TestCat

Automated Testbeds for the Evaluation of Intrusion Detection Capabilities

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIras Kooperative CS F&E Projekte (KFE CS_2022)	**Status**	laufend
Projektstart	01.02.2024	**Projektende**	31.01.2027
Zeitraum	2024 - 2027	**Projektlaufzeit**	36 Monate
Keywords	Angriffserkennung, Testumgebung, Evaluierung, Infrastrukturmodellierung, Netzwerkscanning		

Projektbeschreibung

Kritische Infrastrukturen sind Ziel des geopolitischen Cyberkriegs geworden; fast täglich kommt es zu Hackerangriffen durch staatliche Akteure oder kriminelle Gruppen. Der Einsatz von Abwehrmechanismen wird essenziell, jedoch hängt deren Erkennungsfähigkeit stark von der Qualität verwendeter Indicators-of-Compromise (IoC) und Konfigurationen ab. Da existierende Angriffserkennungssysteme allerdings auf Business-IT fokussieren, kritische Infrastrukturen jedoch über spezielle Systemlandschaften mit hohem Betriebsleittechnik-Anteil (Operational-Technology, OT) verfügen, ist das Risiko unerkannter Angriffe mit weitreichenden Auswirkungen auf die Bevölkerung, aber auch kostspieliger Fehlalarme, trotz bestehender Abwehrmechanismen hoch. Als Konsequenz wird derzeit in Österreich ein staatliches Frühwarnsystem für Betreiber wesentlicher Dienste umgesetzt; für den effektiven Betrieb eines solchen Systems fehlen jedoch Lösungen zur Messung und Bewertung der Fähigkeiten eingesetzter Erkennungsmechanismen sowie deren Indicators-of-Compromise und Konfigurationen für eine evidenzbasierte Validierung, Auswahl, und Konfiguration dergleichen. TestCat verfolgt deshalb die zielgerichtete Erstellung flexibler Testumgebungen, die eine objektive und nachvollziehbare Evaluierung von Angriffserkennungssystemen ermöglichen. Anders als bestehende Testumgebungen, die aufgrund deren statischer Architektur schnell an Aktualität verlieren und nur für bestimmte Anwendungsfälle geeignet sind, nutzt TestCat ein modellgetriebenes Konzept zur automatischen Erstellung einer Vielzahl von diversen Testumgebungen, die gemeinsam eine breitflächige Abdeckung verschiedenster Anwendungsdomänen erlauben. Die in TestCat entwickelten Lösungen zur Testumgebungserstellung zeichnen sich außerdem durch eine hohe Flexibilität, die kontinuierliche Anpassungen gemäß den sich ständig ändernden Systemlandschaften und Angriffstechniken ermöglicht, eine komplexe Simulation von normalem Nutzerverhalten, eine Auswahl relevanter Angriffsvektoren, sowie eine Integration von OT-Komponenten aus. Die juristische Begleitung der Systementwicklung hinsichtlich Datenschutz runden das Projekt ab und stellen eine spätere problemlose Anwendung aus rechtlicher Sicht sicher.

Abstract

Critical infrastructures have become main targets in geopolitical cyberwarfare as intrusions and other attacks against them are carried out by state actors and criminals almost every day. Effective defense mechanisms are thus crucial, however, their capabilities to detect cyber-attacks strongly depend on the quality of available Indicators-of-Compromise (IoC) as well

as detector configurations. Unfortunately, vendors generally design intrusion detection systems towards protection of enterprise IT rather than system environments of critical infrastructures that commonly involve specialized hardware and a significant share of Operational Technology (OT). This causes that the risks of facing undetected attacks on critical infrastructures with large-scale adverse impacts to the population, as well as costly false alarms, remains high. Consequently, Austrian authorities are currently preparing a national early-warning system for operators of essential services, however, solutions that enable measurement and assessment of detection capabilities of deployed mechanisms, including their respective Indicators-of-Compromise and configurations, for an evidence-based validation, selection, and configuration thereof, are still missing. TestCat therefore aims to generate flexible test environments that allow objective and replicable evaluations of intrusion detection systems. Other than existing testbeds that are designed for single-use and quickly become outdated due to their rigid design, TestCat leverages model-driven techniques to automatically produce a large number of diverse test environments that collectively cover a wide area of different application domains. Thereby, TestCat's testbed generation procedures ensure high flexibility to enable perpetual adaptation for continuously changing system landscapes and attack techniques, sophisticated simulation of user behavior, selection of relevant attack vectors, and an integration interface for OT components. Ongoing legal advisory for all developments throughout the project runtime ensures that solutions comply with statutory requirements and enables smooth transition to productive operation in real-world applications.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- CD Security Technologies GmbH
- Wiener Zentrum für Rechtsinformatik/Vienna Centre for Computers and Law, kurz: WZRI/VCCL
- VERBUND AG
- Bundesministerium für Inneres
- Salzburg AG für Energie, Verkehr und Telekommunikation
- LINZ STROM GAS WÄRME GmbH für Energiedienstleistungen und Telekommunikation
- Autobahnen- und Schnellstraßen- Finanzierungs-Aktiengesellschaft
- Bundeskanzleramt
- Deutsche Telekom Cyber Security Austria GmbH
- SBA Research gemeinnützige GmbH