Demande n°3835 - ARED

Acronyme :CRUSH

Identification

Identification

N°	3835
Année	2025
Statut	Brouillon
Date de création	24/01/2025
Date de modification	28/01/2025
Date de soumission	28/01/2025
Acronyme	CRUSH
Intitulé du projet	Conception non-supervisée de méta-classes d'empreintes RF pour l'identification de dispositifs sensibles
Dispositif	ARED
Civilité du porteur	Monsieur
Nom du porteur	Gautier
Prénom du porteur	Matthieu
Courriel	matthieu.gautier@irisa.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	UNIVERSITE RENNES 1
Commune	RENNES
Civilité	Monsieur
Nom	Le Gouguec
Prénom	Fabrice

Unité de recherche

Unité de recherche

Nom de l'unité	IRISA
Civilité	Monsieur
Nom	Gravier
Prénom	Guillaume
Courriel	guig@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	Granit
Le cas échéant, nom du responsable de l'équipe de recherche	Olivier Berder
Activités de recherche et points forts de l'équipe	Securité RF Réseaux de capteurs Architectures adaptatives Radio logicielle Efficacité énergétique
Si implication dans un/plusieurs programmes européens ou internationaux, préciser	

Co-directeur de thèse

Co-directeur de thèse

Civilité	Monsieur
Nom	Gerzaguet
Prénom	Robin
Unité de recherche	IRISA
Etablissement de tutelle	UNIVERSITE RENNES 1

Description

Description du projet

Libellé	Valeur
Résumé synthétique du projet (2000 caractères max)	La vulnérabilité TEMPEST survient lorsque des données confidentielles sont émises via un canal non légitime. Ces canaux, souvent exploités en champ proche, posent des risques accrus avec des transmissions sans fil légitimes comme le Wi-Fi ou Bluetooth, étendant leur portée d'interception. Identifier les émetteurs ciblés reste un défi majeur. Une solution prometteuse est l'utilisation des empreintes radio-fréquences (RF), signatures uniques créées par les distorsions des composants matériels. Ces empreintes permettent une identification discrète, mais leur mise en œuvre pratique reste complexe. L'analyse des émissions RF offre des opportunités à la fois pour l'interception et la défense. Côté attaque, elle aide à exploiter des vulnérabilités spécifiques aux émetteurs. En défense, elle permettrait de regrouper les empreintes pour détecter les anomalies révélant des canaux cachés exploités. Cette double approche est cruciale pour sécuriser les communications. L'objectif de la thèse de doctorat est de proposer des méthodes de clusterisation permettant de regrouper les émetteurs par grappe (par exemple, le type de carte et la nature du constructeur) à partir de leur empreinte RF. Ce type de travail n'est pas présent dans la littérature : chaque dispositif est considéré comme ayant une empreinte unique et cherche à être détecté indépendamment, ou bien les dispositifs sont clusterisés par localisation géographique, et l'empreinte RF considérée dans ce cas est en réalité le canal de propagation. Ces travaux s'articuleront sur trois axes de recherche : - Axe 1 : Expérimental – Créer une base de données unique permettant de discriminer des cartes et constructeurs différents, en s'appuyant sur l'expérience de l'équipe et un protocole expérimental reproductible. - Axe 2 : Méthodologique – Explorer des méthodes de clusterisation adaptées pour regrouper des émetteurs en grappes, soit par l'adaptation des techniques classiques d'identification RF, soit en utilisant de méthodes de clusterisation pour extraire directement des caractéristiques pertinentes. - Axe 3 : Prospectif – Concevoir des méthodes de clusterisation non supervisées pour identifier des dispositifs à empreinte RF anormale et détecter de nouvelles méta-classes associées à des constructeurs non initialement considérés.
Caractère structurant/stratégique du projet (descriptif/ex. : art.5 Rglmt ARED 2025 -2000 car. max)	Cette thèse est dans la continuité des travaux d'Alice Chillet, thèse Creach Labs financée en 2021 et soutenue en novembre 2024. Le sujet de la thèse était « Identification aveugle par apprentissage de l'empreinte radio-fréquence de dispositifs sensibles ». Cette thèse a montré que l'identification des individus uniquement par leur empreinte RF reste une problematique encore tres ouverte, notamment très sensible à l'environnement. L'objectif de cette nouvelle thèse est l'identification des types d'émetteurs et non plus de l'individu. L'objectif étant l'identification de circuits particulièrement sensibles à des attaques. Il s'agit de proposer des méthodes de clusterisation permettant de regrouper les emetteurs par grappe. La thèse repose sur les expertises actuellement développées par l'équipe GRANIT sur l'identification RFF d'une part mais également sur les méthodes d'apprentissage. Par ailleurs, l'équipe a déjà réalisé une base de données de signaux réels avec des radios logicielles, montrant son expertise sur la validation expérimentale des modèles théoriques. Plus globalement, ces travaux s'inscrivent dans la thématique autour de la sécurité RF de l'équipe Granit, thématique initiée en 2018 par la thèse de Corentin Lavaud financé par le Pole d'Excellence Cyber. Divers projets ont pérennisé ces activités : ANR JCJC Red in Black de Robin Gerzaguet, CNRS INS2I ARPOSTEMP et RAPID DGA Recsanet (avec CG wireless et l'UBS).
Porteur du projet : date d'obtention de l'HDR ou dérogation	10 mai 2019
Collaborations scientifiques (nature/pays) et partenariat socio-économique envisagé (3000 car. max.)	Choix de publications importantes liées au sujet : [1] : Corentin Lavaud, Robin Gerzaguet, Matthieu Gautier, Olivier Berder, Erwan Nogues, et al.. Whispering devices: A survey on how side-channels lead to compromised information. Journal Hardware and Systems Security, 2021, (doi: 10.1007/s41635-021-00112-6). [2] : J. Guillaume, M. Pelcat, A. Nafkha, et R. Salvador, « Attacking at Non-harmonic Frequencies in Screaming-Channel

