Adversary Tactic Driven Scenario and Terrain Generation with Partial Infrastructure Specification

Ádám Ruman, Martin Drašar, Lukáš Sadlek, Shanchieh Jay Yang, Pavel Čeleda
Cybersecurity Training

- Education (Cyber Defense Exercise).

- Autonomous agents (reinforcement-learning-based AI solutions).
Training Content Creation

- **Scenarios** - the possible decision sequences the trainee can learn. (the story)

- **Terrains** - an environment where the scenario can be executed. (the world)

- Manual creation is too expensive and inefficient, and we need myriads of them.
Can we feasibly synthesize training content that is verifiably correct, complete, and realistic?
Prerequisite I - Adversary Framework

- Adversary Control State (ACS) to represent attack posture.

- **Quiver** – an enhancement of MITRE ATT&CK, allowing logically sound chaining of its techniques.

- 53 actions, some representing multiple ATT&CK techniques, others only a phase of them.

- Applicability depends on the ACS, application changes the ACS.
Prerequisite II - Terrain Model

- We need to encapsulate the technical details of an infrastructure.
- Heavy interplay with the ACS.
- Must be fitting as a configuration for actual deployment.
Generation Algorithm

- Concurrent terrain and scenario generation – alternatingly scheduled work packages of both.

- Inputs
  - Setting up limitations for the whole synthesis.

- Terrain skeleton
  - Obeying the inputs and industry best practices.

- Scenario
  - State exploration limited by the terrain skeleton and inputs.

- Finalization
  - Choosing successful paths, cutting back the scenario.

- Mining & Serialization
  - The scenario and skeleton is transformed into a system configuration.
Executability Evaluation

- **Split**
  - Consider the terrain and scenario to be totally unrelated.

- **Create a twin scenario**
  - Use a 3rd party attack graph generation tool on the terrain to obtain a new scenario.

- **Lossless transformation**
  - The two scenarios are transformed into a uniform format.

- **Compare**
  - Use graph matching to compare the original scenario and its twin.
Results

– The executability evaluation yields positive results: the generated scenario and terrain pairs correspond well. The adversary framework does not allow logical errors. Correctness ✓

– State exploration considers all possibilities. Completeness ✓

– With artificial limitations of the synthesis, it creates scenarios matching historical APT attacks. Realism ✓
Future Work

- Concurrent state exploration.

- Memory optimizations.

- Model enhancements (to include more details without complicating the computations).
Stay in Touch

Ádám Ruman

ruman@{ics, fi}.muni.cz
LinkedIn, Google Scholar