Juin 2022
Numéro 12

LA GAZETTE DU GDR

Sécurité Informatique - GDR2046

Édito de la directrice

Ce nouveau numéro paraît à la veille des journées nationales, qui se déroulent cette année du 22 au 24 juin au Campus Cyber de La Défense. Vous y retrouverez les habituelles keynotes et conférences plénières, des sessions des groupes de travail, un exposé du prix de thèse, la traditionnelle présentation de REDOCS, l'AG du GDR qui sera l'occasion d'échanger autour de la structuration et du fonctionnement du GDR, mais aussi cette année deux nouvelles sessions concernant les carrières et le club des partenaires.

Ce numéro de juin est l'occasion de féliciter et d'interviewer Véronique Cortier, spécialiste des preuves formelles de sécurité des protocoles cryptographiques, notamment dans le domaine du vote électronique, qui reçoit cette année la médaille d'argent du CNRS. Comme l'ont déjà souligné beaucoup de collègues, c'est une consécration pour des travaux scientifiques de pointe et un engagement dans un domaine lié à des enjeux de société qui prennent beaucoup d'ampleur depuis plusieurs mois, à la jonction des GDR IM et Sécurité.

Nous interviewons et félicitons également André Schrottenloher, lauréat du prix de thèse, qui nous fait découvrir ses travaux sur la cryptanalyse quantique des algorithmes de chiffrement symétriques.

La tournée des laboratoires nous amène cette fois-ci à Lille, pour découvrir les activités en cybersécurité du laboratoire CRIStAL. Passage du côté de Lille également pour un retour sur l'édition 2022 du FIC, qui s'y est déroulé du 7 au 9 juin.

Ce printemps a permis à plusieurs groupes de travail de se retrouver lors d'évènements longs et appréciés, tels les journées MFS qui se sont déroulées pour la première fois sur plusieurs jours à Fréjus en mars, les journées C2 qui se sont tenues à Hendaye en avril, RESSI qui a profité du grand air de Chambon-sur-Lac en mai, et APVP qui vient tout juste d'avoir lieu la semaine dernière à Châtenay-sur-Seine. Les trois premiers vous sont présentés dans ce numéro par des participants. APVP sera présenté dans le prochain numéro, à la rentrée.

Bonne lecture à toutes et à tous !

Caroline Fontaine,
Directrice du GDR Sécurité Informatique

Rubriques

Événements

(Repris en partie du forum du GDR)

Role and effects of ARTificial Intelligence in Secure ApplicatioNs (ARTISAN Summer School 2022), *Valence, France, 4-7 juillet 2022*

2nd International Workshop on Multi-concern Assurance Practices in Software Design (MAPSOD 2022), *co-organisé avec SAFECOMP 2022, Munich, Allemagne, 6 septembre 2022*

2nd International Workshop on Designing and Measuring Security in Software Architecture (DeMeSSA 2022), *Prague, République Tchèque, 19-20 septembre 2022*

Privacy in Statistical Databases 2022 (PSD 2022), *Paris, France, 21-23 septembre 2022*

11th International Workshop on Security Proofs for Embedded Systems (PROOFS 2022), *co-organisé avec CHES 2022, Louvain, Belgique, 22 septembre 2022*

17th International Workshop on Data Privacy Management (DPM 2022), *Copenhague, Danemark, 26 septembre 2022*

IEEE Conference on Communications and Network Security (CNS 2022), *Austin, Texas, États-Unis (en hybride), 26-28 septembre 2022*

21th International Conference on Cyberworlds (CW 2022), *Kanazawa, Japon, 27-29 septembre 2022*

DevOps at Models Workshop (DevOps@MODELS 2022), *23-25 octobre*

Le coin prospectif

Véronique Cortier

La gazette interviewe Véronique Cortier, directrice de recherche CNRS au LORIA et lauréate 2022 de la médaille d'argent du CNRS. Véronique travaille sur la sécurité des protocoles de communication et leur fiabilité. Elle nous parle de son domaine de recherche qui concerne plus particulièrement le vote électronique et des applications de sécurité pour le milieu bancaire.

Bonjour Véronique, tout d'abord félicitations pour la médaille d'argent décernée par le CNRS ! Peux-tu présenter rapidement tes activités, en particulier celles qui ont conduit à l'obtention de ce prix prestigieux ?

Depuis ma thèse, je m'intéresse à la sécurité des protocoles cryptographiques. Plus précisément, je cherche à *prouver* leur sécurité, le plus automatiquement possible. Il s'agit donc de concevoir des algorithmes qui analysent les protocoles, trouvent potentiellement des failles, ou bien apportent la garantie que le protocole est sûr, du moins dans le modèle considéré. Une difficulté particulière est qu'il faut considérer un attaquant arbitraire, qui peut intercepter n'importe quel message, le modifier et le renvoyer. Un de mes sujets de prédilection ces dix dernières années est l'étude des protocoles de vote électronique et ce sont mes travaux sur ce sujet qui ont été récompensés.

