Demande n°3813 - ARED

Acronyme :ARMADA

Identification

Identification

N°	3813
Année	2025
Statut	Brouillon
Date de création	23/01/2025
Date de modification	28/01/2025
Date de soumission	28/01/2025
Acronyme	ARMADA
Intitulé du projet	ARM Microarchitectural Attacks Discovery and Analysis
Dispositif	ARED
Civilité du porteur	Monsieur
Nom du porteur	Hiet
Prénom du porteur	Guillaume
Courriel	guillaume.hiet@centralesupelec.fr

Priorité régionale

Priorité régionale

Priorité régionale	Lien avec une politique publique de la Région (Cybersécurité, Agroécologie, Mer, Mobilités, Ports, Langues de Bretagne)
Regional priority	Lien avec une politique publique de la Région (Cybersécurité, Agroécologie, Mer, Mobilités, Ports, Langues de Bretagne...)

Stratégie régionale de recherche et d’innovation (S3)

Stratégie régionale de recherche et d’innovation (S3)

Domaine d'innovation stratégique principal	Économie numérique sécurisée et responsable
Domaine d'innovation stratégique	.
Levier thématique associé au DIS principal	Cybersécurité

Organisme de tutelle

Organisme de tutelle

Etablissement	CENTRALE SUPELEC
Commune	CESSON-SEVIGNE
Civilité	Monsieur
Nom	LOUET
Prénom	Yves

Unité de recherche

Unité de recherche

Nom de l'unité	IRISA
Civilité	Monsieur
Nom	GRAVIER
Prénom	Guillaume
Tél.	0299847239
Courriel	dir@irisa.fr

Données complémentaires de l'unité de recherche

Libellé	Valeur
Statut et numéro de l'unité de recherche (UMR, USR, EA)	UMR 6074
Le cas échéant, nom de l'équipe de recherche	SUSHI/CAPSULE (co-encadrement)
Le cas échéant, nom du responsable de l'équipe de recherche	Guillaume Hiet (SUSHI) / Pierre-Alain Fouque (CAPSULE)
Activités de recherche et points forts de l'équipe	SUSHI : Sécurité à l'interface logiciel/matériel, sécurité bas niveau, modèles formels et preuves de sécurité CAPSULE : Cryptographie (classique, quantique et post-quantique), sécurité des implémentations cryptographiques, exploitation de canaux auxiliaires matériel et microarchitecturaux.
Si implication dans un/plusieurs programmes européens ou internationaux, préciser	

Co-directeur de thèse

Co-directeur de thèse

Civilité	Monsieur
Nom	Fouque
Prénom	Pierre-Alain
Unité de recherche	UMR IRISA
Etablissement de tutelle	UNIVERSITE RENNES 1

Description

Description du projet

Libellé	Valeur
Résumé synthétique du projet (2000 caractères max)	Les canaux auxiliaires visent à exploiter les effets secondaires de traitement d'information afin de faire fuiter de l'information. Les dernières décennies témoignent du développement considérable de ce domaine de recherche, tant par le vecteur de fuite que par la portée des attaques. Jusqu'à présent, la majorité des recherches se sont concentrées sur les microarchitectures Intel x86, en raison de leur large déploiement. Cependant, les architectures ARM, historiquement dominantes dans le secteur des smartphones et de l'embarqué, gagnent rapidement des parts de marché et sont en voie de déploiement massif sur des plateformes desktop d'ici à 2030 (comme les puces M1 et M2 d'Apple, ou le processeur desktop ARM annoncé par Qualcomm). Face à cette évolution, et la variété de plateformes concernées, il est primordial de porter une plus grande attention à la sécurité de ces microarchitectures. En particulier, contrairement à l'architecture x86, les microarchitectures ARM sont développées par une multitude de fabricants qui personnalisent et modifient les conceptions de base. Cette diversité accroît la complexité de l'analyse des vulnérabilités potentielles et élargit la surface d'attaque en introduisant différentes interactions entre les composants. Comprendre et sécuriser ces architectures hétérogènes est donc un défi crucial pour assurer la protection des systèmes informatiques modernes. Compte tenu de ce contexte, l'objectif de ce projet est d'apporter une analyse approfondie des microarchitectures basées sur ARM afin d'identifier le possible portage d'attaques identifiées sur x86 ou de nouvelles attaques exploitant des vulnérabilités propres aux caractéristiques de cette microarchitecture. L'état de l'art sur les architectures ARM se concentrant principalement sur des attaques sur le cache, de nombreux vecteurs classiques n'ont pas été suffisamment évalués, tels que des prefetchers, de la mémoire ou de la contention dans le pipeline d'exécution.
Caractère structurant/stratégique du projet (descriptif/ex. : art.5 Rglmt ARED 2025 -2000 car. max)	Le présent sujet se situe à l'intersections de deux projets du PEPR CYBERSECURITE : * REV : Le projet étudiant l'exploitation de vulnérabilités microarchitecturales, il s'applique particulièrement au sein du défi "Exploitation de vulnérabilité en investigation numérique", ou REV, du PEPR. En particulier, le projet correspond au WP2 sur la sécurité de l'interface logicielle/matérielle et l'étude de sa surface d'attaque. * ARSENE : Le projet se concentrant sur des processeurs et SoCs ARM, particulièrement répandus dans le monde de l'embarqué, inscrit cette thèse dans les thématiques du projet ARSENE du PEPR. En particulier, certains travaux de sécurité offensive et défensive pourraient mener à des contributions pertinentes dans le lot 2, "sécurité du SoC", en particulier sur les accélérateurs et les mémoires sécurisées.
Porteur du projet : date d'obtention de l'HDR ou dérogation	HDR obtenue en 2021
Collaborations scientifiques (nature/pays) et partenariat socio-économique envisagé (3000 car. max.)	Cette thèse serait menée en collaboration entre l'équipe CAPSULE (Inria, Irisa, CNRS, Univ Rennes) et l'équipe SUSHI (Irisa, CentraleSupélec). À ce titre, les membres du projet seront invités à collaborer avec les différentes équipes impliquées, voire profiter de la large expertise des chercheurs du bassin rennais (e.g. Walter Rudametkin pour le fingerprinting de navigateur, les équipes PACAP/TARAN sur des questions d'architecture, l'équipe SPICY pour les thématiques de sécurité offensive). En outre, la collaboration internationale sera mise en avant lors de la thèse, afin de poursuivre des travaux en communs avec des chercheurs de renommée internationale (Daniel Gruss, Michael Schwarz, Yossi Oren, Clémentine Maurice) afin de former le doctorant à la recherche collaborative et renforcer le lien avec des laboratoires européens.
Si DIS identifié, préciser l'adéquation du projet avec le DIS (2000 car. maximum)	Le projet de thèse ARMADA s'inscrit pleinement dans le DIS "Économie Numérique Sécurisée et Responsable", et en particulier dans le levier thématique "cybersécurité". Ce projet cible l'analyse des vulnérabilités microarchitecturales des processeurs ARM, qui dominent le secteur des systèmes embarqués et mobiles et émergent dans les plateformes desktop. Ces recherches répondent directement aux enjeux croissants de cybersécurité, car les architectures ARM sont de plus en plus exploitées dans des environnements critiques, mais restent relativement peu étudiées comparées aux

	architectures Intel. En étudiant les spécificités des microarchitectures ARM, le projet vise à renforcer la sécurité des composants matériels et logiciels embarqués, tout en explorant de nouvelles techniques d'attaques et de défense. Cette démarche contribue au développement d'une expertise locale dans un domaine stratégique, en lien avec la DGA-MI, Creach Labs et d'autres acteurs régionaux et nationaux de la cybersécurité. De plus, les travaux de cartographie des vulnérabilités et de rétro-ingénierie permettront d'identifier des failles exploitables, de proposer des contre-mesures adaptées et de prévenir des menaces émergentes, assurant ainsi la résilience des systèmes critiques. Le projet renforce également l'intégration de la Bretagne dans les réseaux internationaux de recherche, en collaborant avec des laboratoires de renom et en participant à des initiatives stratégiques telles que le PEPR Cyber et les projets européens. Enfin, ARMADA promeut la souveraineté numérique en contribuant à la sécurisation des technologies ARM.
Si priorité régionale cochée, préciser en quoi le projet s'y rattache effectivement (2000 car.max.)	Le projet ARMADA s'attache à la priorité régionale "Cybersécurité", en lien direct avec le levier stratégique identifié dans le DIS S3 "Économie Numérique Sécurisée et Responsable". Cette priorité, qui vise à renforcer la souveraineté numérique et la sécurité des systèmes critiques, est en accord avec les objectifs présentés par CreachLabs. En explorant les vulnérabilités microarchitecturales spécifiques aux processeurs ARM, le projet répond aux défis actuels de sécurisation des composants matériels et logiciels, essentiels pour les infrastructures critiques et les environnements sensibles. Ce projet bénéficie également de l'intérêt marqué de la DGA-MI, exprimé notamment par David Elleouet (Chargé de l'expertise de la sécurité des composants cryptographiques étatiques à DGA-MI), pour développer une expertise régionale sur ces thématiques. ARMADA constitue une opportunité pour le bassin rennais de se positionner comme un centre d'excellence en recherche appliquée à la sécurité des microarchitectures ARM. À travers cette collaboration, le projet vise non seulement à renforcer les connaissances locales, mais également à les diffuser auprès d'acteurs stratégiques tels que la DGA et l'ANSSI, consolidant ainsi leur capacité à anticiper et contrer les menaces émergentes. En outre, ARMADA promeut une approche proactive en cybersécurité, alignée sur les priorités régionales et nationales, tout en favorisant des synergies internationales avec des chercheurs de renom. Cette dynamique contribue à faire rayonner les compétences bretonnes dans le domaine de la sécurisation numérique, tout en inscrivant la Région Bretagne comme un acteur clé dans le paysage cyber national et européen.
Si priorité régionale "Politique publique Région", préciser (voir liste au point 4, Règlement 2025)	N/A
Cotutelle financière internationale (oui/non)	non
Nom(s) du(des) cofinanceur(s) envisagé(s) ou confirmé(s)	Le dossier a été soumis à CREACHLABS
Si cofinancement industriel, justifier le choix du dispositif ARED au lieu du dispositif CIFRE	
État du cofinancement (indiquer "acquis" ou "demandé")	demandé
Si demandé, date prévisionnelle de réponse du cofinanceur	Liste courte des projets retenus : 21/02/2025 Réponse définitive : 06/06/2025
Si cofinancement refusé, autre(s) source(s) de cofinancement identifiée(s)	
Si reversement prévu, préciser (partenaire, montant)	

