SCIENTIFIC CONTEXT

Modern distributed systems are increasingly complex, with multiple interconnected components, services, and autonomous agents interacting in dynamic environments. Ensuring their cybersecurity requires analysing potential attacks, understanding the strategies available to attackers and defenders, and verifying that critical security properties are preserved. Formal verification provides rigorous methods for addressing these challenges, allowing engineers to reason about system behaviours and establish mathematical guarantees. However, applying these techniques to realistic systems remains challenging. Verification problems can involve large state spaces and complex strategic interactions, while constructing formal models and specifying security properties often requires specialised expertise.

The VITAMIN-C (VerIficaTion of A MultI-ageNt system for Cybersecurity) project aims to address these challenges by combining formal verification with artificial intelligence. Building on VITAMIN, an existing modular model-checking platform for multi-agent systems, the project develops methods and tools for analysing cybersecurity properties in distributed and autonomous systems. Attackers and defenders are represented as agents with specific capabilities, objectives, and available actions. Their interactions are analysed using attack graphs, temporal and strategic logics, and model-checking techniques. The project also investigates how AI can improve the efficiency and accessibility of these verification processes.

A central objective of VITAMIN-C is to integrate AI techniques into the verification workflow. On the computational side, AI models will be investigated to guide the exploration of large state spaces and prioritise promising verification strategies. By learning from previously verified models and their associated results, these components can help identify relevant search directions and reduce the computational effort required by verification algorithms. On the usability side, the project explores AI-assisted interfaces that support engineers in constructing formal models and specifying security properties. These interfaces may exploit natural-language processing and large language models to interpret engineering descriptions, suggest formal representations, and assist users throughout the verification process. In both cases, the correctness of verification results remains the responsibility of the underlying formal methods, which validate the outcomes produced or suggested by AI components.

Within this context, the R&D engineer will contribute to the design, implementation, and evaluation of AI techniques for VITAMIN-C. The work will focus on developing AI components for verification guidance, investigating natural-language and LLM-based assistance for formal modelling, and integrating these capabilities into the existing platform. The engineer will also participate in the preparation of training and evaluation datasets, the development of experimental benchmarks, and the assessment of the proposed approaches in terms of effectiveness, computational efficiency, and reliability. The overall objective is to make formal verification more scalable and accessible while preserving the rigorous guarantees provided by the verification framework.

SKILLS AND EXPERIENCE

Essential knowledge, skills and experience:

- Strong knowledge of AI, Python programming, data processing/analysis and software engineering.
- Proficiency in English.
- Ability to train, evaluate, test and document AI components in a collaborative environment.

Desirable knowledge, skills and experience:

- Experience with deep learning, NLP/LLMs, graph learning, learning-guided search or ML model deployment.
- Interest in formal verification, cybersecurity, trustworthy AI, Docker and practical teaching.

Personal and professional abilities:

- Ability to work collaboratively in multidisciplinary teams.
- Ability to explain technical concepts and contribute to teaching activities.
- Strong organisational, analytical and problem-solving skills.
- Clear technical writing, communication and synthesis skills.