PhD Offer : SCARE (Screaming Channel Attack Recognition and Evaluation)

Robustness Evaluation of an IDS Against Screaming Channel Attacks on Multi-Band Radio Gateways

,

Location: CentraleSupélec, Campus de Rennes, Av. de la Boulaie, 35510 Cesson-Sévigné
Supervisors: Dr. Mohamed El Bouazzati & Pr. Amor Nafkha – IETR / ASIC Team
Target Candidates: Master's degree (M2) or Engineering degree
Starting Date: October 2026
Duration: 3 years

Keywords:
Electromagnetic Side Channels, Screaming Channel, Hardware Security, Intrusion Detection System.

Context

The **Internet of Things (IoT)** has experienced remarkable growth in recent decades, becoming an integral part of modern life. It has driven major transformations across various domains by enabling continuous data monitoring and real-time remote control of systems. IoT applications span numerous sectors, including healthcare, smart homes, smart cities, agriculture, and industrial automation. The architectures of embedded IoT systems heavily rely on **heterogeneous System-on-Chip (SoC)** platforms that integrate both analog and digital components to support the application layer and ensure wireless connectivity [1], [2]. However, this tight integration introduces new security challenges, particularly due to the coexistence of diverse hardware and software components. Recent attacks have increasingly targeted IoT communication protocols such as **LoRaWAN**, **Bluetooth**, and **Zigbee**, exploiting vulnerabilities in their standards or implementations [3]–[6].

Intrusion Detection Systems (IDS) represent one of the key approaches to address these challenges [7], [8]. In recent years, anomaly detection and IDS mechanisms have been deployed within IoT architectures, combining software and hardware probes embedded in the system to monitor activity across multiple layers. Several state-of-the-art solutions, such as **Diwall** [9] and **I2DS** [10], favor hardware-based implementations, while others, including **OASIS** [11] and **BlueShield** [12], adopt software-based approaches. Both hardware and software IDSs typically assume a threat model involving a remote attacker. However, when an adversary gains physical access to the device, these systems may be compromised through traditional physical attacks.

Among the different categories of physical attacks, **side-channel attacks (SCAs)** are particularly concerning for embedded and connected systems. These attacks take advantage of unintentional physical leakages that occur during the execution of algorithms, such as fluctuations in power consumption, electromagnetic (EM) radiation, or execution timing. In heterogeneous SoC designs, **interactions between analog and digital components** can further increase these leakages: **digital operations may interfere with EM emissions**, forming potential side channels that can be exploited. Recent research has shown that such emissions can even be leveraged for remote exploitation through so-called **Screaming Channel** attacks, where electromagnetic signals produced by the processor unintentionally modulate the chip's radio transmissions. This phenomenon makes it possible to retrieve cryptographic information from several meters away—up to 30 meters in certain experiments [13]–[16]. In this context, we focus on IDS implementations deployed in multi-band radio gateways and analyze an expanded threat model in which a nearby adversary combines wireless and physical-layer attacks to compromise or evade intrusion detection. Screaming Channel attacks, which exploit unintended electromagnetic emissions caused by the co-location of mixed-signal components, represent a particularly stealthy vector. By silently leaking the presence and operational fingerprint of an IDS without triggering any detectable network activity, they provide the attacker with valuable information to refine their intrusion strategy and evade detection mechanisms.

Objectives

The primary objective of this PhD thesis is to systematically evaluate the robustness of existing gateway-level IDS against Screaming Channel attacks, and to design principled countermeasures grounded in this enlarged threat model.

- **Threat modeling and literature survey.** Conduct a comprehensive review of electromagnetic side-channel attacks (EM SCAs), Screaming Channel attacks, and existing IDS architectures for IoT and multi-band radio environments. Establish a formal threat model that integrates both wireless and physical attack surfaces.
- **Experimental validation.** Design and build a representative testbed deploying a state-of-the-art or commercial IDS within a multi-band IoT network (e.g., LoRaWAN, Zigbee). Experimentally demonstrate the feasibility of Screaming Channel attacks against active intrusion-detection policies, and characterize the leakage under realistic conditions.
- **Robustness evaluation.** Systematically assess the impact of Screaming Channel attacks on IDS detection capabilities. Quantify relevant metrics including attack success rate, effective operating distance, signal-to-noise characteristics, and degradation of detection performance (e.g., false negative rate, detection latency).
- **Countermeasure design and validation.** Propose, implement, and evaluate hardware and software countermeasures to harden IDS deployments against Screaming Channel threats. Develop a general methodology and design guidelines applicable to gateway-level IDS in heterogeneous radio environments.

Required Skills

- Master's degree or final-year Master's student (or equivalent) in Electronics, Embedded Systems, Computer Engineering, or a related field.
- Foundations in digital signal processing and physical-layer security concepts.
- Basic knowledge of wireless communication protocols and IoT network architectures (e.g., LoRaWAN, Zigbee).
- Experience with hardware debugging and RF measurement tools (oscilloscope, spectrum analyzer, software-defined radio) is a plus.
- Proficiency in C and Python; knowledge of VHDL, Verilog, and/or SystemVerilog is a plus.
- Familiarity with RISC-V processor architecture.
- Prior research experience (internship, research project, or publication) is appreciated.
- Previous experience with side-channel attacks or hardware security is a significant advantage.

