Demande n°3505 - ARED

Acronyme :S-HYBRID

Identification

Identification

N°	3505
Année	2024
Statut	Brouillon
Date de création	25/01/2024
Date de modification	30/01/2024
Date de soumission	30/01/2024
Acronyme	S-HYBRID
Intitulé du projet	Security Monitoring in Heterogeneous Computing
Dispositif	ARED
Civilité du porteur	
Nom du porteur	Hiet
Prénom du porteur	Guillaume
Courriel	guillaume.hiet@centralesupelec.fr

Priorité régionale

Priorité régionale

Priorité régionale	Cybersécurité
Regional priority	Cybersécurité

Stratégie régionale de recherche et d’innovation (S3)

Stratégie régionale de recherche et d’innovation (S3)

Axe transversal	Transitions numérique et industrielle
Domaine d'innovation stratégique	Économie numérique sécurisée et responsable
Domaine d'innovation stratégique	.
Levier thématique	Cybersécurité

Organisme de tutelle

Organisme de tutelle

Etablissement	CENTRALE SUPELEC
Commune	CESSON-SEVIGNE
Civilité	Monsieur
Nom	Bidan
Prénom	Christophe

Unité de recherche

Unité de recherche

Nom de l'unité	IRISA
Civilité	Monsieur
Nom	Gravier
Prénom	Guillaume
Tél.	0299847100
Courriel	directeur@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	Equipe-projet SUSHI
Le cas échéant, nom du responsable de l'équipe de recherche	Guillaume Hiet
Activités de recherche et points forts de l'équipe	Sécurité à l'interface logiciel/matériel, cybersécurité
Si implication dans un/plusieurs programmes européens ou internationaux, préciser	

Co-directeur de thèse

Co-directeur de thèse

Civilité	Monsieur

Description

Description du projet

Libellé	Valeur
Résumé synthétique du projet (2000 caractères max)	La meilleure stratégie pour sécuriser une application nécessite de recourir à différentes approches préventives. Toutefois, ces approches ne sont pas systématiquement employées ni infaillibles. Il est donc important de surveiller l'exécution du système, sur l'hôte lui-même (HIDS), afin de détecter d'éventuelles intrusions. Par ailleurs, de nombreuses approches ont été proposées dans la littérature pour surveiller l'exécution d'applications s'exécutant sur un CPU. Toutefois, un nombre croissant d'applications (par exemple, les

