Juillet 2019
Numéro 3

LA GAZETTE DU GDR

Sécurité Informatique - GDR2046

Édito du directeur

À lire au bureau ou sur la plage, voici la troisième édition de la Gazette du GDR. La saison pré-estivale est généralement riche en évènements, et le GDR Sécurité ne déroge pas à la règle. Ainsi, pas moins de quatre évènements majeurs du GDR ont été organisés depuis le précédent numéro de la Gazette, paru en avril : RESSI du 15 au 17 mai à Erquy en Bretagne ; les Journées Nationales du 12 au 14 juin à Paris ; et cette semaine, à la fois l'École d'été du GDR à Rennes et APVP au Cap Hornu, au cœur de la Baie de Somme.

Pour ceux qui n'auraient pu participer aux Journées Nationales – qui ont enregistré cette année un chiffre record de 250 inscriptions – un aperçu est proposé dans ce numéro, et toutes les présentations seront accessibles prochainement sur le site web du GDR. Le-dit site web a d'ailleurs fait peau neuve, alors n'hésitez pas à faire remonter vos remarques aux membres du bureau du GDR.

Dans ce numéro de la Gazette, vous retrouverez une interview de Lilian Bossuet et Viktor Fischer qui nous présentent les activités en cybersécurité au Laboratoire Hubert Curien à Saint-Étienne, ainsi qu'une interview de Raphaël Bost, lauréat 2019 du prix de thèse, qui nous parle dans le coin prospectif de la Gazette du « searchable encryption ».

Enfin, avant de partir en pause estivale, n'oubliez pas de vous inscrire, ou de dire à vos doctorants de s'inscrire, à REDOCS 2019 ! Il s'agit de la quatrième édition des Rencontres Entreprises DOCtorants en Sécurité, qui auront lieu comme d'habitude sur le campus CNRS de Gif-sur-Yvette du 21 au 25 octobre. C'est gratuit, en pension complète, et ouvert à tous les doctorants en cybersécurité.

Je vous souhaite un bel été !

Gildas Avoine

Rubriques

Événements

(Repris en partie du forum du GDR)

Workshop "Security Proofs for Embedded Systems (PROOFS)" *Atlanta, États-Unis, 24 août 2019*

Workshop "5G Networks Security (5G-NS)" *Canterbury, Royaume-Uni, 26-29 août 2019*

Workshop "Designing and Measuring CyberSecurity in Software Architecture (DeMeSSA)" *Paris, France, 9-10 septembre 2019*

Workshop JFIN 2019 "Journées Francophones de l'Investigation Numérique" *Rennes, France, 17-19 septembre 2019 (évènement labellisé)*

Conférence FPS 2019 "The 12th International Symposium on Foundations & Practice of Security" *Toulouse, France, 5-7 novembre 2019 (évènement labellisé)*

Workshop CSAW'19 "Cyber Security Awareness Week" *Valence, France, 6-8 novembre 2019 (évènement labellisé)*

Workshop "Interplay of Security, Safety and System/Software Architecture (ISSA)" *Luxembourg, 23-27 septembre 2019*

Workshop "Cryptocurrencies and Blockchain Technology" *Luxembourg, 26-27 septembre 2019*

Workshop "Tools for Automatic Program Analysis (TAPAS 2019) " *Porto, Portugal, 8 octobre 2019*

Conférence "Cyber Security In Networking Conference" *Quito, Équateur, 23-25 octobre 2019*

Workshop "Software Hardware Interaction Faults" *Berlin, Allemagne, 28-31 octobre 2019, soumission : 28 juillet*

Conférence "Risks and Security of Internet and Systems (CRiSIS)" *Hammamet, Tunisie, 29-31 october 2019*

Workshop "Smart Card Research and Advanced Application Conference (CARDIS)" *Prague, République tchèque, 11-13 novembre 2019*

Workshop "Software PROtection (SPRO)" *Londres, Royaume-Uni, 15 novembre 2019*

Conférence "C&ESAR Virtualisation et Cybersécurité" *Rennes, France, 19-20 novembre 2019*

Conférence "C&ESAR Intelligence Artificielle & Défense" *Rennes, France, 21 novembre 2019*

Rencontres Entreprises-DOCtrorants en Sécurité : les inscriptions pour les doctorants sont ouvertes (et gratuites !)

https://gdr-securite.irisa.fr/redocs/redocs19

Le GDR Sécurité Informatique organise la quatrième édition des rencontres Entreprises-DOCtrorants en Sécurité (REDOCS) du 21 octobre au 25 octobre 2019 à GIF-SUR-YVETTE. Les doctorants travailleront durant toute une semaine sur des problèmes proposés par des professionnels issus du monde économique ou de la défense nationale. Le premier jour, les professionnels présenteront leurs sujets aux doctorants. Durant la semaine, les doctorants travailleront en groupe pour résoudre le sujet choisi. Enfin, les doctorants restitueront leurs résultats aux professionnels le vendredi matin.

