Février 2023
Numéro 14

LA GAZETTE DU GDR

Sécurité Informatique - GDR2046

Édito de la directrice

Vous aimez jouer ? Au menu de cette gazette, de l'histoire, des mystères, des images, des jeux, des rencontres, et bien sûr de la science... Ce numéro revient sur les événements organisés par le GDR l'automne dernier, et vous fera découvrir l'éventail des travaux menés en cybersécurité au LIP6, ainsi que les recherches de Tina Nikoukhah sur la détection de manipulation des images. Deux interviews supplémentaires vous présenteront un exemple de médiation scientifique avec la création du jeu CyberCrypt, et l'aventure rocambolesque et passionnante du décryptage d'une missive de Charles Quint.

Un grand merci à celles et ceux qui ont partagé leur passion et leur enthousiasme, et qui ont organisé les événements de l'automne. Si vous souhaitez vous aussi partager une expérience originale et enrichissante, n'hésitez pas à nous contacter.

Bonne lecture !
Caroline Fontaine,
Directrice du GDR Sécurité Informatique

Rubriques

ÉVÉNEMENTS 1
LE COIN PROSPECTIF (CYBERCRYPT) 2
RETOUR SUR (JOURNÉE SSM) 3
LE COIN PROSPECTIF (TINA NIKOUKHAH) 3
RETOUR SUR (JOURNÉE SSLR) 5
LE COIN PROSPECTIF (LETTRE DE CHARLES QUINT) 6
RETOUR SUR REDOCS 8
EN DIRECT DES LABOS (LIP6, PARIS) 9
JOBS 12

Événements

(Evénements organisés ou labellisés par le GDR, https://gdr-securite.irisa.fr/lagenda/)

Journée thématique Calcul haute performance pour les systèmes embarqués, *Toulouse, France, 14 mars 2023*

Journées du GT MFS, *Roscoff, France, 28-30 mars 2023*

Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2023), *Neuvy-sur-Barangeon, France, 10-12 mai 2023*

AMUSEC, *Marseille, France, 25-26 mai 2023*

APVP, *Arc-et-Senans, France, 12-15 juin 2023*

CryptArchi, *Cantabria, Espagne, 12-13 juin 2023*

Journées nationales du GDR Sécurité Informatique, *Campus Cyber La Défense, Puteaux, France, 26-28 juin 2023*

Summer School du GDR, "Cyber in Sophia Antipolis", *Sophia Antipolis, France, 3-7 juillet 2023*

(Autres événements, repris en partie du forum du GDR)

Colloque Cybersécurité des grands événements publics : l'envers du décor !, *Direction Générale de la Gendarmerie Nationale, Issy les Moulineaux, France, 20 mars 2023*

Table ronde du CNRS : Cybersécurité : au-delà de la technique, quelle place pour les Sciences Humaines et Sociales ?, *Campus Cyber La Défense, Puteaux, France, 21 mars 2023*

Computer Security Track at the 38th ACM Symposium on Applied Computing (SEC@SAC 2023), *Tallinn, Estonie, 27 mars - 2 avril 2023*

Toulouse Hacking Convention (THCon 2023), *Toulouse, France, 20-21 avril 2023*

53rd IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2023), *Porto, Portugal, 27-30 juin 2023*

5th Workshop on the Security of Software/Hardware Interfaces (SILM 2023), *co-organisé avec Euro S&P 2023, Delft, Pays-Bas, 3-7 juillet 2023*

18th International Conference on Availability, Reliability and Security (ARES 2023), *Bénévent, Italie, 29 août - 1 septembre 2023*

30th Computer & Electronics Security Application Rendezvous (C&ESAR 2023), *Rennes, France, 21-22 novembre 2023*

Le coin prospectif

CYBERCRYPT

La gazette interviewe Sébastien Canard, qui nous explique le principe du jeu CYBERCRYPT, présenté chaque année à la fête de la science (https://www.fetedelascience.fr/cybercrypt) et décrit par ses auteurs dans un article disponible en ligne (https://eprint.iacr.org/2021/063).

Pouvez-vous nous présenter en quelques mots ce qu'est CYBERCRYPT ?

CYBERCRYPT est un jeu collaboratif et pédagogique visant à présenter au public les principes de base de la cryptographie. Il se présente sous la forme d'un plateau, divisé en 3 « âges », et de cartes. Les joueurs y incarnent une équipe qui souhaite lancer une entreprise sur Internet. Étape après étape, ils vont se trouver confrontés à des événements qui vont nécessiter le recours à des outils cryptographiques pour sécuriser leur travail. Plusieurs ateliers sont ainsi proposés pour illustrer différents mécanismes de cryptographie, simples mais pourtant toujours d'actualité. Lorsque les joueurs réussissent un atelier, ils gagnent des points, et peuvent avancer dans le jeu. À la fin du temps imparti, le nombre de points peut soit indiquer le niveau atteint par l'équipe, soit être utilisé pour comparer plusieurs équipes. C'est un jeu qui peut sans problème être joué à partir de 10 ans et qui dure environ 1h.

Comment vous est venu l'idée de CYBERCRYPT ?

Depuis quelques temps, nous étions plusieurs à avoir des idées d'ateliers présentant les concepts de base de la cryptographie. En mettant en commun tout ça, nous les avons alors créés avec ce que nous avions sous la main : des feuilles, des boîtes à chaussures, des rouleaux de papier absorbant, *etc.* Nous avons ensuite présenté nos ateliers à la fête de la science, où nous avons rencontré beaucoup de succès. Cependant, nous avons aussi remarqué que nos ateliers manquaient de couleurs et de visuels, contrairement à ceux des autres stands. Nous avons alors candidaté au prix des Têtes Chercheuses, décerné par le musée Schlumberger. Le projet a été monté par le laboratoire d'informatique de l'Université de Caen (le GREYC) et Orange Innovation, et nous avons gagné le prix de 10 000 euros. Cela nous a permis d'une part d'avoir du matériel de meilleur qualité, capable de mieux résister dans le temps, et d'autre part, de scénariser les ateliers, avec l'idée de créer ce jeu. Après avoir interagi avec des jeunes lors de séances d'échanges, nous avons élaboré le scénario, créé les visuels et les concepts du jeu.

> « CYBERCRYPT est un jeu collaboratif et pédagogique visant à présenter au public les principes de base de la cryptographie. »

Comment se présentent les ateliers et quel est le lien avec le jeu ?

Il y a deux types d'ateliers. Le premier se concentre sur la cryptographie à clé secrète en présentant le fonctionnement, et les faiblesses, des systèmes de la Scytale, de César et Vigenère, d'Enigma, jusqu'au cryptosystème de Vernam. Le second type présente les concepts de base de la cryptographie à clé publique, sous la forme de boîtes et de cadenas, qui permettent d'étudier le principe des clés publiques, de l'attaque de l'homme du milieu et de la certification. Ensuite, ces ateliers sont mis en place dans le jeu. Plus précisément, pendant le premier âge, nous familiarisons les joueurs avec le matériel et les mécanismes historiques de la cryptographie. Lors du deuxième âge, les joueurs vont comprendre pourquoi ces systèmes ne fonctionnent pas, ou en quoi ils ne sont pas assez résistants. Lors de la dernière phase, les ateliers permettent d'expliquer la façon de bien utiliser ces systèmes.