Libellé	Valeur
	un nombre croissant d'applications (par exemple, les applications implémentant des algorithmes d'IA) sont hybrides, i.e. elles déportent une partie de leur calcul sur différentes unités d'exécutions hétérogènes (CPU, GPU, NPU, FPGA, etc.), ce qui complexifie leur supervision. Nous souhaitons développer une approche de détection d'intrusion pour les applications hybrides. L'objectif de cette thèse de doctorat est de proposer une approche de détection d'intrusion pour les applications hybrides en distribuant le processus de détection sur différents moniteurs dédiés à chaque unité d'exécution, tout en limitant l'impact sur les performances du système surveillé et en assurant la protection des moniteurs. Nous proposons de considérer comme cas d'usage les applications hétérogènes développées par High-Level Synthesis (HLS) pour des plateformes utilisant des SoC FPGA (par exemple Xilinx UltraScale+). Nous proposons d'implémenter la génération des moniteurs au sein de l'outil HLS de Xilinx, qui repose sur le compilateur LLVM. Il est ainsi possible d'insérer des passes de compilation pouvant analyser et modifier le code intermédiaire généré par le compilateur.
Caractère structurant/stratégique du projet (niveau régional/établissement)	Ce projet permettra d'accélérer le développement de la nouvelle équipe-projet Inria SUSHI (IRISA) et de renforcer son axe de recherche sur la sécurité des accélérateurs matériels. De manière générale, il permettra de renforcer les activités de recherche et l'expertise des personnels impliqués dans l'EUR Cybersécurité et les formations en cybersécurité à CentraleSupélec et à l'université de Rennes. Il permetra également à CentraleSupélec de développer son activité de recherche en cybersécurité, qui est une spécificité de son campus rennais, et ainsi d'affirmer son encrage dans l'écosystème breton. Le projet porte sur la cybersécurité, qui est un des leviers du Domaine d'Innovation Stratégique « ECONOMIE NUMERIQUE SECURISEE ET RESPONSABLE » de la Stratégie régionale de recherche et innovation (S3) de la région Bretagne. Il devrait également intéresser les équipes en charge de la LID (notamment Frédéric Majorczyk) et de la sécurité des composants matériels à DGA-MI, en particulier des accélérateurs matériels pour l'IA.
Porteur du projet : date d'obtention de l'HDR ou dérogation	2021
Hypothèses, questions posées, points de blocage, approche méthodologique, technique (4000 car. max)	Le projet fait face à trois principaux challenges: - Challenge 1 : La détection d'intrusion doit être distribuée sur les différentes unités d'exécutions hétérogènes. Il faut superviser en même temps l'exécution de différents noyaux de calcul qui s'exécutent sur différentes unités d'exécution et combiner les résultats. Cette tâche est complexifiée par l'hétérogénéité des unités d'exécution. Le recours à la HLS permet d'analyser les différents noyaux de calculs sous une forme homogène (LLVM IR) et de générer des moniteurs pour chaque unité d'exécution, par instrumentation du code. - Challenge 2 : Le moniteur doit être isolé des différentes unités d'exécution. Dans un HIDS, le détecteur est colocalisé avec la cible qu'il est censé surveiller. Il faut donc s'assurer qu'un attaquant ne puisse désactiver ou corrompre le détecteur. Nous proposons d'isoler les différents moniteurs en tirant parti de fonctionnalités matérielles (par exemple, Arm TrustZone, les extensions de virtualisation ou les System Protection Units). - Challenge 3 : Il faut franchir le fossé sémantique résultant de l'isolation. L'isolation du moniteur crée un fossé sémantique : le moniteur n'a plus accès facilement aux données de la cible lui permettant d'inférer son comportement de manière précise. Pour franchir ce fossé sémantique, nous envisageons de combiner différentes approches (analyse statique, instrumentation, mécanisme de traces matériel). Dans un premier temps, il s'agira de définir et formaliser le modèle de détection envisagé (i.e., les propriétés de sécurité à vérifier). On envisage par exemple de s'intéresser au suivi dynamique des flux d'information (DIFT). Dans un deuxième temps il s'agira d'implémenter l'approche proposée dans l'outil de HLS pour des applications simples, déportant une partie de leur calcul dans un nombre limité d'accélérateurs implémentés sur FPGA. Par la suite, il s'agira de généraliser l'approche en considérant des applications plus complexes. L'approche sera évaluée expérimentalement en analysant la sécurité (qualité de la détection et robustesse des moniteurs face à des attaques) et l'impact sur les performances.
Environnement scientifique, positionnement dans contexte régional/national/international (2000 car.)	Les travaux se dérouleront dans l'équipe SUSHI du laboratoire IRISA, département Architecture de l'IRISA et axe transversal cybersécurité de l'IRISA. Ces travaux étendent des travaux initiés dans le cadre du projet ANR TrustGW (collaboration

