Ph.D. proposal:

Modeling and verification of new AI-based techniques for attack and anomaly detection and prevention

Ludovic APVRILLE, Maria MUSHTAQ, Van-Tam NGUYEN
Telecom Paris
LabSoC et SSH teams
450 routes des Chappes, F-06904 Sophia-Antipolis Cedex, France
19, place Marguerite Perey, CS 20031, F-91123 Palaiseau Cedex, France
Email: firstname.lastname@telecom-paris.fr

June 20, 2024

1 Context et problematic

5G networks will progressively interconnect together embedded systems and information systems, thus offering new attack opportunities for cyber-criminals. In these systems, security threats can arise from different aspects. First, the hardware architecture used to support the network (network equipment, user equipment) can open doors to attacks, for instance a malicious network equipment could intercept (confidential) communications or security materials (keys, etc.). Second, the communication protocols used at different layers (physical layer, mac layer, application layer) could contain flaws exploitable by a remote or inside attacker. Last, the implementation of the system itself can offer opportunities to attackers, e.g., because of software bugs (attack using

buffer overflows), of hardware bugs (side-channel attacks). The security modules used to counter some of the attacks can themselves introduce new security vulnerabilities.

To tackle the security of such complex networked systems, several approaches can be used, both at system design and at system monitoring. System design intends to produce a system less susceptible to be successfully attacked, while system monitoring checks at runtime that no attacks are currently being led. Many recent research works suggest to rely on AI to detect attack at runtime. Yet, using such modules impacts the system architecture (cost, performance) and using them in an efficient way in a given system architecture is still an open issue.

2 Objectives

The Ph.D. intends to propose a **new system design and verification approach that can handle systems with security detection modules and with network features such as 5G**.

There already exist techniques for designing such complex systems, but none of these approaches can take into account the specificities of AI detection modules. Moreover, the design approach of these systems must be able to capture the different system elements we have mentioned before, such as network and user equipments, including their hardware and software, and the different communication protocols, in particular the ones used at physical and mac layers.

The involved research teams have published for years on the modeling and verification of complex embedded systems, taking into account hardware and software aspects. Thus, starting from our previous research on system modeling, including SysML-Sec [1] and its support toolkit named TTool [2], the first task will be to define new ways to capture communication layers: physical and mac layers, as well as the supporting hardware. Then, it will be necessary to propose a way to abstract AI security modules in order to add then to system models: their main features such as detection of attacks and anomalies [3], and the prevention of attacks [4] and anomalies will have to be carefully designed. Security constraints not yet supported by our current proposals will have to be addressed as well. Finally, model transformations will have to be defined in order to automate the verification of security and performance properties from the previously defined modeling environment. Obviously, evaluating the ability of the proposed framework to address 5G systems with AI security modules is also part of the work.

This work is to be performed in the scope of a national collaborative project called "PERP-5G". Thus, solutions will be developed in collaborations with other partners of the project and the approach will be evaluated in the scope of case studies developed in the scope of the project.

3 Expected work

To address the problems mentioned above, the Ph.D. candidate will likely proceed as follows:

1. State of the art: Deeply understanding how 5G systems are currently designed and what are the different approaches to detest attacks at runtime, including the ones based on AI.

2. Definition of a modeling framework.
3. Proposal of a model transformation to prove performance and security.
4. Evaluation of this proposal on concrete use cases from the project.
5. Development of extensions to TTool in order to support the newly defined modeling and verification features.

4 Skills

- Excellent skills are expected in modeling, verification and artificial intelligence.
- No knowledge on wireless communication is necessary (but you should be willing to learn and progress in that area)

5 How to apply?

Please send the following documents—**with a unique pdf file**—by email to ludovic.apvrille@telecom-paris.fr, maria.mushtaq@telecom-paris.fr and van-tam.nguyen@telecom-paris.fr Incomplete applications won't be considered. Selected candidates will be evaluated on their technical abilities and on their ability to carry on a research works (for instance: reviewing a research paper).

- Detailed CV
- Motivation letter clearly explaining why they would like to work on the topic of the Ph.D.
- Recommendation letters.
- Academic Transcripts (including ranking)
- List of publications (if any)

References

[1] L. Apvrille and Y. Roudier. SysML-Sec: A Model Driven Approach for Designing Safe and Secure Systems. In *3rd International Conference on Model-Driven Engineering and Software Development, Special session on Security and Privacy in Model Based Engineering*, France, February 2015. SCITEPRESS Digital Library.

[2] Ludovic Apvrille. Webpage of TTool. In *http://ttool.telecom-paris.fr/*, 2023.

[3] Maria Mushtaq, Jeremy Bricq, Muhammad Khurram Bhatti, Ayaz Akram, Vianney Lapotre, Guy Gogniat, and Pascal Benoit. Whisper: A tool for run-time detection of side-channel attacks. *IEEE Access*, 8:83871–83900, 2020.

[4] Maria Mushtaq, Muhammad Muneeb Yousaf, Muhammad Khurram Bhatti, Vianney Lapotre, and Guy Gogniat. The kingsguard os-level mitigation against cache side-channel attacks using runtime detection. *Annals of Telecommunications*, pages 1–17, 2022.