Où et comment peut-on participer au jeu ?

Nous faisons assez régulièrement des interventions dans les collèges et les lycées. Nous séparons les classes en groupes de 10 élèves maximum et nous faisons le jeu en parallèle. Nous avons ensuite une session de discussion pour expliquer comment le jeu se place par rapport à la cryptographie qu'ils utilisent chaque jour, ce que nous faisons aujourd'hui en recherche en cryptographie, et parfois notre cursus.

Nous présentons aussi les ateliers et le jeu chaque année lors de la fête de la science. Le jeu est un peu plus compliqué à utiliser dans ce contexte parce que les visiteurs ont rarement 1h de libre, mais les ateliers rencontrent un franc succès, même auprès des plus jeunes. Nous participons aussi parfois à d'autres manifestations autour de la médiation scientifique.

Nous pouvons aussi fournir l'ensemble des informations nécessaires pour que n'importe qui puisse recréer le jeu dans sa globalité. Tout est libre de droit et de reproduction. C'était l'objectif initial.

Est-ce que tout le monde arrive au bout du jeu ?

L'objectif est que tout le monde y parvienne. Cela reste un jeu pédagogique. Pour rajouter un peu de piment, nous avons mis une durée sur chaque atelier. Lorsque le temps imparti est terminé, nous guidons progressivement les joueurs pour qu'ils parviennent au résultat. Après, plus ils prennent de temps, moins ils gagnent de points.

Est-ce qu'il y a des étapes à venir ?

Cela fait longtemps que nous souhaitons rajouter des ateliers. Nous avons quelques idées autour de l'authentification, du calcul distribué, et éventuellement du chiffrement homomorphe (mais ce dernier est particulièrement complexe). Cependant, tout cela prend du temps, et nous en manquons un peu.

Une autre idée que nous avons est de numériser le jeu et de le rendre disponible sur Internet. Cela pose d'autres questions, mais je pense que cela permettrait une diffusion plus large du jeu.

Merci de nous avoir fait découvrir ce jeu que nous avons hâte de manipuler en vrai, et bonne continuation pour les améliorations que vous avez en tête !

Article rédigé par Sébastien Canard (Orange Labs, Caen) et Céline Chevalier, contact : sebastien.canard@orange.com

Retour sur la journée SSM

Romain Wacquez

Les architectures de calcul en mémoire ou proche mémoire voient leur intérêt croître lors de la conception de systèmes, dans l'objectif de proposer des alternatives aux architectures de Von-Neumann. En effet, ces dernières ont l'inconvénient de créer un goulot d'étranglement entre la partie mémoire et la partie calcul dans les systèmes de traitement de l'information. Si l'on prend en compte l'utilisation en forte croissance de l'internet des objets et de l'intelligence artificielle, le nombre de données collectées est aujourd'hui très important et continue d'augmenter. Cela implique la nécessité de trouver de nouvelles solutions afin d'améliorer l'efficacité des futures architectures de calcul mais aussi de garantir la sécurité des données utilisant ce type d'architectures.

La journée du 12 octobre 2022, qui s'est déroulée au laboratoire LIP6 à Paris, a rassemblé une vingtaine de personnes autour de cette question. Les cinq présentations de la journée ont permis d'aborder la question sous différents angles. Nous avons tout d'abord eu une présentation concrète d'architecture de calculs en mémoire, et cette architecture a été mise en perspective vis-à-vis d'applications en sécurité matérielle comme le PUF ou la cryptographie. Si cette première architecture utilise des mémoires éprouvées (SRAM), deux présentations ont ensuite montré l'usage possible de technologies de mémoires microélectroniques émergentes (STT-MRAM, FeFET) pour le calcul, et plus spécifiquement la réalisation de fonctions de sécurité (portes logiques pour la conception de crypto-processeurs sur silicium). L'impact sur la sécurité et les opportunités en termes de fonctions de sécurité ont été discutés. Enfin des travaux sur la caractérisation d'architecture système intégrant des mémoires ont été présentés. Expérimentalement sur des mémoires commerciales (Flash), ou d'un point de vue plus théorique sur des mémoires émergentes (ReRAM), ces travaux ont mis l'accent sur l'importance de préparer l'avènement de ces architectures en mémoires en identifiant les vulnérabilités associées le plus tôt possible, et cela dans l'objectif d'identifier les solutions les plus pertinentes d'un point de vue sécurité, et de préparer le cas échéant des stratégies de sécurisation.

Cet événement organisé uniquement en présentiel préfigure le retour d'événements scientifiques permettant de se questionner sur des sujets d'envergure et à dynamique forte. L'organisation de cet événement a permis des temps d'échanges longs tout au long de la journée qui ont été très appréciés des participants.

Romain Wacquez (CEA Leti, Mines Saint-Étienne, Gardanne), contact : Romain.Wacquez@cea.fr

Le coin prospectif

Tina Nikoukhah

La gazette interviewe Tina Nikoukhah, post-doctorante au Centre Borelli de l'ENS Paris-Saclay et lauréate 2022 du prix Jeunes Talents L'Oréal-UNESCO. Tina travaille sur la sécurité multimédia dans le domaine de la détection de falsification. Elle a soutenu sa thèse en 2022 sur l'exploitation des traces de compression JPEG pour détecter les manipulations dans les images. Elle s'intéresse également à la médiation scientifique et plus particulièrement à l'éducation aux médias et à l'information. La gazette a décidé d'interroger Tina sur son domaine de recherche en général et sur ses travaux de thèse en particulier.

Bonjour Tina, tu as soutenu ta thèse à la fin de l'année 2022. Peux-tu nous en dire un peu plus sur tes principales contributions ?

Bonjour ! Lors de ma thèse, j'ai développé trois algorithmes pour détecter les falsifications dans les images en analysant les incohérences des traces de compression JPEG. Ces méthodes se distinguent des techniques de l'état de l'art car elles donnent des résultats fiables avec un nombre contrôlé de fausses détections. Elles permettent également de retracer, autant que possible, l'historique de compression d'une image.

Les algorithmes développés ont été publiés et mis à disposition en ligne (via la plateforme IPOL `ipol.im`) afin de pouvoir être utilisés par le plus grand nombre, en particulier par les journalistes (via l'outil de *fact-checking* de l'Agence France-Presse, utilisé dans plus de 40 pays) et la police technique et scientifique. Ces deux collaborations ont été établies dans le cadre de ma thèse et ont également mené à des projets de recherche (ANR DEFALS et IFCN EnVisu4).

En conséquence de ce travail de recherche, j'ai eu la chance de créer un cours au sein du diplôme universitaire d'Éducation aux Médias et à l'Information, proposé conjointement par les écoles ENS Paris-Saclay et ESJ Lille, sur le traitement d'images et la détection de falsification.

Tu poursuis en ce moment tes travaux au Centre Borelli, ENS Paris-Saclay. Quels sont les objectifs que tu vises actuellement en matière de recherche ?

Mes objectifs de recherche sont très variés.

D'une part, je souhaite continuer et étendre mes recherches à d'autres types de manipulations, en particulier les nouvelles méthodes de falsification et de génération d'images. J'ai déjà constaté que les méthodes « classiques » que j'ai développées au cours de ma thèse, qui visent à détecter des incohérences dans les traces de compression, peuvent être utiles dans ces cas. En effet, soit ces images ne possèdent pas un historique d'image « naturelle », soit on observe toujours localement une incohérence de ces traces.