Candidat

Collaboration internationale

Collaboration internationale

Pays	
Etablissement partenaire à l'étranger	

Pièces jointes

Date de mi	Type de pièce	Commentaire	Document	Valide	Commentaire
28/01/2025	ARED - Dépôt - CV du porteur	Obligatoire - Le CV doit préciser si le porteur est titulaire de l'HDR et, le cas échéant, depuis quand, et mentionner la liste des doctorant·e·s déjà encadré·e·s et des publications associées.	CV_qualif.pdf	Non traité	
28/01/2025	ARED - Dépôt - Avis directeur·rice d'unité	Obligatoire - Voir le modèle à suivre dans l'onglet "Documents à télécharger"		Non traité	
28/01/2025	ARED - Dépôt - Justificatif cofinancement	Facultatif - Dépôt de demande, justificatif d'obtention, courrier du cofinanceur pressenti...		Non traité	
28/01/2025	ARED - Dépôt - Lettre partenaire étranger	Facultatif - Lettre d'engagement de l'établissement partenaire étranger en cas de cotutelle internationale		Non traité	
28/01/2025	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
28/01/2025	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
28/01/2025	ARED - Instruction - Lettre de saisine	Lettre de l'établissement à transmettre à la Région (utiliser le modèle disponible dans la rubrique "Documents à télécharger")		Non traité	
28/01/2025	ARED - Versement - Convention de partenariat	Le cas échéant (si autorisation de reversement)		Non traité	
28/01/2025	ARED - Versement 2 - CV doctorant.e	Pour versement tranche 2		Non traité	
28/01/2025	ARED - Versement 2 - Copie du contrat doctoral (ou CDD ou attestation))	Pour versement tranche 2		Non traité	
28/01/2025	ARED - Versement 2 - Attestation bon déroulement travaux année 1	Pour versement tranche 2		Non traité	
28/01/2025	ARED - Versement 2 - Bilan financier année 1	Pour versement tranche 2 ARED		Non traité	
28/01/2025	ARED - Versement 3 - Attestation bon déroulement travaux année 2	Pour versement 50% tranche 3 ARED		Non traité	
28/01/2025	ARED - Versement 3 - Bilan financier année 2	Pour versement 50% tranche 3 ARED		Non traité	
28/01/2025	ARED - Versement 4 - Bilan financier année 3	Pour versement solde année 3 ARED		Non traité	
28/01/2025	ARED - Versement 4 - Certificat administratif précisant statut thèse	Pour versement du solde de la tranche 3		Non traité	

Curriculum Vitae

Guillaume HIET

Professeur contractuel en informatique à CentraleSupélec
Responsable de l'équipe-projet Inria SUSHI

Sommaire

1 Curriculum vitae **2**
1.1 Formation . . . 2
1.2 Expérience professionnelle . . . 3

2 Activités d'enseignement **3**
2.1 Fonctions exercées . . . 4
2.2 Enseignements effectués . . . 4

3 Activités de recherche **5**
3.1 Résumé de la thématique et compétences scientifiques . . . 5
3.2 Projets et collaborations . . . 6
3.3 Responsabilité d'équipe . . . 8
3.4 Activités d'intérêt collectif . . . 9
3.5 Présentations invitées (liste non exhaustive) . . . 10

4 Activités d'encadrement **11**
4.1 Encadrement d'étudiants de master . . . 11
4.2 Encadrement doctoral . . . 12
4.3 Publications et brevets . . . 13

5 Annexes **20**

1 Curriculum vitae

Nom :	**Guillaume HIET**
Date et lieu de naissance :	Le 20 avril 1981 à Montluçon (Allier), 43 ans
Nationalité :	Française
Situation familiale :	Marié, trois enfants
Situation administrative :	Professeur contractuel (CDI) à CentraleSupélec
Equipe de recherche :	Equipe-projet Inria SecUrity at the Software/Hardware Interface (SUSHI)
Unité de recherche :	Laboratoire IRISA (Institut de Recherche en Informatique et Systèmes Aléatoires) - Unité Mixte de Recherche 6074
Section CNU :	27 (Informatique)
Adresse professionnelle :	Campus de Rennes de CentraleSupélec, Avenue de la Boulaie, 35576 Cesson-Sévigné CEDEX.
Email :	guillaume.hiet@centralesupelec.fr
Web :	https://guillaume.hiet.fr

1.1 Formation

Année	Diplôme
2021	**Habilitation à Diriger les Recherches en informatique** de l'Université de Rennes 1 Sujet : *Security at the Hardware/Software Interface* Laboratoire : IRISA Jury : — Thomas Jensen, DR Inria, Président — Lilian Bossuet, Professeur des Universités, Université Jean Monnet, Rapporteur — Karine Heydemann, Maître de Conférence HDR, Sorbonne Université, Rapporteur — Trent Jaeger, Professor, The Pennsylvania State University, Rapporteur — Aurélien Francillon, Professeur à EURECOM — Valérie Viet Triem Tong, Professeur à CentraleSupélec
2005–2008	**Doctorat d'Informatique** de l'Université de Rennes 1 Sujet : *Détection d'intrusions paramétrée par la politique de sécurité grâce au contrôle collaboratif des flux d'informations au sein du système d'exploitation et des applications : mise en œuvre sous Linux pour les programmes Java* Directeur de thèse : Ludovic Mé, Professeur à Supélec Laboratoire : Supélec, équipe SSIR (EA 4039) Mention Très Honorable
2004-2005	**Master Recherche**, Supélec, Rennes, option Informatique, mention Très Bien. Sujet : *Détection d'intrusion paramétrée par la politique de sécurité : un modèle amélioré pour le contrôle de flux de références* Encadrant : Ludovic Mé, Professeur à Supélec
2003–2005	**Diplôme d'Ingénieur Supélec**, Supélec, Gif-sur-Yvette puis Rennes, option Informatique Systèmes et Réseaux
2001–2003	**Diplôme d'Ingénieur ENSAM** (Ecole Nationale Supérieur des Arts et Métiers), Bordeaux puis Paris, diplômé en 2005 (double-diplôme avec Supélec).

1.2 Expérience professionnelle

Année	Nature
2022-	**Professeur contractuel (CDI)** à CentraleSupélec (Rennes) au sein de l'équipe CIDRE puis SUSHI (responsable d'équipe depuis 2024) du laboratoire IRISA
2010-2022	**Maître de Conférence contractuel (CDI)** à CentraleSupélec (Rennes) au sein de l'équipe CIDRE du laboratoire IRISA
2020-2021	**Délégation Inria (100%)** au sein de l'équipe CIDRE du laboratoire IRISA
2019-2020	**Délégation Inria (50%)** au sein de l'équipe CIDRE du laboratoire IRISA
Juillet 2016	**Visiting Scientist** au laboratoire de recherche HP Labs (Bristol, Angleterre) (`1 mois`), collaboration sur la sécurité des micrologiciels de démarrage
2008-2010	**Expert Cybersécurité (CDI)** à AMOSSYS SAS (Rennes), une société de conseil et d'expertise en sécurité des technologies de l'information.
2008-2010	**Enseignant (vacataire)** à Supélec (Rennes)
2005-2008	**Thèse de doctorat (CDD)** a Supélec (Rennes) au sein de l'équipe SSIR
2005-2008	**Enseignant (vacataire)** à Supélec (Rennes) et à l'ESTACA (Laval)
2005	**Stagiaire en Master Recherche (CDD)** à Supélec (Rennes) (`6 mois`)

2 Activités d'enseignement

J'ai effectué mes enseignements en informatique pour des publics variés de spécialistes ou de non spécialistes, en formation initiale comme en formation continue, de niveau licence (première année d'école d'ingénieurs) et master (deuxième et troisième années d'école d'ingénieurs). Ces enseignements ont porté à la fois sur mon domaine de recherche, la sécurité informatique, et sur d'autres domaines de l'informatique. Ma charge d'enseignement, croissante ces dernières années, dépasse généralement la charge d'enseignement nominale attendue. Pour l'année 2019/2020, ma charge d'enseignement était réduite en raison de ma délégation partielle à Inria (50%), dans le cadre de l'organisation du semestre thématique cyber SILM dont j'étais le porteur. En 2020/2021, j'étais en délégation complète (100%) à Inria ce qui m'a permis d'obtenir une décharge complète de ma charge d'enseignement. Cette décharge m'a permis de rédiger et soutenir mon HDR. En 2023/2024, ma charge d'enseignement prévisionnelle (en excluant les décharges pour responsabilité) est de 218 h ETD.

