Janvier 2022
Numéro 11

LA GAZETTE DU GDR

Sécurité Informatique - GDR2046

Édito de la directrice

Malgré un début d'année morose en ce qui concerne la situation sanitaire, j'espère que ce nouveau numéro vous redonnera de l'énergie pour démarrer cette nouvelle année, que je vous souhaite pleine de découvertes et de succès !

Vous verrez que l'enthousiasme scientifique tient bon, et que les événements de l'automne, dont plusieurs se sont déroulés en présentiel, ont eu du succès. REDOCS a fait le plein comme chaque année, et nous avons eu plusieurs journées communes avec d'autres GDR (GPL, RSD, SOC2), ainsi qu'avec la SIF, avec au programme : RISC-V, sécurité et génie logiciel, sécurité matérielle de la cryptographie post-quantique, etc. L'automne a également fait la part belle aux podcasts, puisque plusieurs numéros du célèbre podcast hebdomadaire « No Limit Secu » ont présenté des événements du GDR. Un autre est en cours de préparation, mais chut... vous aurez la surprise lors du prochain numéro...

Et devant nous se profilent de nombreux événements : nouvelles journées MFS dans un format plus long en mars, journées C2 en avril, RESSI en mai, APVP et journées nationales en juin. Sans compter les journées ponctuelles des groupes de travail et ce qui suivra ensuite. Alors tenez bon !

Dans ce numéro, vous trouverez également une présentation du PEPR Cybersécurité par ses « sherpas », une interview de Pierre Laperdrix sur ses travaux portant sur le *browser fingerprinting*, ainsi que la présentation du laboratoire XLIM et de ses activités de recherche en codes, cryptographie et données multimédia.

Bonne lecture à toutes et à tous !

Caroline Fontaine,
Directrice du GDR Sécurité Informatique

Rubriques

Événements

(Repris en partie du forum du GDR)

15e Colloque scientifique de l'IMT — Gestion de crise et numérique : nouvelles menaces et nouvelles solutions, *Palaiseau, France, 30-31 mars 2022*

Toulouse Hacking Convention, *Toulouse, France, 14-15 avril 2022*

2nd IEEE/IFIP International Workshop on Internet of Things Management (manage-IoT 2022) *co-organisé avec NOMS 2022, Budapest, Hongrie, 25-29 avril 2022*

AMUSEC — Forum Aix-Marseille de la cybersécurité , *Marseille, France, 5-6 mai 2022*

17th International Conference on integrated Formal Methods (iFM 2022), *Lugano, Suisse, 7-10 juin 2022*

13th International Conference on Cryptology (AFRICACRYPT 2022), *Fès, Maroc, 18-20 juillet 2022*

Privacy in Statistical Database (PSD 2022), *Paris, France, 14-16 septembre 2022*

Journées Nationales 2022

Les Journées Nationales 2022 auront lieu les 22-23-24 juin au tout nouveau campus Cyber de La Défense. Le programme n'est pas encore disponible, mais notez d'ores et déjà les dates dans votre agenda.

Zoom sur le PEPR Cybersécurité

Bruno Charrat, Gildas Avoine et François Cuny

La gazette interviewe Bruno Charrat, Gildas Avoine et François Cuny, qui représentent les pilotes scientifiques du PEPR Cybersécurité, respectivement pour le CEA, le CNRS et Inria, afin de leur permettre d'apporter des réponses aux interrogations de la communauté au sujet de ce PEPR.

Bonjour Bruno, Gildas et François,
Merci d'avoir accepté de nous parler du PEPR Cybersécurité, dont nous entendons parler depuis quelques mois. Pouvez-vous nous expliquer ce qu'est un PEPR et nous parler plus spécifiquement des objectifs du PEPR Cybersécurité ?

Un PEPR est un « Programme et Équipements Prioritaires de Recherche », financé par le PIA4 [1], et mis en place par l'État sur des sujets stratégiques. Le PEPR Cybersécurité est même une des mesures phares de la stratégie nationale d'accélération en cybersécurité annoncée par le Président de la République en février 2021. Tous les PEPR ne sont pas dans une stratégie d'accélération, seulement certains d'entre eux le sont. Les PEPR permettent de financer dans la durée des activités stratégiques de recherche en amont et viennent ainsi compléter les outils existants (financements récurrents des établissements de l'ESR, ANR, EU, international) sans s'y substituer. Lorsque l'État a confié le pilotage du PEPR Cybersécurité au CEA, au CNRS et à Inria, la lettre de mission définissait assez clairement les grands objectifs :

- lancer des défis scientifiques ;
- structurer des équipes ou des communautés de recherche ;
- obtenir des avancées scientifiques ;
- faire émerger des technologies de rupture bénéficiant à l'ensemble des acteurs français de la filière.