Véronique Cortier

Quelles sont les propriétés sur lesquelles repose le vote électronique ?

Le vote électronique et, en fait, le vote en général, repose sur deux propriétés essentielles. Le secret du vote d'une part : nul ne doit savoir comment j'ai voté. D'autre part, le système de vote doit être vérifiable : un électeur doit pouvoir s'assurer que son vote a bien été compté et que le résultat ne prend en compte que des électeurs légitimes, et cela sans avoir à faire confiance au programme qui tourne sur le serveur qui collecte les votes. D'autres propriétés sont souhaitables dans des contextes à fort enjeu comme la résistance à l'achat de vote ou bien la redevabilité, une notion plus récemment formalisée. Il faut non seulement que le système soit vérifiable mais qu'on sache identifier les responsables lorsqu'un comportement anormal est détecté.

À vrai dire, identifier et formaliser les bonnes propriétés d'un système de vote électronique est une tâche difficile et encore en cours. De façon surprenante, même une propriété fondamentale comme le secret du vote représente un véritable défi de modélisation.

Quels principes cryptographiques sont mobilisés pour assurer le respect de ces propriétés ?

Le vote électronique utilise une large palette de la boîte à outils offerte par la cryptographie. Les systèmes de vote font appel aux primitives classiques comme les chiffrements symétrique et asymétrique, la signature et les fonctions de hachage, mais reposent aussi beaucoup sur les preuves à divulgation nulle de connaissance, qui permettent par exemple de s'assurer que les autorités de déchiffrement ne trichent pas quand elles dépouillent l'urne. Suivant le système considéré, des primitives plus spécialisées peuvent être utilisées comme le chiffrement homomorphe, les signatures en aveugle, le transfert inconscient, ou encore les tests d'égalité de plaintext (PET).

> « Même une propriété fondamentale comme le secret du vote représente un véritable défi de modélisation. »

Peux-tu nous en dire plus sur le système Belenios que vous avez développé ?

Avec Stéphane Glondu et Pierrick Gaudry, nous développons et maintenons le système de vote Belenios. L'objectif est de proposer un moyen relativement simple pour voter, tout en préservant le secret du vote et en proposant un système vérifiable. Concrètement, les électeurs votent en se connectant à la page web de l'élection. Leur vote est chiffré par leur navigateur puis est envoyé au serveur de vote. Pour éviter le bourrage d'urne, non seulement les électeurs doivent s'authentifier auprès du serveur mais également signer leur bulletin chiffré à l'aide d'un code de vote reçu par mail. Ainsi, même si le serveur de vote est corrompu, il ne peut pas ajouter de bulletin valide. Comme le chiffrement utilisé est homomorphe, les bulletins peuvent être combinés pour obtenir un bulletin qui contient le résultat de l'élection. C'est uniquement ce bulletin qui est déchiffré par les autorités. Les autorités prouvent que leur déchiffrement est correct à l'aide d'une preuve à divulgation nulle de connaissance. Ainsi, les électeurs peuvent vérifier que leur bulletin est dans l'urne publique (concrètement, une page web) et vérifier tous les calculs, sans avoir la clé. Soyons

pragmatiques, même les lecteurs de cette gazette ne vont probablement pas tous développer leur propre logiciel de vérification de preuves cryptographiques. Mais il suffit que quelques observateurs indépendants le fassent pour assurer l'intégrité du scrutin.

Belenios est un logiciel open-source et nous proposons une plateforme de vote en ligne, libre et gratuite. Elle est utilisée chaque année pour organiser environ 1400 élections. À ce jour, nous avons traité plus de 100 000 bulletins. Cela ne compte pas les élections organisées à l'aide de Belenios sur des serveurs indépendants du nôtre. Nos utilisateurs ont des profils variés : de nombreux conseils du monde académique bien sûr, mais également beaucoup d'associations ou encore la cour des comptes européenne ou un parti politique allemand.

Selon toi, quels sont les défis à relever dans ce domaine ?

Il y a encore beaucoup à faire, sur tous les fronts ! Tout d'abord, aucun système de vote électronique n'apporte la même sécurité qu'un vote à l'urne bien organisé. Les pistes d'amélioration sont nombreuses. Ainsi l'authentification de l'électeur reste un véritable écueil. Tant que l'électeur recevra des codes de vote ou des mots de passe par mail ou SMS, il lui sera facile de les vendre ou de se les faire voler à son insu, s'il ne vote pas. En outre, si on considère Belenios, il s'agit d'un système vérifiable mais à condition de faire confiance à l'ordinateur de l'électeur. Un ordinateur corrompu peut apprendre le vote de l'électeur mais aussi le modifier, et chiffrer "A" alors que l'électeur a sélectionné le candidat "B". La propriété manquante ici est la vérifiabilité de l'intention : l'électeur doit pouvoir s'assurer que son intention de vote a bien été prise en compte dans son bulletin, même si son ordinateur est malveillant.