D'autre part, je m'intéresse également à la détection de vidéos hypertruquées (*deepfakes*) où je souhaite explorer les traces de compression vidéo qui sont plus complexes. Je travaille en équipe sur ces sujets, en particulier dans le cadre du projet ANR APATE.

Tina Nikoukhah

Enfin, je souhaite continuer à mener des projets de médiation scientifique. J'ai eu la chance de rédiger des articles de vulgarisation scientifique ainsi que d'animer des conférences et ateliers auprès de tout type de public, en particulier les étudiants de tous âges. Je me lance également dans un nouveau projet d'enseignement auprès d'un public non spécialiste en *intelligence artificielle*, terme très vague et souvent mal compris.

> « Lors de ma thèse, j'ai développé trois algorithmes pour détecter les falsifications dans les images en analysant les incohérences des traces de compression JPEG. »

Que penses-tu des progrès en création de faux ?

Auprès du grand public, toute invention peut sembler compliquée et effrayante, mais les progrès en création de faux sont réellement passionnants. Il devient effectivement de plus en plus facile, accessible et rapide de créer de fausses images et vidéos mais je pense que il n'y a pas de raison de s'inquiéter davantage que lors de la création de la photographie par exemple. Je pense que ces méthodes bouleversent la société de la même manière que la photographie a eu un impact sur l'art en fournissant une nouvelle forme d'expression créative, ou sur l'économie en ouvrant de nouveaux secteurs d'industrie.

Quel est l'avenir, selon toi, de la détection de falsification ?

Je pense qu'on devrait davantage adopter des méthodes de sécurité active. Un domaine bien étudié mais peu connu par le grand public ! Le tatouage numérique fragile en est un exemple, qui consiste à ajouter une

signature en amont à l'image pour la marquer comme authentique et la protéger contre les manipulations. Cependant, pour que cela soit véritablement efficace, il est important que toutes les plateformes adoptent cette méthode et soient soumises à une législation qui encourage ou impose ce type de sécurité active. Ainsi, les données et les images seront mieux protégées et la falsification pourra être détectée plus facilement.

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

1. Il est important de mettre en pratique les recherches en sécurité multimédia dans des cas concrets rencontrés par les utilisateurs et de collaborer avec les entreprises et les utilisateurs pour évaluer les solutions proposées.

2. Les doctorants devraient également s'efforcer de faire des recherches reproductibles pour garantir la qualité et la fiabilité de leurs travaux.

3. Enfin, les doctorants peuvent partager leur expertise avec le grand public en écrivant des articles de vulgarisation scientifique et en se concentrant sur la communication de leur travail.

Cela peut sembler comme un effort supplémentaire, mais ces efforts donnent un aspect plus complet à leur recherche et apportent de nombreux bénéfices en termes d'inspiration et de compréhension approfondie du sujet.

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

Article rédigé par Tina Nikoukhah (ENS Paris Saclay) et Céline Chevalier, contact : tina.nikoukhah@ens-paris-saclay.fr

Retour sur la journée thématique sur le génie logiciel et la sécurité

Olivier Levillain et Guillaume Hiet

Le 24 novembre 2022, le GT Sécurité des Systèmes, Logiciels et Réseaux (SSLR) du GDR Sécurité Informatique et le GT Génie Logiciel et Sécurité (GLSec) du GDR GPL ont organisé une journée thématique commune sur le génie logiciel et la sécurité. L'événement s'est tenu au CNAM, à Paris, et a rassemblé une quarantaine de personnes.

Deux orateurs invités ont présenté leurs travaux lors de cette journée. Julien Signoles, ingénieur de recherche au CEA List, a présenté l'outil Frama-C, développé et maintenu depuis plus de 15 ans par le CEA. Il s'agit d'une boîte à outils proposant une panoplie de greffons (plugins) pour l'analyse de code C. Initialement prévu pour garantir des propriétés de sûreté de fonctionnement, Frama-C est aujourd'hui également de plus en plus utilisé pour assurer également des propriétés de sécurité.

Vincent Laporte, chargé de recherche Inria au Loria, a décrit et formalisé le problème du développement de code s'exécutant en temps constant. Après avoir rappelé que les attaques par canaux auxiliaires reposant sur le temps d'exécution sont étudiées depuis près de 30 ans, il nous a décrit une approche reposant sur un langage Jasmin et son compilateur associé, pour produire et vérifier du code *constant time*. Une des difficultés est de modéliser les fuites au bon niveau, car les modèles classiques sont tantôt trop précis (cas des accès mémoire qui se font par ligne) ou trop grossiers (par exemple certaines instructions arithmétiques dont la durée dépend des opérandes, comme la division).

Cette journée a également été l'occasion de discuter de travaux de jeunes chercheurs et jeunes chercheuses, sur des thématiques variées. L'ensemble des sujets présentés, ainsi que certaines des présentations, sont disponibles sur le site de la conférence (`https://glsec22.sciencesconf.org`).

Olivier Levillain (Télécom SudParis) et Guillaume Hiet (CentraleSupélec), contact : olivier.levillain@telecom-sudparis.eu, guillaume.hiet@centralesupelec.fr

Brèves

- L'équipe Sotern (Self-Protecting the Future Internet) a été créée officiellement à l'IRISA (Rennes) à compter du 1er janvier 2023. L'équipe compte 8 permanents et environ autant de non-permanents et travaille sur les questions d'autonomie/automatisation de la sécurité dans les architectures réseaux.
- Les membres du jury du prix de thèse ont reçu 14 soumissions, verdict en avril !

Le coin prospectif

Déchiffrement d'une lettre de Charles Quint

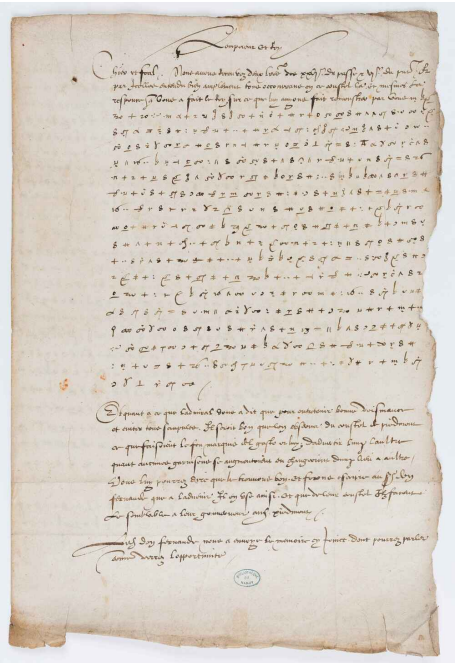
La gazette interviewe Cécile Pierrot, Pierrick Gaudry et Paul Zimmermann (Université de Lorraine, CNRS, Inria, LORIA) au sujet d'un travail pour le moins original, débuté par hasard, le déchiffrement d'une lettre écrite par Charles Quint. Au programme, des conversations anodines (mais d'importance capitale) au cours de repas, des archives contenant de précieux documents, une lettre écrite en moyen français avec un système de chiffrement inconnu, le renfort d'une historienne, un assassinat potentiellement fomenté par François Ier, un changement de calendrier et bien d'autres rebondissements... Suivez le guide !

