

EFFICIENT TRANSLATION OF CYBER-SECURITY SIMULATIONS INTO FORMAL GAME MODELS

SUPERVISORS

- Jean LENEUTRE / jean.leneutre@telecom-paris.fr
- Vadim MALVONE / vadim.malvone@telecom-paris.fr / [Homepage](#)
- PhD: David CORTES / david.cortes@telecom-paris.fr / [Homepage](#)

N. OF STUDENT PARTICIPANTS: 1-2

PROJET OBJECTIVES

Project context

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, which, although useful, 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 [2] 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.

The VITAMIN framework [3] is a compositional model-checking environment for multi-agent systems that enables the verification of safety properties expressed in formal logics for strategic reasoning [1,4]. In parallel, CyberBattleSim [5], an open-source cyber-security research platform developed by Microsoft, provides a simulation environment in which automated attackers interact with abstract network infrastructures. In its standard configuration, CyberBattleSim typically models attackers through reinforcement learning techniques, while defensive behaviors remain static or rule-based. Therefore, current simulation environments do not provide mechanisms allowing adaptive attackers to interact with defenders whose strategies are formally synthesized or validated through model checking.

Bridging formal verification frameworks and 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 realistic, simulated environments, making it possible to assess their effectiveness under dynamic and adversarial conditions while preserving the rigor of formal reasoning.

The proposed framework will be evaluated through experimental analysis assessing robustness and effectiveness of defensive mechanisms under adaptive adversarial behavior. By combining formal modeling, compositional verification, and realistic cyber-security simulation, 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.

Project objectives

A previous internship established a working translation from CyberBattleSim into formal models usable in VITAMIN. However, the resulting construction is costly by design. This project aims to optimize that pipeline while preserving correctness.

TASKS:

- Adapt and extend the VITAMIN framework to enable interoperability with the cyber-security simulation environment.
- Define mechanisms for translating cybersecurity games in Continuous CyberBattleSim [6] into correct and equivalent formal models, such as Concurrent Game Structures to be used in VITAMIN.
- Support these mechanisms via formal definitions that can be independently verified from the code implementation.

TECHNOLOGIES THAT WILL BE EXERCISED:

- Python.
- Jupyter Notebooks.
- LaTeX.
- Command-Line tools.

KNOWLEDGE AND SKILLS SOUGHT:

- Knowledge in programming languages and software engineering.
- General knowledge or interest in Cybersecurity, formal methods and strategic reasoning.

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
- [5] Microsoft Defender Research Team. *CyberBattleSim*. <https://github.com/microsoft/cyberbattlesim>. Created by Christian Seifert, Michael Betser, William Blum, James Bono, Kate Farris, Emily Goren, Justin Grana, Kristian Holsheimer, Brandon Marken, Joshua Neil, Nicole Nichols, Jugal Parikh, Haoran Wei. 2021
- [6] Franco Terranova, Abdelkader Lahmadi, and Isabelle Chrisment. “Scalable and Generalizable RL Agents for Attack Path Discovery via Continuous Invariant Spaces”. In: 2025 28th International Symposium on Research in Attacks, Intrusions and Defenses (RAID). 2025, pp. 440–457. DOI: 10.1109/RAID67961.2025.00029