement toutes les personnes développant des projets d'envergure en C. Cet outil permet d'apporter des modifications globales à la base de code, via l'utilisation de *patchs* sémantiques décrivant ces modifications. Il est notamment utilisé dans un projet que tout le monde connaît, le noyau Linux lui-même ! Après la première pause café, c'est Shweta Shinde, venue de l'ETH Zurich, qui nous présentait les enjeux liés à la souveraineté des utilisateurs sur les *smartphones* qui peuplent leurs poches. À travers l'exemple d'une messagerie sécurisée, nous avons découvert la proposition TEETime qui permettrait de mettre en œuvre, sur la plateforme matérielle Arm, les concepts présentés.

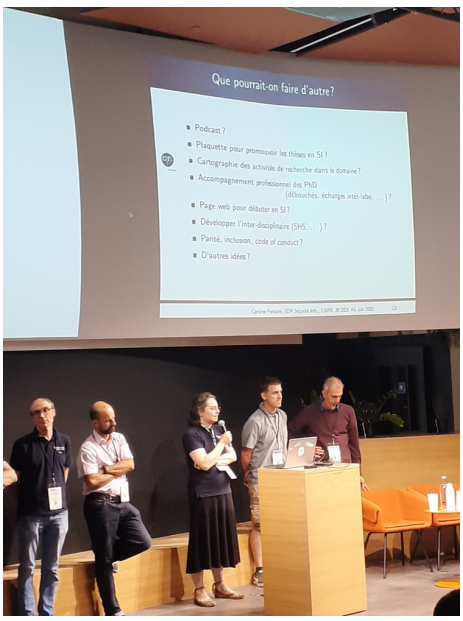
Refroidis au sens propre par la vigoureuse climatisation du campus cyber mais pas au sens figuré, les participants ont ensuite pu assister aux sessions dédiées aux groupes de travail C2 (codage et cryptographie), SDM (sécurité des données multimédia) et PVP (protection de la vie privée). La question du traitement de données respectueux de la vie privée, et des moyens techniques nécessaires pour sa mise en œuvre, était au cœur de nombreuses présentations. La journée s'est conclue par une présentation du PEPR cybersécurité.

La deuxième journée a débuté par deux présentations en session plénière. Andreas Uhl, de l'Université de Salzburg nous a expliqué que bien que les techniques de *deep learning* aient permis de grands progrès dans le domaine de la reconnaissance faciale, elles s'accompagnent de menaces sur la sécurité des données manipulées. Dans la seconde présentation, donnée par Oana Goga du Laboratoire d'Informatique de l'École Polytechnique, ce sont les publicités politiques apparaissant sur les réseaux sociaux en périodes d'élections qui étaient discutées, notamment sous l'angle du respect à la vie privée.

Pour la seconde partie de la matinée, nous avions l'honneur de recevoir Shafi Goldwasser du MIT et Weizmann Institute of Science, qui nous a présenté des pistes pour réconcilier apprentissage automatique et sécurité, en particulier lorsque les calculs sont réalisés sur des serveurs distants. La matinée s'est terminée par des présentations de divers outils utiles à la communauté.

Tout comme la matinée, l'après-midi a commencé par deux présentations en session plénière. Dans la première, c'est Frank Piessens de KU Leuven qui nous a parlé d'attaques sur les enclaves sécurisées présentes dans certains processeurs, en particulier via l'utilisation des interruptions comme technique de mesure. Dans la seconde présentation, c'est Guillaume Cluzel de TrustInSoft qui nous a détaillé l'utilisation d'outils pour la preuve formelle, comme J^3, pour trouver des failles dans les implémentations en C de fonctions de sécurité.

La journée s'est poursuivie par la remise du prix de thèse du GDR à Tina Nikoukhah, dont les travaux portent sur la détection des modifications malveillantes d'images JPEG. Nous avons ainsi appris avec stupeur qu'il n'y avait ni chien ni chat à sa soutenance de thèse ! L'outil Zero qu'elle a développé est notamment intégré dans le plug-in pour navigateurs web InVID-WeVerify, utilisé quotidiennement par les journalistes de l'AFP pour s'assurer de la véracité des images qu'ils utilisent. Enfin, la traditionnelle assemblée générale du GDR s'est tenue. Des discussions nombreuses ont émergé, notamment sur les actions à mener pour faire connaître les activités du GDR auprès des étudiants, dont l'intérêt pour la cybersécurité est certain mais qui n'en cernent pas toujours bien les contours, voire ne connaissent pas du tout le monde de la recherche dans ce domaine, et les opportunités existantes.