	Lab-STICC, IETR, IRISA). De manière générale, ces travaux s'inscrivent dans des collaborations de longue date avec l'équipe ARCAD du Lab-STICC (Guy Gogniat, UBS, Lorient et Pascal Cotret, ENSTA-B, Brest).
Collaborations scientifiques (nature/partenariat/pays) et partenariat socio-économique envisagé	Le projet sera l'occasion de renforcer la collaboration entre la nouvelle équipe SUSHI de l'IRISA et l'équipe ASIC de l'IETR. En outre des collaborations sont envisagées avec l'équipe ARCAD du Lab-STICC. En outre, nous envisageons des collaborations ponctuelles avec Volker Stoltz (HVL, Norvège) et Martin Leucker (Univ. Lübeck) sur l'accélération des moniteurs de sécurité sur FPGA.
Adéquation du projet avec le DIS de rattachement (3000 caractères maximum)	Le projet porte sur la cybersécurité, qui est un des leviers du Domaine d'Innovation Stratégique « ECONOMIE NUMERIQUE SECURISEE ET RESPONSABLE » de la Stratégie régionale de recherche et innovation (S3) de la région Bretagne.
Si priorité régionale, préciser (200 caractères maximum)	Cybersécurité
Cotutelle internationale (indiquer "oui" ou "non"; si oui, préciser le pays et l'établissement)	Non
Nom(s) du(des) cofinanceur(s) envisagé(s) ou confirmé(s)	CREACH Labs
Si cofinancement industriel, justifier le choix du dispositif ARED au lieu du dispositif CIFRE	
État du cofinancement (indiquer "acquis" ou "demandé")	Financement demandé, premier projet sur liste d'attente
Si demandé, date prévisionnelle de réponse du cofinanceur	
Si cofinancement refusé, autre(s) source(s) de cofinancement identifiée(s)	
Si reversement prévu, préciser (partenaire, montant)	

Candidat

Candidat

Genre	Masculin
Nationalité	Sénégalaise

Collaboration internationale

Collaboration internationale

Pays	
Etablissement partenaire à l'étranger	

Pièces jointes

Date de mi	Type de pièce	Commentaire	Document	Valide	Commentaire
30/01/2024	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	

30/01/2024	ARED - Dépôt - Avis directeur·rice d'unité	15 lignes maximum		Non traité	
30/01/2024	ARED - Dépôt - Justificatif cofinancement	Facultatif - Dépôt de demande, justificatif d'obtention, courrier du cofinanceur pressenti...	THESE CREACH LABS 2024 - SecuHybrid.pdf	Non traité	
30/01/2024	ARED - Dépôt - Lettre partenaire étranger	Facultatif - Lettre d'engagement de l'établissement partenaire étranger en cas de cotutelle internationale		Non traité	
30/01/2024	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
30/01/2024	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
30/01/2024	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	
30/01/2024	ARED - Versement - Convention de partenariat	Le cas échéant (si autorisation de reversement)		Non traité	
30/01/2024	ARED - Versement 1/2 - CV doctorant.e	Pour versement tranche 1 (cohortes jusqu'en 2018) Pour versement tranche 2 (cohortes à partir de 2019)		Non traité	
30/01/2024	ARED - Versement 1/2 - Copie du contrat doctoral (ou CDD ou attestation))	Pour versement tranche 1 (cohortes jusqu'en 2018) Pour versement tranche 2 (cohortes à partir de 2019)		Non traité	
30/01/2024	ARED - Versement 1 - Lettre d'approbation école doctorale	Pour versement tranche 1 (cohortes jusqu'en 2018)		Non traité	
30/01/2024	ARED - Versement 2 - Attestation bon déroulement travaux année 1	Pour versement tranche 2		Non traité	
30/01/2024	ARED - Versement 2 - Bilan financier année 1	Pour versement tranche 2 ARED		Non traité	
30/01/2024	ARED - Versement 3 - Attestation bon déroulement travaux année 2	Pour versement 50% tranche 3 ARED		Non traité	
30/01/2024	ARED - Versement 3 - Bilan financier année 2	Pour versement 50% tranche 3 ARED		Non traité	
30/01/2024	ARED - Versement 4 - Bilan financier année 3	Pour versement solde année 3 ARED		Non traité	
30/01/2024	ARED - Versement 4 - Certificat administratif précisant statut thèse	Pour versement du solde de la tranche 3 (à accompagner des pièces justificatives correspondantes pour les cohortes jusqu?en 2018 : avis du jury, attestation de réinscription en ED, justificatif de prolongation ou d'abandon)		Non traité	
30/01/2024	ARED - Versement 4 - Avis du jury si thèse soutenue	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		Non traité	
30/01/2024	ARED - Versement 4 - Attestation de réinscription en ED	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		Non traité	