Enfin, une fois un protocole conçu, il faut analyser sa sécurité. Et donc modéliser les propriétés de sécurité souhaitées et concevoir des techniques d'analyse pour effectuer les preuves, souvent trop complexes, avec trop de cas, pour être effectuées à la main. Deux tâches également difficiles !

Dans un livre co-écrit avec Pierrick Gaudry, paru aux éditions Odile Jacob, nous revenons sur les défis du vote électronique, les propriétés souhaitées, ce que l'on sait faire et tout ce qu'il reste encore à étudier.

Quels conseils peux-tu donner aux jeunes chercheurs intéressés par la sécurité des protocoles de communication ?

Contrairement à nos enseignants de lycée qui nous répétaient souvent qu'il fallait beaucoup travailler, mon principal conseil est qu'il faut s'amuser ! Se laisser guider par sa curiosité, les sujets que l'on trouve intrigants, étonnants et surtout amusants. Bon, il faut aussi un peu travailler... Il est également conseillé de se trouver des partenaires de jeux, c'est-à-dire des collègues avec qui l'on s'entend bien et qui apportent des compétences complémentaires. L'une de mes plus anciennes collaborations vient du fait que je ne croyais pas du tout à un résultat obtenu par un chercheur, Bogdan Warinschi, rencontré lors d'une visite dans un laboratoire américain. À force de lui présenter des contre-exemples (faux), nous avons largement étendu son approche, qui s'est révélée tout à fait correcte.

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

Article rédigé par Véronique Cortier (LORIA, CNRS), Céline Chevalier et Pauline Puteaux, contact : veronique.cortier@loria.fr

Retour sur les journées Codage et Cryptographie 2022

Olivier Blazy, Alain Couvreur

Pour la première fois depuis plus de 3 ans, la communauté codage et cryptographie (C2) a pu se réunir en présentiel. Les journées C2 se sont tenues dans un village de vacances à Hendaye du 10 au 15 avril 2022.

Depuis plus de 20 ans, les journées C2 sont l'événement structurant du groupe de travail C2 commun aux GDR Sécurité Informatique et Informatique Mathématique. Cette conférence qui a lieu tous les 18 mois a pour but de permettre à tous les jeunes de la communauté française de codage et cryptographie de présenter leurs travaux et ainsi de se faire connaître.

Pour cette édition 2022, les organisateurs, Gaëtan Leurent et Léo Perrin (Centre de recherche Inria de Paris, Équipe Cosmiq) ont choisi d'emmener leur commu-

nauté sur les plages du Pays Basque à quelques kilomètres de la frontière espagnole. Difficile de savoir si c'est le choix du lieu ou la seule envie de pouvoir enfin participer à un événement en présentiel après deux années de conférences en ligne, mais une chose est sûre : l'événement a été un franc succès, réunissant plus de 130 participants dont plus des deux tiers étaient des doctorants et post-doctorants. Au programme, 5 conférences plénières et plus de 60 exposés courts de jeunes chercheurs couvrant un large spectre : théorie algorithmique des nombres, codage algébrique, algorithmique quantique, cryptographie symétrique, cryptographie à clé publique classique comme post-quantique, attaques par canaux auxiliaires ou encore protocoles avancés. Le comité de programme a également souhaité une ouverture thématique en donnant de la visibilité aux travaux de Benjamin Grégoire (Centre Inria de Sophia Antipolis, Équipe Marelle) qui a proposé une conférence plénière entre cryptographie et preuves formelles dans laquelle il a présenté un assistant de preuve, *EasyCrypt*, spécialement conçu pour la cryptographie.

La conférence, qui a duré une semaine, s'est déroulée dans une ambiance sérieuse mais plutôt détendue. Elle a surtout été l'occasion pour beaucoup de doctorants de découvrir enfin les conférences en présentiel et les échanges informels qui sont si difficiles à mettre en place dans un événement à distance. Les prochaines journées devraient avoir lieu dans 18 mois, et être organisées par des membres du pôle toulousain.

Pour plus de détails : https://jc2-2022.inria.fr/fr/invited-speakers/

Olivier Blazy, Alain Couvreur, contact : olivier.blazy@polytechnique.edu, alain.couvreur@inria.fr

Brèves

- Les Journées Nationales du GDR se tiennent du 22 au 24 juin, au Campus Cyber de la Défense.
- La Summer School du GDR aura lieu à Nancy du 4 au 8 juillet, organisée par Virginie Lallemand et Lucca Hirschi. Toutes les places ont été prises en quelques jours, et il y a une liste d'attente en cas de désistements.
- Les inscriptions pour REDOCS 2022 sont ouvertes : https://gdr-securite.irisa.fr/redocs22/. Les sujets seront annoncés aux JN.
- Le prix de thèse 2022 du GDR a été attribué à André Schrottenloher, pour sa thèse «Quantum Algorithms for Cryptanalysis and Quantum-safe Symmetric Cryptography», sous la direction de María Naya-Plasencia et André Chailloux.