Ces actions sont de durée longue, six ans, fédératrices et visent à rassembler plusieurs équipes de recherche des universités, des écoles et des organismes de recherche nationaux autour de projets qui sont dotés dans le cas du PEPR Cybersécurité de 5 M€ à 7 M€, environ. Il faut garder à l'esprit que ce PEPR s'inscrit dans la stratégie nationale d'accélération en cybersécurité et qu'il a vocation à contribuer aux objectifs de cette stratégie. Le coordinateur de la stratégie nationale d'accélération en cybersécurité est William Lecat du Secrétariat général pour l'investissement (SGPI).

Qui a choisi les labos qui vont bénéficier des financements ?

Afin de lancer le PEPR, l'État a demandé aux pilotes, c'est-à-dire aux trois responsables des organismes de recherche nationaux, un document de cadrage qui devait :

- donner une cartographie des forces de recherche françaises et des éléments de comparaison internationale ;
- proposer une vision et une stratégie scientifique globalement cohérente avec la stratégie nationale ;
- décrire un programme de déclinaison opérationnelle.

La première étape a donc été d'étudier tous les documents et livres blancs préparés par la communauté scientifique, comme la feuille de route du réseau SPARTA, le livre blanc d'Inria, la cartographie d'Allistene, l'ouvrage du CNRS sur les 13 défis de la cybersécurité, et bien d'autres encore, afin d'identifier les priorités. Puis nous avons échangé avec toutes les parties prenantes de la filière afin de cibler les enjeux les plus stratégiques et de renforcer l'adhésion de tous les acteurs. La forme de l'exercice était très contrainte dans la forme et dans le temps. Pour rédiger notre document de cadrage nous avons ainsi consulté à plusieurs reprises :

- des représentants de la recherche (CPU [2], CDEFI [3], Udice, Allistene) ;
- des autorités et acteurs étatiques (ANSSI, DGA, AID [4]) ;
- les pilotes et financeurs d'initiatives stratégiques (SGPI [5], DGRI [6], ANR, Grand Défi Automatisation de la cybersécurité, Coordinateur de la stratégie d'accélération).

« Le PEPR s'inscrit dans la stratégie nationale d'accélération en cybersécurité. »

Pour analyser notre proposition, l'État s'est fait accompagner d'un comité d'experts. Nous avons eu le retour de l'État sur notre proposition de document de cadrage en juillet 2021. Cela a permis de mobiliser des porteurs identifiés pour leur légitimité et leur compétence

1. Plan d'Investissement d'Avenir
2. Conférence des présidents d'université
3. Conférence des directeurs des écoles françaises d'ingénieurs
4. Agence de l'innovation de défense
5. Secrétariat général pour l'investissement
6. Direction générale de la recherche et de l'innovation

dans la construction des projets qui avaient été sélectionnés. Ils ont eu la mission de mobiliser les équipes nécessaires et pertinentes pour la réalisation du projet et de construire un programme détaillé sur 5 à 6 ans. On a vraiment apprécié leur implication et leur réactivité.

Quels sont alors les projets retenus ?

Le document de cadrage remis à l'État proposait 9 premiers sujets. Nous pourrons communiquer plus largement dans les semaines à venir, mais nous pouvons d'ores et déjà porter à la connaissance de la communauté que, parmi eux, 7 sont en cours de dimensionnement, et les plus avancés, à savoir ARSENE (architectures sécurisées pour le numérique embarqué), IPOP (protection des données personnelles), SECURECOMPUTE (sécurité des calculs), SECUREVAL (améliorer l'évaluation de la sécurité des systèmes logiciels) et SVP (vérification de protocoles de sécurité) devraient être rapidement conventionnés. En parallèle nous apportons les dernières touches à un appel à projets qui permettra de structurer deux communautés, à savoir la sécurité des données multimédia, et la recherche de vulnérabilités. Il devrait être publié à la fin du premier trimestre. Vous remarquerez que les projets sont en fait répartis dans tous les Groupes de Travail du GDR, ce qui n'est pas très surprenant car aussi bien les GT du GDR que les projets du PEPR prennent source dans la communauté scientifique française.

J'ai entendu dire que la cryptographie post-quantique n'est pas dans le PEPR Cybersécurité ?

C'est exact. Le PEPR Quantique avait prévu un projet sur la cryptographie post-quantique. De manière indépendante, nous avions fait de même. Il n'y avait évidement pas de sens à maintenir deux projets. Alors, d'un commun accord entre les deux PEPR, nous avons décidé de mettre toute la cryptographie post-quantique dans un seul PEPR, en l'occurrence le PEPR Quantique pour des raisons de cohérence, car ce sujet était explicitement intégré dans le plan quantique. Les deux PEPR ont travaillé de concert pour définir les actions à conduire et adapter le budget du projet de manière conséquente.

Pour les équipes qui ne sont pas dans cette première vague, quelles possibilités s'offrent à elles ? Peuvent-elles se raccrocher à un projet existant ou peuvent-elles proposer un nouveau projet ?

Les consortiums ne sont pas figés dans le temps, ils peuvent évoluer. De plus, nous avons la possibilité de lancer d'autres projets. Dans le document de cadrage, nous avons par exemple identifié la cryptanalyse comme un sujet majeur qui pourrait faire l'objet d'un appel à projet. La communauté française est au meilleur niveau mondial et il est important de maintenir ce niveau d'excellence. Mais nous réfléchissons également à d'autres sujets. Nous sommes à l'écoute des suggestions de la communauté.