Continuant sur la lancée de la veille, la dernière journée a commencé par deux présentations en session plénière. Dans la première présentation, Duong Hieu Phan de Télécom Paris nous présentait l'utilisation de méthodes cryptographiques restant sûres dans des contextes particuliers, par exemple sous un régime

dictatorial, où l'on peut être forcé de révéler une clé secrète. Des constructions spécifiques permettent dans ce cas de dévoiler un message choisi spécifiquement, en lieu et place du message secret initial. Ensuite, c'est Clémentine Maurice du laboratoire CRIStAL de Lille qui nous a présenté de nouveaux moyens pour mener des attaques exploitant la microarchitecture des processeurs, notamment les mémoires caches, pour retrouver des données secrètes. En particulier, elle nous a montré comment du code JavaScript exécuté dans un navigateur web pouvait suffire à réaliser l'attaque, relaxant ainsi largement le modèle d'attaquant.

La matinée s'est poursuivie par une présentation des activités de l'ANSSI (agence nationale de la sécurité des systèmes d'information) par Geoffroy Hermann, suivie par la présentation par Thibauld Feneuil et Abdul Rahman Taleb de CryptoExperts de la messagerie CRY.ME. Cette dernière, à utiliser à des fins pédagogiques, a vu sa sécurité affaiblie par l'insertion volontaire de nombreuses failles cryptographiques. Il en existe une trentaine, à vous de les débusquer !

La dernière session de la matinée avait pour objet REDOCS (rencontre entreprises doctorants en sécurité). Après une brève présentation par Pascal Lafourcade, c'est Dylan Marinho de l'Université de Lorraine qui nous a présenté ce que son équipe a réalisé lors de l'édition précédente, sur le sujet de la détection de *ransomware*.

Pour conclure ces journées nationales, deux sessions se déroulaient en parallèle. L'une d'elles était commune aux groupes de travail MFS (méthodes formelles pour la sécurité) et SSLR (sécurité des systèmes, des logiciels et des réseaux), l'autre dédiée au groupe de travail SSM (sécurité des systèmes matériels). En assistant à la première, vous pouviez tout savoir sur le test et la vérification de protocoles, d'implémentations ou de systèmes. Dans la seconde, il était question de l'envers du décors concernant la génération de nombres aléatoires dans le matériel, nombres aléatoires qui sont indispensables à bon nombre de constructions cryptographiques.

Remercions encore une fois Adeline Roux-Langlois et Nicolas Porquet pour l'organisation de l'édition 2023 des journées nationales du GDR sécurité informatique. Si vous souhaitez retrouver les supports des présentations, ceux qui nous ont été fournis sont disponibles ici : https://gdr-securite.irisa.fr/ressources/ressources-journees-nationales-2023-slides/

Merci Brice pour ce retour, et rendez-vous du 10 au 12 juin 2024 pour la prochaine édition, qui se déroulera à Rennes !

Brice Colombier (Université Jean Monnet, LHC, Saint-Etienne), contact : b.colombier@univ-st-etienne.fr

Retour sur Cyber In Sophia Antipolis 2023

Badreddine Chah, Lucas Georget, Antonin Reitz et Liliana Rosero

Après les deux précédentes éditions à Toulouse et Nancy, c'était maintenant au tour de Sophia-Antipolis (Alpes-Maritimes) d'accueillir la 8ème école d'été du GDR SI qui s'est déroulée du 3 au 7 juillet dernier. Hébergés au Centre International de Valbonne, dans le Sud-Est de la France, les participants ont pu profiter de la proximité avec Antibes/Juan-les-Pins et Nice pour découvrir cette région fortement ensoleillée. Organisée par EURECOM, le GDR Sécurité Informatique et le projet REV du PEPR Cybersécurité (France 2030), le thème de cette année était donc en partie la recherche et l'exploitation de vulnérabilités. Les participants, de provenances diverses et variés, ont pu étudier de nombreux sujets au travers de cours et travaux pratiques.

Cinq keynotes ont structuré la semaine.

1) En ouverture, Davide Balzarotti (EURECOM) a présenté l'état de l'art des « *memory forensics* », qu'il a définis comme de la rétroingénierie poussée de l'état interne d'un système donné.