2.1 Fonctions exercées

Année	Fonction	Lieu
2010-2022	Maître de Conférence contractuel	CentraleSupélec
2016-2018	Vacataire	ENS de Rennes
2012-2018	Vacataire	Institut National des Hautes Etudes de la Sécurité et de la Justice
2010-2018	Vacataire	Université de Rennes 1
2010-2018	Vacataire	Ecole militaire des transmissions (ETRS)
2013-2015	Vacataire	Université de Limoges
2005-2010	Vacataire	Supélec
2005-2008	Vacataire	ESTACA

2.2 Enseignements effectués

Le tableau 1 synthétise la répartition et l'évolution de ma charge d'enseignement depuis que je suis enseignant-chercheur à CentraleSupélec. Ce tableau donne ma charge en heure équivalent TD (ETD) en formation initiale à CentraleSupélec (cursus ingénieur), en formation continue à CentraleSupélec (principalement dans les mastères spécialisés MCS à Rennes et ASI à Gif) et à l'extérieur (ENS, université de Rennes 1 et de Limoges, INHESJ, ETRS). Les tableaux 4, 3 et 2 en annexe détaillent ma charge d'enseignement pour les trois dernières années.

Table 1 – Evolution de ma charge d'enseignement en heures ETD

Année	Formation Initiale	Formation Continue	Extérieure	Total
2022-2023	248,5	10,5	14	273
2021-2022	217,5	10,5	0	228
2019-2020	97	35	0	132
2018-2019	214	114	34	362
2017-2018	202	91	49	342
2016-2017	176	75,5	55	306,5
2015-2016	149	98	46,5	293,5
2014-2015	163	119	39	321
2013-2014	120	87	44	251
2012-2013	116	46	46	208
2011-2012	95	39	39	172
2010-2011	86	60	34	180

J'ai également assuré des vacations d'enseignement à Supélec en détection d'intrusion et en sécurité Unix (environ 11 heures ETD par an) lorsque j'étais ingénieur expert en cybersécurité à AMOSSYS (2008-2010). Durant ma thèse de doctorat (2005-2008), j'ai assuré des vacations d'enseignement à Supélec (Introduction à Linux, TP de modélisation réseau) et à l'ESTACA en traitement du signal (responsabilité du cours pour le campus de Laval, incluant les cours magistraux, TD, TP et examen). Ces enseignements représentaient 64 heures ETD par an.

3 Activités de recherche

3.1 Résumé de la thématique et compétences scientifiques

Mon domaine de recherche est la **cybersécurité**. Je focalise mes travaux sur les **attaques logicielles**. Ce type d'attaques se distingue des attaques physiques (par exemple, l'injection de fautes) qui nécessitent de mesurer ou influencer une grandeur physique.

Mes recherches porte principalement sur la **détection d'intrusion** basée sur l'hôte (*Host-based Intrusion Detection Systems*) et la **supervision de sécurité** de manière générale. Je m'intéresse plus particulièrement à la sécurité des logiciels « proches du matériel ».

Supervision de sécurité : Dans le cadre de la thèse CIFRE de Georges Bossert, réalisée en collaboration avec la société AMOSSYS, nous nous sommes intéressés à la **rétro-conception de protocoles** de communication. Ces travaux ont été publiés à la conférence ACM AsiaCCS 2014 (rang B d'après CORE).

Dans le projet SecCloud, financé par le Labex CominLabs, nous avons développé une approche de **suivi dynamique de flux d'information (DIFT) au sein du navigateur web** avec mon doctorant Deepak Subramanian. Ces travaux ont fait l'objet de publications dans les conférences FPS 2016 et ACM SIN 2016 (*best paper award*).

De 2015 à 2018 j'ai également co-encadré la thèse de Oualid Koucham en collaboration avec des collègues du laboratoire GIPSA-Lab à Grenoble et de la Direction Générale de l'Armement (DGA). Nous avons proposé des approches de **détection d'intrusion et de corrélation d'alertes adaptées aux systèmes de contrôle industriel**. Ces travaux ont fait l'objet de publications dans les conférences NordSec 2016 et SafeProcess 2018, ainsi que dans le journal Computers and Security en 2022.

Détection d'intrusion assistée matériellement : Mes recherches actuelles visent à répondre aux défis des HIDS que sont la protection de l'IDS et la limitation de l'impact sur le système surveillé en tirant parti de composants matériels dédiés. Ainsi dans le cadre de la thèse CIFRE de Ronny Chevalier, en partenariat avec la société HP, nous avons proposé un **coprocesseur de sécurité pour détecter les intrusions** visant le BIOS de l'ordinateur. Nous avons publié nos résultats dans la conférence ACSAC (rang A d'après CORE, H5 Index 29) en 2017. Ces travaux ont également fait l'objet de deux demandes de brevets qui nous ont été accordés : US11556645B2 (en 2023) et US11308202B2 (en 2022).

De même dans le projet HardBlare, financé par le Labex CominLabs, nous nous sommes intéressés à la définition d'un **coprocesseur dédié au DIFT** implémenté sur FPGA d'un système sur puce (SoC) ZYNQ. Ces travaux ont notamment été publiés à la conférence FPL 2017 (rang A, H5 Index 17).

Plus récemment, dans le cadre d'une collaboration avec Isabelle Puaut de l'équipe-projet Inria PACAP, je participe à l'encadrement de la thèse de Nicolas Bellec sur l'utilisation des analyses de pire temps d'exécution (WCET) pour **détecter des intrusions dans les systèmes temps réel**. Ces travaux ont fait l'objet d'une publication dans la conférence ECRTS en 2022 (rang A d'après CORE) qui a obtenu un *outstanding paper award*.

Réaction aux intrusions : Dans le cadre de la thèse de Ronny Chevalier, nous avons proposé une approche permettant d'apporter des capacités de **survivabilité au niveau du système d'exploitation**. Ces travaux ont fait l'objet de publications à la conférence ACSAC 2019 (rang A d'après CORE) et dans le journal ACM *Digital Threats : Research and Practice* en 2020 ainsi que deux dépôts de brevet qui nous ont été accordés (US10896085B2 et EP3647980B1).

De même, dans le cadre d'une collaboration avec Erven Rohou de l'équipe-projet Inria PACAP, j'ai participé à l'encadrement de la thèse de Camille Le Bon. Dans ces travaux, publiés à l'atelier SILM 2021, nous proposons une approche adaptative permettant d'**instrumenter dynamiquement le code d'une application pour y appliquer des protections**.

Sécurité des interfaces logiciel/matériel : Ces travaux m'ont amené plus généralement à m'intéresser à la sécurité des interfaces logiciel/matériel. J'ai organisé un semestre thématique sur le sujet (SILM), financé par la DGA.

Je me suis également intéressé dans le cadre de la thèse de Thomas Letan, en collaboration avec l'Agence Nationale des Systèmes d'Information (ANSSI), à la **formalisation des plateformes matérielles et des mécanismes de sécurité** qu'elles proposent. Ces travaux ont été publiés à la conférence FM (FME) 2016 (rang A d'après CORE, H5 Index 15).

Nous avons également proposé une nouvelle approche permettant la **vérification modulaire d'architecture matérielle complexe** à l'aide de Coq. Ce travail, réalisé en collaboration avec l'équipe Inria Pi.R2, a été publié à la conférence FM 2018 (rang A) et dans le journal **Formal Aspects of Computing** en 2020.

Ce travail de collaboration avec l'ANSSI se poursuit dans le cadre de la thèse de Matthieu Baty. Nous nous intéressons à la **modélisation et à la preuve formelle de mécanismes de sécurités matériels** sur des processeurs RISCV. Nous spécifions le mécanisme et la propriété de sécurité attendue dans des *Domain Specific Language* embarqués dans Coq. Nous avons ainsi prouvé un mécanisme de *shadow stack* sur un processeur RISCV. Ces travaux ont été publiés à la conférence **IEEE CSF 2023** (rang A).

Je dirige également depuis octobre 2021 la thèse de Jean-Loup Houdot sur la conception d'un compilateur permettant de produire des codes non-vulnérables aux attaques par canaux auxiliaires, en tirant parti de fonctionnalités matérielles. Cette thèse est réalisée dans le cadre du projet SCRATCH financé par le Labex CominLabs. Ces travaux ont été publiés à la conférence **ESORICS 2024** (rang A).