30/01/2024	ARED - Versement 4 - Justificatif de prolongation	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		Non traité	
	ARED - Versement 4 - Justificatif d'abandon de thèse	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		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 Enseignements effectués 3

3 Activités de recherche **4**
3.1 Résumé de la thématique et compétences scientifiques 4
3.2 Projets et collaborations 6
3.3 Activités d'intérêt collectif 8

4 Activités d'encadrement **9**
4.1 Encadrement d'étudiants de master 9
4.2 Encadrement doctoral 10
4.3 Publications et brevets 10

5 Annexes **17**

1 Curriculum vitae

Nom :	**Guillaume HIET**
Date et lieu de naissance :	Le 20 avril 1981 à Montluçon (Allier), 42 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 (résponsable 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. Ces enseignements ont porté à la fois sur mon domaine de recherche, la sécurité informatique, et sur d'autres domaines de l'informatique. Pour l'année 2019/2020, ma charge d'enseignement a diminué en raison de ma délégation partielle à Inria (50%). 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.

2.1 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. Une lettre de Jean-François Lalande, responsable de la formation en cybersécurité à CentraleSupélec, atteste la volumétrie de ma charge d'enseignement (CentraleSupélec ne publie pas d'état de service).

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.

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

Année	Formation Initiale	Formation Continue	Extérieure	Total
2022-2023	219	10,5	0	229,5
2021-2022	217,5	10,5	0	227,5
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

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 brevet. Un brevet nous a été accordé (US11308202B2) et l'autre demande est actuellement en cours d'instruction.

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).

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 CIDRE 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.

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 débuté une thèse de doctorat en 2021, dont j'assure la direction.

Projets terminés

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 en cours

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 débuté une thèse dans le cadre du partenariat stratégique entre Inria et l'ANSSI.

Projets terminés

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].

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

3.3 Activités d'intérêt collectif

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

J'assure régulièrement des relectures d'articles pour des publications en conférence ou en revue :
- SILM (2020, 2021, 2022, 2023, 2024)
- 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, 2023 et 2024.

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). 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 et 2023.

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 [4], principalement organisée par mes collègues Clémentine Maurice et Frédéric Tronel ;
- Un workshop durant la European Cyber Week en Novembre 2019 à Rennes [5], avec mes collègues Frédéric Tronel et Jean-Louis Lanet ;

4. https://silm-school.inria.fr/
5. https://silm-workshop.inria.fr/

— 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 [6] et en 2021 [7] ;
— Un séminaire régulier à Rennes [8], avec Ronan Lashermes.

4 Activités d'encadrement

4.1 Encadrement d'étudiants de master

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.

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

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-	Jean-Loup Houdot	Security-enhancing compiler against side-channel attacks	CominLabs, ANR	25%
2020-	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

Dans le cadre de ma collaboration avec HP, nous avons également effectué quatre demandes de brevets. Une de ces demandes est en cours d'instruction (EP3413532A1/WO2018226814A3) et trois brevets nous ont été accordés (US10896085B2, EP3647980B1, US11308202B2).

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

Cinq publications notables :

1. **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
2. **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
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. **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
5. **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

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] **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.

[6] 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.

[7] **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.

[8] **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.

[9] **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.

[10] 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.

[11] **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.

[12] **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.

[13] **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.

[14] **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.

[15] **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.

[16] **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.

[17] **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.

[18] **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.

[19] **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.

[20] **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.

[21] **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.

[22] **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.

[23] 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.

[24] **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.

[25] **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

[26] 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.

[27] 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

[28] **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.

[29] **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.

[30] **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.

[31] **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

[32] **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.

[33] **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.

[34] **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.

[35] **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.

[36] **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.

[37] **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.

