Projet M2 Cyber - 2025
Better attack graphs through better formal attack dynamics

Dylan Marinho (Sorbonne Université/LIP6),
Thomas Robert (Telecom Paris/LTCI)

September 2025

1 Motivation and context

Securing a system requires that the threat to be dealt with is understood in order to define priorities and also to avoid overseen attack vectors. In order to ease the identification of applicable threats, Logical Attack Graph (LAG) formalisms appeared promising in past two decades[Tay+23]. Even if they are quite useful, their interest is often questioned due to two main issues: the difficulty to automate the integration in such formalisms of the latest attack scenarios, and the difficulty to actually interpret them at scale.

Indeed, the incentive to be as exhaustive as possible make it difficult to sort out irrelevant threat scenarios from critical ones. Yet, this difficulty come also from the multiplication of independent possible attack outcome that create artificial complexity. Different approaches have been proposed to ease automated processing of knowledge based provided in structured natural language (SNL). We are strongly interested in those approaches. Yet, the mapping of SNL description to logical attack graph concept need to be refined especially to cope with the variable level of detail provided in SNL description not always compatible with very detailed modelling provided in LAG like in [Sai+24]. We would also consider joint consequences of attacker elementary action to avoid the apparent complexity that seem to surge as soon as an attack has multiple outcome or consequences that are impossible to achieve separately. This situation is particularly true in the presence of detection mechanisms [Guz+17].

2 Proposed approach

We propose to investigate adaptations or extensions of classical Mulval syntax to provide better modelling of attack logic, and/or improving existing generation pipelines. Hence, the following work plan is proposed:

- Improve formalization of attack propagation, distinguish knowledge refinement, contextual information. Define the base concept to define joint consequences of one attacker action. Investigate how to better model complex attack scenarios in which one action grant many capabilities to simplify attack graphs definition.
- propose a generation logic of attack hypergraph that account for joint consequences (e.g. running a new code but being logged). Make a survey of joint attack step consequences that could be combined to represent more realistic attack dynamics.
- Define different use cases based on historical attacks or attacks mimicking them.

References

[Guz+17] Antonella Guzzo et al. "Malevolent Activity Detection with Hypergraph-Based Models". In: *IEEE Transactions on Knowledge and Data Engineering* 29.5 (2017), pp. 1115–1128. DOI: 10.1109/TKDE.2017.2658621.

[Tay+23] David Tayouri et al. "A survey of MulVAL extensions and their attack scenarios coverage". In: *IEEE Access* 11 (2023), pp. 27974–27991.

[Sai+24] Kéren Saint-Hilaire et al. "Automated Enrichment of Logical Attack Graphs via Formal Ontologies". In: *ICT Systems Security and Privacy Protection*. Ed. by Norbert Meyer and Anna Grocholewska-Czuryło. Cham: Springer Nature Switzerland, 2024, pp. 59–72. ISBN: 978-3-031-56326-3.