<div align="center">

Internship Master's Degree in Computer Science & Networks
</div>

Topic: Analysis and Mitigation of Security Attacks on 5G Slices

Context:

With the rise of 5G networks, the virtualization of networks through slices has become a key approach to offering tailored services that meet diverse user needs. However, this complex architecture introduces new vulnerabilities and increases potential attack surfaces. Understanding these attacks is essential for developing effective security mitigations compliant with the zero-trust paradigm. This internship will rely on the use of an academic 5G platform, an infrastructure dedicated to testing in the 5G environment. The proposed work will be carried out within the SOTERN research team (https://www-sotern.irisa.fr/), which is involved in the PEPR 5G NF HiSec project.

Objectives:

The internship has three main objectives:

1. Conduct a comprehensive literature review on the various attacks that can target slices in 5G networks. This includes analyzing the types of attacks, attack methods, potential impacts on services and mitigation approaches.
2. Identify, analyze and reproduce selected 5G security attacks on academic 5G platform.
3. Develop, implement and evaluate mitigations compliant with the zero-trust paradigm.

Main tasks:

- **Literature Research:** Identify and analyze scientific articles, technical reports, and recent publications on attacks in 5G networks, focusing specifically on slices.
- **Classification of Attacks:** Classify attacks based on their nature (e.g., denial of service attacks, data integrity attacks, confidentiality attacks, etc.), the underlying threat model, etc...
- **Analysis of Practical Cases:** Study selected attack cases to illustrate the risks associated with 5G slices.
- **Implementation and evaluation of Attack Scenarios:** Develop, implement and evaluate selected attack scenarios and their mitigations on the academic 5G platform.
- **Synthesis and Recommendations:** Write a scientific paper detailing the findings of the internship.

Internship Location:

IMT Atlantique - Rennes Campus-SRCD Department - SOTERN research team

2, Rue de la Châtaigneraie - CS 17607 - 35576 Cesson Sévigné Cedex

Level / Duration:

Master's (Bac + 5) / 6 months

Desired Profile:

- Student in computer science, telecommunications, or a related fields.
- Strong knowledge of telecommunications networks (3GPP).
- Knowledge of information system security and protocol analysis.
- Programming skills (Python or other network-oriented languages).
- Ability to analyze scientific publications, delivering oral presentations, and writing reports.
- Autonomy, thoroughness, and analytical skills.

Application Process:

Please send an email to *(issam-abdeldjalil.ikhelef@imt-atlantique.fr)* including:

➢ **A cover letter covering your experience, motivations and possible contacts for recommendation.**

➢ **Your CV and detailed academic results.**

The selected candidate will work in the national project NF-HiSec (End-to-End Security for the Networks of the Future) within the framework of the French economic recovery plan (France 2030). This project's consortium involves several higher education institutions and national research institutes. It aims to explore cybersecurity issues arising in next-generation networks.

Start date : February/March 2025

Application deadline : 31/12/2024

Gratification: 610 euros net per month.

Supervisors:

- Issam Ikhelef (issam-abdeldjalil.ikhelef@imt-atlantique.fr)
- Ahmed Bouabdallah (ahmed.bouabdallah@imt-atlantique.fr)
- Guillaume Doyen (guillaume.doyen@imt-atlantique.fr)
- Fabien Autrel (fabien.autrel@imt-atlantique.fr)
- Grégory Blanc (gregory.blanc@telecom-sudparis.eu)

References:

1. S. Zhang – An Overview of Network Slicing for 5G – IEEE Wireless Communications - June 2019
2. De Alwis, C., Porambage, P., Dev, K., Gadekallu, T. R.,and Liyanage, M., 2024. "A survey on network slicing security: Attacks, challenges, solutions and research directions". IEEE Communications Surveys Tutorials, 26(1), pp. 534–570.
3. Singh, V. P., Singh, M. P., Hegde, S., and Gupta, M., 2024. "Security in 5g network slices: Concerns and opportunities". IEEE Access, 12, pp. 52727–52743.
4. Arora, S., Boutiba, K., Mekki, M., & Ksentini, A. (2022). A 5G facility for trialing and testing vertical services and applications. IEEE Internet of Things Magazine, 5(4), 36-41.
5. H. A. Kholidy, M. Mahmoud, A. Karam, M. Badr, J. Sidoran, M. Mahmud, M. A. Rahman, and A. F. Sayed, "Toward Zero Trust Security in 5G Open Architecture Network Slices," MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM), pp. 1-6, 2022, doi: 10.1109/MILCOM55135.2022.10017474.
6. 3GPP TS 28.530 - Management and orchestration; Concepts, use cases and requirements - Release 18, V18.1.0, Sept. 2024.