Presentation abstract for SWITS 2023

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

Presentation type: Longer paper presentation

Title: Development and Validation of a Threat Modeling Language for the IT domain

Full authors: Sotirios Katsikeas, Andrei Buhaiu, Preetam Mukherjee, Mathias Ekstedt and Simon Hacks

Abstract:

ICT infrastructures are getting more and more complex and defending them against cyber attacks is proving to be a cumbersome task. As cyber threats continue to increase and expert resources are limited, organizations need to find more efficient ways to evaluate their resilience and take proactive measures. Threat modelling is an excellent method of assessing the resilience of ICT systems, for example by forming Attack Graphs that illustrate an adversary's attack vectors. Previously, MAL (the Meta Attack Language) was proposed, which serves as a framework to develop Domain Specific Languages (DSLs) and generate Attack Graphs for modeled infrastructures. coreLang is a MAL-based threat modelling language that utilizes Attack Graphs to enable attack simulations and security assessments. This paper presents the first release version of coreLang in which MITRE ATT&CK tactics and techniques are mapped into coreLang to serve as a validation and identify strengths and weaknesses to benefit the development cycle.