Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

University of Molise

FORESEEN

PRIN-PNRR 2022

Kickoff meeting

Our Team - UniMol

- **Antonella Santone** - Associate professor (Deputy PI)
    - Topics of Interest: Formal Methods, Model Checking
- **Simona Correra** - PhD Student (not paid on the project, yet working on related topics)
    - Topics of Interest: Pattern Recognition, Data Mining
- **Francesco Mercaldo** - Assistant Professor (not paid on the project, yet working on related topics)
    - Topics of Interest: Artificial Intelligence, Security
- **Vittoria Nardone** - Assistant Professor (not paid on the project, yet working on related topics)
    - Topics of Interest: CPS, Data Mining
- **Giulia Varriano** - Phd Candidate (not paid on the project, yet working on related topics)
    - Topics of Interest: Model Checking, Image Processing

WP3 Tasks

- T3.1 Formal model generation [M: 9-20] - T3.1 will produce D4.1
- T3.2 Pattern identification [M: 13-20]
- T3.3 Properties definition [M: 15-16]
- T3.5 Explainability [M: 17-20]

T3.1 Formal model generation [M: 9-20]

The main aim of this task is to build a Formal Model starting from traces generated by the execution of system co-simulation architecture (provided by T2.1 and T2.2).

- Starting from execution traces we can build several automata communicating with each other to simulate the real behavior of the system
- Each automaton can represent an agent involved in the system
- We can consider each trace as a formal action performed by the system
- Every communication can be modeled as a synchronizing action

T3.2 Pattern identification [M: 13-20]

The goal of this task is the identification of patterns suggesting the possibility of an attack.

- We can empirically investigate whether system actions performed during an attack are significantly different from those performed during normal execution
- Then, we can try to identify whether recurrent patterns exist by analyzing the actions performed during an attack

T3.3 Properties definition [M: 15-16]

Once patterns characterizing attacks have been identified, we proceed with the formal properties definition.

- Basically, we can translate each pattern identifying malicious actions into a logical property of the system
- We can use these properties as logical formulae, and each formula identifies a specific malicious pattern
- Finally, these formulae can be verified on the model of the system using model checker tools. If a formula results true over a model it means that the system under analysis has been attacked

T3.5 Explainability [M: 17-20]

Once the model has been formalized, it is necessary to understand how an explainability of the given results can be provided. The report that is expected to be generated, in fact, must be clear and understandable even to non-experts in the domain.