Février 2020
Numéro 5

LA GAZETTE DU GDR

Sécurité Informatique - GDR2046

Édito du directeur

Dans ce numéro hivernal de la Gazette, vous trouverez une actualité particulièrement riche, notamment avec l'annonce des événements 2020 du GDR. Nous pouvons en effet annoncer que les Journées Nationales auront lieu du 1er au 3 juillet à l'Université Paris Dauphine, l'École d'été sera organisée du 6 au 10 juillet au château du CNRS sur le campus de Gif-sur-Yvette, et les REDOCS se tiendront comme d'habitude pendant les congés de la Toussaint, plus précisément du 26 au 30 octobre, également sur le campus de Gif-sur-Yvette (mais pas dans le château...). La participation à tous ces événements est gratuite. Vous recevrez ultérieurement des messages sur la liste du GDR pour les modalités d'inscription.

Au-delà de ces événements, chaque groupe de travail organise également des activités. Pour le premier semestre 2020, il y a eu la journée sur les méthodes formelles pour la sécurité le 31 janvier au LIP6, et il y a à venir deux journées du GT « Sécurité des systèmes matériels » le 18 mars à Paris et le 16 avril à Lyon, ainsi que RESSI du 18 au 20 mai à Nouan-le-Fuzelier en Sologne, et enfin APVP du 24 juin au 26 juin à Saint-Martin-de-Londres au cœur du Languedoc. Les journées C2 qui devaient se tenir du 15 au 20 Mars 2020 à Erdeven en Bretagne doivent malheureusement être reportées à une date ultérieure en raison du contexte actuel lié au Coronavirus.

Parmi les actualités, il y a aussi la campagne de recrutement qui approche. Une synthèse des annonces parues sur le forum est fournie en fin de Gazette. C'est l'occasion de rappeler l'existence de la liste de diffusion « forum » (voir information sur le site web du GDR) sur laquelle chacun d'entre nous peut poster des annonces diverses à destination de la communauté. La majorité de ces annonces trouvent ensuite écho dans la Gazette. Je souligne également que la Gazette est un outil d'échange d'information offert à toute la communauté. Si vous souhaitez partager une information d'intérêt général, n'hésitez pas à nous contacter via l'adresse `gazette-editeurs@gdr-securite.fr`. Quelle que soit la nature de l'information, elle trouvera sa place dans la Gazette.

Dernières informations – et pas des moindres – l'appel pour le prix de thèse 2020 va être publié dans les prochains jours sur la liste de diffusion du GDR, et le Club de partenaires industriels est officiellement créé depuis le 1er janvier.

Il est maintenant temps pour moi de vous souhaiter une très bonne lecture de ce cinquième numéro de la Gazette du GDR.

Gildas Avoine,
Directeur du GDR Sécurité Informatique

Rubriques

ÉVÉNEMENTS 1
EN DIRECT DES LABOS 2
RETOUR SUR LES JOURNÉES SSLR 3
RETOUR SUR LES JOURNÉES SDM 4
LE COIN PROSPECTIF 6
ÉVÉNEMENTS 7
JOBS 8

Événements

(Repris en partie du forum du GDR)

Biométrie sur France Culture *A ré-écouter : l'équipe de la Méthode Scientifique a reçu des collègues du GREYC et du LISSI. Émission du 15/01.*

Virus informatiques sur France Culture *A ré-écouter : l'équipe de la Méthode Scientifique a également reçu des collègues du LORIA. Émission du 05/02.*

Journées Journée autour des Attaques par Injection de Fautes (JAIF) *Paris, France, 18 mars 2020*

Conference Yet Another Conference on CRYPTography and Embedded Devices (YACCRYPTED) *Ile de Porquerolles, 11-15 mai 2020, soumissions avant le 16 février*

Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI) *Nouan-le-Fuzelier, France, 18-20 mai 2020*

Symposium sur la sécurité des technologies de l'information et des communications (SSTIC) *Rennes, France, 3-5 juin 2020*

Conférence Software Attacks and Defenses (SAD) *Genova, Italie, 19 juin 2020, soumissions avant le 28 février*

Suite en dernière page

En direct des labos

Loïc Lagadec

La gazette interview Loïc Lagadec, professeur au Lab-STICC (UMR 6285), le Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance, qui est présent sur les villes de Brest, Quimper, Lorient et Vannes. Plus de 40 chercheurs du laboratoire qui travaillent sur le sujet de la cybersécurité et la cyber défense.