Cela fait plus d'un an que vous travaillez sur le montage du PEPR, quel est votre retour d'expérience ?

Le montage de ce programme est une belle aventure humaine et scientifique. La collaboration entre les porteurs et le reste de la communauté est fluide. Comme ces outils sont encore très récents, beaucoup de choses se construisent au fur et à mesure, et nous sommes heureux de pouvoir compter sur le très fort soutien des autres parties prenantes, comme l'ANR, le coordinateur de la stratégie nationale, ainsi que la DGRI. En tant que « sherpas », nous pouvons aussi témoigner de la très forte implication des PDG et AG des trois organismes de recherche qui ont eu à cœur de mener à bien ce travail dans un esprit collectif au service de la communauté, de viser l'excellence scientifique et d'avoir un impact pour la filière. L'exercice n'a pas toujours été facile, mais il nous semble que ce cap a été maintenu.

Et le GDR ? A-t-il un rôle à jouer dans le PEPR Cybersécurité ?

Bien sûr ! Nous comptons vraiment sur lui ! Nous avons toujours eu la volonté pendant le montage du PEPR de ne pas créer de doublons, de ne pas ré-inventer la roue. Il est important qu'il existe une animation de la communauté autour des thématiques du PEPR. Cela n'aurait toutefois pas eu de sens de créer une nouvelle structure, alors nous comptons sur le GDR pour poursuivre sa mission d'animation, et nous avons prévu de le soutenir financièrement dans cette tâche.

Merci à vous trois de vous êtes prêtés au jeu de l'interview.

Merci surtout à la gazette de nous avoir offert cette opportunité de parler du PEPR. Tout au long de l'année passée, nous avons suivi une ligne de conduite stricte concernant la communication des informations et respecté les étapes du processus de validation du PEPR. Aujourd'hui, c'est un réel plaisir de pouvoir parler ouvertement du PEPR avec la communauté.

Article rédigé par Bruno Charrat (adjoint au directeur de la recherche technologique (DRT) du CEA en charge de la coordination des actions Cybersécurité), Gildas Avoine (prof. INSA Rennes, chargé de mission CNRS), François Cuny (directeur général délégué à l'innovation d'Inria) et Céline Chevalier, contact : bruno.charrat@cea.fr, gildas.avoine@irisa.fr, francois.cuny@inria.fr

Le coin prospectif

Pierre Laperdrix

La gazette interviewe Pierre Laperdrix, chargé de recherche CNRS au sein de l'équipe-projet Spirals, commune à Inria et au laboratoire CRIStAL. Pierre travaille dans le domaine de la sécurité informatique, de la protection de la vie privée et de l'ingénierie logicielle. Il nous parle de son domaine de recherche qui concerne Internet et le *browser fingerprinting* en particulier.

Bonjour Pierre, peux-tu présenter rapidement tes activités ?

Ma recherche se focalise sur la sécurité et le respect de la vie privée sur Internet. Dans mon équipe, nous regardons à la fois ce qui se passe côté utilisateur, mais aussi côté serveur. On utilise des navigateurs pour comprendre les scripts qui y sont exécutés ou les identifiants qui sont stockés. On effectue des mesures à large échelle sur des milliers de sites pour comprendre les échanges de données qui peuvent exister. On analyse aussi les applications sur *smartphone* pour identifier des fuites de données. Bref, à la vitesse d'évolution du web et l'apparition de nouvelles technologies, on n'a vraiment pas de quoi s'ennuyer !

Pierre Laperdrix.

En quoi consiste le traçage par empreintes de navigateurs (browser fingerprinting) ?

Depuis le début du web, les navigateurs partagent des informations avec tous les serveurs dans le monde pour optimiser l'expérience de navigation. Quand je me connecte à un site, mon appareil va indiquer que j'utilise Windows ou Mac comme système d'exploitation, que je demande des pages en français et que j'ai un grand ou un petit écran. Ces informations sont transparentes pour l'utilisateur mais permettent au site de s'adapter pour que la page s'affiche correctement ou qu'elle propose un lien de téléchargement vers la bonne version d'un logiciel.

Cependant, il est possible de détourner l'usage de ces informations pour constituer ce qu'on appelle une « empreinte de navigateur ». Un script malveillant va communiquer avec le navigateur pour récupérer le maximum d'informations sur l'appareil de l'utilisateur et sur sa configuration. Ces informations incluent par exemple le navigateur et sa version, le système d'exploitation, le modèle du *smartphone* ainsi que la version du *firmware* installé, la taille de l'écran, le fuseau horaire de l'utilisateur ou bien le modèle de carte graphique utilisé.

On peut alors se poser la question : pourquoi le *browser fingerprinting* représente-t-il un danger pour les internautes ? La raison est toute simple : il existe une telle diversité d'appareils et de configurations dans le monde que la combinaison de toutes les informations d'une empreinte peut être unique, ce qui signifie qu'il est possible d'identifier un utilisateur parmi beaucoup d'autres et de retracer ses activités en ligne.