Bonjour, nous avons appris que vous avez décrypté une lettre vieille de cinq cents ans, écrite par Charles Quint... et cela éveille notre curiosité. Pouvez-vous nous dire comment vous vous êtes retrouvés à résoudre un tel mystère ?

Nous avons appris l'existence de cette lettre mystérieuse par hasard, lors d'un dîner avec des amis d'amis. Cette lettre chiffrée aurait été envoyée par Charles Quint à l'ambassadeur de France le Sieur Jean de Saint-Mauris il y a cinq cents ans environ, et n'aurait jamais été déchiffrée... Cela a piqué notre curiosité et nous avons essayé de la trouver sur internet, en vain. Pas de trace non plus d'informations sur les techniques de chiffrement utilisées par Charles Quint. Nous nous sommes demandés s'il n'y avait pas erreur sur la personne (Marie Stuart peut-être ?) et avons laissé là cette histoire, sans chercher plus loin. Mais deux ans plus tard, nous en avons de nouveau entendu parler, et nous avons appris qu'elle était à Nancy, sans savoir précisément où. Cette fois-ci nous avons poussé les recherches plus loin, fait jouer le bouche-à-oreilles, jusqu'à découvrir qu'elle était conservée dans la réserve de la bibliothèque du patrimoine de Nancy. Nous nous y sommes rendus et oui la lettre s'y trouvait bien ! Elle était en excellent état et tout à fait lisible.

Comment vous êtes vous attaqués au problème ?

La lettre chiffrée est écrite avec environ 120 symboles différents, sans espace ni ponctuation. Nous avons donc commencé par effectuer un travail de classification avec une table des symboles afin de pouvoir traiter le texte avec Python. Clairement chaque lettre du clair était chiffrée avec plusieurs symboles possibles. Néanmoins, compte tenu de la date de la lettre, au début nous pensions qu'il s'agissait d'une technique de chiffrement relativement rudimentaire que nous pourrions attaquer avec des méthodes statistiques relativement classiques ; cela allait être réglé dans la semaine... La question de la langue utilisée pour la rédaction de la lettre s'est évidemment rapidement posée, d'autant que Charles Quint en parlait beaucoup : latin, français, allemand, espagnol, néerlandais, *etc.* Il nous fallait aussi prendre en compte le fait que la lettre date du 16e siècle et donc nous devions considérer la version de ces langues à cette époque. À la fin de la lettre se trouvaient en clair des formules de politesse en (moyen) français, et la lettre était adressée à l'ambassadeur en France, donc le français semblait être une bonne piste, mais cela aurait aussi très bien pu être un leurre...



Extrait de la missive chiffrée, source Limédia

Quelles ont été les difficultés spécifiques ?

Nous nous sommes donc tout d'abord lancés dans des analyses statistiques, comptabilisant les symboles, les bigrammes, les trigrammes, et en s'appuyant sur les statistiques du moyen français utilisé dans *Pantagruel* de Rabelais, mais cela n'a pas du tout suffi. Même notre tentative de reconnaître les voyelles a échoué. Pourtant, il semblait bien y avoir une structure, car des motifs apparaissaient – et même un motif de onze symboles qui se répétait deux fois – c'était vraiment étrange. Nous avons alors envisagé plusieurs hypothèses, comme l'utilisation de plusieurs symboles pour chiffrer une même lettre de l'alphabet (surtout pour les lettres les plus fréquentes), mais aussi l'utilisation de symboles pour les espaces ou la ponctuation, ou pour des bigrammes ou des trigrammes, de symboles particuliers pour chiffrer les lettres doubles, de symboles spécifiques pour les noms propres de personnalités importantes (rois, pape *etc.*), ou encore de symboles nuls ou de modificateurs. Malgré ces pistes, qui *a posteriori* se sont révélées être les bonnes et étaient inspirées d'autres textes historiques

bien connus, nous n'arrivions pas à exploiter de mesures statistiques : nous étions dans une impasse. C'était vraiment frustrant !

Nous avons cherché des documents historiques, de personnes ayant peut-être déjà travaillé sur le système de chiffrement de Charles Quint. Nous avons appris l'existence d'un traité expliquant les techniques utilisées, écrit par un expert italien pour plusieurs langues, mais cet ouvrage a disparu...

Lors des dernières journées C2, toujours au cours d'un repas, nous avons parlé de notre aventure à Anne Canteaut, qui s'est alors exclamé « Mais il faut que vous en parliez aux historiens, ils pourront certainement vous aider ! ». Grâce à elle et à son frère qui travaille avec des historiens, nous avons donc tiré ce fil, qui nous a mené jusqu'à Camille Desenclos, maîtresse de conférences en Histoire moderne à l'Université de Picardie. Nous tenons à les remercier pour leur aide.

« Compte tenu de la date de la lettre, au début nous pensions qu'il s'agissait d'une technique de chiffrement relativement rudimentaire que nous pourrions attaquer avec des méthodes statistiques relativement classiques. »

Comment l'historienne Camille Desenclos vous a aidés ?

Camille Desenclos est une historienne spécialiste de cette période, et plus particulièrement des correspondances chiffrées de Charles Quint et de ses relations avec la France.

Nous avions cherché d'autres courriers écrits par Charles Quint, mais l'astuce était de chercher des lettres envoyées au même destinataire Jean de Saint-Mauris.

Grâce à Camille, nous avons finalement appris qu'il existait d'autres lettres de la même époque, chiffrées et envoyées par Charles Quint toujours au même ambassadeur. Ces lettres étaient à Besançon. Nous avons pu les voir, et dans la marge, on pouvait lire que certains passages avaient été déchiffrés, probablement pour rendre la lecture plus aisée au destinataire. Il ne s'agissait alors plus d'une attaque à chiffré(s) seul(s), mais d'une attaque à couples clairs/chiffrés, et cela a, bien entendu, grandement facilité la fin de notre travail : en deux jours, nous avions déchiffré la majorité de la lettre.

En effet, cela nous a permis de mener notre analyse sur un corpus plus gros, d'identifier grâce aux passages transcrits dans la marge certains symboles et de comprendre l'élément qui nous manquait : nous avions noté que certains symboles comportaient des variantes avec des sortes de diacritiques, et les couples (clair, chiffré) trouvés à Besançon nous ont montré que ces diacritiques servaient à chiffrer les voyelles, et que les symboles ne correspondaient en fait qu'aux consonnes. Nous avions évoqué cette idée, et c'était un peu frustrant de nous voir donner la réponse... mais nous étions néanmoins heureux d'arriver au but et de voir le message prendre sens. Ceci dit, nous n'étions pas tout à fait au bout car certains morceaux restaient non déchiffrés. Ces passages faisaient notamment intervenir des symboles uniques, présents une seule fois dans le texte. Il semblait s'agir du nom de personnes importantes. L'exercice technique cryptographique était terminé, mais l'histoire n'était pas finie car nous avions envie d'aller au bout, et de comprendre l'intégralité de la dépêche. La partie déchiffrement en lien avec l'histoire a pu commencer. Pour cela, il a fallu nous appuyer sur les connaissances historiques afin d'éclairer les morceaux de phrases manquants, et de progresser petit à petit.

