Research Project

Supervisors: *Vadim Malvone*

Contact: vadim.malvone@telecom-paris.fr

Keywords: *Formal verification, Multi-Agent Systems, Cybersecurity*

Students required: *1*

Formal Methods for Strategic Reasoning in Cyber-Security Scenarios

Ensuring the correctness and resilience of complex systems represents a fundamental challenge in critical domains, where failures may lead to severe consequences. In cyber-security scenarios, systems evolve through continuous interactions between autonomous entities with potentially conflicting objectives, such as attackers attempting to compromise a network and defenders deploying mitigation strategies to preserve system integrity. Traditional evaluation approaches mainly rely on empirical testing or simulation-based experimentation. Although useful, these approaches cannot provide formal guarantees about system behavior under adversarial conditions.

Formal models of Multi-Agent Systems (MAS) provide a rigorous framework to describe and analyze strategic interactions among autonomous agents. By explicitly modeling agents, their available actions, and their strategic capabilities, it becomes possible to apply formal verification techniques such as model checking to prove safety and resilience properties with mathematical guarantees. This approach allows reasoning not only about system executions but also about what agents can enforce under different strategic configurations, going beyond purely observational or statistical evaluation methods.

In parallel, simulation environments for cyber-security research allow the study of attacker–defender interactions in controlled settings where automated agents interact with abstract representations of network infrastructures. These environments are often used to study adaptive adversaries and to evaluate defensive mechanisms under dynamic conditions. However, simulation-based approaches alone typically do not provide mechanisms to ensure that defensive strategies satisfy formally verified security properties.

Bridging formal verification methods with cyber-security simulation environments enables the systematic evaluation of defensive strategies supported by formal guarantees when deployed against intelligent adversaries. Such an integration allows validated defensive strategies to be executed within simulated environments, making it possible to assess their effectiveness under dynamic and adversarial conditions while preserving the rigor of formal reasoning.

The main objectives of this internship project are:

- Study formal models for representing attacker–defender interactions within multi-agent systems.
- Investigate formal verification techniques for reasoning about safety, resilience, and strategic capabilities of agents.
- Define mechanisms for translating formally verified strategies into executable defensive policies within simulated cyber-security scenarios.
- Explore extensions of strategic and temporal reasoning frameworks suitable for modeling adversarial interactions.

- Model representative cyber-security scenarios as multi-agent systems enabling the formal specification of security properties.
- Evaluate the proposed approach through experimental analysis comparing formally derived defensive strategies with adaptive adversarial behaviors in simulated environments.

The proposed framework will be evaluated through experimental analysis assessing the robustness and effectiveness of defensive mechanisms under adaptive adversarial behavior. By combining formal modeling, strategic reasoning, and simulation-based evaluation, the project aims to contribute toward methodologies in which defensive strategies can be both formally validated and experimentally assessed, enabling rigorous analysis of strategic interactions in complex and adversarial cyber environments.

Bibliography

[1] R. Alur, T.A. Henzinger, and O. Kupferman. Alternating-Time Temporal Logic. JACM, 49(5):672–713, 2002.

[2] E. M. Clarke, O. Grumberg, and D. A. Peled. Model Checking. MIT Press, 1999.

[3] A. Ferrando and V. Malvone: VITAMIN: A Compositional Framework for Model Checking of Multi-Agent Systems. CoRR abs/2403.02170 (2024).

[4] F. Mogavero, A. Murano, G. Perelli, and M. Y. Vardi. Reasoning About Strategies: On the Model-Checking Problem. TOCL, 15(4):34:1--34:47, 2014.