Avril 2019
Numéro 2

LA GAZETTE DU GDR

Sécurité Informatique - GDR2046

Édito du directeur

L'actualité du GDR est dense, et c'est un vrai plaisir de la partager avec vous à travers ce deuxième numéro de la Gazette, préparé par Patrick Bas, Annelie Heuser et Solène Bernard. La première nouveauté est liée à l'édition de la Gazette, avec la création d'un modèle en LaTeX. Un grand merci à Céline Chevalier (Paris 2, CRED) qui a ainsi fait profiter la communauté de ses compétences.

Une évolution majeure du GDR – précédemment annoncée mais dont la mise en place vient d'avoir lieu – est la création du GT *Sécurité des Systèmes, des Logiciels et des Réseaux* (SSLR), qui résulte de la fusion des précédents groupes de travail sur les systèmes logiciels d'une part et sur les réseaux d'autre part. Les Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI) profitent de cette évolution pour devenir un événement à part entière du GT SSLR.

Du côté des événements, les inscriptions aux Journées Nationales (CNAM Paris, 12-14 juin) sont ouvertes ! Le programme des séances plénières est d'ores et déjà en ligne sur le site web du GDR.

Les GT sont également très actifs. En ce début d'année, le GT *Méthodes Formelles pour la Sécurité* a organisé une journée de travail (76 participants) sous la houlette de Pierre-Yves Strub à Paris, au CNRS (Michel Ange). Parmi les prochains événements à venir dont les inscriptions sont ouvertes, il y a RESSI 2019 (GT SSLR) et APVP (GT PVP). Quant au GT C2, il a mis en place les très attendus séminaires éponymes dont les premières éditions ont eu lieu à Paris (LIP6) et à Rennes (IRMAR).

Après ces quelques mots sur la vie du GDR, je vous souhaite une bonne lecture de ce numéro 2, où vous retrouverez notamment un focus sur les activités de Florent Retraint (UTT, LM2S), une interview de Davide Balzarotti (EURECOM), et un *Retour sur le FIC* du groupe de travail *Cybersécurité* de l'alliance Allistene.

Gildas Avoine

Rubriques

Événements

(Repris en partie du forum du GDR)

Conférence "13th IFIP WG 11.11 International Conference on Trust Management" *Copenhague (DK), 17- 19 juillet 2019, soumission : 9 avril*

Conférence "8th International Workshop on Security Proofs for Embedded Systems" *Atlanta (USA), 24 août 2019, soumission : 31 mai*

Conférence "11th IEEE International Workshop on Information Forensics and Security" *Delft (PB), 9–12 décembre 2019*

L'école thématique "architecture des systèmes matériels et logiciels embarqués, et méthodes de conception associées (ARCHI)" *Lorient (FR), 20-24 mai 2019, inscription : 20 avril*

Conférence "5th International Symposium on Security and Privacy in Social Networks and Big Data" *Copenhagen (DK), 14-17 juillet 2019*

École d'été "Real-world crypto and privacy" *Šibenik (HR), 17-21 juin 2019*

Conférence "The 17th International Conference on Service-Oriented Computing" *Toulouse (FR), 28-31 October 2019, soumission : 10 mai*

Conférence "16th IEEE International Conference on Advanced and Trusted Computing" *Leicester (UK), 19-23 août 2019*

Événement labellisé par le GDR : Journée "Injection de fautes : attaques physiques, protections matérielles et logicielles, et mécanismes d'évaluation de la robustesse" *Grenoble (FR), 23 mai 2019*

École d'été du GDR

L'école d'été du GDR Sécurité Informatique aura lieu du 8 au 12 juillet 2019 à Rennes et son thème portera sur la sécurité des interfaces matérielles et logicielles. L'école sera cette année organisée par Clémentine Maurice (CNRS) et Frédéric Tronel (CentraleSupélec). Cette édition est organisée dans le cadre du semestre thématique sur la sécurité des interfaces matérielles et logicielles, financé par la DGA-MI, opéré par Inria pour le compte des partenaires académiques du PEC, et dont le porteur est Guillaume Hiet (CentraleSupélec).