Cet évènement, qui s'adresse aux doctorants qui seront prochainement à la recherche d'un emploi, leur permet de se confronter à des problèmes réels, de travailler en groupe, d'élargir leur vision de la sécurité, et de rencontrer des professionnels qui pourront leur faire part de leur expérience. Les étudiants peuvent faire valoir cette formation auprès de leur école doctorale. Parler français n'est pas requis.

Il y aura cette année 3 entreprises – notamment Thales et EDF – pour une quinzaine de doctorants. Les résumés des sujets proposés sont disponibles sur le site web de REDOCS 2019.

En direct des labos

Lilian Bossuet, Viktor Fischer

La Gazette interviewe dans ce numéro Lilian Bossuet et Viktor Fischer, deux enseignants chercheurs du Laboratoire Hubert Curien (UMR CNRS), faisant partie d'une équipe travaillant sur les générateurs d'aléa et sur leurs utilisations dans le domaine de la sécurité.

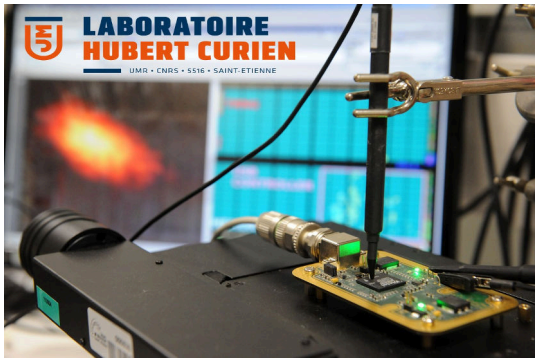
Bonjour Lilian, bonjour Viktor pouvez-vous résumer les activités du LHC en matière de sécurité ?

L'activité historique, et pour laquelle l'équipe est reconnue internationalement, concerne la conception, la caractérisation, l'utilisation et la sécurisation des générateurs d'aléa dynamique (les TRNG pour *True Random Number Generators*) et d'aléa statique (les PUF pour *Physical Unclonable Function*). Nous avons aussi des activités portant sur la conception de systèmes-sur-puce hétérogènes de confiance et l'implantation matérielle sécurisée d'algorithmes de cryptographie.

> « Si le générateur est manipulable par un attaquant, celui-ci peut alors augmenter dynamiquement le biais dans les nombres générés »

Pouvez-vous nous en dire plus sur vos activités liées aux générateurs d'aléas, quelles sont vos applications cibles ?

Tout dépend du type de générateur. Les applications cibles des TRNG sont la génération de clés secrètes pour la cryptographie et la génération de masques aléatoires pour les contre-mesures aux attaques par analyse de canaux cachés (c'est ce que nous avons fait pour le projet H2020 HECTOR https://hector-project.eu/news/rnm). Les applications cibles des PUF ne sont pas encore pleinement définies par l'industrie qui avance à tâtons sur ce domaine, mais nous avons exploité les PUF pour développer les prémices d'un système de licence d'utilisation du matériel (comme pour une licence dans le monde du logiciel) pour lutter contre la contrefaçon et le vol de circuits intégrés (une vidéo du démonstrateur est disponible en ligne : http://www.univ-st-etienne.fr/salware/SALWAREvideo.mkv).



Analyse du rayonnement EM des TRNG.

Quels types d'attaques peut-on envisager sur les générateurs d'aléa ? Que faire pour les prévenir ?

La force des générateurs est d'exploiter une source d'entropie basée sur un phénomène physique robuste. Si celle-ci est manipulable par un attaquant celui-ci peut alors augmenter dynamiquement le biais dans les nombres générés (obtenir par exemple plus de 0 que de 1 en sortie du générateur ou vice versa) et réduire dramatiquement la sécurité. Nous avons montré que ce type de manipulation est possible sur certains types de gé-

nérateurs par l'injection d'un signal électromagnétique aux abords du circuit intégré embarquant le générateur.

