Demande n°3858 - ARED

Acronyme :GUARDONE

Identification

Identification

N°	3858
Année	2025
Statut	Brouillon
Date de création	28/01/2025
Date de modification	28/01/2025
Date de soumission	28/01/2025
Acronyme	GUARDONE
Intitulé du projet	Guarding Unauthorized Access and Runtime Deviations via Optimized ruNtime hardwarE monitors
Dispositif	ARED
Civilité du porteur	
Nom du porteur	Lashermes
Prénom du porteur	Ronan
Courriel	ronan.lashermes@inria.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	Salvador
Prénom	Ruben

Unité de recherche

Unité de recherche

Nom de l'unité	IRISA
Civilité	Monsieur
Nom	Gravier
Prénom	Guillaume
Courriel	guillaume.gravier@irisa.fr

Données complémentaires de l'unité de recherche

Libellé	Valeur
Statut et numéro de l'unité de recherche (UMR, USR, EA)	
Le cas échéant, nom de l'équipe de recherche	
Le cas échéant, nom du responsable de l'équipe de recherche	
Activités de recherche et points forts de l'équipe	Ce projet de thèse aura lieu dans l'équipe SUSHI de l'IRISA. Les recherches de SUSHI sont axées autour de la sécurité à l'interface logiciel/matériel. SUSHI est une jeune équipe de l'IRISA regardant le problème de la sécurité sous l'angle du logiciel bas-niveau et de la microarchitecture.
Si implication dans un/plusieurs programmes européens ou internationaux, préciser	

Co-directeur de thèse

Co-directeur de thèse

Civilité	Monsieur
Nom	Lashermes
Prénom	Ronan
Unité de recherche	IRISA
Etablissement de tutelle	INRIA

Description

Description du projet

Libellé	Valeur
Résumé synthétique du projet (2000 caractères max)	Le projet de thèse GUARDONE vise à renforcer la sécurité des microprocesseurs RISC-V contre les attaques sur le flot de contrôle et les chevaux de Troie matériels, déclenchables par logiciel. Ces attaques permettent d'exécuter des logiciels non autorisés ou de manipuler des données protégées. La solution proposée repose sur l'intégration de moniteurs de sécurité matériels (HSMs) [PAL21] utilisant des algorithmes de machine learning légers pour détecter et bloquer en temps réel les anomalies dans l'exécution des programmes. L'objectif est d'améliorer les mécanismes existants comme la protection mémoire physique (PMP), souvent vulnérables, en intégrant des solutions matérielles robustes, adaptatives et performantes [PAL23]. Le projet s'appuie sur des plateformes FPGA pour valider ces innovations, permettant de cibler des configurations RISC-V spécifiques et des scénarios d'attaques variés. En s'inscrivant dans une dynamique régionale et nationale en cybersécurité, cette thèse explore une approche originale mêlant intelligence artificielle et sécurité matérielle pour répondre à des menaces complexes et évolutives. Les principales étapes de cette thèse incluent : • La capture et simulation des traces d'exécution sous différents scénarios d'attaques. • La conception de modules HSM autonomes, suivie de leur intégration dans des cœurs RISC-V. • La validation de la solution avec des tests de scalabilité et des analyses de performance.
Caractère structurant/stratégique du projet (descriptif/ex. : art.5 Rglmt ARED 2025 -2000 car. max)	Ce projet a pour but la conception de processeurs sécurisés. Une étape nécessaire dans la maîtrise souveraine des briques technologiques pour concevoir des systèmes embarqués sécurisés. Par exemple dans un cadre militaire ou plus simplement pour améliorer la sécurité des systèmes civils.
Porteur du projet : date d'obtention de l'HDR ou dérogation	L'HDR du porteur est prévue pour le premier semestre 2025. Inscription à l'ED déjà faite, manuscrit en cours de finalisation.
Collaborations scientifiques (nature/pays) et partenariat socio-économique envisagé (3000 car. max.)	Cette thèse sera le fruit d'une collaboration entre Inria et CentraleSupélec (à Rennes), entre l'équipe SUSHI et le LHS de l'Inria de Rennes.
Si DIS identifié, préciser l'adéquation du projet avec le DIS (2000 car. maximum)	
Si priorité régionale cochée, préciser en quoi le projet s'y rattache effectivement (2000 car.max.)	
Si priorité régionale "Politique publique Région", préciser (voir liste au point 4, Règlement 2025)	Ce projet s'inscrit pleinement dans la politique "cybersécurité" de la région. Il s'agit d'explorer la sécurité des processeurs.
Cotutelle financière internationale (oui/non)	non
Nom(s) du(des) cofinanceur(s) envisagé(s) ou confirmé(s)	
Si cofinancement industriel, justifier le choix du dispositif ARED au lieu du dispositif CIFRE	
État du cofinancement (indiquer "acquis" ou "demandé")	
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

Collaboration internationale

Collaboration internationale

Pays	
Etablissement partenaire à l'étranger	

Pièces jointes

Date de mi	Type de pièce	Commentaire	Document	Valide	Commentaire
	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.		Non traité	
	ARED - Dépôt - Avis directeur·rice d'unité	Obligatoire - Voir le modèle à suivre dans l'onglet "Documents à télécharger"		Non traité	
	ARED - Dépôt - Justificatif cofinancement	Facultatif - Dépôt de demande, justificatif d'obtention, courrier du cofinanceur pressenti...		Non traité	
	ARED - Dépôt - Lettre partenaire étranger	Facultatif - Lettre d'engagement de l'établissement partenaire étranger en cas de cotutelle internationale		Non traité	
	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
	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	
	ARED - Versement - Convention de partenariat	Le cas échéant (si autorisation de reversement)		Non traité	
	ARED - Versement 2 - CV doctorant.e	Pour versement tranche 2		Non traité	
	ARED - Versement 2 - Copie du contrat doctoral (ou CDD ou attestation))	Pour versement tranche 2		Non traité	
	ARED - Versement 2 - Attestation bon déroulement travaux année 1	Pour versement tranche 2		Non traité	
	ARED - Versement 2 - Bilan financier année 1	Pour versement tranche 2 ARED		Non traité	
	ARED - Versement 3 - Attestation bon déroulement travaux année 2	Pour versement 50% tranche 3 ARED		Non traité	
	ARED - Versement 3 - Bilan financier année 2	Pour versement 50% tranche 3 ARED		Non traité	
	ARED - Versement 4 - Bilan financier année 3	Pour versement solde année 3 ARED		Non traité	
	ARED - Versement 4 - Certificat administratif précisant statut thèse	Pour versement du solde de la tranche 3		Non traité	