Bonjour Loïc, quels sont les objectifs scientifiques du LAB-STICC en matière de sécurité informatique ?

La recherche en cyber sécurité du Lab-STICC couvre naturellement un spectre large, du fait même du positionnement du laboratoire (« des capteurs à la connaissance ») et de la diversité du domaine. Le laboratoire a cependant choisi de se spécialiser sur un ensemble de thématiques et sur trois domaines d'applications. En termes de thématiques, le Lab-STICC concentre en effet ses efforts sur :

- les approches issues du génie logiciel de type *secure by design* pour les composants et pour les systèmes de systèmes ;
- les facteurs humains appliqués à la gestion de crise cyber, incluant les interactions humain-systèmes immersives dans les contextes de cyber sécurité ou l'aide à la décision d'opérateurs de surveillance du cyber espace ;
- les architectures matérielles et systèmes embarqués sécurisés, la sécurisation des communications (IoT ou spatiales, par exemple), l'intégrité des capteurs ainsi que la résilience des réseaux d'accès ou des réseaux de télécommunications.

En termes de domaines d'application le Lab-STICC travaille plus particulièrement sur la cyber maritime, l'industrie du futur (résilience des systèmes SCADA et sécurisation des réseaux d'accès) et les réseaux de télécommunications.

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

Le Lab-STICC est membre du Pôle d'Excellence Cyber (PEC) depuis sa création en 2014. Le laboratoire contribue également très fortement à la chaire de cyber défense des systèmes navals qui regroupe l'Ecole Navale et deux tutelles du laboratoire, IMT Atlantique et l'ENSTA Bretagne (depuis 2019), ainsi que deux partenaires industriels : Thales et Naval Group. La sécurité a toujours été une préoccupation dans l'industrie navale : il s'agit en premier lieu d'assurer la sécurité des équipages mais aussi de transporter le fret à destination sans perte de marchandises, qui peuvent être dangereuses (déchets nucléaires, produits chimiques ou pétroliers, en particulier). Enfin, une large proportion (environ 90 %) du volume du commerce mondial (pétrole, céréales et autres biens vitaux pour les industries et les personnes) transite par mer.

« La sécurité a toujours été une préoccupation dans l'industrie navale... »

Le Lab-STICC est également impliqué, via IMT Atlantique, dans la chaire Cyber CNI (Cyber sécurité des Infrastructures critiques) créée en 2016 et dédiée à la vulnérabilité des systèmes critiques face aux menaces de cyber sécurité (analyse des risques, métriques, remédiation et gestion sécurisée des données).

Le Contrat Plan Etat Région Cyber-SSI (2015-2020), coordonné par deux E/C membres du Lab-STICC a un projet scientifique structuré en cinq sous projets.

Cyber-Crypto adresse la sécurité matérielle et la conception de composants dédiés au calcul homomorphe. *Cyber-Algo* est centré sur la conception d'algorithmes et de dispositifs pour l'investigation et la confidentialité. *Cyber-Ubiquitous* traite de méthodes d'analyse de la sécurité des systèmes ubiquitaires (internet des objets). *Cyber-ICS* s'intéresse à la simulation de la cyber sécurité pour les systèmes industriels. Enfin, *Cyber-Elec* est axé sur la Simulation de la détection de défaillances des systèmes physiques face aux attaques de sécurité.

Le Lab-STICC a également mis en place des échanges en cyber au niveau international avec trois universités australiennes, dans le cadre plus général d'accords de coopération bi-nationaux, dans le domaine naval notamment.

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

Le Lab-STICC mobilise son expertise en cyber dans le cadre de plusieurs formations de niveau I (Bac +5). Ces formations peuvent soit se structurer autour d'un tronc commun généraliste, suivi d'une année de spécialisation, soit être intégralement dédiées à la cyber sécurité.

