University of Stuttgart

Aerospace Engineering and Geodesy

Bachelor/Master thesis:

Development of an LLM-Based Agent for Continuous Aviation Security Risk Assessment

Motivation: Currently security risk assessment (SRA) in aviation is done mostly manually and depends on cyber-security expert's effort. Considering the rapidly changing threat landscape, handling cyber-threats to future aircraft and air traffic management infrastructures will be extensive. Especially, when the usage of commercial-off-the-shelf (COTS) components and a more open networking approach is applied. Therefore, we created a conceptual framework, that utilizes a multi-layer model-based architecture description and a concluding model-based SRA. To keep the models and the risk assessment up-to-date, we proposed leveraging LLMs and connection to external databases for that.

Goal: The goal of this thesis is to develop the agent *secLLM*, which continuously analyzes emerging security threats and provides relevant information to the multi-layer security assessment, enabling continuous cybersecurity risk assessment.

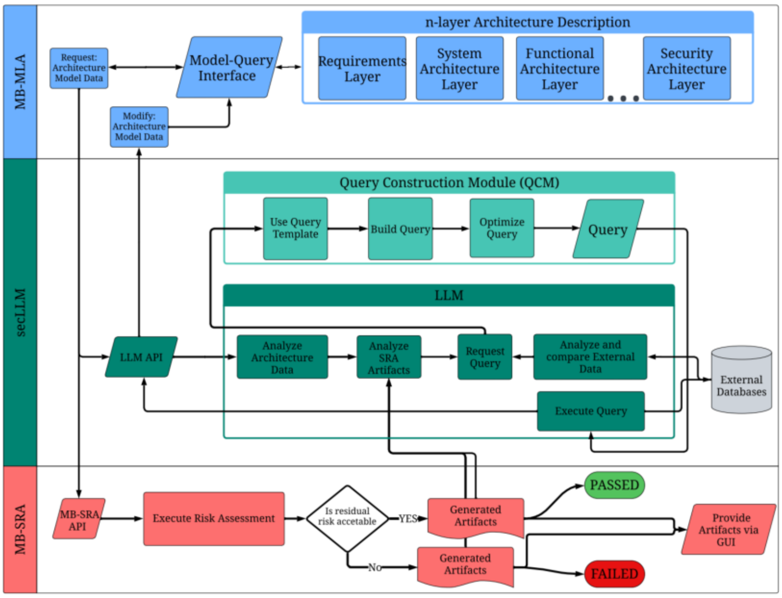
Tasks:

1. Familiarization
    - Model-based Systems Engineering (MBSE)
    - Query and prompt engineering
    - Cybersecurity
    - Cyber-Intelligence databases and API
2. Development of Query Templates
    - Define Use Cases of Query Construction Module
    - Definition of Query Template(s)
3. Development of Optimization Method
    - Definition of Optimization Metrics
    - Derivation of Optimization Method
4. Implementation of the QCM
    - Implement Query Templates and Optimization Method
5. Validation
    - Carry out the defined Use-Cases to demonstrate feasibility and validate the methods and Implementations
    - Evaluation of the results
6. Documentation and final presentation

Interested?

Mario Werthwein
mario.werthwein@ils.uni-stuttgart.de

Prof. Zamira Daw
zamira.daw@ils.uni-stuttgart.de



MB-MLA
Request: Architecture Model Data
Model-Query Interface
n-layer Architecture Description
Requirements Layer
System Architecture Layer
Functional Architecture Layer
...
Security Architecture Layer
Modify: Architecture Model Data
secLLM
Query Construction Module (QCM)
Use Query Template
Build Query
Optimize Query
Query
LLM
LLM API
Analyze Architecture Data
Analyze SRA Artifacts
Request Query
Analyze and compare External Data
Execute Query
External Databases
MB-SRA
MB-SRA API
Execute Risk Assessment
Is residual risk accetable
YES
No
Generated Artifacts
Generated Artifacts
PASSED
FAILED
Provide Artifacts via GUI