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 both potential attacks and the strategies that defenders can adopt in response. Attackers may exploit sequences of vulnerabilities to compromise a system, while defenders may react through countermeasures such as access restrictions, system reconfigurations, or Moving Target Defense mechanisms. Traditional cybersecurity analysis techniques often focus on identifying vulnerabilities and possible attack paths, with limited support for reasoning about the strategic interactions between attackers and defenders.

The VITAMIN-C (VerIficaTion of A MultI-ageNt system for Cybersecurity) project aims to address these challenges through formal verification. Building on VITAMIN, an existing modular model-checking platform for multi-agent systems, the project develops methods and tools for modelling and verifying 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. This approach allows the verification of security properties, such as the preservation of confidentiality and integrity, as well as the synthesis of defensive strategies against known attack scenarios.

A central challenge of the project concerns the scalability of formal verification when applied to realistic cybersecurity scenarios. To address this issue, VITAMIN-C investigates symbolic and abstract model-checking techniques, together with a modular architecture supporting the integration of different verification engines.

Within this context, the R&D engineer will contribute to the design, implementation, and evaluation of formal verification techniques for VITAMIN-C. The work will focus on formal modelling of cybersecurity scenarios, strategic model checking, development and optimisation of verification algorithms, and their integration into the existing platform. The engineer will also participate in experimental evaluations using cybersecurity benchmarks and industrial use cases, contributing to the development of a practical verification tool.

SKILLS AND EXPERIENCE

Essential knowledge, skills and experience:

- Strong knowledge of formal methods, transition systems, verification algorithms and software development.
- Ability to implement, test and document research software in a collaborative environment.
- Proficiency in English.

Desirable knowledge, skills and experience:

- Experience with temporal or strategic logic, model checking, symbolic methods, SAT/SMT or multi-agent systems.
- Experience in cybersecurity, attack graphs, Python/C++, Docker, distributed systems or practical teaching.

Personal and professional abilities:

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