PhD Title: Moving Target Defense to improve the security of virtualised networks

IMT Atlantique : Campus X **Brest** ☐ **Nantes** ☐ **Rennes**
Laboratory : LABSTICC

École doctorale : X **SPIN** ☐ **3MG**

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Context :

IMT Atlantique, internationally recognised for the quality of its research, is a leading general engineering school under the aegis of the Ministry of Industry and Digital Technology, ranked in the three main international rankings (THE, SHANGHAI, QS).

Located on three campuses, Brest, Nantes and Rennes, IMT Atlantique aims to combine digital technology and energy to transform society and industry through training, research and innovation. It aims to be the leading French higher education and research institution in this field on an international scale. With 290 researchers and permanent lecturers, 1000 publications and 18 M€ of contracts, it supervises 2300 students each year and its training courses are based on cutting-edge research carried out within 6 joint research units: GEPEA, IRISA, LATIM, LABSTICC, LS2N and SUBATECH.
The proposed thesis is part of the research activities of the team: Math&Net and of the LABSTICC laboratory and the department of Computer Science.

Research Context:

Virtualised networks have become a major target of cyber attacks that aim at e.g. gaining unauthorised access to data or making networking services unavailable. While virtualisation provides a certain flexibility, it is also associated with an increased attack surface due to the complexity of the software stack and the security risks inherent in sharing hardware resources. Firewalls or IDS/IPS approaches, while effective, are static and cannot be deployed on a massive scale without inducing prohibitive resource usage. The static nature of virtualised network infrastructures - including defensive infrastructures - makes it easier for attackers that have sufficient time to investigate structural vulnerabilities in the network and launch attacks. Moving Target Defense (MTD) consists on adapting the environment in order to prevent or delay an attack on a system. The concept, existing on other context for years, has been applied to networking in the last decade. More recently, the advent of virtualisation technologies has offered new opportunities for this techniques along with more vulnerabilities from the security perspective, bringing both solutions and new challenges.

PhD Research Project

In this context, this thesis is focused on Moving Target Defense (MTD) solutions applied to virtualised networks. The ultimate goal being the development of diverse and dynamic configurations of network systems in order to reduce the attack surface, increase the attacker's uncertainty and thus the complexity required to complete the attack. .

From this perspective, it is crucial to **model the attacker-defender** interactions to formally analyse the MTD strategies to be implemented. Tools such as game theory and artificial intelligence have shown to be well fitted for this objective, while scalabillity of the solutions remains a challenge not yet well addressed by the literature.

Another paramount aspect when defining strategies, is to make these defense strategies **dynamic** and **unpredictable** so as to mask the state of virtualised infrastructures and make vulnerabilities difficult to exploit and infrastructures more resilient to the ever more diverse attacks. In this regard, the main challenges are related to the **formal definition of new reconfiguration strategies that do not allow the attacker to anticipate the strategies** and therefore to circumvent them, or even to understand the changes made to defend the virtualised network.

Moreover, appropriate decisions must analyse the risks and actions costs in order to maximise the security provided while ensuring that the performance impact is minimised. Indeed, there is a delicate **trade-off** between the cost and the impact that this defensive policy may have on the performance of the virtualised network, which must be budgeted for and minimised, while on the contrary, the attacker's effort must be maximised and his/her chances of identifying targets, gathering information and

carrying out successful attacks, minimised. The definition of pertinent performance metrics is a a crucial preliminary step towards this objective.

In addition to *what* to move (defining the set of new configurations to be applied) and *how* to move (the policy selecting the new configuration to be applied) it is crucial to define ***when* to do changes**. Indeed, the timing problem has received very little attention in previous related works. Some empirical studies are present in the literature, providing mainly fixed (constant) intervals, which remain very specific to the threat model and most likely not optimal.

Last but not least, the challenges include **a good understanding and representation of the different steps required for attacks and the vulnerabilities inherent in virtualised networks** in order to define changes to be made ranging from (i) changes/permutations of the virtualised execution environment taking advantage of software diversity for example, (ii) reconfiguration of the network topology with in particular the adaptation of routing, redirection of traffic to honeypots, or even the obfuscating of the network functions implemented.

Require skills:

The applicant should have a Master degree (or equivalent) in computer science with background and/or research interests in the following areas: computer networks, security, NFV/SDN. Prior internships with R&D expertise in these areas will be a plus. Experience in the implementation of software prototypes is expected. Applicant must be fluent in English.

Work Plan:

To approach this thesis, the work plan is as follows:

- State of the art on existing defensive MTD approaches,
- Exploratory study: develop metrics to quantify the attack surface and propose new defensive strategies and their evaluation
- Advanced study: establish a model of the interactions between attacker and defender to support a more formal analysis of the MTD strategies implemented and adapt the defense strategies accordingly, striking a balance between security and feasibility/cost.
- Improvement and optimisation of defensive mechanisms,
- Study of the integration of the proposed solutions in a cloud/NFV/SDN infrastructure

Application:

To apply for this position, please send a detailed application including a cover letter, an up-to date CV, transcripts of grades and reference letters

Additional Information :

Application deadline : May 15th 2023

Start date: September 2023
Contract duration: 36 months
Location: IMT-Atlantique, Brest
Contacts:

- Françoise SAILHAN francoise.sailhan@imt-atlantique.fr
- Isabel Amigo isabel.amigo@imt-atlantique.fr