ONTOLOGY-BASED ATTACK GRAPH ENRICHMENT

Keren Saint-Hilaire
Télécom SudParis[1]
keren.saint-hilaire@telecom-sudparis.eu

Frédéric Cuppens and Nora Cuppens-Boulahia
Polytechnique Montréal[2]
frederic.cuppens@polymtl.ca; nora.boulahia-cuppens@polymtl.ca.

Joaquin Garcia-Alfaro
Institut Polytechnique de Paris[3]
joaquin.garcia_alfaro@telecom-sudparis.eu

Abstract - Academic paper.

Attack graphs provide a representation of possible actions that adversaries can perpetrate to attack a system. They are used by cybersecurity experts to make decisions, e.g., to decide remediation and recovery plans. Different approaches can be used to build such graphs. We focus on logical attack graphs, based on predicate logic, to define the causality of adversarial actions. Since networks and vulnerabilities are constantly changing (e.g., new applications get installed on system devices, updated services get publicly exposed, etc.), we propose to enrich the attack graph generation approach with a semantic augmentation post-processing of the predicates. Graphs are now mapped to monitor alerts confirming successful attack actions and updated according to network and vulnerability changes. As a result, predicates get periodically updated, based on evidence about attack and ontology enrichment. This allows to verify whether changes lead the attacker to the initial goals or to cause further damage to the system not anticipated in the initial graphs. We illustrate the approach under the specific domain of cyber-physical security affecting smart cities. We validate the approach using existing tools and ontologies.

Keywords: Cybersecurity, Alerts Vulnerabilities, Attack Graphs, Security Information and Event Management, Ontologies

[1] 9 rue Charles Fourier, 91011 Evry Cedex/19 place Marguerite Perey, 91120 Palaiseau, France
[2] 2500, chemin de Polytechnique, Montreal (Quebec) H3T 1J4, Canada
[3] 5 Av. Le Chatelier 2ème étage, 91764 Palaiseau, France