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

Nous sommes dans une période où la publicité sur Internet subit de grands changements. Certains mécanismes comme les cookies tiers utilisés très couramment par les agences de publicité vont disparaître, et ce qui se passe sur Internet en termes de collecte de données évolue énormément. Dans ce contexte, le *fingerprinting* essaye de trouver sa place et il peut être très compliqué de comprendre comment et pourquoi il est utilisé.

Un des grands défis du domaine est tout simplement de détecter le *fingerprinting*. Contrairement au cas des cookies pour lequel il est possible de voir qu'un identifiant utilisateur a été stocké dans le navigateur, le *fingerprinting* ne laisse aucune trace. En visitant une page web, l'utilisateur ne sait pas que des informations sur son terminal sont en train d'être collectées alors qu'il est très facile de voir qu'un cookie a été déposé. Des techniques poussées d'analyse sont donc nécessaires pour détecter finement les comportements relatifs à des activités de *fingerprinting*.

« Contrairement au cas des cookies pour lequel il est possible de voir qu'un identifiant utilisateur a été stocké dans le navigateur, le *fingerprinting* ne laisse aucune trace. »

Le deuxième grand défi du domaine est d'identifier la finalité de la collecte d'empreintes. Si un script collecte la résolution d'écran de l'utilisateur, est-ce que c'est pour optimiser l'affichage de la page ou est-ce le premier élément dans la constitution d'une empreinte ? C'est pour cela que le *fingerprinting* existe toujours depuis sa découverte dans les années 2010. La ligne entre un usage légitime de ces informations et un usage à des fins de traçage est très étroite et il peut être facile de se tromper. Sans la compréhension de la finalité d'un script, il est compliqué de développer les défenses adéquates.

Quels conseils peux-tu donner aux jeunes chercheurs intéressés par la protection de la vie privée ?

Dans le domaine de l'Internet, tout évolue extrêmement vite. Les navigateurs ajoutent tous les ans de nouvelles fonctionnalités pour offrir une expérience de plus en plus riche aux utilisateurs. Il y a 20 ans, on affichait seulement du texte et des images alors que maintenant, on peut jouer en multi-joueurs en réalité virtuelle directement depuis son navigateur ! Bien que ces avancées technologiques soient les bienvenues, il ne faut pas oublier l'utilisateur qui est au centre et le fait que tous ces développements ne doivent pas se faire au détriment de la vie privée de chacun. Un conseil que je peux donner aux jeunes chercheurs intéressés par ce sujet est de faire une veille constante des évolutions du web. Une nouvelle technologie ou une décision d'un acteur majeur du web peut avoir d'énormes ramifications sur ce qui se passe en ligne et il est donc important d'être à jour sur ces changements pour pouvoir réagir le plus efficacement derrière.

Merci Pierre de nous avoir fait découvrir le browser fingerprinting et pour tes sages conseils !

Article rédigé par Pierre Laperdrix (Univ Lille, CNRS, Inria), Céline Chevalier et Pauline Puteaux, contact : pierre.laperdrix@inria.fr

Retour sur REDOCS 2021

Pascal Lafourcade

La sixième édition des Rencontres Entreprises DOCtorants en Sécurité informatique (REDOCS) s'est déroulée au Centre International de Rencontres Mathématiques (CIRM `https://www.cirm-math.fr`) du 25 au 29 octobre 2021 à Luminy.

Lors de cette édition les entreprises Airbus et Orange et la CNIL ont proposé les sujets suivants :

— Le sujet d'Airbus visait à développer un rançongiciel factice pour des exercices de red team.

— Le sujet d'Orange consistait à développer des solutions pour pouvoir traiter des données chiffrées dans un contexte multi-utilisateurs.

— Le sujet de la CNIL portait sur l'analyse du respect de la vie privée d'objets connectés du quotidien.

Cette édition a accueilli 15 participants venant de toute la France. Ce fut l'occasion pour les étudiants de rencontrer d'autres personnes et d'avoir des échanges riches et passionnés. Les trois équipes ont apporté des solutions originales aux sujets proposés par les industriels.

Cette semaine intensive de travail s'est déroulée dans la bonne humeur et dans un cadre exceptionnel. La prochaine édition de REDOCS aura lieu au CIRM du dimanche 27 novembre au samedi 3 décembre 2022, pensez à le noter dans vos agendas !

Pascal Lafourcade, contact : pascal.lafourcade@uca.fr

Brèves

• La SIF, en partenariat avec le GDR Sécurité Informatique et les GDR RSD et SOC2, a organisé en octobre 2021 un événement sur deux jours pour faire l'état des lieux sur les plateformes matérielles pour la sécurité. Les ressources sont disponibles à l'adresse suivante : https://www.societe-informatique-de-france.fr/les-journees-sif/journees-securite-14-et-15-octobre-2.