[38] **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 [9]	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 [10])	Introduction aux réseaux et à la sécurité informatique	16,5	27	CTD [11]	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 [12]	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
12. 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	6	13	CM	Responsable du cours
Ing. CS	M2	Sécurité matérielle	4,5	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	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	6,75	20	CM	Responsable du cours
Ing. CS	M1	Systèmes embarqués et IoT	3	20	TP	Responsable du cours
Ing. CS	M2	Introduction à la sécurité	6,75	40	CM	
Ing. CS	M2	Sécurité matérielle	3	13	CM	Responsable du cours
Ing. CS	M2	Sécurité matérielle	4,5	13	TP	Responsable du cours
Ing. CS et MCS	M2	Système d'exploitation	15	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 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 et MCS	M2	Sécurité des OS	15	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	

CAMPAGNE DE BOURSES DE THESE

CREACH LABS 2024

DOSSIER DE PRE-CANDIDATURE

Creach Labs, créé par l'accord général de partenariat[1], lance un appel à candidatures commun avec la DGA, l'AID, la Région Bretagne et l'EUR CyberSchool afin de financer des projets de thèse.

Les personnes éligibles à ces financements en tant que directrice ou directeur de thèse sont les personnels habilités à diriger des recherches des établissements scientifiques signataires de l'accord (soit les tutelles des UMR IETR, IRISA, IRMAR, LabSTICC, IODE), les écoles militaires Saint-Cyr Coëtquidan et l'Ecole Navale ainsi que l'ENSAI.

Les bourses demandées à Creach Labs peuvent être des financements complets ou des demi-financements (si un demi-financement est déjà acquis par ailleurs).

Du fait que le contingent réservé des bourses Région est constitué de demi-financements, nous incitons fortement les porteurs de projets à rechercher d'autres demi-financements.

DATES A RETENIR

10novembre 2023	Date limite de soumission des projets scientifiques
12 janvier 2024	Publication de la liste des projets présélectionnés (listes principale et complémentaire)
12 avril 2024	Point d'étape sur la recherche d'étudiants/étudiantes
31 mai 2024	Date limite de soumission des CV des étudiants/étudiantes Clôture de l'appel
7 juin 2024	Publication des projets financés

[1] Accord général de partenariat, signé en 2021 réunissant la DGA, l'AID, la Région Bretagne, l'ANSSI, le CNRS, Inria, UR1, UR2, UBO, UBS, IMT Atlantique, CentraleSupélec, INSA, ENS Rennes, ENSTA Bretagne, ENIB.

PIECES A JOINDRE AU DOSSIER DE PRE-CANDIDATURE

1. **Le CV court** (sur 2 pages au plus) de la directrice ou du directeur de thèse comportant les informations suivantes :
    - Prénom, nom, nature du poste occupé, nom de l'employeur, cursus ;
    - La liste de publications importantes en lien avec le sujet déposé ;
    - La liste d'étudiants encadrés en indiquant l'année de début de la thèse, si elle est financée par Creach Labs et si la thèse est toujours en cours.
2. Le **CV court** des co-encadrants le cas échéant.
3. Le **formulaire de soumission** de l'AAP CREACH LABS comprenant la **description du sujet de thèse** en moins de 2 pages hors liste de publications.

Les dossiers de pré-candidatures seront transmis en un seul fichier sous format électronique (acronyme.pdf) à karine.chatel[at]creachlabs[point]fr pour le **10 novembre 2023** au plus tard.

LE PROJET DE THESE

Acronyme (8 caractères max.) : SecuHybrid

Titre de la thèse : Security Monitoring in Heterogeneous Computing

Unité de recherche : IRISA

Equipe : SUSHI

Directeur/directrice de thèse : Guillaume Hiet

Adresse mail : guillaume.hiet@centralesupelec.fr

Date d'obtention de l'HDR : 15/12/2021

Etablissement employeur : CentraleSupélec

Co-encadrants : Pierre Wilke (CentraleSupélec/IRISA) et Mickaël Dardaillon (INSA/IETR)

Mots clefs positionnant le sujet de thèse dans le référentiel [2]:

Cliquez ou appuyez ici pour entrer du texte.Ce projet s'intéresse à la détection d'intrusion (**B.3.2.2** et **C.4**) en tirant parti de composant matériel pour assurer la supervision et isoler les moniteurs de sécurité (**B.1.2.2** et **C.11**). Les solutions envisagées ne sont pas spécifiques à un cas d'usage et devrait s'appliquer à tous les cas d'usage identifiés en section **D**. Mots clés ACM : Intrusion detection, Embedded system security, Information flow control

[2] https://www.irisa.fr/appels-a-candidatures-CREACH-LABS-2024

Description synthétique du sujet de thèse en 2 pages maximum (hors liste de publications)

Résumé du projet

La meilleure stratégie pour sécuriser une application nécessite de recourir à différentes approches préventives. Toutefois, ces approches ne sont pas systématiquement employées ni infaillibles. Il est donc important de surveiller l'exécution du système, sur l'hôte lui-même (HIDS), afin de détecter d'éventuelles intrusions. Par ailleurs, de nombreuses approches ont été proposées dans la littérature pour surveiller l'exécution d'applications s'exécutant sur un CPU. Toutefois, un nombre croissant d'applications (par exemple, les applications implémentant des algorithmes d'IA) sont hybrides, i.e. elles déportent une partie de leur calcul sur différentes unités d'exécutions hétérogènes (CPU, GPU, NPU, FPGA, etc.), ce qui complexifie leur supervision. Nous souhaitons développer une approche de détection d'intrusion pour les applications hybrides.

Description des objectifs et originalité de la thèse

L'objectif de cette thèse de doctorat est de proposer une approche de détection d'intrusion pour les applications hybrides en distribuant le processus de détection sur différents moniteurs dédiés à chaque unité d'exécution, tout en limitant l'impact sur les performances du système surveillé et en assurant la protection des moniteurs. Nous proposons de considérer comme cas d'usage les applications hétérogènes développées par High-Level Synthesis (HLS) pour des plateformes utilisant des SoC FPGA (par exemple Xilinx UltraScale+). Nous proposons d'implémenter la génération des moniteurs au sein de l'outil HLS de Xilinx, qui repose sur le compilateur LLVM. Il est ainsi possible d'insérer des passes de compilation pouvant analyser et modifier le code intermédiaire généré par le compilateur.

Description des principaux verrous et techniques envisagées

- **Challenge 1** : **La détection d'intrusion doit être distribuée sur les différentes unités d'exécutions hétérogènes.** Il faut superviser en même temps l'exécution de différents noyaux de calcul qui s'exécutent sur différentes unités d'exécution et combiner les résultats. Cette tâche est complexifiée par l'hétérogénéité des unités d'exécution. Le recours à la HLS permet d'analyser les différents noyaux de calculs sous une forme homogène (LLVM IR) et de générer des moniteurs pour chaque unité d'exécution, par instrumentation du code.
- **Challenge 2 : Le moniteur doit être isolé des différentes unités d'exécution.** Dans un HIDS, le détecteur est colocalisé avec la cible qu'il est censé surveiller. Il faut donc s'assurer qu'un attaquant ne puisse désactiver ou corrompre le détecteur. Nous proposons d'isoler les différents moniteurs en tirant parti de fonctionnalités matérielles (par exemple, Arm TrustZone, les extensions de virtualisation ou les System Protection Units).
- **Challenge 3 : Il faut franchir le fossé sémantique résultant de l'isolation.** L'isolation du moniteur crée un fossé sémantique : le moniteur n'a plus accès facilement aux données de la cible lui permettant d'inférer son comportement de manière précise. Pour franchir ce fossé sémantique, nous envisageons de combiner différentes approches (analyse statique, instrumentation, mécanisme de traces matériel).