3.2 Projets et collaborations

Je suis et j'ai été le porteur principal (coordinateur) des projets suivants :
— SECUTRACE
— HardBlare
— Semestre thématique SILM
— collaborations avec HP Labs
— collaborations avec l'ANSSI
— collaborations avec AMOSSYS

Je suis le responsable scientifique du partenaire IRISA (équipe CIDRE) pour les projets suivants :

— TrustGW
— collaborations avec CS (RAPID COSCOM et FUI SECEF)

3.2.1 Projets collaboratifs

Projets en cours

SECUREVAL (2022-2028) - financement PEPR Cybersécurité : L'objectif est de concevoir de nouveaux outils pour l'évaluation de sécurité. Dans le cadre de ce projet, la contribution de l'équipe SUSHI porte sur les tâches 4.4 Analyses et modèles formels à la frontière logiciel-matériel (dont je suis le leader) et 3.2 Outils d'analyse de vulnérabilités dans les codes binaires.

TrustGW (2021-2025) - financement ANR : Le projet vise à développer une architecture hétérogène logiciel-matériel de passerelle pour l'Internet des objets, qui soit reconfigurable dynamiquement et de confiance. Dans le cadre de ce projet, la contribution de l'équipe CIDRE porte principalement sur la détection d'intrusion visant les applications, notamment au travers de la thèse de Lionel Hemmerlé (2022-2025), dont j'assure la direction.

Projets terminés

SCRATCHS (2021-2024) - financement Labex CominLabs : L'objectif est de co-concevoir un processeur RISC-V et une chaîne d'outils de compilation pour garantir par construction qu'un code sensible à la sécurité est immunisé contre les attaques par canal auxiliaire tout en maximisant les performances à l'exécution. Dans le cadre de ce projet, Jean-Loup Houdot a réalisé une thèse de doctorat dont j'ai assuré la direction.

SECUTRACE (2020-2022) - financement PHC AURORA : L'objectif de ma collaboration avec Volker Stolz de la Western Norway University of Applied Sciences (HVL), est d'étudier et de proposer des approches permettant de concourir à la sûreté de fonctionnement et à la cyber-sécurité des systèmes en exploitant les mécanismes de génération de traces, disponibles dans la plupart des plateformes matérielles.

SECEF (2013-2022) - financement DGA RAPID et FUI (https://www.secef.net/) : L'objectif des projets RAPID COSCOM/SECEF puis FUI SECEF (2020-2022) est de proposer des évolutions du format d'alerte IDMEF afin de couvrir les limitations actuelles de ce format.

Semestre thématique SILM (2019-2020) - financement DGA (https://silm.inria.fr/) : Dans le cadre de ce semestre, dont j'étais le porteur principal, j'ai organisé différents événements (école d'été, ateliers, séminaire, etc.) et j'ai été amené à inviter les chercheurs mondiaux du monde académique, industriel et gouvernemental sur la sécurité à l'interface logiciel/matériel. J'ai également rédigé pour la DGA un livre blanc dressant l'état de l'art du domaine et les axes stratégiques à développer. Ce projet a également financé ma délégation partielle (50%) à Inria pour l'année universitaire 2019/2020 pour organiser ce semestre.

HardBlare (2015-2018) - financement Labex CominLabs (https://project.inria.fr/hardblare/) : L'objectif était de réaliser un coprocesseur dédié au DIFT implémenté en FPGA. Mounir Nasr Allah et Muhammad Abdul Wahab ont réalisé leur thèse dans le cadre de ce projet.

SecCloud (2013-2017) - financement Labex CominLabs et région Bretagne (https:

//project.inria.fr/seccloud/) : SecCloud portait sur la sécurité des navigateurs web et plus particulièrement les problématiques de sécurité liées à l'exécution de code JavaScript. Dans ce contexte, nous avons proposé une approche de DIFT adaptée au navigateur Web. Deepak Subramanian a réalisé sa thèse dans le cadre de ce projet.

3.2.2 Collaborations bilatérales industrielles et gouvernementales

Projets terminés

ANSSI (2015-2018) et (2020-2024) : Je collabore régulièrement avec l'ANSSI, notamment dans le cadre de la thèse de Thomas Letan et de Matthieu Baty. Nous nous sommes intéressés à la formalisation des plateformes matérielles et des mécanismes de sécurité qu'elles fournissent. Ce travail a fait l'objet du développement de frameworks open-source permettant la spécification et la preuve de mécanisme de sécurité matériel [1], ainsi que la vérification modulaire de programme avec effets [2]. Matthieu Baty a réalisé une thèse dans le cadre du partenariat stratégique entre Inria et l'ANSSI.

HP Labs (2014-2019) : J'ai établi une collaboration à long terme avec HP Inc. Labs sur la sécurité de leur plateforme PC. Cette collaboration a donné lieu dans un premier temps à un contrat bilatéral dont le contenu est confidentiel. J'ai également réalisé une visite d'un mois au sein des HP Labs en 2016. Nous avons poursuivi cette collaboration au travers de la thèse de Ronny Chevalier puis du stage de M2 SIF de Titouan Lazard.

AMOSSYS (2010-2014) : Dans le cadre de la thèse CIFRE de Georges Bossert, j'ai collaboré avec la société AMOSSYS. Nous avons proposé une nouvelle approche pour la rétro-conception de protocole de spécification. Ce travail a fait l'objet du développement d'un outil de rétro-conception disponible en open-source [3].

3.3 Responsabilité d'équipe

Je suis depuis janvier 2024 responsable de l'équipe-projet Inria SUSHI (Security at the Software/Hardware Interface) : https://team.inria.fr/sushi/. J'ai piloté le processus de création de cette équipe-projet (coordination et forte implication dans la rédaction du projet d'équipe, soutenance du projet devant les différentes instances d'Inria et de l'IRISA). En tant que responsable scientifique, je pilote et je coordonne les actions de recherche de l'équipe et j'assure l'interface avec les différentes institutions dont Inria. Je participe notamment aux réunions mensuelles du comité des projets du centre Inria de l'université de Rennes.

SUSHI est une équipe commune à CentraleSupélec, Inria et l'ENS de Rennes et fait partie de l'IRISA (UMR 6074). Elle comprend aujourd'hui quatre enseignants-chercheurs de CentraleSupélec, une enseignante-chercheuse de l'ENS et un chercheur de la DGA mis à disposition de l'équipe pour 40% de son temps. L'équipe est hebergée sur le campus de Rennes de CentraleSupélec et dispose également de bureaux dans le centre de recherche Inria de l'Université de Rennes.

La création de cette équipe a permis de renforcer la présence et la visibilité de CentraleSupélec

1. https://github.com/lthms/speccert
2. https://github.com/ANSSI-FR/FreeSpec
3. https://github.com/netzob/netzob

en cybersécurité. Son positionnement original, à l'interface entre le logiciel et le matériel, permet d'étendre et de diversifier les activités de recherche en cybersécurité au sein de CentraleSupélec.

3.4 Activités d'intérêt collectif

Je suis depuis octobre 2022 le co-responsable du groupe de travail Sécurité des systèmes, des logiciels et des réseaux [4] du GDR Sécurité Informatique (2046) et membre du bureau de ce GDR.

Je suis également l'organisateur des journées nationales de ce GDR en 2024 (environ 200 participants) [5]. Ces journées nationales du GDR SI réunissent tous les acteurs (académiques, industriels, étatiques...) de la recherche en sécurité informatique. Pendant trois jours, les participants vivent au rythme des présentations et des discussions scientifiques. C'est également l'occasion d'échanger sur l'organisation et la vie de la communauté (notamment lors de l'assemblée générale du GDR SI). Ces échanges favorisent le développement de collaborations scientifiques en cybersécurité, entre les différents acteurs académiques français, mais également avec les acteurs industriels, étatiques et internationaux qui sont également présents.

J'assure régulièrement des relectures d'articles pour des publications en conférence ou en revue :

- SILM (2020, 2021, 2022, 2023)
- EAI SecureComm (2021, 2022, 2023, 2024)
- Elsevier Computers & Security 2022
- ACM Transactions on Privacy and Security 2020
- IEEE Access 2020
- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2020
- RAID (2011, 2012)
- International Workshop on Trust in Cloud Computing (2015, 2016)
- Journal of Computer Security (2019)
- IEEE Transactions on Systems, Man, and Cybernetics (2013)
- IEEE Design & Test (2019)
- Security and Communication Networks (2013)
- TSI (2013)
- SAR-SSI (2014)

J'ai été membre du comité de programme de la conférence RAID (rang A d'après CORE) en 2011 et 2012, de la conférence EAI SecureComm (2021, 2022, 2023 et 2024) et du workshop SILM en 2020, 2021, 2022 et 2023.

Je participe également à l'évaluation de projets de recherche :

- ANR (2019, 2020, 2022)
- Association Nationale Recherche Technologie (ANRT), l'organisme qui gère les conventions CIFRE (2013)
- Fonds de recherche Nature et Technologies du Québec (2013, 2015, 2016)

J'ai été rapporteur de la thèse de doctorat de Natasha Alkhatib (Télécom Paris, mars 2023), Paul L. R. OLIVIER (EURECOM, mars 2023) et Soline DUCOUSSO (UGA, décembre 2023).

