PhD Offer

Keyboard Compromission Through Electromagnetic Attacks using Wavefront Shaping

Supervision François Sarrazin: Junior Professor Chair at Université de Rennes
Philippe Besnier: Research Director at CNRS

Keywords: Electromagnetic compatibility/cybersecurity, Wave control, Fault-injection

PhD Context: Electromagnetic cybersecurity relates to the use of electromagnetic waves to compromise data. Keyboards are critical targets because they are widely used as a computer peripheral and keystroke retrieval may lead to sensitive information recovery. Various attacks have been proposed to remotely retrieve keystrokes by listening to electromagnetic emanations either in a passive [Vua09] or active [Kaj23] manner using backscattering measurement. However, the feasibility of denial-of-service attacks on computer keyboard remains an open challenge.

PhD Objectives and Work Plan: This PhD aims at developing beyond-state-of-the-art electromagnetic attacks to compromise keyboard availability (denial of service) and integrity (fault injection). To that end, we will take benefit of wavefront shaping techniques in a guided propagation medium such as power or communication cables, in order to enable non-line-of-sight attacks at an extended range. The thesis is organized as follows:

- Electromagnetic compatibility study of keyboards for both immunity and susceptibility
- Development of denial-of-service and fault-injection attacks
- Attack range extension using spatial diversity [Yeo21]
- Proposals for countermeasures

PhD Working Environment: The PhD will take place at the IETR – UMR CNRS 6164 (www.ietr.fr) on the *Beaulieu* campus of the *Université de Rennes*, France. The PhD student will join the eWAVES team (Electromagnetic cybersecurity theme) and will benefit from IETR's world-class technological platforms including Complex Systems Oriented Quantification.

Applicant Profile

Education level: Master or equivalent degree
Background: electrical engineering, physics, or hardware cybersecurity
Language: French is not required

Practical Details and Application

Application deadline: May 31st 2024
Starting date: Around October 2024 for 36 months
How to apply: **send a resume, cover letter and last academic transcripts to francois.sarrazin@univ-rennes.fr**

Bibliography

[Vua09] M. Vuagnoux and S. Pasini, "*Compromising Electromagnetic Emanations of Wired and Wireless Keyboards*," **Conference on USENIX Security Symposium**, Berkeley, CA, USA, pp. 1–16, 2009.
[Kaj23] S. Kaji, D. Fujimoto, M. Kinugawa and Y. Hayashi, "Echo TEMPEST: EM Information Leakage Induced by IEMI for Electronic Devices," **IEEE Transactions on Electromagnetic Compatibility**, vol. 65, no. 3, pp. 655-666, June 2023, doi: 10.1109/TEMC.2023.3252636.
[Yeo21] K. B. Yeo, M. Davy and P. Besnier, "*Non-invasive Optimal Coupling Upon Detection of a Local Change of Impedance in a Cable Network*," **2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium**, Raleigh, NC, USA, 2021, pp. 528-532, doi: 10.1109/EMC/SI/PI/EMCEurope52599.2021.9559312.