Le jury a également souhaité lister une accessit : Lesly-Ann Daniel, pour sa thèse «Symbolic Binary-Level Code Analysis for Security».

Un grand bravo à eux, ainsi qu'à l'ensemble des candidats. Si vous souhaitez en savoir plus sur le prix de thèse : https://gdr-securite.irisa.fr/prix-de-these/.

- Véronique Cortier fait partie des lauréats 2022 des médailles du CNRS et reçoit la médaille d'argent, un grand bravo à elle ! Nous en profitons pour annoncer la parution du livre qu'elle a écrit avec Pierrick Gaudry, intitulé *Le Vote électronique* (et sous-titré *Les défis du secret et de la transparence*), qui vient de paraître fin mai aux éditions Odile Jacob.

Retour sur RESSI 2022

Vincent Nicomette

L'edition 2022 de RESSI s'est donc déroulée en présentiel à Chambon-sur-Lac, à coté de Clermont Ferrand. Organisée de main de maître par Pascal Lafourcade, dans un camping au bord du lac de Chambon, cette édition a tenu toutes ses promesses : sessions de rejeu de papiers et de thèses, keynotes, sessions projets, sessions enseignement, sessions doctorants accompagnées de posters, l'ensemble du programme ayant été concocté par Cédric Eichler et Benjamin Nguyen.

RESSI est avant tout un lieu d'échange où la communauté sécurité a le plaisir de se retrouver et d'échanger sur divers sujets. Et, de ce point de vue, le but a été parfaitement atteint, les échanges ont été riches et les participants visiblement heureux de se retrouver. On a d'ailleurs atteint cette année un record d'affluence de 90 personnes, dont beaucoup de jeunes doctorants, ce qui est tout à fait remarquable. À noter également une présentation du PEPR Cybersécurité par Gildas Avoine pour conclure l'édition, dans lequel beaucoup de participants à RESSI sont impliqués. En bref, une édition riche scientifiquement et toujours dans un bel esprit. Vivement 2023 !

Vincent Nicomette, contact : vincent.nicomette@laas.fr

Retour sur les journées MFS

Élise Klein, Maïwenn Racouchot

Les journées du GT MFS (Groupe de Travail sur les Méthodes Formelles pour la sécurité) sont plusieurs journées de workshop destinées à rassembler les membres de la communauté scientifique (principalement française) des méthodes formelles. Elles étaient organisées autour des axes suivants : la vérification de protocoles, l'implémentation des primitives cryptographiques, l'analyse statique, la vérification de programme, la sécurité des réseaux, la compilation préservant la propriété de temps constant et la vérification dans le modèle calculatoire. Pour cette édition, organisée par Jannik Dreier et Sébastien Bardin, elles se sont déroulées sous un format de trois jours à Fréjus, du 20 au 23 mars 2022.

Au programme de cette année, des *keynotes* sur des sujets clés des méthodes formelles, un panel de présentations par les participants de leurs récents travaux, une session de présentation des outils du domaine et de nombreuses occasions de rencontrer et de discuter avec les autres chercheurs et doctorants. La diversité des personnes présentes, bien que partageant toutes un domaine de recherche, nous a permis de nous ouvrir aux différents versants des méthodes formelles et de gagner ainsi une meilleure vision sur leurs applications possibles.

Le *social event* de cette édition était une randonnée découverte dans le massif de l'Esterel qui nous a permis de découvrir la montagne, avant de finir sur un pique-nique sur la plage afin de profiter du soleil et de discuter. Même les quelques coups de soleil récoltés par les moins habitués à ce temps radieux, et la température relativement fraîche de la Méditerranée en mars, n'ont pas pu ternir la bonne humeur générale.

Et pour finir, quelques citations de participants :

- *« Le lieu était super bien. L'organisation était bien faite et les conférences intéressantes. La promenade était très sympathique et permettait de profiter de l'endroit tout en faisant une pause et permettant de parler en dehors des conférences. »* Un étudiant comblé.
- *« Bien que j'étais nerveuse pour ma première présentation, ces journées se sont très bien passées ! J'ai appris plein de choses et rencontré plein de gens intéressants. Je me rends encore mieux compte à présent de tout ce qu'il me reste à apprendre. Trop hâte de retourner à la prochaine édition ! »* Une étudiante pleine de projets.
- *« Participer au GT MFS m'a permis, pour la première fois, de présenter un travail devant des experts des méthodes formelles. Je trouve cela assez extraordinaire, surtout quand ces mêmes personnes viennent vous féliciter et en apprendre plus sur ce que vous avez fait. C'est gratifiant et dépaysant, surtout sous un soleil aussi radieux que celui de Fréjus. »* Une étudiante ayant besoin de soleil.
- *« Douliou douliou douliou, Saint Tropez ! »* Un lanceur de chants mélomane.
- *« Un grand bravo pour cette première édition longue, et la mise en place de la session outils qui a permis de découvrir les logiciels et de discuter avec leurs développeurs. »* Une participante avide de découvertes.