Dans la première catégorie, on retrouve la Formation d'Ingénieur Généraliste (FIG) d'IMT Atlantique, dont le programme s'inspire du guide métier d'architecte référent pour la partie des compétences concernant le métier d'ARSSI défini par l'ANSSI, ou encore, la formation Systèmes Numériques et Sécurité de l'ENSTA-Bretagne, qui correspond à une voie d'approfondissement et qui propose une approche systémique alliant télécommunications, circuits numériques, informatique et sécurité. Son objectif est de former des ingénieurs généralistes pour la conception de nouveaux systèmes communicants pour lesquels la sécurité est une priorité.

Deux masters, Ingénieur cyber défense et Ingénieur cyber sécurité du logiciel, portés par l'ENSIBS à Vannes

s'appuient également en partie sur l'expertise du Lab-STICC.

Loïc Lagadec.

Enfin, un tout nouveau mastère spécialisé, Cyber sécurité des Systèmes Maritimes et Portuaires accueillera sa première promotion à la rentrée 2020. Ce mastère s'appuie sur quatre écoles dont deux tutelles du Lab-STICC (IMT-A, ENSTA-Bretagne). Il répond à un besoin fort et formera des experts en cyber sécurité aptes à concevoir, défendre et opérer des systèmes spécifiques au domaine maritime et portuaire.

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

Un des axes de travail du Lab-STICC concerne les architectures de calcul sécurisées. Ces architectures sont prototypées sur FPGA, et potentiellement déployées sous forme de circuits ASIC. Elles sont programmables ou reconfigurables, et nécessitent donc la mise au point de chaines de programmation, de configuration, et d'exploitation. La sécurité vient des caractéristiques de l'architecture (hardware), des outils qui permettent de s'en servir (software), et d'une bonne articulation entre ceux-ci (HW/SW). Cette thématique est clé pour les prochaines années, et plusieurs thèses sont planifiées.

Une thèse, débutée en 2019, étudie des mécanismes matériels pour sécuriser la pile logicielle contre les principales attaques logiques par analyse de canaux cachés logiques (par exemple variabilité du temps d'exécution, défauts de cache, congestion sur les ressources partagées), et aussi contre les principales attaques physiques (observation et perturbation). Ces travaux visent la conception d'un démonstrateur sur FPGA à base de processeurs open-source disponibles.

« Une première thèse étudie des mécanismes matériels pour sécuriser la pile logicielle contre les principales attaques logiques par analyse de canaux cachés logiques [...] »

Nous ciblons un RISC 32 bits sans hiérarchie de cache pour des applications de type IOT. La robustesse et les performances de notre solution seront évaluées sur la plateforme d'analyse de la sécurité des composants électroniques disponible au Lab-STICC Lorient. L'exploitation du processeur reposera sur une bibliothèque logicielle de support minimal, et l'adaptation d'une chaîne de compilation (GCC, LLVM...). Enfin, le processeur sera doté de quelques primitives de sécurité (authentification, stockage sécurisé, mise à jour distante de firmware...) afin d'en évaluer les performances et la robustesse à des attaques types.

Une seconde thèse débutant en 2020 dimensionnera des IP spécifiques, à greffer au processeur pour des usages sécurisés. Par exemple, des overlays en phase de prototypages se traduisant par des eFPGA une fois fondue la puce ASIC. Ces travaux font suite à la thèse de T. Bollengier et une puce eFPGA sécurisé est en cours de livraison. Une deuxième implémentation envisagée correspond à une VM hardware de type "Simple Object Machine", avec pour objectif de favoriser l'exécution de langages dynamiques.

Merci Loïc pour ces nouvelles du Finistère, bonne continuation !

Article rédigé par Loïc Lagadec (IMT-Atlantique/Lab-STICC) et Patrick Bas, Contact : loic.lagadec@ensta-bretagne.fr

Retour sur les journées SSLR

Aina Rasoamanana, Olivier Levillain et Aurélien Francillon

Le groupe de travail Sécurité des Systèmes, des Logiciels et des Réseaux (SSLR) a proposé une journée thématique le 27 novembre dernier dans les locaux de l'ESIEA à Paris. L'objectif était de permettre à la communauté « sécurité des systèmes, des logiciels et des réseaux » de se retrouver pour échanger autour du thème de la sécurité du logiciel : « quels outils pour construire, valider, corriger et auditer la sécurité du code en prenant en compte l'évolution des attaques ? ». Environ 60 personnes étaient présentes.