4. https://gdr-securite.irisa.fr/securite-des-systemes-des-logiciels-et-des-reseaux/
5. https ://gdr-secu-jn2024.sciencesconf.org/

J'ai été désigné rapporteur de l'HDR de Damien Couroussé (CEA, août 2024) et de la thèse de Quentin Forcioli (Télécom Paris, soutenance prévue en décembre 2024).

J'ai été désigné rappoteur de la thèse de master de Michael Amar (Ben-Gurion University) dont la soutenance est prévue en mai 2024.

J'ai été examinateur du jury de la thèse de Florent Marchand de Kerchove de Denterghem (Ecole des Mines de Nantes, november 2016) et de Trung Duc Tran (Université Grenoble Alpes, février 2021).

J'ai fait partie du jury de sélection et de recrutement d'un Maître de Conférence à Centrale-Supélec en 2021, 2022, 2023 et 2024.

J'ai organisé les tables rondes à la conférence RESSI 2016.

Dans le cadre de mon semestre thématique, j'ai organisé (ou participé à l'organisation) de différents événements :

- Une école d'été en Juillet 2019 à Rennes [6], principalement organisée par mes collègues Clémentine Maurice et Frédéric Tronel ;
- Un workshop durant la European Cyber Week en Novembre 2019 à Rennes [7], avec mes collègues Frédéric Tronel et Jean-Louis Lanet ;
- Une *master class* et des démonstrations durant le Forum International de la Cybersécurité en Janvier 2020 à Lille, avec Clémentine Maurice et Frédéric Tronel ;
- Un atelier co-localisé avec la conférence internationale IEEE Euro S&P en 2020 [8] et en 2021 [9] ;
- Un séminaire régulier à Rennes [10], avec Ronan Lashermes.

3.5 Présentations invitées (liste non exhaustive)

- Octobre 2023, *SUSHI : SecUrity at the Software-Hardware Interface*, séminaire DGA SPISA-MISSILES
- Juin 2023, *Modélisation et preuve formelle de mécanismes de sécurité matériel*, Séminaire Creach Labs/DGA Sécurité des composants
- Février 2022, *Security at the Hardware/Software Interface*, Séminaire UQAM
- Novembre 2021, *Hardblare - heterogeneous solution for embedded software security*, COEMS Forsterk Seminar : Testing & Tracing (Not only) on Embedded Systems, Trondheim, Norvège.
- Mars 2020, *Hardware-based security monitoring*, Séminaire ANSSI, Rennes
- Février 2020, *HardBlare, a hardware/software co-design approach for Information Flow Control*, SILM Seminar - Special ARM edition, Rennes
- Janvier 2020, *Quelle confiance peut-on placer dans les plateformes matérielles qui exécutent nos applications ?*, Forum International de la Cybersécurité, Lille
- Février 2019, *CIDRE research group - Focus on software/hardware security*, Séminaire Ruhr-Universität Bochum, Rennes
- Février 2018, *Security of Hardware/Software Interfaces*, EIT Digital DTS/DSL workshop,

6. https://silm-school.inria.fr/
7. https://silm-workshop.inria.fr/
8. https://silm-workshop-2020.inria.fr/
9. https://silm-workshop-2021.inria.fr/
10. https://silm-seminar.gitlabpages.inria.fr/

Rennes
— Octobre 2016, *CIDRE team presentation - Focus on software/hardware security research track*, Séminaire ARM, Rennes/Cambridge
— Juillet 2016, *Hardware Design for Tag-Based Security Monitors*, Séminaire IBM, Rennes
— Décembre 2015, *Travaux de recherches en Supervision de sécurité : tendances actuelles*, 6ème édition des Assises du domaine Cyber Défense et SIEM, Club R2GS, Paris
— Septembre 2015, *Les standards au service de l'efficacité*, SECEF Day, Le Plessis-Robinson
— Octobre 2013, *Blare : Information Flow Tracking for Policy-Based Intrusion Detection*, Séminaire Département D1 IRISA, Rennes
— Juin 2012, *xBlare, une famille d'outils pour la détection d'intrusion par suivi des flux d'information*, Séminaire Oberthur, Paris
— Mars 2012, *Inférence de protocoles pour l'évaluation des NIDS*, Commission d'évaluation de la recherche de Supélec, Gif-sur-Yvette
— Juin 2011, *Modélisation et simulation du canal de communication d'un botnet pour l'évaluation des NIDS*, Séminaire DGA, Bruz

4 Activités d'encadrement

4.1 Encadrement d'étudiants de master

J'encadre régulièrement des étudiants dans leur stage de master recherche. Outre l'encadrement du travail de recherche, cette tâche nécessite de suivre l'étudiant depuis le début de l'année scolaire. En effet, l'étudiant doit réaliser une étude bibliographique sur son sujet de recherche durant la première partie de l'année, avant la réalisation de son stage (de février à juin). L'étudiant doit produire un rapport bibliographique ainsi qu'une soutenance. Il est donc nécessaire d'aider l'étudiant dans ce travail et sa recherche mais également de participer à son évaluation. L'organisation du master demande à chaque encadrant de participer aux jurys de soutenance et d'être rapporteur de rapports d'autres étudiants. Cela concerne l'étude bibliographique ainsi que le rapport de stage et la soutenance finale.

J'ai encadré dix étudiants de master qui ont tous soutenu. Parmi ces étudiants, cinq ont poursuivi leurs études en doctorat (Ronny Chevalier, Oualid Koucham, Eric Asselin, Thomas Letan et Mounir Assaf) et j'ai encadré les doctorats de trois d'entre eux (Ronny Chevalier, Oualid Koucham et Thomas Letan). Jianqiao Xu et Titouan Lazard ont été embauchés en tant qu'ingénieur à l'issue de leur master.

Année	Etudiant	Sujet	Provenance
2024	Oumar Niang	Suivi dynamique de flux d'information dans les applications hybrides	UBS
2022	Romain Ninot	Suivi dynamique de flux d'information dans les applications hybrides	CentraleSupélec
2022	Damien Armillon	Surveillance sélective et dynamique de flux d'information à l'aide d'une instrumentation dynamique de binaire	CentraleSupélec
2022	Lionel Hemmerlé	Conception et implémentation d'un langage dédié à l'introspection d'une machine virtuelle au sein d'un hyperviseur	CentraleSupélec
2018	Titouan Lazard	Hardware based monitoring of chipset components	ENS
2016	Jianqiao Xu	Development of Memory-based Attacks for Android Platform	Supélec
2016	Ronny Chevalier	Coprocessor-based Low-level Intrusion Detection	ENS
2013	Oualid Koucham	Development of a Smart Fuzzing Plugin for Netzob	Supélec
2013	Eric Asselin	Automatic Generation of Protocol Decoders	Univ. Limoges
2013	Thomas Letan	Cooperation between OS and Java-level IFC Monitors	INSA
2011	Mounir Assaf	Combining Static and Dynamic Analysis to Detect Intrusion using Information Flow Control	Supélec

J'ai été l'encadrant principal de tous les étudiants de master de 2011 à 2018 (à 50% avec mes collègues de HP Labs pour Titouan Lazard et Ronny Chevalier, à 100% pour les autres). En 2022, j'ai co-encadré Romain Ninot, Damien Armillon et Lionel Hemmerlé à 30% avec mes collègues Pierre Wilke et Frédéric Tronel.

4.2 Encadrement doctoral

Je participe actuellement à l'encadrement de trois doctorants et je dirige deux thèses. J'ai participé à l'encadrement de neuf doctorants qui ont tous soutenu avec succès. Les doctorants que j'ai encadrés ont tous obtenu un emploi en CDI en lien avec la cybersécurité. Le tableau suivant indique l'ensemble des doctorants pour lesquels j'ai participé à l'encadrement. Je suis ou j'ai été le principal encadrant des doctorants dont le nom est indiqué en gras.