D'autres manipulations physiques ne peuvent pas être évitées. Une contre-mesure aux attaques est de détecter ces manipulations physiques. Pour cela il faut embarquer des tests qui valident en permanence la qualité de la source d'entropie et la qualité des nombres générés. Ces tests permettent ainsi de détecter les défauts du générateur et les manipulations malveillantes, mais ils sont très difficiles à réaliser dans le matériel car des mesures physiques précises (par exemple les mesures du bruit transformé en instabilité du signal d'horloge) doivent être réalisés dans les circuits numériques.

L'analyse de la fuite de l'information du type canaux cachés peut aussi être exploitée, d'abord pour localiser physiquement un TRNG et une PUF, et pour ces dernières pouvoir les cloner. Nous avons montré que le canal électromagnétique associé à une analyse spectrale donne de très bons résultats en localisation et manipulation de TRNG et PUF lorsqu'ils exploitent des cellules oscillantes.

> « Nous suivons les recommandations allemandes AIS20/31 devenues depuis 2001 de facto standard en Europe. »

Développez-vous également des méthodes pour mesurer la sécurité du générateur ou vous contentez-vous d'utiliser les recettes du NIST ?

Dans notre approche, nous suivons les recommandations allemandes AIS20/31. Depuis 2001, celles-ci sont devenues de facto standard en Europe. Pour suivre ces recommandations, nous développons un modèle stochastique et des méthodes de mesure interne (au circuit intégré) de paramètres physiques spécifique à un générateur. Le modèle et les méthodes de mesure constituent alors des tests statistiques spécifiques au générateur qui permettent de vérifier en continu l'entropie des nombres générés en sortie. En revanche, la norme américaine NIST SP 800-90 qui est plus récente (la partie concernant la conception de TRNG est valable depuis 2018) se contente d'utiliser des tests statistiques génériques qui sont plus faciles à implanter dans le matériel, mais qui sont moins précis et moins efficaces. Nous suivons donc l'approche qui est la plus rigoureuse et la plus sûre, mais aussi plus difficile à développer.

Question naïve, cela sollicite-t-il beaucoup de temps calcul ?

Non au contraire, l'intérêt de mesures internes (tests embarqués dédiés) est qu'elles sont plus rapides et plus efficaces que les tests « black box » (les tests génériques). Effectivement, les tests génériques nécessitent de 20 000 bits (FIPS 140-1) à 1 Gbit (NIST SP 800-22) de données générées suivant leur précision, alors que les tests embarqués dédiés que nous développons nécessitent entre 4 bits et 4 kbits de données. Les tests embarqués sont donc au minimum 5 fois plus rapides que le moins précis des tests génériques.


Lilian Bossuet et Viktor Fischer.

Merci Lilian, merci Viktor et bonne continuation au LHC !

Article rédigé par Lilian Bossuet, Viktor Fisher (Université Jean Monnet, Laboratoire Hubert Curien) et Patrick Bas., Contact: lilian.bossuet@univ-st-etienne.fr,fischer@univ-st-etienne.fr

Retour sur les journées Nationales

Solène Bernard et Gildas Avoine

Les Journées Nationales 2019 ont rencontré un vif succès avec 250 inscriptions. Ce chiffre montre que ce rendez-vous organisé chaque année à la fin du printemps trouve progressivement sa place dans nos agendas, quand on compare avec les chiffres de 2017 (130 inscriptions) et 2018 (160 inscriptions). Les Journées Nationales, ce n'est pas un lieu où l'on vient présenter sa toute dernière contribution – il y a pour cela les conférences plus traditionnelles – mais un lieu où l'on vient discuter, échanger, s'acculturer aux autres domaines de la sécurité informatique, et un lieu où l'on peut se mettre en quête d'un futur collègue ou d'un futur laboratoire d'accueil. Avis aux doctorants et postdoctorants...

> « Les JN sont un lieu où l'on vient discuter, échanger, s'acculturer aux autres domaines de la sécurité informatique... »

L'édition 2019 des Journées Nationales était organisée par Samia Bouzefrane et Sébastien Bardin, au

CNAM à Paris. L'organisation a été quelque peu bousculée car l'amphithéâtre a été préempté quelques jours avant l'évènement, mais la réactivité des organisateurs a permis de trouver une solution sans modifier le programme scientifique.