Fréderic Besson (Inria/IRISA) a parlé de ses travaux autour de la sécurité des compilateurs. Il a proposé une notion de transformation de programme IFP (*Information-Flow Preservation*) qui garantit qu'un programme cible sera moins vulnérable aux attaques passives des canaux auxiliaires qu'un programme source.

Ryad Benadjila, Arnaud Ebalard et Patricia Mouy (ANSSI) ont travaillé sur la vérification formelle d'un parseur de certificats X.509. Leur outil, écrit en C, a été validé par FramaC pour garantir, dans un sens large, l'absence d'erreurs à l'exécution (RTE, *Runtime Error*).

Ils l'ont également testé avec 200 millions de certificats réels récupérés sur internet.

Sebastian Poeplau (Eurecom) a présenté ses travaux sur l'exécution symbolique, une technique populaire pour tester les logiciels et découvrir des vulnérabilités. Pour cela, la plupart des outils utilisent une représentation intermédiaire, qui sert ensuite à l'exécution symbolique. Son étude analysait l'impact de ces représentations intermédiaires sur les performance et l'expressivité des outils.

Ange Albertini de Google a parlé de ses travaux sur les formats de fichiers, en évoquant de nombreuses anecdotes liées au manque de rigueur dans la définition des formats de fichiers, un phénomène malheureusement toujours d'actualité dans les standards récents.

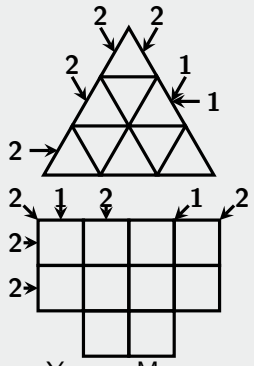
Stéphane Duverger et Éric Lacombe (Airbus) ont présenté deux exposés autour du *fuzzing*. Le premier traitait de l'automatisation de fuzzing d'OS embarqué à l'aide de Gustave, et présentait les nombreuses pistes envisagées par les chercheurs dans le monde pour résoudre ce problème. Le second concernait Fuddly, un *framework* de *fuzzing* et de manipulations de données, créé et utilisé dans le cadre de l'évaluation de la sécurité de systèmes avioniques.

Enfin, le langage de programmation Rust a été présenté par Pierre Chifflier (ANSSI) qui a indiqué des aspects de ce nouveau langage permettant de développer du code plus sécurisé.

Aina Rasoamanana, Olivier Levillain et Aurélien Francillon, Contact : olivier.levillain@telecom-sudparis.eu,aurelien.francillon@eurecom.fr

Mots (de passe) croisés

Chaque case de la grille contient un 0 ou un 1. Chaque chiffre indique le poids de Hamming (nombre de 1) dans la direction de la flèche. Trouvez les mots de passe stockés dans la mémoire ! (solution unique)



Jeu conçu et réalisé par Yoann Marquer, Contact : yoann.marquer@inria.fr

Retour sur les journées du GT SDM

Pauline Puteaux, William Puech

En partenariat avec le GDR ISIS (Information, Signal, Image et ViSion), le GT SDM (Sécurité et données multimédia) a organisé une journée autour des tendances en évaluation de la qualité pour la compression et la sécurisation des contenus émergents, à la DR01 (CNRS Villejuif). Cette journée visait les nouvelles approches d'évaluation de la qualité et de la confidentialité des données multimédia (image, stéréo, vidéo, maillage 3D, etc.) et leur exploitation dans les différentes applications.

En effet, de nombreux travaux de recherche sont dédiés au développement de mesures de qualité ou de confidentialité des données multimédia. Différentes approches ont été proposées dans la littérature avec une exploitation de plus en plus forte de méthodes basées sur l'apprentissage (SVM, ANN, Deep Learning, etc.). Ces méthodes trouvent naturellement différents champs applicatifs. À titre d'exemple, on peut citer leur utilisation pour la reconnaissance de personnes où l'objectif est de mesurer la fiabilité des données biométriques, ou bien encore l'imagerie médicale pour s'assurer des acquisitions réalisées.