Années	Doctorant	Sujet	Financement	Taux d'encadrement
2022-	Lionel Hemmerlé	Conception et implémentation d'un langage dédié à l'introspection d'une machine virtuelle au sein d'un hyperviseur	ANR	25%
2021-2024	Jean-Loup Houdot	Security-enhancing compiler against side-channel attacks	CominLabs, ANR	25%
2020-2024	Matthieu Baty	Formalisation de mécanismes de sécurité pour l'architecture de processeurs RISC-V	ANSSI	37%
2019-2023	Nicolas Bellec	Security enhancement in embedded hard real-time systems (en collaboration avec l'équipe PACAP)	Univ. Rennes 1	25%
2018-2022	Camille Le Bon	Dynamic Binary Analysis and Optimization for Cyber-Security (en collaboration avec l'équipe PACAP)	DGA	35%
2016-2019	**Ronny Chevalier**	Enhanced Computer Platform Security through an Intrusion Detection Approach	CIFRE HP	50%
2015-2018	Oualid Koucham	Intrusion Detection for Industrial Control Systems	DGA	40%
2015-2018	Muhammad Wahab	Reconfigurable coprocessors for embedded software security	CominLabs, région Bretagne	20%
2015-2020	**Mounir Nasr Allah**	Combining Static Analyses with Dynamic Hardware-Based Analyses for Information Flow Control	CominLabs	50%
2014-2018	**Thomas Letan**	Security of the Low-level Components of a Computer Platform	ANSSI	50%
2013-2017	**Deepak Subramanian**	Multi-level Information Flow Monitoring	CominLabs, région Bretagne	50%
2010-2014	**Georges Bossert**	Exploiting Semantic for the Automatic Reverse Engineering of Communication Protocols	CIFRE AMOSSYS	80%

4.3 Publications et brevets

L'ensemble de mes publications est disponibles dans Hal à l'adresse suivante : https://cv.archives-ouvertes.fr/guillaume-hiet

Lien Scopus : https://www.scopus.com/authid/detail.uri?authorId=26424291200

Lien DBLP : https://dblp.org/pid/18/8558.html

Lien Google Scholar : https://scholar.google.fr/citations?user=fLwAG3oAAAAJ

Lien Publons / Web of Science : https://publons.com/researcher/3172327/guillaume-hiet/metrics/

Dans le cadre de ma collaboration avec HP, nous avons également effectué quatre demandes de brevets qui nous ont été accordées (US11556645B2, US11308202B2, US10896085B2,

EP3647980B1).

Dans la liste suivante, j'indique en gras le nom des doctorants que j'ai encadrés.

Cinq publications notables :

1. **Jean-Loup Hatchikian-Houdot**, Pierre Wilke, Frédéric Besson et **Guillaume Hiet**. "Formal Hardware/Software Models for Cache Locking Enabling Fast and Secure Code". In : *Computer Security – ESORICS 2024*. Sous la dir. de Joaquin Garcia-Alfaro, Rafał Kozik, Michał Choraś et Sokratis Katsikas. Cham : Springer Nature Switzerland, 2024, p. 153-173
2. **Matthieu Baty**, Pierre Wilke, **Guillaume Hiet**, Arnaud Fontaine et Alix Trieu. "A generic framework to develop and verify security mechanisms at the microarchitectural level : application to control-flow integrity". In : *CSF 2023 - 36th IEEE Computer Security Foundations Symposium*. Dubrovnik, France : IEEE, juill. 2023, p. 1-16. URL : https://inria.hal.science/hal-04118645
3. **Nicolas Bellec**, **Guillaume Hiet**, Simon Rokicki, Frederic Tronel et Isabelle Puaut. "RT-DFI : Optimizing Data-Flow Integrity for Real-Time Systems". In : *34th Euromicro Conference on Real-Time Systems (ECRTS 2022)*. Sous la dir. de Martina Maggio. T. 231. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany : Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022, 18 :1-18 :24. ISBN : 978-3-95977-239-6. DOI : 10.4230/LIPIcs.ECRTS.2022.18. URL : https://drops.dagstuhl.de/opus/volltexte/2022/16335
4. **Thomas Letan**, Yann Régis-Gianas, Pierre Chifflier et **Guillaume Hiet**. "Modular verification of programs with effects and effects handlers". In : *Formal Aspects of Computing* (déc. 2020). DOI : 10.1007/s00165-020-00523-2. URL : https://hal.archives-ouvertes.fr/hal-03107526
5. **Oualid Koucham**, Stéphane Mocanu, **Guillaume Hiet**, Jean-Marc Thiriet et Frédéric Majorczyk. "Cross-domain Alert Correlation methodology for Industrial Control Systems". In : *Computers and Security* (2022). URL : https://hal.archives-ouvertes.fr/hal-03636549

Revues internationales avec comité de lecture

[1] **Oualid Koucham**, Stéphane Mocanu, **Guillaume Hiet**, Jean-Marc Thiriet et Frédéric Majorczyk. "Cross-domain Alert Correlation methodology for Industrial Control Systems". In : *Computers and Security* (2022). URL : https://hal.archives-ouvertes.fr/hal-03636549.

[2] **Ronny Chevalier**, David Plaquin, Chris Dalton et **Guillaume Hiet**. "Intrusion Survivability for Commodity Operating Systems". In : *Digital Threats : Research and Practice* 1.4 (déc. 2020), p. 1-30. DOI : 10.1145/3419471. URL : https://hal.inria.fr/hal-03085774.

[3] **Thomas Letan**, Yann Régis-Gianas, Pierre Chifflier et **Guillaume Hiet**. "Modular verification of programs with effects and effects handlers". In : *Formal Aspects of Computing* (déc. 2020). DOI : 10.1007/s00165-020-00523-2. URL : https://hal.archives-ouvertes.fr/hal-03107526.

[4] **Guillaume Hiet**, Valérie Viet Triem Tong, Ludovic Mé et Benjamin Morin. "Policy-based intrusion detection in web applications by monitoring Java information flows". In : *International Journal of Information and Computer Security* Vol.3.N°3/4 (2009), 15 pages. URL : https://hal.archives-ouvertes.fr/hal-00448139.

Conférences et ateliers internationaux avec comité de lecture et actes

[5] **Jean-Loup Hatchikian-Houdot**, Pierre Wilke, Frédéric Besson et **Guillaume Hiet**. "Formal Hardware/Software Models for Cache Locking Enabling Fast and Secure Code". In : *Computer Security – ESORICS 2024*. Sous la dir. de Joaquin Garcia-Alfaro, Rafał Kozik, Michał Choraś et Sokratis Katsikas. Cham : Springer Nature Switzerland, 2024, p. 153-173.

[6] **Matthieu Baty**, Pierre Wilke, **Guillaume Hiet**, Arnaud Fontaine et Alix Trieu. "A generic framework to develop and verify security mechanisms at the microarchitectural level : application to control-flow integrity". In : *CSF 2023 - 36th IEEE Computer Security Foundations Symposium*. Dubrovnik, France : IEEE, juill. 2023, p. 1-16. URL : https://inria.hal.science/hal-04118645.

[7] Nicolas Gaudin, **Jean-Loup Hatchikian-Houdot**, Frédéric Besson, Pascal Cotret, Gogniat Guy, **Guillaume Hiet**, Vianney Lapotre et Pierre Wilke. "Work in Progress : Thwarting Timing Attacks in Microcontrollers using Fine-grained Hardware Protections". In : *SILM 2023 - Workshop on the Security of Software / Hardware Interfaces*. Delft, Netherlands, juill. 2023, p. 1-7. URL : https://hal.science/hal-04155139.

[8] **Nicolas Bellec**, **Guillaume Hiet**, Simon Rokicki, Frederic Tronel et Isabelle Puaut. "RT-DFI : Optimizing Data-Flow Integrity for Real-Time Systems". In : *34th Euromicro Conference on Real-Time Systems (ECRTS 2022)*. Sous la dir. de Martina Maggio. T. 231. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany : Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022, 18 :1-18 :24. ISBN : 978-3-95977-239-6. DOI : 10.4230/LIPIcs.ECRTS.2022.18. URL : https://drops.dagstuhl.de/opus/volltexte/2022/16335.

[9] **Camille Le Bon**, Erven Rohou, Frédéric Tronel et **Guillaume Hiet**. "DAMAS : Control-Data Isolation at Runtime through Dynamic Binary Modification". In : *Workshop on the Security of Software / Hardware Interfaces (SILM 2021)*. digital event, France, sept. 2021. URL : https://hal.archives-ouvertes.fr/hal-03340008.

[10] **Ronny Chevalier**, David Plaquin, Chris Dalton et **Guillaume Hiet**. "Survivor : A Fine-Grained Intrusion Response and Recovery Approach for Commodity Operating Systems". In : *ACSAC 2019 - 35th Annual Computer Security Applications Conference*. T. 2019. San Juan, Puerto Rico, déc. 2019. DOI : 10.1145/3359789.3359792. URL : https://hal.inria.fr/hal-02289315.

[11] Jean-François Lalande, Valérie Viet Triem Tong, Pierre Graux, **Guillaume Hiet**, Wojciech Mazurczyk, Habiba Chaoui et Pascal Berthomé. "Teaching Android Mobile Security". In : *SIGCSE '19 - 50th ACM Technical Symposium on Computer Science Education*. Minneapolis, United States : ACM Press, fév. 2019, p. 232-238. DOI : 10.1145/

3287324.3287406. URL : https://hal-centralesupelec.archives-ouvertes.fr/hal-01940652.

[12] **Muhammad Abdul Wahab**, Pascal COTRET, **Mounir Nasr Allah**, **Guillaume Hiet**, Arnab KUMAR BISWAS, Vianney LAPOTRE et Gogniat GUY. "A small and adaptive coprocessor for information flow tracking in ARM SoCs". In : *ReConFig 2018 - International Conference on Reconfigurable Computing and FPGAs*. Cancun, Mexico, déc. 2018, p. 1-17. DOI : 10.1109/reconfig.2018.8641695. URL : https://hal.archives-ouvertes.fr/hal-01911619.