Il serait difficile de faire une retranscription exhaustive du contenu de ces journées en seulement quelques lignes. Nous n'allons donc mettre en lumière que quelques uns des exposés de ces journées en picorant dans chacune des sessions.

Les Journées Nationales ont démarré avec un exposé *keynote* particulièrement intéressant et dynamique d'Herbert Bos (VU University, Pays-Bas) sur la recherche de vulnérabilités dans les logiciels, illustré par sa propre expérience de participation aux « bug bounty », programmes consistant à récompenser les découvreurs de failles. Comme l'année dernière, le second *keynote* avait une dimension historique, avec Jean-Jacques Quisquater (UCLouvain, Belgique) qui nous a présenté l'histoire de la carte à puce, illustrée par de nombreuses anecdotes personnelles. Sur l'ensemble des journées, nous avons eu en séance plénière six exposés qui portaient sur les thématiques des groupes de travail, chaque responsable d'un groupe de travail ayant proposé un orateur pour ces séances.

Enfin, nous avons eu une présentation de Thomas Baignères et Matthieu Finiasz sur les messageries sécurisée, notamment Olvid, une présentation de Cédric Lefebvre qui a participé à REDOCS 2018, et la remise du prix de thèse à Raphaël Bost par l'intermédiaire de l'un de ses directeurs de thèse, Pierre-Alain Fouque.

250 personnes se sont inscrites aux Journées Nationales.

Mercredi après-midi, nous avons notamment eu le plaisir d'écouter Lucca Hirschi – lauréat 2018 du prix de thèse – qui apportait une dimension « méthodes formelles » dans la session sur la sécurité des systèmes, des locigiels et des réseaux, en présentant notamment une analyse de sécurité (avec une approche symbolique) d'un protocole d'authentification utilisé par la 5G. Dans cette même session, Kavé Salamatian nous a présenté ses travaux sur le monitoring d'Internet, par exemple pour détecter une anomalie de routage au niveau du protocole BGP. Il a illustré l'intérêt de ses travaux avec l'incident qui a eu lieu quelques jours auparavant, où tout une partie du trafic européen d'Internet a transité par la Chine !

École d'été du GDR

L'école d'été du GDR Sécurité Informatique était organisée à Rennes du 8 au 12 juillet 2019. Elle regroupait une quarantaine de participants ainsi que 16 intervenants venus de France, d'Europe, d'Israël et d'Australie. Le programme comportait des cours ainsi que des travaux pratiques sur le thème de la sécurité des interfaces logicielles/matérielles. Des activités sociales ont également eu lieu, avec un après-midi à Saint-Malo et un CTF. Les présentations seront prochainement disponibles sur le site web du GDR. Cette édition était organisée par Clémentine Maurice (CNRS) et Frédéric Tronel (CentraleSupélec), dans le cadre du semestre thématique sur la sécurité des interfaces matérielles et logicielles, financé par la DGA-MI et opéré par Inria pour le compte des partenaires académiques du PEC.

`https://silm-school.inria.fr/`

En parallèle, dans la session sur la protection des données personnelles, plusieurs exposés passionnants, dont celui de Sonia Ben Mokhtar sur la ré-identification de personnes à partir de la connaissance de leurs déplacements (typiquement, collection de coordonnées GPS obtenues lors d'un déplacement).

Jeudi était la journée des GT « sécurité et données multimédia » d'une part, et « codage et cryptographie » et « sécurité des systèmes matériels » d'autre part. Ces deux derniers GT avaient en effet décidé d'organiser une session commune. Les deux premières présentations de cette session portaient sur les attaques par canaux auxiliaires. Pour les néophytes, ces attaques permettent de casser un système de chiffrement en analysant les informations auxiliaires liées au processus de chiffrement. Il peut s'agir par exemple d'analyser les ondes électromagnétiques qu'envoie un écran, ou bien du temps que met un CPU à faire des opérations cryptographiques. Afin de lutter contre ces attaques temporelles, Jean-Yves Strub nous a présenté l'environnement de travail Jasmin, dont le compilateur assure des garanties de temps constant sur des opérations cryptographiques. Annelie Heuser, elle, s'est placée du côté de l'attaquant en présentant des techniques d'apprentissage semi-supervisé sur des données obtenues par des canaux auxiliaires.