Lors de ces journées, une attention particulière a été portée à la sécurité des données multimédia (tatouage, cryptographie, etc.) faisant intervenir l'évaluation du niveau de sécurité et/ou de la confidentialité visuelle. En effet, lors de ces journées, 4 des 10 présentations concernaient la sécurité des données multimédia. En termes de types de données multimédia manipulées, notons que 5 des 10 présentations se sont focalisées sur des données 3D et en particulier des maillages surfaciques ou des nuages de points, 2 sur les images, et 3 sur les vidéos dont 1 en stéréoscopie et 1 avec des scènes à 360-degrés.

La journée a été ouverte par une conférence invitée donnée par Sebastian Bosse du Fraunhofer HHI (Allemagne) intitulée *From psychophysics to distortion sensitivity with deep learning-based visual quality estimation : From models of quality and towards models of perception*.

Ces journées ont regroupé 45 personnes représentant les différents laboratoires travaillant dans ce domaine (LS2N, Nantes, LIRIS, Lyon, ARTEMIS, Paris, Greyc, Caen, PRISME, Orléans, XLIM, Poitiers, L3I, La Rochelle, LIRMM, Montpellier...) ainsi que de nombreux industriels (Thales, SAFRAN, VITEC, HUAWEI...). Les résumés des exposés sont disponibles à l'adresse suivante : http://www.gdr-isis.fr/index.php?page=reunion&idreunion=402

Pauline Puteaux et William Puech (LIRMM, Université Montpellier, CNRS), Contact : pauline.puteaux@lirmm.fr

Prix de thèse

Le Prix de thèse revient cette année, sponsorisé par le groupe Orange. Les candidatures sont à soumettre avant le 27 mars 2020 (23h59 heure de Paris).

Plus d'informations : https://gdr-securite.irisa.fr/prix-de-these/

Collaboration franco-allemande en cybersécurité

Un accord de partenariat sur la cybersécurité a été signé le 20 janvier dernier au Helmholtz Center for Information Security (CISPA) à Sarrebruck, entre Michael Backes, président et fondateur du CISPA et Pierre Mutzenhardt, président de l'Université de Lorraine, en présence des représentants du CNRS, d'Inria et des représentants politiques des régions Grand Est et de la Sarre.

Cet accord vise à renforcer ensemble les collaborations en matière de recherche en cybersécurité, ainsi que le transfert et l'innovation entre la France et l'Allemagne. En s'appuyant sur le CISPA et le Loria (CNRS, Inria et Université de Lorraine), cet effort commun vise à impulser la souveraineté numérique en Europe.

Cette coopération se matérialise aujourd'hui par la création de quatre chaires dans des domaines clés de la cybersécurité : cryptographie, vérification de protocoles, certification des objets connectés et respect de la vie privée. Cet accord est la première brique officielle de la construction d'un centre européen de recherche en cybersécurité, qui permettra à la France, à l'Allemagne et au reste de l'Europe de peser à l'échelle internationale et de relever de grands défis scientifiques.

Plus d'informations : https://factuel.univ-lorraine.fr/node/13325

Retour sur le FIC

Comme chaque année, le Forum International de la Cybersécurité a eu lieu en janvier à Lille. Contrairement aux années précédentes, cette édition s'est déroulée sur 3 jours, les 28, 29 et 30 janvier. Le GDR était présent sur le stand du CNRS, situé dans la « zone recherche » de l'Alliance Allistene. Au côté d'Olivier Cappé, directeur-adjoint scientifique de l'INS2I, se sont relayés Gildas Avoine, Patrick Bas et Jean-Yves Marion pour présenter les activités du GDR aux industriels, mais aussi aux jeunes, venus en nombre, pour se renseigner sur les possibilités de faire une thèse en sécurité.

La « zone recherche » de l'Alliance Allistene présente les activités de recherche de l'ensemble de la communauté académique de la sécurité informatique. Elle est structurée en 5 stands, CDEFI/CPU, CEA, CNRS, IMT et Inria, sur lesquels des chercheurs, enseignants-chercheurs et ingénieurs présentent des démos de leurs résultats de recherche, parfois valorisés à travers des start-up.