Approche méthodologique et critères de qualité des résultats obtenus

Dans un premier temps, il s'agira de définir et formaliser le modèle de détection envisagé (i.e., les propriétés de sécurité à vérifier). On envisage par exemple de s'intéresser au suivi dynamique des flux d'information (DIFT). Dans un deuxième temps il s'agira d'implémenter l'approche proposée dans l'outil de HLS pour des applications simples, déportant une partie de leur calcul dans un

nombre limité d'accélérateurs implémentés sur FPGA. Par la suite, il s'agira de généraliser l'approche en considérant des applications plus complexes.
L'approche sera évaluée expérimentalement en analysant la sécurité (qualité de la détection et robustesse des moniteurs face à des attaques) et l'impact sur les performances.

Etat de l'art s'appuyant sur un choix de publications importantes liées au sujet
Certains travaux portent sur la surveillance d'applications hybrides [11] ou le déploiement de moniteurs dans des accélérateurs matériels dédiés [13]. Ces travaux apportent des pistes intéressantes pour distribuer le processus de détection tout en minimisant l'impact sur les performances. Toutefois, ces approches se limitent au suivi des performances et à la mise au point des applications ; pas à la détection d'intrusion. Des travaux sur la synthèse de moniteurs pour des accélérateurs matériels développés en HLS [12], sans tenir compte de la partie logicielle.
Par exemple, le DIFT permet de détecter un large spectre d'attaques contre l'intégrité et la confidentialité. Il peut être implémenté au sein de l'OS [10], dans les applications [7], dans le processeur [8], ou dans un coprocesseur matériel dédié [4, 9]. Toutefois, ces différents travaux de DIFT ne permettent pas de suivre les flux d'informations dans les applications hybrides, où une partie des traitements est déportée sur un FPGA. Quelques travaux se sont intéressés à vérifier les flux d'information d'un circuit au niveau HDL [1-3, 5]. Néanmoins, ces travaux s'intéressent exclusivement à la vérification statique de flux d'information au sein d'un circuit matériel.
L'approche qui nous parait la plus prometteuse consiste à analyser et instrumenter le code intermédiaire d'un outil de type HLS afin d'y insérer un moniteur DIFT spécifique au circuit [6]. Ces travaux portent principalement sur la surveillance d'accélérateurs purement matériels, mais pas de systèmes hybrides.

Financements antérieurs du CREACH LABS
Détection d'intrusion dans les systèmes industriel (2015) et analyse dynamique de binaires (2018, financement obtenu par l'équipe PACAP et co-encadré par G. Hiet). Ces travaux s'intéressaient à la détection d'intrusion au niveau réseau et logiciel. La présente thèse s'intéresse aux applications hybrides et déporte les moniteurs sur des composants matériels dédiés.

Synergie avec le pôle cybersécurité de DGA Maitrise de l'information et/ou s'inscrivant dans la stratégie de spécialisation de la région (S3)
Le projet porte sur la cybersécurité, qui est un des leviers du Domaine d'Innovation Stratégique « ECONOMIE NUMERIQUE SECURISEE ET RESPONSABLE » de la Stratégie régionale de recherche et innovation (S3) de la région Bretagne. Il devrait également intéresser les équipes en charge de la LID (notamment Frédéric Majorczyk) et de la sécurité des composants matériels à DGA-MI, en particulier des accélérateurs matériels pour l'IA.

Synergies entre différentes équipes, explorant l'intérêt de nouvelles techniques dans le domaine de la sécurité (par exemple dans le domaine du droit, de la sociologie, de la géopolitique etc.)
Le projet sera l'occasion de renforcer la collaboration entre la future équipe SUSHI de l'IRISA et l'équipe ASIC de l'IETR. En outre des collaborations sont envisagées avec l'équipe ARCAD du Lab-STICC.

Liste des publications

[1] A. Ardeshiricham, W. Hu, J. Marxen et R. Kastner. “Register transfer level information flow tracking for provably secure hardware design”. In: Design, Automation Test in Europe Conference Exhibition (DATE), 2017, p. 1691-1696

[2] Armaiti Ardeshiricham, Yoshiki Takashima, Sicun Gao et Ryan Kastner. “VeriSketch : Synthesizing Secure Hardware Designs with Timing-Sensitive Information Flow Properties”. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. CCS ’19. London, United Kingdom: Association for Computing Machinery, 2019, p. 1623-1638.