Nous avons ensuite pu écouter Jean-Luc Dugelay, dans la session « sécurité et données multimédia », qui a présenté un état de l'art des attaques des techniques d'identification de visages. Ces attaques peuvent avoir lieu dans le monde réel (avec du camouflage par exemple), ou bien dans le monde numérique, en envoyant des images directement construites pour contourner le système de reconnaissance. Nous avons appris que ces attaques peuvent aussi exploiter les limites de l'humain : en effet, l'homme n'est pas très performant (expérience dans la salle à l'appui) lorsqu'il s'agit d'associer une personne que l'on vient de rencontrer à sa photo. C'est pour exploiter cette faiblesse qu'est né le projet « passeport magique » : une photo d'identité est générée en mixant deux visages, afin qu'un public non averti puisse l'associer à deux personnes différentes.

Jean-François Mainguet, expert dans les lecteurs d'empreintes digitales, nous a ensuite présenté, en agrémentant de sérieuses sources cinématographiques telles que « l'aube du sixième jour » ou « demolition man », de multiples failles possibles d'une identification biométrique. Sécuriser un coffre par un lecteur d'empreinte digitale, est-ce un système sûr, sachant qu'un doigt peut être copié, ou bien pire pour son propriétaire, coupé ? Après l'exposition de tout ce que cette simple observation implique, il a interpellé l'audience en l'invitant à méditer sur une question plus profonde : « Qu'est-ce qu'un doigt vivant ? »

La dernière matinée des Journées Nationales, le vendredi, ne comportait que des séances plénières, notamment Véronique Cortier qui a fait un très bel exposé sur le vote électronique, et Viktor Fischer qui a présenté la problématique de la génération d'aléa sur un composant. Ses activités sont par ailleurs introduites dans la rubrique « En direct des labos » de ce numéro.

Les Journées Nationales se sont achevées avec la remise du prix de thèse 2019 par Olivier Bettan (représentant le sponsor, Thales) et Aurélien Francillon (président du jury du prix de thèse) à Raphaël Bost, enfin presque... Le lauréat étant aux États-Unis au moment de la remise du prix, il a présenté ses travaux à travers une vidéo (disponible sur le site web du GDR), et c'est l'un de ses directeurs de thèse, Pierre-Alain Fouque (l'autre directeur de thèse étant David Pointcheval) qui a symboliquement reçu le prix. Le directeur de thèse a été ovationné pour son travail d'encadrement, mais aussi pour son sprint final qui lui a permis d'arriver in extremis pour la remise du prix : bloqué le matin même dans un train en provenance de Rennes, il est arrivé 10 secondes avant la fin des Journées Nationales, ce qui fait de lui à ce jour le détecteur du record du monde de la participation la plus brève aux Journées Nationales du GDR !

Rendez-vous donc au printemps 2020 à Paris pour la prochaine édition des Journées Nationales et son lot de rebondissements !

Remise du prix de thèse 2019.

Article rédigé par Solène Bernard (CNRS, CRIStAL) et Gildas Avoine (INSA Rennes, IRISA), Contact: solene.bernard@centrale.centralelille.fr

Le coin prospectif

Raphaël Bost

La Gazette interviewe Raphaël Bost, le lauréat du prix de thèse du GDR pour sa thèse « Algorithmes de recherche sur bases de données chiffrées ». Notons que le jury a également nommé deux accessits : Ilaria Chillotti pour sa thèse intitulée « Vers l'efficacité et la sécurité du chiffrement homomorphe et du cloud computing » et Dolière Francis Somé pour sa thèse intitulée « Sécurité et vie privée dans les applications web ».

Bonjour Raphaël, félicitations pour ton prix de thèse. Peux-tu nous présenter les contributions qui ont été à l'origine de ce prix ?