En direct des labos

Florent Retraint

La Gazette interview Florent Retraint, professeur à l'Université Technologique de Troyes, spécialiste en sécurité de l'information et notamment en détection de manipulations sur des images. Florent participe actuellement au Challenge DEFALS, organisé par l'ANR et la DGA (`www.defals.fr`).

Bonjour Florent, quels sont les enjeux liés à la détection d'images manipulées et plus particulièrement au Challenge DEFALS ?

S'il est relativement aisé de produire une image falsifiée en apparence intègre à partir d'une image d'origine, il devient extrêmement difficile de détecter les retouches apportées à une image sans disposer de l'image originale. Le développement d'outils fiables et automatisés permettrait de lever le doute sur une information qui peut :

- Porter préjudice à une personne physique (ex. : ajout d'éléments compromettants à une photographie personnelle) ;
- Modifier l'examen d'un justiciable (ex. : changement de plaques minéralogiques, pédophilie) ;
- Créer un faux événement (ex. : enrichissement de données à des fins de propagande) ;
- Porter un préjudice économique à une société ou un organisme (ex. : retouche d'images de presse, canular industriel).

L'objectif principal du challenge DEFALS financé par l'ANR est de réaliser un système d'analyse permettant la détection automatisée des modifications apportées à des images.

> « Une zone falsifiée a généralement des propriétés statistiques différentes du reste de l'image. »

Quelles sont les différents moyens de détecter la manipulation d'images ?

Les méthodes de falsification d'une image sont très nombreuses et les méthodes permettant de les détecter le sont également. Dans le cas des images au format JPEG (format le plus répandu), il existe des méthodes travaillant dans le domaine fréquentiel et dans le domaine spatial. Les premières cherchent à détecter des incohérences dans les valeurs des coefficients DCT [1] introduites par la falsification. Les méthodes les plus répandues travaillent dans le domaine spatial. On peut notamment citer les méthodes basées sur le bruit présent dans les images. Une zone falsifiée a généralement des propriétés statistiques différentes du reste de l'image. Il est également possible d'étudier la corrélation entre les différents canaux de couleur de l'image.

Florent Retraint

Quels sont les problèmes plus difficiles ?

La difficulté majeure est d'arriver à distinguer une falsification d'une simple modification. En effet, une personne peut agrandir ou changer la luminosité de son image sans intention malveillante. Elle peut également falsifier son image et ensuite changer différents paramètres de cette image. Dans ce cas de figure, la détection de la falsification peut devenir très difficile.

Et en terme de valorisation, que peut-on envisager actuellement dans ce domaine ?

Un enjeu, qui intéresse certains industriels, est la détection de la falsification des papiers d'identité. Par exemple, les forces de sécurité sont intéressées par la détection d'un morphing, c'est-à-dire la combinaison de plusieurs visages pour n'en former qu'un seul. En effet, par cette technique, plusieurs individus peuvent envisager de passer la sécurité avec le même passeport.

Merci Florent, et bonne chance pour la suite du challenge Defals !

Contact: `florent.retraint@utt.fr`

1. Transformée en Cosinus Discrète.

Retour sur le FIC

Isabelle Chrisment, Olivier Cappé

Le Forum International de la Cybersécurité (FIC) s'est déroulé les 22 et 23 janvier 2019 à Lille où il est organisé depuis 2007 par le CEIS (Compagnie Européenne d'Intelligence Stratégique), avec le soutien de la Gendarmerie nationale et de la Région Hauts-de-France. Le FIC est un événement important au niveau européen qui a pour ambition de réunir l'ensemble des parties prenantes de l'économie numérique concernées par la cybersécurité pour[2] :

- *Décloisonner* les enjeux de la cybersécurité en réunissant des acteurs concernés au sein des organisations ;
- *Accélérer* le développement d'un marché européen de la cybersécurité ;
- *Promouvoir* une vision équilibrée et éthique de la sécurité ;
- *Favoriser* l'innovation dans la confiance numérique en accueillant les projets innovants et start-up ;
- *Construire* une approche inclusive de la cybersécurité dans la transformation des organisations ;
- *Fédérer* les écosystèmes en créant des ponts entre les sphères publiques et privées entre le secteur industriel et le milieu académique, entre le monde fonctionnel et les "métiers".