Élise Klein, Maïwenn Racouchot, contact : elise.klein@inria.fr, maiwenn.racouchot@inria.fr

Retour sur le FIC 2022

Caroline Fontaine

Le Forum International de la Cybersécurité, organisé habituellement tous les ans à Lille au mois de janvier s'est un peu décalé avec la pandémie. La dernière édition avait eu lieu en septembre 2021 (voir la gazette numéro 10) et l'édition 2022 s'est tenue les 7-8-9 juin. 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 cybersécurité ; 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, IMT, CDEFI), a encore pris de l'ampleur. Il était doté cette année d'un véritable espace de Master Class dédié, partagé entre les 18 exposés proposés par Allistène et d'autres, orientés SHS. Les 18 exposés Allistène ont permis de couvrir des thématiques très variées touchant les diverses thé-

matiques des GT du GDR. Le public était nombreux, débordant très souvent de l'espace qui nous était alloué, et les discussions qui ont suivi les exposés se sont révélées 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 Caroline Fontaine (directrice du GDR) ainsi qu'Olivier Blazy (co-responsable du GT C2), Jean-Yves Marion (président du conseil scientifique du GDR) et le soutien du staff CNRS : Estelle Hutschka (chargée de communication INS2I), Mandack Gueye (responsable de la valorisation), et Nicolas Porquet (responsable des relations entreprises de la DRE pour le secteur de la cybersécurité).

L'ambiance de l'ensemble de l'« espace recherche » était collégiale et la mutualisation de l'espace de discussion, de la scène et du programme des Master Class vraiment agréable, 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 et que je n'ai pas cités nommément, en particulier les collègues qui ont présenté leurs travaux sur scène, quelle que soit leur tutelle, car les exposés étaient passionnants ! Rendez-vous lors du prochain FIC prévu les 5-6-7 avril 2023 !

Programme et vidéos des Master Class du FIC

Vous trouverez la liste des 18 Master Class organisées par Allistène ici : https://www.inria.fr/sites/default/files/2022-06/Programme_FIC_2022_fran%C3%A7ais.pdf. Les exposés ont a priori été filmés et seront mis en ligne sur le site du FIC, mais en attendant vous pouvez regarder les entretiens proposés par l'INS2I et réalisés avant le salon avec une partie des intervenants :

- Adeline Roux-Langlois (CNRS, IRISA), sur la cryptographie post-quantique : https://www.youtube.com/watch?v=tczEalq_kt4 ;
- Vincent Nicomette et Romain Cayre (INSA Toulouse et Apsys Lab, LAAS), sur la sécurité des protocoles de l'IoT, notamment BLE : https://www.youtube.com/watch?v=d5_dhrKTf8s ;
- Brahim Hamid (Université Toulouse Jean-Jaurès, IRIT), sur le développement d'architectures sécurisées : https://www.youtube.com/watch?v=P5nhe1OsRgM ;
- Arsenia Chorti (ETIS), sur le rôle de la couche physique dans la sécurité de la 6G : https://www.youtube.com/watch?v=5loyWTwo1eY ;
- Vlad Nitu (CNRS, LIRIS), sur les attaques et protections dans l'apprentissage fédéré : https://www.youtube.com/watch?v=MIZbG5G6u5Q) ;
- Estelle Cherrier (ENSICAEN, GREYC), sur l'authentification biométrique et le respect de la vie privée https://www.youtube.com/watch?v=yNqJGxlJMOs ;
- Pierre Laperdrix (CNRS, CRIStAL), sur le traçage par empreintes de navigateur https://www.youtube.com/watch?v=9m9m6ol5pQc.

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

Le coin prospectif

André Schrottenloher

La gazette interviewe André Schrottenloher, lauréat du Prix de thèse du GDR en 2022, pour sa thèse intitulée « Quantum Algorithms for Cryptanalysis and Quantum-safe Symmetric Cryptography » qui a été effectuée sous la direction de María Naya-Plasencia et d'André Chailloux. André est actuellement en postdoc au CWI à Amsterdam, avec Marc Stevens. Il s'intéresse particulièrement au développement d'algorithmes quantiques pour la cryptanalyse symétrique.

Bonjour André, félicitations pour ton prix ! Peux-tu nous en dire un peu plus sur les principales contributions de ta thèse ?

Merci ! La cryptanalyse est essentielle pour assurer la sécurité des outils cryptographiques : on développe des attaques de plus en plus perfectionnées et on s'assure qu'on utilise des cryptosystèmes qui y sont résistants. Mais qu'en est-il contre un adversaire équipé d'un ordinateur quantique ? En cryptographie à clé publique, on connaît bien l'algorithme de Shor, qui permettrait par exemple de casser le cryptosystème RSA. Mais en cryptographie symétrique, à clé secrète, la question a été tout simplement moins étudiée. L'objectif de ma thèse était donc de développer des algorithmes quantiques pour la cryptanalyse symétrique, afin d'estimer de manière plus précise ce qui reste sûr contre un futur attaquant quantique, et à quel point. Ce sont d'une part des algorithmes « génériques » où l'on abstrait l'algorithme attaqué sous forme de boîte noire, d'autre part des cryptanalyses « concrètes » d'algorithmes précis.

