

Presentation abstract for SWITS 2021

Presenter's name: Sotirios Katsikeas, PhD Student @ KTH Royal Institute of Technology

Presentation type: Previously accepted conference paper

Title: An attack simulation language for the IT domain

Full authors: Sotirios Katsikeas, Simon Hacks, Pontus Johnson, Mathias Ekstedt, Robert Lagerström, Joar Jacobsson, Max Wällstedt, and Per Eliasson

Abstract:

Cyber-attacks on IT infrastructures can have disastrous consequences for individuals, regions, as well as whole nations. In order to respond to these threats, the cyber security assessment of IT infrastructures can foster a higher degree of security and resilience against cyber-attacks. Therefore, the use of attack simulations based on system architecture models is proposed. To reduce the effort of creating new attack graphs for each system under assessment, domain-specific languages (DSLs) can be employed. DSLs codify the common attack logics of the considered domain.

Previously, MAL (the Meta Attack Language) was proposed, which serves as a framework to develop DSLs and generate attack graphs for modeled infrastructures. In this article, we propose coreLang as a MAL-based DSL for modeling IT infrastructures and analyzing weaknesses related to known attacks. To model domain-specific attributes, we studied existing cyber-attacks to develop a comprehensive language, which was iteratively verified through a series of brainstorming sessions with domain modelers.

Finally, this first version of the language was validated against known cyber-attack scenarios.