Pour l'anecdote, la lettre comprenait par exemple une phrase dans laquelle Charles Quint demandait à son ambassadeur comment la France réagissait après le trépas de « X »... Qui était « X » ? Le symbole utilisé laissait penser qu'il s'agissait d'un roi, mais sans plus... Comme la lettre semblait datée du 22 février 1546, nous avons cherché quel roi avait bien pu mourir à ce moment-là, mais les recherches historiques n'ont rien donné : aucun roi n'était mort en Europe à la fin de l'année 1545 ni au début 1546. Et pourtant c'était vrai ! Il ne fallait pas interpréter la date dans notre calendrier actuel, mais dans le calendrier de l'époque, dans lequel le début de la nouvelle année se situe au moment de Pâques. On comprend alors qu'il s'agissait de la mort du roi d'Angleterre Henry VIII, survenue le 28 janvier 1547.

En quoi vos travaux ont-ils contribué à enrichir la recherche historique ?

Au-delà du plaisir que cela a représenté pour nous de se frotter à un cryptogramme de cette nature, aussi ancien, le décryptage de ce texte apporte également des éléments qui intéressent nos collègues historiens. C'est extrêmement gratifiant, surtout que notre collègue historienne ne s'y attendait pas, les lettres diplomatiques étant d'habitude peu intéressantes, alors que celle-ci apporte des informations sur la situation géopolitique européenne de l'époque.

Certains passages mentionnent en effet des faits historiques, y apportant un éclairage qui a intéressé les historiens, notamment sur les contextes complexes des guerres de religion, ainsi que des craintes de Charles Quint que François Ier ne fomente un attentat contre lui. Certaines informations montraient clairement également la volonté de l'empereur de faire propager des rumeurs sur le roi de France, comme ce dernier le faisait également à son encontre. Les tournures des phrases n'étaient pas dénuées d'humour, et ce fut vraiment un plaisir que de les voir se révéler petit à petit.

Est-il maintenant possible de voir la missive chiffrée ? D'accéder à son contenu en clair ?

Le document est maintenant mis en valeur à la bibliothèque Stanislas de Nancy. De plus, un *fac simile*

numérique est aussi disponible depuis 2022 (voir encadré ci-après).

Notre transcription en clair n'est pas encore en ligne, elle le sera lorsque nous aurons publié l'article présentant ce travail interdisciplinaire. Depuis, nous avons entendu dire qu'un exemplaire historique du texte en clair existe, et serait probablement celui qui a été écrit avant d'être chiffré. Ce document serait à Vienne, mais nous n'avons pas encore pu le vérifier.

> « Ce qui nous a frappé dans cette aventure, c'est aussi la découverte pour nous des avancées en cryptanalyse à cette époque. »

Avez-vous d'autres objectifs du même genre en tête pour l'avenir ?

Ce n'est clairement pas la fin de notre collaboration avec Camille Desenclos (qui possède une centaine de telles lettres). Nous sommes aussi en contact avec quelqu'un en possession d'une lettre du grand-père de Charles Quint.

Ce travail a été relayé dans beaucoup de médias, y compris à l'étranger, et plusieurs autres lettres (d'autres contextes, et à l'intérêt historique pas forcément clair...) nous ont été envoyées. Ce qui nous a frappé dans cette aventure, c'est aussi la découverte pour nous des avancées en cryptanalyse à cette époque. En effet, si Charles Quint a pris tant de soin à composer des techniques visant à rendre l'analyse du cryptogramme si complexe, c'est qu'il savait (ou que ses conseillers savaient) exploiter des analyses de ce type sur des cryptogrammes moins complexes. Cela ne semblait pas correspondre à ce que l'on nous enseigne habituellement. Les techniques de l'époque sont peu connues et tout semble avoir été oublié. Il serait vraiment intéressant de lire les traités de cryptanalyse de cette époque. Il paraît qu'il en existe, ou plutôt qu'il en a existé, mais que sont-ils devenus ? C'est un autre mystère...

Merci beaucoup d'avoir partagé avec nous cette belle aventure, cela donne vraiment envie de s'attaquer à ce genre de quête ! Nous vous souhaitons également une bonne continuation pour vos autres travaux de recherche, moins médiatisés, mais tout aussi intéressants.

Article rédigé par Cécile Pierrot, Pierrick Gaudry, Paul Zimmermann (Université de Lorraine, CNRS, Inria, LORIA), Caroline Fontaine et Céline Chevalier, contact : cecile.pierrot@inria.fr, pierrick.gaudry@loria.fr, paul.zimmermann@inria.fr

Pour en savoir plus

Le *fac simile* numérique de la lettre originale est disponible à l'adresse suivante : https://galeries.limedia.fr/ark:/31124/dct0sbwx8vmhspk0/p1

L'article suivant contient une image avec le début de la lettre, ainsi que la clef reconstituée : https://www.inria.fr/fr/lettre-chiffree-charles-quint-enigme-cryptographie

Le déchiffrement de cette lettre a fait l'objet d'une forte couverture médiatique, voir par exemple cet article : https://www.theguardian.com/world/2022/nov/24/emperor-charles-vs-secret-code-cracked-after-five-centuries

Retour sur REDOCS

Diane Leblanc-Albarel

La septième édition des rencontres doctorants-entreprises (REDOCS) s'est une nouvelle fois déroulée au Centre International de Rencontres Mathématiques (CIRM), du 28 novembre au 3 décembre 2022.

REDOCS 2022

REDOCS est une occasion pour les doctorantes et les doctorants, de travailler sur des sujets proposés par des entreprises. Cette semaine de travail intensif est une occasion de découvrir un sujet souvent différent de celui traité durant la thèse. C'est également une occasion de se rencontrer, d'échanger et de découvrir de nouvelles façons de penser et de travailler. Cette année les sujets étaient :

- Sujet proposé par Cosmian : La conception d'un protocole d'authentification sécurisé avec une demande forte sur des propriétés de *privacy*.
- Sujet proposé par Cyber-Detect : Réalisation de signatures comportementales pour détecter des logiciels malveillants affectant les systèmes de fichiers.
- Sujet proposé par TrustInSoft : Conception d'une méthode automatique ou semi-automatique pour générer un jeu d'entrées fournissant une couverture d'arêtes à 100% sur chacune de plusieurs implémentations open-source en langage C de parseurs X.509.

Pour la première fois depuis 2019, toutes les équipes ont pu travailler avec leurs référentes et référents entreprise en chair et en os. Les doctorantes et doctorants ont alterné entre phases intensives de travail, présentations des organisateurs, phases moins intensives de travail,

échecs, réflexion et l'incontournable *social event* qui, cette année, était un jeu de piste géant par équipe dans le parc national et les calanques.