2) Le lendemain, Olivier Thomas (Texplained) a exposé ce qu'il est possible de faire en rétroingénierie de circuits intégrés, notamment par rapport à des contre-mesures comme la protection contre l'altération physique d'un élément sécurisé.

3) L'accent a ensuite été mis sur les protocoles de communication sans fils. Ainsi, Mathy Vanhoef (KU Leuven) a pu expliquer les idées principales des attaques récentes sur le protocole Wi-Fi, comme KRACK sur WPA2 ou l'attaque par canal auxiliaire Dragonblood sur WPA3. La suite de la présentation a permis d'aborder les protections comme l'authentification des caractéristiques annoncées par un réseau Wi-Fi pour éviter des attaques par négociation à la baisse (downgrade at-

tacks), intégrée à la norme Wi-Fi 7. Cette présentation était encadrée par un exposé sur la sécurité des réseaux Bluetooth par Daniele Antonioli ainsi qu'un exposé sur la sécurité des réseaux cellulaires de la 2G à la 5G par Adrian Dabrowski.

4) La *keynote* de Sébastien Bardin (CEA) a ensuite permis de détailler les avantages et les inconvénients de l'exécution symbolique, avant de présenter l'outil d'exécution symbolique de binaires BINSEC. Différents travaux reposant sur cet outil tendent à prouver la flexibilité de l'exécution symbolique, depuis l'élimination de faux positifs grâce à la notion d'atteignabilité robuste jusqu'à la détection d'attaques par canal auxiliaire, temporelle sur des primitives cryptographiques ou par exécution spéculative de manière plus générale.

5) Pour conclure la semaine, Daniel Gruss (Graz University of Technology) a présenté différentes attaques par canal auxiliaire, de Spectre, qui repose sur le mécanisme d'exécution spéculative de processeurs, à Rowhammer qui permet la modification du contenu de la RAM par des accès répétés à celle-ci.

L'ensemble des attaques présentées ont mené à l'intégration de contre-mesures, par exemple dans le noyau Linux, dont l'impact sur les performances est non négligeable. Face à ce constat, l'amélioration de contre-mesures existantes est possible, par exemple par le remplacement de l'usage de codes correcteurs d'erreurs dans la RAM ECC par l'usage de code d'authentication de message (CAM).

Nous avons eu l'occasion d'assister aux présentations suivies par des sessions pratiques, avec une forte interaction des participants. Cela nous a permis d'échanger des idées et concepts touchant à la fois la sécurité des systèmes de transmission avec notamment l'attaque KNOB (Key Negotiation of Bluetooth) sur le Bluetooth Low Energy ; la deuxième partie était en relation avec des méthodes formelles, avec la plateforme d'analyse de code binaire BINSEC. Nous avons conclu les travaux pratiques avec l'analyse par canaux auxiliaires, ce type d'analyse est une classe d'attaque qui utilise des informations physiques obtenues sur un système pour récupérer des éléments secrets.

Des conférences sont aussi venues agrémenter le programme sur les aspects légaux dans l'exploitation de vulnérabilités, la sécurité du Bluetooth et des réseaux cellulaires, le suivi en ligne et les empreintes des navigateurs, les différentes techniques de fuzzing, l'utilisation de l'injection de fautes électromagnétiques pour contourner le démarrage sécurisé du système sur puce, et enfin la génération automatique d'exploits pour noyaux.

L'école d'été ne se résumait pas uniquement à des cours magistraux et des travaux pratiques, mais elle offrait également des moments de détente et de socialisation. Nous avons pu participer à diverses activités qui ont contribué à rendre la semaine encore plus agréable. Chaque soir, nous avions accès à la piscine, permettant ainsi de se rafraîchir et de passer de bons moments entre chercheurs et doctorants. De plus, une demi-journée de détente nous a été accordée, au cours de laquelle nous avons pu profiter d'activités aquatiques telles que les "Bananes et Bouées Tractées". Une soirée festive a également été organisée, où nous avons partagé un cocktail et un dîner tous ensemble sur la plage.

Durant cet événement, nous avons eu l'opportunité, d'une part, de découvrir certains domaines de recherche en cybersécurité de la part de différents établissements en Europe, que ce soit sur les aspects offensifs, défensifs ou législatifs. Cette immersion nous a permis d'approfondir nos connaissances sur des sujets variés et de prendre conscience des enjeux actuels et futurs.