[13] **Muhammad Abdul Wahab**, Pascal COTRET, **Mounir Nasr Allah**, **Guillaume Hiet**, Vianney LAPOTRE, Gogniat GUY et Arnab KUMAR BISWAS. "A novel lightweight hardware-assisted static instrumentation approach for ARM SoC using debug components". In : *AsianHOST 2018 - Asian Hardware Oriented Security and Trust Symposium*. Hong Kong, China, déc. 2018, p. 1-13. DOI : 10.1109/asianhost.2018.8607177. URL : https://hal.archives-ouvertes.fr/hal-01911621.

[14] **Oualid Koucham**, Stéphane MOCANU, **Guillaume Hiet**, Jean-Marc THIRIET et Frédéric MAJORCZYK. "Efficient Mining of Temporal Safety Properties for Intrusion Detection in Industrial Control Systems". In : *SAFEPROCESS 2018 - 10th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes*. Warsaw, Poland, août 2018, p. 1-8. URL : https://hal.archives-ouvertes.fr/hal-01877109.

[15] **Thomas Letan**, Yann RÉGIS-GIANAS, Pierre CHIFFLIER et **Guillaume Hiet**. "Modular Verification of Programs with Effects and Effect Handlers in Coq". In : *FM 2018 - 22nd International Symposium on Formal Methods*. T. 10951. LNCS. Oxford, United Kingdom : Springer, juill. 2018, p. 338-354. DOI : 10.1007/978-3-319-95582-7_20. URL : https://hal.inria.fr/hal-01799712.

[16] **Ronny Chevalier**, Maugan VILLATEL, David PLAQUIN et **Guillaume Hiet**. "Co-processor-based Behavior Monitoring : Application to the Detection of Attacks Against the System Management Mode". In : *ACSAC 2017 - 33rd Annual Computer Security Applications Conference*. T. 2017. Orlando, United States : ACM, déc. 2017, p. 399-411. DOI : 10.1145/3134600.3134622. URL : https://hal.inria.fr/hal-01634566.

[17] **Muhammad Abdul Wahab**, Pascal COTRET, **Mounir Nasr Allah**, **Guillaume Hiet**, Vianney LAPOTRE et Guy GOGNIAT. "ARMHEx : A hardware extension for DIFT on ARM-based SoCs". In : *2017 27th International Conference on Field Programmable Logic and Applications (FPL)*. Ghent, Belgium, sept. 2017. DOI : 10.23919/fpl.2017.8056767. URL : https://hal.archives-ouvertes.fr/hal-01558473.

[18] **Muhammad Abdul Wahab**, Pascal COTRET, **Mounir Nasr Allah**, **Guillaume Hiet**, Vianney LAPOTRE et Guy GOGNIAT. "Towards a hardware-assisted information flow tracking ecosystem for ARM processors". In : *26th International Conference on Field-Programmable Logic and Applications (FPL 2016)*. Lausanne, Switzerland, août 2016. DOI : 10.1109/fpl.2016.7577396. URL : https://hal.archives-ouvertes.fr/hal-01337579.

[19] **Oualid Koucham**, Stéphane MOCANU, **Guillaume Hiet**, Jean-Marc THIRIET et Frédéric MAJORCZYK. "Detecting Process-Aware Attacks in Sequential Control Systems". In : *21st Nordic Conference on Secure IT Systems (NordSec 2016)*. Oulu, Finland, nov. 2016, p.20-36. DOI : 10.1007/978-3-319-47560-8_2. URL : https://hal.inria.fr/hal-01361081.

[20] **Thomas Letan**, Pierre Chifflier, **Guillaume Hiet**, Pierre Néron et Benjamin Morin. "SpecCert : Specifying and Verifying Hardware-based Software Enforcement". In : *21st International Symposium on Formal Methods (FM 2016)*. Limassol, Cyprus : Springer, nov. 2016. doi : 10.1007/978-3-319-48989-6_30. url : https://hal.inria.fr/hal-01361422.

[21] **Deepak Subramanian**, **Guillaume Hiet** et Christophe Bidan. "A self-correcting information flow control model for the web-browser". In : *FPS 2016 - The 9th International Symposium on Foundations & Practice of Security*. T. 10128. Lecture Notes in Computer Science. Québec City, Canada, oct. 2016, p. 285-301. doi : 10.1007/978-3-319-51966-1_19. url : https://hal.inria.fr/hal-01398192.

[22] **Deepak Subramanian**, **Guillaume Hiet** et Christophe Bidan. "Preventive Information Flow Control through a Mechanism of Split Addresses". In : *9th International Conference on Security of Information and Networks (SIN 2016)*. Newark, United States, juill. 2016, p.1-8. doi : 10.1145/2947626.2947645. url : https://hal.inria.fr/hal-01344565.

[23] **Georges Bossert**, Frédéric Guihéry et **Guillaume Hiet**. "Towards Automated Protocol Reverse Engineering Using Semantic Information". In : *ASIA CCS '14*. 12 pages. Kyoto, Japan, juin 2014, p. 51-62. doi : 10.1145/2590296.2590346. url : https://hal.archives-ouvertes.fr/hal-01009283.

[24] Emmanuelle Anceaume, Christophe Bidan, Sébastien Gambs, **Guillaume Hiet**, Michel Hurfin, Ludovic Mé, Guillaume Piolle, Nicolas Prigent, Eric Totel, Frédéric Tronel et Valérie Viet Triem Tong. "From SSIR to CIDre : a New Security Research Group in Rennes". In : *1st SysSec Workshop*. Amsterdam, Netherlands, juill. 2011. url : https://hal.archives-ouvertes.fr/hal-00656940.

[25] **Guillaume Hiet**, Valérie Viet Triem Tong, Ludovic Mé et Benjamin Morin. "Policy-Based Intrusion Detection in Web Applications by Monitoring Java Information Flows". In : *CRiSIS 2008*. Tozeur, Tunisia, oct. 2008, 8 pages. url : https://hal.archives-ouvertes.fr/hal-00353000.

[26] **Guillaume Hiet**, Ludovic Mé, Benjamin Morin et Valérie Viet Triem Tong. "Monitoring both OS and program level information flows to detect intrusions against network servers". In : *IEEE Workshop on Monitoring, Attack Detection and Mitigation*. Toulouse, France, nov. 2007. url : https://hal.archives-ouvertes.fr/hal-00268408.

Revues françaises avec comité de lecture

[27] Mathieu Jaume, Valérie Viet Triem Tong et **Guillaume Hiet**. "Spécification et mécanisme de détection de flots d'information illégaux". In : *Revue des Sciences et Technologies de l'Information - Série TSI : Technique et Science Informatiques* 31.6 (2012), p. 713-742. doi : 10.3166/tsi.31.713-742. url : https://hal.archives-ouvertes.fr/hal-00761351.

[28] Christophe Bidan, **Guillaume Hiet**, Ludovic Mé, Benjamin Morin et Jacob Zimmermann. "Vers une détection d'intrusions à fiabilité et pertinence prouvables". In : *La Revue de l'Electricité et de l'Electronique* 9 (oct. 2006), 13 pages. url : https://hal.archives-ouvertes.fr/hal-00269279.

Conférences et ateliers français avec comité de lecture et actes

[29] **Georges Bossert**, Frédéric Guihéry et **Guillaume Hiet**. "Netzob : un outil pour la rétro-conception de protocoles de communication". In : *SSTIC 2012*. Rennes, France, juin 2012, p. 43. URL : https://hal-supelec.archives-ouvertes.fr/hal-00763751.

[30] **Georges Bossert**, **Guillaume Hiet** et Thibaut Henin. "Modelling to Simulate Botnet Command and Control Protocols for the Evaluation of Network Intrusion Detection Systems". In : *SAR-SSI 2011*. La Rochelle, France, mai 2011, p. 1-8. DOI : 10.1109/SAR-SSI.2011.5931397. URL : https://hal-supelec.archives-ouvertes.fr/hal-00658396.

[31] **Guillaume Hiet**, Frédéric Guihéry, Goulven Guiheux, David Pichardie et Christian Brunette. "Sécurité de la plate-forme d'exécution Java : limites et propositions d'améliorations". In : *Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*. Rennes, France, 2010. URL : https://hal.inria.fr/inria-00537820.

[32] **Guillaume Hiet**, Ludovic Mé, Jacob Zimmermann, Christophe Bidan, Benjamin Morin et Valérie Viet Triem Tong. "Détection fiable et pertinente de flux d'information illégaux". In : *Sixth Conference on Security and Network Architectures (SARSSI)*. France, juin 2007, unknown. URL : https://hal-supelec.archives-ouvertes.fr/hal-00268422.

Conférences et ateliers français avec comité de lecture sans actes

[33] **Kévin Le Bon**, Byron Hawkins, Erven Rohou, **Guillaume Hiet** et Frédéric Tronel. "Plateforme de protection de binaires configurable et dynamiquement adaptative". In : *RESSI 2019 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*. Erquy, France, mai 2019, p. 1-3. URL : https://hal.inria.fr/hal-02385216.

[34] **Ronny Chevalier**, David Plaquin et **Guillaume Hiet**. "Intrusion Survivability for Commodity Operating Systems and Services : A Work in Progress". In : *RESSI 2018 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*. Nancy / La Bresse, France, mai 2018. URL : https://hal.inria.fr/hal-02280376.