> « L'algorithme de Shor montre bien qu'il existe des attaques sans équivalents classiques, qui ne peuvent pas être vues comme de simples "accélérations". »

Quelles sont les grandes différences entre cryptanalyse classique et quantique ?

Beaucoup de techniques développées en cryptanalyse classique peuvent être réemployées pour des attaques quantiques. C'est vrai à la fois pour des algorithmes génériques et des attaques concrètes, par exemple contre des versions réduites du standard de chiffrement AES. En fait, dès qu'on peut traduire un problème sous forme de recherche, on peut bénéficier d'une accélération offerte par le célèbre algorithme de Grover. Cela vaut par exemple pour la recherche exhaustive des clés secrètes. Il y a donc une réduction de la sécurité des algorithmes symétriques, mais qui est encore tout à fait maîtrisable.

En revanche, l'algorithme de Shor montre bien qu'il existe des attaques sans équivalents classiques, qui ne peuvent pas être vues comme de simples « accélérations ». Elles ont fait leur apparition plus récemment en cryptographie symétrique, en utilisant l'algorithme de Simon, un prototype de celui de Shor, qui était encore assez peu connu. Sans représenter une menace aussi significative, ces attaques défient encore notre intuition.

Tu poursuis actuellement tes travaux au Centrum Wiskunde & Informatica (CWI) à Amsterdam, avec Marc Stevens. Quels sont les objectifs que tu vises actuellement en matière de recherche ?

Au CWI, j'ai commencé à travailler sur des outils automatiques de recherche d'attaques. C'est un principe de plus en plus répandu en cryptanalyse symétrique. On arrive à modéliser une famille d'attaques comme un espace de recherche ; trouver la meilleure attaque de cette famille devient un problème d'optimisation sous contraintes, qu'on peut résoudre de manière automatique. Je pense que ces outils ont beaucoup de potentiel pour la recherche et l'optimisation d'attaques quantiques, et c'est une de mes priorités. Par ailleurs, je me suis beaucoup penché ces derniers temps sur la cryptanalyse des fonctions de hachage, qui interviennent notamment dans certains schémas de signatures post-quantiques.

André Schrottenloher

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

Rien de très original, je le crains. Pour commencer, un conseil que je ferais bien de suivre moi-même : s'organiser. La thèse est une expérience passionnante, mais très énergivore, qui implique souvent de mener plusieurs projets en parallèle, et où l'on passe des journées entières à sauter d'une tâche à l'autre. Malheureusement, je n'ai pas de solution miraculeuse, puisque c'est justement ce qui m'a paru le plus difficile (et pour information, cela ne s'arrange pas par la suite).

Dans le même format simpliste, mais plus positif : rester curieux. On arrive en thèse pour se focaliser sur

un sujet précis, celui qui fera son chemin jusqu'au manuscrit. Mais il y a autour de nous tout un domaine de recherche qui évolue très vite. Que ce soit en assistant à des conférences ou des séminaires d'équipe, en rencontrant des chercheurs étrangers ou ceux du bureau d'en face à la pause café, il faut garder de l'intérêt pour les thématiques voisines. Ne serait-ce que parce qu'on les retrouvera peut-être plus tard parmi ses propres projets.

Merci de nous avoir fait découvrir ton domaine de recherche, André, et bonne continuation !

Article rédigé par André Schrottenloher (CWI), Céline Chevalier et Pauline Puteaux, contact : Andre.Schrottenloher@cwi.nl

En direct des labos

Patrick Bas

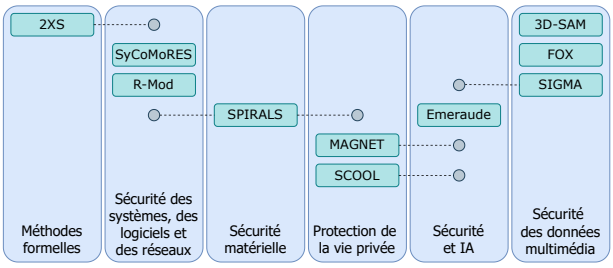
La Gazette interviewe Patrick Bas (DR CNRS), responsable de l'axe transverse en sécurité informatique du laboratoire, qui nous présente l'UMR CRIStAL, située à Villeneuve d'Ascq. L'unité est composée de plus de 470 membres (230 permanents et près de 240 non permanents), dont 28 permanents CNRS et 23 permanents Inria. Les activités de recherche de CRIStAL recouvrent l'informatique, le signal et l'automatique.

Bonjour, quels sont les axes scientifiques de CRIStAL et plus précisément vos objectifs en matière de sécurité informatique ?