Merci beaucoup ! Mes travaux ont porté sur le chiffrement de bases de données et plus exactement sur la manière de chiffrer un ensemble de documents tout en gardant des fonctionnalités de recherche sur le corpus qui soient efficaces en pratique. Ce domaine est appelé **searchable encryption** en anglais, « chiffrement interrogeable » en français (même si je ne suis pas fan du nom). Mes principales contributions sont de trois natures : des résultats théoriques d'impossibilité

qui montrent que ces fonctionnalités de recherche sécurisé ont un coût minimal en terme de calculs, la conception de schémas efficaces en pratique et en théorie (et même optimaux pour certains) de chiffrement interrogeable dynamiques (c'est-à-dire supportant l'ajout et la suppression de documents) sans que cela porte atteinte à la sécurité des données chiffrées – les schémas existant précédemment étaient sensibles à des attaques très sérieuses remettant en cause leur utilisation en pratique – et enfin l'implémentation de ces schémas, afin de démontrer leur employabilité. J'ai ainsi travaillé sur un grand spectre du domaine, du très théorique, au très pratique.

Quels types d'usages sont envisagés pour la recherche chiffrée ?

Raphaël Bost (`https://raphael.bost.fyi`).

Ils sont extraordinairement variés : l'objectif ultime de la communauté est de proposer des bases de données entièrement chiffrées, aussi bien pour les données elles-mêmes que pour les requêtes, qui puissent remplacer les bases de données utilisées actuellement, comme MySQL ou MongoDB (pour les connaisseurs). On les retrouverait donc partout où des données sensibles peuvent être stockées et requêtées.

Sur quels grands principes reposent ce domaine ?

D'un point de vue formel, il s'agit principalement de cryptographie prouvée. On va donc construire un schéma de chiffrement interrogeable à partir de briques telles des fonctions de hachage, du chiffrement symétrique ou encore des permutations à trappe (comme RSA) et utiliser leurs propriétés de sécurité pour démontrer formellement la sécurité du schéma dans un modèle donné. Mais comme il s'agit aussi d'un sujet appliqué, il est important de prendre en compte les impacts des choix de conception, en particulier en termes de performance. Ainsi, la connaissance des systèmes sur lesquels ces schémas vont s'exécuter est importante, du fonctionnement du cache du système d'exploitation, à celui d'un disque dur/SSD.

Quand penses-tu que ce domaine deviendra une réalité pratique ? Quels challenges reste-t-il à résoudre pour aller vers une utilisation massive ?

Pour certaines applications, c'est déjà une réalité : aujourd'hui on sait faire des recherches exactes de mots-clés de manière relativement efficace (par exemple, en n'utilisant que de la cryptographie symétrique) et avec un bon niveau de sécurité. Par contre, il reste encore du travail à effectuer pour des requêtes plus complexes, comme par exemple les jointures ou les recherches approximées (qui peuvent supporter une typo). Au-delà du chiffrement d'un corpus de document, il faudrait aussi développer des solutions pour des bases de données un peu plus exotiques, mais très répandues, telles que les bases de données orientées graphe.

> « L'objectif ultime de la communauté est de proposer des bases de données entièrement chiffrées qui puissent remplacer les bases de données utilisées actuellement »

J'ai cru comprendre que la recherche chiffrée était associée à une fuite d'information inévitable, est-ce une réalité, est-ce un danger en pratique ?

Tout à fait. Prenons un exemple : suite à une requête de recherche, la base de données va retourner une liste de résultats. La taille de cette liste peut révéler beaucoup d'informations à un attaquant : il pourra en effet essayer de retrouver le mot clé recherché par une analyse de fréquence. Un autre exemple serait l'utilisation de chiffrement déterministe pour protéger individuellement les valeurs d'une base de données SQL. Si cette approche est très performante et permet de s'appuyer directement sur les travaux de la communauté des bases de données (elle a été/est d'ailleurs utilisée aujourd'hui pour cela), elle est particulièrement vulnérable à un attaquant faisant une analyse de fréquence sur ces valeurs.

De fait, on peut même rigoureusement démontrer qu'il existe un certain nombre de compromis entre, d'un côté, la performance de la base de donnée chiffrée et, de l'autre, les informations qu'elle laisser fuiter sur le contenu de la base ou les requêtes qui sont faites par l'utilisateur. Une des grandes difficultés du domaine est justement de bien comprendre quels sont ces compromis et donc de bien appréhender l'impact des informations fuitées par la BDD chiffrée. Cela a donné lieu à de nombreux travaux de cryptanalyse qui ont fait énormément avancer nos connaissances dans le domaine : aujourd'hui nous savons que pouvoir supporter des requêtes d'intervalle (récupérer les éléments dont une caractéristique donnée est comprise entre deux valeurs) sans que l'adversaire puisse reconstruire la base en clair nécessite des techniques très coûteuses. Ce sont donc ces travaux de cryptanalyse des fuites qui permettent de mieux comprendre les risques liés à certaines fuites et la praticité des attaques qui en découlent.

