Conception non-supervisée de méta-classes d'empreintes RF pour l'identification de dispositifs sensibles

- Stage niveau master ou ingénieur -

Laboratoire : IRISA
Encadrements et contacts :

- Matthieu Gautier : matthieu.gautier@irisa.fr
- Robin Gerzaguet : robin.gerzaguet@irisa.fr
- Jeanne Lefevre : Jeanne.lefevre@enssat.fr

Lieu : Lannion
Durée : 6 mois à partir de fevrier 2025
Gratification par mois : environ 560€ par mois

Contexte de l'étude

Parmi la liste de menaces de cybersécurité, la vulnérabilité TEMPEST se produit lorsque des données confidentielles sont émises involontairement en raison de la présence d'un canal non légitime. Ce canal peut avoir une nature différente (lumière, son ou électromagnétique) et être dû à différentes causes (fuites électromagnétiques, couplage, exfiltration volontaire, etc.) [1]. Différentes attaques ont ciblé les canaux cachés électromagnétiques et se caractérisent généralement par une interception en champ proche. Il a récemment été démontré que les transmissions sans fil légitimes (par exemple, Wi-Fi ou Bluetooth) peuvent également dissimuler des canaux cachés, augmentant ainsi le risque de compromission [3,4], notamment en raison de l'augmentation de la portée d'interception.

Dans un contexte d'interception pratique, l'identification des émetteurs ciblés reste une problématique majeure encore très ouverte. Une manière d'identifier sans décoder les données est d'utiliser les empreintes Radio-Fréquences (RF). L'empreinte RF est une signature unique créée par les distorsions électromagnétiques des différents composants matériels du dispositif radio. Cette signature est inscrite dans le signal émis et peut être utilisée pour identifier discrètement et avec peu d'informations à priori [4]. L'utilisation de cette technique reste cependant encore sujette à des verrous lors de la mise en pratique.

En effet, l'analyse des émissions des émetteurs RF peut être une source d'information précieuse, que ce soit dans un motif d'interception ou de défense, sans aller nécessairement jusqu'à la reconnaissance du dispositif. Côté attaque, les fuites et vulnérabilités sont dépendantes du type de carte RF utilisées [3]. Être capable de reconnaître la nature d'un émetteur peut ainsi conduire à une analyse ou à une exploitation des vulnérabilités spécifiquement associées à ces plateformes. Côté défense, pouvoir regrouper les empreintes RF d'un même type de constructeur permettrait de détecter les anomalies pouvant révéler l'exploitation d'un canal caché au sein d'un dispositif [5].

Objectifs du stage

L'objectif de ce stage 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.
Les travaux réalisés pendant ce stage seront

- Prendre en main l'environnement d'analyse et de classification des empreintes radio-fréquence développée au laboratoire IRISA [4].

- Analyser et implémenter des méthodes de clusterisation adaptées pour discriminer des grappes d'émetteurs [6], les caractéristiques intéressantes seront extraites par des méthodes d'estimation directe.
- Développer des méthodes de clusterisation non supervisées [7,8] : à partir des descripteurs préalablement choisis, l'objectif sera de (i) détecter les dispositifs ayant une empreinte RF aberrante et (ii) faire apparaître de nouvelles méta-classes associées à des constructeurs non initialement considérés.
-

Profil visé

Vous êtes en dernière année d'école d'ingénieur ou en master. Vous avez de bonnes compétences en traitement numérique du signal et en télécommunications. Des bases en intelligence artificielle peuvent être un plus.
Ce stage peut valider un master recherche, une poursuite de ces travaux en thèse est possible.

Références

[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](https://doi.org/10.1007/s41635-021-00112-6)).

[2] 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](https://doi.org/10.1145/3243734.324380).

[3] 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).

[4] 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](https://doi.org/10.1109/OJCOMS.2024.3414858).

[5] 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](https://doi.org/10.1109/SP46214.2022.9833767).

[6] 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](https://doi.org/10.1109/ICOIN48656.2020.9016627).

[7] 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](https://doi.org/10.1109/TIFS.2020.2978620).

[8] 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](https://doi.org/10.1109/JIOT.2023.3341468).