[35] **Muhammad Abdul Wahab**, Pascal Cotret, **Mounir Nasr Allah**, **Guillaume Hiet**, Vianney Lapotre et Guy Gogniat. "ARMHEx : embedded security through hardware-enhanced information flow tracking". In : *RESSI 2017 : Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*. Grenoble (Autrans), France, mai 2017. URL : https://hal.archives-ouvertes.fr/hal-01558155.

[36] **Muhammad Abdul Wahab**, Pascal Cotret, **Mounir Nasr Allah**, **Guillaume Hiet**, Vianney Lapotre et Guy Gogniat. "A portable approach for SoC-based Dynamic Information Flow Tracking implementations". In : *11ème Colloque du GDR SoC/SiP*. Nantes, France, juin 2016. URL : https://hal-centralesupelec.archives-ouvertes.fr/hal-01311045.

[37] **Oualid Koucham**, Stéphane MOCANU, **Guillaume Hiet**, Jean-Marc THIRIET et Frédéric MAJORCZYK. "Classification des approches de détection d'intrusions dans les systèmes de contrôle industriels et axes d'amélioration". In : *Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2016)*. Toulouse, France, mai 2016. URL : https://hal.archives-ouvertes.fr/hal-01587915.

[38] **Guillaume Hiet**, Hervé DEBAR, Sélim MÉNOUAR et Vérène HOUDEBINE. "Etude comparative des formats d'alertes". In : *C&ESAR (Computer & Electronics Security Applications Rendez-vous) 2015*. Rennes, France, nov. 2015, p. 125-148. URL : https://hal.archives-ouvertes.fr/hal-01242786.

[39] **Deepak Subramanian**, **Guillaume Hiet** et Christophe BIDAN. "Preventive Information Flow Control through a Mechanism of Split Addresses". In : *9ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information*. Saint-Germain-Au-Mont-d'Or, France, mai 2014. URL : https://hal.inria.fr/hal-01344563.

5 Annexes

Les tableaux suivant détaillent mes enseignements à CentraleSupélec sur les trois dernières années universitaires. En 2019-2020, ma charge d'enseignement était réduite du fait de ma délégation Inria (50%). En 2020-2021, ma décharge d'enseignement était complète (délégation Inria à 100%).

Table 2 – Détail des activités pédagogiques (2019-2020)

Public	Niveau	Matière	Volume	Effectifs	Nature	Responsabilités
Ing. CS [11]	L3	Introduction aux réseaux et à la sécurité informatique	6	30	TD	Création sujets TD en 2018
Ing. CS	L3	Introduction aux réseaux et à la sécurité informatique	9	100	CM	Création support de cours en 2018
Ing. CS	L3 (FISA [12])	Introduction aux réseaux et à la sécurité informatique	16,5	27	CTD [13]	Responsable du cours
Ing. CS	M1	Architecture des ordinateurs	6,75	20	CM	Création support de cours
Ing. CS	M1	Architecture des ordinateurs	6,75	20	TP	Création sujets TP
Ing. CS	M1	Systèmes embarqués et IoT	2,25	15	CM	Responsable du cours
Ing. CS	M1	Systèmes embarqués et IoT	13,5	15	TP	Responsable du cours
Ing. CS	M2	Détection d'intrusion	7,5	34	CM	Responsable du cours
Ing. CS	M2	Détection d'intrusion	6	34	TP	Responsable du cours
MCS [14]	M2	Détection d'intrusion	9	19	TP	Responsable du cours
MCS	M2	Détection d'intrusion	6	19	TP	Responsable du cours
Ing. CS	M2	Sécurité des OS	14,5	34	CM	Responsable du cours
Ing. CS	M2	Sécurité des OS	3	34	TP	Responsable du cours
MCS	M2	Sécurité des OS	11,25	19	CM	Responsable du cours
MCS	M2	Sécurité des OS	9	19	TP	Responsable du cours
Ing. CS	M2	Suivi stages	6	5	Projet	

9. Diplôme d'ingénieur CentraleSupélec
10. Formation Initiale sous Statut Apprenti
11. Enseignement mêlant cours et TD durant la même séance
14. Mastère Spécialisé Cyber Sécurité

Table 3 – Détail des activités pédagogiques (2021-2022)

Public	Niveau	Matière	Volume	Effectifs	Nature	Responsabilités
Ing. CS	L3	Introduction aux réseaux et à la sécurité informatique	22,5	30	TD	Création sujets TD en 2018
Ing. CS	L3	Introduction aux réseaux et à la sécurité informatique	18	119	CM	Mise à jour support de cours
Ing. CS	L3 (FISA)	Introduction aux réseaux et à la sécurité informatique	12	27	CTD	
Ing. CS	M1	Architecture des ordinateurs	4,5	27	CM	Mise à jour support de cours
Ing. CS	M1	Architecture des ordinateurs	7,5	27	TP	Création sujets TP en 2019
Ing. CS	M1	Systèmes embarqués et IoT	6,75	17	CM	Responsable du cours
Ing. CS	M1	Systèmes embarqués et IoT	3	17	TP	Responsable du cours
Ing. CS	M1	Projet 2ème année	15	5	Projet	
Ing. CS	M2	Sécurité réseau	4,5	40	CM	
Ing. CS	M2	Sécurité réseau	3	40	TP	
Ing. CS	M2	Sécurité matérielle	4,5	13	CM	Responsable du cours
Ing. CS	M2	Sécurité matérielle	6	13	TP	Responsable du cours
Ing. CS et MCS	M2	Système d'exploitation	6	16	TP	
Ing. CS	M2	Détection d'intrusion	6	40	TP	Responsable du cours
MCS	M2	Détection d'intrusion	4,5	31	CM	Responsable du cours
MCS	M2	Détection d'intrusion	6	31	TP	Responsable du cours
Ing. CS	M2	Attaques en mémoire	15	23	TP	
Ing. CS	M2	Attaques en mémoire avancées	4,5	13	CM	Création support de cours
Ing. CS	M2	Attaques en mémoire avancées	3	13	TP	
Ing. CS	M2	Projet fin d'étude	22,5	11	Projet	
Ing. CS	M2	Systèmes concurrents	4,5	27	CM	Création support de cours
Ing. CS	M2	Systèmes concurrents	6	27	TP	Création sujets TD
Ing. CS et MCS	M2	Sécurité des OS	13,5	71	CM	Responsable du cours
Ing. CS et MCS	M2	Sécurité des OS	7,5	23	TP	Responsable du cours
Ing. CS	M2	Formation à la recherche	6,75	23	CM	
Ing. CS	M2	Formation à la recherche	15	5	Projet	

Table 4 – Détail des activités pédagogiques (2022-2023)

Public	Niveau	Matière	Volume	Effectifs	Nature	Responsabilités
Ing. CS	L3	Introduction aux réseaux et à la sécurité informatique	24	30	TD	Création sujets TD en 2018
Ing. CS	L3	Introduction aux réseaux et à la sécurité informatique	13,5	119	CM	Mise à jour support de cours
Ing. CS	L3 (FISA)	Introduction aux réseaux et à la sécurité informatique	24,75	25	CTD	Responsable du cours
Ing. CS	M1	Architecture des ordinateurs	6,75	28	CM	Mise à jour support de cours
Ing. CS	M1	Architecture des ordinateurs	7,5	28	TP	Création sujets TP en 2019
Ing. CS	M1	Systèmes embarqués et IoT	11,25	20	CM	Responsable du cours
Ing. CS	M1	Systèmes embarqués et IoT	9	20	TP	Responsable du cours
Ing. CS	M2	Introduction à la sécurité	6,75	40	CM	
Ing. CS	M2	Sécurité matérielle	4,5	13	CM	Responsable du cours
Ing. CS	M2	Sécurité matérielle	3	13	TP	Responsable du cours
Ing. CS et MCS	M2	Système d'exploitation	9	16	TP	
Ing. CS	M2	Détection d'intrusion	6	40	TP	Responsable du cours
MCS	M2	Détection d'intrusion	4,5	31	CM	Responsable du cours
MCS	M2	Détection d'intrusion	6	31	TP	Responsable du cours
Ing. CS	M2	Attaques en mémoire	15	23	TP	
Ing. CS	M2	Attaques en mémoire avancées	4,5	13	CM	Mise à jour support de cours
Ing. CS	M2	Projet de deuxième année	12	5	Projet	
Ing. CS	M2	Projet de fin d'étude	30	11	Projet	
Ing. CS	M2	Systèmes concurrents	4,5	27	CM	Mise à jour support de cours
Ing. CS	M2	Systèmes concurrents	6	27	TP	Création sujets TD en 2021
Ing. CS	M2	Programmation en C	3	31	TP	
Ing. CS et MCS	M2	Sécurité des OS	15,75	71	CM	Responsable du cours
Ing. CS et MCS	M2	Sécurité des OS	7,5	23	TP	Responsable du cours
Ing. CS	M2	Formation à la recherche	15	5	Projet	
Ing. CS	M2	Suivi de stages	10	5	Stage	