Le FIC a confirmé son succès cette année en accueillant prés de 10 000 participants (+15% par rapport à l'édition 2018) et 400 partenaires exposants. L'accès au forum est gratuit pour les visiteurs et, en plus des différents stands, le programme comporte des séances plénières, des conférences partenaires, des ateliers et démonstrations techniques ainsi que des exposés à vocation pédagogique (master classes). La thématique de l'édition 2019 du FIC était la *Security & privacy by design* : comment construire une sécurité native, pensée et intégrée non seulement dès la conception des produits et des services mais aussi durant tout leur cycle de vie via une sécurité plus dynamique prenant en compte l'évolution des menaces ?

2. https://www.forum-fic.com
3. https://www.allistene.fr

Un mystérieux logo...

Depuis Janvier 2019, le GDR Sécurité Informatique a un nouveau logo. Cette nouvelle identité visuelle officialise la création du GDR par le CNRS. Ce nouveau logo a été créé par Sophie Navas (https://www.sophienavas.fr/) . Il vise à symboliser les différentes thématiques du GDR qui vont de l'analyse de binaires, jusqu'à la cryptographie en passant pas la protection des données et des systèmes symbolisée par le bouclier. Comme de nombreux logos liés à la sécurité, il contient de nombreux mystères, par exemple pencher la tête vers la droite vous aidera à trouver un symbole de la sécurité !

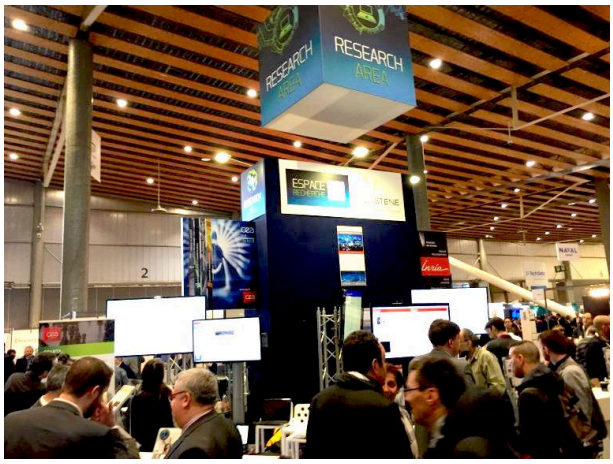
« Le FIC a confirmé son succès cette année en accueillant prés de 10 000 participants. »

Depuis trois ans, le groupe de travail Cybersecurité de l'alliance Allistene[3] (Alliance des sciences et technologies du numérique) participe à l'organisation du FIC, afin de faciliter les échanges entre les académiques et les représentants industriels ou institutionnels (ministères, régions, élus) qui représentent la très grande majorité des participants du forum.

La contribution d'Allistene se traduit concrètement par la présence d'un espace recherche identifié qui regroupe les établissements représentés dans l'alliance Allistene : CEA, CNRS, CDEFI/CPU, Institut Mines-Télécom et Inria. Cet espace recherche constitue un point de rencontre pour les participants académiques au FIC et il permet de présenter plus largement des activités de recherche issues des laboratoires.

En 2019, sur les deux jours, plus de vingt-cinq démonstrations ont été présentées par des chercheurs, enseignants-chercheurs ou ingénieurs de recherche, mettant en exergue le spectre large des recherches académiques en cybersécurité : de la confidentialité des données et des techniques d'anonymisation à la détection des attaques et la mise en place de contremesures, en passant par l'évaluation de code contre l'injection de

fautes ou la sécurité matérielle. Plusieurs startups valorisant des travaux issus des laboratoires étaient également présentes sur les stands de l'espace recherche. Compte tenu de l'hétérogénéité des participants du FIC, la présentation sur l'espace recherche requiert un effort de pédagogie mais permet de s'adresser à un public très varié.



Espace Recherche FIC'19. (Crédit : Claude Labit)

Allistene propose également des intervenants et des sujets pour les master classes, qui sont des sessions pédagogiques de 45 minutes sur des sujets plus orientés recherche. En 2019 sont intervenus dans ce cadre Karthikeyan Bhargavan (Inria Paris), Jean-Yves Marion (LORIA), Caroline Fontaine (LSV) ainsi qu'Allan Blanchard (Inria Lille) et Nikolai Kosmatov (CEA List).

