M2 research internship on Verification of Attack Graph based Games

Institute: Telecom Paris, Institut Polytechnique de Paris

Research team and lab: Autonomous & Critical Embedded Systems (ACES), Information Processing and Communications Laboratory (LTCI)

Contacts:

Jean LENEUTRE (jean.leneutre@telecom-paris.fr)

Vadim MALVONE (vadim.malvone@telecom-paris.fr)

Disciplines: Cybersecurity, Formal Verification, Game Theory, Threat Modelling, Multi-agent system model checking.

Context and objectives:

A number of research studies attempt to propose semi-formal or formal models of security threats corresponding to multi-step attack scenarios. Amongst those, one of the most used formalism to model and reason about these attacks scenarios is *Attack Graphs* (for a recent survey, see for instance [Kay2016].

This graph is generated given a description of the system architecture (topology, configurations of components, etc.) together with the list of existing vulnerabilities, the attacker's profile (his capability, passwords knowledge, privileges, etc.) and attack templates (attacker's atomic action, including preconditions and postconditions). An attack path in the graph corresponds to a sequence of atomic attacks. Attack graphs can then be used to perform security analysis both offline (computation of security metrics, selection of an optimal security hardening policy) or online (ongoing attack scenario prediction).

In the latter case of an online scenario, few works address a more dynamic analysis trying to capture interactions between an (or several) attacker(s) and a defender in order to ease the selection of reactive security countermeasures.

The goal of this internship is to address the problem of dynamic selection security countermeasures using an approach based on game theory and multi-agent system verification.

Game theory in AI is a powerful mathematical framework to reason about reactive systems. The latter are characterized by an ongoing interaction between two or more entities, called players, and the behavior of the entire system deeply relies on this interaction. Game theory has been largely investigated in a number of different fields such as economics, biology, and computer science, and more recently cybersecurity [AB2010].

An important application of game theory in computer science and, more recently, in AI, concerns formal-system verification. In particular, game theory has become a powerful tool for the verification of reactive systems and embedded systems. This story of success goes back to the late seventies with the introduction of the model checking technique [CGP99]. The idea of model checking in order to check whether a system satisfies a desired behavior is to check whether a mathematical model of the system meets a formal specification. For the latter, temporal logics, such as LTL and CTL, are generally used. First applications of model checking just concerned closed systems, which are characterized by the fact that their behavior is completely determined by their internal states. However, in practice as of the systems are open in the sense that they are characterized by an ongoing interaction with other systems. To overcome this problem, model checking has been extended to multi-agent systems. Breakthrough contributions along this direction concern the introduction of logics for the strategic reasoning such as Alternating-time Temporal Logic (ATL) [AHK02], Strategy Logic (SL) [MMP14], and their extensions. Verification tools such as PRISM-game [CFK2012] or MCMAS [LR2006] allow to encapsulate the behavior of several agents interacting in a cooperative or non-cooperative way, and aiming at a certain goal.

Tasks:

The tasks of this internship are divided into three macro steps:

1. Study the state of the art on formal verification for multi-agent systems and on attack graphs.

2. Find an optimal approach to handle attack graphs in formal verification on Multi Agent System.

3. Develop a tool that handles the new proposed approach.

Desirable Skills: one or more **of the following**

- Cybersecurity, threat modelling.
- Formal verification, model checking.
- Game theory.

Other information:

The internship will be located at Télécom Paris in Palaiseau (40mn south of the center of Paris by public transport). It is expected that the work initiated during the internship will be continued in the framework of a PhD.

How to apply?

Applicants should send an electronic archive to vadim.malvone@telecom-paris.fr and jean.leneutre@telecom-paris.fr containing the following:

- a letter of motivation,
- a detailed CV,
- post-baccalaureate transcripts (at least M1 and available results for M2 or equivalent) indicating, as far as possible, the ranking in the class,
- a document (study project report, article, etc.) written in English (if not in French) describing one of your contributions in the field of computer science and networks.

References:

[AB2010] Alpcan, T., & Başar, T. (2010). Network security: A decision and Game-Theoretic approach. Cambridge University Press.

[AHK02] R. Alur, T.A. Henzinger, and O. Kupferman. Alternating-Time Temporal Logic. JACM, 49(5):672–713, 2002.

[CFK2012] Chen, T., Forejt, V., Kwiatkowska, M., Parker, D., & Simaitis, A. (2012). Automatic Verification of Competitive Stochastic Systems. *TACAS*.

[CGP99] E. M. Clarke, O. Grumberg, and D. A. Peled. Model Checking. MIT Press, 1999.

[Kay2016] K. Kaynar. A taxonomy for attack graph generation and usage in network security. J. Inf. Secur. Appl., 29(C):27–56, aug 2016.

[LR2006] A. Lomuscio and F. Raimondi. MCMAS: A Model Checker for Multi-agent Systems". In: Tools and Algorithms for the Construction and Analysis of Systems. Ed. By Holger Hermanns and Jens Palsberg. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 450-454.

[MMP14] 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.