UNIVERSITY OF SKÖVDE

COMBITECH

EUROPEAN UNION
Internal Security Fund ISF

Dynamic and Automatic Vulnerability Assessment for Cyber-Physical System

Abstract:

Assessing vulnerabilities supports analytics-based decision-making processes to protect Critical Infrastructures (CIs), in order to focus on specific risks rising from threat-exploitability with varying degrees of impact-severity. The notion of risk remains elusive, as evidenced by the increasing investigations on CIs security operations centres (SOCs) where analysts employ various detection, assessment, and defence mechanisms to monitor security events. Normally, SOCs involve advances of multiple automated security tools such as network vulnerability scanners and Common Vulnerability Scoring System (CVSS), combined with analysis of data contained and produced by CPS as well as alarms retrieved from vulnerability repositories such as Common Vulnerability Exposure (CVE). The security operators need further to forecast the match between these vulnerabilities and the state of intricate CIs layer networks, while prioritising patching investments using vulnerability-scoring mechanisms. This process shows the central role of security operators in SOCs and their need for support to keep pace with dynamically evolving vulnerability-alert repositories. Recent advances in data analytics also prompt dynamic data-driven vulnerability assessments whereby data contained and produced by CPS include hidden traces of vulnerability fingerprints. However, the huge volume of scanned data requires high capability of information processing and analytical reasoning, which could not be satisfied considering the imprecise nature of manual vulnerability assessment.

A knowledge-base system that consolidates both sides into empirical rules appears to be missing, yet it promises to offer a suitable level of decision-support. In our research, we propose to target on a dynamic and automated vulnerability-assessment approach. The proposed streamlined approach employs computational intelligence techniques to analyse data retrieved from vulnerability-alert repositories and CPS layer networks within an innovative accurate and automatic scoring system, away from traditional manual and highly subjective mechanisms. Our approach suggests to substitute offline, costly, error-prone and pure subjective vulnerability assessment processes with an automatic, accurate and data-evidenced approach, to improve situation awareness (SA) and to support security decision making. In doing so, we investigate judicious computational-intelligence techniques such as fuzzy-logic, machine learning and data mining, applied to vulnerability assessment problems.

Presenter: Yuning Jiang, PhD student in Informatics in Högskolan i Skövde.

Related Project: ELVIRA.

This research has been supported in part by the EU ISF Project A431.678/2016 ELVIRA (Threat modeling and resilience of critical infrastructures), coordinated by Polismyndigheten/Sweden.