• En 2021 plusieurs épisodes du podcast hebdomadaire NoLimitSecu https://www.nolimitsecu.fr/ ont parlé du ou ont été liés au GDR : Gildas Avoine a presenté le GDR dans l'épisode #301 ; Charlie Jacomme, lauréat du prix de thèse du GDR, a présenté son travail suite au prix dans l'épisode #337 ; Pascal Lafourcade a présenté l'ouvrage ludique qu'il a écrit sur la cryptographie dans l'épisode #332 ; Benjamin Nguyen a présenté le « hackathon » d'APVP dans l'épisode #339 ; et pour finir Pascal Lafourcade a présenté REDOCS dans l'épisode #347.

Retour sur la journée inter-GDR sur la sécurité et le génie logiciel

Olivier Levillain

Le 9 novembre dernier, le GT SSLR (Sécurité des Systèmes, des Logiciels et des Réseaux) du GDR Sécurité Informatique et le nouveau GT GL_Sec (Génie Logiciel et Sécurité) du GDR GPL (Génie de la Programmation et du Logiciel) ont co-organisé une journée au CNAM. L'événement a accueilli environ 30 personnes. Au programme, deux conférences invitées et la présentation de travaux de thèses variés.

La journée s'est ouverte sur une intervention de Stéphane Ducasse, DR Inria au centre Inria Nord Europe et responsable de l'équipe RMoD (*Code Analysis and Remodularization of Applications*). Partant du constat que le logiciel est une chose complexe qui évolue de manière continue, Stéphane nous a proposé des réflexions sur la notion de *legacy systems*. Tout d'abord, contrairement à une idée reçue, de tels systèmes existent dans n'importe quel langage, puisqu'il suffit de quelques années pour que l'état d'un projet logiciel mal entretenu se dégrade. Afin d'aider les développeurs à évaluer la situation, l'équipe RMoD a notamment travaillé sur des outils de visualisation faciles à exploiter (représentations graphiques de la complexité des classes d'un projet, répartition des contributions des développeurs sur les différents modules d'un projet, *etc.*). À la fin de son intervention, l'orateur a invité la communauté à échanger avec lui sur les besoins de visualisation liés à la sécurité.

En début d'après-midi, Jean-Philippe Le Luet, *leader* du centre de compétences *Security by Design* de l'entité Crédit Agricole Technologies et Services, nous a présenté la mise en place de la démarche *Security by Design* dans son entreprise, avec un fonctionnement en mode Agile. L'intervenant a commencé par décrire l'ampleur de la tâche : des centaines de projets, découpés en une dizaine de milliers de composants, dont une grande partie peut être considérée comme des *legacy systems*. Pour intégrer de manière progressive la méthode agile dans le groupe, de nombreux outils ont été mis en œuvre, que ce soit pour le développement (GitLab, Jira, *etc.*) ou pour l'évaluation de la sécurité des applications (analyse statique de code, outils de qualité de code, recherche de vulnérabilités, *etc.*). Cette présentation s'est terminée sur un premier état des lieux de la démarche, qui a mis en évidence le besoin d'établir des priorités dans la correction des problèmes détectés, avec certains modules très vulnérables, et très partagés au sein de nombreux projets.

Nous remercions chaleureusement nos invités, ainsi que l'ensemble des personnes ayant présenté leurs travaux de thèse pendant cette journée. Les supports des conférences invitées et de certaines des autres interventions sont disponibles sur le site de la journée : `https://journee-gl-secu.sciencesconf.org/`

Olivier Levillain, contact : olivier.levillain@telecom-sudparis.eu

Retour sur la journée SSM

Cédric Marchand

Avec l'arrivée de l'ordinateur quantique, les algorithmes de chiffrement et de signature basés sur des problématiques « traditionnelles » de théorie des nombres – à savoir le logarithme discret ou le problème de factorisation d'entiers – pourront être cassés dans un temps raisonnable. Les algorithmes de cryptographie post-quantique ont pour but de fournir une solution à cette nouvelle ère informatique qui s'annonce. Les problèmes sur lesquels la sécurité de ces crypto-systèmes repose sont d'une autre nature (recherche de plus court vecteur dans un réseau euclidien, décodage d'un code aléatoire ou encore résolution de systèmes algébriques multivariés). Cette différence leur profère une sécurité supérieure face aux attaques utilisant un algorithme quantique. Cependant, un algorithme peut être mathématiquement sûr ou reposer sur un problème mathématique qui, même pour un ordinateur quantique, serait considéré comme très difficile à résoudre (dans un temps raisonnable), cela ne garantit pas qu'il soit pour autant impossible d'utiliser d'autres biais pour l'attaquer. C'est justement l'objet des attaques matérielles, et notamment les attaques par canaux auxiliaires et les attaques par injection de fautes. La question qu'il convient alors de se poser est la suivante : quelle est la robustesse des algorithmes post-quantiques face aux attaques matérielles ? La journée du 10 novembre 2021, qui s'est déroulée au laboratoire LIP6 à Paris, a rassemblé une trentaine de personnes autour de cette question (25 présents sur place et 5 à distance). Les 5 présentations de la journée ont permis de faire un tour d'horizon des implantations matérielles mais aussi des attaques qui ont pu être conduites sur ces implémentations. Ainsi, des implémentations sur microcontrôleur et par synthèse de haut niveau sur plateforme matérielle de type FPGA ont été présentées. Du côté des attaques, l'application d'une analyse par canal auxiliaire de type SPA (*Simple power analysis*) mais aussi des attaques en faute par onde électromagnétique et par laser ont été présentées. Cette journée est la première journée du GT-SSM à avoir été organisée en présentiel depuis