How to Apply — Deadline: April 7th, 2026

Candidates should send their application by email with the subject line `[PhD SCARE IDS] + Full name` at :

- `mohamed.el-bouazzati@centralesupelec.fr`

The application package must include the following documents:

- A curriculum vitae
- Cover letter
- Academic transcripts from the last three years
- Two recommendation letters from academic supervisors or professors

References

[1] N. Semiconductors, *Iw693 – 2×2 dual-band (5-7 ghz) / 1×1 (2.4 ghz) concurrent dual wi-fi 6/6e + bluetooth combo solution*, Accessed: 2025-11-10, 2025. [Online]. Available: https://www.nxp.com/products/IW693.

[2] T. Instruments, *Cc3235s simplelink 32-bit arm cortex-m4 dual-band wi-fi® wireless mcu with 256 kb ram*, Accessed: 2025-11-10, 2024. [Online]. Available: https://www.ti.com/product/CC3235S.

[3] R. Cayre, F. Galtier, G. Auriol, *et al.*, "Wazabee: Attacking zigbee networks by diverting bluetooth low energy chips," in *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2021, pp. 376–387. DOI: 10.1109/DSN48987.2021.00049.

[4] R. Cayre, F. Galtier, G. Auriol, *et al.*, "Injectable: Injecting malicious traffic into established bluetooth low energy connections," in *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2021, pp. 388–399. DOI: 10.1109/DSN48987.2021.00050.

[5] S. S. Jung, M. Valero, A. Bourgeois, *et al.*, "Attacking and securing beacon-enabled 802.15.4 networks," *Wireless Networks*, vol. 21, no. 5, pp. 1517–1535, 2015. DOI: 10.1007/s11276-014-0855-2.

[6] M. M. Fouda, Z. M. Fadlullah, and N. Kato, "Assessing attack threat against zigbee-based home area network for smart grid communications," in *The 2010 International Conference on Computer Engineering & Systems*, 2010, pp. 245–250. DOI: 10.1109/ICCES.2010.5674861.

[7] T. Bilot, B. Jiang, Z. Li, *et al.*, "Sometimes simpler is better: A comprehensive analysis of state-of-the-art provenance-based intrusion detection systems," in *34th USENIX Security Symposium (USENIX Security 25)*, 2025, pp. 7193–7212.

[8] M. S. Korium, M. Saber, A. Beattie, *et al.*, "Intrusion detection system for cyberattacks in the internet of vehicles environment," *Ad Hoc Networks*, vol. 153, p. 103 330, 2024.

[9] M. El Bouazzati, P. Tanguy, G. Gogniat, *et al.*, "Diwall: A lightweight host intrusion detection system against jamming and packet injection attacks," *ACM Trans. Embed. Comput. Syst.*, vol. 24, no. 5, Sep. 2025. DOI: 10.1145/3711833. [Online]. Available: https://doi.org/10.1145/3711833.

[10] I. Morianos, K. Georgopoulos, A. Brokalakis, *et al.*, "I2ds: Fpga-based deep learning industrial intrusion detection system," in *Embedded Computer Systems: Architectures, Modeling, and Simulation*, L. Carro, F. Regazzoni, and C. Pilato, Eds., Cham: Springer Nature Switzerland, 2025, pp. 165–176.

[11] R. Cayre, V. Nicomette, G. Auriol, *et al.*, "Oasis: An intrusion detection system embedded in bluetooth low energy controllers," in *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, ser. ASIA CCS '24, Singapore, Singapore: Association for Computing Machinery, 2024, pp. 700–715. DOI: 10.1145/3634737.3645004.

[12] J. Wu, Y. Nan, V. Kumar, *et al.*, "BlueShield: Detecting spoofing attacks in bluetooth low energy networks," in *23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*, San Sebastian: USENIX Association, Oct. 2020, pp. 397–411. [Online]. Available: https://www.usenix.org/conference/raid2020/presentation/wu.

[13] J. Guillaume, M. Pelcat, A. Nafkha, *et al.*, "Attacking at non-harmonic frequencies in screaming-channel attacks," in *Smart Card Research and Advanced Applications*, S. Bhasin and T. Roche, Eds., Cham: Springer Nature Switzerland, 2024, pp. 87–106.

[14] P. Ayoub, R. Cayre, A. Francillon, *et al.*, "Bluescream: Screaming channels on bluetooth low energy," in *2024 Annual Computer Security Applications Conference (ACSAC)*, 2024, pp. 636–649. DOI: 10.1109/ACSAC63791.2024.00060.

[15] G. Camurati, A. Francillon, and F.-X. Standaert, "Understanding screaming channels: From a detailed analysis to improved attacks," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2020, no. 3, pp. 358–401, Jun. 2020. DOI: 10.13154/tches.v2020.i3.358-401. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/8594.

[16] J. Guillaume, M. Pelcat, A. Nafkha, *et al.*, "Multi-screaming-channel attacks: Frequency diversity for enhanced attacks," *(Submitted to IEEE Transactions on Information Forensics and Security (TIFS))arXiv preprint arXiv:2504.02979*, 2025.