Bonjour, les activités en sécurité de CRIStAL sont présentes dans environ un tiers des équipes (10 sur 33) et concernent environ 10% des membres du laboratoire, qui compte actuellement 470 personnes.

« Les activités en sécurité sont présentes dans environ un tiers des équipes »

Comme souvent en cyber-sécurité, les thématiques de recherche sont diverses et recoupent les thématiques des Groupes de Travail du GdR : sécurité des systèmes des logiciels et des réseaux, méthodes formelles, protection de la vie privée, sécurité des contenus, sécurité matérielle, sécurité et IA.



Les axes de recherche en sécurité informatique des équipes du CRIStAL.

Sécurité des systèmes, des logiciels et des réseaux : L'équipe *2XS* est spécialisée dans la détection d'intrusion dans les réseaux de communication internet ou de radio-transmission (Bluetooth). Elle a notamment développé des attaques et des contre-attaques permettant d'éprouver mais aussi de renforcer la sécurité des firmwares embarqués dans les contrôleurs radio.

L'équipe *SyCoMoRES* cherche à analyser les propriétés fonctionnelles des codes assembleurs afin par exemple de détecter des accès mémoire illégaux.

L'équipe *R-Mod* travaille sur des méthodes de sécurisation des langages basées sur l'isolement de parties du langage ou/et l'utilisation de bacs à sable.

L'équipe *SPIRALS* a un axe de recherche porté sur le traçage de navigateurs web à partir d'empreintes générées par les navigateurs. Ces méthodes très sélectives peuvent être utilisées de manière à authentifier l'utilisateur du navigateur.

Protection de la vie privée : L'équipe *MAGNET* développe des méthodes d'apprentissage respectueuses de la vie privée. Ces méthodes sont souvent basées sur le principe d'un apprentissage distribué sur plusieurs utilisateurs dont certains peuvent potentiellement être malveillants.

Les équipes *MAGNET* et *SCOOL* conçoivent également des systèmes de décision reposant sur la confidentialité différentielle. Le principe est de construire des statistiques artificiellement bruitées afin de cacher l'utilisation de données personnelles dans du bruit.

L'équipe *SPIRALS* étudie les propriétés de contrôle d'accès dans une base de données afin, par exemple, de détecter à partir de la sémantique de la base s'il est possible ou non d'exfiltrer des données.

Méthodes formelles pour la sécurité : L'équipe *2XS* propose des méthodes formelles pour éprouver la sécurité sur les logiciels embarqués. Ces méthodes sont par exemple utilisées pour étudier la sécurité des protocoles de communication entre objets connectés.

Sécurité et contenus multimédia : Les équipes *3D-SAM* et *FOX* proposent des méthodes de biométrie à partir de l'analyse des visages, des corps, en vue de la reconnaissance des comportements humains. La reconnaissance des comportements humains est étudiée dans un environnement personnel et de foule en relation avec la sécurité des personnes.

L'équipe *SIGMA* travaille sur l'insertion de données cachées (la stéganographie) et leur détection (la stéganalyse) dans des contenus anodins tels que les images numériques. Une autre partie des activités de cette

équipe se focalise sur la détection de manipulation des images et leur protection par des méthodes d'analyse forensique, de tatouage, ou de chiffrement sélectif.

Patrick Bas

Sécurité des systèmes matériels : L'équipe *SPIRALS* évalue la sécurité des micro-processeurs notamment vis-à-vis d'attaques par canaux auxiliaires. Ces méthodes permettent possiblement d'inférer un élément de sécurité (clé de chiffrement par exemple) à partir de mesures logicielles directement prises sur le système.

> « En stéganalyse, nous avons organisé en 2020 un concours Kaggle qui a réuni plus de 1000 équipes. »

Sécurité et IA : Ces travaux visent à vérifier qu'un algorithme d'apprentissage automatique effectue bien la tâche qui lui est demandée et ce même en présence d'un adversaire. Les équipes *SCOOL* et *MAGNET* travaillent ainsi sur des méthodes équitables qui permettent de garantir qu'une prédiction ne souffre pas d'un biais qui pourrait être introduit par l'adversaire en modifiant la base d'apprentissage. L'équipe *SIGMA* travaille sur des attaques qui permettent de générer les exemples adverses (exemples représentant une classe donnée mais classés en une autre classe) mais aussi de les détecter avant l'appel au classifieur. Cette thématique est aussi étudiée par l'équipe *Emeraude* sur les réseaux de neurones à impulsions (SNN).

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

CRIStAL bénéficie d'un éco-système naturellement lié aux disciplines de la cyber-sécurité avec la présence du Campus-Cyber Lillois, de l'OTAN, du centre de formation de cybersécurité du ministère de l'Intérieur, de la tenue annuelle du Forum International de la Cybersécurité et de la présence d'entreprises motrices telles que Advens, Vadesecure, Stormshield, Orange Cyberdéfense, Thales, Atos, OVH Cloud, Worldline.