la pandémie. Cela a été très apprécié par les participants et les échanges lors de cette journée ont été très riches et intéressants. L'ensemble des retours reçus à l'issue de cette journée nous encourage à reconduire les journées en présentiel au maximum si la situation le permet. L'ensemble des vidéos disponibles et des fichiers de présentations sont présents sur le site du GDR à l'adresse suivante : https://gdr-securite.irisa.fr/journee-thematique-gt-ssm-algorithmes-de-chiffrement-post-quantiques-et-securite-materielle/

Cédric Marchand, contact : cedric.marchand@ec-lyon.fr

En direct des labos

Philippe Carré et Philippe Gaborit

La Gazette interviewe Philippe Carré (Vice-Président Numérique Université de Poitiers, membre de l'axe ASALI, Laboratoire XLIM, Université de Poitiers) et Philippe Gaborit (responsable de l'équipe Cryptis, Laboratoire XLIM, Université de Limoges), qui nous présentent l'institut de recherche XLIM. Il s'étend sur les villes de Limoges, Brive, Poitiers et Angoulême en région Nouvelle-Aquitaine et ses thématiques de recherche recouvrent l'électronique, les mathématiques, l'informatique, l'image et la photonique.

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

XLIM est une unité multidisciplinaire rattachée à l'Institut des Sciences de l'Ingénierie et des Systèmes (INSIS) en tant qu'institut principal du CNRS, à l'Institut des Sciences Mathématiques et de leurs Interactions (INSMI), à l'Institut des Sciences de l'Information et de leurs Interactions (INS2I) et à l'Institut des Sciences de l'Univers (INSU) en tant qu'instituts secondaires. L'unité compte 471 membres, dont 236 permanents et 235 non-permanents. Le laboratoire est constitué de 6 axes de recherche : l'axe Systèmes Radio-Fréquences ; l'axe Radio-Fréquences et Électronique Imprimée pour les Télécoms et l'Énergie ; l'axe Systèmes et Réseaux Intelligents ; l'axe Photonique ; les deux axes liés à la sécurité informatique sont l'axe Synthèse et Analyse d'Image qui regroupe 3 équipes dans les domaines de la modélisation géométrique, du traitement, de la synthèse et de l'analyse d'images, et l'axe Mathématiques et Sécurité de l'Information qui regroupe 4 équipes dans les domaines du calcul formel, de l'analyse variationnelle, de l'optimisation numérique, de la théorie des nombres et de la cryptographie. En matière de sécurité informatique, une grande partie de la recherche se concentre dans l'équipe Cryptis, qui est une équipe de recherche Mathématiques-Informatique, à large spectre de recherche en cryptographie/sécurité sur le continuum de la théorie à la pratique et très reliée au Master CRYPTIS. L'équipe a quatre axes de recherche principaux, autour de :

- la cryptologie, avec notamment la cryptologie post-quantique et la cryptographie quantique,
- les attaques physiques et la cryptologie des systèmes embarqués,
- la sécurité des systèmes et réseaux : sécurité des réseaux, protection de la vie privée, systèmes embarqués, sécurité de la 5G,
- l'application des mathématiques discrètes au codage, à l'arithmétique effective avec par exemple le *watermarking*, le *network coding*, les algorithmes de décodage ou encore l'arithmétique effective.

Actuellement, l'équipe évolue en gardant ses fondamentaux sur le côté interaction math-info et ses applications à la cryptographie et la sécurité, mais en essayant de plus développer l'axe quantique et notamment les codes correcteurs quantiques. Nous nous concentrons également sur des aspects de sécurité prouvable de bout en bout dans les réseaux mobiles 5G (en allant vers la 6G), ainsi que dans la messagerie asynchrone. D'une manière complémentaire, un volet autour de la sécurité des données multimédia est portée par l'équipe Icones, de l'axe Synthèse et Analyse d'Image. L'équipe mène plus généralement des travaux autour de la donnée, de l'image et des modèles de représentation ou de décision en lien avec l'IA. En matière de sécurité, ces recherches se concrétisent dans :

- la détection de données enfouies (stéganalyse) en s'appuyant à la fois sur des stratégies basées sur des tests d'hypothèses (vision statistique, fonction de croyance) et sur des stratégies basées sur de la modélisation (structure Deep),
- l'optimisation des stratégies d'enfouissement (tatouage) en utilisant à la fois des concepts de codes correcteurs (avec l'équipe Cryptis) pour la robustesse et en intégrant la modélisation du Système Visuel Humain pour l'invisibilité.


Philippe Carré et Philippe Gaborit.