Les moments de détente et de convivialité ont joué un rôle crucial dans la création d'une atmosphère propice à l'échange et à la collaboration. Ces rencontres et ces échanges ont renforcé notre motivation à poursuivre nos efforts dans la recherche et ont ouvert des perspectives passionnantes pour des collaborations futures.

Merci pour ce retour, et rendez-vous pour l'édition 2024 à Bourges, du 15 au 19 juillet !

Badreddine Chah (UTBM), Lucas Georget (EDF R&D et LAAS-CNRS), Antonin Reitz (Inria Paris) et Liliana Rosero (Amadeus), contact : lgeorget@insa-toulouse.fr, Badreddine.chah@utbm.fr, antonin.reitz@inria.fr, liliana.rosero@polytechnique.edu

Retour sur les Journées C2

Marc Renard et Daphné Trama

La communauté codage et cryptographie (C2) s'est une nouvelle fois retrouvée à l'occasion des journées C2 2023. Ces dernières se tenaient cette fois-ci à Najac, près de Toulouse, du 15 au 20 octobre 2023.

Au programme, quatre conférences plénières passionnantes et didactiques (Gilles Zémor nous a parlé de codes quantiques, Alice Pellet-Mary de réseaux euclidiens, Christina Boura de cryptanalyse différentielle, et Damien Vergnaud de calcul distribué "in the head"), et plus de 70 exposés de doctorants (un nouveau record !). Ce ne sont pas moins de 170 membres de la communauté qui ont pu assister à de courtes présentations recouvrant une large diversité de sujets tels que les codes cycliques tordus, des signatures à base de codes, la cryptographie post-quantique à base de réseaux euclidiens, la cryptanalyse de différents cryptosystèmes symétriques comme asymétriques, l'intégrité des données, le chiffrement homomorphe, etc.

Entrelacés dans le programme scientifique, plusieurs temps forts ont été organisés par le comité égalité-parité, qui s'était constitué au sein du GT C2 en 2022 : session de sensibilisation, présentation et discussion autour d'une charte, et pauses café thématiques. Ces pauses ont permis de mettre en place des lieux de rencontre pour aborder en petit comité (mixte ou non) des sujets tels que le syndrome de l'imposteur ou la difficulté d'être chercheuse dans un milieu majoritairement masculin. Ces pauses thématiques ont rencontré un franc succès, et ces dernières se sont quelques fois révélées trop courtes au goût de nombreux participants.

La charte s'adresse quant à elle aux organisateurs et organisatrices d'événements scientifiques et vise avant tout à les soutenir en les aidant à ne pas oublier certains points essentiels au bien-être de tous et toutes. Accompagnée d'un « code de conduite », elle a été relue, discutée et améliorée puis a reçu un vote de soutien lors de l'AG. La version finale sera prochainement disponible.

Nous avons également eu l'occasion d'échanger autour d'une table ronde (topologiquement parlant) sur des sujets d'actualité, comme les lois à venir à propos de la protection des données personnelles en France. Et la traditionnelle AG du GT C2 a été l'occasion de discuter de moults sujets importants pour la communauté.

La conférence s'est déroulée dans une ambiance chaleureuse, sérieuse et bienveillante, le tout sur fond de coupe du monde de rugby. La météo n'a pas forcément été de notre côté, mais les commodités sur place telle que la piscine chauffée ou le sauna ont largement compensé. Et l'équipe des organisateurs était au top !

Marc Renard et Daphné Trama (CEA et Université Paris-Saclay), contact : marc.renard@cea.fr, daphne.trama@cea.fr

Retour sur REDOCS 2023

Antoine Mallet

Réalisant une thèse académique, j'ai apprécié le changement de paradigme offert par REDOCS, où il s'agit d'apporter des réponses à des problèmes issus de l'industrie. Nous étions quatorze participants cette année. Une ambiance très amicale a régné toute la semaine, aux repas communs, pauses-goûter et sorties en plein air. Travailler avec des collègues de disciplines connexes a été une vraie chance. Toute la semaine, les idées originales se sont succédées, mêlant pragmatisme et originalité. Nous avons gardé cette dynamique jusqu'au vendredi matin, où, devant les entreprises, les autres participants ainsi qu'un groupe d'étudiants en master, nous avons présenté notre travail . Fignolées jusqu'à tard la veille (ou, pour être honnête, tôt le matin-même, nous nous sommes dit "à tout à l'heure !" au moment de rejoindre nos chambres), les présentations des trois groupes ont été une franche réussite.