Parmi les autres stands importants du Forum, nous retiendrons les pôles régionaux (les Hauts de France et la Bretagne occupant chacun des stands très importants), ceux des institutions concernées (le Ministère de l'Intérieur et le Ministère des Armées), et les grandes entreprises à la pointe du domaine, qu'elles soient françaises ou étrangères. Une mention spéciale pour le stand de la société YesWeHack (peut-être aussi pour son bar en fin de journée), qui est une plate-forme similaire à Kaggle qui propose de mettre en contact les sociétés désireuses d'éprouver leur système informatique avec plus de 15 000 Hackeurs Éthiques (appelé des « Hunters » par la société), de façon officielle ou officieuse. Un système de récompenses est mise en place pour motiver les Hunters à déceler des failles dans les système.

Brève rédigée par Patrick Bas, Contact : Patrick.Bas@centralelille.fr

FIC 2020.

Le coin prospectif

María Naya-Plasencia

La gazette interview María Naya-Plasencia, DR Inria et lauréate 2019 du prix « Inria – Académie des sciences du jeune chercheur/de la jeune chercheuse ». María travaille sur la cryptanalyse quantique, sur la conception de primitives cryptographiques à bas coût et sur les fonctions de hachage. La gazette a décidé de la questionner sur son domaine de recherche en général et sur ses travaux en particulier.

Bonjour María, avant de rentrer dans le vif du sujet, peux-tu nous rappeler quels sont les principes de base de la cryptographie symétrique post-quantique ?

La cryptographie symétrique utilise la même clé pour chiffrer et pour déchiffrer l'information, tandis que la cryptographie asymétrique utilise deux clés différentes. Chacune des deux familles a ses avantages, et dans la plupart des cas on utilise des systèmes appelés hybrides qui combinent les deux. La cryptanalyse est l'étude de la sécurité des fonctions cryptographiques, et elle est indispensable pour pouvoir leur faire confiance et anticiper des problèmes causés par des attaquants. L'arrivée de l'ordinateur quantique, et donc l'existence d'attaquants avec accès à un ordinateur quantique, impliquerait que la plupart des primitives asymétriques couramment utilisées ne seraient plus sûres, et la communauté cherche très activement des remplaçants. Les effets sur la cryptographie symétrique actuelle sont moins nets, mais dans certains modèles, certaines primitives peuvent devenir dangereuses. Pour évaluer leur sécurité, on étudie les capacités de cryptanalyse des attaquants quantiques. La cryptographie symétrique post-quantique est donc une cryptographie symétrique sûre dans un monde où des attaquants ont des capacités quantiques.

> « Certaines primitives [symétriques] peuvent devenir dangereuses. »

Quel angle d'attaque peut-on choisir pour mettre à mal la sécurité d'un schéma de chiffrement ?

Il y a deux principaux scénarios considérés dans les attaques symétriques quantiques :

- le modèle où l'attaquant a accès à un ordinateur quantique mais où il ne peut réaliser que des requêtes classiques à la fonction cryptographique,

- et le modèle en superposition où l'attaquant, en plus d'avoir accès à un ordinateur quantique pour effectuer ses calculs, peut ainsi effectuer des requêtes avec des états superposés à l'oracle de chiffrement.

Les attaques du deuxième type sont évidement plus puissantes, et peuvent utiliser par exemple l'algorithme de Simon pour retrouver efficacement des périodes cachées. On peut ainsi cryptanalyser avec ces attaques certaines constructions sûres dans le monde classique avec une très faible complexité. Même si le modèle est moins réaliste, ces attaques sont à prendre en compte. Dans le premier modèle, on réussit à améliorer des familles de cryptanalyse classiques avec une accélération quadratique : connaître les meilleures attaques, qu'elles soient classiques ou quantiques, permet ainsi de déterminer la marge de sécurité de certaines primitives.

María Naya-Plasencia.

Penses-tu qu'il y aura des solutions de chiffrement post-quantique utilisables dans un avenir proche ?

Oui, je le pense. La communauté cryptographique dépense beaucoup d'efforts dans ce sens depuis des années, comme par exemple la compétition du NIST pour trouver des nouveaux standards post-quantiques [NDLR : voir également la gazette n°1 et l'interview de Philippe Gaborit].