	Attacks », in Smart Card Research and Advanced Applications, S. Bhasin et T. Roche, Éd., Cham: Springer Nature Switzerland, 2024, p. 87106. doi: 10.1007/978-3-031-54409-5_5. [3] : Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. 2018. Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18), doi: 10.1145/3243734.324380. [4] : Corentin Lavaud, Robin Gerzaguet, Matthieu Gautier, Olivier Berder, Erwan Nogues, et al. Architecture temps-réel pour l'interception de signaux Bluetooth porteurs de compromission, in 29ème colloque du Groupement de Recherche en Traitement du Signal et des Images (GRETSI'23). [5] : A. Chillet, R. Gerzaguet, K. Desnos, M. Gautier, and al, "Understanding Radio Frequency Fingerprint Identification With RiFyFi Virtual Databases" IEEE Open Journal of the Communications Society, doi: 10.1109/OJCOMS.2024.3414858. [6] : G. Camurati and A. Francillon, "Noise-SDR: Arbitrary Modulation of Electromagnetic Noise from Unprivileged Software and Its Impact on Emission Security" 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2022, pp. 1193-1210, doi: 10.1109/SP46214.2022.9833767. [7] : S. G. Lee and C. Lee, "Developing an Improved Fingerprint Positioning Radio Map using the K-Means Clustering Algorithm," 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 2020, pp. 761-765, doi: 10.1109/ICOIN48656.2020.9016627. [8] : J. Gong, X. Xu and Y. Lei, "Unsupervised Specific Emitter Identification Method Using Radio-Frequency Fingerprint Embedded InfoGAN," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2898-2913, 2020, doi: 10.1109/TIFS.2020.2978620. [9] : H. Zhang, L. Zhao and Y. Jiang, "Triplet Network and Unsupervised-Clustering-Based Zero-Shot Radio Frequency Fingerprint Identification With Extremely Small Sample Size," in IEEE Internet of Things Journal, vol. 11, no. 8, pp. 14416-14434, 15 April 2024, doi: 10.1109/JIOT.2023.3341468.
Si DIS identifié, préciser l'adéquation du projet avec le DIS (2000 car. maximum)	Ce projet s'inscrit pleinement dans le domaine d'Innovation Stratégique « Economie numérique sécurisée et responsable » puisqu'il s'agit de concevoir et de mettre en oeuvre des techniques de traitement du signal numérique pour identifier des transmissions de signaux par empreinte RF. Ces travaux en lien avec les problématiques d'identification et d'interception de signaux compromettants font partie inhérentes des scénarios TEMPEST et sont parfaitement en phase avec le sous domaine lié à la cyber-sécurité. La sécurité des systèmes d'information est un enjeu crucial à de multiples échelles et la protection des données sensibles (mécanisme de défense) comme l'identification et l'interception de données (mécanisme d'attaque) présentent des intérêts stratégiques. Ce sujet de thèse est donc particulièrement intéressant pour le centre de recherche de la DGA-MI à Bruz et notamment son département dédié à la Sécurité des Systèmes d'Informations avec lequel nous sommes en contact (Erwan Nogues).
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)	Cybersécurité
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
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_gautier.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	