Cette année ont également été organisés deux ateliers Franco-Japonais, animés par Hervé Débar (Télécom SudParis), coordinateur du projet euro-japonais H2020 EUNITY. Le premier atelier abordait la problématique de la Cybersécurité des grands événements, notamment sportifs, avec l'approche des Jeux Olympiques de Tokyo en 2020 et ceux de Paris en 2024. Le deuxième atelier, plus en lien avec la thématique du FIC 2019, s'est focalisé sur la cybersécurité « by design » et les objets connectés.

Le FIC 2019 a également donné lieu à la présentation, en présence du PDG d'Inria, Bruno Sportisse, du livre blanc Inria sur la cybersécurité, coordonné par Steve Kremer, Ludovic Mé, Didier Rémy et Vincent Roca. Ce livre blanc [4] fait le point sur les thématiques et les activités de recherche des équipes projets Inria dans le domaine de la cybersécurité.

Enfin, le GdR sécurité était également présent sur l'espace recherche et y a notamment distribué des exemplaires du premier numéro de la gazette.

L'édition 2020 du FIC étant d'ores et déjà en préparation, n'hésitez pas à contacter les membres du groupe de travail Cybersecurité [5] de l'alliance Allistene si vous êtes intéressés par le sujet.

Article rédigé par Isabelle Chrisment (TELECOM Nancy, LORIA) et Olivier Cappé (CNRS, DI ENS) pour le GT Cybersécurité d'Allistene, Contact: isabelle.chrisment@loria.fr,olivier.cappe@ens.fr

Le coin prospectif

Davide Balzarotti

Davide Balzarotti est professeur au département "sécurité numérique" de l'institut Eurecom, et il est lauréat d'une bourse ERC. Ses recherches couvrent divers aspects de la sécurité des systèmes et des logiciels, avec un intérêt particulier sur l'analyse de binaires et de malwares, sur la rétro-ingénierie et sur la sécurité du web. Pour plus de facilité, la gazette a interviewé Davide dans la langue de Shakespeare.

Hello Davide, can you explain to us how and why you came to the field of binary and malware analysis ?

I got into binary analysis for fun, by playing the Defcon Capture the Flag competitions with the Shellphish team during my Ph.D. For few years that remained just a hobby, as my research at the time focused mostly on intrusion detection and web security. I actually started doing research on malware analysis when I moved back to Europe, because our group was involved into running and maintaining Anubis (one of the first online malware dynamic analysis sandboxes), which provided us with a quite unique dataset of malicious samples to play with.

« Dynamic analysis is our best weapon to study and understand malware. »

Which recent attacks do you consider the most dangerous and which do you find the most interesting from a research perspective ?

Hard to pick one as there are plenty of worrying trends everywhere – from the shift towards more targeted and server-oriented ransomware, to the risk of a compromised supply chain. On the analysis side, I am particularly worried about the increasing diversity of target platforms. Malware for IoT is still in its puberty, but once it will reach the complexity of its Windows

4. PDF :https://files.inria.fr/dircom/extranet/LB_cybersecurity_WEB.pdf
e-pub : https://files.inria.fr/dircom/extranet/livre_blanc_cybersecurite.epub
HTML : https://files.inria.fr/dircom/extranet/livre_blanc_cybersecurite/livre_blanc_cybersecurite.html
5. https://www.allistene.fr/organisation-allistene/groupes/groupe-cybersecurite/

counterpart it will be hard to maintain an analysis infrastructure comparable to what we developed in the past decade for windows executables. Dynamic analysis is our best weapon to study and understand malware, and we all know how difficult it is to perform dynamic analysis of software for embedded systems.

Davide Balzarotti

Which detection methods do you believe have the most impact in future ?

Malware is a very generic term, which makes malware detection a complex and multifaceted problem. Any generic solution falls short one way or another and therefore I believe we will see more and more integrated, multi-layered approaches. For instance, the detection of ransomware and cryptominers required dedicated techniques, which are designed for a specific class of malicious software. And then there is the urge of throwing a bit of ML and deep learning everywhere, hoping it will improve malware analysis and detection the same way it helped image and audio recognition. While I am optimistic that deep learning will prove itself useful in the right circumstances, the adversarial nature of malware analysis and detection complicates their application. For the time being, it looks more like researchers are still running around with a hammer looking for a nail.