Quels sont les challenges qui te semblent les plus intéressants dans ce domaine ?

Avoir une bonne connaissance de ce que les attaquants quantiques pourront faire est fondamental pour pouvoir bien mener à terme ces tâches. La cryptanalyse quantique, qui est en train de se développer de plus en plus, est très importante, elle est associée à un champ de recherche passionnant et indispensable.

> « La cryptanalyse quantique [...] est associée à un champ de recherche passionnant et indispensable. »

Quels conseils peux-tu donner aux jeunes chercheurs intéressés par la cryptographie ?

Une bonne façon de s'intéresser à ces questions est de regarder les compétitions actuelles du NIST : celle pour trouver des primitives post-quantiques et celle pour trouver des primitives à bas coût ; puis d'essayer de trouver des attaques. Ce sont des recherches très importantes, qui peuvent rapidement devenir captivantes. Il y a beaucoup à apprendre par rapport à la cryptanalyse quantique, donc c'est un très bon moment pour commencer à s'y intéresser.

Merci María, et bonnes continuations post-prix !

Article rédigé par María Naya-Plasencia (DR Inria au sein du projet Equipe Secret), Annelie Heuser et Patrick Bas, Contact : maria.naya_plasencia@inria.fr

Événements

(Repris en partie du forum du GDR)

Journées Codage & Cryptographie (C2) *Erdeven, France, reportées à une date ultérieure*

Journée du GT SSM sur l'apprentissage automatique pour l'analyse des canaux cachés *Lyon, France, 16 avril 2020*

Conférence Computer Security Foundations Symposium *Boston, États-Unis, 22-25 juin 2020*

Atelier sur la Protection de la Vie Privée (APVP) *Saint-Martin-de-Londres (Languedoc), 24-26 juin 2020*

Conférence Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) *Lisbonne, Portugal, 24-26 juin 2020, soumissions avant le 16 février*

Summer School on Training And Research On Testing (TAROT) *Porto, Portugal, 6-10 juillet 2020*

Journées nationales du GDR Sécurité Informatique *Paris, 1-3 juillet 2020*

International Workshop on the Arithmetic of Finite Fields (WAIFI) *Rennes, France, 6-8 juillet 2020*

École d'été du GDR Sécurité Informatique *Gif-sur-Yvette, 6-10 juillet 2020*

Conférence Africacrypt *Le Caire, Égypte, 20-22 juillet 2020, soumissions avant le 1er février*

Rencontres Entreprises-Doctorants en Sécurité (REDOCS) *Gif-sur-Yvette, 26-30 octobre 2020*

Club des partenaires indutriels du GDR

Le GDR ambitionne de renforcer les liens entre les communautés académique et industrielle dans le domaine de la sécurité informatique. Ce n'est pas un objectif vain, bien au contraire, les collaborations entre ces deux communautés sont nombreuses et bénéficient de dispositifs variés pour faciliter leur mise en place. Le GDR vise à améliorer la connaissance que les entreprises ont des laboratoires académiques, qui constituent une vraie richesse nationale trop peu exploitée, mais le GDR vise également à aider les entreprises pour leur veille technologique, à les mettre en relation avec des doctorants arrivant sur le marché du travail, à les rapprocher de potentiels collaborateurs académiques et industriels pour le montage de projets, etc.

Pour cela, le GDR a souhaité se doter d'un *Club de partenaires industriels*, qui est officiellement ouvert à l'adhésion depuis le 1er janvier 2020. Le Club vise à rassembler des entreprises qui mènent des activités de recherche et développement en sécurité informatique. La gouvernance du Club est confiée à ses membres, sous la responsabilité de la direction du GDR. Il est attendu des membres du Club qu'ils soient force de proposition pour mettre en place des actions à mener en collaboration avec la communauté académique. La réussite du Club dépend donc de l'implication de ses membres et de leur volonté à tirer profit de cet outil mis à leur disposition. L'adhésion est conditionnée au paiement d'une cotisation pour permettre le financement des actions que le Club décidera de mettre en place, par exemple des journées thématiques, la participation aux REDOCS, des événements de réseautage, le prix de thèse, etc. Olivier Bettan (Thales) et Fred Raynal (Quarkslab), participants de la première heure aux activités du GDR, ont été chargé de mettre en place le Club et ses premières activités, qui devraient avoir lieu au printemps.