La semaine s'est déroulée dans un cadre de travail exceptionnel. La qualité de l'accueil, tant humainement que sur le plan matériel, nous a tous enthousiasmés, et nous a naturellement encouragés dans nos efforts. Mais, au-delà du CIRM, le cadre naturel est aussi à souligner. A la moitié de la semaine, une petite sortie,franchement bienvenue, nous a permis de réaliser le trésor naturel dans lequel nous nous trouvions. En effet, en une demi-heure de marche, nous montions sur un belvédère offrant une vue magnifique sur les calanques, Marseille, le mont Puget et la Méditerranée. La semaine s'est terminée sur un quartier libre le vendredi après-midi. L'occasion pour certains de se reposer, autour de jeux de société. Pour d'autres, d'explorer d'avantage la nature alentour, en grimpant au mont Puget, ou en descendant à la calanque de Sugiton poser les pieds dans l'eau.

En conclusion, j'encourage les doctorantes et les doctorants à participer aux prochaines éditions de REDOCS. C'est une très belle expérience, que peu d'autres métiers peuvent offrir.

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/

1 poste PR et 2 postes MCF, IUT de Vannes / IRISA (Vannes + Rennes)

PR : profil système/réseau/cybersécurité
2 MCF : profil systèmes/réseaux/sécurité, intelligence artificielle
Nicolas Le Sommer,
nicolas.le-sommer@univ-ubs.fr

2 postes d'enseignants-chercheurs, Ecole de l'Air et de l'Espace, Salon de (Provence)

1 poste Cybersécurité + 1 poste IA
Olivier Bartheye,
olivier.bartheye@ecole-air.fr
Jérémy Buisson, jeremy.buisson@ecole-air.fr

Poste PR (section 27), Polytech Grenoble-INP / Verimag (Grenoble)

Profil : système, architectures logicielles et matérielles, sécurité, réseaux
David Monniaux
david.monniaux@univ-grenoble-alpes.fr

2 postes d'ingénieurs, Lab-STICC (Lorient)

Profil : sécurité des systèmes IoT et des systèmes sur puce
Durée : 2 ans
Vianney Lapôtre, vianney.lapotre@univ-ubs.fr

Poste MCF, ENSSAT / IRISA (Lannion + Rennes)
Profil : sécurité des réseaux
Damien Lolive, damien.lolive@irisa.fr
François Goasdoué, fg@irisa.fr

Poste PR IMT, IMT Atlantique / IRISA (Rennes)
Profil : cybersécurité
Date limite de candidature : 31 mars
Géraldine Texier,
geraldine.texier@imt-atlantique.fr
Romaric Ludinard,
romaric.ludinard@imt-atlantique.fr
Guillaume Doyen,
guillaume.doyen@imt-atlantique.fr

1 poste PR et 2 postes MCF, Université Clermont Auvergne / LIMOS (Clermont-Ferrand)
PR Clermont Auvergne INP / ISIMA, 46-1 27e section : optimisation combinatoire et recherche opérationnelle ou gestion de données et intelligence artificielle
MCF IUT Clermont Auvergne, 26-1 27e section : données, base de données, apprentissage artificiel
MCF Clermont Auvergne INP / ISIMA, 26-1 27e section : sécurité informatique, cyber sécurité
Pascal Lafourcade, pascal.lafourcade@uca.fr

Poste MCF section 27/61, IUT du Limousin / XLIM (Limoges)
Enseignement : Hébergement et services web/ Dev ops/ Sécurité de l'information et des applications web. Développement web
Recherche : Sécurité des systèmes et réseaux / Cryptographie / Cybersécurité / Intelligence Artificielle
Emmanuel Conchon,
emmanuel.conchon@unilim.fr

Poste MCF IMT, Télécom SudParis (Evry, Palaiseau)
Profil : réseaux et cloud
Date limite de candidature : 20 mars
Maryline Laurent,
maryline.laurent@telecom-sudparis.eu
Vincent Gauthier,
vincent.gauthier@telecom-sudparis.eu

Poste Chaire Professeur Junior, Télécom SudParis (Palaiseau)
Profil : cybersécurité (cyber responsable)
Date limite de candidature : 7 mars
Maryline Laurent,
maryline.laurent@telecom-sudparis.eu