Can you tell us a bit more about your latest ERC grant, in which directions will you be researching in ?

My ERC grant (named BitCrumbs) focuses on improving the analysis of compromised devices. This of course includes new research in the area of malware analysis, but it also covers computer forensics, in particular on the memory analysis side. The plan is also to work on traditional computers as well as developing new analysis techniques for IoT and embedded devices.

« The most common mistake is simply not to try. »

Any advice you can give to future ERC applicants ?

The most common mistake is simply not to try. It undeniably requires a considerable amount of work to put together a good application and I heard too many times talented researchers postponing it from one year to the next because they do not find time and they believe the chances of getting funded are very low anyway. The second mistake is to just recycle some text that one has already lying around to save time and hack together a quick proposal. My advice to applicants is instead to avoid shortcuts and invest the necessary time : it is a demanding task but believe me, it is worth every minute you invest in it. In fact, too often researchers jump from one paper to the next, with little vision of what they want to achieve in the long term. An ERC application forces you to spend some weeks thinking how to put everything you do into context and developing a logical research plan. Even if the proposal is not funded, the process itself is still an incredibly useful experience

Thanks for these precious advices Davide ! Best wishes !

Contact: davide.balzarotti@eurecom.fr

Vie du GdR

Fusion de 2 groupes de travail

Après plusieurs années d'existence, les groupes de travail thématiques SRI (Sécurité des Réseaux et Infrastructures) et SSL (Sécurité des Systèmes Logiciels) ont fusionné pour donner naissance au groupe de travail Sécurité des Systèmes, Logiciels et Réseaux (SSLR). Cette fusion répond à la volonté du GDR de s'adapter à l'évolution de la communauté scientifique. À l'automne dernier, les GT SRI et SSL avaient déjà partagé une journée thématique à EURECOM.

Le groupe de travail fusionné sera animé par Aurélien Francillon et Olivier Levillain. Carlos Aguilar Melchor (ancien responsable du GT SRI) et Jean-Yves Marion (ancien co-responsable du GT SSL avec Aurélien Francillon) ont été invités dans le bureau pour aider à assurer la transition.

Le GT SSLR a pour ambition de s'intéresser à une approche holistique de la sécurité, de prendre en compte et de combiner plusieurs approches pour s'intéresser à la sécurité de systèmes complexes. Cette démarche passe à la fois par un point de vue vertical (des couches logicielles de plus haut niveau jusqu'à l'interface avec le matériel) et par un point de vue horizontal cherchant à couvrir toutes les plateformes (les infrastructures classiques, les *smartphones*, les systèmes cyber-physiques, les systèmes de contrôle industriel, les objets connectés,

le *cloud computing*...).

Pour appréhender la sécurité des systèmes, logiciels et réseaux de manière globale, il est également important de s'intéresser aux interactions entre différents domaines de la sécurité informatique : logiciel/matériel, systèmes/réseaux, utilisation de la cryptographie, etc.

Les sujets de recherche couverts par ce GT vont de la conception de systèmes sécurisés à l'analyse de systèmes existants, en passant par la modélisation des menaces et l'étude de nouveaux paradigmes et techniques.

Organisation du GT SSLR

Responsables
Aurélien Francillon, *EURECOM*
Olivier Levillain, *Télécom SudParis, SAMOVAR*

Bureau
Carlos Aguilar Melchor, *ISAE Supaero*
Sébastien Bardin, *CEA LIST*
Olivier Festor, *Télécom Nancy, LORIA*
Jean Leneutre, *Télécom ParisTech, LTCI*
Jean-Yves Marion, *Université de Loraine, LORIA*
Ludovic Mé, *Inria*
Vincent Nicomette, *INSA Toulouse, LAAS*
Melek Önen, *EURECOM*
Marie-Laure Potet, *G-INP, Vérimag*
Sarah Zennou, *Airbus*

Conférence
RESSI

Les rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI) constituent un événement scientifique qui a pour objectif de regrouper et d'animer la communauté francophone de la recherche académique et industrielle ainsi que celle de l'enseignement relatif à la sécurité des réseaux et des systèmes d'information.