Retour d'une doctorante

REDOCS 2022 fut l'occasion pour moi de travailler sur un sujet que je voulais découvrir depuis longtemps. Ce sujet m'a énormément plu. Notre référente entreprise nous a guidés et aidés tout au long de la semaine. Je finis cette édition avec l'impression d'avoir beaucoup appris et l'envie d'approfondir le sujet sur lequel j'ai travaillé. Après avoir participé à trois REDOCS, si une personne me demande si ça vaut le coup de participer, je dirai oui sans hésiter. On dort peu certes (parce que l'on veut à la fin de la semaine présenter la meilleure solution possible), mais on apprend énormément. Côté scientifique, je trouve que REDOCS permet de se rappeler que même quand on ne connaît pas un sujet, on peut se former dessus. On ne devient évidemment pas un expert en une semaine, mais en travaillant en équipe, il est possible d'acquérir les bases d'un domaine et de faire des choses impressionnantes en peu de temps. C'est également l'occasion de tester un sujet de recherche qui pourrait nous plaire mais dont on ne connaît pas grand-chose. De plus, travailler avec des doctorantes et des doctorants d'autres laboratoires et d'autres domaines est, d'après moi, un formidable moyen de se former et d'apprendre. Faire une thèse, c'est aussi, il me semble, apprendre à réfléchir sur de nouvelles problématiques et à traiter plus facilement des questions inconnues dans des contextes nouveaux. Je trouve que participer à REDOCS permet d'en prendre conscience et de mettre en pratique cette compétence. Côté personnel, je me suis fait des amis et amies à chaque édition de REDOCS, j'ai rencontré des personnes avec qui je suis toujours en contact aujourd'hui et qui m'ont grandement appris. Beaucoup de rigolades et de découvertes, de paysages et de rencontres que je n'oublierai pas. Le cadre exceptionnel du CIRM permet de se plonger dans l'aventure REDOCS sans avoir à se soucier de rien d'autre que de chercher, discuter, réfléchir et admirer, en fond, le mont Puget.

PS : L'eau des calanques n'est pas si froide, même en décembre, un petit plongeon et on est plus créatif et d'attaque pour reprendre la recherche.

Diane Leblanc-Albarel (CNRS, INSA Rennes, IRISA), contact : diane.leblanc-albarel@irisa.fr

En direct des labos

La Gazette interviewe Antoine Miné et Damien Vergnaud, responsables de l'axe « sécurité, sûreté et fiabilité » du LIP6 (https://www.lip6.fr/recherche/team.php?acronyme=SSR), le laboratoire d'informatique de Sorbonne Université (UMR 7606) dirigé par Fabrice Kordon. Le laboratoire est composé de 19 équipes où travaillent 171 chercheurs et enseignants-chercheurs ainsi que 165 doctorants. Il est localisé au centre de Paris.

Bonjour, quels sont les axes scientifiques du LIP6 et, plus précisément, vos objectifs en matière de sécurité informatique ?

La recherche du LIP6 se structure autour de quatre axes scientifiques : l'axe « intelligence artificielle et sciences des données », l'axe « architecture, systèmes et réseaux », l'axe « théorie et outils mathématiques pour l'informatique » et l'axe « sécurité, sûreté et fiabilité ». Les 19 équipes du laboratoire participent chacune à un, et souvent à plusieurs, de ces axes. En matière de sécurité, la recherche est variée et étudie aussi bien le niveau matériel que les niveaux logiciel, système et réseau, avec des applications allant de l'informatique embarquée au web.

Les équipes APR et MoVe développent des méthodes formelles. Un premier objectif est de s'assurer que les systèmes et logiciels obéissent à leur spécification et sont exempts de comportement indéfinis, ce qui permet de limiter leur surface d'attaque. L'équipe MoVe développe le logiciel ITS-Tools de vérification par *model-checking*, ainsi que des algorithmes distribués de vérification pour augmenter leur efficacité. Elle travaille à la synthèse automatique de programmes distribués corrects à partir d'une spécification ainsi qu'à la vérification de systèmes distribués de taille paramétrique, c'est-à-dire de systèmes où le nombre d'agents participant n'est pas connu à l'avance, tout en étudiant la complexité des algorithmes de vérification associés. En cyber-protection, les travaux de MoVe ont pour objectif la mise en perspective des visions « attaquants » et « défenseurs » pour identifier les connaissances acquises par l'attaquant, ainsi que la détection de vulnérabilités.

L'équipe APR développe des approches « langages » pour la sûreté et la sécurité : systèmes de types pour les systèmes distribués, méthodes de développement sûr par raffinement en exploitant les assistants de preuve. L'équipe développe également des techniques d'analyse statique : l'analyseur MOPSA a pour objectif l'extension des méthodes d'interprétation abstraite à l'analyse de nouveaux langages et propriétés. L'outil cible la preuve d'absence de vulnérabilité en sûreté (accès mémoire, etc.) dans des programmes multi-langages, des propriétés de flot d'information, de dénis de service, l'analyse de *patches* et de portabilité, avec application aux logiciels avioniques embarqués, aux applications système et à la vérification de *smart contracts*.

L'équipe NPA s'intéresse à la sécurité des réseaux. Elle développe des architectures de systèmes et réseaux résilients, résistants aux fautes et aux attaques : réseaux de robots et de capteurs, réseaux véhiculaires, réseaux du futur, *blockchains*. Un autre axe de recherche concerne les aspects de métrologie liés à la sécurité des réseaux et la détection d'intrusion. L'équipe travaille également à la tolérance aux attaques byzantines en développant de nouveaux cadres fondamentaux, mieux adaptés aux réseaux modernes, sans fil et mobiles.

« En matière de sécurité, la recherche est variée et étudie aussi bien le niveau matériel, que les niveaux logiciel, système et réseau, avec des applications allant de l'informatique embarquée au web. »

L'équipe Complex Networks développe des méthodes pour l'étude de données modélisées par des flots de liens. En matière de sécurité, cet outil a pour objectif la détection d'anomalies dans des séquences d'interactions, notamment des transactions financières et du trafic réseau. Il est appliqué par exemple à la détection des fraudes financières, des usurpations d'identité, des attaques et des intrusions.

L'équipe ALMASTY est principalement orientée vers l'utilisation de techniques algorithmiques et mathématiques efficaces pour proposer et améliorer les cryptosystèmes modernes et évaluer leur niveau de sécurité autour des sujets suivants : sécurité réductionniste, (pseudo-)aléa en cryptographie, sécurité contre les attaques par canal auxiliaire, calcul réparti sécurisé, cryptographie (post-)quantique, cryptanalyse et calcul haute performance.

L'équipe ALSOC définit et développe des méthodes et des outils de conception de systèmes matériels et logiciels robustes à différents types d'attaque (attaques physiques ou logicielles).

Les travaux de l'équipe CIAN visent à sécuriser les circuits intégrés contre les menaces de piratage, surproduction, rétro-ingénierie, et chevaux de Troie matériels, en implantant dans les circuits intégrés des contre-mesures matérielles ou en proposant un flot de conception de confiance.

L'objectif de l'équipe PolSys en matière de sécurité informatique est d'analyser la sécurité des nouveaux standards de cryptographie post-quantique (et de fournir à la communauté scientifique des outils essentiels à ces analyses). Pour cela, elle développe et s'appuie sur une famille d'algorithmes et d'implantations haute-performance relevant du calcul formel pour mettre en œuvre des techniques de cryptanalyse algébriques.

L'objectif de l'équipe QI est d'utiliser le matériel quantique pour donner un avantage prouvable en matière de sécurité pour la communication sur des réseaux quantiques par rapport à ce qui est possible avec les systèmes « classiques » conventionnels. Cela va des cas où la sécurité au sens de la théorie de l'information est possible au niveau quantique mais pas au niveau classique (par exemple, dans la distribution de clés quantique) aux cas où il est possible de prouver des avantages en termes d'efficacité par rapport aux systèmes classiques (par exemple, en calcul réparti sécurisé).