Quels conseils pourrais-tu donner aux étudiants de thèse travaillant en sécurité informatique ?

Vaste question. Je dirais d'abord qu'ils doivent être le plus rigoureux possible : le domaine repose soit sur des preuves, soit sur des expériences et dans les deux cas, les résultats ne sont probants que s'ils sont obtenus de manière rigoureuse. Ensuite, la curiosité est primordiale : les meilleures idées viennent souvent en étudiant des papiers qui sortent du sujet étudié. C'est en prenant un autre point de vue, du recul sur son sujet de recherche que l'on peut contribuer le plus. Enfin, il ne faut pas oublier que l'objectif d'une thèse est d'acquérir de l'autonomie dans un travail de recherche et développement et que cela doit être en soi un objectif pour un doctorant.

Merci Raphaël pour tous ces conseils et ses informations précieuses, bonne continuation !

Article rédigé par Raphaël Bost (DGA-MI), Annelie Heuser et Patrick Bas, Contact: raphael.bost@polytechnique.org

Nos collègues sur les ondes

Deepfake et forensics sur France Culture (26 juin). À ré-écouter sur la plage : l'équipe de *la Méthode Scientifique* a reçu des collègues de l'IRISA, du LIGM et du CMLA pour parler de création et de détection de vidéos Deepfake.

Jobs

(Repris en partie du forum du GDR)

Offre de thèse, IRISA (EMSEC), Rennes

Titre : Cryptographic Communication Protocols. Url : http ://www.avoine.net/proposal_protocols.pdf ***Contact : Gildas Avoine, gildas.avoine@irisa.fr***

Offre de thèse, INRIA/IRISA, Rennes

Titre : Sécurité des Réseaux de Neurones et Dissimulation d'Information. ***Contact : Teddy Furon, teddy.furon@inria.fr, Patrick Bas, patrick.bas@centralelille.fr***

Enseignants-Chercheurs, ESIEA, Laval

Trois postes d'enseignants-chercheurs en cybersécurité à pourvoir (au fil de l'eau) à l'ESIEA Laval. ***Contact : Loïc Roussel, loic.roussel@esiea.fr***

Offre de thèse, Telecom Paris (ACES), Saclay

Titre : Optimisation du risque de sécurité pour l'apprentissage sur données de qualité hétérogène. ***Contact : Thomas Robert, thomas.robert@telecom-paris.fr***

Offre de thèse, Eurecom, Sophia-Antipolis

Titre : Security of IoT devices in 5G networks through fingerprinting and side-channel analysis. ***Contact : Aurélien Francillon, aurelien.francillon@eurecom.fr, et Clémentine Maurice, clementine.maurice@irisa.fr***

Offre de thèse, L3i (Images et Contenus), La Rochelle

Titre : Authentification hybride de documents par leurs contenus graphiques et textuels. ***Contact : Petra Gomez-Krämer, petra.gomez@univ-lr.fr, et Antoine Doucet, antoine.doucet@univ-lr.fr***

Chercheur postdoctoral, Télécom SudParis, Evry ou Palaiseau

Projet : IoT Traffic Generation Platform. ***Contact : Gregory Blanc, gregory.blanc@telecom-sudparis.eu***

Trois offre de thèse, LIG (SLIDE), Grenoble

Titres : Detection and impact analysis of issue and political ads, Measuring and preventing the impact of harmful online ads on children and teenagers, et Design of transparency mechanisms for online targeted advertising. ***Contact : Oana Goga, oana.goga@cnrs.fr, et Patrick Loiseau, patrick.loiseau@inria.fr***

Offre de thèse (CIFRE), Orange Labs, Caen

Titre : Conception d'un noyau sécurisé pour les processeurs avec MPU pour l'IOT et composition de preuves et d'évaluations de sécurité. ***Contact : Gilles Grimaud, gilles.grimaud@univ-lille.fr, et Chrystel Gaber, chrystel.gaber@orange.com***

Chercheur postdoctoral, L3i, La Rochelle

Sujet : Content-based document signature for IoT security. ***Contact : Mickaël Coustaty, mickael.coustaty@univ-lr.fr, et Petra Gomez-Krämer, petra.gomez@univ-lr.fr***