Postes MCF, INSA Toulouse / LAAS (Toulouse)
Profil : cybersécurité (section 27)
Pierre Lopez, pierre.lopez@laas.fr

7 PR et 15 MCF, IRISA (Rennes)
Dont une bonne part avec des profils liés à la sécurité : https://www.irisa.fr/campagne-emploi-2024-postes-mcfpr
voir les contacts sur les fiches de postes

Poste MCF IMT, IMT Atlantique / Lab-STICC (Brest)
Profil : génie logiciel (lien cybersécurité souhaité)
Date limite de candidature : 31 mars
Fabien Dagnat,
fabien.dagnat@imt-atlantique.fr

2 postes PR et 7 postes MCF, Université de Lorraine / LORIA (Nancy, Metz,)
Dont plusieurs avec des profils liés à la sécurité : https://www.loria.fr/fr/emplois/
voir les contacts sur les fiches de postes

3 postes d'enseignants-chercheurs, ESIEE (Paris)
Profils : informatique,
informatique orientée transition environnementale, data et applications
Laurent Perroton, laurent.perroton@esiee.fr

2 postes MCF, Sorbonne Université / LIP6 (Paris)
Profils : conception et analyse d'algorithmes, Systèmes embarqués et systèmes sur puce
Antoine Miné, antoine.mine@lip6.fr

Poste de PR ou MCF Ecole Polytechnique (Palaiseau)
Profil : cybersécurité
Olivier Blazy, olivier.blazy@polytechnique.edu

Poste MCF, IUT Grand Ouest Normandie (Caen)
Profil : biométrie, architecture et modèles de sécurité, et sciences de l'investigation (Forensique)
Christophe Charrier,
christophe.charrier@unicaen.fr

Stage 6 mois, Télécom SudParis (Palaiseau)
Sujet : implémentation (en partie) d'un framework d'évaluation pilotée par les données pour améliorer la qualité des détecteurs d'intrusion réseau
Grégory Blanc,
gregory.blanc@telecom-sudparis.eu

Stage 6 mois, Thales Digital Identity & Security (Meudon)

Sujet : développement logiciel
Adel Djoudi, djoudiadel@gmail.com

2 stages recherche, laboratoire ERIC (Lyon)

Premier stage : dans le cadre du projet ANR BI4People sur le calcul multipartite sécurisé
Deuxième stage : dans le cadre du projet FIL sur l'apprentissage basé sur les graphes de connaissances de vulnérabilités dynamiques et des connaissances organisationnelles d'une entreprise pour renforcer la cybersécurité.
Mohamed-Lamine Messai,
mohamed-lamine.messai@univ-lyon2.fr

Thèse de doctorat, Télécom SudParis (Palaiseau)

Sujet : Génération de graphes de causalité (projet PEPR Superviz)
Eric Totel, eric.totel@telecom-dusparis.eu

Postdoc, Télécom SudParis (Palaiseau)

Sujet : Génération de données de test par la transformation de trafic
Durée : 2 ans
Grégory Blanc,
gregory.blanc@telecom-sudparis.eu

2 stages de recherche, Télécom Paris (Palaiseau)

Sujet : attaques par canaux auxiliaires
Julien Béguinot,
julien.beguinot@telecom-paris.fr

Thèse de doctorat, Mines Saint-Etienne, Campus Provence (Gardanne)

Sujet : Simulating and Modelling the Effects of Thermal Laser Stimulation on Integrated Circuits
Jean-Baptiste Rigaud, rigaud@emse.fr
Raphael Viera, raphael.viera@emse.fr

Thèse de doctorat et éventuellement stage M2, CEA List (Saclay)

Sujet : Guidage astucieux des outils de génération de tests
Michaël Marcozzi , michael.marcozzi@gmail.com

Postdoc, Orange (Cesson-Sévigné)

Sujet : implémentation et l'analyse des protocoles d'attestation
Durée : 1 à 3 ans
Ghada Arfaoui, ghada.arfaoui@orange.com

Postdoc, Mines Saint-Etienne

Sujet : chiffrement de bout en bout dans les réseaux 5G multi-tenants (dans le cadre du projet NF_HiSec du PEPR 5G)
Durée : 2 ans et 3 mois
Philippe Jaillon, philippe.jaillon@emse.fr