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

Les enseignants chercheurs et chercheurs de CRIStAL dispensent des cours en cybersécurité dans des parcours de Master de l'Universtié de Lille (Master Informatique, option cloud computing et internet des objets ou Master Data-Science), de l'université Paris Dauphine, mais également dans des options d'écoles d'ingénieurs se trouvant sur le campus (Polytech'Lille, l'IMT Nord Europe et CentraleLille Institut).

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

En stéganalyse, nous avons organisé en 2020 un concours Kaggle qui a réuni plus de 1000 équipes. Ce concours, co-organisé aux cotés de Rémi Cogranne (UTT), fut un petit succès international (voir https://www.kaggle.com/c/alaska2-image-steganalysis). Au niveau européen, nous animons ce domaine au travers du projet H2020 Uncover qui regroupe 11 agences de sécurité européennes pour 22 partenaires (voir https://www.uncoverproject.eu).

Merci Patrick pour toutes ces informations sur l'organisation de CRIStAL et vos domaines de recherche !

Article rédigé par Patrick Bas (Laboratoire CRIStAL, UMR CNRS 9189 Université de Lille, Centrale Lille), Céline Chevalier et Pauline Puteaux, contact : patrick.bas@cnrs.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.

Chercheur Senior (CDI), INSERM, LaTIM, Brest

Sujet : Sécurité et intelligence artificielle de confiance en santé

Gouenou Coatrieux,

gouenou.coatrieux@imt-atlantique.fr

Ingénieur Back-end - Chiffrement (CDI), Piwwop, Bordeaux

Sujet : Développement d'une application mobile de partage sécurisé de documents – expert communications chiffrées de bout-en-bout et back-end

micro services
rh@piwwop.com

Ingénieur Devops (CDI), Piwwop, Bordeaux

Sujet : Développement d'une application mobile basée sur des communications chiffrées de bout-en-bout et sur un back-end microservices – spécialiste devops
rh@piwwop.com

Poste d'ingénieur de recherche, Heriot-Watt University (Édimbourg, Ecosse)

Sujet : Software Security – Serious Coding : A Game Approach to Security for the New Code-Citizens
Durée : 12 à 15 mois
Manuel Maarek,
M.Maarek@hw.ac.uk

Postes de post-doctorat et d'ingénieurs de recherche, IRISA (Rennes)

Sujet : Development of Squirrel, a proof assistant for security protocols
Durée : 1 an ou plus
Stéphanie Delaune,
stephanie.delaune@irisa.fr
David Baelde,
david.baelde@irisa.fr

Poste de post-doctorat, CERI SN, IMT Nord Europe (Villeneuve d'Ascq)

Sujet : Machine learning techniques for anomaly detection in communication-oriented architectures/protocols
Ahmed Meddahi,
ahmed.meddahi@imt-nord-europe.fr
Hassen Drira,
hassen.drira@imt-nord-europe.fr

Poste de post-doctorat, Telecom Paris (Palaiseau)

Sujet : Formal Validation of C-ITS Protocols
Pascal Lafourcade,
pascal.lafourcade@uca.fr
Mounira Msahli,
mounira.msahli@telecom-paris.fr

Poste d'ATER, CentraleSupélec, Laboratoire IRISA (Rennes)

Sujet : Enseignement en Informatique, Sécurité Informatique
Recherche dans l'équipe CIDRE
Jean-François Lalande,
jean-francois.lalande@centralesupelec.fr

Trois postes d'ATER, Université de Limoges, Laboratoire XLIM (Limoges)

Sujet : Enseignement en Informatique, Recherche en Synthèse d'images réalistes, en Cybersécurité et intelligence artificielle, ou en Cryptographie et sécurité de l'information
Emmanuel Conchon,
emmanuel.conchon@unilim.fr

Thèse de doctorat, Télécom SudParis, LORIA et LIP6 (Paris)

Sujet : Réponse aux attaques basée sur l'IA et la programmabilité des réseaux du futur
Gregory Blanc,
gregory.blanc@telecom-sudparis.eu

Thèse de doctorat, Technology & Strategy et ICude Lab (Strasbourg)

Sujet : Cybersecurity for industrial networks
Fabrice Theoleyre,
fabrice.theoleyre@cnrs.fr

Thèse de doctorat, INRIA Lille, Villeneuve d'Ascq (collaboration avec le CISPA, Sarrebruck, Allemagne)

Sujet : Security analysis of existing and new Web standards
Pierre Laperdrix,
pierre.laperdrix@inria.fr
Romain Rouvoy,
romain.rouvoy@inria.fr
Walter Rudametkin,
walter.rudametkin@inria.fr
Clémentine Maurice,
clementine.maurice@inria.fr

Thèse de doctorat, ENS et LIP6 (Paris)

Sujet : Quantum Security of Multiparty Computation
Céline Chevalier,
celine.chevalier@ens.fr
Alex B. Grilo,
Alex.Bredariol-Grilo@lip6.fr
Damian Markham
damian.markham@lip6.fr