Fabrice Kordon

Quelles sont vos collaborations dans ces domaines avec le tissu local, national et international ?

Le laboratoire bénéficie de nombreuses collaborations académiques et dans les entreprises.

Les équipes du laboratoire participent à de nombreux projets ANR en lien avec la sécurité (par exemple, SAPORO, PROSECCO, COFFI, IDROMEL, GORILLA, POSTCRYPTUM, SANGRIA, KLEPTOMANIAC, MOOSIC, STEALTH, SecNISQ, NISQ-TCS, SoLuQS, QUANTIFY). Au niveau national , l'équipe MoVe collabore avec l'équipe CIDRE (INRIA Rennes). Un partenariat entre l'équipe Complex Networks du LIP6 et la société Bleckwen est soutenu par l'ANR sous la forme d'un Labcom (« Laboratoire commun ») autour de l'analyse de flots de données et de fraudes financières. Des collaborations avec les entreprises se font également au moyen de thèses, par le dispositif CIFRE ou par la mise à disposition par les entreprises d'ingénieurs en poste pour réaliser des thèses académiques. Nous collaborons ainsi avec Airbus sur les logiciels embarqués, Nomadic Labs sur les *smart contracts*, ST Microelectronics sur la robustesse des systèmes sur puce, avec CryptoExperts, Google, IDEMIA, PQShield et Thales en cryptographie et avec Nokia Bell, PASQAL, Quandela et VeriQloud en informatique quantique. La start-up CryptoNext Security a été créée par des membres du LIP6.

Les équipes ALSOC et APR du laboratoire participent au PEPR Cybersécurité dans le projet Secureval, ce qui permet de renforcer les liens académiques au niveau national, avec par exemple le CEA, l'INRIA, les Universités Grenoble Alpes, Paris-Saclay, Rennes 1. L'équipe QI participe au PEPR Quantique via les projets EPIQ, DIQKD et QCommTestBed.

Au niveau international, l'équipe Polsys a participé au procédé de standardisation de cryptographie post-quantique du NIST et de la *Chinese Association for Cryptologic Research* (CACR) et contribue à divers organismes de standardisation autour de la cryptographie post-quantique (IEEE, IETF, Cloud Security Alliance, ETSI). L'équipe QI participe à de nombreux projets européens (ERC ou H2020 comme QOPT, QUANGO, QUDICE, QUSCO, QIA, et QSNP).

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

Les formations adossées à nos recherche sont principalement des parcours du Master d'informatique de Sorbonne Université.

— Le parcours « Sécurité, Fiabilité et Performance du Numérique » associe l'enseignement en cryptologie et en calcul haute-performance.
— Le parcours « Science et Technologie du Logiciel » est centré sur l'apprentissage de méthodes rigoureuses pour la conception, le développement et la vérification des logiciels.
— Le parcours « Systèmes et Applications Répartis » a pour objectif de former des spécialistes en conception et développement de systèmes répartis et propose des formations en sécurité et fiabilité des systèmes.
— Le parcours « Information Quantique » est centré sur le calcul et les communications quantiques, et inclut les problématiques de sécurité (cryptographies quantique et post-quantique, vérification, etc.)

Outre les filières recherche, qui orientent les élèves vers des stages de recherche et éventuellement des doctorats en laboratoire ou en entreprise, certains parcours offrent des filières professionnelles (dont certaines en apprentissage), ce qui permet de sensibiliser les futurs ingénieurs aux problématiques de sécurité et de leur présenter des travaux de recherches contemporains qui offrent des solutions à ces problèmes.

Nous enseignons également dans le Master Parisien de Recherche en Informatique, un Master multi-institutions très axé sur la recherche académique et dans l'industrie. Plusieurs membres du LIP6 ont participé ces dernières années à l'École d'été du GDR Sécurité Informatique et à d'autres écoles à destination des doctorantes, doctorants, jeunes chercheuses et jeunes chercheurs. L'équipe QI et le centre d'informatique quantique de Sorbonne Université a organisé l'École de printemps d'Informatique Théorique en 2021 sur l'informatique quantique.

L'équipe Polsys co-organise le programme thématique sur la cryptographie post-quantique de l'Institut Henri Poincaré qui aura lieu à l'automne 2024.

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

Les équipes CIAN et ALSOC ont réalisé des avancées originales dans le domaine de la sécurisation au niveau matériel et à l'interface entre logiciel et matériel. Ainsi, l'équipe CIAN a développé la technologie « SyncLock » de sécurisation anti-piratage des émetteurs-récepteurs radio fréquence. Ce circuit est indispensable dans les objets connectés permettant la communication sans fil. Cette technologie, primée par le concours i-PhD en 2022, a été brevetée en mars dernier et fait l'objet d'un programme de prématuration CNRS. L'équipe ALSOC a développé le logiciel ARMISTICE autour de la problématique de la preuve de masquage, qui est une contre-mesure logicielle contre les attaques par canal auxiliaire. Ce travail se distingue par le fait qu'il modélise le cœur de processeur à un niveau micro-architectural, ce qui lui permet de précisément modéliser la consommation de courant liée aux données et donc d'apporter des preuves d'absence de fuite plus précises que celles fournies aux niveaux algorithmiques ou ISA. L'équipe a également proposé des techniques originales, implantées dans le compilateur LLVM, pour s'assurer que les protections logicielles installées au niveau source pour détecter les attaques en faute sont préservées tout au long du flot de compilation optimisant.

Pour illustrer la diversité des travaux en sécurité du laboratoire, nous pouvons mentionner brièvement des avancées dans trois autres domaines bien différents : l'équipe Complex Networks a proposé une méthode de détection de transactions anormales dans des séquences massives, basée sur des métriques issues de théorie des graphes, l'équipe PolSys développe et distribue depuis deux ans msolve, une bibliothèque open-source de calcul de bases de Gröbner dont les performances sont les meilleures du moment, et l'équipe QI a créé et implanté des protocoles de délégation de calcul quantique vérifiables et réalisé une démonstration expérimentale à longue distance de la distribution de clés quantiques à variation continue.

Merci .... pour toutes ces informations sur l'organisation du LIP6 et vos domaines de recherche !

