BEYOND5G – Thesis proposal #1 on Security Quantification (WP3T2)

Joaquin Garcia-Alfaro Christophe Kiennert Gregory Blanc
Télécom SudParis
Institut Polytechnique de Paris
{firstname.family_name}@telecom-sudparis.eu

Context

Network and function virtualization technologies (SDN/NFV) are considered enablers to 5G slices, that is virtual and physical resources are dynamically allocated and orchestrated by an infrastructure provider to fulfil the needs of a customer or a service provider. 5G slicing could be vulnerable to a number of threats across time including information leakage at design time, policy tampering at deployment stage, or application vulnerability exploitation or denial of service during runtime [3]. At the same time, those same enablers allow slice owners to specify security policies and constraints that would apply to their slice. Such policies and constraints are negotiated with infrastructure and service providers in the form of service-level agreements (SLA). Finally, these policies are deployed automatically and evaluated continuously so as to anticipate changes. Therefore, it is needed to quantify security indicators and deploy means to continuously monitor them. The slice owner or operator would gain insights on the security level of the slice and subsequently verify the enforcement of security policies. This ultimately ensures that security is guaranteed throughout the slice lifecycle.

Objectives.

The objective of the proposed work is to develop a number of indicators of security to quantify the level of security of a system in order to gain situational awareness. This will enable operators to take informed decision on the security of the slice. Therefore, the candidate will pursue the following goals:

- quantify risks related to cybersecurity
- quantify mitigation and detection systems in a dynamic 5G slicing system
- quantify the efficiency and collateral damages of automated countermeasures

Proposal

The proposed work aims at securing 5G slices and verifying that deployed policies are compliant with what was specified by the slice owner in terms of slicing and security. From the metrics collected throughout the infrastructure, we will be able to gain insights on the state of the slice, and its security level.

Thus, we propose to define a model of the slice as a digital twin in order to quantify its risks. The security policies are often expressed in a domain-specific language, and together with the aforementioned model, we propose to quantify the coverage of mitigation and detection systems – by deriving security policies from the owner's specifications (SLAs) to the implemented dataplane configurations – with respect to expected threats, through injection against the digital twin.

Finally, we will improve on existing response quantification methodologies [1, 2] to adapt to 5G needs, to measure the trade off between the efficiency of the response and its potential collateral damages against the slice.

Application

We are open to applications to be reviewed as soon as possible, and followed by an (remote) interview, if accepted. Potential candidates MUST hold a Master-level degree or equivalent (e.g., a French *diplôme d'ingénieur*) and have experience in domains related to this thesis offer (network virtualization, digital twin, modelization, optimization) as well as a strong motivation for research. The candidate SHOULD provide the following items as an application package by email to all the thesis supervisors:

- up-to-date resume (CV);
- a copy of the latest degree (or ongoing if completion date is September 2021);
- letters of recommendation, or a list of references (people that would recommend the candidate).

Incomplete packages will not be reviewed.

The thesis work will take place at Télécom SudParis (Palaiseau or Evry), within a restricted access area, for which the candidate will need to get clearance. The thesis work will contribute to a national project funded by Bpifrance, the French public investment bank.

[1] G. Gonzalez-Granadillo, H. Debar, G. Jacob, C. Gaber, and M. Achemlal. Individual countermeasure selection based on the return on response investment index. In *Proc. of MMM-ACNS'12*. Springer, 2012.

[2] A. Motzek, G. Gonzalez-Granadillo, H. Debar, J. Garcia-Alfaro, and R. Möller. Selection of Pareto-efficient response plans based on financial and operational assessments. *EURASIP Journal on Information Security*, 2017.

[3] N. G. Olimid, Ruxandra F. 5G Network Slicing: A Security Overview. *IEEE Access*, 8:99999–100009, 2020.