RESSI, dont la première édition a eu lieu en 2015. est une émanation de la conférence SAR-SSI (Sécurité des Architectures Réseaux et des Systèmes d'Information). Cette année, RESSI devient l'un des événements du groupe de travail SSLR (sécurité des systèmes, logiciels et réseaux, voir ci-dessus).

Comme tout événement du GDR, RESSI n'a pas pour objectif la publication de contributions originales, mais est un lieu de rencontre et d'échange entre enseignants-chercheurs. La spécificité de RESSI est liée à la richesse de son programme :

- des tutoriaux sur les paradigmes émergeants ;
- des présentations autour de l'enseignement ;
- des présentations courtes et une session posters pour les doctorants et doctorantes en SSI ;
- la présentation de projets collaboratifs d'envergure régionale, nationale ou européenne ;
- une table ronde permettant la rencontre entre acteurs institutionnels, industriels et académiques ;
- un *challenge* de sécurité ;
- le rejeu de communications et de soutenances de thèse de l'année passée.

Après Troyes, Toulouse, Grenoble et Nancy, la cinquième édition se déroulera du 15 au 17 mai prochain en Bretagne. Elle sera organisée par Inria, et les responsables du comité de programme sont Grégory Blanc et Olivier Levillain (Telecom SudParis, SAMOVAR). Le programme et les modalités d'inscriptions sont disponibles sur le site de la conférence (https://ressi2019.sciencesconf.org/).

Jobs

(Repris en partie du forum du GDR)

PhD, IRISA, Vannes, France

Title : Intrusion Detection and Zero Day Attacks by Tracking Sequences of System Calls, keywords : Intrusion detection ; Anomaly Detection ; Sequence of system calls ; Zero day attacks ; Massive sequential data.
Contact : Pierre-François Marteau, pierre-francois.marteau@univ-ubs.fr,

PostDoc, Inria Nancy Grand Est

Identifying and Breaking IoT Intrusion Chains, date limite : 5 juin 2019.
Contact : Jérôme François, jerome.francois@inria.fr

Maître-assistante(e) en cybersécurité, IMT Lille Douai

Spécalité : cybersécurité, date limite : 30 avril 2019.
Contact : Gregory Blanc, gregory.blanc@telecom-sudparis.eu

PostDoc, L3i lab, University of La Rochelle

Spécalité : Computer Science/ Image Processing/ Document Analysis/ Pattern Recognition. Durée : 12 moins, disponible : avril/mai 2019.
Contacts : Mickael Coustaty, Petra Gomez, mickael.coustaty@univ-lr.fr, petra.gomez@univ-lr.fr

PostDoc, Sorbonne University, LIP6, Paris

Sujet : hardware implementation of Elliptic Curve Method on FPGA.
Contact : Roselyne CHOTIN, Roselyne.Chotin@lip6.fr

Thèses de doctorat, IRISA, Rennes

L'équipe EMSEC de l'IRISA propose régulièrement des sujets de thèse en cybersécurité. En ce moment, une proposition sur les protocoles de communication sécurisée et une autre sur les compromis temps-mémoire cryptanalytiques. La date limite de candidature pour le premier sujet est le 18 avril.
Contact : Gildas Avoine, gildas.avoine@irisa.fr

Stagiaire de Master 2 (ou M1), Télécom SudParis (Evry)

Sujet : Sécurité et attaques réseaux. Le stage se déroulera à Télécom SudParis (Evry), pour une durée de 4 à 6 mois.
Contact : Olivier Levillain, olivier.levillain@telecom-sudparis.eu

Stagiaire de Master 2, LaBRI à Bordeaux, L3I à La Rochelle, et du XLIM à Limoges

Sujet : Détection de fraudes, protection des données privées, sécurisation des communications.
Contacts : Akka Zemmari, Petra Gomez, zemmari@labri.fr, petra.gomez@univ-lr.fr

Stagiaire de Master 2/ élève-ingénieur de troisième année, l'École des Mines de Saint-Etienne

Sujet : Amélioration de la sécurité du système AIS (Automatic Identification System) par ajout de dispositifs informatiques et/ou électroniques.
Contact : Pierre Barthelemy, p.barthelemy@univ-amu.fr