Article rédigé par Antoine Miné, Damien Vergnaud (responsables de l'axe « Sécurité, sûreté et fiabilité » du LIP6) et Céline Chevalier, contact : antoine.mine@lip6.fr, damien.vergnaud@lip6.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. Si vous souhaitez vous abonner pour les recevoir en temps réel, rendez-vous sur https://gdr-securite.irisa.fr/listes/

Poste de responsable de la sécurité des systèmes d'information (CDI), Storyzy (Toulouse)

Sujet : Responsable de la politique de sécurité des systèmes d'information : prévention, protection, détection, résilience et remédiation
Yulliwas Ameur, ameur.yulliwas@gmail.com

Poste d'ingénieur-chercheur (CDI), Thalès (Palaiseau)

Sujet : Méthodes formelles
Nikolaï Kosmatov, nikolaikosmatov@gmail.com

Poste de professeur, ENSEEIHT, LAAS-CNRS (Toulouse)

Sujet : Systèmes numériques matériels (section 63)
Pierre Lopez, pierre.lopez@laas.fr

Quatre postes de MCF, LAAS-CNRS (Toulouse)

Sujets : Intelligence Artificielle : Machine Learning pour les systèmes de confiance (section 27) / Électronique numérique, électronique des systèmes - Conception, architecture et caractérisation (section 63) / Systèmes et instrumentations hyperfréquences pour les domaines des communications, de la santé, de l'environnement et du spatial (section 63) / Systèmes électroniques, objets connectés, autonomie énergétique (section 63)
Pierre Lopez, pierre.lopez@laas.fr

Deux postes de MCF, Université Paris 8, LIASD (Saint Denis)

Sujets : IA et modélisation / Synthèse d'images, IA et modélisation
Pablo Rauzy, pr@up8.edu
Nicolas Jouandeau, n@up8.edu

Deux postes de MCF, Université Gustave Eiffel, ESIEE Paris, LIGM (Noisy le Grand)

Sujets : Informatique (section 27) / Informatique et cybersécurité (section 27)
Laurent Perroton, Jean Cousty, prenom.nom@esiee.fr
Stéphane Vialette, stephane.vialette@univ-eiffel.fr

Poste de MCF, IUT Clermont-Ferrand, LIMOS (Clermont-Ferrand)

Sujet : Réseaux et sécurité (section 27)
Pascal Lafourcade, pascal.lafourcade@uca.fr

Poste de MCF, INSA Rennes, IRISA (Rennes)

Sujet : Cybersécurité, ou Génie Logiciel, ou Intelligence Artificielle
Gildas Avoine, Jean-Louis Pazat, prenom.nom@insa-rennes.fr
Guillaume Gravier, guillaume.gravier@irisa.fr

Poste de MCF, Télécom SudParis (Evry)

Sujet : Cybersecurity engineering, threat and vulnerability management, digital trust
Maryline Laurent, Joaquin Garcia-Alfaro, prenom.nom@telecom-sudparis.eu

Poste de MCF, IUT Grand Ouest Normandie, GREYC (Saint-Lô/Caen)

Sujet : Analyse d'images, Apprentissage automatique, Cybersécurité (section 27)
Christophe Charrier, christophe.charrier@unicaen.fr
Christophe Rosenberger, christophe.rosenberger@ensicaen.fr

Poste de MCF, LAMIH, UPHF-INSA Hauts de France (Valenciennes)

Sujet : Informatique / Architectures, Données et Services Performants et Sécurisés pour Systèmes Mobiles et Embarqués (section 27)
Antoine Gallais, Laurent Dubar et René Mandiau, prenom.nom@uphf.fr

Poste de post-doctorat, King's College London (Londres, UK)

Sujet : Security of Extended Reality Systems
Luca Vigano, luca.vigano@kcl.ac.uk

Poste de post-doctorat, Lip6, Sorbonne Université (Paris)

Sujet : Étude de vulnérabilités et attaques physiques à distance sur un dispositif de communication quantique QKD
Eleni Diamanti, eleni.diamanti@lip6.fr

Thèse de doctorat, KTH Royal Institute of Technology (Stockholm)

Sujet : CHAINS : Consistent Hardening and Analysis of Software Supply Chains
Musard Balliu, musard@kth.se

Thèse de doctorat, Université Catholique de Lille, INRIA et IN Groupe (Lille)

Sujet : IoT based decentralized identity checking
Nicolas Gouvy,
Nicolas.Gouvy@univ-catholille.fr
Nathalie Mitton, Nathalie.Mitton@inria.fr

Thèse de doctorat, CEA List (Palaiseau)

Sujet : Inférence de spécifications d'interaction avec stratégie adversariale
Boutheïna Bannour, boutheina.bannour@cea.fr

Thèse de doctorat, IETR/DGA (Nantes)

Sujet : XAirGap : Creating and detecting long distance covert channels on airgapped computers
Maria Mendez Real,
maria.mendez@univ-nantes.fr

Thèse de doctorat, IRIT (Toulouse)

Sujet : Formalization of Security Mechanisms Placement : A Scenario-based Approach
Brahim Hamid, brahim.hamid@irit.fr
Abdelhakim Baouya,
abdelhakim.baouya@irit.fr
Nan Messe, nan.messe@irit.fr

Thèse de doctorat, LTCI, Télécom Paris (Palaiseau)

Sujet : Approche ingénierie dirigée par les modèles pour évaluer la sécurité des systèmes Cyber-physiques
Jean Leneutre,
jean.leneutre@telecom-paris.fr

Thèse de doctorat, CRIStAL (Lille)

Sujet : Apprentissage profond pour la détection de falsifications et l'évaluation de la confidentialité dans les images numériques
Pauline Puteaux, pauline.puteaux@cnrs.fr
Patrick Bas, patrick.bas@cnrs.fr

Trois stages de Master, INSA Centre Val de Loire, LIFO (Bourges)

Sujets : Use of semantic pertinence to improve accuracy in differentially private projection processes / Differential privacy in relational or graph databases / Semantic attack on graph databases
Adrien Boiret, adrien.boiret@insa-cvl.fr

Deux stages de Master, IETR (Rennes/Nantes)

Sujets : Etude des menaces en cybersécurité des équipements électroniques par voie électromagnétique / Conception de niveau système pour l'estimation de la sécurité des systèmes multiprocesseurs à ressources partagées
Maria Mendez Real,
maria.mendez@univ-nantes.fr

Stage de Master, INSA Centre Val de Loire, LIFO (Bourges)

Sujet : Étude des signatures assainissables et application à l'anonymisation
Benjamin Nguyen
benjamin.nguyen@insa-cvl.fr
Xavier Bultel, xavier.bultel@insa-cvl.fr

Stage de Master, GREYC (Caen)

Sujet : Détection de deepfakes vidéo
Christophe Charrier
christophe.charrier@unicaen.fr
Emmanuel Giguet, emmanuel.giguet@unicaen.fr

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

Sujet : Security Analysis of a Cyber-Physical Platform
Gregory Blanc,
gregory.blanc@telecom-sudparis.eu
Jean Leneutre,
jean.leneutre@telecom-paris.fr
Olivier Levillain,
olivier.levillain@telecom-sudparis.eu

Stage de Master 1, IRIT (Toulouse)

Sujet : Développement logiciel pour learn-ocaml : authentification modulaire et analyse de sécurité
Yannick Chevalier yannick.chevalier@irit.fr
Erik Martin-Dorel, erik.martin-dorel@irit.fr

Stage de Master, INSA Centre Val de Loire (Bourges)

Sujet : Modélisation logique de la confiance dans les architectures Zero Trust
Laurent Bobelin laurent.bobelin@insa-cvl.fr
Sabine Frittella, sabine.frittella@insa-cvl.fr

Stage de Master, IRISA (Rennes)

Sujet : Autoprotection des systèmes par une approche blockchain : application à l'exfiltration des données
Mohamed Chalouf
mohamed-aymen.chalouf@irisa.fr
Romaric Ludinard,
romaric.ludinard@imt-atlantique.fr
Guillaume Doyen, guillaume.doyen@irisa.fr

Équipe éditoriale

Directrices éditoriales :
- Céline Chevalier, *CRED, Univ. Paris 2*
- Pauline Puteaux, *CRIStAL, CNRS*

Directrice de publication :
- Caroline Fontaine, *LMF, CNRS*