[3] Andrew Ferraiuolo, Rui Xu, Danfeng Zhang, Andrew C. Myers et G. Edward Suh. “Verification of a Practical Hardware Security Architecture Through Static Information Flow Analysis”. In: Proceedings of the Twenty-Second International Conference on Architectural Support for Programming Languages and Operating Systems. ASPLOS ’17. Xi’an, China: Association for Computing Machinery, 2017, p. 555-568

[4] Hari Kannan, Michael Dalton et Christos Kozyrakis. “Decoupling dynamic information flow tracking with a dedicated coprocessor”. In: Dependable Systems & Networks, 2009.IEEE. 2009, p. 105-114

[5] Xun Li, Mohit Tiwari, Jason K. Oberg, Vineeth Kashyap, Frederic T. Chong, Timothy Sherwood et Ben Hardekopf. “Caisson: A Hardware Description Language for Secure Information Flow”. In: Proceeding of the 32nd ACM SIGPLAN Conference on Programming Language Design and Implementation. PLDI ’11. San Jose, California, USA: Association for Computing Machinery, 2011, p. 109-120

[6] C. Pilato, K. Wu, S. Garg, R. Karriet F. Regazzoni. “TaintHLS: High-Level Synthesis for Dynamic Information Flow Tracking”. In: IEEE Transactions on Computer-Aided Design of Integrated Circuits andSystems38.5 (2019), p. 798-808

[7] Feng Qin, Cheng Wang, Zhenmin Li, Ho-seop Kim, Yuanyuan Zhou et Youfeng Wu. “LIFT: A Low-Overhead Practical Information Flow Tracking System for Detecting Security Attacks”. In: Proceedings of the 39th Annual IEEE/ACM International Symposium on Microarchitecture. MICRO 39. USA: IEEE Computer Society, 2006, p. 135-148

[8] G Edward Suh, Jae W Lee, David Zhang et Srinivas Devadas. “Secure program execution via dynamic information flow tracking”. In: Acm Sigplan Notices. T. 39. 11. ACM. 2004, p. 85-96

[9] M. A. Wahab, P. Cotret, M. N.Allah, G. Hiet, V. Lapôtre et G. Gogniat. “ARMHEx: A hardware extension for DIFT on ARM-based SoCs”. In: 27th International Conference on Field Programmable Logic and Applications (FPL). 2017

[10] Nickolai Zeldovich, Silas Boyd-Wickizer, Eddie Kohler et David Mazières. “Making Information FlowExplicit in HiStar”. In: Proceedings of the 7th USENIX Symposium on Operating Systems Design and Implementation - Volume 7. OSDI ’06. Seattle, WA, 2006, p. 19-19

[11] Giacomo Valente, Tiziana Fanni, Carlo Sau, Tania Di Mascio, Luigi Pomante, and Francesca Palumbo. 2021. A Composable Monitoring System for Heterogeneous Embedded Platforms. ACM Trans. Embed. Comput. Syst. 20, 5, Article 42 (September 2021), 34 pages.

[12] M. B. Hammouda, P. Coussy and L. Lagadec, "A Unified Design Flow to Automatically Generate On-Chip Monitors During High-Level Synthesis of Hardware Accelerators," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 36, no. 3, pp. 384-397, March 2017, doi: 10.1109/TCAD.2016.2587278.

[13] Minjun Seo and Roman Lysecky. 2018. Non-Intrusive In-Situ Requirements Monitoring of Embedded System. ACM Trans. Des. Autom. Electron. Syst. 23, 5, Article 58 (September 2018), 27 pages. https://doi.org/10.1145/3206213

Cliquez ou appuyez ici pour entrer du texte.

Cliquez ou appuyez ici pour entrer du texte.