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

Depuis la fusion des régions, nous travaillons sur le tissu local mais aussi plus généralement avec la région Nouvelle Aquitaine, notamment via le projet NAQUIDIS (https://naquidis.com/) qui est fortement soutenu par la région Nouvelle Aquitaine et vise à développer les technologies autour du quantique, ce qui inclut le post-quantique en particulier. Des interactions existent aussi avec les laboratoires du proche environnement comme le Laboratoire de Mathématiques et Applications (LMA) autour de la construction des modèles statistiques de détection d'informations dissimulées.

Nous sommes aussi fortement impliqués avec des industriels au niveau national dans des thèses CIFRE, notamment avec Orange, le CEA, WORLDLINE, ou encore ICOHUP, d'autres projets sont en cours de développement avec des entreprises locales, comme l'entreprise Einden pour des problématiques de tatouage.

À travers des projets ANR actuels comme les ANR MOBIS5, CBCRYPT ou BARRACUDA, nous avons aussi des connexions avec de nombreuses équipes du domaine en France au sein des institutions de recherche comme par exemple Inria, LIMOS, IRISA, LiX, ENS Paris, Eurecom ou le laboratoire de Psychologie et Neurocognition.

Au niveau international l'équipe Cryptis a participé au concours international du NIST sur la standardisation post-quantique ce qui a conduit à des collaborations avec des chercheurs de nombreuses universités et entreprises internationales comme Google, Amazon, Intel, Université de Floride, Université de Bochum, mais aussi Sogang University en Corée ou la National University of Singapore.

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

Les recherches menées au sein de l'équipe Cryptis sont adossées au master CRYPTIS qui est composé de 2 parcours en partie mutualisés : un parcours *Sécurité Informatique* dans la mention Informatique et un parcours *Mathématiques Cryptographie Codage et Applications* dans la mention Mathématiques et applications. Ces parcours sont en présentiel et préparent aux métiers liés à la confidentialité, la sécurité de l'information et la cryptologie. Cette formation s'appuie sur 20 enseignants-chercheurs d'XLIM pour assurer une formation à la fois diverse et pointue, avec un cursus alliant des mathématiques fondamentales (théorie des nombres, algèbre des corps finis) et de l'informatique (réseaux, programmation, calcul scientifique). On y dispense environ 900h d'enseignement en présentiel dont 30% sous forme de travaux pratiques et projets.

Les recherches menées au sein de l'équipe Icones sont adossées aux différentes formations du secteur Mathématiques et Numérique de l'université de Poitiers (master Informatique, master Traitement du signal et des images, master Mathématiques et applications). Ce sont dans ces formations que les étudiants acquièrent les fondamentaux en lien avec ce volet de la sécurité de la donnée multimédia (statistique, IA, ...).

Ces travaux s'illustrent aussi au sein de l'École Universitaire de Recherche dans les matériaux céramiques avancés et les technologies de l'information et de la communication (EUR TACTIC), projet labellisé École Universitaire de Recherche par l'ANR et déposé par l'Université de Limoges, en partenariat avec l'Université de Poitiers, et le CNRS.

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

L'équipe Cryptis a été très active pour proposer des nouveaux systèmes de chiffrement à base de codes correcteurs d'erreurs, sur la métrique de Hamming, mais aussi sur la métrique rang (une variation sur la métrique de Hamming). Ces avancées ont donné lieu à huit soumissions au concours de standardisation international du NIST. Deux propositions sur les codes (les protocoles BIKE et HQC) sont encore en course dans ce processus, qui dure depuis plus de 4 ans maintenant. On attend les réponses du 3e tour de manière imminente.

> « Ces avancées ont donné lieu à huit soumissions au concours de standardisation international du NIST. »

Ces dernières années, de nombreux travaux ont par ailleurs été menés en collaboration avec Inria, l'Université de Rouen et certains chercheurs du NIST sur les attaques algébriques pour arriver à bien évaluer la sécurité des primitives cryptographiques basées sur la métrique rang. Ces travaux ont donné lieu à des publications à EUROCRYPT en 2020 et ASIACRYPT en 2020, et ont fait avancer l'idée qu'on se faisait de la sécurité de la métrique rang par les attaques algébriques et permis de mieux comprendre leur sécurité réelle. Cela a donné lieu à de très jolis résultats mélangeant la cryptographie et le calcul formel. Récemment le NIST a annoncé qu'ils allaient lancer un nouvel appel pour des signatures post-quantiques très bientôt, nous travaillons donc activement aussi sur le sujet sur des signatures efficaces

en métrique de Hamming, mais aussi en métrique rang. Une autre partie de notre recherche s'est concentrée autour des problématiques de sécurité et de vie privée dans les réseaux 5G. Par exemple, nous avons travaillé sur le sujet des interceptions légales dans les réseaux mobiles. Dans cette optique, nous avons proposé une solution réconciliant les besoins d'interception légale avec un meilleur respect de la vie privée (travail publié à ESORICS 2021).

