Dynamic Cyberattack Simulations with DynaMAL

Viktor Engström
vengs@kth.se

May 12, 2023

1 Abstract

Attack graph models and subsequent analyses often assume that their models are static. However, real IT environments and cyberattacks are dynamic. For example, environments can change when devices move or configurations change. That is, as elements are added, removed, or rewired. The cyberattack, in turn, emerges from an interplay between attackers and targets. Specifically how:

1. Attackers interact with and change environments,
2. Changing conditions affect the attacker.

We present the Dynamic Meta Attack Language (DynaMAL), a graph-oriented modeling and simulation metalanguage to analyze how the attacker-environment dynamic produces attacks. DynaMAL works with a combination of multi-layered and dynamic graphs to replicate both attacker interactions and changing environments. DynaMAL itself specifies the domain-specific modeling rules and simulation logic. When executed, DynaMAL simulation models present an attacker agent with the current potential actions according to the simulation logic. As the attacker progresses through the simulation, every choice is recorded to incrementally grow the attack graph.