À l'heure où nous publions cette cinquième édition de la Gazette, trois entreprises ont déjà rejoint le Club du GDR : Orange, Attox.io et Almerys. Orange sera par ailleurs le parrain du prix de thèse 2020.

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 des postes, mais il est contenu dans les fiches de postes de toutes les annonces listées.

Professeur en informatique (Caen)
ENSICAEN, GREYC (UMR 6072)
Info : R. Clouard, S. Malo (enseignement), Ch. Charrier, Ch. Rosenberger (recherche)

Professeur en cybersécurité (Rennes)
IMT Atlantique, IRISA (UMR 6074)
Info : https ://tinyurl.com/job-001

MC en informatique (Aix-Marseille)
Université d'Aix-Marseille, LIS (UMR 7020)
Info : Y. Vaxès, P-A Reynier (recherche), J-M Talbot (enseignement)

MC en informatique (Aurillac)
Université Clermont Auvergne, LIMOS (UMR 6158)
Info : https ://tinyurl.com/job-003

MC en informatique (Coëtquidan)
Écoles de St-Cyr Coëtquidan (Ministère des Armées)
Info : https ://tinyurl.com/job-004

MC en informatique (Grenoble)
Grenoble INP - Ensimag / Verimag (UMR 5104)
Info : https ://tinyurl.com/job-005

MC en Cryptologie et sécurité de l'information (Paris)
Sorbonne Université, LIP6 (UMR 7606)
Info : https ://tinyurl.com/job-002

MC en informatique (Valence)
Grenoble INP - Esisar, LCIS
Info : Oum-El-Kheir Aktouf (enseignement) et V. Beroulle (recherche)

Enseignant-chercheur en informatique et cybersécurité (Noisy-le-Grand)
ESIEE, LIGM (UMR 8049)
Info : https ://tinyurl.com/job-006

Enseignant-Chercheur en vérification ou analyse du logiciel de systèmes cyber physique (Saclay)
Télécom Paris, LTCI
Info : https ://tinyurl.com/job-007

Chaire (MC) de recherche en Cybersécurité (Paris)
Institut des hautes études de défense nationale
Info : Françoise Levy-dit-Vehel

Chaire (MC) d'enseignement et de recherche en Cybersécurité (Rennes)
CentraleSupélec, Inria RBA / IRISA (UMR 6074)
Info : Valérie Viet Triem Tong, Christophe Bidan

Postes Inria
Les centres de Paris, Rennes et Saclay affichent explicitement la sécurité dans les profils recherchés.
Info : https ://tinyurl.com/job-008

PostDoc ou ingénieur de recherche, IRISA (Rennes)
Sujet : malware analysis through side-channel information
Contact : Annelie Heuser

PostDoc, Laboratoire Hubert Curien (Saint-Étienne)
Titre : sécurité des systèmes matériels
Contact : Lilian Bossuet

Thèse de doctorat, IETR (Rennes)
Sujet : Mitigating coupled information leakages in mixed-signal reconfigurable SoCs
Contact : Rubén SALVADOR, Amor NAFKHA, et Maxime PELCAT

Offre de stage, EDF R&D Saclay (Palaiseau)
Titre : Sécurité des mécanismes de mise à jour logicielle
Contact : Frédéric Silvi, frederic.silvi@edf.fr

Offre de stage, SiFive France (La Ciotat)
Sujet : l'implémentation des algorithmes cryptographiques post-quantiques
Contact : Yann LOISEL, yann.loisel@sifive.com

Équipe éditoriale

Directeurs éditoriaux :
- Patrick Bas, *CRIStAL, CNRS*
- Annelie Heuser, *IRISA, CNRS*

Responsables de la production :
- Solène Bernard, *CRIStAL, CNRS*
- Céline Chevalier, *CRED, Univ. Paris 2*

Directeur de publication :
- Gildas Avoine, *IRISA, INSA Rennes*