Merci Philippe et Philippe pour toutes ces informations sur l'organisation de XLIM et vos domaines de recherche. Bonne chance pour vos futures soumissions au concours du NIST !

Article rédigé par Philippe Carré (Laboratoire XLIM, UMR CNRS 7252 Université de Poitiers), Philippe Gaborit (Laboratoire XLIM, UMR CNRS 7252 Université de Limoges), Céline Chevalier et Pauline Puteaux, contact : gaborit@unilim.fr, philippe.carre@univ-poitiers.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.

Postes de maître de conférences et de professeur des universités, LMF/ENS Paris-Saclay (Saclay)

Sujet : Méthodes formelles et sécurité
Mihaela Sighireanu (dir. département enseignement),
sighireanu@lsv.fr
Patricia Bouyer (dir. laboratoire),
bouyer@lsv.fr
Caroline Fontaine (resp. équipe),
fontaine@lsv.fr

Poste de professeur, Université de Sherbrooke (Québec)

Sujet : Informatique - Intelligence artificielle/sciences des données, sécurité informatique, jeux vidéo et/ou internet des objets
Marc Frappier,
Marc.Frappier@USherbrooke.ca

Poste de maître de conférences, IRIT/UT2J (Toulouse)

Sujet : Ingénierie des systèmes de confiance : Ingénierie logicielle, cyber-sécurité et sûreté
Jean-Marc Pierson,
jean-marc.pierson@irit.fr
Ileana Ober,
ileana.ober@irit.fr
Brahim Hamid,
brahim.hamid@univ-tlse2.fr

Poste de maître de conférences, Université de Rennes 1/IRISA (Rennes)

Sujet : Informatique et sécurité du logiciel
Sophie Allain,
Sophie.Allain@univ-rennes1.fr
David Bromberg,
david.bromberg@irisa.fr
Steven Derrien,
steven.derrien@irisa.fr
Nicolas Markey,
nicolas.markey@irisa.fr
Stéphanie Delaune,
Stephanie.Delaune@irisa.fr

Poste d'ingénieur chercheur en CDI, EDF (Palaiseau)

Sujet : Cyber-sécurité
Youssef Laarouchi,
youssef.laarouchi@edf.fr

Poste de post-doctorat, Institut Polytechnique de Paris (Palaiseau)

Sujet : Simulation/co-simulation/emulation to model systems and threats
Durée : 18 mois
Grégory Blanc,
gregory.blanc@telecom-sudparis.eu

Poste de post-doctorat, IETR (Rennes)

Sujet : Laser fault injection in secure electronic systems
Durée : 18 mois
Laurent Pichon,
laurent.pichon@univ-rennes1.fr
Philippe Babilotte,
philippe.babilotte@univ-rennes1.fr

Deux postes de post-doctorat, CEA LIST Paris-Saclay (Gif-sur-Yvette)

Sujet 1 : Designing Compilation Techniques for Improving Efficiency of E-ACSL, a Runtime Assertion Checker for C Programs
Sujet 2 : Control Flow Integrity for Remote Attestation
Durée : 24 mois

Julien Signoles,
Julien.Signoles@cea.fr

Thèse de doctorat, LIP6 (Paris)

Sujet : Formal leakage-free analysis and modelling of microarchitectural sources of leakage
Karine Heydemann,
karine.heydemann@lip6.fr
Quentin Meunier,
quentin.meunier@lip6.fr

Thèse de doctorat, Lab-STICC (Lorient)

Sujet : Architecture de communication sécurisée d'un SoC vis-à-vis des attaques physiques et logiques
Vianney Lapôtre,
vianney.lapotre@univ-ubs.fr
Guy Gogniat,
guy.gogniat@univ-ubs.fr

Thèse de doctorat CIFRE, Thales ThereSIS (Palaiseau) et LaTIM (Brest)

Sujet : Sécurisation de l'Apprentissage Fédéré
Katarzyna Kapusta,
katarzyna.kapusta@thalesgroup.com

Stage, Télécom SudParis, Institut Polytechnique de Paris (Palaiseau)

Sujet : Verifiable network resilience, policy translation for stateful data planes
Grégory Blanc,
gregory.blanc@telecom-sudparis.eu

Stage, ERIC (Lyon)

Sujet : Détection d'attaques dans une application IoT à partir des fichiers de traces (fichiers log) des objets connectés
Mohamed-Lamine Messai,
mohamed-lamine.messai@univ-lyon2.fr

Deux stages, SAMOVAR/LTCI, Institut Polytechnique de Paris (Palaiseau)

Sujet 1 : Security Modelling and Assessment
Sujet 2 : Digital Twin for Securing Building Management Systems
Grégory Blanc,
gregory.blanc@telecom-sudparis.eu

Stage, LAMIH (Valenciennes)

Sujet : Mémoire visuelle et cybersécurité
Antoine Gallais,
antoine.gallais@uphf.fr
Enka Blanchard,
koliaza@gmail.com

Stage, IRISA (Rennes)

Sujet : Suivi dynamique de flux d'information dans les applications hybrides
Guillaume Hiet,
guillaume.hiet@centralesupelec.fr